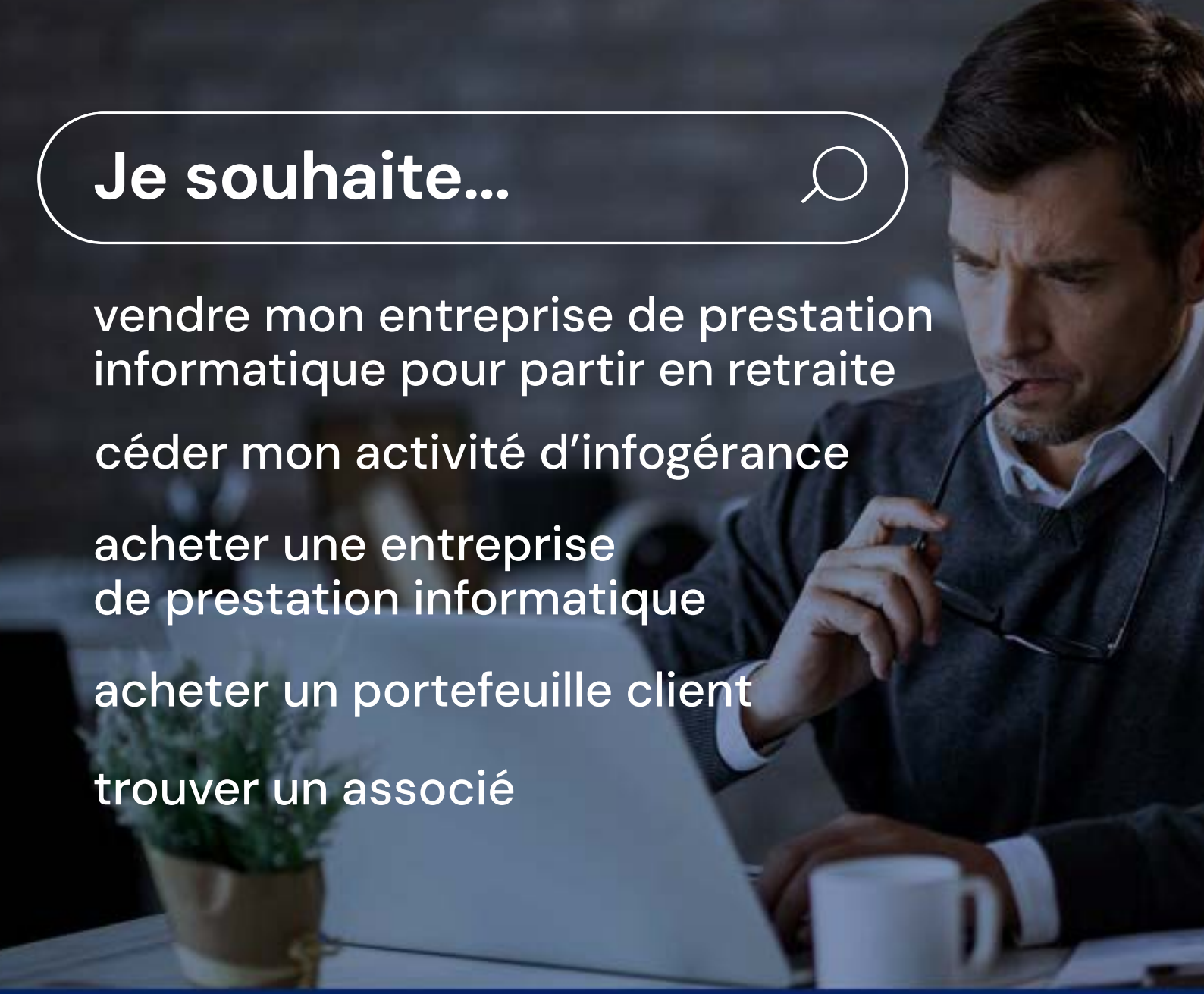
GUIDE DU MSP

Le référentiel des solutions
de la prestation informatique

2026 - 2027

ndnm.



Je souhaite...

vendre mon entreprise de prestation informatique pour partir en retraite

céder mon activité d'infogérance

acheter une entreprise de prestation informatique

acheter un portefeuille client

trouver un associé

artaban.me

La plateforme de mise en relation entre cédants et acquéreurs dans le secteur de la **prestation informatique.**

Scannez le QR Code pour être recontacté

0% **Pas de frais sur la vente,** vous ne payez que la mise en relation.

Totalement anonyme : C'est vous qui acceptez les demandes de mise en relation.

Pourquoi avons-nous conçu ce guide ?

Malgré l'essor de l'intelligence artificielle, obtenir une vision d'ensemble des solutions informatiques et de cybersécurité disponibles sur le marché n'a jamais été aussi compliqué.

Au gré des développements internes et des acquisitions, les éditeurs adoptent tour à tour des stratégies dites "de plateformes", intégrant au sein d'une même interface gestion de l'EDR, de la sauvegarde, de la sécurité de la messagerie et de la gestion des identités et des accès.

Pour les prestataires informatiques, la veille devient complexe : quelle solution choisir ? Vaut-il mieux assembler plusieurs outils ou opter pour une interface unifiée ?

Notre étude de marché Panorama de la prestation informatique 2025 a démontré que 40% des entreprises françaises sondées n'avaient toujours pas adopté le modèle MSP. Si certains automatisent déjà le traitement des tickets grâce à l'IA, d'autres n'ont pas encore été sensibilisés aux solutions RMM, PSA ou de gestion documentaire. Quant aux distributeurs, un prestataire sondé ne collabore en moyenne qu'avec 4 à 5, dont 2 pour l'achat de matériel, un chiffre faible au regard de la variété des acteurs présents sur le marché et de leurs spécialisations. En conséquence, le prestataire s'enferme dans un écosystème restreint et passe à côté d'opportunités lui permettant d'améliorer sa rentabilité.

Depuis bientôt six ans, NDNM accompagne les prestataires informatiques dans leurs enjeux commerciaux et marketing. Cette position d'observateur privilégié nous a permis de constater que le choix des éditeurs se fait quasi exclusivement à travers le prisme des fonctionnalités produits, sans prise en compte du programme partenaire associé. Or, dans un marché où de nombreuses solutions sont fonctionnellement très proches, la qualité d'un programme partenaire peut constituer un levier de croissance et une aide au développement : accompagnement commercial, génération de leads, co-marketing, formation, support, conditions financières... Autant d'éléments encore trop souvent méconnus.

C'est pour répondre à ce manque de visibilité que nous avons conçu cette première édition du Guide du MSP. Un référentiel de plus de 150 pages, offrant une vision du marché neutre, structurée et indépendante. À travers 20 catégories et plus de 100 pages de solutions, chaque fiche présente les fonctionnalités clés du produit et son programme partenaire, accompagnée d'un QR code pour vous permettre de demander une démonstration. Le tout conçu pour vous faire gagner du temps et comparer, en un coup d'œil, l'essentiel.

Ce guide est donc le vôtre. Posez-le sur votre bureau, consultez-le pour un nouveau besoin client, feuilletez-le pour challenger vos choix technologiques. Griffonnez-le, annotez-le, partagez-le avec vos équipes : c'est précisément pour cela qu'il a été imprimé.

Bonne lecture.

sommaire

Après une décennie de modèle MSP, un nouveau chapitre s'ouvre pour les acteurs de la prestation informatique

Apparu initialement aux États-Unis, le modèle MSP (Managed Services Provider) s'impose progressivement en Europe à partir de 2016, avant de se diffuser sur le continent africain quelques années plus tard.

Son objectif initial était simple : faire évoluer la prestation informatique traditionnelle d'un mode curatif, payé à l'intervention, vers un mode préventif, facturé par utilisateur et par mois.

Fini les devis techniques incompréhensibles facturés au doigt mouillé. Le prestataire propose désormais un abonnement mensuel par utilisateur, permettant au client de comprendre ce qu'il paie. En standardisant son offre sur l'ensemble de son portefeuille clients, il gagne en efficacité et évite de gérer des environnements hétérogènes, sources de complexité et de fragilité dans le maintien opérationnel quotidien.

Côté budget, le changement est tout aussi significatif pour le client final : au lieu de subir des coûts de déplacement et d'intervention qui s'accumulent d'un trimestre à l'autre, il dispose d'une ligne de dépense stable et prévisible.

Sur le terrain, la transformation est tangible. Un technicien qui se déplaçait autrefois chez le client pour résoudre chaque incident gère aujourd'hui en moyenne 300 postes de travail à distance. Si cette performance est louable pour la marge du prestataire (le ratio du nombre de postes gérés par technicien s'améliore et les coûts de déplacement se réduisent), elle implique néanmoins un accompagnement au changement dans la relation avec le client final.

Habitué à la présence physique du technicien dans ses locaux, ce dernier associait naturellement la résolution de ses problèmes à cette proximité. Avec le modèle MSP, la majorité des actions s'effectue désormais à distance. La demande, autrefois en partie informelle, transite exclusivement par e-mail, chabot ou par téléphone, ce qui peut générer un sentiment de friction et une perte de proximité dans la relation.

Présenté sous la forme d'un document de synthèse, le QBR donne accès à trois catégories d'indicateurs :

Performance du support
nombre de tickets traités sur la période, temps de réponse moyen, temps de résolution moyen sur 15 jours, catégorisation des demandes.

Gestion proactive du parc informatique
fin de période de garantie, machines à renouveler prochainement.

Risques cyber
nombre d'e-mails bloqués, nombre de malwares détectés, comportements à risque au sein de l'entreprise, équipes et collaborateurs les plus ciblés, incidents de sécurité détectés.

Au-delà de la mise en valeur du travail accompli, le QBR constitue un levier de développement commercial pour le MSP. En conseillant son client sur l'actualité réglementaire et les tendances technologiques émergentes comme l'automatisation ou l'intelligence artificielle, il ouvre le champ des possibles et peut déclencher de nouveaux projets et investissements.

Le MSP : un modèle exigeant qui impose une profonde transformation

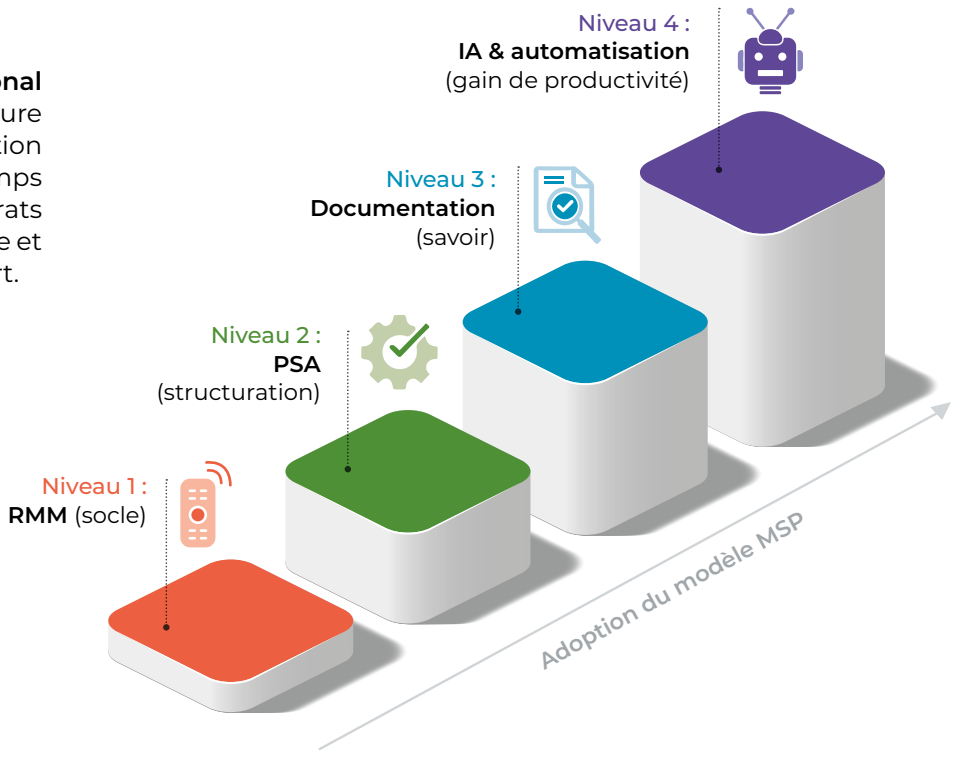
Pour opérer la transition vers un modèle fondé sur la prévention et l'anticipation, les prestataires informatiques doivent transformer leur socle technologique en y intégrant un ensemble de solutions spécifiques, communément appelé la « stack MSP ».

Cette stack repose sur deux principaux logiciels. Le premier est le **RMM (Remote Monitoring and Management)**, qui assure la gestion à distance des postes de travail, des terminaux mobiles et des serveurs. Ses fonctionnalités couvrent la supervision en temps réel des systèmes d'exploitation, la gestion automatisée des mises à jour (patch management), la prise en main à distance, l'inventaire matériel et logiciel du parc, le déploiement de scripts et de politiques de sécurité, ainsi que la détection d'anomalies via des alertes configurables. Le RMM constitue la colonne vertébrale de l'activité quotidienne du MSP : c'est depuis cette console que le technicien administre l'ensemble des environnements clients.

Le second est le **PSA (Professional Services Automation)**, qui structure l'ensemble des processus de gestion du prestataire : suivi du temps d'intervention, gestion des contrats et licences, facturation récurrente et traitement des tickets de support.

En pratique, le RMM est le produit le plus répandu, car indispensable au quotidien. Le PSA, en revanche, exige un niveau de maturité organisationnelle plus élevé. Son intégration impose au MSP de cartographier l'ensemble de ses processus existants (gestion des tickets, escalades, onboarding et offboarding client, suivi du temps), puis d'y migrer l'intégralité de ses données : clients, contrats, licences, inventaires de produits et solutions commercialisées.

À cela s'ajoute la connexion du PSA avec son environnement immédiat : RMM, outils de facturation, solutions de sauvegarde, de cybersécurité et CRM. L'optimisation des workflows de gestion des tickets et la mise en place de tableaux de bord de suivi deviennent alors un prérequis opérationnel.



À ces deux premiers outils s'ajoutent deux briques complémentaires :

La gestion de la documentation : un outil centralisé de gestion des connaissances (mots de passe, procédures, configurations réseau, fiches clients), qui garantit la continuité de service en créant un espace d'intelligence collective. Les échanges informels laissent place à une culture du savoir partagé : chaque information est documentée, structurée et accessible à l'ensemble de l'équipe technique, réduisant la dépendance à un technicien qui détiendrait seul l'historique client.

Les outils d'intelligence artificielle et d'automatisation : cette brique, plus récente, se greffe sur la stack MSP pour réduire le travail manuel et accélérer le traitement des demandes. Deux catégories de solutions se distinguent.

La première concerne **l'automatisation des workflows opérationnels**. Ces plateformes permettent au MSP de connecter l'ensemble de ses outils comme le PSA, RMM, les environnements clients Microsoft 365 et Google Workspace ou les solutions de cybersécurité dans le but d'automatiser les tâches répétitives sans écrire une ligne de code. Onboarding d'un nouvel utilisateur, réinitialisation de mot de passe, escalade de ticket, attribution de licences : ces actions, autrefois réalisées manuellement, sont désormais orchestrées à travers des workflows visuels déployables sur l'ensemble du portefeuille clients.

La seconde concerne **l'intelligence artificielle appliquée au service desk.** Ces solutions positionnent l'IA au point d'entrée de la relation client, directement dans Microsoft Teams ou Slack. Lorsqu'un utilisateur formule une demande dans son canal de messagerie habituel, l'IA trie automatiquement le ticket, le catégorise, le priorise et collecte les informations nécessaires avant même qu'un technicien n'intervienne. Le temps de résolution s'en trouve considérablement réduit, et l'enregistrement du temps passé se fait automatiquement dans le PSA.
La combinaison des deux ouvre la voie à ce que le marché appelle la résolution « zero-touch » : une demande formulée par l'utilisateur final, traitée de bout en bout sans intervention humaine. Ce niveau d'automatisation, encore émergent, préfigure la prochaine évolution de la stack MSP.

Si ces briques ne concernent aujourd'hui que les MSP les plus matures, leur généralisation pourrait redessiner les organisations en supprimant purement et simplement le support de niveau 1 dans les équipes techniques avec, à la clé, un gain opérationnel significatif et une pression à la baisse sur les prix du marché.

> “La combinaison des deux ouvre la voie à ce que le marché appelle la résolution « zero-touch »”

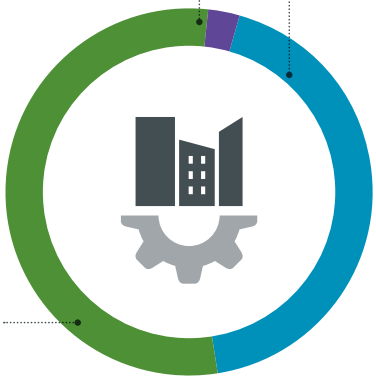
Vers une inévitable transformation du modèle MSP

Notre étude de marché « Panorama de la prestation informatique en France », publiée en 2025, dressait un constat révélateur : seuls 60,55% des prestataires informatiques interrogés déclarent utiliser une solution RMM. Une décennie après l'émergence du modèle MSP en Europe, son adoption reste partielle et inégale.

Un marché à trois vitesses

L'analyse fait apparaître trois profils d'acteurs aux niveaux de maturité très différents.

Les pure players MSP (environ 3% du panel)
Ces structures, généralement récentes, ont adopté le modèle MSP dès leur création. Souvent fondées par d'anciens techniciens souhaitant lancer leur propre activité, elles comptent rarement plus de cinq salariés mais affichent un niveau de maturité élevé sur l'ensemble de la stack. Leur avantage est structurel : en partant d'une feuille blanche, elles n'ont pas le poids d'un historique organisationnel à transformer. Cette agilité leur permet d'industrialiser rapidement leurs offres et de se positionner avec des processus optimisés dès le départ.



Les MSP en devenir (environ 43% du panel)
Ce dernier groupe rassemble les prestataires traditionnels souvent issus du monde de la bureautique qui fonctionnent encore sur un modèle curatif : intervention sur site, facturation à l'acte, relation de proximité. Ces acteurs disposent d'un portefeuille clients établi mais doivent engager une transformation en profondeur, technologique, commerciale et organisationnelle, pour migrer vers le modèle MSP. Le chemin est long, car il ne s'agit pas seulement d'adopter un outil, mais de repenser l'ensemble de la chaîne de valeur.

Les MSP hybrides (environ 54% du panel)
Cette catégorie regroupe les prestataires ayant intégré une partie du modèle, souvent le volet commercial (abonnement mensuel) ou quelques briques technologiques (RMM), sans avoir basculé l'ensemble de leur activité. Ces sociétés exercent le plus souvent une activité d'infogérance classique et utilisent les atouts du modèle MSP comme une commodité opérationnelle, sans en adopter pleinement la culture ni les processus. Le PSA est rarement déployé, la documentation reste informelle, les workflows ne sont pas automatisés.

Un marché sans barrière à l'entrée

Paradoxalement, il est aujourd'hui plus simple de créer une entreprise sur le modèle MSP que de transformer une organisation existante. Aucune barrière à l'entrée significative ne freine les nouveaux entrants. Les solutions RMM et PSA, qu'elles soient facturées à l'agent ou au nombre de techniciens, sont accessibles pour une moyenne de 150 € par mois, hors coûts de formation et d'intégration. Le ticket d'entrée technologique n'a jamais été aussi bas.

Ce constat redessine les dynamiques concurrentielles du secteur. La performance ne se joue plus sur l'accès aux outils, qui sont désormais à la portée de tous, mais sur deux leviers de différenciation : la spécialisation sectorielle (santé, industrie, juridique, collectivités) et la performance commerciale, c'est-à-dire la capacité à vendre, déployer et fidéliser à grande échelle. Dans un marché où l'offre technologique se standardise, ce sont le positionnement et l'exécution qui feront la différence.

Du modèle MSP au modèle MSSP : une transformation à marche forcée

Poussés par une demande croissante, les prestataires informatiques ne peuvent plus se contenter de gérer des infrastructures. Ils doivent désormais intégrer des services de cybersécurité (détection, réponse aux incidents, suivi de la gouvernance), sous la forme d'un guichet unique capable de répondre aux attentes de leurs clients comme aux exigences de leurs assureurs.

La cybersécurité : un marché en croissance, mais encore sous-investi

La dynamique est réelle : le marché français de la cybersécurité a progressé de 10% en 2025. Pourtant, la réalité du terrain reste paradoxale. Selon le baromètre national de Cybermalveillance.gouv.fr, les trois quarts des TPE-PME investissent encore moins de 2 000 € par an dans la cybersécurité. L'écart entre la prise de conscience et le passage à l'acte demeure considérable, en particulier pour les structures de moins de 50 salariés.

Les prestataires informatiques ont intégré les solutions de protection par étapes successives : antivirus, puis EPP (Endpoint Protection Platform), puis EDR (Endpoint Detection and Response). Mais la sophistication croissante des attaques et le durcissement des critères d'assurabilité imposent un changement de dimension. Il ne s'agit plus seulement de protéger, mais de surveiller et de répondre en continu, 24 heures sur 24, 7 jours sur 7. Ce niveau de service correspond aux fonctions d'un MSSP (Managed Security Service Provider) et repose sur une capacité opérationnelle que la plupart des prestataires ne possèdent pas.

Des obstacles structurels

Pour les MSP comme pour les prestataires traditionnels, cette évolution soulève plusieurs difficultés majeures.

1

L'absence de compétences en cybersécurité.
Si la gestion d'un parc informatique et sa sécurisation relèvent toutes deux du domaine de l'IT, ce sont en réalité deux métiers distincts. Administrer des postes de travail ne prépare pas à analyser des flux réseau, corréler des événements de sécurité ou piloter une réponse à incident. Or, les profils qualifiés en cybersécurité sont rares et coûteux sur le marché de l'emploi.

2

L'impossibilité d'internaliser un SOC.
Le SOC (Security Operations Center) constitue le cœur opérationnel d'un dispositif de surveillance continue. Son fonctionnement repose sur des analystes spécialisés, des outils logiciels complexes (SIEM, XDR, EDR, SOAR) et une organisation en astreinte permanente. Selon la société Formind, la création d'un SOC internalisé représente un investissement pouvant atteindre 280 000 € par an, en intégrant les frais de personnel et de licences pour un fonctionnement 24/7. Un montant hors de portée pour des prestataires dont la grande majorité compte moins de 20 salariés.

3

La complexité de la délégation à un tiers.
La souscription à une offre MDR (Managed Detection and Response) externalisée constitue une alternative crédible, permettant d'offrir un service de détection et de réponse sans supporter le coût d'un SOC interne. Toutefois, confier à un tiers un accès aux systèmes d'information des clients finaux impose de clarifier la répartition des responsabilités en cas d'incident, de formaliser les engagements contractuels et de maintenir la confiance dans une relation désormais tripartite.

Un modèle de collaboration à construire

Les rôles se dessinent clairement. Le MSP conserve sa position de relais local et d'expert du contexte informatique du client : il connaît le parc, les utilisateurs, les applications métier et les contraintes opérationnelles. Le MDR (Managed Detection and Response) apporte ce qui lui manque à savoir la corrélation des événements, l'analyse des menaces et la détection en continu. Le prestataire informatique devient le guichet unique du client, adossé à des spécialistes pour les fonctions qu'il ne peut pas porter seul.

Chez NDNM, nous observons cette convergence depuis fin 2024, et le constat est clair : les MSP qui l'ont intégrée gagnent des parts de marché. Leur rôle a changé. Il ne s'agit plus seulement de gérer l'informatique de leurs clients, mais d'orchestrer un écosystème de partenaires au service de leur sécurité.

Intelligence artificielle : réagir plutôt que subir

En février 2026, deux journalistes du média américain CNBC ont développé un clone fonctionnel de Monday.com, une plateforme de gestion de projet valorisée 5 milliards de dollars, en moins d'une heure, sans aucune compétence technique et pour un coût inférieur à 15 dollars. Leur seul outil : Claude Code, l'agent de programmation autonome développé par Anthropic. Le système a analysé seul les fonctionnalités de la plateforme, les a reproduites, puis a ajouté des modules complémentaires sans intervention humaine.

Un tournant pour l'industrie logicielle

L'expérience a provoqué une onde de choc sur les marchés financiers. L'action Monday.com a chuté d'environ 20% dans les jours qui ont suivi, entraînant dans sa chute l'ensemble du secteur SaaS, avec une correction globale de près de 30% sur les valeurs logicielles. La question posée par les investisseurs est brutale : pourquoi payer des licences élevées par utilisateur quand un produit équivalent peut être répliqué en une heure ? Pourquoi continuer à payer un intégrateur pour configurer un logiciel si l'IA sait le faire ?

Cette prouesse repose sur une avancée majeure : l'orchestration multi-agents. Anthropic a développé un système dans lequel Claude coordonne des équipes d'agents spécialisés tels qu'un chef de projet, développeur front-end, développeur back-end ou un testeur, chacun disposant de son propre contexte et de compétences distinctes. Ces agents travaillent en parallèle, se corrigent mutuellement et itèrent jusqu'à atteindre le résultat final. Claude Code peut ainsi mener des projets complexes de manière totalement autonome sur des durées de 7 à 10 heures en continu.

> “Les avantages acquis et les rentes de situation dont bénéficient certains prestataires comme la facturation à la journée pour l’intégration, la configuration, le paramétrage ou le maintien en condition opérationnelle d’équipements informatiques ne seront probablement plus garantis dans les 18 à 24 prochains mois.”

Ce que cela signifie pour la prestation informatique

Cet épisode constitue un signal d’alerte pour l’ensemble du secteur. Les avantages acquis et les rentes de situation dont bénéficient certains prestataires comme la facturation à la journée pour l’intégration, la configuration, le paramétrage ou le maintien en condition opérationnelle d’équipements informatiques ne seront probablement plus garantis dans les 18 à 24 prochains mois.

L’intelligence artificielle ne remplacera pas les interventions physiques : installer physiquement un poste de travail, câbler un réseau, ou déployer un équipement sur site. Ces actions resteront l’apanage du technicien de terrain. En revanche, il est raisonnable d’anticiper l’émergence à moyen terme d’agents IA autonomes, qu’ils soient open source ou propriétaires, qui seront capables de prendre en charge les principales opérations de maintenance logicielle : mises à jour, diagnostics, résolution d’incidents de premier niveau, application de correctifs, réponse aux demandes de support de premier niveau. Le tout pour un coût marginal.

L’impact sera massif pour les acteurs de la prestation traditionnelle. À l’instar des traducteurs, community managers, rédacteurs ou photographes dont le volume de travail a été fortement amputé par l’IA générative, les prestataires dont l’activité repose exclusivement sur le support technique et la maintenance pourraient se retrouver en difficulté. Sans évolution de leur proposition de valeur, leur modèle économique deviendra vulnérable.

De la maintenance à la création de valeur

C'est pourquoi nous recommandons aux prestataires informatiques de repenser la manière dont ils accompagnent leurs clients. À la gestion et à la sécurisation du parc informatique, il devient essentiel d'associer un accompagnement à la production, à la transformation et à l'exploitation de la donnée dans l'entreprise.

Ce repositionnement s'articule autour de la conception et de la maintenance de workflows d'automatisation des processus internes, à l'aide de solutions telles que n8n, Zapier ou Make. Le principe est simple : identifier les processus chronophages chez le client, puis les automatiser pour améliorer la productivité de ses collaborateurs.

Les cas d'usage sont nombreux et touchent l'ensemble des fonctions de l'entreprise :

- **Administration et RH :** automatisation de l'onboarding, génération de documents contractuels, synchronisation entre SIRH et paie.
- **Commerce et relation client :** qualification automatique des leads, enrichissement CRM, relances séquencées, synchronisation devis-commandes-facturation.
- **Finance et comptabilité :** rapprochement factures-paiements, extraction de données fournisseurs, alimentation de tableaux de bord financiers.
- **Support et communication interne :** routage intelligent des demandes, création automatique de tickets, notifications conditionnelles dans Teams ou Slack.
- **Marketing :** publication multi-canal programmée, reporting automatisé, segmentation dynamique des bases de contacts.

Le fonctionnement de ces plateformes d'automatisation est très similaire à celui des outils déjà présents dans la stack MSP incluant workflows visuels, connecteurs API, logique conditionnelle. La montée en compétence devrait donc être facilitée pour des équipes déjà familiarisées avec les environnements RMM et PSA.

En améliorant mois après mois les processus internes de ses clients, le prestataire augmente leur productivité et consolide une position de partenaire indispensable. Il n'est plus relégué au maintien en condition opérationnelle, un rôle que l'IA menace directement, mais devient un véritable centre de profit pour les entreprises qu'il accompagne.

Le mot de la fin

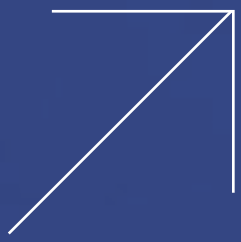
Le modèle MSP, après une décennie de transformation, a profondément fait évoluer la prestation informatique en Europe. Mais le marché ne s'arrête pas là. La convergence entre gestion d'infrastructure, cybersécurité et intelligence artificielle redessine les contours du métier. Le prestataire de demain ne sera ni un simple MSP, ni un MSSP, ni un intégrateur d'IA. Il sera les trois à la fois ou il laissera la place à ceux qui auront su prendre ce virage.

Chez NDNM, nous aurons le plaisir de continuer à accompagner les acteurs de la prestation informatique dans cette transformation. Car c'est dans les périodes de rupture que naissent les plus belles opportunités. Nous restons convaincus que les prestataires qui choisiront d'évoluer ont devant eux le plus beau chapitre de leur histoire.

Sébastien Gest
Président Fondateur du cabinet NDNM

> “Le prestataire de demain ne sera ni un simple MSP, ni un MSSP, ni un intégrateur d'IA. Il sera les trois à la fois ou il laissera la place à ceux qui auront su prendre ce virage.”

Concevoir votre **Stack MSP**



RMM
(Remote Monitoring and Management)

Longtemps considéré comme l'élément fondateur de la stack MSP, le RMM ne cesse de se réinventer. Initialement centré sur la supervision des postes de travail et serveurs, la gestion des correctifs et la prise en main à distance, il occupe désormais un rôle plus structurant dans l'architecture des services managés.

Cette évolution est liée à l'élargissement des périmètres gérés. Les environnements hybrides, les usages cloud et la multiplication des terminaux ont poussé les éditeurs à faire évoluer leurs plateformes. Pour renforcer la protection, les EDR sont intégrés ou connectés au RMM.

L'IA facilite la génération de scripts pour les opérations de maintenance. En tant que brique centrale, le RMM s'inscrit aujourd'hui dans un écosystème interconnecté avec les outils de sécurité, sauvegarde, gestion des identités ou de facturation.

Cette interopérabilité conditionne la capacité du MSP à industrialiser ses services et maîtriser ses coûts. La densification réglementaire a renforcé les exigences de traçabilité, de visibilité et de contrôle des configurations. Pour les prestataires expérimentés, le RMM n'est plus seulement un outil opérationnel, mais un levier pour passer à l'échelle.

Kaseya 365 Endpoint

Kaseya

Pays d'origine : États-Unis

Gestion des appareils, sécurité et sauvegarde à un tiers du coût. RMM, patching, AV, EDR, détection ransomware, backup et MDR dans un abonnement simple conçu pour booster l'efficacité et la rentabilité.

Kaseya 365 Endpoint

Cette solution s'adresse :
PME

70 % d'économies abonnement unique et peu coûteux

1/3 du coût pour une protection endpoint complète

75 % de gain d'efficacité grâce à une automatisation accrue

Principales fonctionnalités

Supervision et gestion à distance : Visibilité et contrôle complets sur tous les endpoints. Inclus : Datto RMM.

Patch management : Gardez tous les appareils à jour facilement grâce à une gestion logicielle avancée. Inclus : Datto RMM.

Détection des ransomwares : Bloquez les ransomwares grâce à une surveillance continue et une détection intelligente des menaces. Inclus : Datto RMM.

Antivirus : Protégez votre activité avec une détection avancée et une veille mondiale sur les menaces. Inclus : Datto AV.

EDR (Endpoint Detection & Response) : Identifiez, contenez et neutralisez les menaces avec une protection intelligente des endpoints. Inclus : Datto EDR.

Sauvegarde des endpoints : Sauvegardes automatisées et chiffrées pour limiter les pertes et accélérer la reprise. Inclus : Datto Endpoint Backup.

Points clés

- Supervision et gestion holistiques
- Patching des logiciels tiers
- Réduction des coûts d'outils
- 20 automatisations intégrées par module
- Gain d'efficacité et gain de temps
- Réduction des erreurs humaines
- Automatisations inter-outils pour les tâches
- Moins de tâches manuelles

Distribué par
BeMSP
Hermitage Solutions

Kaseya
(+44) 800 048 8847
250 Longwater Avenue,
Green Park, Reading RG2 6GB,
Royaume-Uni
www.kaseya.com

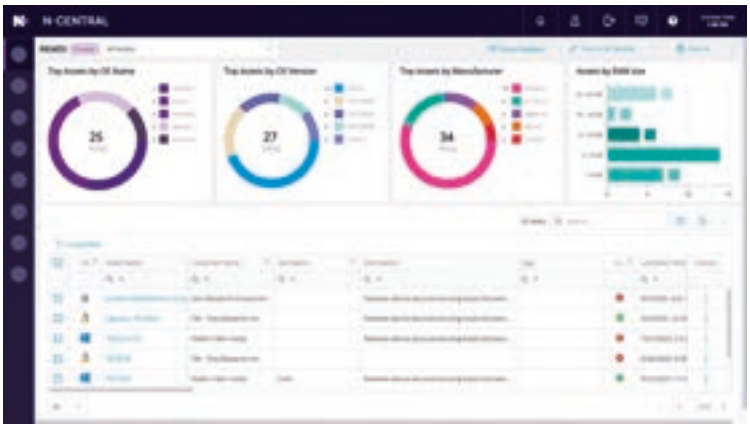
Demandez une démonstration

N-central RMM

N-able

Pays d'origine : États-Unis

N-able propose deux solutions de gestion à distance puissantes. N-sight, conçu pour les petits MSP souhaitant être opérationnel rapidement et N-central, qui vous permet de gérer de grands réseaux et de développer vos opérations informatiques. Optimisez vos ressources avec une supervision proactive.



Cette solution s'adresse :
ETI

25 000 MSP
ont adopté un RMM N-able

500 000 PME protégées

Plus de 8 millions
de points de terminaison

Principales fonctionnalités

Gestion unifiée des terminaux : Visibilité et contrôle complets sur l'ensemble des appareils de votre réseau : Windows, Mac, Linux, appareils en réseau, etc.

Appli automatique de correctifs : Automatisez le déploiement de correctifs pour Windows, Linux, Mac et des centaines d'applications tierces. Suivi sur la réussite.

Moteur de règles complet : Utilisez des règles puissantes et intuitives pour identifier, protéger et réagir aux changements dans votre parc IT.

Automatisation intelligente : Éliminez le stress lié aux activités IT manuelles avec des automatisations contribuant à anticiper et uniformiser vos workflows.

Outils ouverts et évolutifs : Des intégrations poussées (plus de 90 possibles) et des API, auxquelles s'ajoute notre portail développeur optimisé avec l'IA.

Reporting détaillé : Mettez en avant vos actions grâce à la seule solution proposant un reporting décisionnel intégré.

Points clés

- Disponible en mode SaaS pour plus de simplicité
- Support de l'équipe Infinigate en France
- N-ableMe : un portail partenaire dédié
- Preuve de conformité RGPD globale N-able
- Abonnement mensuel avec facturation à la fin du mois
- Gérez plusieurs clients depuis une seule console
- Disponible on-premise pour un contrôle total
- Certifications ISO 27001 et SOC 2 de N-able

Distribué par
Infinigate France

N-able
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/n-able/

Demandez une démonstration

RMM
RG System Suite

Pays d'origine : France

RG System Suite centralise la supervision, l'automatisation et la gestion des parcs IT dans une console unique 100 % française et certifiée ISO 27001. Grâce à une supervision augmentée par l'IA, surveillez, intervenez et sécurisez les environnements de vos clients avec un pilotage proactif.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

650 Partenaires MSP

500K Agents RMM déployés

10K Utilisateurs actifs

Principales fonctionnalités

IA intégrée (nouveauté 2026) : Exécution de tâches plus rapide, fiabilité accrue. Réduction des manipulations manuelles, montée en puissance de l'automatisation.

Supervision en temps réel : Suivi en temps réel de l'état de santé de vos parcs et machines physiques ou virtuelles, avec réception d'alertes instantanées.

Automatisation des tâches : Gain de temps et automatisation de vos tâches grâce à des workflows.

Scripts personnalisés : Interface dédiée avec des scripts prêts à l'emploi et personnalisables.

Déploiement d'applications : Gestion automatisée des installations et mises à jour d'applications grâce à la bibliothèque Chocolatey.

Rapports d'activité : Configuration et envoi de rapports automatiques et paramétrables.

Points clés

- Multi-tenant
- Plateforme développée et hébergée en France
- Certifiée ISO 27001
- Full SaaS
- Facturation à l'agent, sans engagement
- Disponible en marque blanche
- Channel Account Manager dédié
- Support 100% français

Distribué par
Cris Réseaux
Actual Systèmes
DSD

Septeo IT Solutions
(+33) 4 11 93 42 00
194 Avenue de la Gare
Sud de France - 34970 Lattes
www.rgsystem.septeo.com

Demandez une démonstration

SuperOps (PSA RMM)

SuperOps

Pays d'origine : États-Unis

SuperOps est un système d'exploitation IT alimenté par l'IA, conçu pour la gestion informatique moderne. Pensée pour les MSP et les équipes IT internes, la plateforme unifie la gestion des postes, la gestion des tickets, le PSA et le RMM, afin de permettre aux équipes de travailler plus rapidement.

3.5x rentabilité plus élevée

30 % Augmentation du chiffre d'affaires

300 % Efficacité opérationnelle accrue

Principales fonctionnalités

Patch Management : SuperOps automatise les correctifs OS et logiciels, assurant sécurité, conformité et IT évolutif avec peu d'effort manuel.

Rapports et analyses : Le reporting SuperOps transforme les données en tableaux de bord, suit les KPI et partage des insights pour plus de transparence.

Supervision réseau : SuperOps simplifie la gestion réseau avec scans, onboarding rapide, surveillance ICMP/SNMP, alertes proactives et MTTR réduit.

Gestion de projet : La gestion de projet PSA de SuperOps centralise tâches, délais et ressources pour livrer les projets IT plus efficacement.

Gestion des appareils mobiles : La solution permet de surveiller et gérer Android et iOS, d'assurer la sécurité, la santé des appareils et un support efficace.

Gestion du helpdesk : Le Service Desk SuperOps centralise tickets et automatisations pour un support rapide, intelligent et efficace.

Points clés

- Support technique 24/7
- Cloud / SaaS
- Support francophone
- Intégration Google Workspace
- Multitenant
- Certifications de sécurité
- Conforme RGPD
- Facturation mensuelle

Distribué par
Ipsteel
Net Point

Ipsteel
(+33) 1 40 86 04 26
4 Avenue Laurent Cely
92400 Asnières sur Seine
www.ipsteel.com

Demandez une démonstration

Atera RMM

Atera

Pays d'origine : Israël

Atera RMM permet de surveiller en temps réel l'état du système d'information, d'automatiser les tâches courantes, de gérer les correctifs et de résoudre les problèmes à distance avant qu'ils n'impactent les opérations.

www.atera.com/products/rmm

ConnectWise RMM

ConnectWise

Pays d'origine : États-Unis

ConnectWise RMM centralise la surveillance des endpoints, la gestion des correctifs, l'automatisation des tâches et l'accès sécurisé à distance. La solution aide les MSP à détecter proactivement les problèmes, réduire le bruit des alertes et optimiser l'efficacité opérationnelle.

www.connectwise.com/platform/rmm

Gorelo RMM

Gorelo

Pays d'origine : États-Unis

Pensée pour la simplicité d'usage, Gorelo propose sur une interface intuitive qui réduit la courbe d'apprentissage. La solution combine RMM et PSA dans un environnement unifié, limitant les frictions entre outils et aidant les MSP à rester concentrés sur la résolution des incidents.

www.gorelo.io/remote-management

Level RMM

Level.io

Pays d'origine : États-Unis

Level intègre un moteur d'automatisation conditionnelle avancé permettant de déclencher des actions selon des états système ou alertes. Pensée pour la scalabilité, la solution est certifiée SOC 2 Type II et assure une gestion sécurisée des accès à distance.

level.io

MDM / UEM

Le MDM a dépassé son rôle historique de gestion des smartphones pour devenir, avec l'UEM, une brique centrale de gouvernance du poste de travail. La généralisation du télétravail, la diversité des terminaux et la montée des usages cloud ont renforcé les exigences de contrôle, de standardisation et de sécurité sur les postes de travail, tout au long de leur cycle de vie : conformité, accès aux ressources, niveau de durcissement et conditions d'usage.

De leur côté, les plateformes ont gagné en maturité sur Windows et macOS, avec l'automatisation de l'enrôlement, le déploiement applicatif, la gestion des mises à jour et des scénarios zero-touch. Elles étendent également leur couverture aux environnements Google, en particulier dans les organisations fortement orientées cloud et mobilité.

L'intégration avec l'identité devient structurante : SSO, MFA et accès conditionnel permettent d'aligner l'état du poste avec les droits accordés à l'utilisateur, quel que soit l'annuaire sous-jacent.

Mobile
Check Point

Pays d'origine : Israël

Assure la sécurité de vos données d'entreprise en sécurisant les appareils mobile iOS et Android de vos employés contre tous les vecteurs d'attaques : applications, fichiers, réseau et système d'exploitation

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

Leader Forrester Wave 2024 Rapport de Mobile Threat Defence

99 % Détection emails de phishing (Miercom)

98.2% Détection des malwares (Miercom)

Principales fonctionnalités

Protection complète : La protection des données d'entreprise sur la surface d'attaque mobile : applications, réseaux et systèmes d'exploitation.

Protection contre menaces avancées : Telles que les malwares avancés, les tentatives d'hameçonnage, les attaques de type Man-in-the-middle, et les vulnérabilités.

Intégration avec les MDM/UEM : Microsoft Intune, Workspace ONE, MobileIron, Samsung Knox, IBM Maas360, Citrix, BlackBerry, Jamf, Google et SOTI.

Administration simple : Une sécurité évolutive et simple à administrer pour tous les types de télétravailleurs, avec déploiement Zéro touch.

Convivial : Prise en main rapide avec aucun impact sur l'expérience utilisateur ou la confidentialité.

App unifiée avec Harmony SASE : Permet la connection au réseau privé de Harmony SASE avec la même application mobile.

Points clés

- Licence Pay-As-You-Go
- Console multi-tenant
- Protection continue assurée par les experts de Check Point
- Gestion unifiée de la sécurité via un portail web unique

Distribué par
Arrow ECS
Infinigate
Westcon

Check Point Software
20 Avenue André Prothin
92400 Courbevoie
www.checkpoint.com

Demandez une démonstration

PSA
(Professional Services Automation)

Dans un modèle MSP fondé sur la récurrence, les engagements de service et la contractualisation à long terme, le PSA (Professional Services Automation) permet le pilotage de la performance de l'activité, et structure l'ensemble de la chaîne de gestion : suivi du temps, contrats, coûts, capacité, planning des équipes.

En s'interconnectant avec le RMM, le PSA permet de rapprocher les actions de production avec les revenus générés. Cette corrélation met en lumière les dérives de marge, les contrats structurellement déficitaires ou les surcharges opérationnelles récurrentes. Il devient également un outil d'arbitrage, permettant de prioriser les ressources, d'objectiver les décisions et d'ajuster les modèles de services au plus près de la réalité opérationnelle.

Dans un contexte de pression continue sur les marges, le PSA assure le lien entre l'opérationnel et la gouvernance de l'activité. Il conditionne la capacité à standardiser les workflows, à accompagner la croissance sans désorganiser la production et à piloter la rentabilité à l'échelle, sans multiplier les exceptions.

HaloPSA

Halo

Pays d'origine : Royaume-Uni

HaloPSA est la plateforme PSA tout-en-un qui centralise votre activité MSP. Elle unifie services, ventes et opérations pour structurer votre organisation, automatiser vos processus et piloter votre performance avec une vision claire, au service de votre croissance.

Cette solution s'adresse :

TPE **PME** **ETI** **Grands comptes**

5000+ MSP déployés

96 % des clients renouvellent

30 ans d'expertise PSA

Principales fonctionnalités

Gestion des tickets : Centralisez et priorisez les demandes clients pour améliorer la réactivité, le respect des SLA et la satisfaction client.

Ventes & CRM : Gérez prospects, opportunités, devis et clients dans un CRM intégré pour suivre chaque relation et booster vos ventes.

Contrats et facturation : Structurez contrats, abonnements et facturation récurrente pour sécuriser vos revenus et maîtriser votre rentabilité.

Pilotage et reporting : Pilotez votre activité grâce à des tableaux de bord clairs personnalisables pour suivre performance, SLA, charge et rentabilité.

Portail client : Offrez à vos clients un portail personnalisable en libre-service pour suivre leurs demandes ainsi que vos actions proactives.

Intégrations et IA : Harmonisez vos processus avec une IA configurable et unifiez vos outils via 250+ intégrations pour un écosystème MSP complet.

Points clés

- Support et accompagnement clair, efficace et en français
- Gestion multi-organisations, sans surcoût
- Accessible partout, sans infrastructure à maintenir
- On-premise possible pour des besoins spécifiques
- Conforme ISO 27001 et SOC 2 Type 2
- Conforme RGPD
- Un expert dédié pour vous accompagner à tout moment
- Un espace partenaire pour toutes vos demandes

Halentra
(+33) 1 85 09 15 15
60 Rue François 1er
75008 Paris
www.halentra.com

Demandez une démonstration

Kaseya 365 Ops

Kaseya

Pays d'origine : États-Unis

Kaseya 365 Ops centralise PSA, documentation et gestion IT dans une plateforme unifiée. L'IA renforce l'automatisation pour accélérer les tâches, standardiser les services, fiabiliser les process et fluidifier la coordination des équipes.

Kaseya 365 Ops

Cette solution s'adresse :
PME

7 outils IT essentiels pour un service fluide et intégré

10 heures + gagnées par tech chaque mois

50+ intégrations natives Travail optimal, sans coût additionnel

Principales fonctionnalités

Gestion des services IT : Centralisez tickets, projets et planning dans une solution unique. Inclus : Autotask.

Documentation IT et procédures : Sécurisez actifs, mots de passe et SOP pour un service plus rapide et fiable. Inclus : IT Glue.

Cycle de vie et stratégie : Structurez vos QBR avec reporting automatisé, suivi des assets et budgets. Inclus : myITprocess.

Gestion des mots de passe : Offrez un gestionnaire simple et sécurisé pour les utilisateurs, avec rotation automatique des mots de passe. Inclus : MyGlue.

Découverte et cartographie réseaux : Identifiez les assets clients et mappez leur infra automatiquement. Inclus : Network Glue.

Points clés

- Workflows IA pour automatiser les opérations IT
- Réduction des erreurs par l'automatisation
- KPI clairs pour QBR et reporting client
- Vue centralisée sur la performance IT
- Accès instantané à la doc, assets et SOP
- Stack unifié pour industrialiser vos services

Distribué par
BeMSP
Hermitage Solutions

Kaseya
(+44) 800 048 8847
250 Longwater Avenue, Green Park, Reading RG2 6GB, Royaume-Uni
www.kaseya.com

Demandez une démonstration

N-able MSP Manager

N-able

Pays d'origine : États-Unis

Pensé pour les MSP en croissance, MSP Manager optimise le suivi du temps, la facturation et la gestion des tickets. Il facilite la capture des heures facturables, la personnalisation des services et l'intégration avec les RMM N-able. Une solution complète pour aligner service et rentabilité.

www.n-able.com/products/msp-manager

Ruddr

Ruddr

Pays d'origine : États-Unis

Conçu pour les petites équipes, Ruddr permet un suivi précis des projets avec une analyse fine des marges par client, ressource ou phase. Son API ouverte facilite l'intégration dans l'environnement existant, sans complexité superflue. Idéal pour les MSP axés delivery et pilotage financier.

www.ruddr.com

SuperOps PSA

Superops

Pays d'origine : Inde

SuperOps intègre l'IA au cœur de son PSA pour automatiser la documentation, enrichir les tickets et suggérer des réponses contextuelles.
Cette approche permet d'optimiser le temps de traitement, de standardiser les interventions et d'améliorer la qualité de service sur l'ensemble du cycle support.

superops.com/psa-software

Syncro PSA

Syncro MSP

Pays d'origine : États-Unis

Syncro unifie PSA, RMM et intégration Microsoft 365 dans un environnement unique. Sa force réside dans la cohérence opérationnelle : chaque action (ticket, alerte, facturation) alimente un même flux, limitant les frictions et doublons.

syncromsp.com/platform/psa

ITSM

Historiquement cantonné à la gestion des tickets et au suivi des demandes, l'ITSM a évolué vers une approche basée sur la gestion des processus, intégrant la gestion des incidents, demandes, changements, problèmes, gestion de projets, catalogues de services et automatisation des workflows.

La valeur ne réside plus dans le volume de tickets traités, mais dans la capacité à structurer des parcours standardisés et documentés, capables de réduire les écarts de traitement.

Pour un MSP, l'enjeu n'est plus de « traiter des tickets » : l'ITSM devient à la fois un outil de production et de contractualisation. Il porte les SLA, la traçabilité des actions et la qualité de service perçue par le client. Les attentes se renforcent sur les portails clients, la transparence des engagements, les intégrations avec le RMM, le PSA ou les outils de sécurité, ainsi que sur la réduction du bruit opérationnel via la capitalisation de la connaissance et l'automatisation des réponses aux demandes récurrentes.

L'ITSM devient ainsi une brique centrale d'industrialisation. Il permet de sortir d'une gestion au cas par cas pour piloter une production mesurable, prévisible et alignée sur les engagements clients.

Intelligence des actifs IT pour MSP

Lansweeper

Pays d'origine : Belgique

Lansweeper aide les MSP à travailler plus vite et plus efficacement grâce à une plateforme d'intelligence des actifs, multi-tenant et automatisée. Plus de visibilité, plus de services et plus de revenus, avec une solution simple, évolutive et abordable.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

20 000+ clients dans le monde entier

0,25€ par actif scanné par mois

60+ intégrations

Principales fonctionnalités

Découverte universelle des actifs : Analyse approfondie de l'environnement technologique de vos clients pour garantir une visibilité précise, cohérente et complète.

Inventaire des actifs : Une source fiable réunissant tous les équipements et logiciels clients, multitenant, rapide à déployer et pleinement automatisée.

Analyses exploitables : Des données complexes transformées en intelligence pour des décisions plus intelligentes.

Orchestration : Simplifiez l'IT : orchestration et automatisation pour des workflows intelligents.

Intégrations : Connectez votre stack sans friction. CMDB, SIEM, ITSM... tout s'intègre.

Intelligence alimentée par l'IA : L'IA Lansweeper analyse les actifs, détecte les risques et fournit des conseils pour optimiser et accélérer les opérations IT.

Points clés

- Portail de gestion multisite
- Facturation mensuelle à l'usage
- Le Cloud pour gérer tous vos actifs technologiques
- Disponible on-prem (sur site)
- Portail partenaire dédié
- Support entreprise pour tous les MSP
- MSP Technical Success Manager & Partner Account Executive
- Lansweeper Academy

Lansweeper
(+32) 52 69 66 96
212 Fraterstraat
9820 Merelbeke, Belgique
https://www.lansweeper.com/partners/msp/

Demandez une démonstration

Outil de prise en main à distance

La prise en main à distance s'est imposée comme un geste quotidien dans l'activité des prestataires informatiques, au point d'être longtemps perçue comme un simple utilitaire. La généralisation du travail à distance et l'externalisation de l'exploitation ont profondément modifié son statut : l'outil n'est plus seulement un moyen d'intervenir rapidement, mais un accès direct et sensible au système d'information du client.

Ces solutions intègrent désormais des mécanismes d'authentification renforcée, de gestion granulaire des droits et de journalisation des sessions. La question n'est plus uniquement technique, mais opérationnelle : savoir qui intervient, dans quel contexte, sur quel périmètre et pour combien de temps. L'intégration avec les briques IAM/PAM et les politiques de sécurité devient une nécessité.

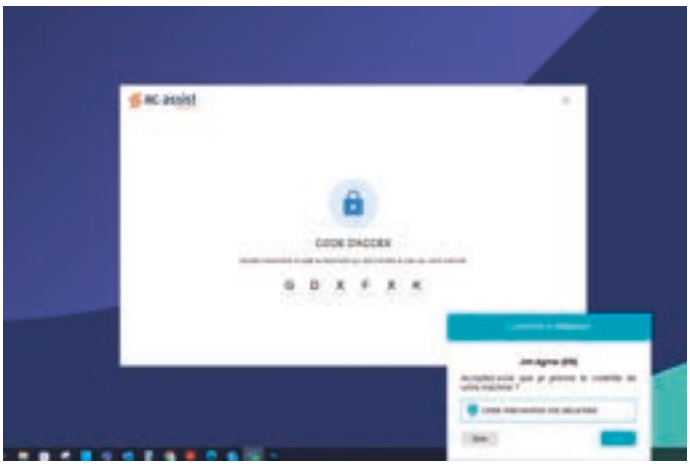
Pour les MSP, la valeur de la prise en main à distance se joue désormais dans son intégration au reste de la chaîne opérationnelle. Reliée à l'ITSM et au RMM, elle permet de documenter les interventions, de produire des preuves d'action et de sécuriser les accès au quotidien.

Assist

RG System Suite

Pays d'origine : France

Intervenez rapidement sur les postes ou mobiles de vos clients grâce à Assist, la solution de prise en main à distance full web, simple, sécurisée et hébergée en France. Intégrée à la plateforme RMM RG System Suite, elle offre une assistance efficace où que vous soyez.



Cette solution s'adresse :

TPE **PME** **ETI** **Grands comptes**

2M+ de prises en main à distance

100 % SaaS

99%+ de disponibilité du support

Principales fonctionnalités

Connexion avec ou sans agent : Assistance de vos clients en quelques clics, via un code unique ou un accès permanent grâce à deux types d'agents.

Historique des connexions : Suivi détaillé et archivage des interventions réalisées sur chaque machine.

Enregistrement de session : Enregistrement des interventions à distance offrant un résumé complet pour chaque session.

Chat intégré : Échanges en direct avec vos clients pour optimiser chaque prise en main à distance.

Transfert de fichiers sécurisé : Envoi rapide de fichiers, sans limite de poids ou de format, avec chiffrement des flux.

Données matérielles : Accès aux informations détaillées des machines distantes (processeur, RAM, OS...).

Points clés

- Aucune installation, 100% SaaS
- Solution développée et hébergée en France
- Certifiée ISO 27001
- Channel Account Manager dédié
- Facturation par canal, ajustable selon vos besoins
- Support 100% français

Distribué par
Cris Réseaux
Actual Systèmes
DSD

Septeo IT Solutions
(+33) 4 11 93 42 00
194 Avenue de la Gare
Sud de France
34970 Lattes
www.rgsystem.septeo.com

Demandez une démonstration

Anydesk

Anydesk

Pays d'origine : Allemagne

AnyDesk offre une prise en main à distance rapide, légère et hautement sécurisée. Son protocole propriétaire DeskRT minimise la latence, même à faible bande passante. Disponible en cloud ou on-premise, la solution prend en charge la gestion de sessions en file d'attente et l'accès non supervisé.

anydesk.com

RemotePC

RemotePC

Pays d'origine : États-Unis

RemotePC cible les environnements multi-utilisateurs avec une gestion des accès, des groupes, et des journaux d'activité. Particulièrement adapté au travail hybride, il permet un accès distant cloisonné par utilisateur, garantissant confidentialité et traçabilité dans les usages professionnels.

www.remotepc.com

RustDesk

RustDesk

Pays d'origine : Singapore

RustDesk propose une alternative open source aux solutions SaaS de prise en main à distance, avec un déploiement self-hosted simple via Docker. Idéal pour les environnements exigeant une souveraineté totale des données, une personnalisation avancée et un contrôle strict des accès.

rustdesk.com

SplashTop

SplashTop

Pays d'origine : États-Unis

Splashtop se distingue par sa prise en charge étendue des environnements hétérogènes (Windows, macOS, Linux, iOS, Android) et par sa compatibilité avec les politiques de sécurité d'entreprise (authentification SSO, MFA, contrôle d'accès). Une solution robuste pour les équipes informatiques distribuées.

splashtop.com

Produits de **Cybersécurité**

Sécurité de la messagerie

Malgré la généralisation des mécanismes d'anti-spam et d'anti-phishing, la messagerie reste l'un des principaux vecteurs d'attaques.

Face à une succession de modes opératoires permettant de passer à travers des méthodes de détection traditionnelles, les solutions ont progressivement évolué vers des approches multicouches, combinant analyse comportementale, détection de tentatives de fraude ciblées, lutte contre l'usurpation d'identité et capacités de remédiation.

L'enjeu ne se limite plus à l'identification d'un message malveillant, mais à la gestion de campagnes actives : retrait de messages déjà distribués, analyse des liens, correction d'erreurs de configuration, accompagnement de la réponse à incident. L'intégration native avec les environnements cloud, notamment Microsoft 365 et Google Workspace, s'impose désormais comme un prérequis opérationnel.

Pour les MSP, la sécurité de la messagerie s'inscrit ainsi comme un service managé à part entière. La valeur ne se mesure plus seulement en taux de détection, mais dans la capacité à fournir des indicateurs permettant de valoriser la qualité de leur prestation.

365 Total Protection

Hornetsecurity

Pays d'origine : Europe

Hornetsecurity est un leader mondial des solutions cloud de nouvelle génération pour la sécurité, la conformité, la sauvegarde et la sensibilisation. Son produit phare, 365 Total Protection, est la solution la plus complète du marché pour Microsoft 365.

125 000+
Clients

12 000+
Partenaires & MSPs

98.2%
Taux de satisfaction clients

Principales fonctionnalités

Sécurité email : Garantissez la continuité de vos communications avec des filtres intelligents bloquant les attaques les plus avancées.

Sauvegarde : Sauvegarde et restauration automatisées de M365, avec stockage illimité, indépendant de Microsoft, et accès en self-service.

Conformité : Contrôlez le partage de données dans M365, évitez toute fuite et respectez simplement les exigences de conformité locales.

Sensibilisation à la cybersécurité : Automatisé. Continu. Sans effort. Une formation qui s'adapte automatiquement à chaque utilisateur.

Multi-Tenant Management : Sécurisez, uniformisez et mettez en conformité l'ensemble de vos tenants Microsoft 365 en toute simplicité.

Dashboard centralisé : Des solutions et fonctionnalités déployées et gérées sans effort depuis une plateforme multi-tenant unique : le Control Panel.

Points clés

- Cloud / SaaS
- Hébergement souverain
- Certifications de sécurité
- Portail partenaire
- Support francophone
- Conforme RGPD
- Intégration M365
- Multitenant

HORNETSECURITY
(+33) 3 59 61 66 50
2bis, Avenue Antoine Pinay
59510 Hem
www.hornetsecurity.com

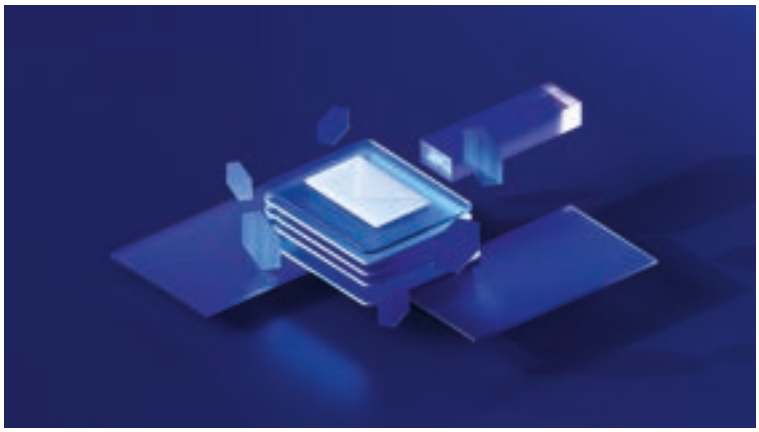
Demandez une démonstration

Acronis Email Security

Acronis

Pays d'origine : Suisse

Acronis Email Security pour Acronis Cyber Protect Cloud. Renforcez la sécurité de vos clients en interceptant les attaques déployées via e-mail avant qu'elles n'atteignent les utilisateurs finaux. Protégez le canal de communication le plus exposé grâce à des technologies de protection inégalées.



Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

750 000 entreprises protégées dans le monde via des MSP Acronis

20 000 fournisseurs de services utilisent la plateforme Acronis

7,5 millions d'attaques bloquées en 12 mois grâce à Acronis

Principales fonctionnalités

Filtre antispam : Bloquez les communications malveillantes grâce aux données combinées de plusieurs technologies de pointe.

Protection contre le contournement : Une technologie unique pour prévenir les techniques de contournement qui échappent à la détection des défenses traditionnelles.

Protection contre l'usurpation d'ID : Prévenez efficacement les attaques (usurpations d'identité, domaines similaires, imitations du nom affiché).

Service d'intervention sur incidents : Surveillez l'ensemble du trafic client et analysez les actions malveillantes avec un reporting et un support continus.

Analyse e-mails sortants pour M365 : Limitez les risques d'atteinte à la réputation et améliorez la précision de la protection en détectant les e-mails malveillants.

Filtre antiphishing : Détectez les URL malveillantes grâce à 4 moteurs de réputation des URL et à une technologie de reconnaissance d'image avancée.

Points clés

- Hébergement par Acronis
- Hébergé en France
- Console multi-tenant
- Facturation mensuelle
- Protection complète de Microsoft 365 avec Email Security
- Formations et certifications sur-mesure pour les MSP
- Conformité réglementaire éprouvée
- Solution certifiée

Distribué par
TD SYNNEX

Acronis
(+33) 1 87 16 91 19
20-22 Rue Marius Aufan
92300 Levallois-Perret
cloud.tdsynnex.fr

Demandez une démonstration

Cleanmail

Alinto

Pays d'origine : France

Cleanmail est une solution de protection professionnelle des emails. Elle offre une sécurité renforcée contre l'ensemble des menaces actuelles. Facile à déployer et à utiliser, elle assure une protection en temps réel tout en optimisant la délivrabilité des messages.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

10 000+ Organisations accompagnées

26 ans d'expérience

1 000 000+ Utilisateurs

Principales fonctionnalités

Filtrage et sécurité : Protection contre les spams, les virus, les tentatives de phishing et toutes les menaces transmises par email.

Quarantaine : Zone de quarantaine sécurisée pour consulter les emails classés comme spam avec la possibilité de les analyser et/ou les libérer.

Gestion des politiques de sécurité : Différents réglages de sécurité sont paramétrables par l'administrateur qui profite également d'un accès facile aux logs.

Continuité d'activité : Cleanmail offre un webmail de secours assurant un PCA lorsque le serveur de messagerie principal est indisponible.

Scanner sortant : Filtrage de tous les emails sortants ajoutant une couche de sécurité supplémentaire, garantissant votre flux et votre réputation.

Administration granulaire : Délégation granulaire (revendeurs, clients, domaines) pour la gestion du service. Intégrabilité par API.

Points clés

- Cloud / SaaS
- PaaS Multitenant
- Equipe Support Expert
- Accompagnement technique et commercial
- Facturation à l'usage
- Marque Blanche
- Logiciel & Hebergement éco-responsables
- Conformité RGPD

Distribué par
OCI
CELESTE
Linkt
WHM-IT
ADICO

Alinto
(+33) 4 81 09 01 10
19 Quai Perrache
69002 Lyon
www.alinto.com

Demandez une démonstration

Email & Collaboration Security

Check Point

Pays d'origine : Israël

Harmony Email & Collaboration Security protège Microsoft 365 et G-Suite avec une sécurité en profondeur. La solution analyse tous les emails entrants, sortants et internes, bloque phishing et malwares, et sécurise aussi les environnements collaboratifs comme Teams, Slack et le partage de fichiers.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

30 000 entreprises Utilisent déja notre protection Email

Leader dans le dernier Gartner Magic Quadrant

+99% Taux de capture le plus haut du secteur

Principales fonctionnalités

Sécurité complète de la messagerie : Protège votre messagerie cloud contre toutes les menaces de type Zero-Day, les codes QR compromis et les malwares.

Zero day malwares et ransomware : ThreatCloud AI combine 60 moteurs d'IA avancée et big data sur les menaces pour offrir les taux de prévention les plus élevés.

Vols d'identités et menaces internes : Analyse les événements de chaque utilisateur et les compare à leur comportement historique, ainsi qu'aux activités anonymes.

Déploiement et évaluation rapide : L'architecture inline par un API breveté permet une protection très efficace facile à déployer et à tester en quelques minutes.

Support étendu : Protège Office 365 email, OneDrive, Teams et Sharepoint, Gmail and GDrive, Slack, Box, Dropbox, et Citrix ShareFile.

De nombreuses options : Archivage, Formation, Gestion de DMARC/SPF/DKIM, Identités sur le dark web, Gestion des incidents, Gestion des postures SAAS, DLP.

Points clés

- Licence Pay-As-You-Go
- Console multi-tenant
- Protection 24/7 assurée par les experts de Check Point.
- Gestion unifiée de la sécurité via un portail web unique
- Gestion de quarantaine simplifiée avec Office 365
- NFR pour les partenaires

Distribué par
Arrow ECS
Infinigate
Westcon

Check Point Software
20 Avenue André Prothin
92400 Courbevoie
www.checkpoint.com

Demandez une démonstration

Email Security for M365

GLIMPS

Pays d'origine : France

Notre solution souveraine protège vos messageries M365 contre les menaces les plus sophistiquées. Elle intègre des fonctionnalités complètes pour une analyse multi-vectorielle (contenu du mail, pièces jointes et URLs), s'appuyant sur nos dernières technologies d'intelligence artificielle.

Cette solution s'adresse :
TPE **PME** **ETI**

6 ans de R&D en IA
pour la détection des menaces avancées

< 3 secondes
pour analyser un mail

30 moteurs de détection

Principales fonctionnalités

Analyse approfondie en temps réel : L'intégralité du mail et ses pièces jointes sont analysés par plus de 30 moteurs de détection ciblant les dernières menaces.

Anti-phishing : IA propriétaire exclusive, BEC et usurpation, vérification SPF/DKIM/DMARC, 500+ règles spécialisées, anti-spam.

Sécurité des pièces jointes : Deep Learning GLIMPS, détection zero-day, antivirus multiples, extraction récursive.

Liens et URLs : Blocage des domaines dangereux, base anti-phishing enrichie, catégorisation web.

Corrélation globale : Analyse croisée (corps et en-têtes)/ pièces jointes/URLs pour un verdict unifié et une détection des attaques multi-vecteurs.

Remédiation automatique : Mise en quarantaine des menaces sans action de l'utilisateur, sans latence sur la distribution et les performances M365.

Points clés

- IA propriétaire
- Visibilité totale sur les menaces
- Multi-tenant
- Architecture SaaS
- Intégration simplifiée via Microsoft Graph API
- Facile à prendre en main
- Solution créée et hébergée en France
- Confidentialité des données

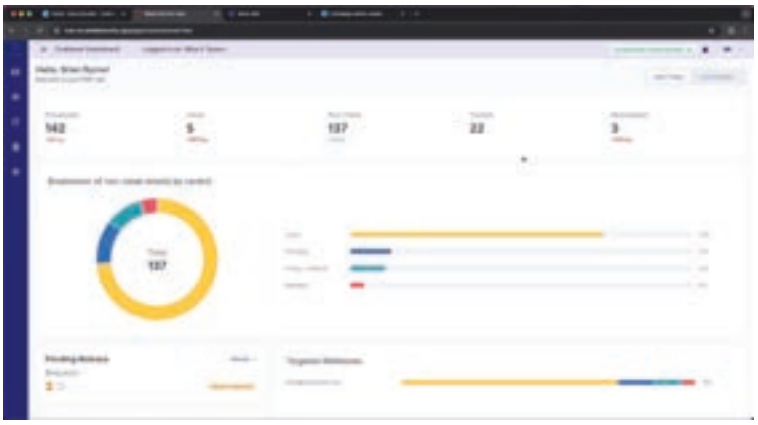
GLIMPS
(+33) 2 44 84 78 44
1179 Avenue des Champs Blancs
35510 Cesson-Sévigné
www.glimps.re

Demandez une démonstration

Extended Email Security
Bitdefender

Pays d'origine : Roumanie

GravityZone Extended Email Security intègre deux couches d'analyse :
- une passerelle de messagerie sécurisée (SEG) pour le phishing, les spams et les malwares
- une API O365 pour analyser en continu les BAL, détecter, placer en quarantaine ou supprimer les menaces.



Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

94% des malwares sont distribués par Email

30% des attaques par Email utilisent des liens malveillants

99,999 % est le taux de détection du phishing de Bitdefender

Principales fonctionnalités

Deux couches de protection : Une défense continue qui fonctionne au niveau du périmètre et de la BAL.

Flexibilité du déploiement : Mise en place de la SEG ou du filtrage basé sur une API ou les deux pour adapter la sécurité aux architectures cloud ou hybrides.

Architecture cloud-native : La CAPES offre un déploiement rapide, une évolutivité adaptative et une visibilité temps réel sur les écosystèmes de messagerie.

GUI moderne et intuitive : Elle permet aux administrateurs et aux utilisateurs finaux d'être autonomes, avec un minimum de formation.

Authentification des e-mails : Protégez votre domaine et réputation grâce aux normes SPF, DKIM et DMARC.

Résumé de quarantaine : Quarantaine en libre-service, les employés peuvent libérer des messages en toute sécurité et en toute simplicité.

Points clés

- Facturation mensuelle à la boite O365
- API Office 365
- Solution orientée MSP
- Hébergement en Europe
- Ingénieurs support en France
- Intégration XDR dans GravityZone
- Formation et certification gratuites
- Licences gratuites pour les partenaires MSP

Distribué par
Arrow ECS SAS France
Ingram Micro France SAS
RG System by Septeo
FieldTrust BELUX

Bitdefender SAS
(+33) 1 47 35 72 73
49 Rue de la Vanne
92120 Montrouge
www.bitdefender.fr

Demandez une démonstration

OpenText Email Threat Protection

OpenText Cybersecurity

Pays d'origine : Canada

Protection email avancée : anti-phishing, anti-malware, sandboxing, contrôle des liens et usurpation d'identité. Déploiement rapide via cloud, gestion centralisée pour MSP et très faible taux de faux positifs.

99 % Des emails malveillants bloqués

3 secondes Analyse rapide des messages

95 % Réduction des risques d'hameçonnage

Principales fonctionnalités

Anti-Phishing Avancé : Détecte les tentatives d'usurpation et liens malveillants.

Protection Malware : Analyse en temps réel des pièces jointes.

Sandboxing Cloud : Exécute les fichiers suspects en environnement isolé.

Filtrage Contenu : Règles personnalisées par client MSP.

DKIM/DMARC/SPF : Vérification complète de l'authenticité email.

Console Multi-tenant : Contrôle centralisé pour MSP.

Points clés

- Réduit les attaques de phishing
- Fort taux de détection
- Très faible faux positifs
- Déploiement rapide
- Compatible Microsoft 365
- Analyse liens en temps réel
- Gestion centralisée MSP
- Haute disponibilité cloud

Distribué par
OpenText Cybersecurity

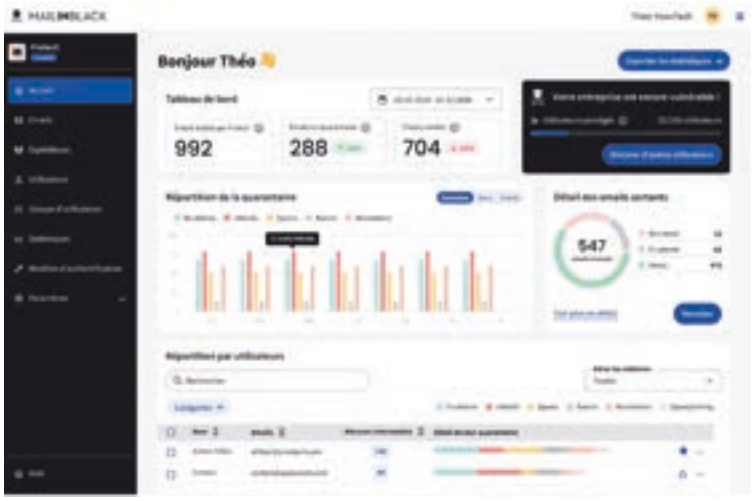
OpenText Cybersecurity
(+33) 1 47 96 65 24
Cœur Défense Tour B
92400 Paris la Défense
cybersecurity.opentext.com

Demandez une démonstration

Protect
Mailinblack

Pays d'origine : France

Protect identifie et bloque les messages frauduleux avant qu'ils n'atteignent les collaborateurs : phishing, spearphishing, ransomware, spam. Utilisable de manière indépendante ou intégrable à l'offre U Cyber 360°, Protect réduit les risques de cyberattaques et allège les boîtes mail.



Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

+20 ans d'expertise en cybersécurité

25 000 organisations protégées

96% de renouvellement clients

Principales fonctionnalités

Protection anti-virus et anti-spam : Au cœur de Protect, cette protection est renforcée par une IA qui affine le filtrage des spams sans nuire à l'expérience.

Protection anti-spearphishing : Protect identifie et priorise les vulnérabilités utilisateurs pour bloquer les fraudes et les compromissions ciblées.

Cockpit de pilotage : Votre plateforme vous permet de comprendre et agir avec précision (état des vulnérabilités, comportements à risque, remédiations).

Alerting : Protect assure une surveillance active et des alertes avancées pour détecter instantanément usurpations et activités suspectes.

Protect Out : Protect sécurise vos envois et assure la protection de vos destinataires grâce à sa technologie d'analyse des mails sortants.

Secure Link : Secure Link intégré à Protect bloque les URLs forgées, ayant pu contourner la 1ère analyse via obfuscation.

Points clés

- Cloud / SaaS
- On-premise
- Hébergement souverain
- Multitenant
- Portail Partenaire dédié
- Formation et certification incluses
- Licences NFR (Not For Resale)
- Support francophone

Distribué par
Actual Systèmes
MCA Technology
Arrow ECS France
Soft Value

Mailinblack
(+33) 4 88 60 07 80
4 Place Sadi Carnot
13002 Marseille
www.mailinblack.com

Demandez une démonstration

ESET PROTECT Complete

ESET

Pays d'origine : Slovaquie

Une cybersécurité complète pour protéger les endpoints, environnements Cloud et messageries de vos clients à un coût maîtrisé. Ajoutez une couche de protection supplémentaire aux environnements de messagerie, de collaboration et de stockage Microsoft 365 et Google Workspace.

Principales fonctionnalités

Protection multicouche avancée : Une prévention des endpoints face aux malwares, menaces 0-day et de l'exploitation des vulnérabilités.

Protection de la messagerie : Couche de défense supplémentaire au niveau du serveur de messagerie pour contrer le spam et les malwares.

Protection M365 et Google Workspace : Fonctionnalités de filtrage mail et d'analyse des malwares qui contribuent à protéger les communications et le le stockage Cloud.

Athena Global Services
(+33) 1 55 89 08 88
5 Avenue du Prieuré
Bâtiment B, 77700 Serris
www.eset.com/fr

Distribué par
ACTN
Actual Systèmes
DSD
EDOX
Hermitage Solutions

Sécurité des emails

BARRACUDA NETWORKS

Pays d'origine : États-Unis

Barracuda Email Protection : protection de Microsoft 365 contre les menaces les plus avancées. Découvrez nos plans Advanced, Premium et Premium Plus et composez l'offre la mieux adaptée pour relever les défis cyber de vos clients.

Principales fonctionnalités

Email Protection Advanced :
Détection et réponse alimentées par l'IA
- Réponses automatisées aux incidents
- Prévention contre la fuite de données

Email Protection Premium :
Advanced + :
- Backup M365 illimité
- Scan malware avant restauration
- Correction des partages de fichiers inappropriés

Email Protection Premium Plus :
Premium + :
- Archivage dans le cloud
- Formation à la sécurité*
- Simulation d'attaque*

* clients MSP : formations de sensibilisation à la sécurité et des simulations d'attaques disponibles sous forme de service managé complémentaire.

Infinigate France - BU BARRACUDA
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/barracuda-networks/

Distribué par
Infinigate France

Serenamail

Alinto

Pays d'origine : France

Serenamail est un relais SMTP sécurisé dédié à la délivrabilité des emails transactionnels. Il garantit une fiabilité des envois tout en protégeant les adresses IP et la réputation des domaines. La supervision et l'accès aux logs en libre-service permettent de suivre les envois en temps réel.

www.alinto.com

GreatHorn Cloud Email Security Platform

Greathorn

Pays d'origine : États-Unis

GreatHorn combine détection comportementale, analyse en temps réel et réponse automatisée pour contrer les attaques avancées par email (BEC, spearphishing, URLs malveillantes). La plateforme fournit recherche granulaire et suppression en masse des menaces détectées, réduisant le temps de réponse.

www.greathorn.com/products/cloud-email-security/

IRONSCALES

IRONSCALES

Pays d'origine : Israël

IRONSCALES protège contre le phishing, le BEC et les deepfakes grâce à l'utilisation de l'intelligence artificielle. La solution agit directement depuis la boîte de réception (Microsoft 365, Google Workspace), ce qui permet une détection et une remédiation immédiate, sans passer par une passerelle (SEG).

ironscales.com

SpamTitan

TitanHQ

Pays d'origine : Irlande

SpamTitan propose une protection robuste contre les ransomwares, malwares et liens piégés grâce à un filtrage multicouche combinant antivirus, analyse comportementale et sandboxing. Une solution conçue pour offrir à la fois visibilité centralisée et contrôle granulaire sans complexité excessive.

www.spamtitan.com

Environnement de travail collaboratif

Les plateformes collaboratives sont devenues des environnements fortement intégrés, combinant messagerie, partage documentaire, coédition, visioconférence et automatisation de workflows. Des environnements qui reposent majoritairement aujourd'hui sur les plateformes Microsoft 365 ou Google Workspace, souvent complétées par des outils spécialisés.

Cette intégration fonctionnelle a complexifié leur exploitation : multiplication des espaces, gestion granulaire des droits, ouverture à des utilisateurs externes et interconnexions applicatives multiples. Ces évolutions les plus structurantes portent sur la gouvernance : gestion des accès, cycle de vie des contenus, traçabilité des usages et alignement avec l'identité (SSO, MFA, accès conditionnel) sont devenus indispensables pour maintenir un contrôle opérationnel sans freiner les usages.

Ces environnements imposent une approche qui va au-delà du support applicatif. Il ne s'agit plus seulement de déployer ou de supporter des plateformes, mais de définir des règles d'usage, des modèles d'espaces et des politiques de sécurité reproductibles.

Signitic

Signitic

Pays d'origine : France

Signitic est un outil d'harmonisation de signatures mail pour Microsoft 365 et Google Workspace. Avec Signitic transformez chaque envoi en un média pilotable et performant. Simplifiez votre gouvernance IT et boostez votre marketing grâce à une gestion 100% automatisée.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

850000 utilisateurs de la solution

10 ans d'expérience sur le marché

5000 clients à travers l'Europe

Principales fonctionnalités

Centralisation et harmonisation : Transformez chaque e-mail en média marketing performant. Pilotez vos campagnes et automatisez la gestion de vos signatures.

Pilotez vos bannières mail : Diffusez vos campagnes marketing via chaque e-mail. Programmez vos bannières, ciblez vos audiences et mesurez vos performances.

Cartes de visite digitales : Dématérialisez vos cartes de visite : créez, partagez via QR Code ou NFC et synchronisez vos nouveaux contacts avec votre CRM.

Points clés

- Connectez Microsoft 365 à Signitic en un clic & sans effort
- Liez Google Workspace à Signitic en un clic et sans effort
- Notre équipe support est basée à Lyon et répond en français
- La sécurité et conformité RGPD garanties à 100%
- Signitic est certifié ISO/IEC 27001
- Signitic est une Solution SaaS
- Engagement RSE
- Notre support est joignable par téléphone, mail et chat

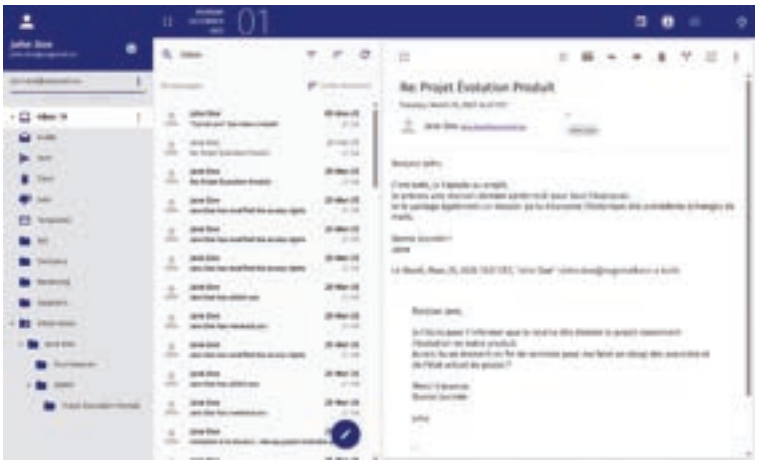
Signitic
(+33) 4 69 96 99 76
152 Rue Pierre Corneille
69003 Lyon
www.signitic.com

Demandez une démonstration

Sogomail
Alinto

Pays d'origine : France

Un service de messagerie collaborative, souverain et sécurisé. Il facilite la gestion et le partage des dossiers de mails, calendriers et contacts. Bâti sur des briques open source, il est compatible avec les protocoles standards, il fonctionne dans un environnement multi-tenant et carrier grade.



Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

10 000+ Organisations accompagnées

26 ans d'expérience

1 000 000+ Utilisateurs

Principales fonctionnalités

Fonctionnalités groupware : Sogomail facilite la collaboration des utilisateurs grâce au partage des dossiers, calendriers, contacts,..

Gestion avancée : Administration par API avec une gestion granulaire des droits utilisateurs et des profils.

Accessibilité : Compatible avec tous les clients de messagerie (Outlook, Thunderbird..) et smartphones, tablettes, etc.

Support des protocoles standards : IMAP, POP, SMTP, CalDAV, CardDAV, Active Sync. Compatible avec Outlook pour une interopérabilité complète. MAPI (prev 2026).

Marque blanche : Sogomail s'adapte complètement à l'image de votre marque (couleur, logo & URL), et s'intègre sans effort à votre environnement.

Flexibilité de déploiement : Possibilité de déployer Sogomail en configuration multi-tenant, selon vos besoins dans le cloud Alinto ou sur vos infrastructures.

Points clés

- Cloud / Saas
- PaaS Multitenant
- Équipe Support Expert
- Accompagnement technique et commercial
- Facturation à l'usage
- Marque Blanche
- Logiciel & Hebergement éco-responsables
- Conforme RGPD

Distribué par
Orange Business
CELESTE
Canalpus Telecom
Luminess
Inetum

Alinto
(+33) 4 81 09 01 10
19 Quai Perrache
69002 Lyon
www.alinto.com

Demandez une démonstration

eXo Platform

eXo Platform

Pays d'origine : France

eXo Platform est un espace de travail collaboratif open source combinant intranet, réseau social d'entreprise, gestion documentaire et portail applicatif. Conçu pour les organisations recherchant souveraineté numérique et personnalisation, il intègre des fonctions avancées de gouvernance et d'IA contextuelle.

www.exoplatform.com

Interstis

Interstis

Pays d'origine : France

Pensée pour le secteur public et les organisations sensibles, Interstis propose une plateforme collaborative hébergée en France, certifiée SecNumCloud. Elle centralise messagerie, documents, visioconférence et gestion de projet dans un environnement souverain et conforme aux exigences RGPD.

www.interstis.fr

Twake Workplace

Twake Workplace

Pays d'origine : France

Twake est une solution open source qui se distingue par une architecture modulaire facilitant l'intégration d'outils tiers (OnlyOffice, Jitsi, Nextcloud). Elle permet de construire un environnement de travail collaboratif sur mesure, avec un contrôle complet des flux de données et des permissions.

twake.app

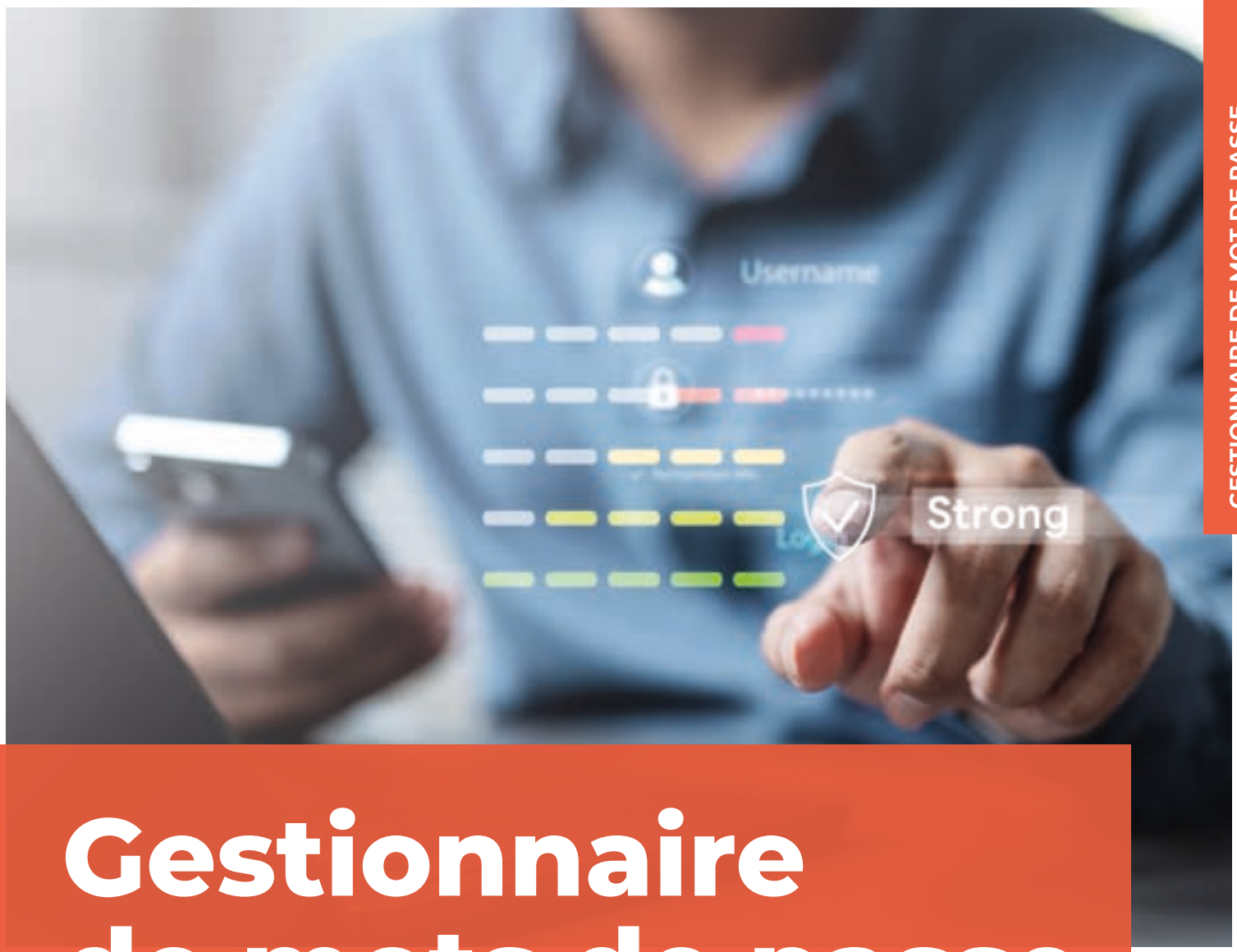
Wimi

Wimi

Pays d'origine : France

Wimi structure le travail d'équipe autour d'espaces projet centralisant documents, discussions, tâches et visioconférences. Sa gestion des droits avancée permet d'impliquer clients et partenaires sans compromettre la confidentialité. Une solution adaptée aux environnements multi-acteurs et projets sensibles.

www.wimi-teamwork.com/fr



Gestionnaire de mots de passe

La généralisation des identités dans le cloud, la multiplication des comptes applicatifs et l'usage massif d'API et de services SaaS ont déplacé le sujet du stockage sécurisé vers la gestion granulaire des privilèges et des contextes d'accès. Les gestionnaires de mots de passe intègrent désormais des mécanismes de chiffrement de bout en bout, de partage contrôlé, de rotation automatique des secrets et d'audit des usages.

L'enjeu technique se situe désormais dans l'intégration avec l'identité et l'authentification forte : synchronisation avec les annuaires, MFA, politiques conditionnelles et journalisation des accès. Les frontières avec le PAM deviennent plus poreuses, notamment sur la gestion des comptes à privilèges applicatifs et des accès temporaires.

Le gestionnaire devient avant tout un outil de normalisation des accès : définir des règles cohérentes de création, de stockage et de révocation, tout en réduisant les pratiques à risque comme le partage non maîtrisé, les mots de passe en dur. Dans la pratique, l'enjeu reste souvent moins technologique que managérial : faire respecter l'usage du gestionnaire face aux contournements persistants et aux workflows applicatifs mal intégrés.

MSP Console
LastPass

Pays d'origine : États-Unis

LastPass aide les entreprises à renforcer la sécurité autour des identifiants & mots de passe grâce à un coffre-fort numérique & des fonctionnalités comme le dark web monitoring, SaaS Protect & MFA. La console MSP permet de facilement gérer et déployer des licences pour chaque client.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

Depuis 17 ans expert en gestion des identités & accès

1 Milliard de mots de passe protégés

1200 clients B2B français

Principales fonctionnalités

Une plateforme fiable & évolutive : Une plateforme fiable pour gérer les mots de passe via un coffre-fort numérique avec une expérience utilisateur facile.

SaaS Monitoring & Protect : Réduisez les risques de Shadow IT-IA grâce à plus de visibilité et de contrôle sur l'utilisation des applications SaaS.

Dark Web Monitoring : Vos clients seront informés en cas d'identifiant compromis via notre fonctionnalité de surveillance du dark web.

Tableau de bord intuitif : Simplifiez la gestion des clients avec un tableau de bord personnalisé : l'adoption, l'utilisation et le niveau de sécurité.

Partage sécurisé des identifiants : Permettez un partage sûr des informations d'accès entre équipes et clients, sans compromettre la confidentialité.

Gestion des licences : Attribuez facilement des licences à vos clients, quelle que soit leur taille, et ajustez-les selon l'évolution de leur activité.

Points clés

- Console multi-tenant
- Compatible M365 (et IDPs) & connexion fédérée
- Facturation Mensuelle
- Portail partenaire pour les besoins Marketing & Technique
- NFR incluses
- Des formations & certifications à disposition
- Conformité RGPD
- Conformité SOC 2, SOC 3, ISO 27001 & 27701

Distribué par
Actual Systèmes
Net Point

LastPass
(+353) 8 77 92 37 55
Ella House
41.2 Merrion Square
Dublin 2, Irlande
www.lastpass.com

Demandez une démonstration

Sikker

Mailinblack

Pays d'origine : France

Utilisable de manière indépendante ou intégrable à l'offre U Cyber 360°, Sikker centralise les identifiants dans un coffre-fort chiffré en zero-knowledge, facilite l'usage quotidien (remplissage automatique des mots de passe, partage sécurisé) et empêche la compromission de vos mots de passe.

Cette solution s'adresse :

TPE **PME** **ETI** **Grands comptes**

+20 ans d'expertise

25 000 organisations protégées

96% de renouvellement clients

Principales fonctionnalités

Protection de vos accès : Centralisez et protégez vos mots de passe, informations confidentielles et données bancaires dans un coffre fort ultra sécurisé.

Simplicité & gain de temps : Générateur de mots de passe robustes en un clic, connexion rapide et sécurisée, mise à jour automatique des identifiants.

Collaboration fluide & sécurisée : Coffres-forts partagés, contrôle granulaire des accès, partage instantané et chiffré.

Surveillance & prévention avancées : Sikker travaille en arrière-plan pour surveiller en continu les fuites de données et vous informer en cas de compromission.

Sécurité intransigeante : Protection de niveau militaire (Chiffrement AES 256-bit), Argon2, HKDF, RSA & Zero-Knowledge.

Pilotage centralisé : Le dashboard permet aux admins une gestion optimisée des mots de passe grâce à des alertes sur les usages de leurs collaborateurs.

Points clés

- Cloud / SaaS
- On-premise
- Hébergement souverain
- Multitenant
- Portail Partenaire dédié
- Formation et certification incluses
- Licences NFR (Not For Resale)
- Support francophone

Distribué par
Actual Systèmes
MCA Technology
Arrow ECS France
Soft Value

Mailinblack
(+33) 4 88 60 07 80
4 Place Sadi Carnot
13002 Marseille
www.mailinblack.com

Demandez une démonstration

UpSignOn
RG System Suite

Pays d'origine : France

Sécurisez, centralisez et partagez les identifiants de vos clients dans un coffre-fort chiffré, hébergé en France et accessible uniquement aux membres autorisés. UpSignOn by Septeo vous permet de mieux structurer les accès sensibles et de fluidifier la collaboration de vos équipes au quotidien.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

100 % Français

30 min temps de déploiement moyen observé

4 ans+ d'utilisation par les MSP

Principales fonctionnalités

Gestion des informations sensibles : Gestion des mots de passe, codes TOTP pour la double authentification et données bancaires en toute sécurité.

Console de supervision : Console de supervision offrant une vue d'ensemble de l'activité et de la robustesse globale des mots de passe.

Niveaux d'accès personnalisés : Gestion personnalisée des niveaux d'accès pour contrôler qui peut consulter, modifier ou administrer les informations partagées.

Synchronisation automatique : Les données sont synchronisées automatiquement entre tous les appareils connectés.

Gestion des appareils autorisés : Vue des appareils connectés au coffre-fort pour un meilleur contrôle des accès.

Extension de navigateur : Remplissage automatique des formulaires et enregistrement instantané des nouveaux mots de passe via l'extension de navigateur.

Points clés

- Sécurité avancée avec chiffrement de bout en bout
- Une solution 100 % française hébergée en France
- Multi-tenant et multi-plateformes
- Full SaaS
- Tarification claire avec abonnement mensuel ou annuel
- Support francophone
- Channel Account Manager dédié

Distribué par
Cris Réseaux
Actual Systèmes
DSD

Septeo IT Solutions
(+33) 4 11 93 42 00
194 Avenue de la Gare
Sud de France
34970 Lattes
upsignon.eu

Demandez une démonstration

IAM/PAM

La généralisation des environnements cloud, des API et des services SaaS a déplacé l'IAM vers une fonction de contrôle dynamique des accès, étroitement liée au contexte, à l'identité et au niveau de risque. L'IAM n'est plus un annuaire enrichi, mais un moteur de décision conditionnant l'accès aux ressources à partir de signaux multiples.

Son périmètre dépasse désormais largement les comptes utilisateurs classiques. La montée en puissance des identités non humaines (API, workloads, scripts, chaînes CI/CD) constitue un point de tension supplémentaire, leur cycle de vie échappant encore largement aux modèles traditionnels.

L'accès conditionnel et le MFA adaptatif s'imposent comme des mécanismes natifs des environnements cloud. Le PAM prolonge cette logique en adressant les comptes à privilèges, humains comme applicatifs, via l'élévation temporaire, la traçabilité et la rotation des secrets.

Conséquence : la frontière historique entre IAM et PAM s'estompe au profit d'approches unifiées fondées sur le moindre privilège. L'efficacité d'un ensemble IAM/PAM se mesure désormais à la gestion des droits dans le temps : création, élévation, révocation et traçabilité des accès, y compris pour des usages temporaires ou automatisés.

WALLIX PAM / WALLIX ONE PAM (SaaS)

WALLIX

Pays d'origine : France

WALLIX est un éditeur européen de cybersécurité, expert en PAM et IAM. Ses solutions protègent les accès et identités des utilisateurs, sécurisent les environnements IT et industriels, et accompagnent plus de 4 000 organisations dans 100+ pays vers un numérique de confiance.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

4 000+ Organisations protégées

300+ partenaires certifiés dans le monde

20 ans d'expertise dans la cybersécurité

Principales fonctionnalités

Gestion des accès à privilèges (PAM) : Contrôle centralisé, rotation automatisée des mots de passe, accès sécurisé aux applications web.

Enregistrement des sessions : Enregistrement vidéo complet, pistes d'audit pour la conformité.

Rotation des mots de passe : Rotation automatisée des identifiants à privilèges afin d'éliminer les mots de passe statiques et de maintenir la conformité.

AAPM : Éliminez les mots de passe codés en dur dans les scripts et les fichiers de configuration.

Accès legacy et OT : Accès sécurisé et unifié aux nouveaux comme aux systèmes legacy OT via l'unniversal Tunneling.

Sécurité OT/IT : Connexion transparente aux systèmes de production industriels, protection des environnements SCADA.

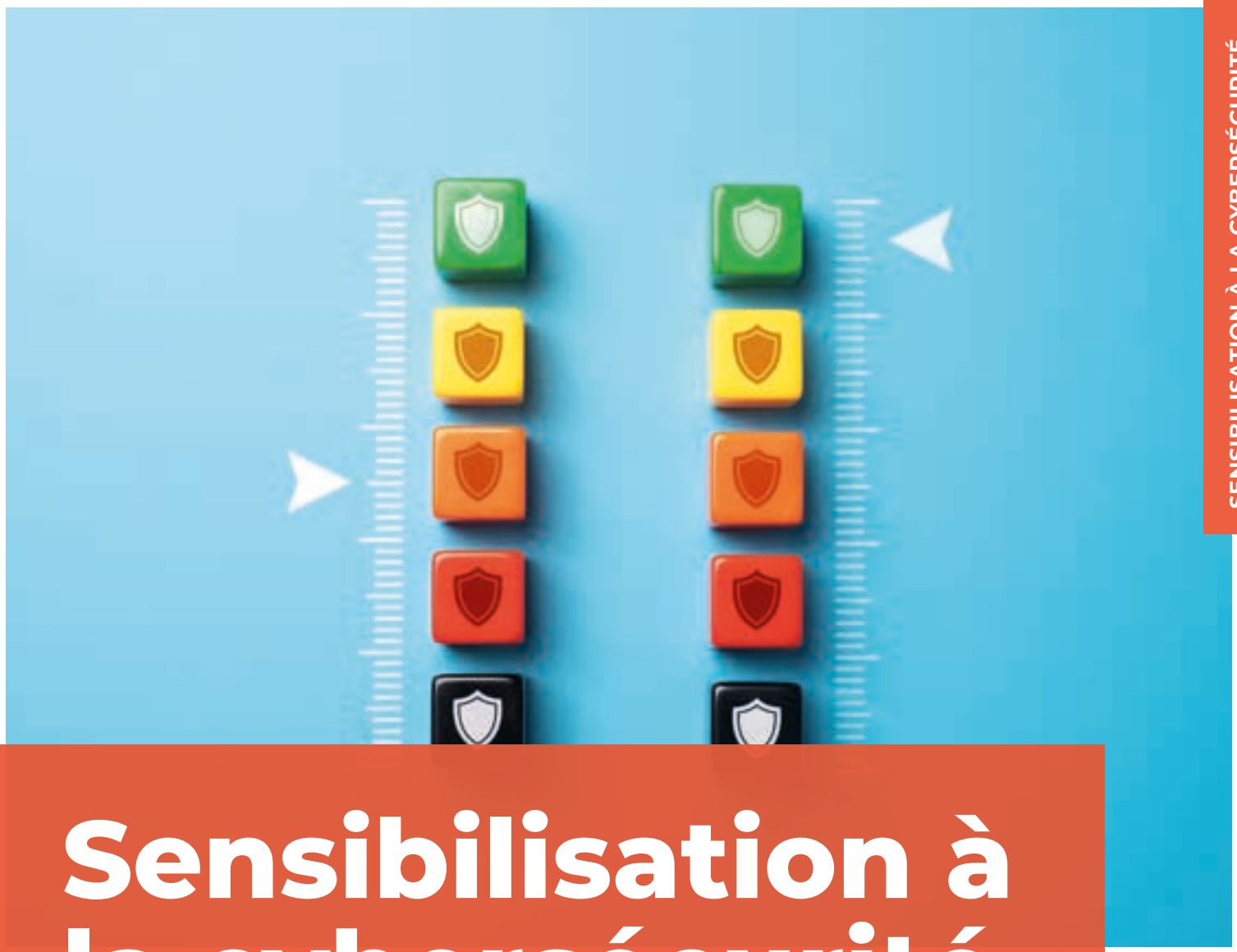
Points clés

- Certifié BSI, équivalent CSPN ANSSI
- Conforme aux exigences NIS2, DORA, RGPD et AI Act
- Flexibilité max : déploiement Cloud, SaaS ou On-premise
- Visionnaire Magic Quadrant Gartner 3 années de suite
- Solution souveraine européenne
- Déploiement sans agent
- Support francophone, pour un accompagnement de proximité
- Large bibliothèque documentaire disponible

Distribué par
CRIS RESEAUX

WALLIX
250 bis Rue du Faubourg Saint Honoré
75008 Paris
www.wallix.com

Demandez une démonstration



Sensibilisation à la cybersécurité

Qu'elle se présente sous la forme d'une campagne statique, d'un serious game, d'un agent IA ou qu'elle s'intègre au moment de la détection de la menace, l'action de sensibilisation à la cybersécurité est aujourd'hui protéiforme.

Scénarios contextualisés, campagnes continues, simulations de phishing adaptatives, indicateurs de progression individuels et collectifs : la sensibilisation s'inscrit dans le temps long et s'ancre dans les usages réels. Elle n'est plus reléguée à un simple e-mail factice et couvre l'ensemble des cas d'usage de l'entreprise : mail, SMS, Teams, WhatApp, QR-Code, appel téléphonique.

Ses résultats ne se limitent plus à des taux de clic ou de complétion. Ils alimentent des arbitrages concrets : ciblage des populations à risque, renforcement de contrôles techniques, ajustement des politiques de sécurité. Opérationnellement, ces dispositifs permettent d'indiquer là où le RSSI doit engager des actions correctives. Économiquement, ils constituent une brique non négligeable des offres de cybersécurité managée, avec un fort potentiel de récurrence.

Cyber Coach & Cyber Academy

Mailinblack

Pays d'origine : France

Utilisable de manière indépendante ou intégrable à l'offre U Cyber 360°, Coach & Academy forment une solution complète de sensibilisation et formation cyber : Coach entraîne les collaborateurs via des simulations d'attaques réalistes et Academy consolide les acquis grâce à des formations engagées.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

+20 ans d'expertise

25 000 organisations protégées

96% de renouvellement clients

Principales fonctionnalités

Audit des vulnérabilités humaines : Évalue le niveau de vulnérabilité des collaborateurs face aux cybermenaces afin d'identifier les comportements à risque.

Simulations d'attaques réalistes : Teste les réflexes des utilisateurs en simulant des attaques réalistes (phishing, ransomwares, BitB, QR Code, Clé USB...).

Sensibilisation automatisée : Déploie des campagnes de sensibilisation continues et adaptatives, ajustées au niveau de maturité de chaque utilisateur.

Formation e-learning cybersécurité : Accède à une plateforme de formation en ligne avec des modules courts, interactifs et accessibles à tous les collaborateurs.

Parcours ludique et gamifié : Engage les utilisateurs grâce à des mécaniques de jeu favorisant l'apprentissage et l'amélioration continue des compétences.

Reporting et suivi des performances : Analyse les résultats via des tableaux de bord clairs pour mesurer l'impact des actions de sensibilisation et formation.

Points clés

- Cloud / SaaS
- Hébergement souverain
- Account Manager dédié
- Multitenant
- Portail Partenaire dédié
- Formation et certification incluses
- Licences NFR (Not For Resale)
- Support francophone

Distribué par
Actual Systèmes
MCA Technology
Arrow ECS France
Soft Value

Mailinblack
(+33) 4 88 60 07 80
4 Place Sadi Carnot
13002 Marseille
www.mailinblack.com

Demandez une démonstration

OpenText Security Awareness

OpenText Cybersecurity

Pays d'origine : Canada

Formations simples, tests de phishing et reporting clair pour réduire le risque humain. Programme clé en main pour MSP, facile à déployer et à mesurer afin d'augmenter la maturité clients.

Cette solution s'adresse :
TPE **PME** **ETI**

70 % Réduction prouvée des attaques

5x Moins de clics sur les liens piégés

90 % Employés sensibilisés durablement

Principales fonctionnalités

Modules de Formation : Sessions courtes et engageantes pour les utilisateurs.

Tests de phishing : Campagnes simulées automatisées.

Reporting utilisateur : Scores et progrès mesurés facilement.

Catalogue multi-langues : Adapté à toutes les équipes en France et à l'étranger.

Déploiement MSP : Automatisation des campagnes par client.

Rappels automatiques : Améliore les taux de complétion.

Points clés

- Réduit le risque humain
- Formation continue
- Rapports faciles pour MSP
- Contenu simple à comprendre
- Multi-langues
- Simulations réalistes
- Améliore la conformité
- Très faible coût de gestion

Distribué par
MIEL
IPSteel
OpenText Cybersecurity

OpenText Cybersecurity
(+33) 1 47 96 65 24
Cœur Défense Tour B
92400 Paris la Défense
cybersecurity.opentext.com

Demandez une démonstration

La plateforme cyber des employés
RIOT

Pays d'origine : France & États-Unis

Riot est la première solution de suivi en temps réel de la cybersécurité des employés. La plateforme aide les équipes cyber, quelle que soit la taille de l'entreprise, à évaluer et renforcer la posture cyber des collaborateurs, devenus la première ligne de défense face aux cyberattaquants.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

2 000 000+
d'employés protégés

2 000+ clients
dans le monde entier

4.8/5 Évaluation
sur G2

Principales fonctionnalités

Voici Albert, votre coach cyber : Renforcez la posture cyber de vos équipes dans les gestes du quotidien, en les faisant agir pendant leur formation.

Smishing & Phishing tout-terrain : Créez vos propres scénarios d'attaque avec l'IA, ou choisissez parmi plus de 400 templates e-mails et SMS éprouvés.

Sonar, le partage en sécurité : Scannez vos Drive et impliquez réellement les employés dans la gestion des accès.

Slash, la hotline cyber 7j/7 : Protégez les emails en temps réel, alerte les employés, bloque les usurpations et met automatiquement en quarantaine les menaces.

Studio, du contenu sur-mesure : Décrivez à Albert vos enjeux, il créera une formation sur mesure, fidèle à sa voix.

Brèches : restez informés : Détectez les fuites de données qui impliquent vos employés, alertez les et aidez les à sécuriser leurs informations.

Points clés

- Riot est certifié SOC 2, et ISO 27001 fin 2026
- Assistance premium 24/7
- Riot est conforme au RGPD
- Intégration native avec Microsoft 365
- Intégration native avec Google Workspace
- Installation rapide et fluide, sans matériel requis
- Gestion centralisée et sécurisée de plusieurs entités

Distribué par
Wavestone
Wakers
Sonema
Agesys
Easy Service

RIOT SECURITY
20 Rue de Turenne
75004 Paris
tryriot.com

Demandez une démonstration

Arsen

Arsen

Pays d'origine : France

Arsen propose des simulations réalistes de phishing, vishing (voix), smishing (SMS) et deepfake, renforcées par l'IA, pour entraîner les utilisateurs à reconnaître les cyberattaques. Chaque campagne s'adapte aux profils ciblés, avec des rapports détaillés permettant de prioriser les actions de formation.

arsen.co/en

CyberGuru

Cyber Guru

Pays d'origine : Italie

Cyber Guru mise sur une formation continue intégrée au rythme de travail. En combinant micro-apprentissages, tests contextuels et indicateurs de progression, la solution aide les organisations à ancrer des réflexes de cybersécurité et à répondre aux exigences de conformité internes ou sectorielles.

www.cyberguru.it

Gophish

Gophish

Pays d'origine : États-Unis

Gophish est un framework open source conçu pour lancer rapidement des campagnes de phishing simulé. Léger, autonome et pilotable via API, il permet aux équipes sécurité de créer leurs propres scénarios, suivre les résultats en temps réel et intégrer l'outil dans leur pipeline de test.

getgophish.com

uSecure

uSecure

Pays d'origine : Royaume-Uni

uSecure se distingue par son approche basée sur des scores de risque individuel et collectif, permettant de prioriser les actions selon les profils. La plateforme propose des modules thématiques courts, des campagnes phishings automatisées et des tableaux de bord dédiés aux équipes de gouvernance.

usecure.io

Demain
tous MSSP

EDR / XDR

Les solutions EDR/XDR s'inscrivent aujourd'hui au-delà de la simple collecte de télémétrie du poste de travail. Elles permettent désormais de normaliser et de corréler des événements hétérogènes (activités poste, signaux d'identité, messagerie, réseau et environnements cloud), afin de reconstruire des chaînes d'attaque exploitables.

Le XDR se distingue moins par la variété des sources que par la qualité de la corrélation et du contexte appliqué aux alertes : réduction du bruit, priorisation avec des moteurs de détection intégrant privilèges, exposition et criticité des actifs pour limiter les alertes non actionnables.

Il ne s'agit plus de déployer un agent, mais bien d'être capable de configurer, superviser et opérer ces outils à l'échelle, avec des processus clairs d'escalade et de remédiation.

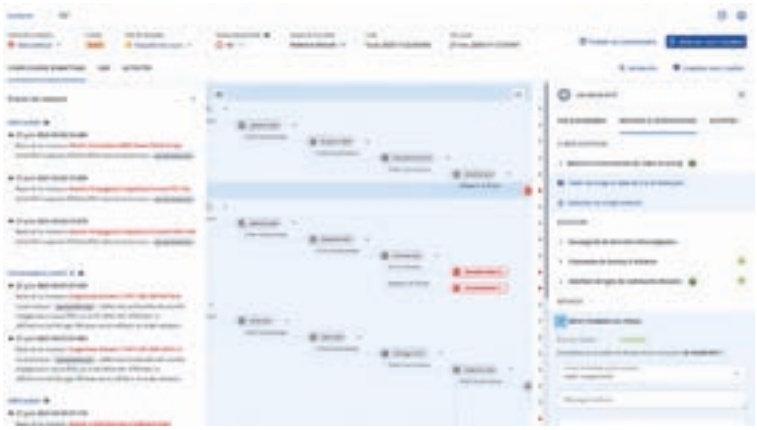
L'EDR/XDR introduit de fait une contrainte de plus en plus forte sur l'organisation du prestataire, tant en compétences qu'en responsabilité opérationnelle, avec des effets directs sur les coûts, la standardisation des offres et les modèles de mutualisation. C'est à ce niveau que se creuse l'écart entre intégration opportuniste et service de sécurité réellement opéré.

Acronis EDR / XDR

Acronis

Pays d'origine : Suisse

Détectez et neutralisez rapidement les menaces les plus sophistiquées grâce à une solution boostée par l'IA. Capacités de réponse étendues, intégrations natives avec la sauvegarde et le PRA. La plateforme Acronis Cyber Protect Cloud assure la continuité d'activité et reste simple d'utilisation.



Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

750 000 entreprises protégées dans le monde via des MSP Acronis

20 000 fournisseurs de services utilisent la plateforme Acronis

7,5 millions d'attaques bloquées en 12 mois grâce à Acronis

Principales fonctionnalités

Détection et réponse avancées : Identification rapide des menaces et actions de remédiation immédiates pour limiter l'impact des incidents.

Vue complète de la chaîne d'attaque : Résumés d'incidents basés sur l'intelligence artificielle et interprétations des attaques dans le cadre MITRE ATT&CK®.

Priorisation des incidents : Obtenez une vue classée par ordre de priorité des incidents à étudier plutôt qu'une liste non hiérarchisée de toutes les alertes.

Détection proactive des menaces : Améliorez la traque des menaces avec une cyberveille capable d'identifier les indicateurs de compromission.

XDR intégré et centralisé : Corrélation des événements de sécurité issus des pare-feu Fortinet, de Microsoft Entra ID et de la protection de la messagerie.

Points clés

- Hébergement par Acronis
- Hébergement en France
- Console multi-tenant
- Facturation mensuelle
- Portail partenaires
- Formations et certifications sur-mesure pour les MSP
- Conformité réglementaire éprouvée
- Solution certifiée

Distribué par
TD SYNNEX
Infinigate France
ALSO

Acronis
(+33) 1 87 16 91 19
20-22 Rue Marius Aufan
92300 Levallois-Perret
www.acronis.com

Demandez une démonstration

Business Premium

MICROSOFT

Pays d'origine : EMEA

Profitez d'une suite d'outils complète et unifiée : Office, Teams, OneDrive, SharePoint et plus. Gérez vos tâches, collaborez efficacement et sécurisez vos données grâce à des fonctionnalités avancées de productivité, d'administration et de cybersécurité.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

242 %+ ROI
en moins de 6 mois

-30 % de risques
fuite de données

-99 %
de compromissions MFA

Principales fonctionnalités

Sécurité avancée des postes : Protection EDR intégrée contre ransomwares, menaces zero-day et attaques avancées, sans solution tierce.

Gestion unifiée des appareils : Pilotez, sécurisez et mettez à jour PC, mobiles et tablettes depuis une console cloud centralisée.

Identités et accès sécurisés : Authentification multifacteur et contrôle des accès pour bloquer les attaques liées aux identités.

M365, votre espace de travail sûr : Collaborez en toute confiance avec Teams, Outlook et OneDrive dans un environnement sécurisé.

Protection intelligente des données : Identifiez, classez et protégez automatiquement les données sensibles pour éviter toute fuite.

L'IA au coeur de Business Premium : Associez Copilot Business à Business Premium pour un environnement productif, sécurisé et boosté par l'IA.

Points clés

- Solution idéale pour PME et ETI
- Protection des données conforme au RGPD
- Sécurité certifiée Microsoft
- Intégration native de l'IA Copilot
- Environnement de travail sûr
- Protection continue contre les cybermenaces
- Enablement et montée en compétences
- Accompagnement partenaire dédié TD SYNNEX

Distribué par
TD SYNNEX

TD SYNNEX
7 Avenue Hergé
77700 Chessy
cloud.tdsynnex.fr

Demandez une démonstration

Endpoint
Check Point

Pays d'origine : Israël

Notre solution endpoint est une solution complète de sécurité des postes de travail et des serveurs, conçue pour vous protéger contre les menaces les plus avancées, pour réduire rapidement l'impact des vulnérabilités grâce à une détection et à une réponse automatisée.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

Automatisation de 90% des tâches d'investigation et correction

60 moteurs d'IA

33 ans de sécurité, d'innovation, d'expertise

Principales fonctionnalités

Agent unifié : Plateforme de protection avancée du poste de travail, EDR, Protection Web, Filtrage URL, Phishing, Gestion des Vulnérabilités.

Support multi OS : Prise en charge de Windows, Mac, Linux, serveurs, VDI, et navigateurs.

Protection Zero day : ThreatCloud AI combine 60 moteurs d'IA avancés et 33 ans de threat-intel pour offrir le meilleur taux de prévention.

Protection contre les ransomwares : Analyse comportementale avancée permettant la detection et remediation contre les attaques les plus sophistiquées.

Protection du navigateur : Blocage des attaques de phishing les plus avancées avant qu'elles n'atteignent les utilisateurs.

Services managés MDR/XDR : Les experts de Check Point peuvent surveiller l'ensemble de votre infrastructure 24/7.

Points clés

- Licence Pay-As-You-Go
- Console multi-tenant
- Protection continue assurée par les experts de Check Point
- Gestion unifiée de la sécurité via un portail web unique

Distribué par
Arrow ECS
Infinigate
Westcon

Check Point Software
20 Avenue André Prothin
92400 Courbevoie
www.checkpoint.com

Demandez une démonstration

Endpoint Security
WatchGuard Technologies

Pays d'origine : États-Unis

Optimisées par l'IA, nos solutions combinent la protection des terminaux et EDR avec le service d'application Zero-Trust pour détecter les menaces en toute autonomie et riposter aussitôt avec précision. WatchGuard accède au rang de Leader et Outperformer dans le rapport Radar EDR 2025 de GigaOm.

Cette solution s'adresse :
TPE **PME** **ETI**

2/3 de la journée des admins sont dédiées aux alertes

100 % de classification avec le Zero Trust

1 agent unique et léger

Principales fonctionnalités

Zero-Trust intégré : Classifie 100 % des applications et bloque les mouvements latéraux pour réduire les risques et alléger la charge MSP.

Threat Hunting managé : Détection proactive des intrusions et attaques internes pour réduire MTTD/MTTR et renforcer l'offre MSSP.

Agent unique ultra-léger : Un seul agent pour toutes les protections, réduisant erreurs, complexité et impact sur la performance client.

IA auto-apprenante avancée : Analyse comportementale et détection LotL pour stopper ransomware et attaques sans fichier en temps réel.

Remédiation et rollback auto : Restauration automatique, isolation et récupération des fichiers chiffrés pour limiter l'intervention MSP.

Console Cloud multi-plateforme : Gestion simplifiée de tous les endpoints via une console unique Web, adaptée au multi-client MSP.

Points clés

- Gestion EPDR 100% Cloud pour MSP
- Administration centralisée multi-clients
- Support 24/7 pour incidents critiques
- Ressources MSP pour montée en compétence
- Compatible Chrome et services Google
- Protection renforcée Windows et Azure
- Sécurité Cloud adaptée aux exigences RGPD
- Agent unique : performance et simplicité

Distribué par
Arrow ECS
Infinigate France

WatchGuard Technologies
+33 97 755 4336
22 Boulevard de Stalingrad
92320 Châtillon
www.watchguard.com/fr

Demandez une démonstration

ESET PROTECT

ESET

Pays d'origine : Slovaquie

Vos clients évoluent, vos services aussi.
Optez pour une plateforme de cybersécurité pensée pour répondre à vos besoins.
Fort de 35 ans d'innovation, ESET PROTECT vous permet de prévenir, détecter et répondre aux menaces, tout en garantissant une gestion centralisée, adaptée à votre modèle MSP.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

1er éditeur européen de cybersécurité

1 milliard+ d'internautes protégés

500 000+ entreprises clientes

Principales fonctionnalités

Cloud ou On-Premise : ESET PROTECT est disponible en Cloud ou On-Premise, selon vos besoins et votre infrastructure.

Multi-tenant : Définissez différents types ou groupes d'utilisateurs, avec des accès compartimentés à ESET PROTECT.

Visibilité en temps réel : Offre une visibilité en temps réel de tous les endpoints managés : postes de travail, serveurs, machines virtuelles et mobiles.

Mobile Device Management : Le MDM Cloud inclus, Microsoft Intune, Apple Business Manager et VMware Workspace ONE sont pris en charge.

Reporting simple et personnalisé : ESET PROTECT propose plus de 170 rapports prédéfinis et personnalisables avec plus de 1000 types de données.

Intégrations RMM, SIEM et SOAR : L'intégration avec des outils tels que les RMM, SIEM et SOAR est possible grâce à nos API.

Points clés

- Console Cloud
- Console On-Premise
- Multi-tenant
- Intégration SIEM, RMM & SOAR
- Facturation mensuelle
- Automatisation des tâches
- ISO 27001
- Support en Français

Distribué par
ACTN
Actual Systèmes
DSD
EDOX
Hermitage Solutions

Athena Global Services
(+33) 1 55 89 08 88
5 Avenue du Prieuré
Bâtiment B, 77700 Serris
www.eset.com/fr

Demandez une démonstration

ESET PROTECT Elite

ESET

Pays d'origine : Slovaquie

Parce que l'exigences de vos clients en matière de cybersécurité ne laissent aucune place au compromis, ESET PROTECT Elite combine prévention, détection et réponse avancée pour éviter tout incident.

Grâce à l'ensemble de ses technologies avancées, vous gardez une longueur d'avance sur les menaces.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

#1 G2 Grid® Report for EPP - Fall 2025

21 couches de protection endpoint

850 chercheurs à travers le monde

Principales fonctionnalités

Protection multicouche avancée : Prévention des endpoints face aux malwares, menaces 0-day et de l'exploitation des vulnérabilités.

Vulnérabilité et patch management : Surveille activement les vulnérabilités des systèmes d'exploitation et des applications courantes, et automatise les correctifs.

Protection de la messagerie : Couche de défense supplémentaire au niveau du serveur de messagerie pour contrer le spam et les malwares.

Protection M365 et Google Workspace : Fonctionnalités de filtrage mail et d'analyse des malwares qui contribuent à protéger les communications et le le stockage Cloud.

Authentification multifacteur : Efficace et facile à utiliser, protège votre entreprise des mots de passe faibles et des tentatives d'accès non autorisées.

Extended Detection & Response (XDR) : Renforce la prévention des atteintes à la sécurité en offrant une meilleure visibilité et une solution de Threat hunting.

Points clés

- Conforme RGPD
- Intégration via GraphAPI
- Intégration via API Google
- Facturation mensuelle
- ISO 27001
- Service MDR disponible
- Intégration dans outils tiers via API
- Support en Français

Distribué par
ACTN
Actual Systèmes
DSD
EDOX
Hermitage Solutions

Athena Global Services
(+33) 1 55 89 08 88
5 Avenue du Prieuré
Bâtiment B, 77700 Serris
www.eset.com/fr

Demandez une démonstration

GravityZone EDR et XDR

Bitdefender

Pays d'origine : Roumanie

Bitdefender GravityZone EDR surveille en continu les terminaux et serveurs pour détecter les activités suspectes et fournit les outils pour faire face aux attaques les plus évasives. La visualisation des menaces guident les investigations, révèlent les lacunes de sécurité ainsi que leur impact.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

Jusqu'à 90%
de réduction des efforts de sécurité

Accélération
de la réponse aux incidents de 50%

Réduction
des incidents jusqu'à 85%

Principales fonctionnalités

Bitdefender GravityZone EDR : Agent unique intégrant l'antivirus, le machine learning, le sandboxing et l'EDR pour Windows, MacOS et Linux.

Bitdefender GravityZone XDR : permettent l'ajout de contextualisation des incidents, la découverte de signaux faibles externes aux Endpoints.

GravityZone XDR Identity : permet la surveillance de l'Active Directory On-Premises, Entra ID et Microsoft InTune.

GravityZone XDR Productivity : permet la surveillance Microsoft Office 365 - Teams, Drive, Sharepoint, Emails - ou Google Workspace.

GravityZone XDR Network : permet la surveillance et la detection des scan de réseau, des mouvements latéraux et de l'exfiltration des objets connectés.

GravityZone XDR Mobile : permet la surveillance et la détection d'incidents des téléphones mobiles et tablettes IOS, Android, Chrome.

Points clés

- MSP : Facturation mensuelle à l'usage
- Support gratuit en français basé en France
- Console partenaire multitenant en français
- Surveillance de O365, de l'AD, d'Entra ID et d'Intune
- Console SaaS hébergée en Europe
- Licence NFR EDR et XDR gratuite pour les partenaires
- E-Learning : Formations et Certifications gratuites
- Certifications : ISO 27001, 27018, 9001, 14001

Distribué par
Arrow ECS SAS France
Ingram Micro France SAS
RG System by Septeo
FieldTrust BELUX

Bitdefender SAS
(+33) 1 47 35 72 73
49 Rue de la Vanne
92120 Montrouge
www.bitdefender.fr

Demandez une démonstration

Kaseya 365 User

Kaseya

Pays d'origine : États-Unis

Sécurisez les utilisateurs, leurs données et leurs outils cloud avec une plateforme unifiée : email, phishing, dark web, sauvegarde SaaS et automatisation. Gagnez du temps, réduisez les risques et améliorez la posture sécurité, sans complexifier l'IT.

Kaseya 365 User

Cette solution s'adresse :
PME

12 heures gagnées en gestion chaque mois

86 % d'amélioration des pratiques de sécurité utilisateurs

10 min pour créer un test de phishing

Principales fonctionnalités

Sauvegarde + restauration SaaS : Sauvegardes automatisées pour M365 & Entra ID. Inclus : Datto SaaS Protection & Entra Backup.

Détection et réponse cloud (CDR) : Détectez et répondez aux menaces SaaS en temps réel. Inclus : SaaS Alerts.

Protection M365 & Google Workspace : Protégez données et utilisateurs tout en assurant productivité et conformité.

Surveillance dark web : Identifiez les identifiants exposés avant qu'ils soient exploités. Inclus : Dark Web ID.

Formation + test de sensibilisation : Formations automatisées pour détecter et éviter les menaces. Inclus : BullPhish ID.

Sécurité email : Défense contre phishing, usurpation et menaces avancées. Inclus : INKY.

Points clés

- Sécurisez M365 et Google Workspace au-delà du endpoint
- Réduisez les tickets grâce à l'automatisation intégrée
- Identifiez, bloquez et corrigez les menaces rapidement
- Gérez tout depuis une console multi-client unifiée
- Utilisez bots et IA pour limiter l'intervention humaine
- Proposez des offres MSP packagées et standardisées
- Réduisez la charge support et gagnez en productivité
- Améliorez la marge sans multiplier les outils

Distribué par
BeMSP
Hermitage Solutions

Kaseya
(+44) 800 048 8847
250 Longwater Avenue
Green Park, Reading RG2 6GB
Royaume-Uni
www.kaseya.com

Demandez une démonstration

N-able EDR

N-able

Pays d'origine : États-Unis

Protection avancée des endpoints grâce à une détection comportementale continue. L'EDR N-able, reposant sur SentinelOne®, identifie, isole et neutralise rapidement les menaces sophistiquées comme les ransomwares, tout en offrant une visibilité complète et des réponses automatisées.

Cette solution s'adresse :
PME **ETI**

100 % de détections. Couverture irréprochable

0 latence de détection

88 % d'alertes inutiles en moins

Principales fonctionnalités

Gestion unifiée des terminaux : Visibilité et contrôle complets sur l'ensemble des appareils de votre réseau : Windows, Mac, Linux, appareils en réseau, etc.

Remédiation automatisée : Isolement, neutralisation et correction des menaces sans intervention manuelle, réduisant le risque et le temps d'arrêt.

Rollback après attaque : Restaure les endpoints à un état sain après ransomware ou compromission, minimisant les pertes opérationnelles.

Threat Hunting avancé : Outil de chasse aux menaces pour explorer les indicateurs de compromission et comprendre la chaîne d'attaque.

Visibilité et forensique : Fournit des données détaillées et historiques de l'activité système pour enquêter et analyser les incidents.

Visibilité unifiée des menaces : Tableau de bord centralisé offrant une vision globale des incidents, statuts d'agents et risques de sécurité pour réponse rapide.

Points clés

- N-ableMe : un portail partenaire dédié
- Support de l'équipe Infinigate en France
- Preuve de conformité RGPD globale N-able
- Abonnement mensuel avec facturation à la fin du mois
- Gérez plusieurs clients depuis une seule console
- Console hébergée dans le cloud
- Certifications ISO 27001 et SOC 2 de N-able

Distribué par
Infinigate France

N-able
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/n-able/

Demandez une démonstration

OpenText Core EDR

OpenText Cybersecurity

Pays d'origine : Canada

Protection proactive contre les ransomwares et les menaces zero-day. Analyse comportementale, isolation automatique et gestion dans un tableau de bord unique pour MSP. Sécurité moderne, sans surcharge.

Cette solution s'adresse :
TPE **PME** **ETI**

99 % Des menaces détectées automatiquement

1 seconde Analyse quasi instantanée

100 % Isolation automatique des endpoints

Principales fonctionnalités

Détection comportementale : Identifie les activités suspectes en temps réel.

Isolation automatique : Contient les endpoints infectés immédiatement.

Analyse des processus : Traque les comportements anormaux.

Réponse automatisée : Actions immédiates contre les ransomwares.

Console Multi-tenant : Conçue pour les MSP.

Forensics intégrés : Analyse post-incident simple et rapide.

Points clés

- Protection contre les ransomwares
- Visibilité complète du endpoint
- Réduction du temps de réponse
- Automatisation avancée
- Réduit les risques humains
- Adapté aux PME et MSP
- Très faible charge système
- Intégrable à MDR

Distribué par
MIEL
IPSteel
OpenText Cybersecurity

OpenText Cybersecurity
(+33) 1 47 96 65 24
Cœur Défense Tour B
92400 Paris la Défense
cybersecurity.opentext.com

Demandez une démonstration

PHASR
Bitdefender

Pays d'origine : Roumanie

PHASR, Proactive Hardening and Attack Surface Reduction, est une solution de durcissement révolutionnaire qui permet de réduire de manière proactive, personnalisée et dynamique, la surface d'attaque en limitant l'accès aux outils de gestion du système et aux outils de script natifs à Windows.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

84% des incidents grave de Cyber
exploitent des techniques LOTL

89 % des cas d'attaque LOTL
utilise le protocole RDP

71 % des cas d'attaque LOTL
utilise Powershell

Principales fonctionnalités

Renforce vos défenses : permet un durcissement approfondi et personnalisé, il s'adapte au comportement des utilisateurs et limite l'accès outils risqués.

Bloque les attaques LOTL : Lorsque les attaquants n'ont plus accès à PowerShell ou WMI, les attaquants ne peuvent plus s'infiltrer et passer inaperçus.

Empêchez les mêmes méthodes : Avec une sécurité différente par endpoints les mêmes schémas d'attaques sur plusieurs systèmes ne fonctionnent plus.

Durcissement sur mesure : permet un durcissement personnalisé, il limite l'accès aux outils risqués pour les utilisateurs qui n'en ont pas besoin.

Réduction de la surface d'attaque : s'adapte en continu et en toute autonomie à l'évolution du comportement des utilisateurs et aux nouveaux vecteurs d'attaque.

Des renseignements les plus récents : s'appuie sur Bitdefender Threat Intelligence pour que le durcissement soit efficace, même face aux vecteurs d'attaque émergents.

Points clés

- MSP : Facturation mensuelle à l'usage
- Support gratuit en français basé en France
- Console partenaire multitenant en français
- Surveillance de O365, de l'AD, d'Entra ID et d'Intune
- Console SaaS hébergée en Europe
- Licence NFR EDR et XDR gratuite pour les partenaires
- E-Learning : Formations et Certifications gratuites
- Certifications : ISO 27001, 27018, 9001, 14001

Distribué par
Arrow ECS SAS France
Ingram Micro France SAS
RG System by Septeo
FieldTrust BELUX

Bitdefender SAS
(+33) 1 47 35 72 73
49 Rue de la Vanne
92120 Montrouge
www.bitdefender.fr

Demandez une démonstration

XDR souverain

EUROPEAN DEFENSE PLATFORM

Pays d'origine : France

Infinigate présente la European Defense Platform XDR. En partenariat avec HarfangLab et Sekoia, cette solution 100 % française, vous aide à renforcer la surveillance et répondre aux menaces chez vos clients.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

1M+ d'actifs protégés dans le monde

1,5M+ d'endpoints équipés

1000 règles de détection

Principales fonctionnalités

6 moteurs de détection : Analyses antivirus basées sur la signature, le comportement et l'IA.

Données de télémétrie complètes : Vous disposez d'un panel d'outils d'investigation et de remédiation afin d'identifier les attaques et remonter à la source.

Playbook préconfiguré : Catalogue complet de règles et de contre-mesures disponible. Vos analystes gagnent du temps dans les réponses sur incident.

100% basé sur API : Vous connectez facilement et rapidement vos principales solutions Cyber au SOC.

Points clés

- Solution 100% cloud
- Hébergé en France
- 1 interlocuteur unique
- Accompagnement par équipe française
- Console multi-tenant
- Solution multi-certifiées

Distribué par
Infinigate France

EUROPEAN DEFENSE PLATFOR
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/sekoia/bundle-harfanglab-x-sekoia/

Demandez une démonstration

EDR - EPP - ASM

HarfangLab

Pays d'origine : France

Leader européen de la sécurité des endpoints, HarfangLab est certifiée ANSSI. Sa plateforme prévient, détecte et bloque les cyberattaques grâce à des règles de détection fines et transparentes, et à une télémétrie riche permettant des investigations approfondies.

Principales fonctionnalités

Endpoint Detection and Response : Détection IA, signatures, comportements et IoC. Protection ransomware et DLL sideloading. Investigation et remédiation par IA.

Endpoint Protection Platform : Antivirus, pare-feu et gestion des périphériques USB pour un blocage proactif des menaces.

Attack Surface Management : Visibilité complète sur le parc IT, gestion du Shadow IT et des vulnérabilités.

INFINIGATE FRANCE
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/harfanglab

Distribué par
Infinigate France

EDR

WithSecure

Pays d'origine : Finlande

Withsecure Elements EDR est une solution de détection et de réponse sur les endpoints, conçue pour identifier rapidement les comportements malveillants, analyser les incidents de sécurité et réagir automatiquement aux menaces.

Principales fonctionnalités

Détection des menaces basée sur le comportement : Analyse en continu des activités sur les endpoints afin d'identifier les comportements suspects ou malveillants, y compris les menaces inconnues.

Réponse automatisée aux incidents : Isolation immédiate des postes compromis, suppression des fichiers malveillants et limitation de la propagation des attaques, sans intervention manuelle.

MDR intégré 24 heures sur 24, 7 /7 : Service SOC externe 24/7. Un service de détection et réponse managé inclus.

Infinigate France - BU WITHSECURE
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/withsecure/

Distribué par
Infinigate France

ESET PROTECT Advanced

ESET

Pays d'origine : Slovaquie

Gardez une longueur d'avance sur les nouvelles menaces et les ransomwares. La solution comprend une technologie de détection avancée des menaces qui bloque les nouvelles menaces 0-day, et une fonctionnalité de chiffrement complet des disques.

www.eset.com/fr

ESET PROTECT Enterprise

ESET

Pays d'origine : Slovaquie

Combinez une défense robuste à une détection proactive pour réduire efficacement les risques de cyberattaques. La solution ESET XDR offre de robustes fonctionnalités de sécurité et de gestion des risques pour analyser et remédier rapidement à tout problème de sécurité dans le système d'information.

www.eset.com/fr

Security for Containers

Bitdefender

Pays d'origine : Roumanie

GravityZone Security for Containers est une solution de sécurité multiplateformes destinée aux conteneurs et aux environnements Linux. Elle combine un EDR à une détection avancée des exploits Linux et à une analyse approfondie des attaques.

www.bitdefender.fr

Security for Mobile

Bitdefender

Pays d'origine : Roumanie

GravityZone Security for Mobile est un outil de sécurité polyvalent qui lutte contre les menaces mobiles, une visibilité sur celles-ci, réduit les risques de vol de données et de perte d'identifiants, détecte les applications non conformes, couvre les modes de travail hybrides et le télétravail.

www.bitdefender.fr

Vous tenez la preuve de notre expertise entre vos mains.

Imaginez ce que nous pouvons faire pour votre croissance.

NDNM est un cabinet de conseil français, expert des enjeux commerciaux et marketing dans l'IT et la cybersécurité, qui accompagne **plus de 100 acteurs internationaux** (éditeurs, distributeurs, prestataires informatiques, MSP, MSSP).

ÉDITEURS ET DISTRIBUTEURS

Vous cherchez à étendre votre réseau de partenaires ?

Nous activons les leviers d'influence les plus puissants du marché pour asseoir votre leadership.

- **Stratégie Channel** : design de programmes partenaires et Go-to-Market indirect.
- **Influence média** : visibilité premium via nos actifs propriétaires (Guide du MSP).
- **Événementiel B2B** avec nos conférences Cybertalk.

PRESTATAIRES, MSP & ESN

Vous cherchez à structurer votre croissance ?

Nous transformons votre expertise technique en machine commerciale.

- **Packaging de l'offre**: transition vers le modèle MSP/MSSP et pricing.
- **Animation commerciale** : recrutement, coaching et process (CRM/Playbook).
- **Marketing Service Provider** : votre service marketing externalisé à l'année (contenus, campagnes, notoriété).

ndnm.

Depuis 2020, le partenaire de confiance des acteurs de l'IT et de la cybersécurité.
www.ndnm.fr

Échangeons sur vos enjeux

MDR

Le MDR est un service de détection et de réponse opéré, adossé à un SOC externalisé et mutualisé : une équipe qui qualifie, investigue et pilote la réponse. C'est précisément ce qui le distingue des solutions EDR/XDR traditionnelles : si ces outils détectent, encore faut-il des équipes pour transformer le signal en action.

Côté MSP, l'équation est d'abord économique. Exploiter un EDR/XDR en production impose d'avoir une équipe dédiée, des méthodes et de véritables compétences. Monter un SOC interne revient à supporter des coûts d'investissements importants (effectifs, process, outillage), souvent disproportionnés, y compris pour une structure mature.

Il n'est d'ailleurs pas étonnant de constater que ceux qui en opèrent un le font rarement sur une couverture totale 24/7.

Le MDR apporte une alternative réaliste : mutualiser chez un éditeur cette exploitation et rendre accessible une chaîne de détection/réponse en continu, sans construire toute l'organisation en interne.

Barracuda Managed XDR

BARRACUDA NETWORKS

Pays d'origine : États-Unis

Barracuda Managed XDR : Libérez vos clients de la fatigue des alertes cyber et collaborez avec notre équipe SOC primée 24h/24 pour fournir des services sur Email, Endpoints, Réseau, Cloud et serveurs.

Cette solution s'adresse :
PME

22 ans Expertise en Cybersécurité

Principales fonctionnalités

Visibilité étendue : 6 périmètres couverts (réseaux, endpoints, mail, cloud, serveurs, détection des vulnérabilités) au travers d'une plateforme unique.

Équipe SOC 24/7 : Surveillance 24/7 alertes filtrées par IA accompagné de cyber analystes vous accompagnant au quotidien.

Détection et réponse 24/7 : Remédiation coordonnée et automatisée pour contenir les attaques. Restauration immédiate des environnements.

Console MSP consolidée : Gestion centralisée des clients et des politiques de sécurité. Vision de l'état de chaque client / alertes.

Intégration : Large écosystème d'éditeurs supporté. Les MSP peuvent conserver les outils existants chez leurs différents clients.

Points clés

- XDR : cybersécurité proactive 24/7 par des experts SOC
- XDR Endpoint : détection/réponse avancées aux menaces 24/7
- XDR Email : surveillance proactive contre phishing et BEC
- XDR Cloud : contre accès et attaques non autorisés
- XDR Network: détection des menaces réseau et activités 24/7
- XDR Server : défense et élévation de privilèges

Distribué par
Infinigate France

Infinigate France - BU BARRACUDA
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/barracuda-networks/

Demandez une démonstration

MDR Managed Detection and Response

Bitdefender

Pays d'origine : Roumanie

Le service MDR vous donne accès aux personnes, aux processus et aux technologies dont vous avez besoin pour satisfaire pleinement vos besoins de sécurité et obtenir les résultats que vous recherchez.
Les EDR/XDR requièrent une surveillance en continu, avec un nombre d'alertes toujours croissant.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

70% de réduction de faux positifs avec le SOC Bitdefender

76 % des attaques par ransomware se produisent hors des heures ouvrées

466 000 € est le coût moyen d'une Cyberattaque pour une PME

Principales fonctionnalités

Plateforme de sécurité de pointe : Inclut notre plateforme de sécurité, régulièrement classée numéro 1 dans les tests menés par MITRE, AV-TEST et AV-Comparatives.

SOC disponible 24h/24, 7j/7 : Notre réseau mondial de SOC travaille lorsque vous ne travaillez pas et vous couvre partout dans le monde, à tout moment.

Actions préapprouvées (APA) : Une gamme complète d'APA permet des interventions rapides et décisives afin d'atténuer les effets des incidents de sécurité.

Chasses aux menaces : L'analyse continues des données, des renseignements sur les menaces et les attaquants facilitent la chasse aux menaces.

Analyse des causes profondes : Identification des vecteurs de menace initiaux, de l'impact potentiel des incidents Analyses et rapports complets après Action.

Portail & rapports MDR : Le portail MDR donne accès aux tableaux de bord, aux rapports mensuels.
Offre une visibilité inégalée sur le service MDR.

Points clés

- Une analyse plutôt que des alertes
- Réponses rapides et décisives
- SLA de 30 minutes
- Recommandations d'experts
- Sécurity Account Manager francophone
- Facturation mensuelle à l'usage
- Service disponible à partir d'1 licence
- Certification SOC 2 Type 2

Distribué par
Arrow ECS SAS France
Ingram Micro France SAS
RG System by Septeo
FieldTrust BELUX

Bitdefender SAS
(+33) 6 14 49 32 06
49 Rue de la Vanne
92120 Montrouge
www.bitdefender.fr

Demandez une démonstration

MDR/MPR
Check Point

Pays d'origine : Israël

Avec Infinity MDR/MPR, les experts de Check Point surveillent l'ensemble de votre infrastructure, couvrant vos pare-feux, vos postes, votre messagerie et vos outils de collaboration.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

100000 clients protégés

2,8 milliards d'événements analysés par jour

32 ans de sécurité, d'innovation, d'expertise

Principales fonctionnalités

Sécurité automatisée : L'application automatique des recommandations et des bonnes pratiques liées à votre environnement.

Sérénité opérationnelle : Réduisez les coûts opérationnels de votre SOC grâce à un service de sécurité managé réactif et entièrement transparent.

Transparence totale : Portail Web intuitif offrant une vue détaillée des incidents, analyses des menaces et des recommandations de sécurité.

Support multi-éditeurs : Gestion unifiée des incidents de sécurité remontés par les principaux éditeurs de sécurité.

Points clés

- Licence Pay-As-You-Go
- Console multi-tenant
- Protection 24/7 assurée par les experts de Check Point
- Service co managé par Check Point
- Gestion unifiée de la sécurité via un portail web unique

Distribué par
Arrow ECS
Infinigate
Westcon

Check Point Software
20 Avenue André Prothin
92400 Courbevoie
www.checkpoint.com

Demandez une démonstration

N-able MDR (Adlumin)

N-able

Pays d'origine : États-Unis

N-able MDR, basé sur la technologie Adlumin, fournit une détection et une réponse managées 24/7 assurée par des experts. Il combine analyse comportementale, threat hunting et expertise humaine pour identifier rapidement les attaques et réduire significativement les risques de compromission.

Cette solution s'adresse :
PME **ETI**

500 000+
alertes traitées entre décembre 2024 et février 2025

83 171 tickets de sécurité créés sur cette période

963 incidents résolus par l'équipe d'Adlumin MDR

Principales fonctionnalités

Détection des menaces en temps réel : Passez en revue les détections et les alertes chaque jour, puis validez les directement depuis le tableau de bord.

Capacités complètes de réaction : Des experts peuvent prendre des mesures avancées de réaction depuis la plateforme, quelle que soit la technologie utilisée.

Surveillance du deep web et dark net : Gardez un œil sur les comptes d'entreprise afin de détecter les failles sur l'open, le deep et le dark web.

Respect des exigences de conformité : Assistance grâce au reporting automatisé sur la conformité (p. ex., PCI DSS, NIST et HIPAA).

Analyses des privilèges : Analyse des privilèges de chaque compte, système et groupe. Les utilisateurs peuvent savoir qui peut accéder à leurs données.

Vulnérabilité réseau et hôtes : Analyses annuelles de vulnérabilité réseau avec des rapports détaillés (logiciels obsolètes, mots de passe faibles,..).

Points clés

- Une équipe d'experts intervenant 24/7
- Basé sur la solution cloud native de type SaaS Adlumin XDR
- Preuve de conformité RGPD globale N-able
- Intégration de Google Workspace comme source de données
- Analyse des données Microsoft 365
- Abonnement mensuel avec facturation à la fin du mois
- Certifications ISO 27001 et SOC 2 de N-able
- Gérez plusieurs clients depuis une seule console

Distribué par
Infinigate France

N-able
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/n-able/

Demandez une démonstration

ThreatDown MDR & EDR

Malwarebytes

Pays d'origine : États-Unis

ThreatDown MDR, propulsé par EDR, assure une surveillance et une analyse d'experts avec réponse précise aux menaces. Il offre une détection avancée, isolation et remédiation complète, incluant le ransomware rollback 72 h, pour garantir la continuité des opérations et sécuriser vos appareils.

Cette solution s'adresse :
TPE **PME** **ETI**

10 années+
d'expertise anti-menaces

72 h ransomware rollback

3M+ appareils protégés dans le monde

Principales fonctionnalités

Surveillance 24/7 & investigation : Surveillance continue des appareils avec triage expert et détection rapide des menaces émergentes.

Détection avancée des menaces : Détection comportementale et renseignement automatisé via EDR et corrélation SIEM pour révéler les menaces furtives.

Réponse précise aux incidents : Les analystes contiennent et remédient rapidement aux menaces. Réduisez l'impact et le temps de réponse grâce à leur expertise.

Threat hunting proactif : Hunting actif et basé sur IOC pour révéler les compromissions discrètes et les activités suspectes sur les appareils.

Remédiation & isolation avancées : Nettoyage complet des artefacts et modes d'isolation multiples pour stopper la propagation et éradiquer les menaces.

Ransomware rollback : Restaure les appareils infectés en quelques minutes grâce au 72 h ransomware rollback unique de ThreatDown.

Points clés

- Plateforme SaaS cloud-native
- Console multi-client pour MSP
- Détection et réponse alignées RGPD
- Formations et certifications partenaires
- Prêt pour marque blanche MSP
- Support technique 24/7 par des experts
- Accès aux ressources et outils partenaires
- Licences NFR disponibles pour tests MSP

Distribué par
BeMSP

Malwarebytes
2445 Augustine Dr Suite 550
Santa Clara, CA 95054, États-Unis
www.threatdown.com

Demandez une démonstration

Managed Detection and Response

WatchGuard Technologies

Pays d'origine : États-Unis

WatchGuard MDR offre une protection complète 24/7 sur réseaux, endpoints et identités, plus les apps Cloud tierces. Grâce à l'IA et à l'expertise SOC, vous gagnez du temps : moins d'alertes, plus d'efficacité, le tout depuis une plateforme unifiée.

Cette solution s'adresse :
TPE **PME**

<1 faux positif par mois

6 alertes en moyenne par mois

6 minutes pour répondre aux menaces

Principales fonctionnalités

Vue unifiée de la sécurité : Vision centralisée des activités malveillantes sur endpoints, réseau, identités et Cloud pour réduire la complexité MSP.

SOC 24/7 combinant IA + humains : Le mix automatisation + interventions humaines + réponse active (blocage, confinement, isolations) apporte une réactivité <6 min.

Conçu dès le départ pour les MSP : Le service est pensé nativement pour les MSP, avec gestion client, portail dédié, TAM, et maintien du contrôle du client.

Traque proactive et réponse avancée : Chasse aux menaces manuelle, analyse des causes profondes, récupération post-incident — services premium souvent absents.

Automatisation et réponse rapide : Filtre le bruit, exécute des actions immédiates et contient les menaces avant qu'elles ne se propagent dans l'environnement.

Portail de visibilité en temps réel : Vue live des alertes, actions du SOC et indicateurs de protection dans une interface unique pour les MSP.

Points clés

- CAM & TAM dédiés
- Gestion centralisée multi-clients dans 1 seul portail
- Portail MDR temps réel : alertes, actions, rapports
- SOC actif 24/7 avec réponse immédiate
- Plateforme MDR 100% Cloud, déploiement accéléré
- Intégration native Microsoft 365 et réponse API
- Supervision et détection intégrées Google Workspace
- Moins d'un faux positif par mois pour les MSP

Distribué par
Arrow ECS
Infinigate France

WatchGuard Technologies
+33 97 755 4336
22 Boulevard de Stalingrad
92320 Châtillon
www.watchguard.com/fr

Demandez une démonstration

OpenText MDR

OpenText Cybersecurity

Pays d'origine : Canada

Supervision 24/7 avec experts SOC. Détection avancée, analyses continues et réponses guidées. Idéal pour MSP qui veulent renforcer leur offre sécurité sans créer leur propre centre opérationnel.

Cette solution s'adresse :

TPE **PME** **ETI**

24/7/365
Surveillance continue des attaques

5 minutes
Temps moyen de réponse SOC

98 %
Menaces stoppées par le SOC

Principales fonctionnalités

Supervision 24/7 SOC : Surveillance des environnements en continu par nos experts.

Analyse des menaces : Corrélation avancée pour détecter les attaques.

Réponse guidée : Instructions claires pour éradiquer la menace.

Alertes priorisées : Filtrage pour éviter la surcharge MSP.

Rapports d'incidents : Visibilité détaillée pour chaque client.

Intégration facile : Compatible avec les infrastructures MSP.

Points clés

- Renforce l'offre MSP
- Pas besoin de SOC interne
- Réduit les faux positifs
- Protection 24/7
- Rapidité de réponse
- Expertise externalisée
- Complément idéal à l'EDR
- Zéro complexité opérationnelle

Distribué par
MIEL
IPSteel
OpenText Cybersecurity

OpenText Cybersecurity
(+33) 1 47 96 65 24
Cœur Défense Tour B
92400 Paris la Défense
cybersecurity.opentext.com

Demandez une démonstration

Sophos MSP & Services MDR

Sophos

Pays d'origine : Royaume-Uni

Sophos MSP & MDR offre aux MSP un portefeuille de sécurité unifié avec détection et réponse 24/7, ainsi que des solutions de sécurité incluant endpoint, pare-feu, e-mail et cloud. Les MSP profitent d'une facturation mensuelle flexible et d'une gestion centralisée via Sophos Central.

Cette solution s'adresse :
PME **ETI** **Grands Comptes**

99,98 % de menaces bloquées automatiquement

24/7 une équipe d'experts à votre service

82 % de réduction des incidents de sécurité

Principales fonctionnalités

Managed Detection and Response : Chasse aux menaces, détection et réponse 24/7 assurées par les experts Sophos.

Facturation MSP flexible : Paiement mensuel à l'usage, basé sur le volume.

Gestion centralisée : Gérez tous les environnements clients depuis une seule console.

Portefeuille complet de sécurité : Solutions pour endpoints, mobiles, pare-feu, e-mails, serveurs, cloud et plus encore.

Rétention de la clientèle accrue : opportunité de diversification et d'extension attractive.

Réponse automatisée aux menaces : Détection renforcée par l'IA et confinement automatique des menaces.

Points clés

- Plateforme de cybersécurité unifiée pour les MSP
- MDR assuré par des analystes experts en menaces
- Facturation mensuelle à l'usage
- Intégration fluide avec les outils RMM et PSA
- Protection complète multi-couches
- Supervision et réponse aux incidents 24/7
- Grande évolutivité pour la croissance des MSP
- Détection des menaces optimisée par l'IA

Sophos
(+33) 1 34 34 80 00
3 Rue du Colonel Moll
75017 Paris
www.sophos.fr

Demandez une démonstration

WithSecure Elements

WithSecure

Pays d'origine : Finlande

Un seul agent, une plateforme unifiée : Les solutions WithSecure permettent d'identifier plus rapidement les menaces et de réduire leur impact grâce à une combinaison de technologies avancées et de services de supervision experts.

Cette solution s'adresse :
TPE **PME** **ETI**

35+ ans d'expertise en cybersécurité

99,90 % temps de réponse sous 15 minutes

500 millions+ endpoints protégés mondialement

Principales fonctionnalités

Détection des menaces basée sur le comportement : Analyse continue des activités sur les endpoints pour repérer les comportements suspects, y compris les menaces inconnues.

Réponse automatisée aux incidents : Isolation immédiate des postes compromis, suppression des fichiers malveillants et limitation de la propagation des attaques, sans intervention manuelle.

MDR intégré 24 heures sur 24, 7/7 : Service SOC externe 24/7. Un service de détection et réponse managé inclus.

Gestion des expositions XM : Avec Exposure management, obtenez une gestion centralisée des expositions de vulnérabilités avec scoring de risque.

Plateforme cloud 100% modulable : Architecture cloud conçue spécifiquement pour les MSP. Isolation des données clients garantie. Tableaux de bord multi-tenants.

Un modèle de facturation pensé pour les MSP : Facturation mensuelle basée sur le nombre d'endpoints protégés. Le volume peut être ajusté chaque mois selon vos besoins.

Points clés

- Support technique 24/7
- Cloud SaaS multi-tenant
- Plateforme cloud unifiée
- Automatisation des réponses (isolation, remédiation)
- MDR intégré sans SOC interne
- Gestion de vulnérabilités
- Certifications NIS 2 - DORA - RGPD
- Compatible Windows, Mac, Linux

Distribué par
Infinigate France

BU Withsecure
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/withsecure/

Demandez une démonstration

CyclonShield
NUCLEON SECURITY

Pays d'origine : France

Un service de détection et de réponse géré conçu pour neutraliser les attaques avant qu'elles n'aient un impact sur vos opérations, combinant une surveillance continue, une analyse comportementale avancée et une gestion de bout en bout des incidents de cybersécurité.

Principales fonctionnalités

Surveillance 24h/24 et 7j/7 : Surveillance 24h/24 et 7j/7 pour la détection et la réponse instantanées aux menaces.

Détection avancée des menaces : Gestion des vulnérabilités et des menaces avec identification proactive

Expertise technique et R&D intégrée : une réponse ultra-rapide aux attaques, fournies par nos experts en cybersécurité et notre IA de pointe.

NUCLEON SECURITY
(+33) 1 84 17 27 15
25 Rue Ponthieu
75008 Paris
nucleon-security.com

Distribué par
Net Point
Actual Systèmes
Provicloud

ESET MDR for MSP
ESET

Pays d'origine : Slovaquie

ESET MDR accompagne les MSP en enrichissant l'expertise de leurs équipes de sécurité. Ce service fournit un soutien spécialisé avec des outils de pointe pour une protection optimale et permet de remonter les activités malveillantes et de mettre en œuvre des actions de remédiation.

Principales fonctionnalités

Detection & Response 24/7 : Notre service de MDR est le plus rapide pour détecter et bloquer les menaces avec un MTTR moyen de 6 minutes.

Rapports sur-mesure : Le partenaire MSP reçoit des rapports hebdomadaires et mensuels, et peut générer des rapports personnalisé sur les incidents.

Technical Account Manager français : Le TAM français reçoit en parallèle les alertes d'incident et apporte son expertise sur leur compréhension et les actions à mener.

Athena Global Services
(+33) 1 55 89 08 88
5 Avenue du Prieuré,
Bâtiment B, 77700 Serris
www.eset.com/fr

Distribué par
ACTN
Actual Systèmes
DSD
EDOX
Hermitage Solutions

Cybersecurité

RG System Suite

Pays d'origine : France

Depuis votre console RMM RG System Suite, accédez à Bitdefender GravityZone pour protéger efficacement les terminaux de vos clients. La plateforme permet un déploiement centralisé et une gestion simplifiée de la cybersécurité, parfaitement adaptée aux environnements MSP.

www.rgsystem.septeo.com

BlackPoint

BlackPoint Cyber

Pays d'origine : États-Unis

Blackpoint combine supervision 24/7, logique de détection brevetée et analyse contextuelle pour traquer les attaques avancées. Son point fort : transformer chaque incident en source d'amélioration continue, en corrélant vulnérabilités, comportements et infrastructures à risque dans un SOC unifié.

blackpointcyber.com/platform/managed-detection-and-response

Cyna

Cyna

Pays d'origine : France

Conçu pour les MSP, le MDR de Cyna va au-delà de la simple détection : un SOC 24/7 basé en France supervise, enquête et agit, appuyé par une équipe CERT membre d'InterCERT. Intégration fluide avec les EDR du marché et portail partenaire pour un pilotage unifié des incidents.

cyna-it.fr

Trend Vision One

Trend Micro

Pays d'origine : Japon

Trend Micro combine détection multi-surface (endpoint, cloud, messagerie, réseau) et investigation centralisée au sein de sa plateforme Vision One. Son MDR s'appuie sur une expertise SOC internalisée pour contextualiser les alertes, automatiser les réponses et réduire le temps de détection.

www.trendmicro.com/en_gb/business/services/managed-xdr.html

Firewall

L'évolution des architectures hybrides, des accès distants et des usages cloud a déplacé le firewall vers une fonction de contrôle dynamique des flux, des identités et des applications. Il opère désormais à un niveau applicatif, en combinant inspection approfondie des protocoles, identification des usages réels et prise de décision basée sur le contexte.

Les évolutions les plus structurantes tiennent à la convergence des fonctions : filtrage L7, IPS, contrôle applicatif, inspection TLS, intégration DNS et politiques fondées sur l'identité plutôt que sur l'adresse IP.

La capacité à appliquer des règles cohérentes entre sites physiques, environnements cloud et utilisateurs distants devient un prérequis.

Les architectures s'orientent vers des modèles distribués, avec des fonctions firewall étendues aux environnements IT/OT, virtualisés, on-premise et cloud natif, tout en restant pilotables depuis des consoles unifiées. La complexité ne se situe plus dans le matériel, mais dans l'exploitation : concevoir des règles lisibles, maintenables et alignées avec les usages métiers, tout en limitant les exceptions et les dérives.

Hybride Mesh Network Security

Check Point

Pays d'origine : Israël

Protégez votre réseau avec les passerelles de sécurité les plus efficaces du marché, alimentées par l'IA. Bénéficiez de la meilleure prévention des menaces, d'une évolutivité transparente et d'une gestion unifiée des politiques.

Cette solution s'adresse :

TPE **PME** **ETI** **Grands comptes**

100 000+
Clients protégés

99.59% Meilleur score du marché par NSS Labs

33 ans de sécurité, d'innovation, d'expertise

Principales fonctionnalités

Protection Réseau Complète : Pare-feux de nouvelle génération, VPN, IPS, Control d'accés web et applications, Anti-malware zéro day, zéro phishing, SD-WAN.

Gamme PME et reseaux d'agences : Allant de 1,2 à 9 Gbps par boitier, avec option Wifi 7 et 5G.

Gamme Enterprise : Flexible et évolutive allant de 5 à 64 Gbps,.

Gamme virtuelle : Pour les clouds hybrides, publics et privés avec la même gestion centralisée que les appliances physiques.

Gestion centralisée Cloud & on prem : Gestion unifiée des appliances disponible en hardware, en VM et en SaaS.

Choix de licence CAPEX, OPEX & PAYG : Possibilité d'achat en CAPEX ou en mode souscription (OPEX): Facturation mensuelle ou annuelle.

Points clés

- Licences Pay-As-You-Go ou Firewall as a Subscription
- Console multi-tenant
- Protection 24/7 assurée par les experts de Check Point
- Gestion unifiée de la sécurité via un portail web unique
- Appliances physiques et virtuelles

Distribué par
Arrow ECS
Infinigate
Westcon

Check Point Software
20 Avenue André Prothin
92400 Courbevoie
www.checkpoint.com

Demandez une démonstration

Managed Protection Security Suite

SONICWALL

Pays d'origine : États-Unis

Un pare-feu efficace requiert une gestion active et des configurations à jour pour une protection optimale. Avec la solution MPSS de SonicWall, les experts gèrent votre pare-feu de génération 7 ou 8, assurant ainsi une protection continue contre les cybermenaces.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

30 ans+ d'expertise en cybersécurité

6 milliards d'attaques réseau critiques bloquées

68 jours d'interruptions évitées en 2024

Principales fonctionnalités

Ne manquez jamais une mise à jour : Les experts SonicSentry gèrent mises à jour et configurations pour un pare-feu toujours optimal.

État du pare-feu en temps réel : SonicSentry alerte si le pare-feu est hors ligne ou modifié. Protection optimale garantie.

Santé et rapports de productivité : Observez les menaces bloquées par votre pare-feu les 30 derniers jours et le trafic improductif pouvant ralentir votre réseau.

Support renforcé : Les clients MPSS ont un support dédié SonicSentry, incluant une assistance d'urgence hors heures pour les problèmes critiques.

Points clés

- Support amélioré 24h/24, 7j/7
- Mises à jour du firmware et des correctifs
- Rapports et analyses sur 30 jours
- Vérifications mensuelles de l'état du pare-feu
- Alertes automatisées 24h/24 et 7j/7 pour les événements
- Cybersécurité : Garantie cyber embarquée de 200 000 $

Distribué par
Infinigate France

Sonicwall France
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/sonicwall/

Demandez une démonstration

Sécurité Réseau

WatchGuard Technologies

Pays d'origine : États-Unis

Les solutions WatchGuard offrent une protection réseau complète pour environnements sur site, cloud ou hybrides. Firewalls, NDR, Zero Trust et services avancés garantissent une sécurité intégrée contre les menaces actuelles, assurant la continuité des opérations.

Cette solution s'adresse :
TPE **PME** **ETI**

1300 attaques de malwares contrées / an

24/7 Support primé

1 console unique de gestion

Principales fonctionnalités

Pour les architectures hybrides : Les appliances Firebox assurent sécurité, performance et intégration pour infrastructures hybrides on-premise, cloud et distantes.

Inspection et protection SSL : Plus de 80 % du trafic est HTTPS : les firewalls Firebox WatchGuard le sécurisent intégralement, TLS 1.3 inclus.

Les dernières technologies VPN : VPN site-à-site et mobiles sécurisés avec Firebox : SSL et IPSec/IKEv2 pour des connexions fiables.

IA et Sandboxing : Offrez à vos clients une défense proactive grâce à IntelligentAV, APT Blocker et sandboxing Firebox.

Détection IA et réponse aux menaces : Surveillez tout le réseau et priorisez les risques avec ThreatSync IA, inclus dans Total Security Suite.

Intégration endpoints & identités : Firebox intègre endpoints et gestion des identités pour un environnement sécurisé on-premise ou distant, sans complexité.

Points clés

- Gestion Firebox centralisée via WatchGuard Cloud
- Administration multi-clients simple et scalable
- Support et supervision technique 24/7 inclus
- Protection étendue pour environnements hybrides M365
- Protection robuste pour réseaux physiques et virtuels
- Inspection complète HTTPS/ TLS 1.3 intégrée
- Sandboxing APT Blocker + IA IntelligentAV inclus
- VPN IPSec/IKEv2 & SSL pour télétravail sécurisé

Distribué par
Arrow ECS
Infinigate France

WatchGuard Technologies
+33 97 755 4336
22 Boulevard de Stalingrad
92320 Châtillon
www.watchguard.com/fr

Demandez une démonstration

DynFi Firewall

DynFi

Pays d'origine : France

DynFi est un pare-feu open source français conçu pour les entreprises. Il combine filtrage réseau avancé, VPN, proxy, IDS et gestion centralisée multi-sites via DynFi Manager. Déployable sur appliance ou en virtuel, il offre une maîtrise complète et transparente du périmètre réseau.

dynfi.com/en/dynfi-firewall

IPFire

IPFire

Pays d'origine : Allemagne

IPFire est une distribution firewall open source intégrant inspection de paquets, segmentation réseau (DMZ, VLAN), VPN, proxy et IDS/IPS. Adaptée aux environnements hétérogènes, elle se pilote via une interface web complète et bénéficie d'une communauté active et d'audits réguliers.

www.ipfire.org

OPNsense

OPNsense

Pays d'origine : Pays-Bas

OPNsense est une plateforme de pare-feu et de routage open source riche en fonctionnalités : inspection d'intrusion avec Suricata, VPN multiples (WireGuard, IPsec, OpenVPN), haute disponibilité via CARP, et interface web moderne. Conçue pour la fiabilité, la transparence et la personnalisation réseau.

opnsense.org

pfSense Plus

Netgate

Pays d'origine : États-Unis

Développé par Netgate, pfSense Plus repose sur FreeBSD et cible les environnements professionnels. Il se distingue par ses capacités de configuration fine (NAT, routage, règles complexes), son intégration dans des architectures virtualisées, et un système modulaire adapté aux réseaux exigeants.

www.pfsense.org

Suivi de la conformité

La densification réglementaire oblige aujourd'hui les prestataires informatiques à s'adapter. À mesure que les environnements se fragmentent et que les référentiels s'empilent, les approches déclaratives ne tiennent plus : ce qui n'est pas mesuré en continu finit mécaniquement par diverger. La conformité cesse alors d'être une question réglementaire pour devenir un problème d'exploitation.

Les outils ont évolué pour répondre à cette dérive. Ils ne se contentent plus de cartographier des exigences, mais confrontent en permanence les règles aux configurations réelles, aux usages effectifs et aux évolutions quotidiennes du système d'information. La conformité se lit désormais comme un état dynamique, fait d'écarts identifiés, de tolérances assumées et de remédiations priorisées.

Cette approche transforme la manière dont les équipes pilotent les environnements. Les audits ne remettent plus en cause l'existant, ils en valident l'état. Les écarts deviennent des KPI exploitables, au même titre que des alertes techniques. Le suivi de la conformité s'impose ainsi comme un outil de stabilisation, capable d'accompagner leur évolution sans perdre la maîtrise des exigences qui s'y appliquent.

Compliance Reporting

WatchGuard Technologies

Pays d'origine : États-Unis

WatchGuard Compliance Reporting automatise la conformité avec ThreatSync+ NDR. Basé sur NIST 800-53 et ISO 27001, il génère facilement rapports et alertes hiérarchisées, permet d'ajouter ou modifier des contrôles et simplifie la création de rapports via un simple bouton.

Cette solution s'adresse :
TPE **PME** **ETI**

Visibilité instantanée

Obtenez un score global de conformité

Principales fonctionnalités

Visibilité instantanée : Obtenez un score global de conformité et détaillez l'efficacité de chaque contrôle en un clic pour vos clients.

Couverture réglementaire étendue : Conforme aux normes ISO 27001, NIST, Cyber Essentials et CIS pour audits, assurance et conformité sectorielle.

Rapports faciles à générer : Créez et personnalisez des rapports de conformité automatiquement, réduisant le temps passé aux tâches manuelles.

Économie de temps et coûts : Automatisez la collecte de données, la validation et la génération de rapports pour économiser des centaines d'heures.

Adapté aux petites équipes : Permet aux MSP et petites équipes de gérer facilement la conformité réseau avec un minimum de ressources.

Evolutif et personnalisable : Ajoutez, modifiez ou déployez rapidement des contrôles prédéfinis ou personnalisés pour suivre les nouvelles exigences.

Points clés

- Solution 100 % cloud sécurisée et toujours disponible
- Un contact privilégié pour un support personnalisé
- Rapports ISO 27001, NIS2, DORA
- Gestion des données alignée avec la RGPD
- Assistance instantanée, tous les jours, toute l'année
- Tableau de bord centralisé pour piloter vos clients
- Pour vous aussi : licence NFR
- Formations et certifications intégrées pour vos équipes

Distribué par
Arrow ECS
Infinigate France

WatchGuard Technologies
+33 97 755 4336
22 Boulevard de Stalingrad
92320 Châtillon
www.watchguard.com/fr

Demandez une démonstration

FlexCarto

ARKANLIS

Pays d'origine : France

FlexCarto est votre assistant IA pour une Gouvernance sans faille de votre Système d'information (SI). Cette plateforme tout-en-un (Cartographie, Sécurité, Conformité) simplifie la sécurité et la conformité réglementaire de votre SI pour gagner en temps et en efficacité.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

100 % Maitrise du SI

-70 % Temps de préparation d'audits

-60 % de non-conformités

Principales fonctionnalités

Cartographie du SI : Gestion d'applications, des dépendances, des versions, des tâches (avec assistance IA). Analyse d'impact, modélisation du SI.

Sécurité du SI : Assistance IA pour l'analyse de risques, l'évaluation de criticité, la gestion des tâches et les clausiers SSI.

Conformité RGPD : Assistance IA pour créer les traitements de chaque applications et analyser les risques associés. Catalogue d'AIPD.

Conformité globale du SI : Assistance IA pour évaluer la conformité du SI et générer les tâches prioritaires. Imprimer son rapport pour l'audit.

Catalogue de conformités : NIS2, HAS, ANSSI, CARE, PSSI, CAC, HDS, RGS, RGAA, DORA, ISO 27001, ISO 26000 (RSE) et d'autres à la demande.

Gouvernance du SI : Gestionnaire de tâches et tableaux de bord pour DSI, RSSI et DPO pour anticiper et prioriser ses activités et budgets.

Points clés

- Version cloud
- On premise
- Hébergement certifié ISO 27001
- Solution souveraine
- Pensé et créé par des experts (DSI, RSSI, DPO)
- Assistance IA intégré
- Logiciel tout en 1 (cartographie, sécurité, conformité)
- Pas de limite d'utilisateurs

Distribué par
SCC
UGAP
CAIH

ARKANLIS
contact@arkanlis.com
72 Rue de la République
76140 Le Petit Quevilly
www.flexcarto.com

Demandez une démonstration

GravityZone Compliance Manager

Bitdefender

Pays d'origine : Roumanie

offre aux entreprises une visibilité immédiate sur la conformité de leurs endpoints. Conçue pour simplifier la conformité et rationaliser la préparation aux audits, elle regroupe la sécurité, les risques et la conformité au sein d'une même plateforme.

Bitdefender SAS
(+33) 1 47 35 72 73
49 Rue de la Vanne
92120 Montrouge
www.bitdefender.fr

Distribué par
Arrow ECS SAS France
Ingram Micro France SAS
RG System by Septeo
FieldTrust BELUX

Principales fonctionnalités

Comble les lacunes de conformité : Corrigez rapidement les lacunes de conformité, de réduire les risques, rationaliser la remédiation en quelques clics.

Rapports automatisés et vérifiables : Génère facilement des rapports PDF ou XLSX, incluant les données du tableau de bord, les modifications, un état de la conformité.

Normes de conformité : RGDP, PCI DSS, la directive NIS 2, les contrôles CISv8, la norme SOC 2, la norme CMMC 2.0, la loi HIPAA, la norme ISO 27001, Etc.

CISO Assistant

intuitem

Pays d'origine : France

CISO Assistant facilite le pilotage de la conformité, des risques et des audits dans des organisations complexes. Il permet de centraliser preuves, contrôles et référentiels sans duplication, de modéliser les risques de manière continue, et d'alléger la charge des équipes DSI et des consultants.

intuitem.com/fr/ciso-assistant

Deming

Deming

Pays d'origine : Luxembourg

Deming est un outil open source destiné aux RSSI pour structurer et suivre leur SMSI en conformité avec ISO 27001:2022. Léger, autonome et non cloud, il permet de planifier les contrôles, enregistrer les preuves, suivre l'efficacité des mesures, et générer les rapports attendus en audit.

www.sourcentis.com/en/deming

Scan de vulnérabilité

Le scan de vulnérabilité s'est installé comme un mécanisme de lecture du risque, capable d'alimenter des décisions alignées sur les réalités de production. Exposition réelle, rôle de l'actif, surface d'attaque associée, contrôles déjà en place : le scan devient un point de convergence entre l'inventaire, la menace et l'usage.

Pour un prestataire informatique mature, l'enjeu se déplace naturellement vers la priorisation et l'orchestration : décider quoi corriger, quoi compenser, quoi surveiller, et dans quel ordre. Les impacts sont immédiats. Opérationnellement, les résultats ne vivent plus dans des rapports isolés mais s'intègrent aux chaînes de production existantes (ITSM, patch management, SOC, XDR).

Économiquement, le scan de vulnérabilités sert de fondation à des services managés récurrents comme le VOC et dans les accompagnements RSSI externalisés. Il impose une articulation entre exploitation, sécurité et conseil, et oblige le prestataire à structurer des processus de décision et de reporting orientés risque, compréhensibles au-delà des équipes techniques.

OpenText Core DNS Protection

OpenText Cybersecurity

Pays d'origine : Canada

Bloquez les menaces avant qu'elles n'atteignent le réseau. Filtrage DNS, préventions des fuites, contrôle continu des utilisateurs et rapports pour les MSP. Simple à déployer et puissant pour sécuriser chaque client.

Cette solution s'adresse :
TPE **PME** **ETI**

1/3 des attaques transitent par le DNS

785 K€ Coût moyen d'une attaque DNS

43 % Sociétés sans DNS sécurisé

Principales fonctionnalités

Filtrage DNS Cloud : Bloque les menaces avant qu'elles n'atteignent le réseau.

Prévention des fuites DNS : Garantit que toutes les requêtes passent par le service sécurisé.

Catégorisation Web : Contrôle l'accès aux sites par catégories ou règles MSP, incluant les employés travaillant à distance quel que soit le réseau utilisé.

Protection DoH/DoT : Sécurise les résolutions même en DNS chiffré.

Reporting Multi-tenant : Rapports clairs pour chaque client depuis un seul portail.

Déploiement simple : Installation en quelques minutes via agent ou réseau.

Points clés

- Bloque les menaces en amont
- Réduit la surface d'attaque
- Outil MSP multi-clients
- Faible charge réseau
- Vitesse de navigation préservée
- Aucune infrastructure requise
- Règles par groupe d'utilisateurs
- Contrôle total et visibilité

Distribué par
MIEL
IPSteel
OpenText Cybersecurity

OpenText Cybersecurity
(+33) 1 47 96 65 24
Cœur Défense Tour B
92400 Paris la Défense
cybersecurity.opentext.com

Demandez une démonstration

External Attack Surface Management

Bitdefender

Pays d'origine : Roumanie

External Attack Surface Management (EASM) identifie et analyse les actifs connectés à Internet et leur exposition, facilitant ainsi la priorisation des risques et leur atténuation rapide.

Principales fonctionnalités

Découverte exhaustive des actifs : identifie les actifs, les applications, les sous-domaines, les IP, les cloud tiers et les certificats expirés et exposés.

Gestion des vulnérabilités : Analyse en continu les actifs découverts, détecte les vulnérabilités, les erreurs de configuration susceptibles d'être exploitées.

Domaines similaires : identifie les domaines usurpés pouvant être utilisés pour imiter l'apparence de l'organisation dans le cadre d'attaques.

Bitdefender SAS
(+33) 1 47 35 72 73
49 Rue de la Vanne
92120 Montrouge
www.bitdefender.fr

Distribué par
Arrow ECS SAS France
Ingram Micro France SAS
RG System by Septeo
FieldTrust BELUX

Fortra VM

FORTRA

Pays d'origine : États-Unis

Fortra VM est une solution de gestion des vulnérabilités, d'un des principaux acteurs de la cybersécurité. Offerte en multi-tenant, marque blanche et avec les meilleures marges du marché. Spécialement adaptée pour des acteurs MSP/MSSPs de toutes tailles, à la recherche de fonctionnalités avancées.

Principales fonctionnalités

Identifier : Détectez avec précision et efficacité les vulnérabilités pouvant être exploitées par des cybercriminels.

Évaluer et hiérarchiser : Identifiez et priorisez les vulnérabilités exploitables selon le secteur, la criticité, l'exposition et la valeur des actifs.

Rapporter : Des rapports puissants permettent de suivre la remédiation, les tendances de sécurité et de répondre aux exigences de conformité.

FORTRA
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/fortra/

Distribué par
Infinigate France

Cyberwatch

Cyberwatch

Pays d'origine : France

Cyberwatch se distingue par sa capacité à opérer en réseau isolé et à couvrir des périmètres hétérogènes (Linux, Windows, équipements réseau, IoT). Le moteur de corrélation croise les vulnérabilités avec le contexte métier pour prioriser les actions. Déploiement possible en appliance, sans dépendance cloud.

cyberwatch.fr

OpenVas

Greenbone

Pays d'origine : Allemagne

OpenVAS est le moteur de détection de vulnérabilités open source développé par Greenbone AG. Il permet des scans authentifiés, une détection des failles connues (CVE), et repose sur un système de plugins mis à jour quotidiennement. Utilisé en local, il constitue la base technique des solutions de Greenbone.

www.openvas.org

Trivy

Aqua Security

Pays d'origine : Israël

Trivy est un scanner open source tout-en-un pour les environnements cloud-native. Il détecte les vulnérabilités, licences et erreurs de configuration dans les images Docker, les dépôts Git, les artefacts CI/CD et les clusters Kubernetes. Léger, rapide et intégré aux workflows DevSecOps.

trivy.dev

Zed Attack Proxy

Zed Attack Proxy

Pays d'origine : États-Unis

ZAP est un scanner open source dédié aux tests de sécurité des applications web. Il permet l'analyse passive et active, l'automatisation via API, et l'extension par plugins. Couramment utilisé en CI/CD, il s'adresse aux pentesters comme aux développeurs.

www.zaproxy.org

Hébergement et infrastructure

Hyperviseurs, clusters de stockage, services cloud, interconnexions réseau et mécanismes de reprise coexistent dans des architectures distribuées, rarement homogènes. À cette complexité s'ajoutent des contraintes croissantes de souveraineté, de localisation des données et de dépendance aux fournisseurs, qui influencent directement les choix d'hébergement.

Face à cette diversité d'environnements, l'infrastructure n'est plus administrée, elle est pilotée. Orchestration, templates et supervision transverse deviennent indispensables pour maintenir la cohérence dans des environnements hybrides mêlant cloud public, infrastructures privées et hébergement local.

La maîtrise passe désormais par la capacité à faire évoluer ces environnements sans rupture, tout en maintenant un contrôle fin de la performance, de la capacité et des coûts. L'exploitation devient un exercice continu : corréler incidents, dérives financières et évolutions technologiques pour absorber le changement sans perdre le contrôle.

Acronis Disaster Recovery

Acronis

Pays d'origine : Suisse

Fournissez des services de plan de reprise d'activité économiques qui permettent de démarrer vos serveurs instantanément sur le Cloud Acronis ou Azure, sans aucune infrastructure complémentaire. Le tout piloté par des scénarios automatisés depuis une seule console, Acronis Cyber Protect Cloud.

Cette solution s'adresse :

TPE **PME** **ETI** **Grands comptes**

750 000 entreprises protégées dans le monde via des MSP Acronis

20 000 fournisseurs de services utilisent la plateforme Acronis

7,5 millions d'attaques bloquées en 12 mois grâce à Acronis

Principales fonctionnalités

Restauration auto incrémentielle : Les ressources continuent de s'exécuter pendant la synchronisation des données.

Protection continue, à la demande : Restauration à un moment donné pour tout type de sauvegarde.

Options de connectivité multiples : VPN site à site ou point à site, VPN multisite IP sec.

Options de restauration flexibles : Restauration fiable, de la reprise intégrale des systèmes à la récupération granulaire de fichiers, dossiers et applications.

Reprise sécurisée après incident : Restauration sécurisée des systèmes vers un point de sauvegarde sain, garantissant une continuité d'activité sans réinfection.

Basculement automatisé : Déclenchement simplifié et automatisé du basculement pour une reprise rapide des systèmes critiques.

Points clés

- Hébergement par Acronis ou Azure
- Hébergement en France
- Console multi-tenant
- Facturation mensuelle
- Portail partenaires
- Formations et certifications sur-mesure pour les MSP
- Conformité réglementaire éprouvée
- Solution certifiée

Distribué par
TD SYNNEX
Infinigate France
ALSO

Acronis
(+33) 1 87 16 91 19
20-22 Rue Marius Aufan
92300 Levallois-Perret
www.acronis.com

Demandez une démonstration

Bureau à Distance
JOTELULU

Pays d'origine : France

Le Bureau à Distance de Jotelulu est LA première solution entièrement conçue pour permettre aux entreprises IT de déployer rapidement et gérer efficacement des serveurs d'applications dans le cloud.

Cette solution s'adresse :
TPE **PME** **ETI**

1500+ Partenaires Actifs

55000+ Utilisateurs quotidiens

99,99 % Disponibilité du Service

Principales fonctionnalités

Déploiement express : Déployez rapidement vos bureaux virtuels au moyen d'une interface simple et intuitive.

Sécurité intégrée : Bénéficiez d'une suite de sécurité intégrée incluant: Pare-feu, VPN, IPS/IDS, anti-DDOS, chiffrement et double authentification.

Sauvegarde incluse : Protégez vos données avec une stratégie de sauvegarde complète : horaire, journalière et hebdomadaire.

Scalabilité à la demande : Adaptez les performances et ressources aux besoins de l'activité métiers.

Marque blanche : Offrez une expérience sur mesure avec un portail d'accès personnalisé aux couleurs de votre entreprise et de vos clients.

Publication d'applications : Publiez vos applications métiers pour un accès contrôlé et ciblé.

Points clés

- Hébergé en France
- Multi-tenant
- Conformité ISO 27001 et HDS
- Programme partenaire
- Support illimité en français 24/7
- Coûts maîtrisés
- Performances optimales
- Support francophone

Distribué par **Jotelulu**

Jotelulu
(+33) 1 87 65 31 20
81 Rue Réaumur
75002 Paris
www.jotelulu.com/fr-fr/productos/remote-desktop

Demandez une démonstration

Cyber, Cloud & AI
Scalair

Pays d'origine : France

Scalair est une entreprise experte en Cybersécurité (MSSP) et Cloud Souverain, sélectionnée dans le programme Scale Up de la French Tech. Scalair conçoit, déploie et opère des solutions innovantes, dont une plateforme IA privée & hébergée en France, pour protéger les données des entreprises.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

200 clients protégés

20,5 % de croissance du CA

15 années d'expertise

Principales fonctionnalités

Infrastructure : Cloud souverain, certifié ISO 27001/HDS. Hébergement managé, résilient et conforme, sans engagement de durée.

Network Security : Sécurité réseau managée (Cato Networks), interconnexion sites/cloud/nomades avec inspection et Internet sécurisé (SASE / ZTNA).

Email & Collaboration Security : Sécurité messagerie & collaboration avec filtration avancée anti-phishing/malware et sauvegarde illimitée de vos environnements O365.

Endpoint Security : EDR HarfangLab managé par notre SOC, certifié et qualifié par l'ANSSI. Détection-réponse en temps réel sur postes et serveurs.

Identity : Zero Trust, gouvernance des accès et des privilèges, MFA et contrôle continu des comptes via notre PAM managé.

AI : Plateformes IA souveraines conçues par Scalair, hébergées sur notre Cloud, pour des usages métiers critiques, avec un ROI assuré.

Points clés

- Sans engagement de durée
- ISO 27001 & HDS
- Interlocuteurs dédiés
- Support 24/7
- 100% français
- Plateforme de management
- Conforme RGPD
- Expertise Cyber

Scalair
(+33) 3 20 68 21 21
2 bis Avenue Antoine Pinay
59510 Hem
scalair.fr

Demandez une démonstration

Dell PowerEdge XE9780/XE9785

Dell Technologies

Pays d'origine : France

Quand la vision rencontre la puissance : l'IA à votre portée. Avec Dell AI Factory, passez de l'idée à l'impact en simplifiant conception, déploiement et montée en charge. Les Dell PowerEdge XE9780/XE9785 accélèrent vos modèles, réduisent le time-to-market et s'adaptent à vos workloads.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

Jusqu'à 37%
Optimisation des performances

Jusqu'à 8 GPU par serveur
Support haute densité GPU pour l'IA

Jusqu'à 192 GPU par rack
Densité GPU extrême pour l'IA (rack)

Principales fonctionnalités

Infrastructure IA haute performance : Serveurs conçus pour l'entraînement et l'inférence de modèles IA exigeants en environnements professionnels.

Haute densité GPU : Support de configurations GPU avancées pour traiter des charges IA intensives et évolutives.

Architecture évolutive : Architecture pensée pour accompagner l'augmentation des workloads IA sans refonte majeure.

Déploiement industrialisé : Conçu pour s'intégrer dans des architectures standardisées et des projets IA structurés.

Fiabilité de niveau entreprise : Plateforme robuste adaptée aux environnements critiques et aux exigences de continuité.

Optimisation énergétique : Conception visant à contribuer à améliorer l'efficacité énergétique et les coûts d'exploitation.

Points clés

- Déploiement sur infrastructure dédiée
- Accompagnement commercial et technique
- Conformité donnée et sécurité
- Support pour environnements critiques
- Conçu pour architectures multi-clients
- Accès aux ressources partenaires Dell Technologies
- Accompagnement et certifications disponibles

TD SYNNEX
34 Avenue Léonard de Vinci
92400 Courbevoie
www.dell.com

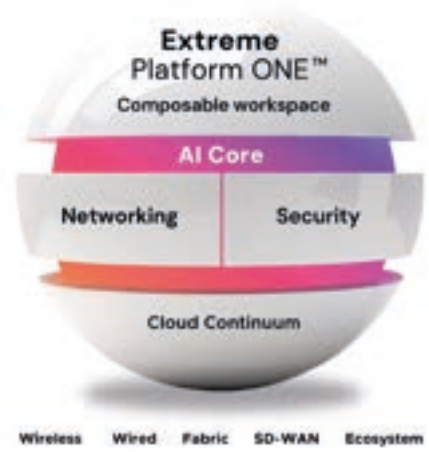
Demandez une démonstration

Extreme Platform ONE™

Extreme Networks

Pays d'origine : États-Unis

La première plateforme réseau tout-en-un intégrant une IA conversationnelle, multimodale et agentique. Extreme Platform ONE™ unifie le réseau, la sécurité et l'IA dans une expérience puissante, pour améliorer l'efficacité, la scalabilité et l'innovation du réseau.



Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

95 % de satisfaction du support (CSAT)

80+ pays à travers le monde

11 000+ partenaires

Principales fonctionnalités

Gestion multi-domaines : Centralisation et supervision des environnements sur une seule plateforme.

Automatisation des workflows : Réduction des tâches manuelles grâce à des processus automatisés.

Personnalisation avancée : Tableaux de bord et flux adaptés aux besoins spécifiques.

Zero-Touch, Zero Trust : Sécurité renforcée avec contrôle d'accès complet.

Support de pointe : Assistance proactive avec Service Agent.

IA intégrée : Optimisation des opérations et réponses instantanées.

Points clés

- Cloud natif
- Multi-tenant (dans le cadre de l'offre MSP)
- Facturation à l'usage (dans le cadre de l'offre MSP)
- Support technique 24/7
- Conformité RGPD
- Portail partenaire dédié
- Licences de démo pour les Labs
- Formations

Distribué par
Westcon-Comstor

Extreme Networks
(+33) 1 86 99 92 19
3 Rue Christophe Colomb
91300 Massy
www.extremenetworks.com/fr

Demandez une démonstration

HCI
LENOVO / NUTANIX

Pays d'origine : Chine & États-Unis

Accélérez l'innovation commerciale et simplifiez vos opérations IT avec Lenovo HX et Nutanix.

Profitez d'une plateforme multicloud hybride performante et simple, permettant d'exploiter toutes vos charges de travail avec flexibilité, évolutivité et sécurité, de la périphérie jusqu'au cloud.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

90 Net Promoter Score

10 ans+ de partenariat

3000 Clients+
dans le monde

Principales fonctionnalités

Performances accrues : Une infrastructure plus moderne et plus fiable avec une résilience renforcée et des SLA optimisés. Support 24/7h.

Services Cloud à valeur ajoutée : IaaS et VM hosting, DRaaS & Backup-as-a-Service, Kubernetes & Containers, AI & GPU Workloads, VDI, Database ,Cloud Edge..

Simplicité et agilité : Plateforme tout-en-un, gestion centralisée, évolutivité selon vos besoins, mise à jour en one click, time to market rapide.

Tarification transparente : Des prix fixés à l'avance, avec une tarification claire, prévisible et un engagement inscrit dans la durée.

Des solutions IA prêtes à l'emploi : Construisez et déployez rapidement votre IA d'entreprise, seule solution IA Edge-to-Cloud, GPT-in-a-Box.

Capacités Multi-Tenant : Isolation locataires, Forecasting, Self-Service, Gouvernance des couts, Microsegmentation, Automatisation, ..

Points clés

- Hébergement dédié ou mutualisé
- Cloud souverain et contrôle des données
- Réduction du TCO jusqu'à 40%
- Programme partenaire dédié
- Accès aux formations et certifications
- Engagement de 12 à 60 mois
- Extension vers le cloud public
- Support 24/7 et un seul point de contact

TD SYNNEX
34 Avenue Léonard de Vinci
92400 Courbevoie
cloud.tdsynnex.fr

Demandez une démonstration

SolarWinds Observability

SolarWinds

Pays d'origine : États-Unis

Les MSP font confiance à SolarWinds pour renforcer leur résilience opérationnelle, de l'observabilité unifiée à la gestion des services. Ses solutions simples, puissantes et sécurisées pour l'IT hybride génèrent des revenus récurrents et de multiples opportunités de ventes additionnelles (upsell).

Cette solution s'adresse :
ETI

300K+ Clients SolarWinds dans le monde entier

84 % des entreprises du Fortune 500®

20+ années de leadership sur Supervision

Principales fonctionnalités

Détection avant impact client : Passez de réactif à proactif. Alertes en temps réel et détection d'anomalies pour corriger les problèmes avant impact client.

Optimisation des Équipes IT : L'AIOps élimine la gestion des urgences et permet de se concentrer sur les tâches plus forte valeur ajoutée.

Surveillance de bout en bout : Détection de la cause première des problèmes. Élimination des angles morts réseau post croissance.

Gestion de la capacité réseau : Optimisation des applications grâce aux données d'utilisation réelles. Haute performance et maîtrise des coûts de bande passante.

Amélioration de la Sécurité : Détecte les vulnérabilités de sécurité cachées. Réduit les risques, atténue les brèches et accélère la correction des incidents.

Time-to-value rapide et rentabilité : Déploiement simple, prise en main rapide et ROI visible en quelques semaines — sans projet long ni expertise rare.

Points clés

- Cloud / SaaS
- On-premise
- Multitenant
- Portail partenaire dédié
- Support francophone
- Formation et certification incluses
- Account manager dédié
- Licences NFR (Not For Resale)

Distribué par
Kappa Data France
NMS Distribution France
Kappa Data BeNeLux
Westcon BeNeLux
Adfontes BeNe

SolarWinds
3-5 Rue Saint Georges
75009 Paris
www.solarwinds.com

Demandez une démonstration

SASE
Check Point

Pays d'origine : Israël

Solution unifiée de sécurité reseau hybride et d'accès distant zero-trust - Protection SAAS et SD-WAN.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

99.999% SLA

80+
Datacenters privés

10x plus rapide dans la protection Internet

Principales fonctionnalités

Protection Internet Hybride : Accédez au web sans risque grâce aux protections appliquées sur les postes, les navigateurs et le cloud.

Protection Web complète : Filtrage web, DNS, et protection contre les malwares. Navigation sécurisée avec isolation des données et protection DLP.

Accès privé full mesh (ZTNA) : Accès granulaire et sécurisé en mode zero trust pour l'ensemble des ressources protégées (utilisateurs et/ou sites).

Protection SAAS : Cartographie de votre écosystème SaaS, identification et correction des risques pour réduire votre surface d'attaque.

Protection des terminaux mobiles : Protection des appareils mobiles avec une protection avancée contre les menaces et des contrôles de confidentialité.

SD-WAN sécurisé : Connectivité optimisée pour plus de 10 000 applications métier. Protection complète avec ThreatCloud AI.

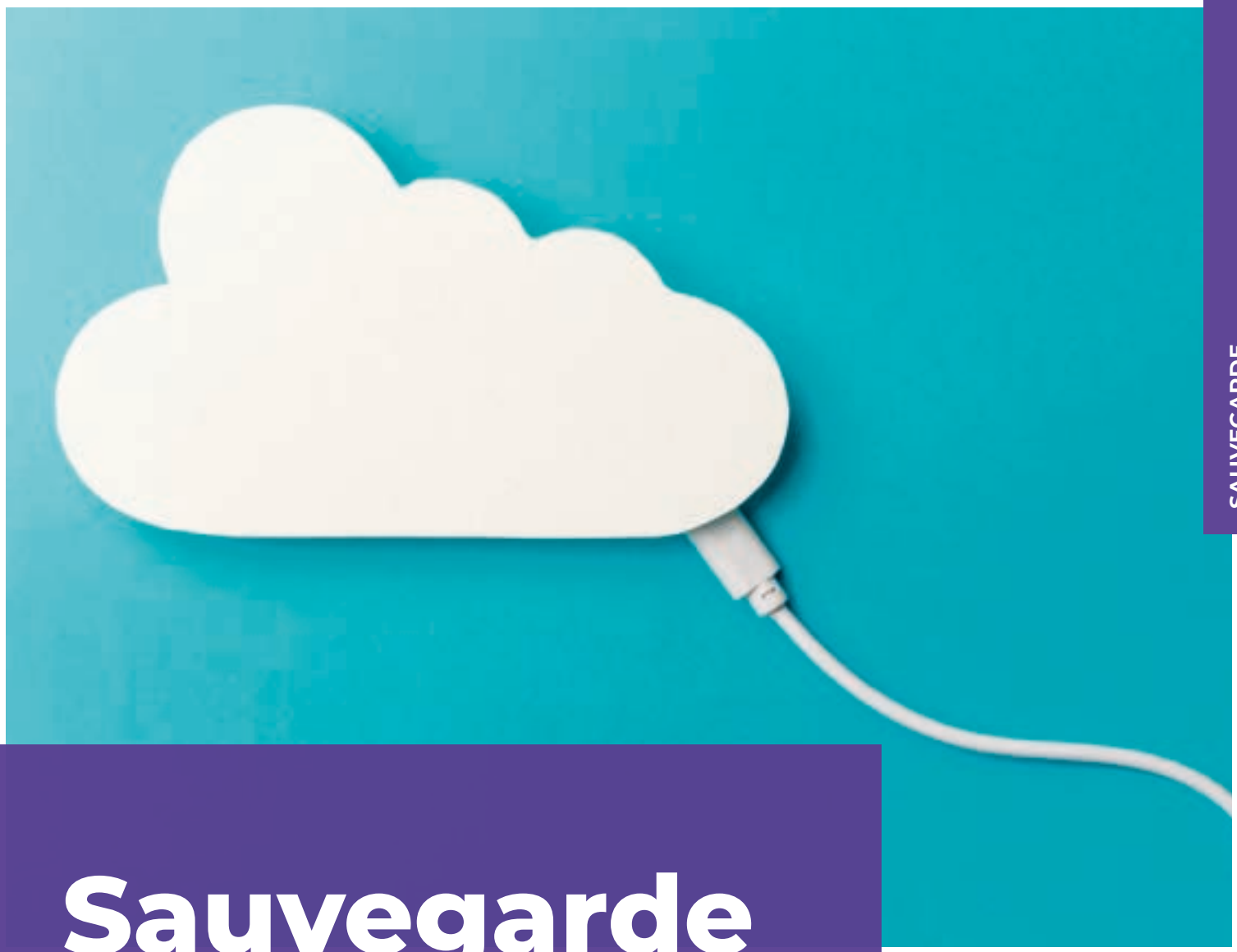
Points clés

- Licence Pay-As-You-Go
- Console multi-tenant
- Protection 24/7 assurée par les experts de Check Point
- Gestion unifiée de la sécurité via un portail web unique

Distribué par
Arrow ECS
Infinigate
Westcon

Check Point Software
20 Avenue André Prothin
92400 Courbevoie
www.checkpoint.com

Demandez une démonstration



Sauvegarde

Les architectures de sauvegarde sont désormais conçues pour résister aux scénarios de compromission. Snapshots applicatifs cohérents, sauvegardes immuables, copies isolées logiquement ou physiquement, chiffrement de bout en bout et séparation des plans de contrôle deviennent des prérequis.

L'objectif n'est plus seulement la protection des données, mais la garantie de leur restaurabilité malgré les aléas. L'intégration avec les hyperviseurs, les environnements cloud et les applications critiques est également devenue centrale. La sauvegarde s'appuie désormais sur des mécanismes de cohérence applicative, d'automatisation des contrôles et de segmentation des dépôts.

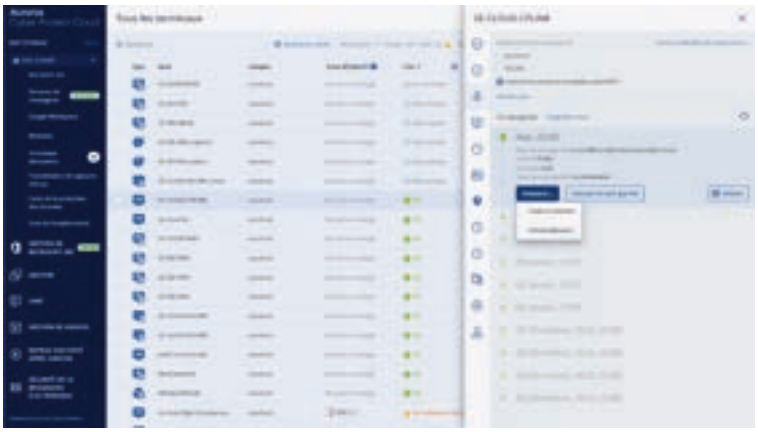
Au-delà de l'architecture, la définition de RPO/RTO réalistes, la hiérarchisation des données et la validation régulière des plans de reprise conditionnent l'efficacité réelle du dispositif. À l'inverse, une sauvegarde non testée ou mal opérée ne constitue qu'une protection théorique en situation de crise.

Acronis Backup

Acronis

Pays d'origine : Suisse

Bénéficiez d'un service de sauvegarde conçu spécialement pour les MSP. Ce service protège tous les environnements, s'intègre à votre offre existante et vous aide à réduire les interruptions d'activité chez vos clients. Acronis Backup est disponible dans Acronis Cyber Protect Cloud.



Cette solution s'adresse :

TPE **PME** **ETI** **Grands comptes**

750 000 entreprises protégées dans le monde via des MSP Acronis

20 000 fournisseurs de services utilisent la plateforme Acronis

7,5 millions d'attaques bloquées en 12 mois grâce à Acronis

Principales fonctionnalités

Sauvegarde complète des données : Sauvegarde de fichiers, de disques, d'images et d'applications.

Sauvegarde des principaux systèmes : Mac, Windows, Linux, Microsoft 365, Google Workspace, Synology, Hyper-V, VMware, Proxmox VE, etc.

Options de stockage hybrides : Stockage dans le cloud hébergé par Acronis, clouds publics tels que Microsoft Azure ou stockage local du fournisseur MSP.

Migration multi-environnements : Migration entre environnements cloud, locaux et virtuels.

Options de restauration flexibles : Restauration fiable, de la reprise intégrale des systèmes à la récupération granulaire de fichiers, dossiers et applications.

Sauvegardes immuables : Vos données restent intègres et protégées contre toute altération ou suppression.

Points clés

- Différents hébergements possibles : Cloud, local, hybrid
- Hébergement en France
- Console multi-tenant
- Facturation mensuelle
- Protection complète de Microsoft 365
- Formations et certifications sur-mesure pour les MSP
- Conformité réglementaire éprouvée
- Solution certifiée

Distribué par
TD SYNNEX
Infinigate France
ALSO

Acronis
(+33) 1 87 16 91 19
20-22 Rue Marius Aufan
92300 Levallois-Perret
www.acronis.com

Demandez une démonstration

Veeam CSP

Veeam Cloud Service Provider

Pays d'origine : États-Unis

Le programme VCSP offre un modèle mensuel flexible pour proposer BaaS, DRaaS, hébergement protégé, backup cloud public et M365, avec l'accès à tout le portefeuille Veeam pour développer des services managés complets et évolutifs.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

20 000+ MSP
s'appuient déjà sur Veeam dans le monde

550 000+ clients
Protégés par Veeam

#1 9 années consécutives selon le Gartner

Principales fonctionnalités

Sauvegardes immuables : Support de l'immutabilité sur S3, S3-compatible, Azure Blob, Linux Hardened Repository. Protection anti-ransomware WORM intégrée.

Orchestration du DR (DRaaS) : Failover automatisé, runbooks, tests de restauration programmés, conformité, RTO/RPO prédictifs. Idéal pour proposer du DR managé.

Protection multi-plateformes : VMware, Hyper-V, Nutanix, Proxmox, physiques, NAS, Kubernetes (Kasten), Azure, AWS, GCP, Microsoft 365.

Vérification automatisée des backup : SureBackup / SureReplica : boot automatisé en sandbox + validation applicative.

Détection d'anomalies : Machine Learning pour détecter anomalies de volume, taux de changement, comportements suspects.

API REST + automatisation complète : Provisioning, onboarding client, déploiements massifs d'agents, monitoring et reporting via VSPC ou scripts PowerShell.

Points clés

- Veeam Service Provider Console - management multi-tenant
- Solutions software et SaaS
- Sauvegarde de l'écosystème Microsoft 365
- Support expert, réactif et fiable 24/7
- Facturation mensuelle et à l'utilisation
- Souveraineté des données
- Déploiement en local
- Marque blanche

Distribué par
TD SYNNEX

Veeam Software
102 Terrasse Boieldieu
92085 La Défense
cloud.tdsynnex.fr

Demandez une démonstration

Cove Data Protection

N-able

Pays d'origine : États-Unis

Cove Data Protection de N-able, c'est la solution de sauvegarde cloud simple et performante pour serveurs, postes et Microsoft 365. Elle garantit une restauration rapide, une gestion centralisée et une protection fiable des données critiques contre les pertes et cyberattaques.

Cette solution s'adresse :

TPE **PME** **ETI**

180 000 entreprises protégées

14 000 MSP satisfaits et protégés

2 Millions+ d'utilisateurs M365 protégés

Principales fonctionnalités

Sauvegarde Cloud centralisée : Sauvegarde serveurs, postes et Microsoft 365 avec stockage cloud intégré, simples et rapides.

Restauration complète ou granulaire : Récupération de fichiers individuels, systèmes complets ou bare-metal selon les besoins..

Chiffrement AES 256 bits : Données protégées en transit et au repos avec chiffrement standard industriel. Stockage dans un data center certifié HDS.

Optimisation TrueDelta : Déplace jusqu'à 60 fois moins de données que la sauvegarde image classique.

Retenue jusqu'à 7 ans : Conserve les données Microsoft 365 pour conformité et besoins réglementaires.

Tableau de bord unique : Gère tous les backups multi-sites et tenants dans une seule interface web.

Points clés

- Architecture centrée sur le cloud
- Support de l'équipe Infinigate en France
- Preuve de conformité RGPD globale N-able
- Protection et restauration des données Microsoft 365
- Facturation mensuelle avec une tarification transparente
- Gérez plusieurs clients depuis une seule console
- Certifications ISO 27001, SOC 2 et HIPAA 1
- Stockage redondant dans les datacenters d'Equinix à Paris

Distribué par
Infinigate France

N-able
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/n-able/

Demandez une démonstration

Disaster Recovery

Jotelulu

Pays d'origine : France

Quand l'activité de vos clients est en jeu, chaque seconde compte. Découvrez la première solution de plan de reprise d'activité (PRA) simple et abordable pour les entreprises qui ne peuvent pas se permettre d'interruptions.

Cette solution s'adresse :
TPE **PME** **ETI**

3 Régions | **1h** RPO | **1h** RTO

Principales fonctionnalités

Configuration assistée : Lancez votre plan DR en quelques clics, gagnez du temps et minimisez les erreurs.

Simulation de reprise : Anticipez les crises en réalisant des simulations de sinistres, et générez des rapports d'audit.

RTO et RPO personnalisés : Décidez des fréquences de réplication selon vos exigeances (toutes les 1, 3, 6, 12 ou 24 heures).

Bascule en un clic : Profitez d'une protection sans effort grâce à la bascule instantanée de l'intégralité de vos systèmes.

Dashboard de pilotage : Gérez vos plans de reprise depuis une interface simple et centralisée.

Événements et notifications : Restez informé en temps réel de tout événement.

Points clés

- Hébergement en France
- Multi-tenant
- Conformité ISO 27001 et HDS
- Programme partenaire
- Support illimité en français 24/7
- Coût raisonnable
- Performance optimale

Distribué par
Jotelulu
Partenaires Jotelulu

Jotelulu
(+33) 1 87 65 31 20
www.jotelulu.com/fr-fr/productos/disaster-recovery

Demandez une démonstration

Leviia Storag3 (S3)

Leviia

Pays d'origine : France

Leviia Storag3 est une solution S3 souveraine de backup cloud conçue pour la vente indirecte, offrant aux partenaires un pilotage multi-clients, une gestion sur mesure, une sécurité de haut niveau et un modèle économique prévisible.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

600+ clients

99 % des clients renouvellent

100 % souverain et prévisible

Principales fonctionnalités

Stockage sur-mesure par client : Allouez précisément la capacité de stockage de chaque client, à partir de 10Go, et adaptez les volumes en toute simplicité.

Gouvernance client flexible : Vous gérez un abonnement par client avec 3 modes de gestion au choix : uniquement par vous, par votre client, ou les deux.

Visibilité claire des consommations : Suivez les usages de vos clients sur 30j. Volume stocké, transféré, téléchargé. Anticiper les besoins et sécuriser la facturation.

Pilotage complet par API sécurisée : Notre API permet de gérer en totalité les identifiants et de récupérer leurs informations de configuration et d'usage.

Versioning et immuabilité intégrées : Protégez les données critiques avec versioning et verrouillage des buckets, indispensables pour backup et PRA.

Gérez votre équipe : Gérez les droits et accès avec différents rôles : admin, lecture seule, facturation, statistiques, etc.

Points clés

- Géo-répartition des Données sur 3 Data Centers
- Aucun frais cachés / supplémentaires
- Certifications ISO27001 & HDS
- Hébergement Souverain
- Console dédiée Partenaire
- Support Français et Réactif
- Durabilité 99,999999999%
- Conforme RGPD

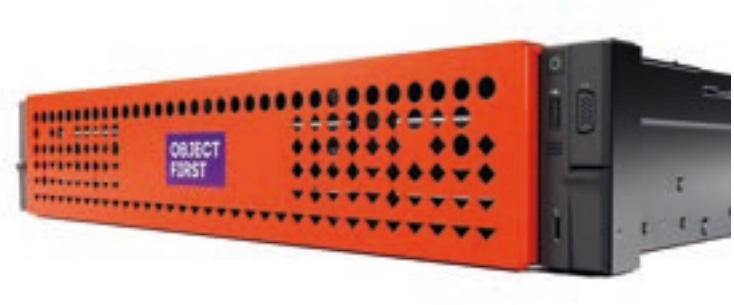
Leviia
14 Avenue de l'Europe,
77144 Montévrain
www.leviia.com

Demandez une démonstration

Ootbi
Object First

Pays d'origine : France

Quand (et non pas « si ») vous êtes victime d'un ransomware, votre avenir dépend de votre cyber-résilience. Object First offre un stockage conçu pour Veeam, totalement sécurisé, simple à installer et maintenir, puissant et fiable dans la durée. Avec Object First, vous devenez simplement résilients.



Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

15 min
Installé en 15 mn

8BG/s Vitesse de récupération maximale

7PB Capacité max. par Veeam SOBR

Principales fonctionnalités

Sécurité : Pentesté par un organisme externe, absolument immuable; permet notamment la compliance DORA et NIS2.

Simplicité & Fiabilité : Coûts d'installation, d'utilisation et de maintenance les plus faibles du marché. Gestion de flotte et monitoring (Fleet Manager).

Scalabilité : De 20To à plus de 7Po, sans limite.
Les appliances de tailles variées peuvent être mélangées, placées chez le SP ou chez le tenant.

Multi Tenant : Multi tenancy configurée au niveau de la console Veeam.

CAPEX ou consommation mensuelle : Choisissez entre un investissement en CAPEX, ou bien en un paiement mensuel pour la quantité de stockage consommée.

Performance : Vitesses de backup et de reprise garanties jusqu'à 8GB/s.

Points clés

- Sécurisé, simple, fiable, évolutif
- Conforme au RGPD, à la loi DORA et à la norme NIS2
- Portail partenaire dédié et gestion d'interface
- Facturation mensuelle
- Multi Tenant
- Gestionnaire de compte dédié
- Formation et certification incluses
- Support Technique 24/7

Distribué par
TD SYNNEX

Object First
(+33) 7 89 45 28 78
14 Rue de Chateaudun
75009 Paris
objectfirst.com

Demandez une démonstration

OpenText Cloud to Cloud Backup

OpenText Cybersecurity

Pays d'origine : Canada

Solution complète de sauvegarde et de récupération des applications SaaS, telles que MS 365, Google Workspace, SalesForce, Box et Dropbox, avec une gestion centralisée, une restauration granulaire, une récupération rapide et des options de conservations flexibles.

Cette solution s'adresse :
TPE **PME** **ETI**

81 % des sociétés ont perdu des données SaaS

35 % comptent sur leur fournisseur SaaS

Pour 25% des sociétés la cause n°1 la suppression malveillante

Principales fonctionnalités

Protection : OpenText Core Cloud-to-Cloud Backup protège contre la perte de données, les violations et les ransomwares.

Sauvegarde automatique en France : Sauvegardes automatiques de Microsoft 365, Google Workspace, Salesforce, Box et Dropbox. Datacenters AWS en France.

Restauration granulaire : Restauration rapide, flexible et granulaire (items, boîtes mail, sites...).

Restauration "point-in-time" : Restaure les données à un instant précis.

Stockage et rétention illimités : Conservez toutes vos données sans limite de volume ni de durée pour une protection complète et continue.

Redondance totale : Vos données sont copiées sur plusieurs sites pour garantir une disponibilité continue et éliminer tout risque de perte.

Points clés

- Console unique de gestion
- Interface intuitive, self-restore
- Mise en place en 2 minutes, 3 étapes
- Support MS 365, Google Workspace, Salesforce, Box, Dropbox
- Restauration flexible : point-in-time, par mots-clés
- Conformité réglementaire
- Accès limité via MFA et LDAP
- Datacenters en France

Distribué par
MIEL
OpenText Cybersecurity

OpenText Cybersecurity
(+33) 1 47 96 65 24
Cœur Défense Tour B
92400 Paris la Défense
cybersecurity.opentext.com

Demandez une démonstration

Stockage Objet Cloud

Impossible Cloud

Pays d'origine : Allemagne

Impossible Cloud propose un stockage compatible S3 et conforme au RGPD dans des centres de données de l'UE. Plus de 2 000 entreprises nous font déjà confiance pour la sauvegarde, la reprise après sinistre, l'archivage et la protection contre les ransomwares.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

100+ Experts en Europe

25+ Intégrations cloud et backup

6+ Régions de data centers

Principales fonctionnalités

Versioning des objets : Enregistrement et gestion de toutes les versions passées des objets pour éviter les pertes de données accidentelles.

Verrouillage des objets : Verrouillage grâce à un mécanisme conforme WORM afin de rendre les données immuables et de les protéger contre les ransomwares.

Protection des données : Chiffrement des données grâce au codage d'effacement avancé, garantissant une sécurité maximale lors du transfert et du stockage.

Intégrations fluides : Connection aux solutions de sauvegarde déjà utilisées pour un déploiement rapide et une protection fiable des données.

Haute durabilité : Distribution des données sur plusieurs nœuds, garantissant leur sécurité et leur accessibilité sur le long terme.

ACL et CORS : Gestion des autorisations avec des politiques par bucket, des listes de contrôle d'accès (ACL) et configuration CORS.

Points clés

- Conformité RGPD
- Hébergé en France
- Support en Français
- ISO 27001
- Multi-tenant
- Console partenaire
- Tarification transparente
- Marque blanche

Distribué par
Softvalue Distribution

Softvalue Distribution
(+33) 1 89 70 99 54
26 Rue Mars et Roty
92800 Puteaux
www.impossiblecloud.com

Demandez une démonstration

Arcserve Cyber Resilient Storage

Arcserve

Pays d'origine : États-Unis

Arcserve Cyber Resilient Storage est une solution de stockage de sauvegarde immuable intégrée à Arcserve UDP et ShadowProtect, conçue pour protéger les données contre les ransomwares et assurer conformité et récupération rapide des sauvegardes.

Principales fonctionnalités

Stockage immuable : Les données sauvegardées sont protégées contre toute modification ou suppression non autorisée

Sécurité avancée et gouvernance : Architecture multicouche pour protéger les données et répondre aux exigences de conformité

Gestion centralisée : Interface unique intuitive pour gérer sauvegardes et stockage sur site ou dans le cloud.

ARCSERVE
(+33) 1 80 20 56 19
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com/fr/vendors/arcserve/

Distribué par
Infinigate France

Backup Files and Data

RG System Suite

Pays d'origine : France

Assurez la protection des données sensibles de vos clients avec RG System Suite, une solution hébergée en France et conforme au RGPD. Depuis une console unique, pilotez toutes les sauvegardes et restaurez-les en quelques clics en cas d'incident.

www.rgsystem.septeo.com

Backup Microsoft 365

RG System Suite

Pays d'origine : France

RG System Suite offre une protection complète pour Exchange, OneDrive, SharePoint et Teams. Basée sur Veeam Backup pour Microsoft 365, cette solution garantit aux MSP un contrôle sur les données de leurs clients, même en cas de suppression ou d'attaque.

www.rgsystem.septeo.com

Archivage réglementaire

L'archivage réglementaire est rarement au centre des discussions informatiques. Jusqu'au jour où un contrôle, un audit ou un contentieux en révèle les insuffisances. De la facturation électronique à la dématérialisation des processus RH, la montée des exigences de conformité a fait évoluer l'archivage bien au-delà du simple stockage de long terme.

Les solutions intègrent désormais des mécanismes garantissant l'intégrité et la valeur probatoire des documents : scellement, horodatage, gestion fine des durées de conservation, traçabilité des accès et restitution contrôlée. L'archivage s'inscrit maintenant dans les flux applicatifs et collaboratifs, notamment la messagerie, les GED ou les outils métiers, afin de limiter les manipulations manuelles et les risques d'erreur.

L'enjeu n'est plus seulement de conserver, mais de pouvoir restituer rapidement des éléments fiables et opposables. Pour le prestataire informatique, il s'agit alors de travailler sur des règles structurées et reproductibles : périmètre des contenus, responsabilités, engagements contractuels et capacité à répondre à un contrôle. Intégré aux flux existants, l'archivage s'inscrit dans une logique de récurrence et de gouvernance documentaire, sans alourdir l'exploitation.

Pineappli

LuxTrust

Pays d'origine : France

Pineappli est une solution d'archivage électronique certifiée NF461, sécurisée et souveraine, développée et hébergée dans l'UE. Évolutive et interopérable, elle garantit conformité, traçabilité et valeur légale durable de vos archives numériques.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

100% européenne
Stockage régionalisé au sein de l'UE

+20 ans d'expertise
Au service de la confiance numérique

Solution unique
GED, archivage, transferts sécurisés

Principales fonctionnalités

Archivage intelligent automatisé : Versement simple (API, dossiers, manuel), classement, métadonnées, règles de conservation paramétrables et attestations horodatées.

Intégration fluide aux métiers : API native pour ERP, GED, RH ou finance. Stockage évolutif, recopie automatique et interface intuitive adaptée à vos usages.

Déploiement selon vos besoins : Disponible en SaaS public, SaaS privé ou mode hybride avec maintien des certifications, dont NF461.

Sécurité maximale des archives : Chiffrement avancé, technologie brevetée, empreintes numériques et contrôles d'intégrité automatiques hebdomadaires.

Certifications de référence : Certifiée NF461, NF Z42-013/020, ISO 27001 et HDS pour répondre aux standards les plus exigeants.

Conformité et valeur probante : Conforme eIDAS et RGPD, avec horodatages et cachets électroniques qualifiés assurant une valeur légale irréfutable.

Points clés

- Certifications de sécurité
- Conformité RGPD
- Cloud/SaaS
- Hébergement souverain
- Marque blanche
- Multi-tenant
- Support multilingue
- Support technique 24/7

LuxTrust
(+352) 621 781 267
6 Rue Auber
75009 Paris
www.luxtrust.com

Demandez une démonstration

Signature électronique

La signature électronique est désormais un point de passage obligé pour de nombreux processus métiers. L'enjeu n'est plus de "faire signer", mais de garantir la valeur probante d'un acte numérique tout en l'intégrant aux flux existants. C'est cette capacité d'industrialisation, plus que la fonctionnalité elle-même, qui a profondément fait évoluer l'outil.

L'intégration aux ERP, CRM, outils RH ou plateformes documentaires a déplacé la signature au cœur des parcours applicatifs. Les mécanismes d'identification se sont renforcés, les niveaux de preuve se sont affinés, et la traçabilité est devenue exploitable en cas de contrôle ou de litige.

Ce repositionnement modifie les usages et les responsabilités ce qui en fait une opportunité commerciale pour les MSP. Les équipes IT ne se contentent plus de déployer un service, elles participent à la définition des chaînes de validation, des rôles, et des exigences juridiques associées. La signature électronique devient ainsi un levier de standardisation des processus, capable d'accélérer les échanges sans fragiliser la conformité ni la gouvernance documentaire.

COSI

LuxTrust

Pays d'origine : France

COSI est une plateforme de signature électronique souveraine, sécurisée et conforme eIDAS. Développée et hébergée dans l'Union européenne, elle s'adapte aux exigences des secteurs les plus sensibles.
Sécurisez chaque transaction et document avec fluidité et confiance.

Cette solution s'adresse :
PME **ETI** **Grands comptes**

100% européenne
Gardez le contrôle total de vos données

+20 ans d'expertise
Au service de la confiance numérique

Hub de services de confiance
Signature, cachet, horodatage

Principales fonctionnalités

Conformité eIDAS : 3 niveaux de signature électronique eIDAS (simple, avancée, qualifiée), service de validation.

Automatisation à grande échelle : Workflows visuels configurables avec suivi en temps réel, gestion de fichiers volumineux et campagnes de signature en masse.

Interopérabilité & formats : Remplissage des documents avec champs interactifs (Acroforms), signature de documents par lots et multi-formats (PDF, XML etc.).

Identités numériques qualifiées : Compatibilité avec de multiples identités numériques européennes et asiatiques pour signer partout dans le monde.

Sécurité & valeur probante : Confidentialité par hash signing, piste d'audit cachetée et accessible à tout moment, préservation des signatures existantes.

Déploiement & intégration : Cloud public, privé ou on-premise. API modulaires et connecteurs prêts à l'emploi. Archivage électronique intégré.

Points clés

- Conformité eIDAS et RGPD
- Certifications de sécurité
- Cloud/SaaS
- On-premise
- Hébergement souverain
- Multi-tenant
- Support multilingue
- Marque blanche

LuxTrust
(+352) 621 781 267
6 Rue Auber
75009 Paris
www.luxtrust.com

Demandez une démonstration

Autres services et produits

Ce guide a pour vocation de présenter un large éventail de solutions technologiques destinées aux prestataires informatiques. Il se conclut naturellement par un focus sur plusieurs services complémentaires qui facilitent la gestion et le développement de leur activité.

Parmi eux, un ERP-CRM conçu pour les sociétés de services informatiques, propose une approche intégrée de la relation client, du suivi de contrat et de la facturation.

S'ajoutent à cela un courtier en cyberassurance permettant d'élargir votre offre tout en générant des revenus additionnels, une agence de prospection B2B spécialisée dans les secteurs de l'IT et de la cybersécurité pour accompagner la croissance commerciale, et un service de financement dédié à l'investissement en matériel et en infrastructure réseau.

Comme pour l'ensemble des solutions présentées dans ce guide, un QR code permet de prendre rendez-vous directement avec la société référencée, afin de faciliter la mise en relation.

artis.net
ARTIS

Pays d'origine : France

Éditeur français d'une solution métier ERP-CRM, ARTIS accompagne les professionnels de l'informatique, des télécommunications, de la bureautique et de la sûreté électronique en automatisant et en optimisant leurs processus de gestion.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

Depuis 35 ans
éditeur et intégrateur ERP-CRM

10 000 utilisateurs d'artis.net

Plus d'1 million
de contrats gérés par artis.net

Principales fonctionnalités

CRM / Gestion de la relation client : Gestion des sociétés et des contacts, des actions commerciales, du parc client / concurrent, génération des devis et des affaires, pilotage des forces de vente (BI).

Chaîne des ventes : Génération des commandes, des bons de livraison, des factures, signature électronique des documents.

Gestion des contrats : Gestion des contrats de maintenance, de service, licences informatiques, contrats opérateurs télécoms.

Chaîne des achats : Commande d'articles référencés jusqu'à la facture fournisseur, EDI Article avec vos catalogues constructeurs/grossistes.

PSA / Gestion des services : Gestion du ticketing / SAV, planification des interventions, gestion de projet, ordonnanceur, gestion des mots de passe...

Portail client : Gestion des demandes clients, suivi des interventions, affichage détaillé des consommations, factures électronique.

Points clés

- Mode SaaS ou On premise
- Éditeur français
- ERP-CRM spécialisé pour l'IT
- Multi société
- Mobilité
- EDI Grossistes
- Portail client
- Formations certifiées Qualiopi

ARTIS
(+33) 2 40 80 29 55
6 Rue Marie Curie
44230 Saint-Sébastien-sur-Loire
www.artis.fr

Demandez une démonstration

Assurance Cyber
CYBERASSURE

Pays d'origine : France

CYBERASSURE est le premier courtier en assurance cyber exclusivement dédié aux prestataires IT.
Protégez vos clients en leur offrant la solution de sécurité ultime : une cyber assurance proactive incluant des outils de monitoring avancés.

24/7
Accompagnement 24h/7

7,5 M€ Garantie
Jusqu'à 7,5 millions d'euros

12h Durée moyenne
de remédiation

Principales fonctionnalités

Responsabilité civile cyber : Prise en charge des conséquences financières liées à toute réclamation d'un tiers suite à une fuite de données/transmission virus.

Responsabilité civile Media : Couvre le coût et les frais de défense liés à toute réclamation d'un tiers suite à une divulgation d'informations confidentielles.

Perte d'exploitation : Couvre vos pertes de marge brute d'exploitation suite à une interruption totale ou partielle de votre système informatique.

Cyber fraude : Prise en charge des conséquences financières résultant d'une cyberfraude à votre encontre, due à une intrusion malveillante.

Mobilisation d'experts dédiés : Accompagnement à chaque étape : ingénieurs, spécialistes en cybersécurité, juristes, gestionnaires de crise, et bien d'autres.

Frais de reconstitution de votre SI : Couvre les frais engagés pour remettre vos systèmes d'information en état de fonctionnement.

Points clés

- Continuité des activités
- Plateforme de prevention (Scan cloud, AD, phishing)
- Gestion des cyberattaques
- Assistance spécialisée
- Responsabilité légale
- Protection des données

CYBERASSURE
(+33) 1 85 39 01 71
5 Rue du chant des oiseaux
78360 Montesson
www.cyberassure.fr

Demandez une démonstration

Prospection B2B pour les MSP

LEADGEND

Pays d'origine : France

LeadGend est un cabinet de prospection B2B spécialisé autour des métiers de la Cybersécurité et de l'IT.

Nous accompagnons tout type de clients, MSP, MSSP, éditeurs, Intégrateur, distributeur etc. dans l'accélération de leur croissance commerciale.

10 000+ RSSI/DSI contactés

250+ nouveaux contacts par mois par client

50+ échanges par semaine par client

Principales fonctionnalités

CRO part time : Management suivi et formation des équipes commerciales internes.

Création de base de données : Identification des personas, ciblage des comptes, recherche des décideurs, qualification et collecte des contacts.

Réalisation de campagnes d'appels : Minimum de 30 appels quotidiens réalisés par client.

Génération de rendez-vous qualifiés : Génération en moyenne de 2 rendez-vous par semaine et par client.

Création d'un pipe commercial : Identification des besoins et projets clients, définition des indicateurs et gestion complète du cycle de vente.

Contractualisation : Négociation, rédaction des propositions commerciales et closing.

Points clés

- Expérience
- Expertise
- Flexibilité
- Réseau
- Outillage
- Résultats
- Trésorerie maîtrisée
- International

Leadgend
(+33) 6 59 23 12 26
9 Rue des Colonnes
75002 Paris
www.leadgend.fr

Demandez une démonstration

Solutions de paiement pour les MSP

TD SYNNEX Capital

Pays d'origine : France

Le financement fournit les capitaux essentiels nécessaires pour construire ou améliorer rapidement les infrastructures. Ces mêmes infrastructures qui vous permettront d'étendre vos activités et de servir plus efficacement une clientèle grandissante.

Cette solution s'adresse :
TPE **PME** **ETI** **Grands comptes**

13.2 % Croissance annuelle du financement IT

4,2 Mds € Marché français de la location IT

48% des entreprises financent une partie de leurs achats IT

Principales fonctionnalités

Augmentez votre trésorerie : Bénéficiez d'un financement immédiat pour l'ensemble de la solution : matériel, logiciel et services inclus.

Préservez votre capital : Gardez vos fonds pour d'autres besoins de l'entreprise comme les recrutements, le marketing ou le développement.

Paiements adaptés à vos revenus : TD SYNNEX Capital ajuste les échéances à vos besoins ainsi qu'à l'utilisation prévue par votre client final.

Développez votre activité : Grâce au financement, agrandissez votre entreprise sans avoir à supporter d'emblée le coût total d'un nouvel équipement.

Restez à la pointe : Accédez aux dernières technologies sans devoir investir immédiatement, protégeant ainsi vos investissements contre l'obsolescence.

Points clés

- Durées de 12 à 60 mois
- Report du premier paiement
- Échelonnement des paiements
- Crédit-bail et location
- Tous les produits, quelle que soit leur provenance

Distribué par
TD SYNNEX

TD SYNNEX Capital
(+33) 6 67 91 64 81
7 Avenue Hergé
77700 Chessy
fr.tdsynnex.com

Demandez une démonstration

Les **distributeurs**

Actual Systèmes

Distributeur expert en matériel et solution IT. Avec plus de 15 offres MSP au catalogue, la BU Solutions apporte aux Service Providers conseil, sécurité et développement, automatisation, formation, et garantit un service de qualité à ses clients dans une interface centralisée.
Réactivité, conseil et proximité.

1 250 Service Provider

1er agrégateur Acronis Français

15 Offres MSP

34 personnes à votre écoute

Solutions MSP distribuées

Cyber Protect Cloud
Acronis

Sauvegarde

Acronis Cyber Protect Cloud est une solution complète pour les MSP, combinant sauvegarde, cybersécurité et plan de reprise d'activité dans une interface centralisée.

Gestion Identités
LastPass

IAM

LastPass centralise et sécurise les mots de passe et les accès, permettant aux utilisateurs de se connecter facilement et en toute sécurité, même à distance.

VSPC
Veeam

Sauvegarde

Veeam VSPC, la console d'administration pour une gestion flexible et autonome de vos licences Veeam. Optez pour un mode de facturation à l'usage sans engagement.

MSP ADMINISTRATOR
ESET

EDR / XDR

Grâce à sa console MSP intuitive, vous pouvez facilement gérer les licences de vos clients, tout en assurant une protection proactive contre les cybermenaces.

Plateforme cyber
Mailinblack

Sécurité de la messagerie

Protégez votre organisation grâce à une suite de solutions françaises performantes : sécurisation des emails, formation, sensibilisation des collaborateurs & gestionnaire de mots de passe.

Solution Managée
XGUARD EDR

EDR / XDR

XGUARD est la solution managée combinant un SOC français et un EDR avancé, pensée pour offrir une cybersécurité complète, simple à déployer et ultra-compétitive.

Actual Systèmes
(+33) 5 57 92 37 92
3 Rue Adrienne Bolland
33185 Le Haillan
actualsystemes.com

Prenez rendez-vous pour découvrir notre catalogue

BeMSP

BeMSP aide les MSP à structurer, automatiser et sécuriser leurs opérations avec une sélection d'outils leaders, des méthodes éprouvées et des partenaires de confiance. Revenus récurrents, service premium et sérénité opérationnelle deviennent les leviers d'une activité pérenne, efficace et rentable.

600 MSP accompagnés

40 solutions dédiées aux MSP

1 000 membres dans notre communauté exclusive

25 experts MSP à votre service

Solutions MSP distribuées

Kaseya 365 Endpoint
Kaseya

RMM

Supervision et gestion à distance intégrées dans une plateforme unifiée : déploiement, support, sécurité, monitoring... sans friction.

Datto RMM
Kaseya

RMM

Surveillez, gérez et automatisez vos environnements IT à distance. Déploiement, patching et alertes intégrés pour un support proactif et efficace.

Kaseya 365 User
Kaseya

Sécurité de la messagerie

Protection des utilisateurs simplifiée : prévention, détection, réponse et reprise intégrées pour renforcer la sécurité et limiter les interruptions.

Autotask PSA
Kaseya

PSA

Pilotez vos services IT de A à Z avec un PSA complet : tickets, temps, contrats, facturation et reporting. Structurez, développez et anticipez grâce à l'IA.

Kaseya 365 Ops
Kaseya

PSA

Plateforme unifiée avec PSA, documentation et automatisation. L'IA optimise les flux pour des opérations plus rapides, standardisées et parfaitement fluides.

IT Glue
Kaseya

Gestion documentaire

Centralisez et sécurisez votre documentation IT : mots de passe, assets, SOP et relations clients, accessibles en un clic pour un support rapide et fiable.

BeMSP
(+33) 9 75 18 70 01
59 Rue de Verdun
69500 Bron
www.bemsp.fr

Prenez rendez-vous pour découvrir notre catalogue

BeMSP

Solutions MSP distribuées

Datto SIRIS 6
DATTO

Sauvegarde

Les solutions BCDR Datto unissent sauvegarde, virtualisation et restauration locale/cloud pour une reprise après sinistre ultra-rapide et une continuité sans faille.

Acronis Cyber Protect Cloud
ACRONIS

Sauvegarde

Console unique pour gérer sauvegarde, antimalware, détection comportementale et reprise rapide. IA intégrée, RTO/RPO courts, coûts maîtrisés.

ThreatDown
MALWAREBYTES

MDR

Protection tout-en-un avec EDR, MDR, rollback, IA, antiphishing, patching et remédiation 24/7. Une plateforme intuitive pour sécuriser tous les endpoints.

ConnectSecure
CONNECTSECURE

Scan de vulnérabilité

Identifiez, priorisez et corrigez les failles grâce à un scan de vulnérabilités complet. Visibilité, conformité et remédiation depuis une seule console.

LiongardIQ
LIONGARD

Suivi de la conformité

Visibilité temps réel, détection des écarts, insights IA et actions automatisées pour sécuriser la surface d'attaque et renforcer la résilience cyber.

Keeper MSP
KEEPER

Gestionnaire de mot de passe

Gérez et sécurisez mots de passe, identifiants et secrets dans une architecture zero trust. Coffres-forts chiffrés, partage sûr et conformité intégrée.

usecure
USECURE

Sensibilisation à la cybersécurité

Automatisez la formation cyber, les tests phishing et la gestion des chartes. Identifiez les risques humains et renforcez la cyber-résilience de vos clients.

Ironscales
IRONSCALES

Sécurité de la messagerie

Sécurité email intelligente avec IA adaptative, remédiation automatisée et déploiement instantané sans changer le flux MX. Traitez les incidents 60× plus vite.

BeMSP
(+33) 9 75 18 70 01
59 Rue de Verdun
69500 Bron
www.bemsp.fr

Prenez rendez-vous pour découvrir notre catalogue

Cris Réseaux

Cris Réseaux, distributeur national expert en cybersécurité, accompagne plus de 1500 prestataires IT, MSP et ESN avec un portefeuille complet et interconnecté de solutions. Nous aidons à renforcer la sécurité, la performance et la conformité avec un accompagnement de l'avant-vente à l'intégration en passant par la formation et le support.

1 500 partenaires actifs

7 agences en France

8 éditeurs

90% de satisfaction partenaires

Solutions MSP distribuées

Network Security
STORMSHIELD

Firewall

La gamme SNS regroupe les firewalls Stormshield, offrant une cybersécurité unifiée et robuste, certifiée ANSSI, avec firmware unique et hautes performances réseaux.

365 Total Protection
HORNETSECURITY

Sécurité de la messagerie

Hornetsecurity sécurise Microsoft 365 via une suite unifiée : protection email, conformité, sauvegarde, IA avancée, continuité d'activité et gestion des permissions.

Vision One
TrendAI

EDR / XDR

Plateforme de cybersécurité unifiée protégeant endpoints, cloud, email et identités, avec gestion de la posture de sécurité, protection de l'IA et remédiation.

WALLIX PAM
WALLIX

IAM/PAM

WALLIX PAM protège les comptes à privilèges, centralise et audite les accès via le Bastion, sécurise les sessions avec MFA et assure la conformité réglementaire.

Olfeo SSE
OLFEO BY EKINOPS

SASE/SSE

Plateforme SSE européenne souveraine, protégeant le trafic web via SWG cloud, Zero Trust, prévention des pertes de données et politiques d'accès unifiées IT.

RG SYSTEM SUITE
SEPTEO IT SOLUTIONS

RMM

RG System Suite est une plateforme SaaS tout-en-un pour MSP qui supervise, sécurise et sauvegarde les environnements IT via une console multi-tenant automatisée.

Cris Réseaux
(+33) 4 42 97 55 75
255 Rue Louis Berton
13290 Aix-en-Provence
www.cris-reseaux.com

Prenez rendez-vous pour découvrir notre catalogue

Hermitage Solutions

Distributeur à valeur ajoutée et expert en infra, cyber, IA, MSP, Hermitage Solutions est le partenaire de 400+ MSP. Nous offrons des solutions de pointe et un accompagnement dédié (technique, commercial conseil, formations) pour vous aider à structurer et optimiser vos offres.

700 partenaires dont plus de 400 MSP

20 ans d'expertise

30 marques au catalogue

26 collaborateurs

Solutions MSP distribuées

KASEYA

RMM

RMM, sécurité, sauvegarde et gestion de parc en une seule plateforme unifiée pour MSP. Optimisez l'efficacité et automatisez vos workflows.

ATERA

RMM

Une solution SaaS tout-en-un, combinant RMM, ticketing/ PSA et IA autonome pour surveiller, gérer, automatiser et optimiser l'informatique.

KEEPER MSP

Gestionnaire de mot de passe

Keeper MSP est une plateforme de protection et gestion des mots de passe et données sensibles de vos clients dans des coffres-forts chiffrés et sécurisés.

ESET

MDR

Solutions de cybersécurité multicouches (postes, serveurs, messagerie). Console d'administration multi-tenant pour une gestion simple par les MSP.

ACRONIS

Sauvegarde

Une plateforme permettant aux MSP de proposer un service de sauvegarde et cybersécurité unifiée pour protéger, restaurer et sécuriser les données de leurs clients.

SOPHOS

MDR

Plateforme de sécurité intégrée (endpoint, pare-feu, MDR). protection automatisée, détection des menaces. Gestion multi-tenant simplifiée via Sophos Central.

Hermitage Solutions
(+33) 4 78 28 75 41
3 Rue de l'Arbre Sec
69001 Lyon
hermitagesolutions.com

Prenez rendez-vous pour découvrir notre catalogue

Infinigate France

Distributeur à valeur ajoutée spécialisé en cybersécurité, réseaux et cloud sécurisé. Infinigate France accompagne les revendeurs IT avec des solutions innovantes, des services techniques, des formations et un support expert pour développer leur activité et répondre aux enjeux de leurs clients.

3 000 partenaires IT partout en France

35 éditeurs

80 collaborateurs

Solutions MSP distribuées

Sécurité | Réseau AI
HPE JUNIPER NETWORKING

Hébergement et infrastructure

Solutions réseau et sécurité AI native pour connecter, protéger et optimiser les infrastructures du edge au cloud pour des réseaux fiables et automatisés.

Cyberdéfense souveraine
EUROPEAN DEFENSE PLATFORM

EDR / XDR

Infinigate présente la European Defense Platform XDR, avec HarfangLab et Sekoia, 100 % française, pour renforcer surveillance et réponse aux menaces.

Sécurité réseaux
WATCHGUARD

Firewall

Permet aux fournisseurs de services managés de sécuriser réseaux, terminaux et accès clients via firewalls et services intégrés, avec gestion centralisée efficace.

Sécurité des accès
YUBICO

IAM/PAM

Solution d'authentification forte basée sur des clés de sécurité matérielles pour protéger les accès, comptes et identités contre le phishing et les intrusions.

Sécurité réseaux
CHECK POINT

Sécurité de la messagerie

Offre complète de services cyber (prévention, SASE, Email, Endpoint, XDR) aux fournisseurs via une plateforme unifiée à gestion centralisée.

Gestion d'identité
OKTA

IAM/PAM

Plateforme de gestion des identités et des accès pour sécuriser les connexions, centraliser les droits et renforcer l'authentification des utilisateurs.

Infinigate France
(+33) 1 80 73 04 25
40 Avenue Pierre Lefaucheux
92100 Boulogne-Billancourt
www.infinigate.com

Prenez rendez-vous pour découvrir notre catalogue

Kappa Data

Kappa Data, spécialiste international de la distribution IT cybersécurité et réseaux, accompagne ses clients et revendeurs avec des solutions adaptées, un suivi personnalisé, des services de proximité et des formations certifiantes sur les dernières technologies.

1 800+ partenaires actifs à l'international

25 éditeurs

6 agences

100 collaborateurs

Solutions MSP distribuées

Plateforme SMC
STORMSHIELD

Firewall

Centralise la supervision, la gestion et la mise à jour de tous les équipements, tout en automatisant la sécurité, les opérations et la conformité.

Exposure Management
RUNZERO

Scan de vulnérabilité

Gestion de la surface d'attaque interne et externe, en offrant une visibilité complète des équipements IT, IoT & OT via scanners actifs/passifs et intégrations API.

EDR & EPP
WITHSECURE

EDR / XDR

Solution pour postes et serveurs, pensée pour MSP, alliant prévention, détection et réponse aux incidents avec gestion centralisée multi-clients.

CloudWAF
RADWARE

Firewall

Offre une protection infogérée complète pour sites web et API, avec CloudWAF, Anti-DDoS, gestion des bots et sécurité Web & support 24/7.

MSP Workspace
EXTREME NETWORKS

Hébergement et infrastructure

Plateforme Cloud pour MSP, permettant de déployer et gérer les reseaux filaires, Wi-Fi et VPN, avec contrôle d'identité, visibilité complète et gestion centralisée.

Email Protection
BARRACUDA NETWORKS

Sécurité de la messagerie

Sécurise les messageries en combinant prévention des menaces, filtrage, détection, protection des identités et sauvegarde des emails.

Kappa Data
(+33) 3 20 61 96 76
Kappa Data France
35 Rue Winston Churchill
59160 Lille
www.kappadata.fr

Prenez rendez-vous pour découvrir notre catalogue

MIEL

MIEL est distributeur à valeur ajoutée de nouvelles technologies IT. Pour aider les MSP à adopter les dernières solutions pour optimiser les coûts, développer le MRR, sécuriser les infras et différencier leurs services, nous proposons démos, essais gratuits, PoC, formation et support après-vente.

1 985
naissance, à Paris

60+ collaborateurs

800+ partenaires fidèles

570+ personnes formées par an

Solutions MSP distribuées

Cortex XSIAM
PALO ALTO NETWORKS

Firewall

SOC next gen piloté par l'IA, unifie les données, automatise détection et réponse pour réduire MTTD/MTTR et concentrer les analystes sur les attaques avancées.

Cyber defense
LOGPOINT

EDR / XDR

Plateforme européenne SIEM+SOAR+NDR, on-prem ou SaaS multi-tenant, offre un modèle flexible et une visibilité complète grâce à l'ingestion massive de logs.

IT Autopilot
ATERA

PSA

RMM, automatisation du support, accès à distance, automatisation de l'IT, et gestion des correctifs, scripts, tickets et rapports. Copilote et autopilote IA.

Remote Application Server
PARALLELS

Environnement de travail collaboratif

Gestion simplifiée des applis et des postes de travail virtuels. SPLA attractif et TCO réduit. Excellente expérience utilisateur. Evolutivité et admin simplifiées.

NodeZero
HORIZON3.AI

Scan de vulnérabilité

Permet de proposer des services de pentest permanent et autonome pour valider la posture de sécurité des clients à tout moment et appliquer les bons correctifs.

Threat Exposure Management
FLARE

Scan de vulnérabilité

Proposez de surveiller l'exposition de vos clients aux menaces. Scruter les fuites de leurs données sur le web, le dark web et les réseaux menaçants.

MIEL
(+33) 1 60 19 34 52
Parc Burospace 5
91570 Bièvres
www.miel.fr

Prenez rendez-vous pour découvrir notre catalogue

MIEL

Solutions MSP distribuées

365 Total Protection
HORNETSECURITY

Sécurité de la messagerie

Suite complète pour la sécurité, le risque, la gouvernance, la conformité et la sauvegarde de Microsoft 365, en commençant par la messagerie et la sensibilisation.

Hybrid Cloud
VIRTUOZZO

Hébergement et infrastructure

Alternative à VMware. Cloud MSP sans complexité : IaaS en libre-service, PaaS, orchestration Kubernetes et gestion de bases de données, administration simplifiée.

Stockage de backup
EXAGRID

Sauvegarde

Appliances pay-as-you-grow de stockage immuable du backup : restauration rapides, sécurité complète et récupération après ransomware, avec une fiabilité inégalée.

PAM
BEYONDTRUST

IAM/PAM

Proposez de gérer les comptes à privilège. Système facile à déployer, complet, flexible, évolutif et collaboratif, accessible en modèle sur site, cloud, ou hybride.

Cloud-To-Cloud Backup
OPENTEXT CYBERSECURITY

Sauvegarde

Sauvegarde et protection Cloud des données SaaS Microsoft 365, Google, Salesforce, Box, Dropbox. Redondance totale, récupération rapide et granulaire.

IGEL-OS
IGEL

Environnement de travail collaboratif

Déployez un O/S ultraléger sécurisé sur les endpoints en complément de VDI et de browser sécurisé. Administrez-les en central. Chainon manquant du digital workspace.

Segmentation
ILLUMIO

Firewall

Technologie de cartographie des workloads et de micro-segmentation conçue par Illumio, qui s'intègre parfaitement à n'importe quelle pile de sécurité.

Network Resilience
OPENGEAR

Outil de prise en main à distance

Visibilité, maintenance et récupération du réseau en toute circonstance grâce à une infra hors bande et l'accès à distance aux ports console. Admin centralisée.

MIEL
(+33) 1 60 19 34 52
Parc Burospace 5
91570 Bièvres
www.miel.fr

Prenez rendez-vous pour découvrir notre catalogue

NET POINT

Net Point est un distributeur de solutions de sécurité informatique & cloud . Fournisseur & agregateur nous centralisons et intégrons les meilleures offres du marché au travers d'un portail de commande unique «PROVICLOUD» pour nos partenaires.

250 VAR et MSP actifs

12 éditeurs et constructeurs

#1 CLOUD MARKETPLACE PROVICLOUD

Solutions MSP distribuées

CYBER PROTECT CLOUD
ACRONIS

Sauvegarde

Sauvegarde, reprise d'activité après sinistre, cybersécurité et gestion des terminaux intégrées en une solution unique pour les fournisseurs de services (MSP/MSSP).

SOC Managé
NUCLEON SECURITY

MDR

MDR souverain 24/7 par Nucleon Security : détection proactive et réponse automatisée aux menaces via IA Zero Trust, avec traitement local des données sensibles.

RMM & PSA
ATERA

RMM

Une solution puissante pour les MSP. Optimisez votre efficacité à grande échelle grâce à une solution tout-en-un pour gérer, patcher et sécuriser chaque appareil.

RMM & PSA
SUPEROPS

RMM

Votre plateforme PSA-RMM de proximitéSuperOps est une plateforme pensée pour les MSP qui souhaitent centraliser et moderniser la gestion des infrastructures IT.

BUSINESS MSP
LASTPASS

Gestionnaire de mot de passe

Simplifiez la gestion des mots de passe des clients, LastPass est une solution de gestion des identités et des accès conçue pour protéger les données sensibles.

FIREBOX
WATCHGUARD

Firewall

La sécurité sans complexité. Les appliances Firebox de WatchGuard sont le parfait équilibre entre performances, faible coût total d'acquisition (TCO) et simplicité.

NET POINT
(+33) 1 84 17 27 15
5 Rue du chant des oiseaux
78360 Montesson
www.netpoint.fr

Prenez rendez-vous pour découvrir notre catalogue

TD SYNNEX

TD SYNNEX, leader mondial de la distribution technologique accompagne plus de 150 000 clients dans 100 pays. Notre offre, la plus large du marché, couvre les technologies à forte croissance : cloud, IA ou cybersécurité. Notre rôle : connecter l'écosystème grâce à notre position centrale.

2 500 Vendors

200 000 produits et solutions

150 000 clients dans le monde

12 000 clients en France

Solutions MSP distribuées

Acronis
ACRONIS
Voir Acronis Email Security (p38)

Microsoft
MICROSOFT
Voir MICROSOFT Business Premium (p65)

Dell
DELL
Voir Dell PowerEdge XE9780/XE9785 (p108)

Object First
OBJECT FIRST
Voir Object First Ootbi (p119)

Lenovo
LENOVO
Voir LENOVO / NUTANIX HCI (p110)

Veeam
Veeam
Voir Veeam Cloud Service Provider (p115)

TD SYNNEX France
0 825 32 8000
5 Avenue de l'Europe
Bussy-Saint-Georges
77600 Marne la vallée Cedex 03
fr.tdsynnex.com

Prenez rendez-vous pour découvrir notre catalogue

Westcon-Comstor

Westcon-Comstor est un distributeur mondial expert de solutions technologiques dans trois domaines : la cybersécurité, le réseau et les infrastructures Cloud.
Nous apportons de la valeur et des opportunités commerciales à nos partenaires.

1 000 partenaires en France

15 éditeurs / constructeurs

70 collaborateurs en France

dont **1/3** Ingénieurs avant-ventes

Solutions MSP distribuées

Harmony™
CHECK POINT SOFTWARE

Sécurité de la messagerie

Une couverture complète des 4 vecteurs d'attaque dont la protection des emails et des outils collaboratifs (Harmony Email & Collaboration).

Extreme Platform ONE™
EXTREME NETWORKS

Hébergement et infrastructure

La première plateforme réseau tout-en-un intégrant une IA conversationnelle, multimodale & agentique unifiant ainsi le réseau, la sécurité & l'IA.

Secure MSP Center
CISCO

Environnement de travail collaboratif

Plateforme unifiée de gestion en mode SaaS des solutions Cisco pour protéger les utilisateurs intégrant au choix Authentification, DNS, Proxy, Passerelle Web et EDR.

MSSP Services
ZSCALER

Outil de prise en main à distance

ZIA : Passerelle de sécurité pour tout le trafic internet et les applications SaaS.
ZPA : Solution d'accès aux applications privées basée sur le principe du Zero Trust.

MSSP Program
CROWDSTRIKE

EDR / XDR

Solutions de cybersécurité qui surveillent en temps réel les terminaux pour détecter, analyser et répondre aux menaces avancées (deux options disponibles).

Westcon-Comstor
14 Rue Sarah Bernhardt
92600 Asnières-sur-Seine
www.westconcomstor.com

Prenez rendez-vous pour découvrir notre catalogue

Glossaire

Retrouvez dans ce glossaire les termes et acronymes présentés dans ce guide.

A

ATO (Account Takeover)
Prise de contrôle non autorisée d'un compte utilisateur par un attaquant. Ce type d'attaque exploite souvent des identifiants volés ou compromis pour accéder aux systèmes et données d'une organisation.

B

BaaS (Backup as a Service)
Service de sauvegarde hébergé dans le cloud, facturé à l'usage. Le fournisseur gère l'infrastructure, la sécurité et la maintenance, tandis que le MSP se concentre sur la définition des politiques de sauvegarde pour ses clients.

BEC (Business Email Compromise)
Attaque ciblée par email visant à tromper une organisation pour obtenir des virements frauduleux ou des informations sensibles. L'attaquant se fait passer pour un dirigeant ou un partenaire de confiance.

C

CAPEX (Capital Expenditure)
Dépenses d'investissement en capital pour l'acquisition d'actifs matériels ou logiciels. Contrairement à l'OPEX, le CAPEX implique un paiement initial important pour un bien qui sera amorti sur plusieurs années.

Console multi-tenant
Interface de gestion centralisée permettant à un MSP d'administrer les environnements de plusieurs clients depuis un seul point d'accès. Chaque client reste isolé des autres, avec ses propres configurations et données.

D

DLP (Data Loss Prevention)
Ensemble de technologies et processus visant à empêcher la fuite de données sensibles hors de l'organisation. Le DLP surveille, détecte et bloque les transferts non autorisés d'informations confidentielles.

DRaaS (Disaster Recovery as a Service)
Service de reprise d'activité après sinistre hébergé dans le cloud. En cas d'incident majeur, le DRaaS permet de basculer rapidement les systèmes critiques vers une infrastructure de secours pour maintenir la continuité des opérations.

E

EDR (Endpoint Detection and Response)
Solution de cybersécurité assurant la détection et la réponse aux menaces sur les postes de travail et serveurs. L'EDR surveille en continu les endpoints, identifie les comportements suspects et permet d'isoler ou de neutraliser les menaces.

G

Graph API
API de Microsoft permettant d'accéder aux données et services de Microsoft 365, Azure AD et d'autres produits Microsoft. Cette API standardisée facilite l'intégration et l'automatisation des tâches d'administration.

H

HDS (Hébergement de Données de Santé)
Certification française obligatoire pour héberger des données de santé à caractère personnel. Elle garantit un niveau de sécurité et de confidentialité conforme aux exigences du secteur médical.

Hébergement souverain
Hébergement des données sur le territoire national ou européen, soumis à la législation locale. Cette approche répond aux exigences de souveraineté numérique et de conformité RGPD en gardant le contrôle des données.

I

IAM (Identity and Access Management)
Ensemble de processus et technologies gérant les identités numériques et leurs droits d'accès aux ressources informatiques. L'IAM contrôle qui peut accéder à quoi, quand et dans quelles conditions.

IaaS (Infrastructure as a Service)
Modèle cloud fournissant des ressources informatiques virtualisées (serveurs, stockage, réseau) à la demande. Le MSP garde le contrôle sur les systèmes d'exploitation et applications, tandis que le fournisseur gère l'infrastructure physique.

Immuabilité / Stockage immuable
Caractéristique d'une donnée qui ne peut être modifiée ou supprimée pendant une période définie. En matière de sauvegarde, l'immuabilité protège contre les ransomwares et les suppressions accidentelles en garantissant l'intégrité des copies.

IOC (Indicator of Compromise)
Élément technique indiquant une potentielle intrusion ou compromission d'un système. Les IOC incluent des adresses IP suspectes, des hashs de fichiers malveillants ou des comportements anormaux utilisés pour détecter les menaces.

L

LotL (Living off the Land)
Technique d'attaque utilisant les outils légitimes présents dans le système cible (PowerShell, WMI) plutôt que des malwares. Cette approche permet aux attaquants de passer inaperçus en se fondant dans l'activité normale.

M

MDR (Managed Detection and Response)
Service géré combinant technologies de détection et expertise humaine pour surveiller, analyser et répondre aux menaces 24/7. Le SOC externe traite les alertes, enquête sur les incidents et applique les mesures de remédiation.

MDF (Market Development Funds)
Fonds marketing alloués par un éditeur ou distributeur à ses partenaires pour développer le marché. Ces budgets soutiennent des actions commerciales, formations ou événements promouvant les solutions du fournisseur.

MITRE ATT&CK
Base de connaissances des tactiques et techniques utilisées par les cyberattaquants, maintenue par l'organisation MITRE. Ce référentiel aide les équipes de sécurité à comprendre les menaces, tester leurs défenses et prioriser leurs investissements.

MRR (Monthly Recurring Revenue)
Revenu mensuel récurrent généré par les abonnements et contrats de service. Cet indicateur clé mesure la santé financière d'un MSP et sa capacité à générer des revenus prévisibles et pérennes.

MSP (Managed Service Provider)
Prestataire informatique gérant et supervisant à distance l'infrastructure IT de ses clients, sur la base d'abonnements récurrents. Le MSP assure la maintenance, la sécurité, les sauvegardes et le support des environnements informatiques.

MSSP (Managed Security Service Provider)
Prestataire spécialisé dans la gestion externalisée de la sécurité informatique. Le MSSP offre des services comme la surveillance SOC, le MDR, la gestion de firewalls et la réponse aux incidents de sécurité.

MTTR (Mean Time To Respond)
Temps moyen nécessaire pour répondre à un incident de sécurité, depuis la détection jusqu'à la neutralisation de la menace. Un MTTR faible indique une capacité de réaction rapide face aux cyberattaques.

MTTD (Mean Time To Detect)
Temps moyen nécessaire pour détecter une intrusion ou une menace dans le système. Réduire le MTTD permet de limiter les dégâts causés par une attaque en intervenant plus rapidement.

N

NDR (Network Detection and Response)
Solution détectant les menaces au niveau du cœur de réseau en analysant le trafic en temps réel. Le NDR identifie les comportements anormaux, les mouvements latéraux et les tentatives d'exfiltration de données.

NFR (Not For Resale)
Licences gratuites ou à tarif réduit fournies aux partenaires MSP pour tester, démontrer ou utiliser en interne une solution. Les NFR ne peuvent être revendues aux clients finaux et servent à la formation ou la démonstration.

O

OPEX (Operational Expenditure)
Dépenses opérationnelles récurrentes liées au fonctionnement quotidien de l'activité. Dans le cloud et les services managés, l'OPEX remplace le CAPEX en transformant les investissements lourds en abonnements mensuels.

P

PAM (Privileged Access Management)
Solution gérant et sécurisant les accès à privilèges élevés (administrateurs, comptes système). Le PAM contrôle, surveille et enregistre l'utilisation des comptes privilégiés pour prévenir les abus et détecter les compromissions.

PRA (Plan de Reprise d'Activité)
Ensemble de procédures permettant de restaurer les activités critiques après un sinistre majeur. Le PRA définit les priorités de reprise, les ressources nécessaires et les délais cibles (RTO, RPO).

PSA (Professional Services Automation)
Logiciel centralisant la gestion des services professionnels d'un MSP : ticketing, gestion de projets, facturation, contrats et reporting. Le PSA améliore l'efficacité opérationnelle et la visibilité sur l'activité.

R

Ransomware Rollback
Fonctionnalité permettant de restaurer un système dans son état antérieur à une attaque par ransomware, en annulant les modifications malveillantes. Cette capacité limite considérablement l'impact d'un chiffrement par ransomware.

RMM (Remote Monitoring and Management)
Plateforme permettant à un MSP de superviser et gérer à distance les infrastructures de ses clients. Le RMM centralise la surveillance, l'automatisation, le déploiement de correctifs et l'administration des systèmes.

RPO (Recovery Point Objective)
Durée maximale acceptable de perte de données lors d'un incident. Un RPO de 4 heures signifie que l'organisation peut tolérer la perte des données des 4 dernières heures en cas de sinistre.

RTO (Recovery Time Objective)
Durée maximale acceptable d'interruption d'un service ou système après un incident. Le RTO détermine la rapidité avec laquelle les opérations doivent être restaurées pour limiter l'impact sur l'activité.

S

S3 (Simple Storage Service)
Standard de stockage objet popularisé par Amazon Web Services, devenu une référence pour le stockage cloud. De nombreuses solutions de sauvegarde utilisent le protocole S3 ou des alternatives compatibles S3.

SASE (Secure Access Service Edge)
Architecture réseau combinant les fonctions SD-WAN et la sécurité cloud (firewall, ZTNA, filtrage web) dans un service unifié. SASE sécurise les accès des utilisateurs distants aux applications, quel que soit leur emplacement.

SIEM (Security Information and Event Management)
Plateforme collectant, corrélant et analysant les événements de sécurité de multiples sources pour détecter les menaces. Le SIEM agrège les logs et génère des alertes sur les activités suspectes.

SLA (Service Level Agreement)
Contrat définissant les engagements de service entre un prestataire et son client, incluant les niveaux de performance, disponibilité et temps de réponse. Les SLA établissent les pénalités en cas de non-respect des engagements.

SOAR (Security Orchestration, Automation and Response)
Plateforme automatisant les réponses aux incidents de sécurité en orchestrant différents outils et processus. Le SOAR accélère le traitement des alertes en exécutant automatiquement des actions de remédiation prédéfinies.

SOC (Security Operations Center)
Centre opérationnel dédié à la surveillance et à la réponse aux incidents de sécurité. Le SOC analyse les alertes 24/7, enquête sur les menaces et coordonne les actions de défense et de remédiation.

SOC 2 (Service Organization Control 2)
Norme d'audit américaine évaluant les contrôles de sécurité, disponibilité, intégrité et confidentialité d'un fournisseur de services. La certification SOC 2 Type II atteste de l'efficacité de ces contrôles sur une période donnée.

SPLA (Services Provider License Agreement)
Programme de licences Microsoft permettant aux prestataires de services d'héberger des logiciels Microsoft pour leurs clients avec une facturation à l'usage. Le SPLA convient aux modèles d'hébergement mutualisé et de cloud privé.

T

TAM (Technical Account Manager)
Responsable de compte technique dédié assurant le lien entre le fournisseur et le partenaire MSP. Le TAM apporte son expertise technique, accompagne les déploiements et facilite la résolution des problèmes complexes.

TCO (Total Cost of Ownership)
Coût total de possession d'une solution incluant l'acquisition, le déploiement, l'exploitation, la maintenance et le retrait. Le TCO permet de comparer objectivement différentes options en considérant tous les coûts sur le cycle de vie.

V

Vulnerability Management / Gestion des vulnérabilités
Processus continu d'identification, d'évaluation, de priorisation et de correction des failles de sécurité dans les systèmes. Une gestion efficace des vulnérabilités réduit la surface d'attaque en comblant les brèches exploitables.

W

White Label / Marque blanche
Possibilité de personnaliser une solution avec sa propre marque et identité visuelle. Le white label permet aux MSP de proposer des services sous leur marque sans révéler les technologies sous-jacentes.

WORM (Write Once Read Many)
Technologie de stockage empêchant la modification ou la suppression des données après leur écriture. Le WORM garantit l'immuabilité des sauvegardes et leur conformité avec certaines réglementations d'archivage.

X

XDR (Extended Detection and Response)
Évolution de l'EDR intégrant la détection et la réponse sur plusieurs couches (endpoints, réseau, cloud, email). Le XDR corrèle les événements de sécurité de sources multiples pour une vision unifiée des menaces.

Z

Zero Trust / Confiance zéro
Modèle de sécurité ne faisant confiance par défaut à aucun utilisateur ou dispositif, même interne au réseau. Le Zero Trust vérifie systématiquement l'identité et le contexte avant d'autoriser chaque accès aux ressources.

ZTNA (Zero Trust Network Access)
Solution d'accès réseau basée sur les principes du Zero Trust, remplaçant les VPN traditionnels. ZTNA accorde des accès granulaires aux applications spécifiques selon l'identité et le contexte, sans exposer l'ensemble du réseau.

Liste des événements IT

Mars 2026

4 mars **Martinique**

Roadshow GoMSP

Roadshow dédié aux MSP permettant de rencontrer les éditeurs de l'écosystème Watsoft, de découvrir des solutions pour les services managés (cybersécurité, RMM, PSA, sauvegarde, cloud) et d'échanger entre pairs dans un format de proximité.

https://www.watsoft.com/watsoft-roadshow-solutions-it-msp/

6 mars **Guadeloupe**

Roadshow GoMSP

Deuxième étape du roadshow GoMSP réunissant prestataires IT et partenaires technologiques autour des enjeux opérationnels des MSP : automatisation, sécurisation des environnements clients et développement des services managés.

https://www.watsoft.com/watsoft-roadshow-solutions-it-msp/

9 au 11 mars **Londres**

IT Nation Connect Europe

Événement communautaire européen dédié aux MSP, IT Nation Connect Europe propose trois jours de conférences, d'ateliers et de sessions de networking centrés sur la croissance, la rentabilité et l'industrialisation du modèle de services managés. Le programme combine retours d'expérience, bonnes pratiques opérationnelles et rencontres avec l'écosystème d'éditeurs et de partenaires.

https://itnation.connectwise.com/connect-europe

17 mars **Le Mans**

Cybertalk

Cybertalk est une conférence qui regroupe le temps d'une matinée, professionnels de l'IT et éditeurs internationaux autour de tables rondes et de démonstations techniques. Un format intéressant pour vous permettre de faire de la veille technologique tout en élargissant votre réseau.

https://www.cybertalk.fr

31 mars au 2 avril **Lille**

Forum InCyber Europe (FIC)

Événement européen de référence qui rassemble l'ensemble de l'écosystème cybersécurité : offreurs de solutions, institutions, grands comptes et prestataires autour de conférences, d'un espace d'exposition et de temps de networking. Idéal pour les MSP qui souhaitent suivre les tendances du marché, identifier de nouveaux partenaires et affiner leur positionnement dans l'écosystème cyber.

https://www.forum-fic.com/

Avril 2026

8 au 9 avril **Paris**

Salon IA.Cloud

Forum orienté solutions réunissant exposants, démonstrations et conférences autour des enjeux cybersécurité, cloud et intelligence artificielle, avec une approche tournée vers les décideurs.
Pertinent pour comparer rapidement les offres du marché, identifier de nouveaux outils SecOps, IAM ou cloud security et enrichir son catalogue de services.

https://www.salon-cloud-security.com/

30 avril **Nantes**

Roadshow GoMSP

Rencontre régionale entre MSP et éditeurs avec démonstrations de solutions, retours d'expérience et échanges sur l'industrialisation des services managés et la rentabilité du modèle MSP.

https://www.watsoft.com/watsoft-roadshow-solutions-it-msp/

Mai 2026

5 au 6 mai **Toulouse**

Toulouse Hacking Convention (THCon)

Conférence cybersécurité (avec CTF associé) axée sur des contenus techniques avancés, réunissant chercheurs, pentesters, RSSI et équipes sécurité autour de retours d'expérience et de démonstrations concrètes.
Up-skilling technique : intéressant si vous maintenez un haut niveau d'expertise (pentest, audit, détection) ou si vous souhaitez renforcer les compétences sécurité de vos équipes.

https://thcon.party/

17 au 19 mai **Orlando**

MSPGeekCon 2026

Événement communautaire international dédié aux professionnels des services managés, MSPGeekCon propose trois jours de sessions techniques, de retours d'expérience et d'échanges entre pairs autour des enjeux opérationnels des MSP : cybersécurité, automatisation, outils de la stack et nouvelles tendances comme l'intelligence artificielle. L'événement met l'accent sur le partage de connaissances, la montée en compétence et la collaboration au sein de la communauté.

https://mspgeekcon.com/

20 au 21 mai **Bruxelles**

Cybersec Europe

Salon autour de la cybersécurité sur deux jours organisé à Brussels Expo, combinant exposition de solutions, conférences et rencontres entre offreurs et décideurs IT/cyber européens.
Utile pour les MSP adressant la Belgique ou le Benelux : développement de partenariats, veille marché européenne et identification de nouvelles solutions à intégrer au catalogue.

https://www.cyberseceurope.com/

Juin 2026

2 au 4 juin **Monaco**

Ready For IT

Convention d'affaires dédiée à la transformation digitale et aux infrastructures IT, reposant sur un format de rendez-vous one-to-one entre décideurs et offreurs de solutions, complété par des conférences et des retours d'expérience.
Un format très orienté business pour rencontrer des décideurs sur des projets identifiés, accélérer le cycle de vente et positionner des offres d'infogérance, cloud ou cybersécurité.

https://www.ready-for-it.com/

2 au 4 juin **Londres**

Infosecurity Europe

L'un des principaux salons européens dédiés à la cybersécurité, avec un large espace d'exposition, des démonstrations de solutions et un programme de conférences couvrant l'ensemble des domaines de la sécurité des systèmes d'information.
Un rendez-vous clé pour identifier de nouveaux éditeurs européens, comparer les plateformes du marché et enrichir son catalogue de services managés.
https://www.infosecurityeurope.com/

4 juin **Rouen, Hôtel Mercure Centre Champ de Mars**

Cybertalk

Au cœur de la Normandie, l'événement Cybertalk Rouen réunira les professionnels de l'IT pour une matinée d'échanges sur les enjeux concrets de la cybersécurité en entreprise, avec des retours d'expérience et des rencontres entre acteurs locaux.
Format très adapté pour développer la visibilité régionale, rencontrer des prospects PME/ETI et activer des opportunités commerciales locales.
https://www.cybertalk.fr/

3 au 5 juin **Rennes**

SSTIC

Symposium technique de référence en France, centré sur la recherche en sécurité informatique, l'analyse de vulnérabilités, la cryptographie et les méthodes avancées de défense.
Forte valeur pour les équipes MSP : montée en compétence, crédibilité expertise et amélioration des capacités d'audit, de détection et de réponse à incident.
https://www.sstic.org/

11 juin **Niort, Hôtel Mercure**

Cybertalk

Cybertalk Niort rassemblera l'écosystème des décideurs IT régionaux autour de cas concrets de cybersécurité et de retours d'expériences.
Intéressant pour adresser des secteurs structurés (assurance, services) avec des offres packagées autour de la cybersécurité et l'infogérance.
https://www.cybertalk.fr/

11 juin **Lyon**

Roadshow GoMSP

Journée d'échanges dédiée aux prestataires IT autour des outils et des bonnes pratiques pour optimiser la gestion des infrastructures, renforcer la cybersécurité et automatiser les services.
https://www.watsoft.com/watsoft-roadshow-solutions-it-msp/

16 au 18 juin **Prague**

Kaseya Connect Europe

Événement européen majeur dédié aux MSP et aux professionnels de l'IT, Kaseya Connect Europe rassemble plus de 1 500 participants autour de trois axes : formation technique, stratégie business et networking.
Le programme combine sessions de formation, ateliers pratiques, démonstrations produits et rencontres avec l'écosystème de partenaires et d'éditeurs. L'objectif est d'aider les prestataires à optimiser leurs opérations, développer de nouvelles offres et améliorer leur rentabilité.
https://www.kaseyaconnect.com/europe/

Septembre 2026

9 au 11 septembre **Calgary (Telus Convention Centre - Canada)**

CanITCon 2026

Événement technologique dédié aux MSP canadiens, CanITCon réunit la communauté MSP autour de conférences orientées business. Un événement pour partager des retours d'expérience concrets et des sessions de networking entre pairs et partenaires.
Le programme met l'accent sur les échanges sans contenu marketing, le partage de bonnes pratiques et l'identification d'opportunités de croissance pour les prestataires de services managés.
https://thecanitcollective.ca/canitcon/

16 au 17 septembre **Lyon**

SIDO Lyon

Événement consacré aux technologies IoT, IA, robotique et XR, avec une forte orientation sur les cas d'usage industriels et les projets de transformation. Pertinent pour les MSP positionnés sur l'industrie, les environnements connectés et les projets d'infrastructures IoT.
https://www.sido-lyon.com/

16 au 17 septembre **Lyon**

Lyon Cyber Expo

Salon régional dédié à la cybersécurité en parallèle du SIDO. Ce salon réunit offreurs de solutions et entreprises autour de conférences et de retours d'expérience.
Un bon levier pour générer des leads locaux et développer sa visibilité auprès des PME et ETI régionales.
https://www.lyoncyberexpo.com/

17 septembre **Paris**

Roadshow GoMSP

Étape francilienne réunissant l'écosystème MSP autour des tendances du marché, des nouvelles solutions et des stratégies de développement des services managés.
https://www.watsoft.com/watsoft-roadshow-solutions-it-msp/

Octobre 2026

7 au 10 octobre **Monaco**

Les Assises de la cybersécurité

Rendez-vous majeur de l'écosystème cyber, basé sur des rencontres one-to-one entre décideurs et offreurs de solutions, complétées par un programme de conférences stratégique.
Un incontournable pour le positionnement marché, la signature de partenariats et l'accès à des projets grands comptes.
https://www.lesassisesdelacybersecurite.com/

14 au 15 octobre **Paris**

Mobility for Business

Événement consacré aux environnements de travail mobiles et aux outils numériques, incluant les sujets de sécurisation des accès et des terminaux. Pertinent pour les offres MDM/UEM, le poste de travail sécurisé et la gestion des accès à distance.

https://www.mobility-for-business.com/

16 au 17 octobre **Paris**

Hexacon 2026

Conférence orientée sécurité offensive et red team, avec des contenus techniques avancés et des démonstrations. Utile pour les équipes techniques qui souhaitent monter en compétence sur les approches offensives et renforcer les prestations d'audit.

https://www.hexacon.fr/

Octobre 2026

21 au 22 octobre **Barcelone**

MSP GLOBAL

Événement international entièrement dédié au modèle MSP : stratégie, industrialisation des services, outils et alliances.

Un rendez-vous prioritaire pour faire évoluer son business model, structurer ses offres managées et développer des partenariats à l'échelle européenne.

https://www.mspglobal.com/

27 au 29 octobre **Nuremberg**

it-sa Expo&Congress

Grand salon européen dédié à la cybersécurité, avec une forte présence d'éditeurs et de solutions pour le marché professionnel. Intéressant pour identifier de nouveaux vendeurs européens et comparer les solutions à intégrer au catalogue.

https://www.itsa365.de/

Novembre 2026

16 au 19 novembre **Rennes**

European Cyber Week

Forum européen consacré à la cyberdéfense, à l'IA et aux enjeux de sécurité pour les secteurs publics et stratégiques. Pertinent pour les MSP travaillant avec le secteur public, la défense ou les environnements critiques.

https://www.european-cyber-week.eu/

18 novembre **La Réunion**

Roadshow GoMSP

Rencontre dédiée aux MSP de l'océan Indien pour découvrir les solutions clés du modèle managé, échanger avec les éditeurs et partager des retours d'expérience terrain.

https://www.watsoft.com/watsoft-roadshow-solutions-it-msp/

18 au 19 novembre **Paris**

Cloud & Cyber Security Expo Paris

Salon consacré aux solutions de sécurisation des environnements cloud : protection des données, gestion des identités et des accès, SecOps. Intégré au Tech Show Paris, il permet de croiser facilement les approches cloud, data et IA avec les enjeux cybersécurité.

Un rendez-vous clé pour structurer des offres de cloud sécurisé, comparer les plateformes du marché et identifier des outils directement intégrables dans des services managés.

https://www.techshowparis.fr/cloud-cyber-security-expo

25 et 26 novembre **Toulouse**

CBC

Convention professionnelle dédiée à la cybersécurité, réunissant fournisseurs de solutions, experts et décideurs autour de conférences, démonstrations et temps de networking orientés retours d'expérience et projets concrets.

Idéal pour renforcer sa présence dans le Sud-Ouest, développer des relations locales et générer des opportunités commerciales auprès des entreprises du territoire.

https://cbc-convention.com/

Décembre 2026

1 au 3 décembre **Ottawa-Gatineau**

Forum InCyber Canada

Déclinaison nord-américaine du Forum InCyber, l'événement réunit acteurs publics, grandes organisations, startups et offreurs de solutions autour des enjeux de souveraineté numérique, de protection des infrastructures et de coopération internationale en matière de cybersécurité.

Idéal pour appréhender le marché nord-américain, nouer des alliances technologiques et identifier des opportunités de collaboration transatlantiques.

https://northamerica.forum-incyber.com/

Janvier 2027

27 au 28 janvier **Paris**

Cyber Show Paris

Salon dédié aux décideurs cybersécurité, avec un espace d'exposition et un programme de conférences axés sur la protection des données, la résilience des organisations et les solutions opérationnelles du marché.

Idéal pour identifier rapidement des solutions cyber intégrables à vos offres managées, rencontrer des partenaires et capter de nouvelles opportunités commerciales.

https://www.cybershowparis.fr/

Février 2027

3 au 4 février 2027 **Paris La Défense**

IT Partners

Rendez-vous annuel du channel IT en France, réunissant MSP, éditeurs, constructeurs et grossistes autour du développement commercial, des nouveautés solutions et des rencontres partenaires. L'événement permet d'avoir une vision concrète des tendances du marché et de préparer sa stratégie pour l'année à venir.

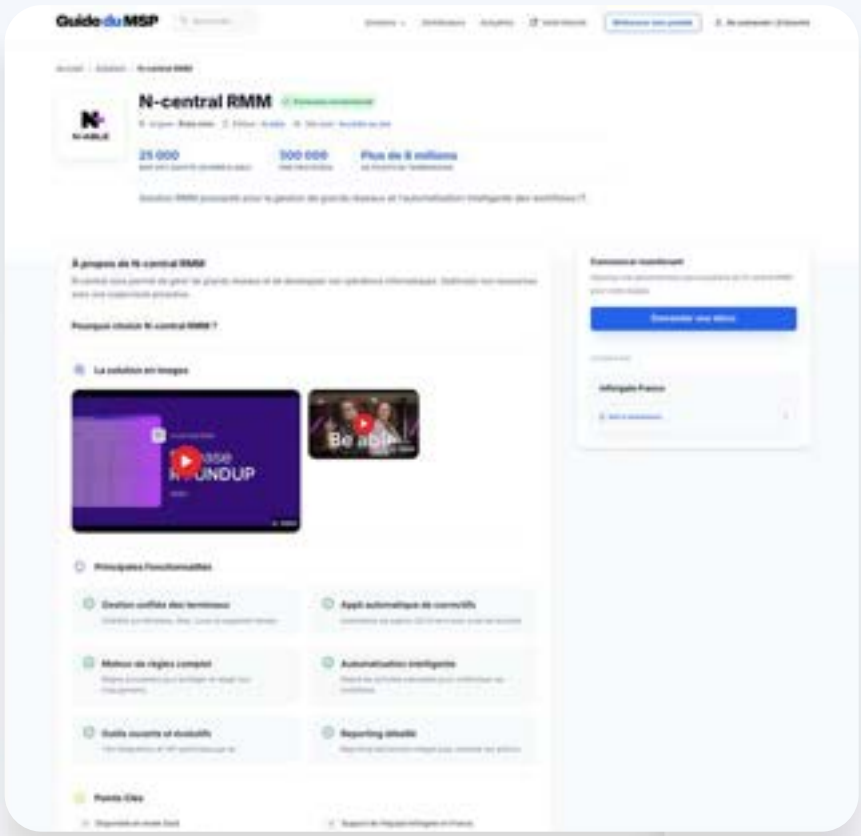
https://www.itpartners.fr/

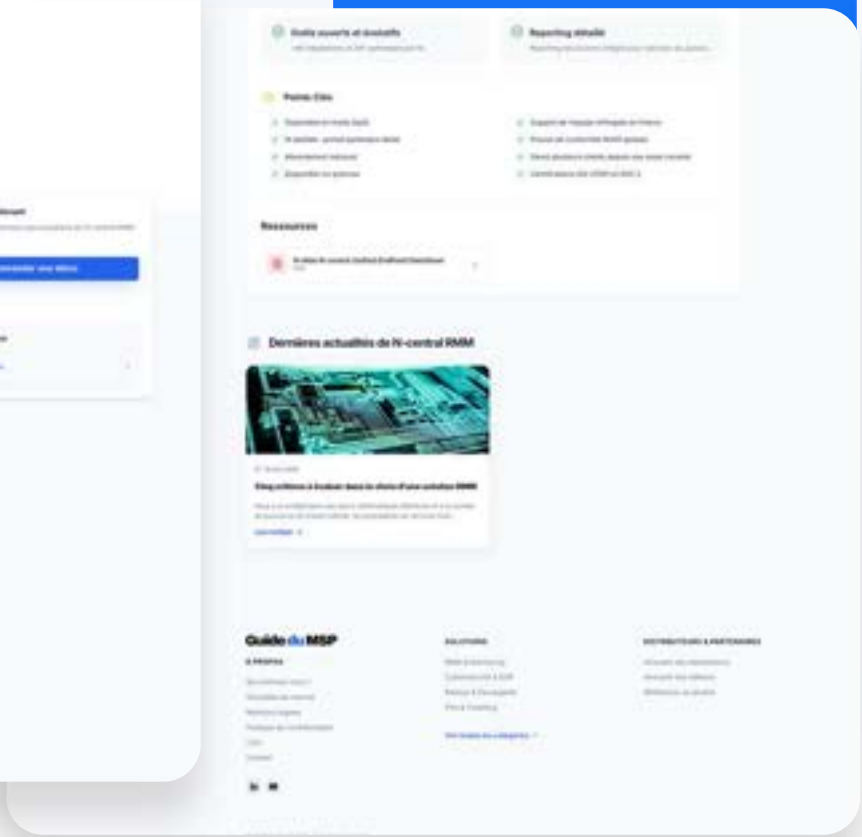
Guide du MSP

Retrouvez-nous sur les réseaux :

Continuez l'expérience du Guide du MSP sur notre site internet et rejoignez une communauté francophone de professionnels de l'IT.

https://www.guide-du-msp.com





Découvrez des centaines de solutions référencées à travers 23 catégories.

Accédez à des vidéos et fiches techniques pour comprendre leur fonctionnement.

Recevez chaque mois une newsletter pour ne rien rater des dernières tendances et des évolutions produits.

Faites une **demande de démonstration en un clic.**

Accédez à des deals exclusifs.

Découvrez des **éditeurs et distributeurs de solutions MSP et MSSP.**

Téléchargez le guide en version PDF
www.guide-du-msp.com/guide2026