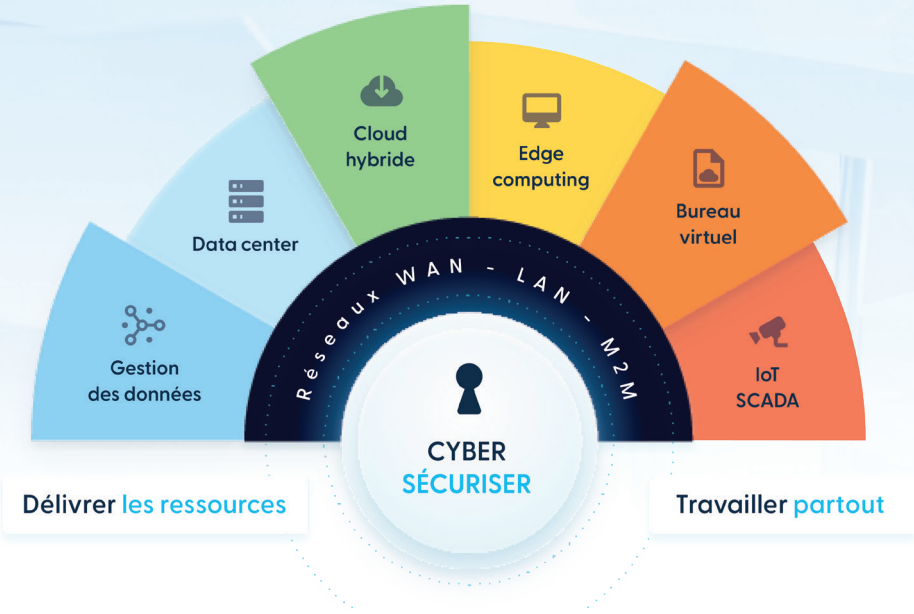
Nos réponses technologiques

pour l'IT d'entreprise
d'aujourd'hui et de demain



Nos partenaires

Vers la transformation digitale des entreprises

Miel a été créée en 1985 dans le but de proposer aux entreprises les technologies qui modernisent leur informatique. Depuis, Miel découvre et introduit sur le marché français les technologies innovantes à l'attention des services informatiques des entreprises. Souvent issus du marché le plus innovant, les États-Unis, les fournisseurs choisis proposent des avancées spectaculaires dans la manière d'assurer la productivité et la sécurité de l'informatique.

Le métier de Miel est de diffuser ces innovations en France par le biais d'un réseau de partenaires revendeurs et intégrateurs dûment qualifiés. La plupart du temps seul représentant de l'éditeur en France, Miel assure la promotion marketing et commerciale des produits, forme les personnels techniques des partenaires et des clients et constitue le centre de support technique avant- et après-vente indispensable à ce niveau de technicité.

Notre équipe a ainsi lancé en France les solutions de mémoire flash (SanDisk), de connectivité (Digi), d'accès sécurisé (Citrix), de qualité de service WAN (Packeteer), de réseaux sans fils (Cisco Aironet), de terminaux Windows (Neoware), autant de technologies qui sont maintenant monnaie courante.

Avec un effectif de 55 personnes (ingénieurs technico-commerciaux pour une grande majorité), Miel privilégie la proximité vis-à-vis de ses partenaires à valeur ajoutée, la forte compétence technique de ses équipes avant- et après-vente et l'efficacité de sa logistique d'importation.

Basée à Bièvres (91) près de Paris, ses équipes sont à la disposition des revendeurs partenaires pour des interventions conjointes partout en France.

Ligne Directe 01 60 19 34 52

Nos solutions

Digital Workplace

Espaces de travail numériques, applications et données. Cloud public, privé ou hybride. Accès universel et sécurisé.

Monitoring temps réel des environnements Citrix, VMware et Microsoft RDS

Simplification et optimisation des impressions quel que soit l'environnement.

Impression sécurisée à la demande grâce au follow-me-printing.

Centralisation de dongles USB dans le data center virtualisé.

O/S léger pour endpoint VDI/DaaS qui transforme tout poste x86-64 en terminal d'accès aux espaces de travail portés dans le Cloud (VDI, DaaS). Administration centralisée

Data centers dernier cri

Virtualisation, sécurisation et optimisation du stockage. PCA. PRA. Hyperconvergence.

Sauvegarde hautement disponible dans le Cloud et sur site des machines, physiques ou virtuelles, et des postes de travail.

Commutation réseau Cloud haute performance pour le data center. TAP aggregation. Pilotage du réseau par logiciel.

Accès réseau haute performance et sécurisé aux applications. Load balancing et Application Delivery Controller (ADC)

Ligne Directe 01 60 19 34 52

Cybersécurité

Plateforme de cybersécurité complète en continu, ouverte et basée sur l'I.A. Next-gen Firewall. Intelligence partagée dans le Cloud. Protection Zero-day des endpoints.

Solution de SIEM unifiée nouvelle génération. Collecte de logs, analyse et supervision complète. Visibilité en temps réel.

Visibilité et contrôle automatisé de tous les accès au LAN. Orchestration des systèmes de sécurité. NAC.

Accès et prise en main à distance ultra sécurisés. Stockage et sécurisation des identifiants pour les utilisateurs privilégiés.

Protection de la messagerie : anti-malware, anti-phishing et anti-spear-phishing, antispam et gestion des graymails. Sécurité intégrée 0365.

Analytics, VPN SSL, filtrage d'accès, single-sign-on, gestion des appareils mobiles (MDM/EMM).

Gestion des vulnérabilités, évaluation des risques, analytique et automatisation pour la sécurité, l'opérationnel et le développement IT

Evaluer les risques ou la réputation, profiler les attaquants, guider les investigations, et cartographier la cyber activité malveillante.

Micro-segmentation pour empêcher les mouvements latéraux et appliquer les stratégies Zero-Trust.

Veille cyber quotidienne sous la forme d'un service personnalisé. Avec bulletins aux équipes techniques et aux managers de SOC.

Cybervalidation automatique
Valider la sécurité en comblant et en révélant automatiquement de manière continue les brèches réellement exploitables.

Réseaux du Cloud computing

Extreme™ Customer-Driven Networking

Réseau distribué intelligent piloté dans le Cloud et automatisé SD-LAN avec points Wi-Fi, switches, routeurs.

peplink

Augmentation et sécurisation des liens Internet, WAN et 3G/4G. Load Balancing et aggrégation.

citrix™

SD-WAN : un réseau résilient capable de supporter le trafic applicatif d'aujourd'hui.

DIGI™

M2M. Connexion de tout équipement au réseau. Modules programmables pour l'OEM et l'embarqué.

opengear A DIGI COMPANY

Résilience du réseau
Console servers orchestrés en central. Automatisation NetOps. Continuité de service des systèmes.

Sommaire

Sommaire

Software Defined Cloud Networking

Arista Networks est le leader du "Software Defined Cloud Networking" (SDCN), qui représente le nouveau standard des data centers et des environnements réseaux haute performance. Au cœur des solutions réseaux d'Arista se trouve le système d'exploitation EOS (Extensible Operating System). Cette plateforme logicielle unique, entièrement ouverte est conçue pour évoluer indéfiniment en fonctionnalités. La plateforme Cloudvision permet de commander EOS à l'échelle globale du réseau et d'intéropérer avec des solutions applicatives ou d'orchestration par une interface graphique de pilotage et de programmation. Arista propose ainsi des plateformes de commutation avec les meilleurs résultats en termes de performances, densité, encombrement et consommation du marché des switches de data center.

Gamme

- **7500R** : châssis modulaire de 150Tbps, haute densité 10/25/40/50/100GbE.
- Jusqu'à 432 ports 100GbE non bloquant
- **7300X** : châssis modulaire haute performance 10/40GbE. Haute densité
- 10/25/40/50/100GbE. Jusqu'à 256 ports 100GbE non bloquant
- **7280** : Premier switch Top of Rack 100GbE, jusqu'à 224 ports 1/10GbE ou 6 ports 100GbE
- **7250X** : jusqu'à 64 ports QSFP+ 40 Gbps
- 7150S : switch 24/52/64 ports SFP+ à latence ultra faible
- **7060** : 10/25/40/50/100 Gbps. Jusqu'à 64 ports 100Gbps
- **7050** : switch jusqu'à 64 ports cuivre ou SFP+ 10GbE, non bloquant
- **7010** et **7048** : switch de data center 48 ports GbE avec 4 ports 10GbE SFP+

Technologies

- Cloud Networking
- Software Defined Data Center
- Extensible Operating System (EOS)
- Multi châssis Link Aggregation
- VM Tracer : visibilité sur les VMs
- Tap Aggregation : réseau de monitoring
- Analyse réseau : DANZ, LANZ

Besoins clients

- Datacenter 10/40/100GbE
- Virtualisation, stockage et convergence LAN
- Réseaux Cloud évolutifs
- Latence minimale et densité maximale
- Calculs haute performance
- SDN, orchestration, intégration des réseaux virtuels

Arguments de vente

- O/S modulaire permettant une mise à jour et une administration complète à chaud
- O/S ouvert. Accès aux outils Linux. Intégration d'outils tiers
- Intégration aux solutions d'orchestration, de SDN et de services L4-L7 (Load
- Balancing, Sécurité)
- Plus haute densité 10/40/100GbE du marché
- Analyse très précise des données du réseau grâce à l'agrégation de ports TAP
- Châssis modulaire le plus dense, le moins consommateur et le moins cher du marché
- Meilleur rapport prix/performance du marché
- Architecture non bloquante
- Latence ultra faible

Ligne Directe 01 60 19 02 30

Visibilité et contrôle sur tous les comptes et utilisateurs à privilèges

BeyondTrust offre la plateforme PAM la plus flexible du marché et permet aux entreprises de gérer et d'adapter la définition de la sécurité et des privilèges à mesure que les menaces évoluent et impactent les endpoints, serveurs, objets connectés (IoT), environnements cloud et réseaux.

La suite de logiciels est capable de traiter les sujets liés à la prise en main à distance de manière totalement sécurisée, la gestion des accès privilégiés, la suppression des privilèges utilisateurs excessifs, la gestion des vulnérabilités et enfin l'audit en temps réel des comptes à privilèges, couplé à un coffre-fort de mots de passe.

Gamme

- Password Safe
- Endpoint Privilege Management
- Privileged Remote Access
- Enterprise Vulnerability Management
- Remote Support
- Auditor
- AD Bridge

Technologies

- Protocoles natifs (RDP, SSH) ou technologie brevetée Jump Bomgar
- Interpréteur de commandes, actions spéciales personnalisées
- Support multi-moniteurs, multi-sessions
- Accès Shell sécurisé
- Connexion sans VPN
- Injection transparente des identifiants

Besoins clients

- Protection des identifiants et mots de passe
- Suppression des droits admin
- Suppression des mots de passe dans les applications
- Contrôle des applications
- Prise en main à distance des postes de travail fixes et appareils mobiles
- Contrôle et gestion des accès des tiers
- Mise en conformité et respect des réglementations

Arguments de vente

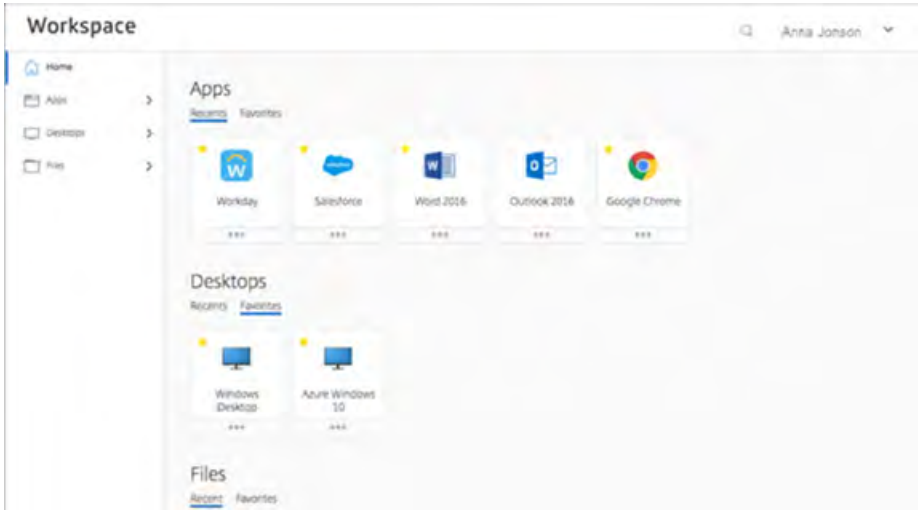
- Scanner, gérer, auditer et contrôler les comptes privilégiés de tous types
- Sécuriser les accès et le support des PC, terminaux ou systèmes partout dans le monde
- Sécuriser, gérer et auditer les accès à distance privilégiés des tiers et des salariés
- Supprimer les privilèges utilisateur excessifs sur les systèmes Windows, Mac, Unix, Linux et réseaux
- Identifier, prioriser et corriger les vulnérabilités avec des outils intégrés de configuration, de gestion des correctifs et de reporting de conformité
- Auditer, établir des rapports et remettre en états vos systèmes à grande échelle sur vos plateformes Microsoft Windows
- Centraliser l'authentification d'environnement MAC, LINUX et UNIX au sein de l'ActiveDirectory

Ligne Directe 01 60 19 02 30

Virtualisation d'applications et de postes de travail

Virtual Apps & Desktops permet de virtualiser les applications et les postes de travail en tant que services mobiles, en apportant une gestion simplifiée et en réduisant les coûts pour les services informatiques. C'est un accès en libre-service pour les utilisateurs.

Virtual Apps & Desktops propose de la virtualisation d'applications et de postes pour tous les modes de travail. Les clients peuvent utiliser n'importe quel poste de travail, client léger optimisé ou périphérique BYO. Au travers d'un portail appelé Workspace App, les utilisateurs peuvent désormais souscrire, en libre-service et en toute simplicité, à tout type d'applications Windows, Web, SaaS, mobiles et aux données des utilisateurs.



Gamme

Virtual Apps & Desktops est commercialisé par utilisateur CCU (simultané) ou par utilisateur nommé (utilisateur et/ou poste)

- Choisissez le package de fonctionnalités adapté à vos besoins : **Standard, Advanced ou Premium***, puis le mode de déploiement : **licences «on-premise» perpétuelles ou annuelles, ou services Cloud.**

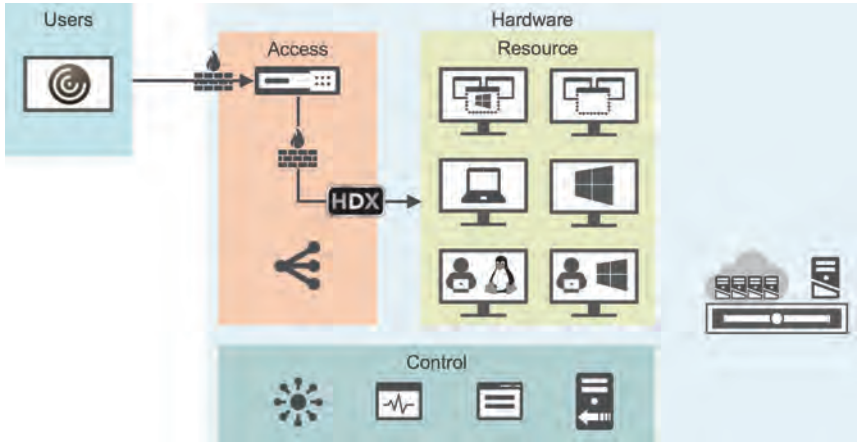
*(cf. matrice des fonctionnalités par édition en annexe 1 page 104).

Technologies

- Seamless local apps application
- Workspace App
- Load Balancing
- Pack d'optimisation Microsoft Teams
- HDX Mobile et 3D PRO
- AppDNA
- Accès distant à des postes lourds
- Intégration à la console Microsoft System Center

Besoins clients

- Adapter le mode de mise à disposition pour le bon utilisateur au bon moment
- Réduire les coûts
- Étendre les avantages de la virtualisation de postes et d'applications à la plupart des utilisateurs
- Augmenter la productivité grâce à un accès en tout lieu
- Intégrer le BYOD sans compromettre la sécurité
- Protéger l'activité grâce à une sécurité renforcée des postes virtuels



Arguments de vente

- Regroupe toutes les fonctionnalités d'accès depuis une console centralisée
- Disponibilité des données dans n'importe quel environnement BYO
- Mise à disposition de postes de travail entièrement personnalisée
- Accès intégré et sécurisé à toutes les applications Windows, Web, SaaS et mobiles et aux données des utilisateurs
- Expérience utilisateur similaire sur tous les périphériques
- Collaboration audio et vidéo en temps réel
- Prise en charge des applications graphiques 3D professionnelles

Accéder en toute sécurité aux applications et données en tout lieu

Citrix Workspace propose une expérience orientée utilisateur où tout ce dont les utilisateurs ont besoin pour travailler se trouve au sein d'une application unifiée, avec un accès conditionnel et des performances simples basés sur le contexte de l'utilisateur et des stratégies élaborées par les équipes IT. Citrix Workspace agrège ainsi toutes les applications et données, qu'elles soient sur site ou dans le Cloud pour une expérience utilisateur optimale.

Gamme

- Il existe 4 éditions de Citrix Workspace : **Essential, Standard, Premium ou Premium Plus**
- L'offre est commercialisée en licence par utilisateur.

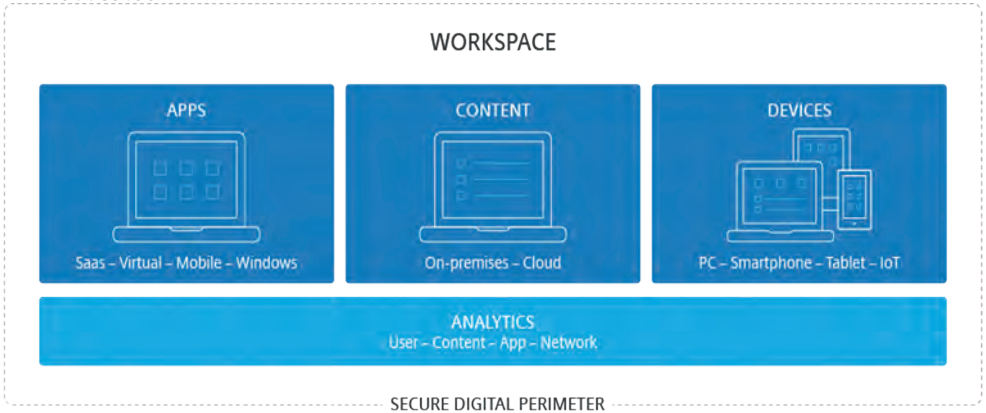
Matrice des fonctionnalités par édition cf. annexe 2 page 108

Technologies

- Contenu personnalisé par utilisateur
- Sécurisé par nature
- Portail unifié pour l'accès à l'ensemble des applications et données
- Expérience haute performante

Besoins clients

- Délivrer les applications, postes, données et services sur tout périphérique
- Donner plus de liberté et plus de flexibilité aux utilisateurs
- Permettre aux utilisateurs d'accéder en libre-service à toutes les applications
- Répondre aux besoins de performance, de sécurité et de mobilité de chaque utilisateur

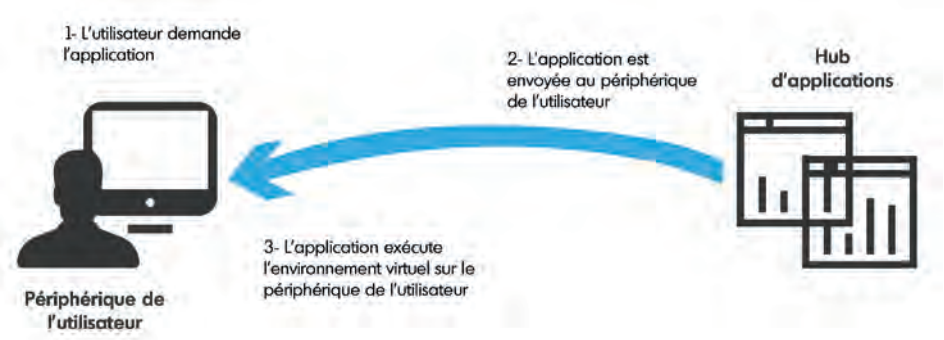


Arguments de vente

- Améliore la productivité des employés grâce à l'accès instantané aux applications, données et postes de travail
- Offre une expérience haute performance sur tout réseau
- Facilite la mobilité du personnel grâce à l'accès en libre-service aux ressources d'entreprise, ainsi qu'aux applications SaaS, Cloud…
- Sécurise le contenu d'entreprise dans le cloud ou sur le périphérique
- Offre une solution unique et flexible pour la gestion complète

Virtualisation d'application

Utilisée par plus de 100 millions de personnes dans le monde, **Citrix Virtual Apps** est la première solution qui permet la mise à disposition d'applications virtuelles, délivrant des applications Windows aux employés sur n'importe quel périphérique et en tout lieu.
En centralisant le contrôle avec Virtual Apps , l'entreprise offre à son équipe la liberté de la mobilité tout en renforçant la sécurité et en réduisant les coûts.



Gamme

- Virtual Apps est commercialisé en utilisateur simultané
- Il existe 3 éditions de Citrix Virtual Apps : Standard, Advanced, Premium
- Virtual Apps Premium est la plateforme unique permettant de mettre à disposition les applications avec l'ensemble des fonctionnalités.

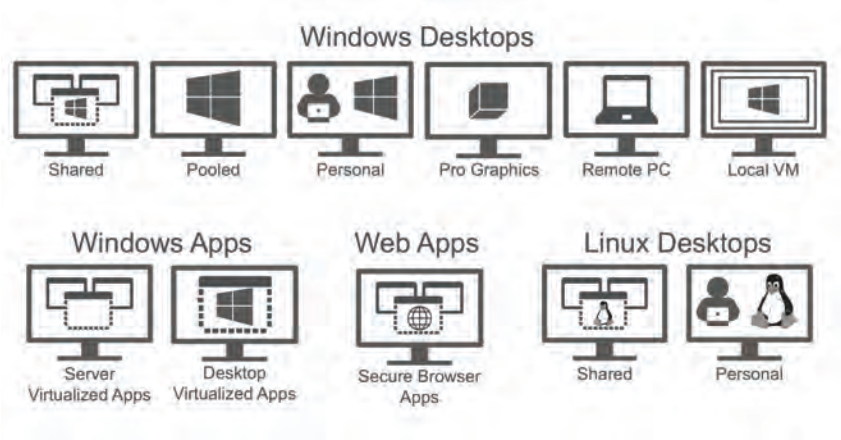
Voir la matrice des fonctionnalités par édition en annexe 1 page 104

Technologies

- Librairie d'applications d'entreprise en libre-service
- Expérience utilisateur haute définition - HDX
- Continuité de service
- Sécurité et conformité
- Répartition de charge
- Gestion des profils
- Evolutivité à l'échelle de l'entreprise

Besoins clients

- Donner une autonomie aux employés en délivrant cinq générations d'applications Windows sur tout périphérique
- Réduire les délais de transaction des applications client/serveur jusqu'à 300%
- Permet au personnel d'être plus productif avec leurs applications d'entreprise
- Prendre en charge les périphériques BYOD en toute simplicité

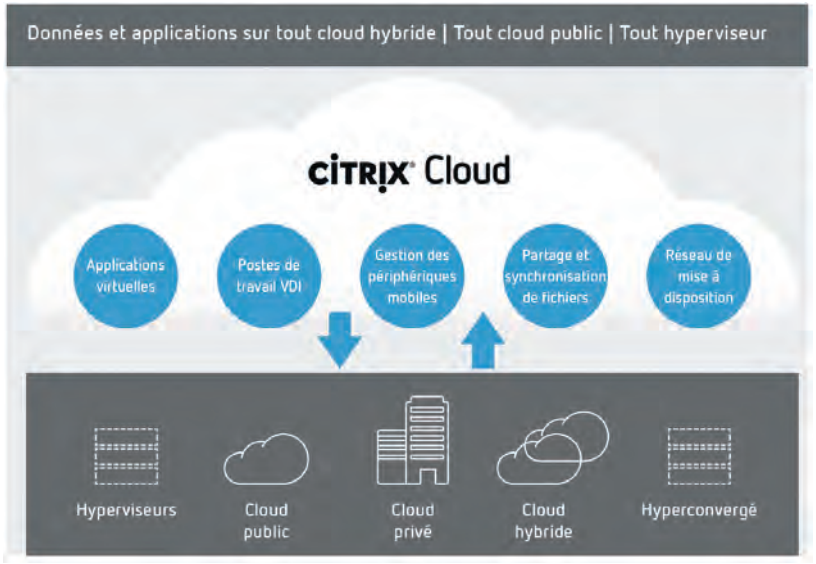


Arguments de vente

- Offrir un accès sécurisé aux applications en réduisant le risque de la perte de données.
- Mise à disposition des applications virtuelles adaptée à chaque scénario d'accès
- Réduire les coûts et la complexité liés à la gestion d'applications
- Ravissez les utilisateurs avec un accès simplifié aux applications virtuelles
- Facilite la résolution des principales problématiques informatiques et de l'entreprise

Déplacer un espace de travail depuis n'importe quel cloud ou infrastructure

Avec une infrastructure Citrix dans le Cloud mais des Workloads (Applications) restant sous le contrôle du client, **Citrix Cloud**, offre la possibilité de choisir où sont hébergées ses applications et ses données. Grâce à des connecteurs, il est possible de jongler entre un cloud Amazon ou Azure, des cloud privés chez des partenaires hébergeurs ou son propre datacenter. Cette Plateforme permet d'unifier les applications, postes de travail, données, gestion des périphériques et réseaux virtuels sur n'importe quel cloud ou infrastructure. Cette approche intégrée est la façon la plus simple de créer et de mettre à disposition des espaces de travail numériques.



Gamme

- **Citrix Workspace Service** (Accès à l'ensemble des technologies Citrix)
- **Virtual Apps & Desktops Service**
- **Virtual Apps Service**
- **Content Collaboration Service**
- **Endpoint Management Service**

(cf. page 30)

Technologies

- Connecteur Multi-Cloud (Azure, Amazone, Oracle Cloud, Google Cloud, etc..)
- Smart Tools : Outils facilitant la migration vers le Cloud
- Accès sécurisé via un Citrix ADC

Besoins clients

- Déployer rapidement une infrastructure Citrix
- S'affranchir des mises à jour de la plateforme
- Offrir un accès distant sécurisé depuis n'importe quel device à toutes les ressources de l'entreprise
- Faciliter la gestion des applications et bureaux
- Haute disponibilité de l'infrastructure Citrix
- Débordement des Workloads sur un cloud public ou privé

Migrez vers le Cloud à votre rythme grâce à Citrix

(cf annexe 3 page 109)

Arguments de vente

- Un panneau de gestion unique pour l'ensemble de votre espace de travail numérique sécurisé
- Solution complètement agnostique du fournisseur d'infrastructure cloud
- Un contrôle sécurisé des applications, postes et données de l'entreprise, dans le datacenter ou le cloud
- Des mises à jour automatisées qui réduisent les délais de maintenance et permettent de toujours bénéficier de la dernière version

Ligne Directe 01 60 19 16 74

Gérer les applications, les données et les périphériques mobiles

Citrix Endpoint Management (ex XenMobile) est une révolution pour la mobilité d'entreprise. Le produit garantit sécurité et conformité à l'informatique, tout en offrant aux utilisateurs la liberté des périphériques, des applications et des données mobiles.
Les utilisateurs bénéficient d'un accès en un seul clic à toutes leurs applications mobiles, SaaS et Windows à partir d'une librairie applicative unifiée, y compris à des applications de messagerie, de navigateur, de partage de données et de support intégrées en toute transparence.

Gamme

- **Endpoint Management Standard :** MDM : gestion des périphériques mobiles (sécurité des applications et des données sur les périphériques mobiles d'entreprise et personnels).
- **Endpoint Management Advanced :** MDM + gestion des applications Worx, SSO, containerisation et Store applicatif unifié et Gestion des devices Win 10 et Mac OS.
- **Endpoint Management Premium :** EPM Advanced Edition + la gestion des données avec Content Collaboration Advanced 0Gb

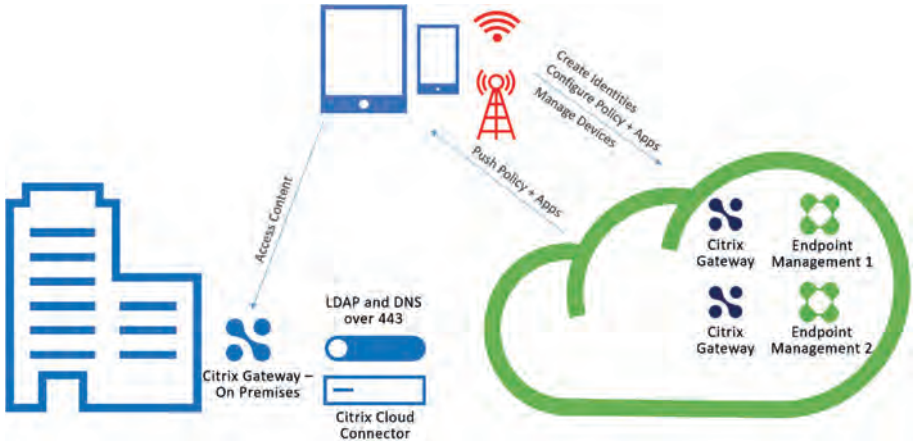
Les licences sont disponibles soit par user soit par Device en souscription Cloud.

Technologies

- Secure Mobile Apps
- Kit de développement d'applications Secure Apps
- Librairie applicative d'entreprise unifiée
- Intégration transparente des applications Windows
- Authentification unique multi-facteurs

Besoins clients

- Gérer et sécuriser les périphériques professionnels et personnels, les applications et les données
- Centraliser le support des périphériques, applications et données mobiles
- Accès sécurisé à la messagerie, au Web et aux documents
- Expérience utilisateur efficace sur tout périphérique

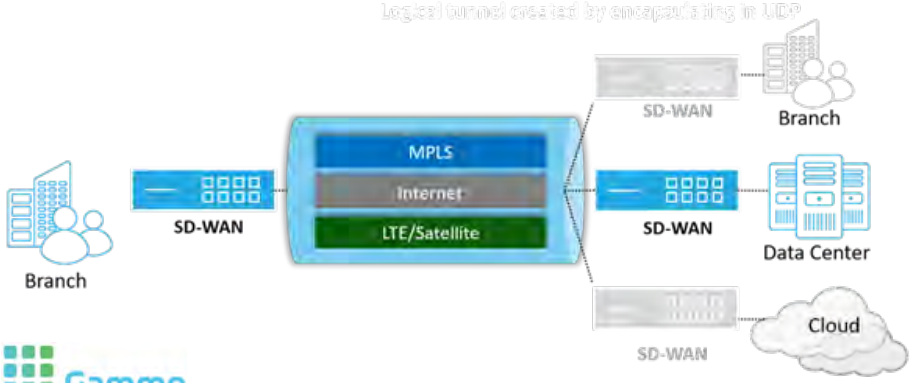


Arguments de vente

- Ensemble complet d'outils pour gérer et sécuriser les périphériques, les applications et les données
- Interdire ou autoriser des applications, détecter les périphériques débridés et supprimer le contenu d'un périphérique non conforme
- Point d'accès unique à toutes les applications Windows, Web, SaaS et mobiles sur tout périphérique mobile
- Authentification unique pour toutes les applications mobiles, Web et Windows
- Favoriser la compatibilité de toute application mobile avec l'entreprise
- Partage, synchronisation et modification sécurisés des documents

Augmenter la performance et la résilience du WAN

Citrix SD-WAN™ est une solution de virtualisation du WAN qui garantit une expérience optimale pour les applications qui transitent sur le WAN. SD-WAN assure une mise à disposition fiable des applications aux utilisateurs en mettant en place une agrégation des différents types de liens et une QOS fine.



Gamme

- Existe sous forme d'Appliance physique ou Virtuelle (VPX) disponible sur tout type d'hyperviseur
- Disponible dans tous les cloud publics avec le Bring Your Own License (BYOL) Amazon, Azur et Google
- **Gamme SD-WAN** : de 1 à 6000 Mbps
- **Gamme SD-WAN VPX** : de 2 à 200 Mbps
- Console de management cloud ou on-premise

Technologies

- Agrégation des liens pour créer un lien virtuel
- Assignation des liens paquet par paquet
- Duplication des paquets sur le WAN
- Simplicité d'exploitation : interface HTML5 centralisé dans le cloud avec SD-WAN Orchestrator
- Un temps de convergence en quelques ms qui rend les bascules invisibles pour l'utilisateur et les applications
- Optimisation des flux HDX pour les environnements Citrix
- Compression, accélération et déduplication des flux
- Visibilité et firewall applicatif sur le réseau grâce à la technologie QOSMOS et le Deep Packet Inspection (DPI)
- Utilisation de la technologie FastStart pour une utilisation de la pleine bande passante
- Optimisation du protocole TCP
- Internet Local Break out pour tous les flux applicatifs et métier

Besoins clients

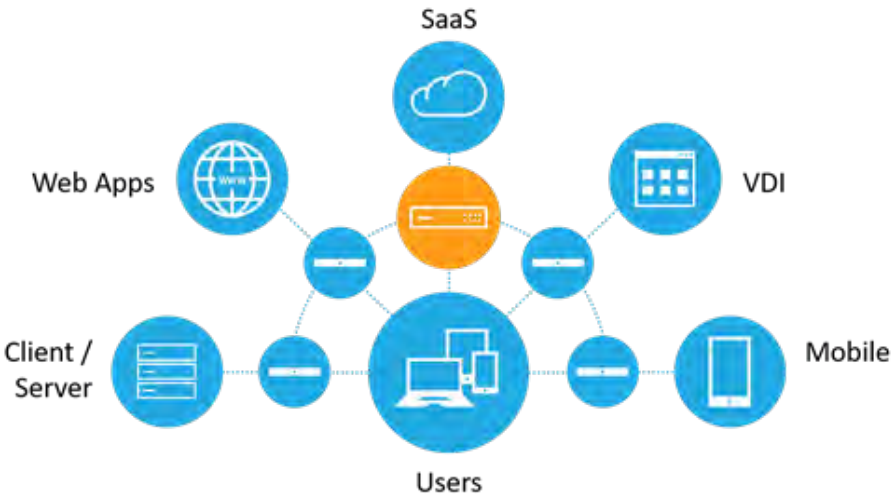
- Améliorer l'expérience utilisateur sur le réseau WAN
- Fiabiliser l'accès de l'utilisateur à ses ressources depuis son poste quel que soit l'endroit où elles se trouvent
- Réduire les latences sur le réseau
- Avoir de la visibilité applicative pour pouvoir mettre en place des stratégies de répartition des flux
- Améliorer la bande passante disponible

Arguments de vente

- Seule solution permettant l'accélération, l'optimisation et la QOS du flux HDX
- Visibilité et mesure des performances réseau
- Déploiement zero touch
- Fiabilisation et résilience du réseau
- Outil de management, monitoring et reporting de la solution centralisée
- Simplification de la gestion du réseau
- Meilleure expérience utilisateur
- Disponible dans les clouds publics Amazon, Azur et Google
- Compatible avec tous les hyperviseurs du marché
- Grande variété d'Appliances adaptées à tous les types de structures
- Réduction de la dépendance au MPLS
- « Pay As You Grow » plateforme évolutive pour protéger l'investissement de l'entreprise

Contrôleur de mise à disposition d'applications pour la mobilité et le Web

Citrix étant le leader incontesté de la mise à disposition d'applications et de services, les solutions **Citrix ADC** sont déployées sur des milliers de réseaux dans le monde pour optimiser, sécuriser et contrôler la mise à disposition de tous les services d'entreprise et de Cloud. Elles permettent une disponibilité des applications à 100%, un délestage des serveurs d'applications et de bases de données, une accélération des performances et une protection avancée contre les attaques.



Gamme

- 6 gammes d'Appliances différentes et 3 éditions (Standard, Advanced et Premium) permettant une évolution à la demande
- 3 modes de licencing offrant plus de souplesse pour s'adapter à la stratégie du client (Perpétuel, Zero Capacity, Pooled Capacity)
- Disponible dans tous les clouds publics, Amazon, Azur et Google

Voir la matrice des produits par édition en annexe 4 page 110

Besoins clients

- Continuité de service des applications
- PCA/PRA (répartition de charge multi-sites)
- Optimiser des bases de données SQL
- Réduire les temps de réponses applicatifs
- Réduire les coûts d'infrastructure
- Gérer dynamiquement des environnements Hybrid Multi Cloud
- Proposer du travail à distance sécurisé pour les utilisateurs
- Optimiser Citrix Virtual Apps & Desktop

Arguments de vente

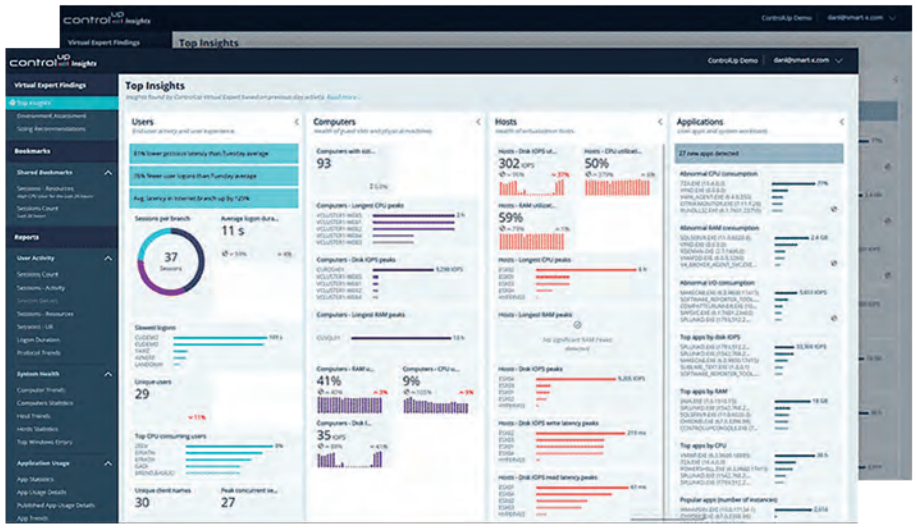
- Intégration complète, code unique sur l'ensemble de la gamme
- Solution incluant GSLB, VPN SSL et un pare-feu applicatif
- Visibilité Applicative
- Gestion Centralisée avec la console Application Delivery Manager (ADM)
- Consolidation SDX
- Disponibilité des applications performantes et sécurisées pour tous les utilisateurs quel que soit l'endroit où ils se trouvent
- Solution la plus adaptée à la gestion des environnements hybrid multi cloud grâce à un mode de licencing innovant et unique sur le marché

Technologies

- Assure la disponibilité et le bon fonctionnement des applications avec la technologie Protocol Level Health Checks
- Load Balancing de Server et de Datacenter (GSLB) pour une meilleure scalabilité des performances
- Caching HTTP, Optimisation TCP, Compression Web, Optimisation SQL
- Portail Captif AAA compatible SSO et MFA
- Web App Firewall (WAF)
- VPN SSL et SSL Offload
- Insight pour la visibilité applicative
- Détection d'attaque DDOS en couche 4 et 7
- Bot Management

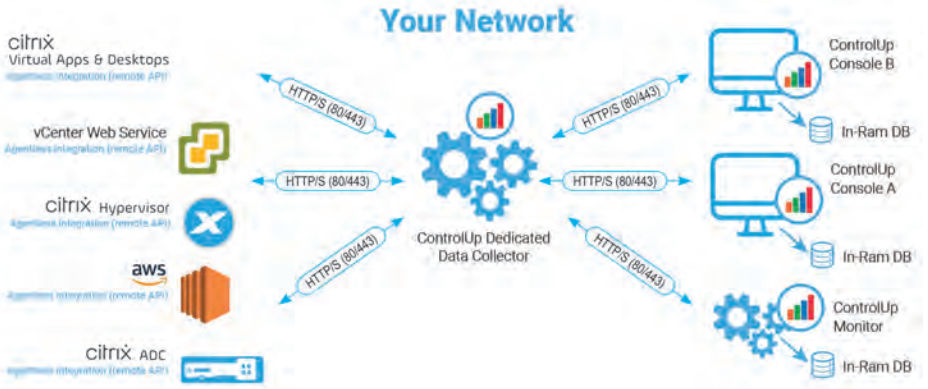
Monitoring temps réel des environnements Citrix, VMware et Microsoft RDS

ControlUp propose à l'aide de sa **console Real-Time** basée sur un moteur temps-réel, un tableau de bord remontant l'ensemble des métriques liées aux environnements Citrix, VMWare et Microsoft, permettant aux administrateurs de détecter en un coup d'œil les problèmes de performance liés aux ressources disponibles (CPU, RAM, Stockage, bande passante, ...) et ainsi agréger ces informations pour rendre compte de l'expérience des utilisateurs. Cette console Real-Time permet de monitorer l'état de santé des *hosts*, machines, sessions et processus de ces environnements, en rafraichissant toutes les 3 secondes chaque cellule de la console. Lorsqu'un stress d'une machine ou d'une session est détecté, l'assistant virtuel de ControlUp permet d'accompagner l'administrateur à en trouver la cause, en signalant les différentes mesures dépassant les seuils (consommation de bande passante, RAM, CPU), puis en proposant d'agir sur ces métriques en poussant un script directement dans la session de l'utilisateur, ou en terminant un processus par exemple.
La seconde console, **ControlUp Insight** permet de résumer l'état des ressources monitorées toutes les 24h, mettant en lumière des indicateurs, des statistiques de performance, des facteurs de risques liés aux activités des applications et des utilisateurs. Cette console permet de s'assurer du bon dimensionnement des serveurs, du nombre d'utilisateurs actifs, des applications les plus consommatrices en termes de ressources. Une plateforme complète pour s'assurer de la bonne santé des infrastructures.



Besoins clients

- **Monitorer et manager** l'expérience utilisateur
- Résoudre les problèmes de performances
- Analyser le dimensionnement des infrastructures
- Automatiser la résolution des problèmes récurrents



Arguments de vente

- Déploiement facile et rapide
- Remontée de données automatique
- Bibliothèque de scripts consistante
- Gestion de toutes les infrastructures centralisées (RDS, Citrix, VMWare, Nutanix, ...)
- Analyse granulaire de l'état de santé des équipements
- Assistant virtuel pour un troubleshooting rapide

Technologies

- Surveillance de la consommation des ressources (RAM, CPU, IO, bande
- passante, ...)
- Vue granulaire des processus en temps réel
- Une grande bibliothèque de scripts disponibles pour le troubleshooting

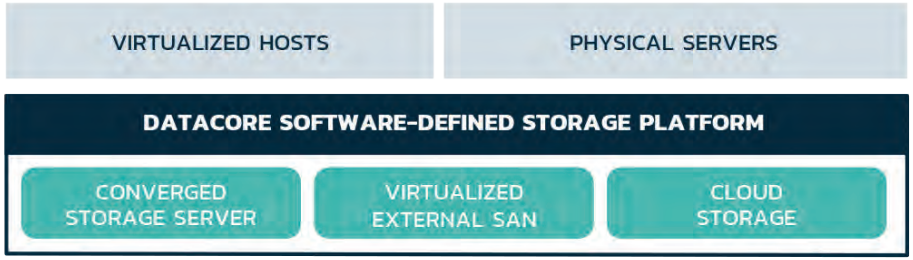
Gamme

- 2 modes de déploiement (**On-Premise et Cloud**)
- 3 éditions basées sur le temps de rétention des données :
  - **Pro** (1 jour de rétention)
  - **Enterprise** (1 mois de rétention)
  - **Platinium** (1 an de rétention)
- Des **add-on** : Automation (automatisation de lancement de scripts basés sur des triggers), Scoutbees (bot de test de la disponibilité des applications

DATACORE

Optimiser tous les stockages

Le logiciel **SANsymphony-V** relève les défis liés au stockage et inhérents aux stratégies de virtualisation, de cloud computing, de continuité d'activité et de reprise d'activité grâce à des technos de software defined storage. Il forme une couche de virtualisation active et transparente entre la plaque-serveur et la plaque-stockage afin d'optimiser la disponibilité d'accès aux données et les performances, des petites configurations jusqu'aux grands data centers. SANsymphony-V permet l'accélération des applications, l'accès ininterrompu aux données, le prolongement du cycle de vie de vos baies et leur interopérabilité, quel que soit le constructeur.



Gamme

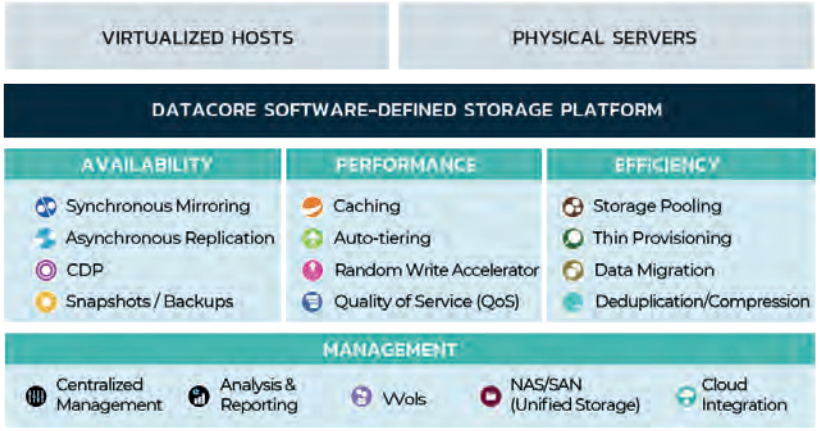
- Licencing au To
- 2 types de Licences : perpétuelles avec renouvellement ou en mode souscription
- 3 versions
- Enterprise : comprend toutes les options
- Standard : toutes les options sauf le FC
- Large Scale : sans les options d'accélération pour les projets de données froides

Technologies

- SAN, NAS, SCIS, 10Go, FiberChannel, FCoE etc…
- Miroir Actif/Actif
- Réplication asynchrone bidirectionnelle
- Snapshot et CDP
- Tiering et Auto-Tiering
- Thinprovisioning
- Zoning et QoS du stockage
- Reporting, capacity planning
- Compression et déduplication

Besoins clients

- Virtualisation de stockage, PRA/PCA
- Haute disponibilité et garantie de continuité totale d'accès au stockage
- Réplication entre baies SAN de différents constructeurs
- Réductions des latences et multiplication des i/o
- Réduction des coûts de stockage
- Archivage des données



Arguments de vente

- DataCore arrive premier aux tests comparatifs indépendants sur le stockage
- Indépendance totale vis-à-vis des constructeurs
- Haute disponibilité actif/actif, zéro interruption d'accès au stockage
- Administration centralisée et intuitive
- Tiering et Auto-Tiering : utilisation optimisée des différents disques SATA, SAS, SSD
- Administration intégrée dans VCenter de VMware et SCOM de Microsoft
- Réplication multi-nœuds
- Cluster DataCore
- Allocation dynamique et ajout de stockage à la demande

Ligne Directe 01 60 19 16 74

DATACORE

Stockage objet en Cloud privé

DataCore Swarm fournit une solution de stockage objets sur site qui simplifie considérablement la gestion, le stockage et la protection des données, tout en permettant un accès S3/HTTP à tout périphérique, application ou utilisateur final. Swarm transforme les archives de données en bibliothèque de contenus flexible et immédiatement accessible, qui rend possibles les flux de travail distants. Vous n'avez plus à déplacer les données dites froides dans des solutions disparates à des fins de conservation à long terme, de livraison ou d'analyse.
En regroupant tous les fichiers sur Swarm, on retrouve rapidement les données voulues et on réduit le coût total de possession en faisant évoluer le matériel en permanence.

Gamme

- **Licencing** au To source (indépendamment des réplications multiples possibles des données protégées)
- Les licences **Swarm** sont associées à des support 1, 3 ou 5 ans
- **FileFly** est une licence séparée pour gérer les fonctions d'archivage

Technologies

- Multiprotocole (HTTP, S3, NFS, SMB)
- Elastic Content Protection (Replication + Erasure Coding)
- Automatic Failure Recovery : vérification permanente des disques pour garantir la pérennité des données
- File Search and Query : recherche multi-critères sur l'ensemble des données stockées
- Worm & Integrity Seals : immuabilité, garantie conforme de non-modification des données
- Cloud Disaster Recovery : Réplication multi-sites et Cloud DR

Besoins clients

- Gérer de grands volumes de fichiers, du To aux centaines de Po de données et des milliers de tenants avec un personnel limité
- Exiger l'évolutivité du stockage dans le cloud, mais les données doivent rester sécurisées sur site
- Archiver sur du stockage objet beaucoup plus économique les données non fréquemment consultées.
- Optimiser les fonctionnalités de recherche rapide et multi-critères sur les données froides.
- Partager le découpage de fichiers & Diffusion (données médicales, Médias plateformes Streaming, HPC, IoT, Vidéosurveillance, données publiques etc…)
- Garantir la sécurisation ultime des données sauvegardées ou archivées contre tous les ransomwares et crypto-lockers

CONSOMMATEURS			
UTILISATEURS FINAUX		APPLICATIONS ET SERVICES WEB	APPAREILS
MÉTHODE D'ACCÈS			
S3/HTTP		NFS*	SMB**
OPÉRATIONS ET INFORMATIONS	**SERVICES DE GESTION DES DONNÉES ET DE L'INFRASTRUCTURE**		**COMMANDE ET CONTRÔLE**
AUDIT DE L'UTILISATION, MESURES ET QUOTAS	ESPACE DE NOMS UNIVERSEL	EXPANSION RAPIDE	CONSOLE
GESTION DE L'IDENTITÉ	UN OU PLUSIEURS SITES	OPTIMISATION DE LA CAPACITÉ OU DES PERFORMANCES	
DÉLÉGATION ET LIBRE-SERVICE	SÉCURITÉ ET AUTHENTIFICATION	RECHERCHE DE FICHIERS ET REQUÊTES	REST API
GRAPHIQUES HISTORIQUES ET EN TEMPS RÉEL	PROTECTION DU CONTENU ADAPTABLE (RÉPLICATION + CODE D'EFFACEMENT))	PARTAGE, STREAMING ET EXTRAITS VIDÉO	MÉTADONNÉES PERSONNALISABLES
GRAPHIQUES SUR L'INTÉGRITÉ ET LES PERFORMANCES	RÉCUPÉRATION AUTOMATIQUE APRÈS UNE PANNE	WORM ET SCEAUX D'INTÉGRITÉ	
ORCHESTRATION	CHIFFREMENT EN COURS DE TRANSFERT ET AU REPOS	REPRISE APRÈS SINISTRE SUR LE CLOUD	ADMINISTRATION GRANULAIRE
TOUTE COMBINAISON DE SUPPORTS DE STOCKAGE ET DE SERVEURS X86			
Disque dur		SSD	

*L'ACCÈS NFS EST PRIS EN CHARGE PAR SWARMFS. **L'ACCÈS SMB EST PRIS EN CHARGE PAR DATACORE FILEFLY.

Arguments de vente

- Plateforme logicielle évolutive en permanence, indépendante du matériel.
- Gérer de manière unifiée toute combinaison de serveurs x86, de disques durs et SSD, de NAS ou SAN externes
- Meilleures fonctionnalités avec un coût au To très optimisé par rapport aux solutions S3 ou d'archivage existantes
- Partenariats et Certifications avec Veeam, Commvault, Atempo etc… pour offrir une immuabilité garantie de leurs données sauvegardées
- Un seul administrateur système/informatique peut gérer des dizaines ou des centaines de pétaoctets

Ligne Directe 01 60 19 16 74

Les meilleurs disques à disposition de vos serveurs

Enfin les meilleurs disques aux vrais prix ! **Western Digital**, qui fournit plus de 60% des disques vendus dans le monde, équipe les plus grands constructeurs de serveurs et de baies de stockage. Western Digital et son entité HGST proposent aujourd'hui ces disques directement à la distribution, afin d'équiper en stockage de haute qualité les solutions de SDS (Software-Defined Storage). Ces JBOD (Just a Bunch Of Disks – juste un paquet de disques) sont proposés sous forme d'un châssis complétement passif, donc à des prix défiant toute concurrence, et sont le complément parfait en prix et en performance des solutions SDS (Windows, Linux, Datacore, VMware, solutions logiciels d'hyper-convergence, etc.).

Gamme

- Cartes Ultrastar® : capacités SSD pour Tiers 1 ultra rapide, format NVMe sur bus PCIe
- Châssis Ultrastar® Data60 : JBOD 4U capacitive ou hybride capacitive/SSD
- Châssis FLASH 2U24 : JBOD 2U Full-Flash

Technologies

- Très faibles consommations d'énergie pour le Green IT
- Technologies de refroidissement brevetées pour un échauffement minimal des disques
- Atténuation optimisée des vibrations pour garantir une perte minimale de performance des disques
- Connecteurs SAS 12Gb/s pour un débit maximal
- Disques SSD au format NVMe

Besoins clients

- Larges volumétries de disques capacitifs
- Besoin de Stockage ultra-rapide
- Stockage hybride
- Forte réduction du prix du To capacitif ou Flash

Arguments de vente

- Les plus fortes densités : Jusqu'à 720To et 1,2Po sur 4U
- Les plus hautes performances : de 11 à 180To Full-Flash sur 2U
- Très faibles consommations d'énergie, technologies de refroidissement brevetées, atténuation de vibration : pertes minimes de performance des disques
- Châssis passifs : taux de pannes quasi nul, installation immédiate, pilotage total par les solutions de SDS

Ligne Directe 01 60 19 02 30

Console Management : Serveurs de ports console

Ces produits permettent de concentrer et d'accéder à distance aux ports console série des serveurs, routeurs, switches et produits réseaux actifs. Ils assurent à l'administrateur en charge de ces équipements la possibilité de prendre la main en toutes circonstances, même en cas de panne sévère rendant leur interface réseau inutilisable.
Ces solutions d'administration par port série console s'utilisent seules ou en complément des outils d'exploitation réseau habituels. Elles s'adressent aux entreprises dont les équipements sont critiques, localisés sur les sites distants ou hétérogènes.

Gamme

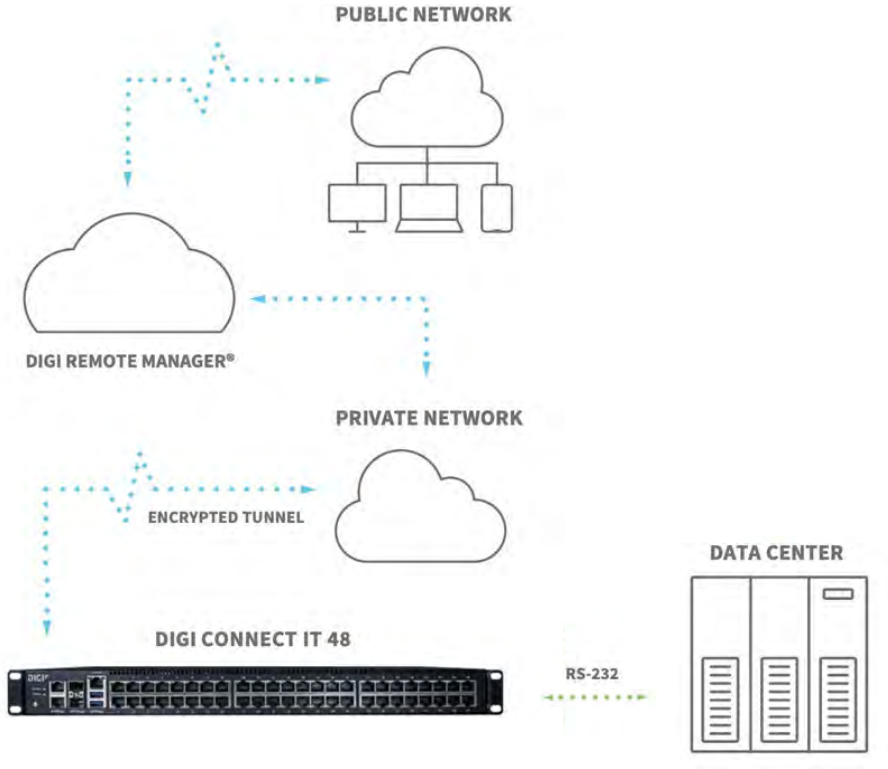
- Digi Passport : 8, 16, 32 et 48 ports série.
- Digi Connect IT avec module 4G LTE : 1, 4, 16 et 48 ports série.

Technologies

- Supports des OS Linux®, Windows Server® 2003, Mac OS® X, Solaris®, UNIX
- Radius et TACACS
- Clustering
- Telnet et HTTP
- Chiffrement SSH, SSL Alertes SNMP ou SMTP
- Dual Ethernet et dual Alim pour la redondance
- IPv4/IPv6

Besoins clients

- Supervision des éléments actifs du réseau
- Accès en mode secours
- Gestion distante des ports console et des alimentations électriques
- Plan de reprise d'activité
- Centralisation de l'administration du SI



Arguments de vente

- Produits industriels fiables et garantis 5 ans
- SAV et support technique France (Miel)
- Gamme large et pérenne (1 à 48 ports, cluster possible, 220 ou 48 volts)
- Paramétrage et administration simples et conviviaux (logiciel de découverte, interface Web, configurations sauvegardées et mise à jour en HTTP)
- Haut niveau de sécurité : connexions chiffrées
- Intégration facile avec l'existant (RADIUS, TACACS, SNMP ou SMTP etc.)
- Câblage très économique. Intégration avec tout produit réseau ou serveur du marché

Ligne Directe 01 60 19 09 85

Routeurs industriels 4G : pour l'IoT et les environnements industriels

Les routeurs **Digi industriels** sont des produits intelligents capables de raccorder et gérer tous les systèmes industriels fixes ou mobiles : Compteurs, capteurs, signalétique, bornes d'affichage numérique, terminaux de paiement... Ils ont été conçus pour résister aux vibrations, chocs, eau et températures extrêmes. Intégrant tous les standards de sécurité et d'administration, les routeurs Digi peuvent aussi être déployés et gérés à distance grâce au Digi Remote Manager. Programmables en Python, il est possible d'y ajouter toutes les fonctionnalités spécifiques pour interconnecter des machines industrielles.

Gamme

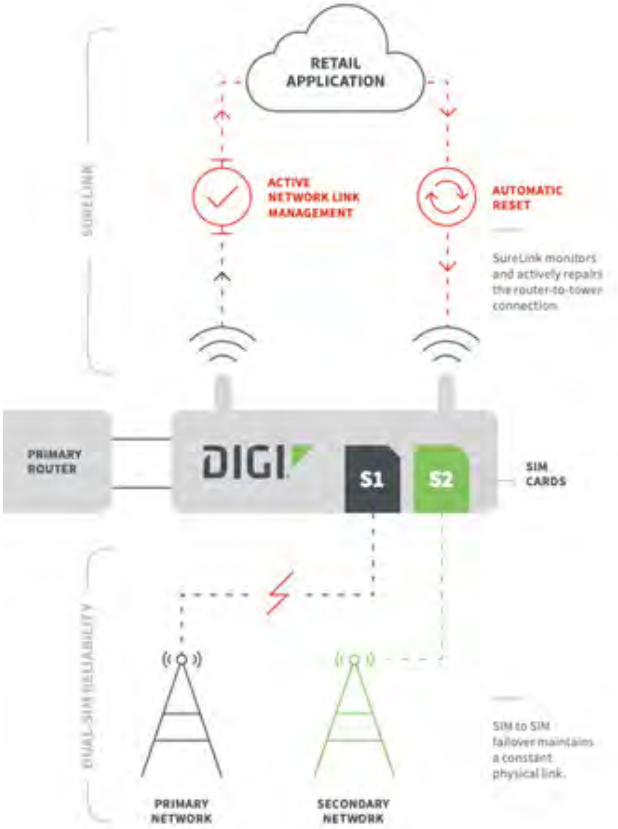
- **IX14, TX54 et TX64, WR11 XT, WR21, WR31, LR54, WR44R, WR54, WR64** : routeurs spécialisés pour la connectivité dans le transport public. (Bus, Trams et trains)
- **Connect Sensor** : Remontées 4G IoT de capteurs analogiques, numériques ou de niveaux alimentés par batteries, Températures étendues

Technologies

- LTE 4G Cat1/Cat4
- IPSec, OpenVPN
- Port Série RS232
- Alimentation adaptée en 9-30V

Besoins clients

- Télécollecte sur des sites isolés
- Monitoring d'équipements industriels
- Backup 4G
- Prise en main à distance
- Mobilité des systèmes



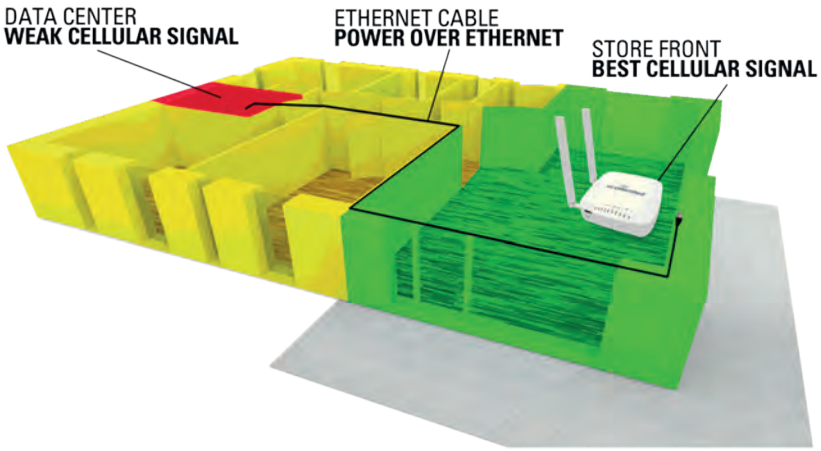
Arguments de vente

- Maintien d'une connexion permanente bidirectionnelle 24/24 – 7/7
- Double carte SIM pour basculement automatique "Fail-Over"
- Produits industriels fiables (garantie jusqu'à 5 ans)
- Scripts Python pour les développements avancés
- Sécurité : client VPN et Firewall intégrés
- Surveillance du réseau cellulaire et reprise automatique sur incident
- Logiciel de supervision et de paramétrage du parc déployé
- Paramétrage à distance (Web, commandes ou SMS)

Ligne Directe 01 60 19 09 85

Routeurs 4G Entreprise pour la connectivité des sites distants

Digi propose une gamme de **routeurs 4G** pour les entreprises, qui se caractérise par sa grande simplicité d'installation et son déploiement en masse. Avec la batterie Pack fournie il est possible d'identifier en quelques minutes la meilleure zone de réception pour installer le routeur. Les nombreux accessoires de fixation fournis aident à sécuriser l'installation. Les routeurs 4G de Digi offrent une liaison Cellulaire LTE-Advanced (Cat 6) avec plusieurs ports Ethernet Gigabits, dont des ports WAN dédiés, ainsi qu'un port série. En utilisant la solution Digi Remote Manager, il est possible de définir facilement les configurations de référence, les déployer à distance, suivre leurs états, sans avoir recours à un technicien spécialisé sur site.



Gamme

- Digi EX12, EX15, 6310-DX, 6330-MX, 6350-SR et Digi CORE® plug-in LTE modem

Technologies

- LTE 4G+ Cat6, Cat11, Cat13
- VRRP+
- IPSec, OpenVPN
- QoS, VLAN
- Firewall Stateful

Besoins clients

- Retail, Data Center, Entreprises
- Lien réseau principal site distant sans ADSL/Fibre, site temporaire, ou site sans accès à l'infrastructure réseau (Shop in Shop).
- Solution de back-up en cas de perte du lien réseau principal (rupture câble).
- Solution de backup de réseau distant en cas de panne équipement (management out-of-Band)

Digi Remote Manager : La solution cloud de gestion et de monitoring de vos équipements

Arguments de vente

- Haute connectivité 4G+
- VRRP+ : Redondance des routeurs virtuels et basculement automatique
- Kit de déploiement rapide intégré
- Management à distance
- Tous les protocoles Réseaux et Sécurité nécessaires embarqués

Centralisation de vos liaisons séries et USB

Les serveurs de ports DIGI permettent de raccorder au réseau Ethernet des périphériques série ou USB pour les gérer à partir d'un ou plusieurs serveurs situés sur le même réseau LAN ou WAN. Ces solutions trouvent leur place dans les systèmes centralisés nécessitant le raccordement de périphériques déportés (supervision de réseaux dongle USB, gestion d'automates, points de ventes etc.). Ces passerelles sont proposées avec un logiciel breveté, le **RealPort**, qui permet d'émuler localement sur le serveur central des ports série ou USB.

Gamme

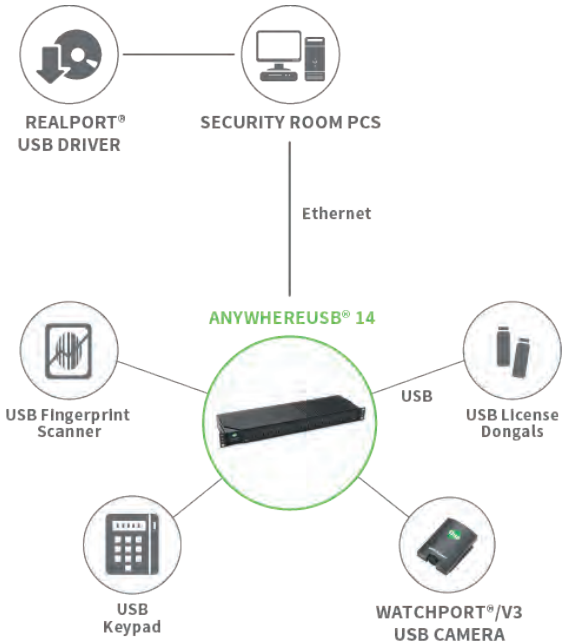
- Produits USB/Ethernet : **Anywhere USB**® Plus
- Produits Série/Ethernet : **PortServer**® TS / **PortServer**® TS MEI
- Produits USB/Série : **Hubport**® / **Edgeport**®
- Produits Série/Ethernet monovoie : **Digi One SP, Digi One IA, Digi Connect SP**

Technologies

- Emulation de ports COM, TTY, USB
- Gestion des micro-coupures réseau
- Ports Séries RS232, RS422, RS485
- MODBUS, TCP et UDP Socket
- USB 3.0, Power USB
- Tunnel Série

Besoins clients

- Attribuer des ports USB Physiques à des machines virtuelles (Certifié VMWare et MS Hyper-V)
- Connectivité des périphériques USB aux postes dans le LAN
- Mise à jour des flottes de périphériques type tablettes dans les points de vente.



Arguments de vente

- Solutions fiables, garantie 5 ans et pérennes
- SAV et support technique Français via MIEL
- Gamme étendue (industrielle, auto-alimenté, WiFi, programmable)
- Drivers pour plus de 20 systèmes d'exploitation
- Réglage des temps de réponses
- Mise à jour gratuite des Firmwares et pilotes
- Format Rackable ou Rail-Din

Systèmes embarqués

ConnectCore : Construits sur les derniers processeurs, tels que NXP i.MX8, NXP i.MX6UL et NXP i.MX6. Les solutions de System-on-Module (SOM) ultra-compactes et hautement intégrées de DIGI offrent de nombreuses solutions sans fil, 802.11ac, Bluetooth avec des options d'ajout de réseau cellulaire et Zigbee.

Xbee : Les modules Digi XBee fournissent une connectivité sans fil via une multitude de protocoles. Faciles à déployer, pré-certifiés et configurables à l'aide de XCTU et de l'application mobile XBee, ces modules peu coûteux répondent à tous les besoins de conception sans fil. Idéal pour connecter les équipements et sondes sur des réseaux maillés ou non.

Gamme

- ConnectCore® 6/6+/6UL/8X
- XBee3® Cellular LTE-M/NB-IoT
- XBee3® Cellular LTE CAT1
- XBee3® DigiMesh 2.4
- XBee3® Zigbee 3
- XBee3® Gateway

Technologies

- Zigbee norme 802.15.4
- DigiMesh
- Bluetooth 4.2
- Wifi norme a/b/g/n/ac
- 4G LTE-M/NB-IoT/Cat1
- Certification IEC 60068, IEC 60601, HALT (ConnectCore®)
- Processeur ARM® Cortex®, GPU Vulkan® (ConnectCore®)

Besoins clients

- Réduire le Time-to-Market
- Passage aux technologies sans-fil
- Acquisition de données
- Remplacer des unités de contrôle coûteuses et volumineuses
- Trouver une alternative fiable aux systèmes embarqués grand public

Arguments de vente

- Qualité industrielle
- Supervision et management centralisés avec le Digi Remonte Manager
- Sécurisé par la technologie DIGI TrustFence®
- Compatible Android, Windows-IoT et Yocto Projet Linux
- Connectivité pré-certifiée Wifi et Bluetooth intégré
- Gamme de température étendue
- Programmable en Micro-Python
- Faible consommation électrique
- Environnement de développement fourni DIGI (XCTU, SmartIOMUX)

DOMAINTOOLS

Transformer les données des domaines en intelligence contre les attaques

DomainTools aide les analystes sécurité à transformer les données sur les IP et les noms de domaines en intelligence contre les cyberattaques. Par une analyse approfondie, DomainTools évalue les risques ou la réputation, dessine le profil les attaquants, guide les investigations, et cartographie la cyber activité malveillante. Les opérateurs de Soc, les analystes, les « *threat hunters* » ont à leur disposition une source unique d'informations exploitables automatiquement et instantanément par leurs outils (SOAR, SIEM, Threat Intel)

Précis

+95% des domaines actuellement enregistrés

Rapide

Tous les domaines nouvellement enregistrés et découverts

Complet

Près de 2 décennies de données historiques DNS et Whois

Gamme

- **Iris :** Plateforme d'investigation
- **Domain Risk Score :** Prédiction des domaines malveillants
- **PhishEye :** Détection de noms de domaine usurpés
- **Iris APIs :** Enrichissement et orchestration

Technologies

- **« Risk-Scoring »** prédictif basé sur le Machine Learning
- Historique, profilage et trafic DNS
- Information, contextualisation, et indexation collaborative des incidents
- Investigation des menaces et évaluation des risques des domaines
- Intégration par API aux solutions SOAR et SIEM

Ligne Directe 01 60 19 09 85

Besoins clients

- Information sur les IPs et domaines pour les outils du SOC
- Réduction des risques venant de domaines inconnus ou nouveaux
- Prevention du phishing et de l'usurpation de domaine. Protection des marques
- Investigation détaillée des IoCs et de leur contexte
- Enrichissement des solutions d'orchestration pour réponse à incident

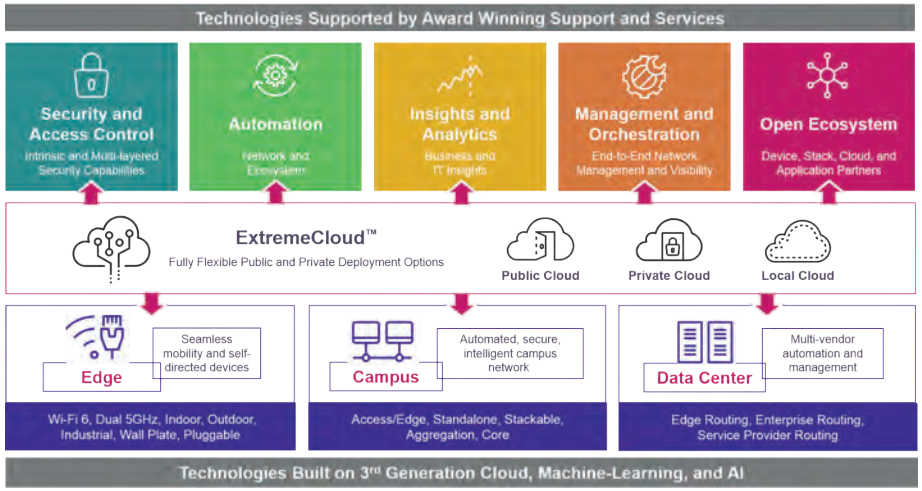
ANOMALI · CORTEX XSOAR · CROWDSTRIKE · EclecticIQ · elastic · IBM Security Resilient · MALTEGO · MISP Threat Sharing · POLARITY · RAPID7 · Recorded Future · splunk> · splunk> phantom · TheHive · Cortex · ThreatConnect · THREATQ

Arguments de vente

- La base de données DNS et d'enregistrement de domaines la plus riche du monde
- Intégrée à une interface utilisateur simple et intuitive orientée investigation
- Algorithmes propriétaires de *machine learning* pour la prédiction de risques, basés sur près de 20 ans d'observation et de données
- Système leader d'indicateurs de risque des domaines ou des connexions, basé sur l'infrastructure et la proximité des menaces
- Ecosystème éprouvé d'intégrations aux meilleures solutions de SOAR et de *Threat Intelligence* du marché

Piloter votre réseau à la vitesse du cloud

Basé sur une plateforme de 3ème génération, **ExtremeCloud IQ** mise sur le Machine Learning et l'intelligence artificielle (IA) pour simplifier la gestion, améliorer la visibilité et le contrôle, et réduire les coûts et la complexité pour toute l'entreprise – du périmètre du réseau jusqu'au cœur du data center. Du déploiement à la maintenance, la dernière plateforme de management a été conçue pour rationaliser chaque aspect du réseau. En plaçant l'humain au cœur des enjeux, la solution libère les équipes IT et métiers des tâches rébarbatives et chronophages pour leur permettre de se recentrer sur leur mission première.



Gamme

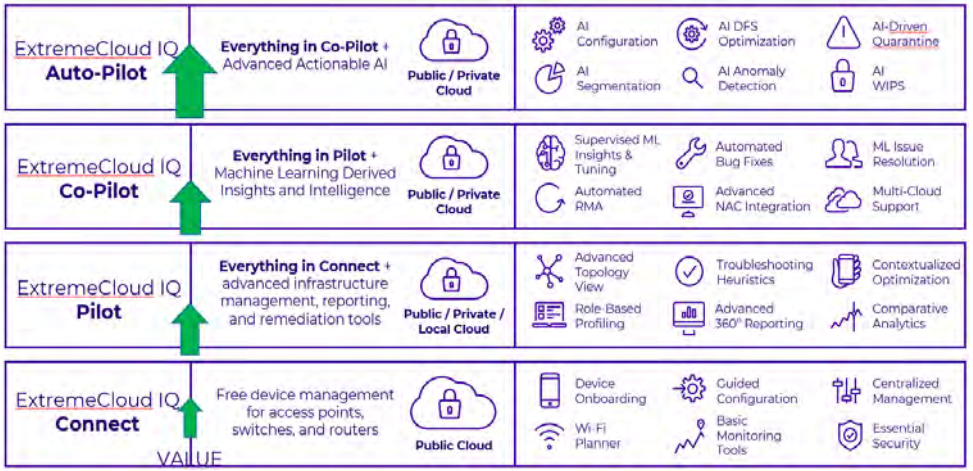
- ExtremeCloud IQ Connect
- ExtremeCloud IQ Pilot
- ExtremeCloud IQ Co-Pilot
- ExtremeCloud IQ Auto-Pilot
- Extreme Management Center : Agnostique des composants réseau

Technologies

- Machine Learning
- Intelligence Artificielle
- Règles basées sur les rôles à l'échelle du réseau global
- PSK – PPSK
- ZTP : Zero-Touch Provisioning

Besoins clients

- Gestion unifiée du réseau, du périmètre au Data center
- Déploiement flexible et évolutif, sans surcout
- Gestion des invités simple et sécurisée
- Visibilité applicative et des clients transitant sur le réseau
- Résolution des problèmes optimisée
- Automatisation de son réseau avancée
- NAC / SAM



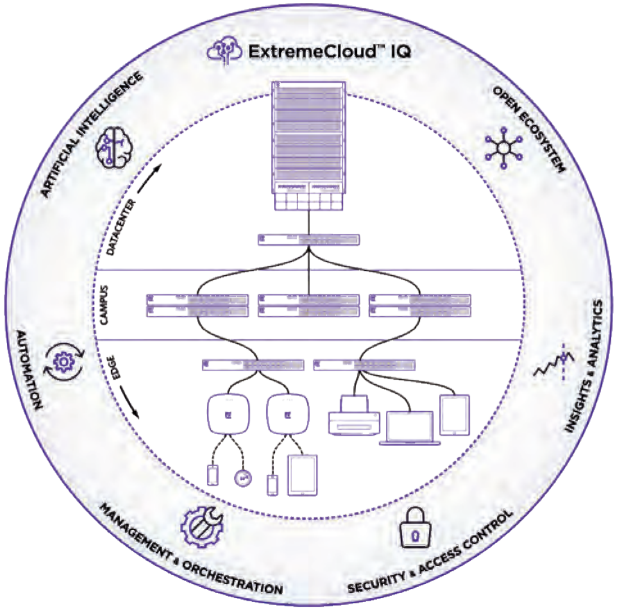
Arguments de vente

- Visibilité à 360° sur les clients, équipements et réseaux
- Gestion unifiée des politiques, du périmètre jusqu'au data center
- Indicateurs clés d'intégrité du réseau
- Déploiement et gestion des APs et switchs simplifiés au maximum
- Dernière technologie d'automatisation et d'orchestration grâce au Machine Learning et l'IA.
- Outils conçus pour favoriser la résolution des problèmes
- Support effectué par le partenaire ou directement par le GTAC d'Extreme Networks

Ligne Directe 01 60 19 02 30

Du Wi-Fi jusqu'au cœur du Data center

Extreme Networks continue d'innover technologiquement en proposant une gamme complète afin de construire son infrastructure réseau de la périphérie jusqu'au cœur du data center. Son offre composée d'AP Wi-Fi 6, de switch campus et de cœur de réseau Data Center est en constante évolution et s'adapte aux futurs besoins demandant plus de performance, de flexibilité, de simplicité à des coûts toujours plus optimisés. Associé à la plateforme de gestion agnostique du réseau Extreme Management Center / ExtremeCloud IQ, la solution est capable de s'adapter à une infrastructure réseau existante, de la gérer et de la faire évoluer simplement vers les dernières technologies réseau d'entreprise.



Gamme

- Wi-Fi 6 ou 5, intérieur ou extérieur, antennes internes ou externes
- Switch d'accès, d'agrégation, de branche, de cœur et data center
- Routeur campus, Data center et Service Provider

Technologies

- Wi-Fi 6, Dual 5 Go sélectionnable logiciellement
- Extreme Fabric Connect : Entre 4 et 10 protocoles réduit à 1
- Extreme OS : EXOS commun à toute la gamme switch
- QoS, authentification, sécurité
- SD-WAN, NAC / SAM

Besoins clients

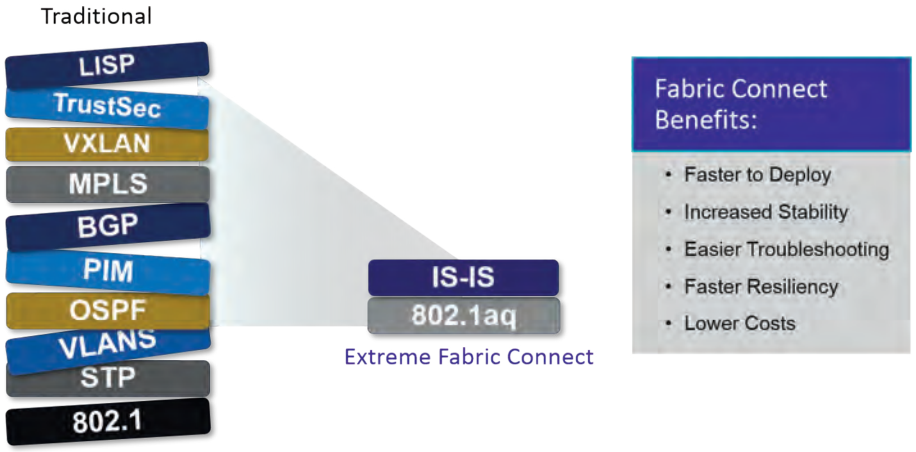
- Déploiement / Renouvellement en Wi-Fi 6
- Déploiement / Renouvellement du réseau filaire d'accès ou data center
- Déploiement d'un nouveau site distant éphémère ou permanant
- Télétravail ou E-learning
- Gestion des politiques de sécurités unifiées

Arguments de vente

- Wi-Fi nouvelle génération ultra performant (802.11ax), intérieur et extérieur
- Construction de l'infrastructure réseau du périmètre jusqu'au Data center
- Plateforme de gestion globale du réseau en Cloud grâce à ExtremeCLoud IQ avec ML et IA
- Plateforme de gestion globale agnostique du réseau avec XMC, on-premise
- Performance Wi-Fi équivalente au filaire

Extreme Fabric Connect

L'entreprise moderne exige de l'agilité, une connectivité évolutive et résiliente et une sécurité réseau inhérente, mais sans la complexité des réseaux traditionnels. **Extreme Fabric Connect** (basé sur le pontage de chemin le plus court amélioré / IEEE 802.1 aq) représente une nouvelle façon de concevoir, de construire et d'exploiter des réseaux. Celui qui offre simplicité et agilité tout en améliorant la sécurité et la stabilité.



Gamme

- Physique ou virtuel
- Switch campus de 8 à 48 ports / Cœur de réseau
- Campus avec ports 1Go, 10 Go ou Multi Gigabit / Data center : 25 Go, 40 Go, 100 Go
- Châssis fixes ou modulables
- POE et/ou stackable
- Management par ExtremeCloudIQ, Extreme Management Center (XMC) ou ligne de commande.

Technologies

- Extreme Fabric Connect IEEE 802.1aq / IETF 632

Besoins clients

- Création d'un réseau virtuel flexible et agile
- Déploiement automatisé pour de nouveaux switchs et simplifié pour de nouvelles applications
- Interconnexion avec des points d'accès Wi-Fi, full POE
- Management de son réseau globalisé à travers une interface

Switch Model	Max Active 10/100/1000 BASE-T Ports	Max Active 1/2.5 GbE SFP Ports	Aggregated Switch Bandwidth	Frame Forwardind Rate
X435-8T-4S	8	4	36 Gbps	26.8 Mpps
X435-8P-4S	8	4	36 Gbps	26.8 Mpps
X435-8P-2T-W	10	-	20 Gbps	14.9 Mpps
X-435-24T-4S	24	4	68 Gbps	50.6 Mpps
X-435-24P-4S	24	4	68 Gbps	50.6 Mpps

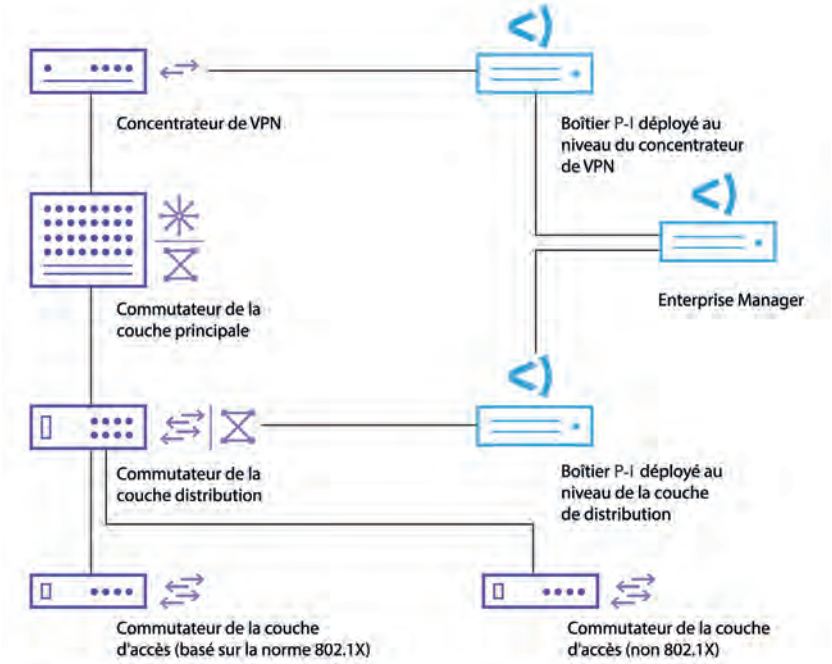
Switch Model	Max PoE Budget
X435-8P-4S	124W
X435-8P-2T-W	100W*
X435-24P-4S	370W

Arguments de vente

- Facilité/rapidité de déploiement grâce au Zero Touch Provisioning (ZTP)
- Automatisation de nombreux processus réseau : Déploiement de nouvelles applications plus rapidement
- Amélioration de la sécurité grâce aux technologies inhérentes aux switchs : Isolation des IoT, blocage des mouvements latéraux, etc
- Amélioration de la stabilité grâce à la diminution drastique du nombre de protocoles réseaux

Contrôle d'accès au réseau LAN et Wi-Fi

ForeScout Technologies est l'un des principaux fournisseurs de solutions de gestion d'accès aux réseaux. ForeScout permet aux utilisateurs d'accéder aux ressources réseau de l'entreprise là où ils en ont besoin et quand ils en ont besoin, sans compromettre la sécurité. La solution permet d'identifier, d'évaluer, de prévenir et de résoudre dynamiquement les risques de sécurité tels que : utilisateurs indésirables et inconnus, appareils et applications inconnus, systèmes non gérés et non sécurisés, comportements malveillants et non-respect de la politique de sécurité. La solution permet en plus de définir et de mettre en œuvre une segmentation globale du réseau pour sécuriser les infrastructures de plus en plus complexes et interconnectées des campus, aux datacenters en passant par le Cloud et les technologies opérationnelles (OT).



Gamme

5 licences disponibles pour un déploiement en Appliance ou en VM :

- **eyeSight** (visibilité)
- **eyeSegment** (Segmentation)
- **eyeControl** (contrôle d'accès)
- **eyeManage** (management)
- **eyeRecover** (haute disponibilité)

Technologies

- Sans Agent
- Non Intrusif
- BYOD
- Visibilité IT/OT
- Contrôle d'accès

Besoins clients

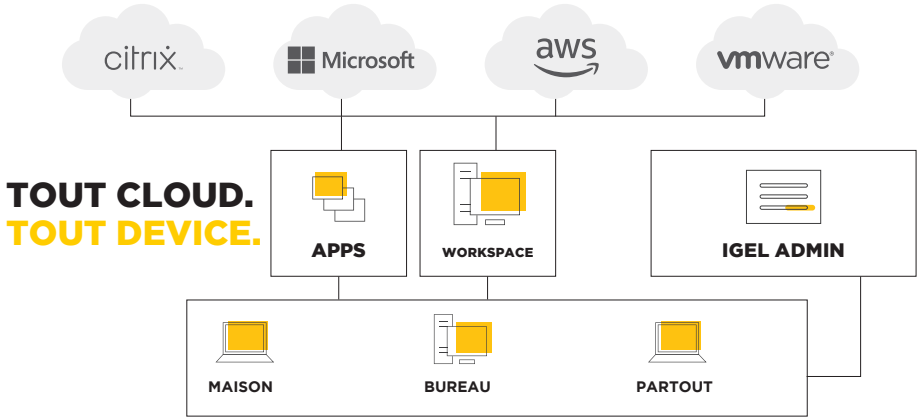
- Visibilité complète à travers l'ensemble du périmètre de l'entreprise : IT et OT
- Sécurisation du LAN, WLAN, ICS/SCADA, IoT et IIoT
- Avoir un contrôle total des équipements connectés sur son réseau
- Contrôler le BYOD
- Réduire les risques et maitriser les menaces

Arguments de vente

- Déploiement sans agent
- Simple à mettre en œuvre
- Solution non intrusive
- Contrôle évolutif des appareils mobiles
- Solution extensible
- Agnostique de l'infrastructure existante
- Sécurisation des équipements mobiles et du BYOD
- Intégration avec l'écosystème de sécurité existant
- Partenariat fort avec Palo Alto Networks et McAfee

Transformer tout poste en client ultra-léger pour les workspaces du Cloud

IGEL propose aux utilisateurs un endpoint ultra-léger, sécurisé, puissant et facile à administrer. IGEL OS transforme n'importe quel client léger ou appareil compatible x86-64 en un endpoint piloté par logiciel et complètement géré par l'entreprise. IGEL OS peut remplacer l'O/S d'un poste qu'on souhaite recycler ou uniformiser, ou on peut le substituer temporairement (au boot) sur un poste compatible, comme sur le poste personnel d'un employé en télétravail par exemple. Ainsi équipé, l'utilisateur peut effectuer toutes ses tâches à partir des applications SaaS ou des bureaux virtuels VDI ou DaaS (Citrix, Microsoft, VMware, Google, Amazon...) mis à disposition par l'entreprise dans un cloud privé ou public.



Gamme

- **IGEL Workspace Edition** (licence user/device perpétuelle) avec **Maintenance obligatoire** 1, 2 ou 3 ans, renouvelable. **UMS inclus** (Universal Management Suite) : gestion et contrôle centralisés
- **Enterprise Management Pack** : ajoute IGEL Cloud Gateway pour le contrôle et la gestion des postes non connectés directement au réseau de l'entreprise (souscription 1, 2 ou 3 ans pour le nombre de postes concernés)
- **IGEL UD POCKET2** : pour transformation temporaire d'un poste compatible en client ultraléger IGEL par un démarrage à partir d'une clé USB

Besoins clients

- Uniformiser et contrôler le poste de travail de l'utilisateur pour maximiser le R.O.I de la migration des espaces de travail dans le Cloud (SaaS, DaaS, VDI).
- Transformer ou prolonger la durée de vie de PCs et clients légers au lieu de réinvestir dans des postes sur des projets VDI et DaaS
- Utiliser le matériel personnel de l'employé pour la mise en œuvre rapide du télétravail
- Maintenir des postes utilisateurs en opération en cas d'attaque par ransomware

Technologies

- Système d'exploitation client ultra-léger
- Parfait pour VDI, SaaS et DaaS
- Base Linux très sécurisée
- IGEL OS Creator / clé USB UD POCKET

Arguments de vente

- Satisfaire l'utilisateur : support de toutes les solutions VDI, DaaS, SaaS, des clients légers tiers et de tous les périphériques clients nécessaires (Plus de 110 partenaires technologiques IGEL Ready).
- Réduire les coûts : recycler et étendre la durée de vie des postes ; gérer Windows sur le bureau virtual, pas sur les postes ; aucun agent à gérer sur le poste ; travailler sur des postes avec seulement 2GB de RAM et 2GB de stockage
- Gagner en efficacité : interface utilisateur ultra simple ; une seule administration, à l'échelle de l'entreprise ; portabilité grâce au boot à partir de la clé optionnelle USB IGEL UD POCKET2
- Garantir la sécurité : O/S sécurisé modulaire en lecture seule ; pas de virus, pas de ransomware ; O/S exécuté dans la mémoire, un poste neuf retrouvé à chaque reboot.

Ligne Directe 01 60 19 02 30

Combiner IGEL OS avec un matériel client léger spécialement conçu

Vous pouvez combiner le software IGEL avec le hardware IGEL afin de proposer une expérience familière et fluide avec une sécurité et des performances optimales. Les matériels IGEL sont adaptés à un grand nombre de cas d'usage, du simple accès à Internet et aux applications de bureau comme un client léger classique aux plateformes d'espaces de travail du Cloud pour les workloads des utilisateurs les plus exigeants..

Gamme

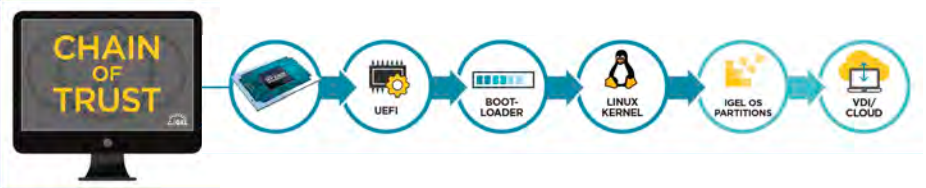
- **UD2, UD3 ou UD7 :** UD2, solution économique pour les besoins les plus simples d'accès à Internet, aux applications de bureaux et aux environnements VDI de l'entreprise. Pour des besoins plus importants en termes de tâches graphiques, on choisira l'UD3 (lecture vidéo 4K par exemple) ou UD7 (production vidéo, CAD/CAM...).
- **Licences IGEL Workspace Edition et Maintenance** (1-3 ans) par device à prévoir

Technologies

- IGEL OS
- Hardware client ultraléger
- UMS Universal Management Suite
- Connectivités sans fil selon modèles
- Refroidissement sans ventilateur

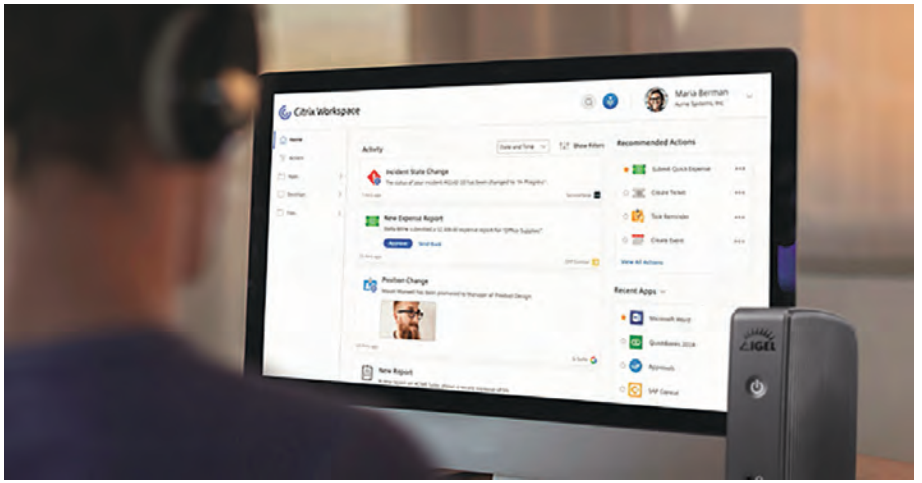
Besoins clients

- Equiper les employés d'un poste facile à déployer, à sécuriser et à manager, pour l'accès aux applications et environnement Cloud (VDI, SaaS, DaaS).



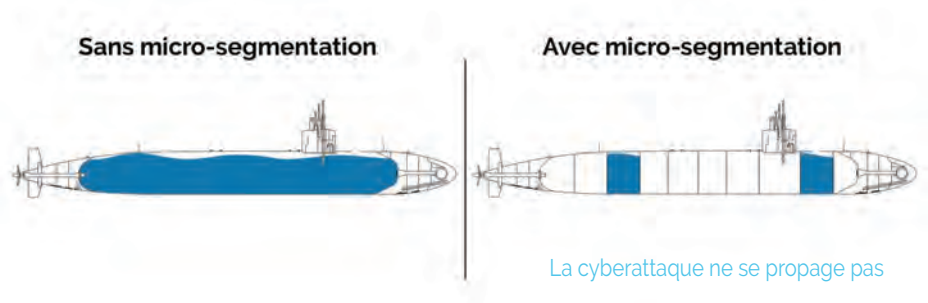
Arguments de vente

- Equipé avec IGEL OS, sa "chaine de confiance" et son administration centralisée
- Gamme réduite avec modèles et options de connectivité adaptés aux principaux cas d'usage VID et DaaS
- Extension de garantie à 5 ans par simple enregistrement
- Gestion de Windows sur l'environnement virtuel, pas sur les postes
- Support assuré par le constructeur
- Coût total de possession réduit



Limiter l'impact des ransomwares grâce à la micro-segmentation

La micro-segmentation est une technique de sécurité qui divise en segments les environnements clouds et data centers jusqu'à la charge applicative. Plus granulaire et plus profond, donc, que la segmentation réseau des firewalls. La micro-segmentation détache la segmentation du réseau en tirant parti du firewall de l'hôte pour appliquer les règles aux communications Est-Ouest en plus du Nord-Sud.



Besoins clients

- Réduire la surface d'attaque : visibilité et contrôle sur les accès par mouvement latéral
- Assurer la conformité réglementaire : isoler les systèmes sensibles pour leur appliquer les règles nécessaires
- Améliorer la lutte contre les brèches : superviser le trafic et contenir les mouvements latéraux

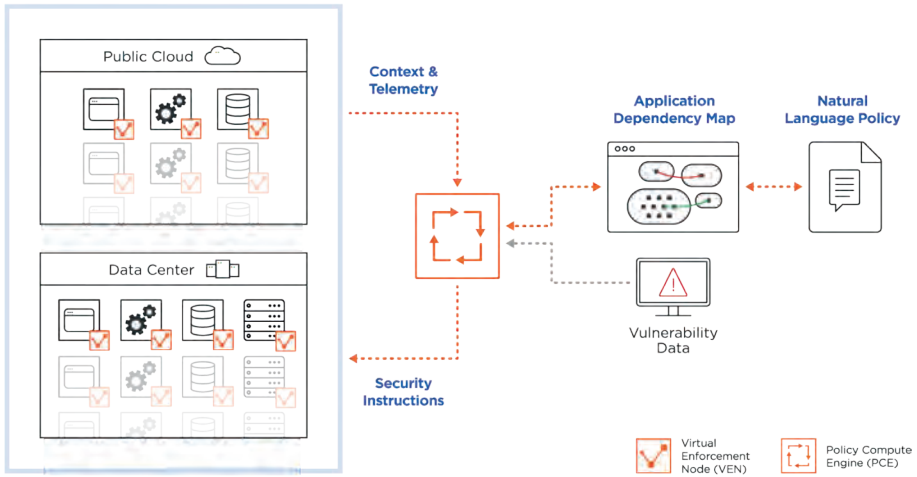
Gamme

- **Illumio Core** (pour les environnements cloud et data center)
- **Illumio Edge** (pour les endpoints)

Technologies

- Micro-segmentation
- Segmentation basée host
- Segmentation de sécurité
- Zero-Trust
- Mouvements latéraux Est-Ouest

Illumio récupère les infos des environnements via des agents (VEN -Virtual Enforcement Node) pour établir une carte à partir de laquelle on visualise ce qui doit être protégé et mettre en place des règles automatisées de segmentation avec des instructions en langage naturel (PCE -Policy Compute Engine).



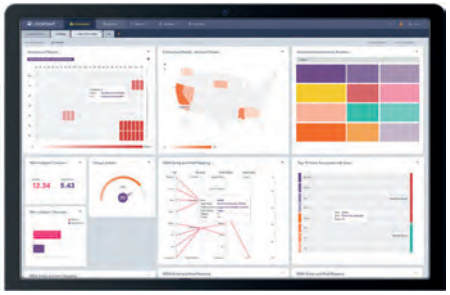
Arguments de vente

- Pour compléter la segmentation réseau et aller plus en profondeur
- Modèle de déploiement flexible : cloud Illumio ou on-premises (logiciel ou appliance virtuelle)
- Installation des agents partout : sur serveur bare-metal, machine virtuelle, container, instance cloud public
- Langage naturel basé sur 4 dimensions -rôle, application, environnement et lieu (non pas VLAN, zones, sous-réseaux, IPs...). Possibilité d'utiliser les éléments de systèmes tiers CMDB, IPAM, orchestration...
- Règles rédigées manuellement ou avec un générateur fourni.
- Administration via interface Illumio ou des systèmes tiers grâce aux APIs.

LOGPOINT

Solution SIEM unifiée, simple, performante et accessible

LogPoint, pionnier européen du SIEM nouvelle génération, est une société Danoise présente sur le marché depuis 2008.
À ce jour, près de 300 clients à travers l'Europe font confiance à LogPoint. La technologie de la plateforme a été conçue pour gérer sans effort le Big data.
Les utilisateurs de LogPoint apprécient sa facilité de gestion et d'utilisation (adaptation, anticipation, conformité, Défense…).
LogPoint est la plate-forme la plus flexible pour collecter, analyser et surveiller toutes les données, qu'elles soient générées par des applications, des bases de données, des infrastructures ou qu'elles concernent des actifs sensibles, des systèmes industriels ou des systèmes de sécurité.



Gamme

- Dimensionnement en fonction du nombre de nœuds (de 25 à >1000)
- 3 gammes d'appliances physiques : Standard, Pro et Pro XL

Technologies

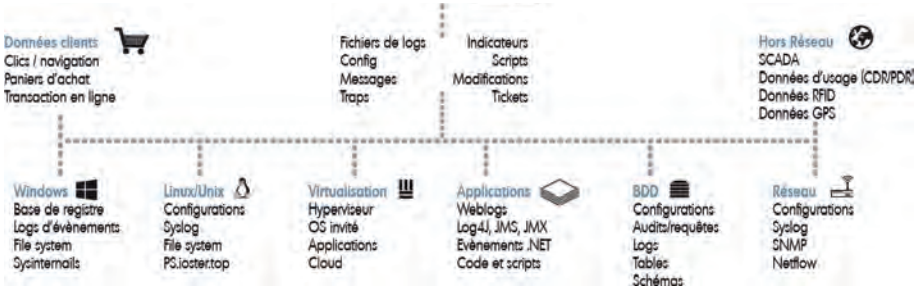
- Serveurs
- AD
- Base de données
- SAP
- AS400
- Firewall
- Equipements réseaux
- Scada
- Postes de travails
- (Amazon, Azure, Office 365)

Besoins clients

- Gérer la sécurité
- Centraliser l'info de l'ensemble de l'infra
- Suivi de la politique de sécurité
- Conformité (ISO27001, GDPR, LPM, Données de Santé,…)
- Alerting et reporting
- Corrélation d'évènements de sécurité

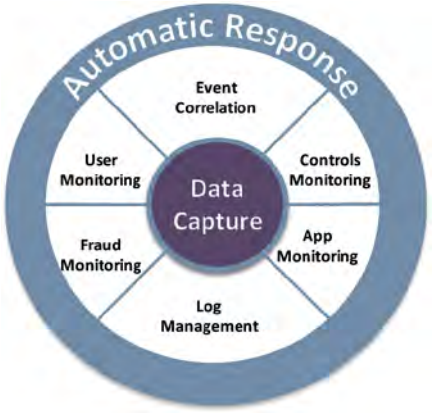
LogPoint se veut agnosique et récupère tous les logs de tous les systèmes d'information. Si la normalisation n'existe pas encore, LogPoint, gratuitement, fait le développement sous 8 jours.

LOGPOINT



Arguments de vente

- Facile à installer et à utiliser au quotidien
- Log Management & SIEM Européen
- Certifié EAL3+
- Licensing prédictif à l'IP, indépendamment du volume !
- Normalisation sous 8 jours intégrée à la licence
- Threat Intelligence (Critical Stack &Emerging Threat)



Management à distance, sécurisé et intelligent

Opengear fournit une solution de gestion hors bande (OOB -Out-of-Band) sécurisée. La solution offre un chemin alternatif à vos équipements à distance, et ce, même en cas de défaillance du réseau principal. Séparée du réseau de production, elle permet aux administrateurs de surveiller, d'accéder à tous les dispositifs et de les gérer en toute sécurité sans aucun impact sur la production.

Les points forts

Failover to Cellular : Bascule vers le réseau cellulaire 4G LTE en cas d'indisponibilité du WAN

Zero Touch Provisioning : déploiements simplifiés, tâches automatisées, moins d'erreur

Smart Out-of-Band : connectivité intelligente, identification rapide et correction proactive des erreurs sur les équipements.

Administration centralisée Lighthouse : vue et gestion de tous les équipements de votre réseau même injoignables

Gamme

- Infrastructure Manager IM7200
- Console Manager CM7100
- Resilience Gateway ACM7000-L
- Remote Site Gateway ACM7000

Technologies

- Console management 2.0
- Smart Out-of-Ban
- Zero Touch Provisioning
- Redondance 4G
- Docker container
- Lighthouse
- NetOps
- VPN

Besoins clients

- Déploiements SD-WAN
- Construction ou refresh de datacenters
- Automatisation NetOps (Networks Operation)
- Connectivité et management des sites distants

Arguments de vente

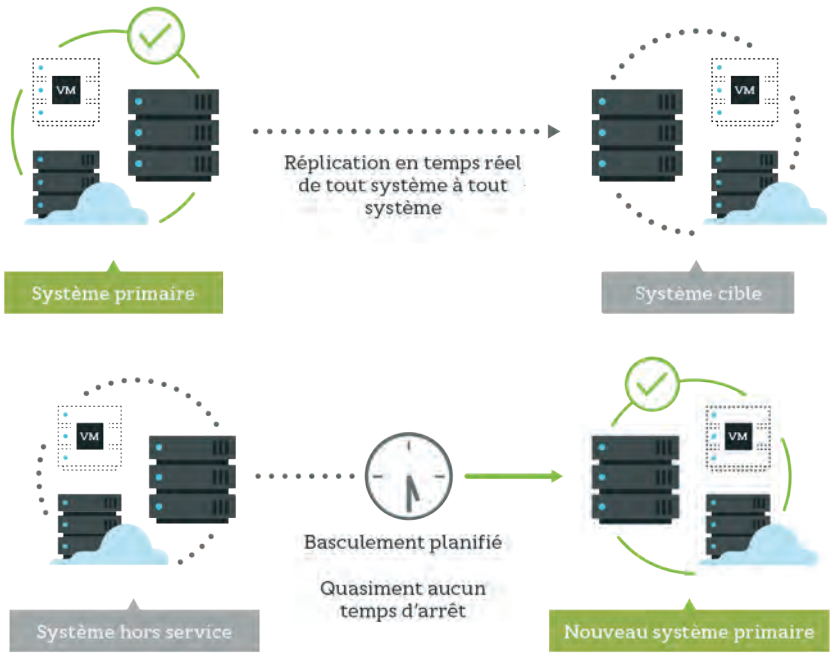
- Opengear automatise et simplifie les configurations des équipements distants
- Console de management sécurisée, avec une solution « On Premises ».
- Installation « transparente » dans les infrastructures existantes
- Complémentaire aux solutions SD-WAN avec la gestion intelligente OOB.
- Remédie aux problèmes identifiés via un accès Série-over-IP ou VPN.
- Surveille les environnements DataCenters avec gestion intelligente des PDU
- Simplifie les migrations des infrastructures IT.

opentext™
Security Solutions

Solution complète de protection des données

Carbonite offre une gamme complète de solutions pour la sauvegarde Cloud, sur site ou hybride des serveurs physiques, des environnements virtualisés et des postes de travail.

Mais plus globalement, Carbonite propose toutes les solutions de la simple sauvegarde dans le cloud au PRA as-a-service, en passant par les migrations de données ou les réplications hautement disponibles de VM.

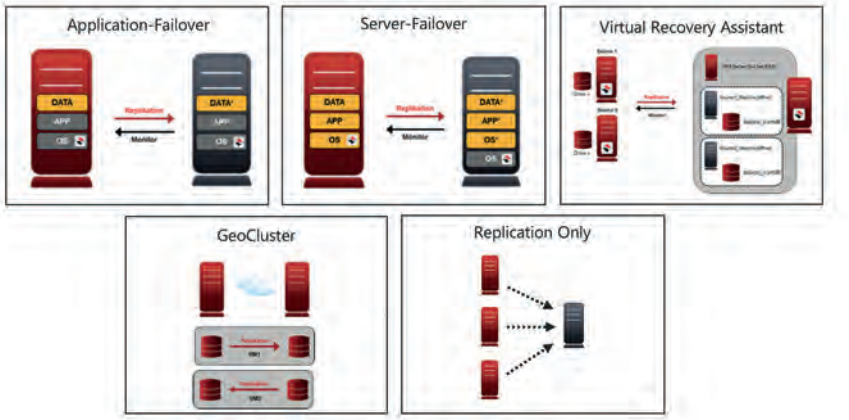


Gamme

- Carbonite Server
- Carbonite Availability
- Carbonite Move
- Carbonite EndPoint

Besoins clients

- Sauvegarde des serveurs physiques et/ou des serveurs virtuels (VMware, HyperV, KVM etc…)
- Sauvegarde des postes de travail (Windows, Mac, Linux…)
- Sauvegarde sur site, dans un data centre externe en mode Cloud, projet hybride
- Réplications des VMs en Haute Disponibilité, toute combinaison source/destination entre VMware, HyperV, KVM ou autre
- Réplication de serveurs physiques vers serveurs physiques ou virtuels
- Projet de Migration de données : sur un site, inter-sites, du site client vers le Cloud, etc…



Arguments de vente

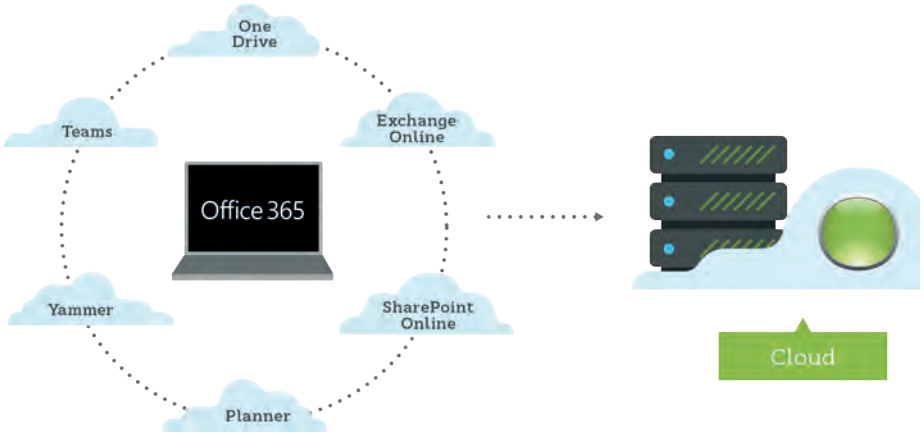
- Technologie éprouvée, car gérant plus de 300Po de données dans ses data centers pour la sauvegarde Saas vendue à ses clients
- Portail unique accueillant les différentes solutions de sauvegarde et réplication
- Très large richesse fonctionnelle pour s'adapter à tous les environnements source et cible existants
- Solutions offrant les meilleurs temps de sauvegarde et restauration
- Nécessite des infras de stockage 2 à 3 fois moins lourdes que les solutions concurrentes

opentext™
Security Solutions

Solution de sauvegarde pour optimiser Office 365

Carbonite Backup for Office 365 est issue d'un partenariat entre Microsoft et Carbonite, afin de compléter et optimiser la sauvegarde/restauration proposée par Office 365.

C'est une solution 100% Cloud pour garantir une véritable sauvegarde de TOUS les services d'Office 365 (dont Teams, Planner, SharePoint etc…), une restauration rapide et totalement granulaire, et tous les outils nécessaires à la sécurisation des données et la conformité RGPD.



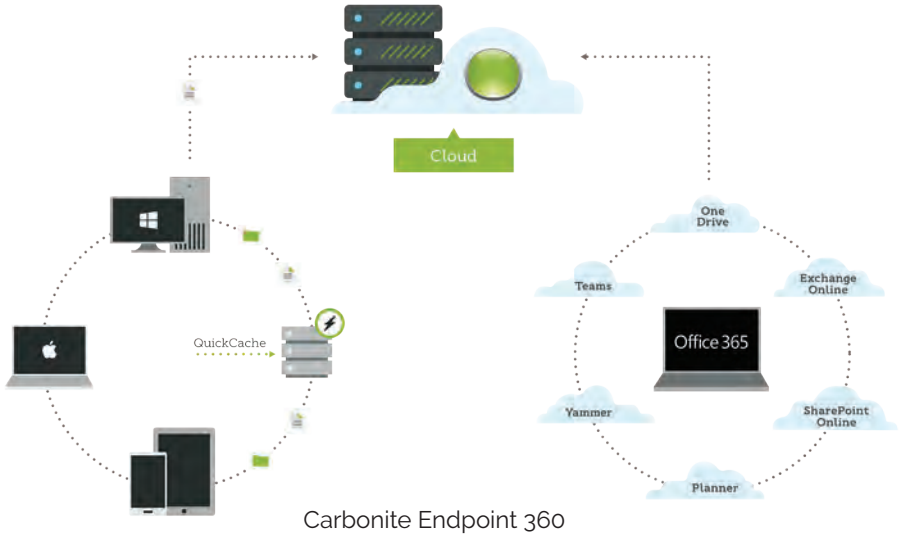
Gamme

2 Editions de Carbonite Backup for Office 365
- Standard Edition : Souscription 1 ou 3 ans par siège, capacité mutualisée de stockage de 100Go par user
- Advanced Edition : Souscription 1 ou 3 ans par siège, capacité de stockage illimitée

Bundle Endpoint Protection :
- **Carbonite EndPoint 360 Standard Edition** : bundle par siège d'une souscription Carbonite Backup for Office365 Standard Edition et d'une souscription Carbonite EndPoint pour la sauvegarde des données hors Office365
- **Carbonite EndPoint 360 Advanced Edition** : bundle par siège d'une souscription Carbonite Backup for Office365 Advanced Edition et d'une souscription Carbonite EndPoint pour la sauvegarde des données hors Office365

Besoins clients

- Vraie sauvegarde avec historisation sur 1 ou 2 ans, jusqu'à 4 fois par jour (pas uniquement la gestion de la corbeille pendant 30 jours proposée par Office365)
- Sauvegarde et restauration rapide de tous les éléments d'Exchange O365, mais aussi Teams, Planner, SharePoint, OneDrive, Project, Groups, Yammer etc…
- Propriété des données, souveraineté des données (France)
- Gestion simplifiée des utilisateurs quittant la société : élimination de ses données pour le droit à l'oubli, restauration aisée et rapide si suppression malveillante des données
- Restauration pendant une potentielle interruption de service Office 365,



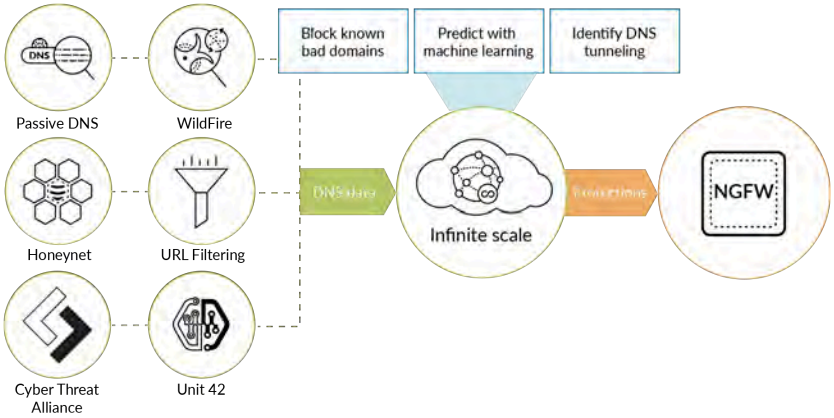
Carbonite Endpoint 360

Arguments de vente

- Solution 100% Cloud (prix incluant déjà le matériel provisionné par Carbonite pour la sauvegarde dans son Cloud)
- Cloud Carbonite en géolocalisation garantie chez Azure France
- Restauration granulaire : un email seul, une pièce jointe seule, 1 fichier seul sous SharePoint, restauration des permissions seules si elles ont été modifiées sans changer le contenu, restaurations indépendantes sous Teams des conversations, fichiers, tableaux de planification, groupes etc…
- Clés de chiffrement privées

Plateforme de sécurité nouvelle génération

Palo Alto Networks propose une plateforme unique de prévention contre les menaces connues et inconnues. Par un contrôle granulaire de l'utilisation des applications, en identifiant chaque composant clé d'une menace et en partageant l'information, la plateforme Palo Alto Networks offre une protection à chaque phase du cycle d'une cyber-attaque, au niveau du réseau physique, dans le data center virtuel, dans le cloud et jusqu'au poste de travail. Composée du firewall nouvelle génération inventé par Palo Alto Networks, d'une intelligence cloud de détection des menaces inconnues et d'une solution avancée de protection du poste client, la plateforme permet de réduire à zéro la surface d'exposition aux risques et maintenir en permanence la conformité et l'efficacité du système d'information.

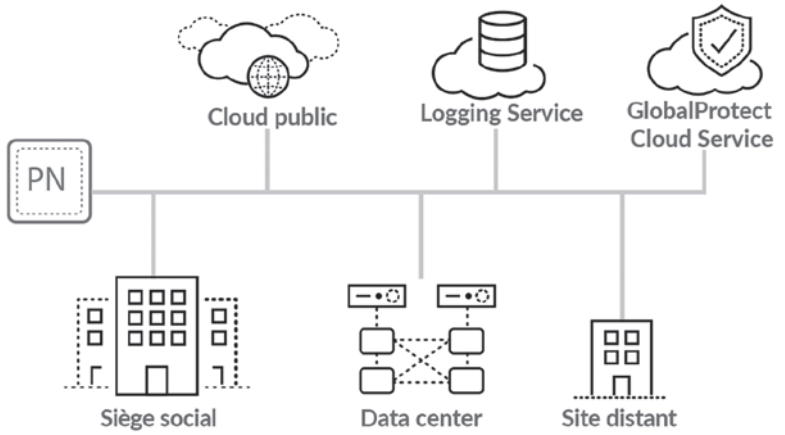


Gamme

- **Gamme matérielle de firewalls** PA-220, PA-800, PA-3000, PA-5000, PA-5200 et PA-7000
- **Versions virtuelles VM-Series** (ESX, NSX, Hyper-V, KVM (NetScaler), AWS, Azure)
- **Panorama** : reporting et management centralisés (appliance physique ou machine virtuelle)
- Licences de **filtrage URL** et **Prévention de menaces**
- **Global Protect** : contrôle des utilisateurs distants, mise en conformité du poste des utilisateurs
- **WildFire** intelligence cloud contre les malwares et les vulnérabilités inconnus
- **Traps** pour la protection avancée des postes clients
- **Autofocus :** solution de reporting et de gestion analytique des menaces
- **Prisma SaaS :** Solution de contrôle des services cloud

Besoins clients

- Se protéger contre les malwares modernes
- Identification et règles de contrôle des applications et des utilisateurs
- Déchiffrement, identification et contrôle des applications chiffrées
- Contrôle des utilisateurs distants
- Contrôle des services cloud
- Protection avancée du poste client



Arguments de vente

- Visibilité de toutes les applications, y compris celles qui changent dynamiquement de port, sont chiffrées ou n'utilisent pas de port standard
- Protection native contre TOUTES les attaques et de tout type (exploits, logiciels malveillants, DNS, « command and control », et URL)
- Détection par la base installée et reprogrammation automatique de la protection en moins de 5 minutes pour toutes les plateformes déployées (30.000 clients)

Technologies

- Plateforme SP3 Single Pass Parallel Processing
- App-ID, User-ID technologies
- Traps
- Client VPN/SSL et Global Protect

Architecture SD-WAN avec connectivité et sécurité nativement intégrée

L'offre **SD-WAN** de Palo Alto Networks permet d'adopter facilement une architecture SD-WAN de bout en bout avec une sécurité et une connectivité intégrée de manière native.
En utilisant Prisma Access comme hub SD-WAN, il est possible d'optimiser les performances de l'ensemble de votre réseau. Cela minimise la latence et garantit la fiabilité, offrant ainsi une expérience utilisateur exceptionnelle dans les succursales.
Il est également possible d'utiliser le hub SD-WAN en tant que service, éliminant la complexité de la construction de votre Infrastructure hub SD WAN, ou mettre en place l'infrastructure hub SD-WAN sois-même et l'interconnecter en utilisant les pares-feux de nouvelle génération de Palo Alto Networks. Quel que soit votre modèle de déploiement, l'intégration étroite de toutes ces fonctionnalités permet de gérer la sécurité et le SD-WAN à travers une seule interface intuitive.

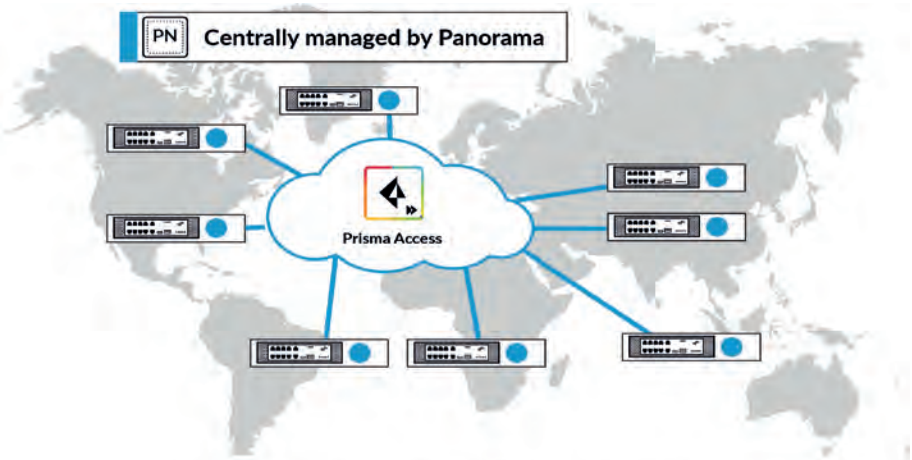


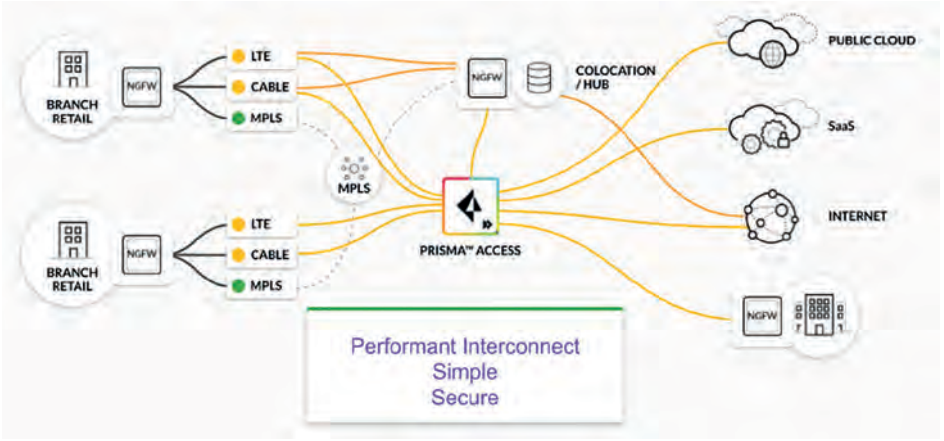
Figure 1: Palo Alto Networks SD-WAN cloud-based approach

Gamme

- Souscription **SD-WAN** à activer au niveau de toutes les Appliances physiques – version minimum supportée PAN-OS 9.1.
- **Prisma Access pour SD-WAN hub** : licence Prisma Access SD-WAN Branch Interconnect

Besoins clients

- Solution SD-WAN sécurisée
- Performances fiables
- Reduction de complexité
- Provisionning simple des sites distants
- Diminution des coûts



Arguments de vente

- Déploiement du SD-WAN en toute sécurité grâce à des fonctionnalités de sécurité intégrée nativement dans les solutions de Palo Alto ;
- Expérience utilisateur exceptionnelle en utilisant Prisma Access comme Hub SD-WAN pour optimiser les performances ;
- Gestion centralisée de la connectivité et la sécurité via la console Panorama
- Déploiement simplifié des sites distants grâce à la fonctionnalité « Zero touch Provisionning »
- Options de déploiement flexible : mesh, hub and spoke, cloud.

Technologies

- Collecte des métriques relatives aux lien, latence, perte de paquets et gigue
- Sélection intelligente du chemin en se basant sur les métriques
- Agrégation de liens basée sur la session
- Qualité de service et Traffic Shaping
- Tunnels IPsec et Hub and Spoke avec configuration et visualisation automatique
- Haute disponibilité SD-WAN en mode Actif/Passif

Plateforme de sécurité nouvelle génération

L'offre **Strata** s'appuie sur le meilleur firewall nouvelle génération du marché auquel s'intègrent des innovations constantes sous forme de souscription. Palo Alto Networks propose une plateforme unique de prévention contre les menaces connues et inconnues. Par un contrôle granulaire de l'utilisation des applications, en identifiant chaque composant clé d'une menace et en partageant l'information, la plateforme Palo Alto Networks offre une protection à chaque phase du cycle d'une cyber-attaque, au niveau du réseau physique, dans le data center virtuel, dans le cloud et jusqu'au poste de travail. Composée du firewall nouvelle génération inventé par Palo Alto Networks, d'une intelligence cloud de détection des menaces inconnues et d'une solution avancée de protection du poste client, la plateforme permet de réduire à zéro la surface d'exposition aux risques et maintenir en permanence la conformité et l'efficacité du système d'information.

Gamme

- Firewalls matériels : PA-220, PA-800, PA-3200, PA-5200 et PA-7000
- Versions virtuelles VM-Series (ESX, NSX, Hyper-V, KVM (NetScaler), AWS, Azure)
- Reporting et management centralisés (appliance physique ou machine virtuelle)
- Licence Threat Prevention
- Licences de filtrage URL
- Licence WildFire
- DNS Security
- SD-WAN
- GlobalProtect™

Technologies

- Plateforme SP3 Single Pass Parallel Processing
- Technologies APP-ID, USER-ID et CONTENT-ID
- Client VPN/SSL et Global Protect
- Intelligence analytique dans le cloud de détection des menaces inconnues

Besoins clients

- Protection contre les malwares modernes
- Identification et règles de contrôle des applications et des utilisateurs
- Déchiffrement, identification et contrôle des applications chiffrées
- Contrôle des utilisateurs distants
- Contrôle des services cloud

Palo Alto Networks, leader mondial de la cybersécurité

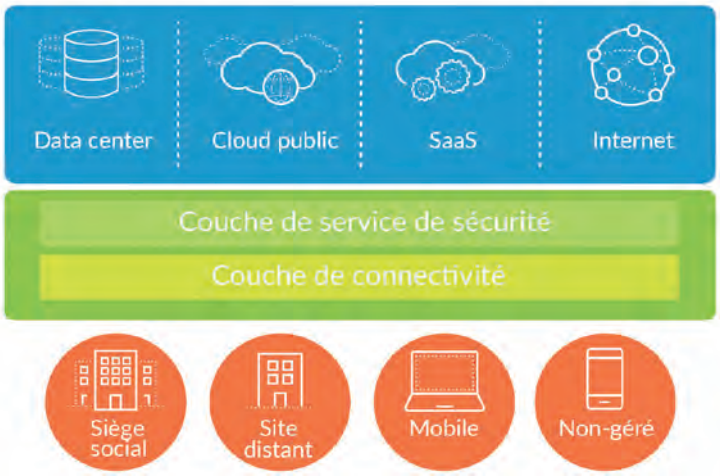
Arguments de vente

- Visibilité de toutes les applications, y compris celles qui changent dynamiquement de port, sont chiffrées ou n'utilisent pas de port standard
- Protection native contre TOUTES les attaques et de tous types (exploits, logiciels malveillants, DNS, « command and control », et URL)
- Détection par la base installée et reprogrammation automatique de la protection en moins de 5 minutes pour toutes les plateformes déployées (30000 clients)

Accès sécurisé pour les utilisateurs mobiles et sites distants

Prisma Access offre une protection directement depuis le cloud pour sécuriser les accès. Il combine connectivité et sécurité pour tous les utilisateurs où qu'ils se trouvent. Prisma Access offre une protection contre les cyberattaques, en appliquant les politiques de sécurité de manière homogène à chaque emplacement, même si ni l'application ni l'utilisateur ne sont sur votre réseau.

La protection automatisée et complète bloque les malwares connus et inconnus, les exploits, les vols d'identifiants, les activités de commande et contrôle et bien d'autres vecteurs d'attaques, sur tous les ports et pour tous les protocoles. Conçu dans le cloud pour le cloud, Prisma Access couvre les sites distants et les utilisateurs mobiles partout dans le monde grâce à sa couche de connectivité.



Gamme

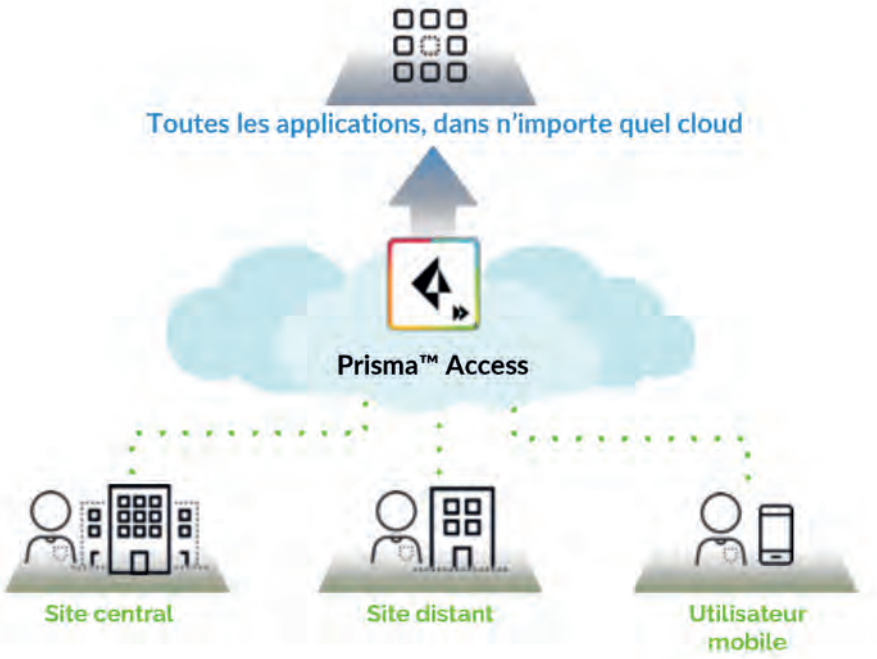
- **Prisma Access** pour sites distants
- **Prisma Access** pour utilisateurs mobiles.

Technologies

- +100 DC Palo Alto Network dans plus de 70 Pays.
- Connexion au point de présence PoP le plus proche.

Besoins clients

- Sécurité flexible, agile et évolutive
- Sécuriser les équipes mobiles travaillant dans le cloud
- Sécuriser des succursales connectées au cloud
- Gérer et sécuriser des changements des stratégies WAN (connexions MPLS vers du SD-WAN)



Arguments de vente

- Pas besoin de configurer et de préparer du matériel, ni de l'envoyer aux quatre coins du monde
- Déployer une protection partout, en quelques minutes
- Solution évolutive
- Facilité de mise en œuvre d'un nouveau site avec les mêmes politiques de sécurité que les autres
- Les changements de politique sont mis en œuvre automatiquement dans le cloud : Plus besoin d'appliquer les modifications et validations jusqu'à la périphérie.
- Options de déploiement flexible : mesh, hub and spoke, cloud.

Sécuriser les applications SaaS avec Prisma SaaS

L'utilisation des applications SaaS (Software as a Service) apporte de nouveaux risques et zones d'ombre dans le réseau d'une entreprise. Le SaaS peut être un vecteur de propagation menaces, de fuites de données ou de non-conformité réglementaire. **Prisma SaaS** offre une visibilité complète et un contrôle granulaire pour toutes les activités des utilisateurs sur les fichiers stockés dans les applications Saas « sanctioned » (contractualisées par l'IT : o365, box …), en fournissant une analyse détaillée de l'utilisation de ces applications, sans nécessiter de modifications matérielles, logicielles ou réseaux supplémentaires. Avec des fonctionnalités étendues de contrôle du SaaS sur la plate-forme Palo Alto Networks, la protection des données dans le cloud devient possible.

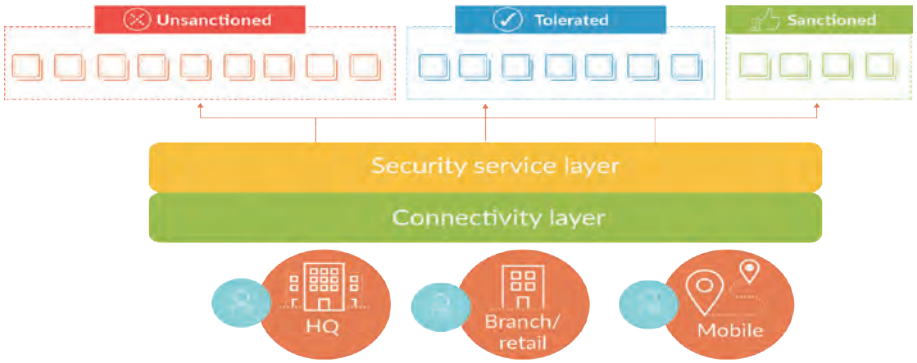


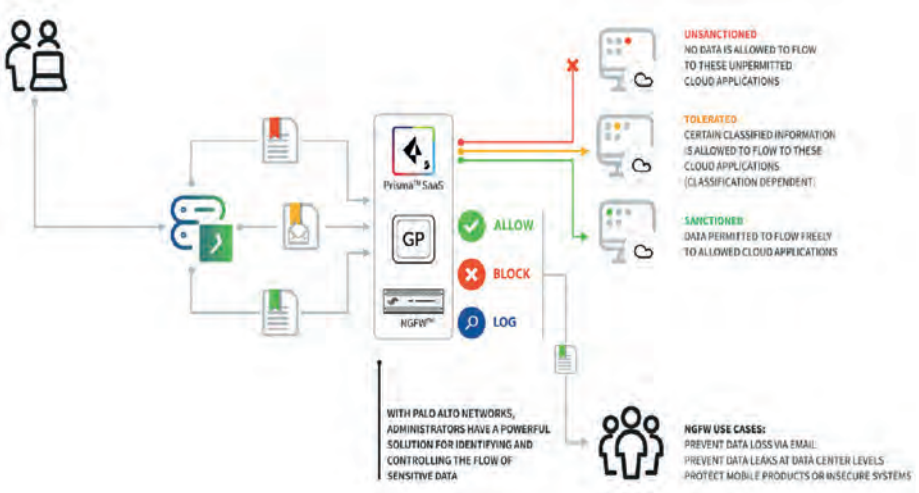
Figure 1: Cloud-delivered CASB approach

Gamme

- **API Prisma SaaS**
- Service pour toutes les applications SaaS supportées

Besoins clients

- Prévention de la menace sur le SaaS
- Visibilité sur l'exposition de vos données
- Contrôle contextuel de l'exposition des données
- Sécurité automatisée étendue au SaaS



Arguments de vente

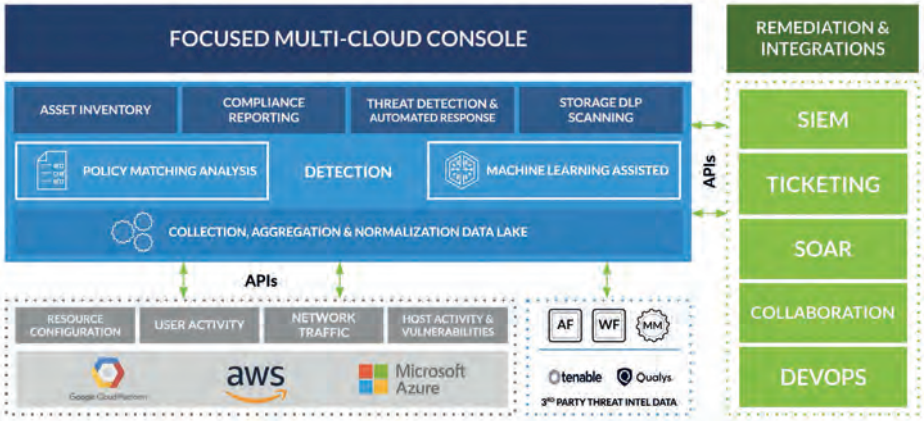
- Visibilité complète sur tous les utilisateurs et activités des dossiers et fichiers, permettant de savoir exactement ce qui se passe à n'importe quel moment dans le temps
- Analyse rétroactive de l'exposition des données et des créations des comptes SaaS
- Analyse approfondie de l'utilisation quotidienne du SaaS qui permet de déterminer rapidement si l'entreprise s'expose à des problèmes de conformité règlementaire
- Politique de contrôle granulaire et contextuelle qui permet de mettre en quarantaine les utilisateurs ou les données dès qu'un problème survient
- Protection avancée contre les menaces pour bloquer les malwares connus et identifier et bloquer les malwares inconnus

Technologies

- API sur le service cloud sans impact sur la performance
- Prévention de la menace grâce à l'intégration avec WildFire
- Moteur de DLP
- Intégration sur 30+ applications

Sécuriser les déploiements cloud

Prisma Cloud est un service de conformité et de sécurité qui identifie de manière dynamique les ressources du cloud et les données sensibles. Il détecte ensuite les configurations risquées, les menaces réseau, les activités suspectes des utilisateurs, les malwares, les fuites de données et les vulnérabilités de l'hôte sur GCP, AWS et Azure. Il combine la collection la plus complète de politiques de sécurité basées sur des règles et un *machine learning* de pointe pour détecter les menaces.



Gamme

- **Prisma Cloud** pour Amazon AWS
- **Prisma Cloud** pour Google Cloud Services
- **Prisma Cloud** pour Microsoft AZURE
- **Prisma Cloud** pour Alibaba Cloud
- **Prisma Cloud** pour Docker / IBM Cloud / Kubernetes / OpenShift / Pivotal / Rancher

Besoins clients

- Sécuriser tout l'environnement Cloud natif, y compris les applications, les données, le réseau, le calcul, le stockage, les utilisateurs et les services PaaS
- Assurer un contrôle de conformité cohérent dans le cloud.
- Identifier et prévenir les menaces et les activités suspectes

Arguments de vente

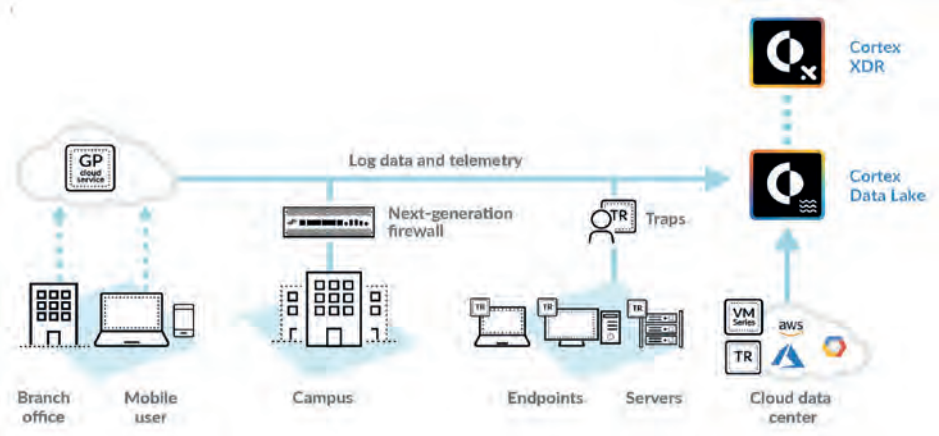
- Découvrir automatiquement toutes les ressources déployées dans le Cloud.
- Tracer les changements au niveau des ressources pour des raisons d'Audit ou de Forensic.
- Automatisez la sécurité tout au long du cycle de vie de l'application et implémentez des contrôles de sécurité dans le cadre de vos pipelines CI / CD.
- Garantissez une sécurité et une conformité cohérentes dans les environnements multi-cloud et cloud hybride.
- Prisma mise sur l'automatisation pour identifier, classifier, surveiller et protéger vos données stockées, mais aussi pour prévenir toutes les fuites potentielles.

Technologies

- API Prisma Cloud
- DevSecOps sécurisé

Traquez et stoppez les attaques insidieuses

La détection et réponse **Cortex XDR** intègre nativement un réseau, un terminal et des données sur le cloud pour stopper les attaques sophistiquées. En utilisant l'analyse comportementale, elle identifie des menaces inconnues et hautement évasives, ciblant le réseau. Le machine learning et les modèles d'IA dévoilent des menaces de n'importe quelle source, y compris des appareils gérés et non gérés.
Cortex XDR accélère le tri d'alertes et les réponses aux incidents en fournissant une image complète de chaque menace et en dévoilant automatiquement la cause initiale.
Une intégration rigoureuse aux points d'application permet de répondre rapidement aux menaces et d'appliquer les connaissances issues des enquêtes afin de détecter des attaques similaires à l'avenir.

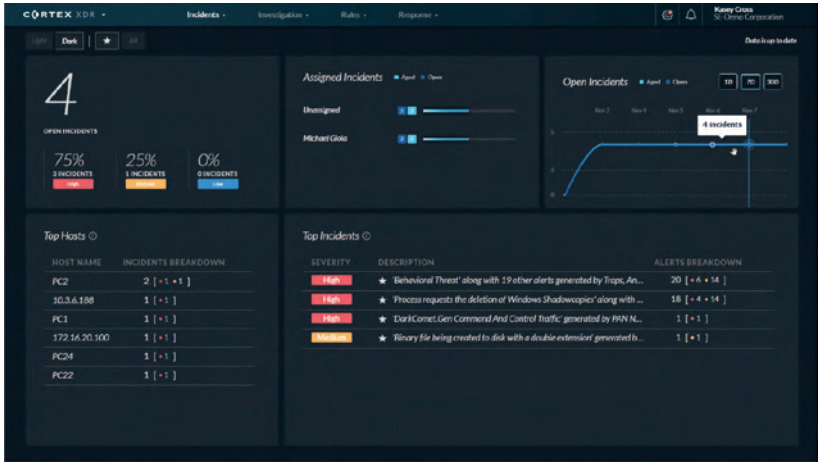


Gamme

- **Cortex XDR** est une plateforme cloud permettant un stockage de données de 30 jours à une durée illimitée.
- Trois types de licence :
- **Cortex XDR Prevent** : fonctions de protection des endpoints, y compris la prévention des exploits et la protection contre les logiciels malveillants, avec la possibilité de gérer et de configurer les politiques de sécurité de contrôle des endpoints et des périphériques.
- **Cortex XDR Pro par Endpoint** : fonctionnalités Cortex XDR Prevent + la collecte de données EDR et de la corrélation avec des alertes tierces.
- **Cortex XDR Pro par To** : permet l'analyse des logs des firewalls Palo Alto Networks ou autres (Check Point, Cisco et Fortinet) mais n'inclut pas la protection des endpoints.

Besoins clients

- Révéler automatiquement les attaques insidieuses
- Stopper l'accoutumance aux alertes et l'attrition
- Réduire le délai d'identification moyen (MTTI)
- Réduire le délai de contention moyen (MTTC)
- Protéger des équipements mobiles Android
- Se défendre contre les malwares et vulnérabilités zero-day
- Collecter des informations sur les attaques et réponses automatiques



Arguments de vente

- Permet de gagner en visibilité dans le réseau, terminal et données sur le cloud
- Détecte automatiquement les attaques sophistiquées 24/7
- Élimine le backlog d'alertes
- Permet de réduire de façon notable les fausses alertes positives
- Améliore la productivité SOC
- Augmente le retour sur des investissements actuels avec Cortex

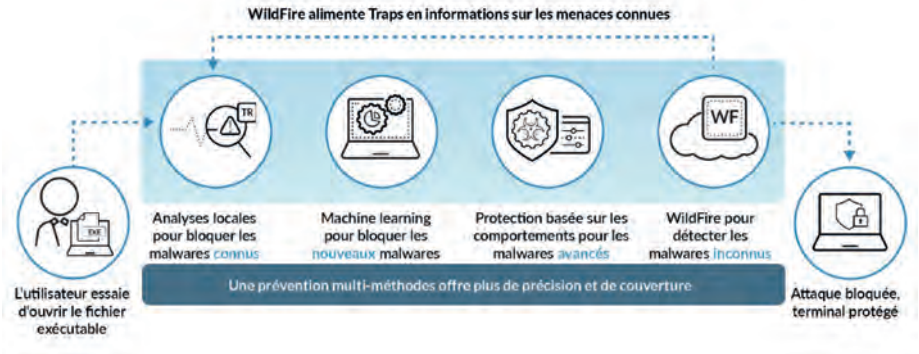
Technologies

- Enquête automatisée d'alertes
- Analyse de la cause initiale et de l'impact post-incident
- Confinement des incidents et récupération
- IoC et recherches de renseignements sur les menaces
- Machine learning supervisé et non supervisé
- Détection de malwares et d'attaques sans corps
- Détection d'attaques ciblées
- Détection de menace interne
- Prévention contre les malwares, les ransomwares et les exploits avec Traps

Cortex XDR pour Endpoint : Prévention, détection, investigation et réponse

Les fonctionnalités de la solution Traps sont désormais disponibles dans **Cortex XDR**, plateforme d'investigation automatique et de réponse. Avec cette intégration, l'agent Traps est désormais l'agent Cortex XDR à partir de la version 7.0. Les fonctionnalités déjà disponibles dans la plateforme TMS sont désormais disponibles dans l'interface Cortex XDR qui inclut désormais un nouvel onglet « Endpoint »

Traps adopte une technologie de rupture qui privilégie la prévention plutôt de la détection ce qui lui permet de prévenir contre 99% des menaces et en l'intégrant aujourd'hui à cortex XDR, les clients auront la possibilité de lancer des investigations automatiques et d'apporter une réponse aux menaces qui réussissent malgré tout à passer entre les mailles du filet.



Gamme

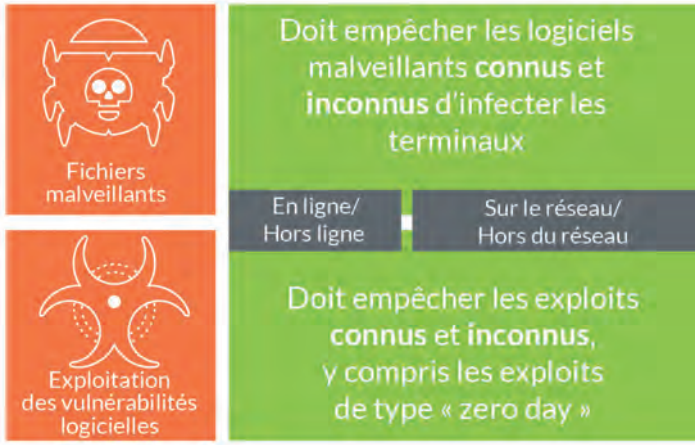
- Client Cortex XDR Agent pour postes Windows, MAC, Linux et Android

Technologies

- Module de prévention des exploits par protection transparente des processus utilisateur
- Restriction de fichiers à base de règles
- Inspection et vérification via WildFire : solution de SandBoxing
- Capture d'éléments post-mortem
- Protection menaces provenant des devices amovibles
- Vue de causalité
- Analyse détaillée des événements de menace comportementale dans la vue causalité

Besoins clients

- Protection des terminaux
- Protection des serveurs
- Protection des postes virtuels et des charges de travail dans le cloud
- Protection des équipements mobiles Android
- Défense contre les malwares et vulnérabilités zero-day
- Investigation rapide
- Réduction des faux positifs et Réponse aux attaques



Arguments de vente

- Prévention contre tous les exploits, même ceux visant les vulnérabilités zero-day
- Prévention contre tous les malwares, même les inconnus
- Pas de téléchargement de base de signatures, pas de mise-à-jour fréquente donc pas d'impact sur la production et l'expérience utilisateur
- Collecte des informations détaillées sur l'attaque pour aider à une analyse via Cortex XDR
- Client léger, évolutif et convivial
- Intégration étroite avec la sécurité réseau et la sécurité du cloud pour un échange rapide d'informations et une protection à travers toute l'organisation

PENTERA

Cyber-validation automatique

Pentera offre une plateforme unique pour tous les besoins de validation en matière de cybersécurité. Elle découvre en continu la surface d'attaque interne et externe des entreprises, et valide leurs niveaux de sécurité face aux menaces avancées en testant les sécurités exactement comme le ferait un attaquant, mais à la vitesse de la machine. La plateforme prouve l'impact potentiel de l'exploitation de chaque faille de sécurité et hiérarchise en conséquence les mesures correctives..

Gamme

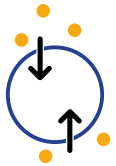
- **Pentera CORE :** Découverte des assets, des vulnérabilités et validation de sécurité à l'intérieur du réseau
- **Pentera SURFACE:** Découverte des assets exposés sur Internet et validation de sécurité depuis l'externe vers l'interne

Technologies

- Scan de vulnérabilité nouvelle génération
- Utilisation automatique de toutes les techniques de pentesting en correspondance avec le cadre Mitre Att&ck
- Plan de remédiation hiérarchisé en fonction des résultats de la Kill Chain

Besoins clients

- Valider sa posture de sécurité
- Identifier et couvrir toutes les surfaces d'attaques
- Identifier le risque réel
- Être informé continuellement sur les dernières menaces
- Améliorer l'efficacité des équipes de cybersécurité
- Optimiser les coûts liés aux tests d'intrusion



Couverture de toutes les surfaces d'attaques

Une plateforme unique qui découvre, évalue et exploite les surfaces d'attaque internes et externes pour identifier les véritables risques de sécurité

Identifier le risque réel

En émulant de réelles attaques, les organisations découvrent leur surface d'attaque exploitable et révèlent les failles de sécurité

Facilité d'utilisation

Ne nécessitant ni agents, ni manuels de stratégie, Pentera valide en toute autonomie la résilience face aux dernières attaques

Être informé des dernières menaces

L'équipe de recherche de Pentera Labs alimente en continu la plateforme Pentera avec des tests de validation des menaces et des techniques de piratage récentes

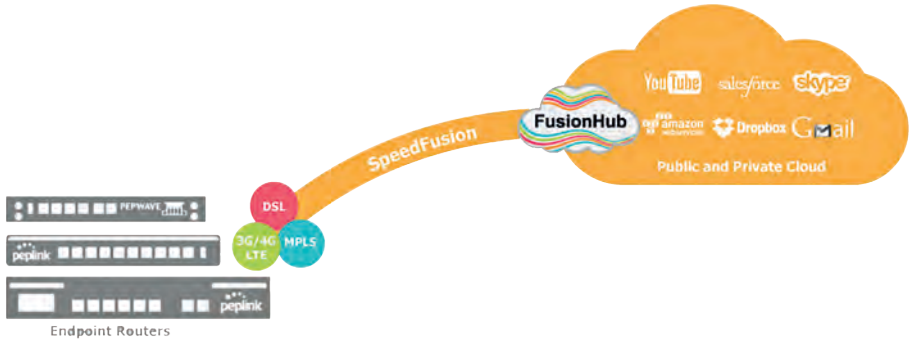
Arguments de vente

- Validation continue et automatisée de la sécurité
- Identification et remédiation chirurgicale des vulnérabilités réellement exploitables
- Résultats clairs facilement exploitables
- Couvre à la fois les vulnérabilités, les erreurs de configuration, les erreurs et faiblesses des identifiants

Répartition de charge, agrégation de liens

Les routeurs SD-WAN mobiles **Pepwave** de **Peplink** fournissent agilité et souplesse, en intérieur comme en extérieur. La solution permet d'agréger plusieurs liaisons 3G/4G pour une connexion redondante plus sécurisée, avec plus de débit et des flux ininterrompus pour les utilisateurs.

Les Peplink Balance permettent d'optimiser le réseau en connectant de manière transparente de nouveaux liens de fournisseurs différents et à bas coûts (ADSL, câbles, 3G/4G etc.). La gestion est facile, conviviale et intuitive grâce à la plateforme InControl 2. Avec leur solution VPN et leur relai DNS intégrés, les Peplink Balance sont la solution par excellence d'optimisation des réseaux pour tout type d'entreprises.



Gamme

- **Routeur Peplink Balance** : routeurs multi WAN
- **Routeur Pepwave Max** : routeurs 3G/4G/WiFi/xDSL
- **FusionHub** : appliance virtuelle pour SpeedFusion
- **MediaFast** : Routeur de mise en cache web, vidéo, audio

Technologies

- Load balancing & Failover
- Modem 3G/4G
- IPSec VPN
- SpeedFusion
- Dynamic DNS
- NAT et IP Forwarding
- IPv6
- QoS
- Firewall
- WIFI 802.11bgn

Besoins clients

- Augmenter sa bande passante
- Fiabilité du WAN
- Avoir un accès rapide et ininterrompu aux applications
- Déploiement mobile ou temporaire
- Réduire les coûts de communication

Arguments de vente

- Bande passante agrégée (xDSL, 3G, 4G, Satellite...)
- Hautement sécurisé (VPN)
- Accès ininterrompu à 100% aux applications Internet/Web/Cloud
- Demande d'accès aux réseaux mobiles & Wireless
- Secours transparent en cas de déconnexion
- Réduction instantanée des coûts WAN
- Persistance des sessions pour le transfert de gros fichier
- Maintien des flux VOIP et vidéo
- Connexion ininterrompue grâce au « Unbreakable VPN » dans le SpeedFusion
- In control 2 : outil de gestion centralisée

Gestion des risques, Sécurité Analytique et SecOps pour l'entreprise

Trop souvent, les équipes IT, sécurité et les développeurs opèrent en silos, et peinent à travailler ensemble. L'exposition au risque cyber qui en résulte est trop forte pour permettre à l'entreprise de continuer à innover. **Rapid 7** vise à gérer le risque grâce à une vision à 360° de l'exposition du SI, à la détection de compromission par l'analytique et à l'optimisation et la rationalisation des actions pour répondre aux incidents. Cette visibilité collective, appuyée par de l'analytics et de l'automatisation crée un langage commun pour les équipes (SecOps). Ce langage abat les barrières et, au final, accélère l'innovation et rend vos équipes plus efficaces.

Grâce à la collecte unifiée de données, la plateforme Rapid7 Insight procure la visibilité, l'analytics et l'automatisation nécessaire pour unir les équipes et amplifier l'efficacité. Rapid7 est le seul éditeur à se concentrer seulement sur l'aide à l'implémentation des pratiques SecOps et fournit la technologie, l'expertise et les outils de promotion d'une cybersécurité innovante dans l'entreprise.

Gamme

- **InsightVM** (gestion de vulnérabilités analytics du endpoint)
- **InsightAppSec** (test dynamique des applications, basé dans le cloud)
- **InsightIDR** (combine SIEM, UBA et EDR pour détecter les intrusions)
- **InsightOps** (consolidation des logs analyses, alertes)

Technologies

- SIEM et analyse du comportement utilisateur
- Gestion des vulnérabilités
- Test dynamique de la sécurité des applications
- Orchestration et automatisation
- UBA-powered SIEM et Gestion des logs

Besoins clients

- Scan et Gestion des vulnérabilités
- Tests de pénétration
- Sécurité des applications
- Détection et réponse aux incidents
- Implémenter la pratique SecOps

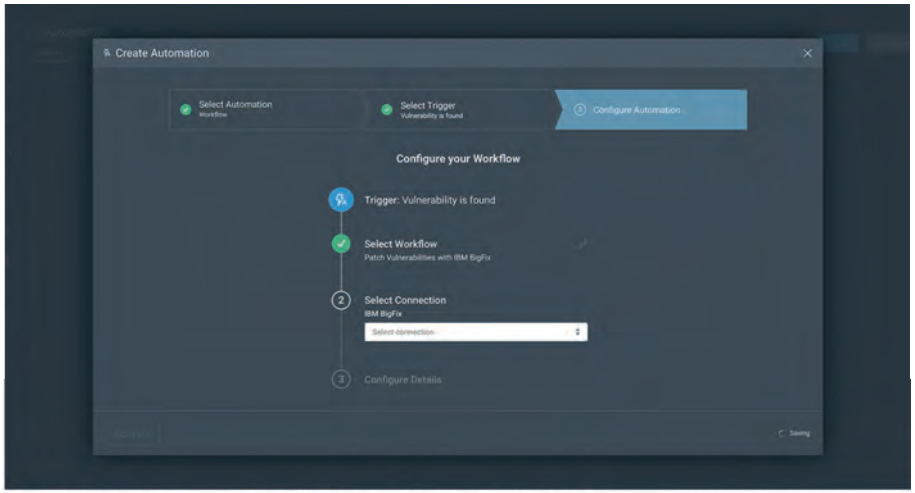


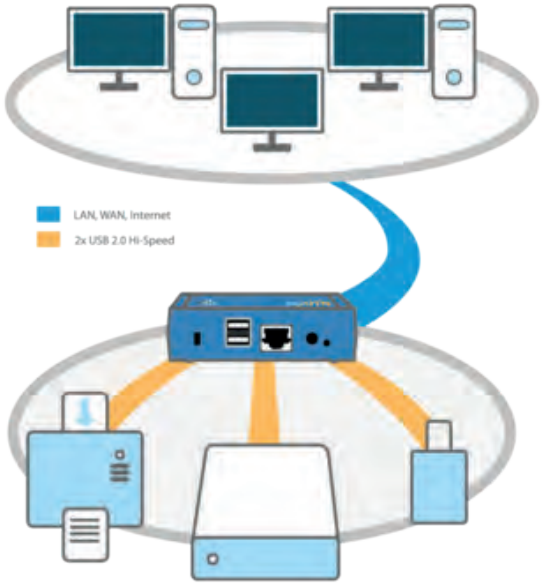
Figure 1: Automation-assisted patching workflow configuration in InsightVM

Arguments de vente

- Collecte unifiée de toutes les données IT
- Solution facilement évolutive
- S'intègre avec les outils déjà en place

Centralisation de dongles dans le data center

La Solution **MyUTN** de la Société **SEH** vous permet de centraliser vos dongles dans un endroit sécurisé. Le serveur de dongle MyUTN80 partage jusqu'à 8 dongles USB sur le réseau. Les dongles sont alors disponibles pour plusieurs utilisateurs sans qu'il soit nécessaire de les retirer puis de les reconnecter.



Gamme

- My Utn150 : Jusqu'à 3 dongles
- My UTN 80 : Jusqu'à 8 dongles avec fermeture par clé du boitier
- My UTN 800 : jusqu'à 20 dongles

Technologies

- Indépendance des interfaces USB
- Notification d'évènement
- Contrôle d'accès au port

Besoins clients

- Mettre en sécurité les dongles
- Centraliser les dongles USB
- Faire remonter l'USB sur une architecture Virtuelle
- Attribuer les dongles à des utilisateurs au lieu d'une machine

CITRIX Ready

vmware PARTNER
STANDARD TECHNOLOGY ALLIANCE

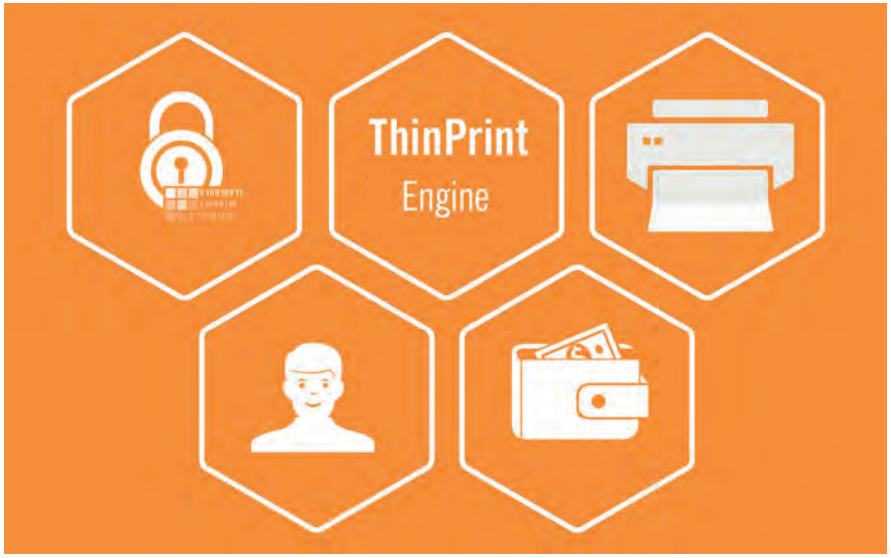
Arguments de vente

- Les dongles sont disponibles pour plusieurs personnes
- Solution idéale pour les environnements virtualisés
- Simple à mettre en place et garantie 3 ans
- Protection des dongles dans les lieux publics (Hopitaux, Ecoles, Etc..)

Ligne Directe 01 60 19 16 74

Gestion des impressions en architecture centralisée

Les solutions **ThinPrint** optimisent les impressions en environnement serveur centralisé. ThinPrint permet la réduction de la bande passante allouée aux transferts de données d'impression (QoS), apporte le driver universel d'impression et réduit considérablement le volume d'impression grâce à des algorithmes de compression. ThinPrint peut être mis en œuvre au sein d'une configuration Citrix, Windows TSE ou VMware à travers n'importe quel type de réseau et à partir de postes de tout type : PC, Smartphones, tablettes, terminaux clients légers.



Gamme

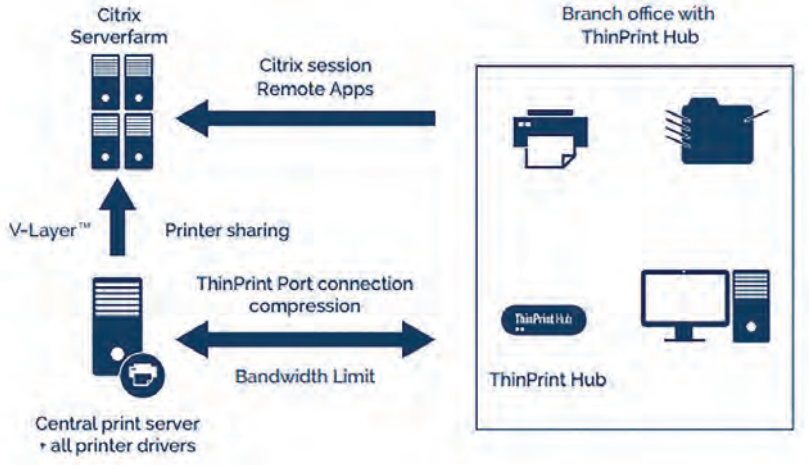
- Licence définitive : ThinPrint Perpetual : 1 licence par user nommé (valable pour Citrix Virtual Apps & Desktop, VMware View, RDS…)
- Licence Annuelle : Souscription au service pour 1 an minimum par user nommé (valable pour Citrix Virtual Apps and Desktop, VMware View, RDS…)

Technologies

- Driver Universel
- Qualité de Service
- Streaming optimisé
- Compression

Besoins clients

- Bande passante saturée par les impressions
- Impressions lentes
- Mixité de drivers 32 bit / 64bit
- Eviter les conflits de drivers
- Utilisations du multi-bac, recto-verso, etc… en environnement TSE /Citrix
- Imprimantes non compatibles TSE /Citrix
- Gérer les impressions SAP, AS400, Unix…

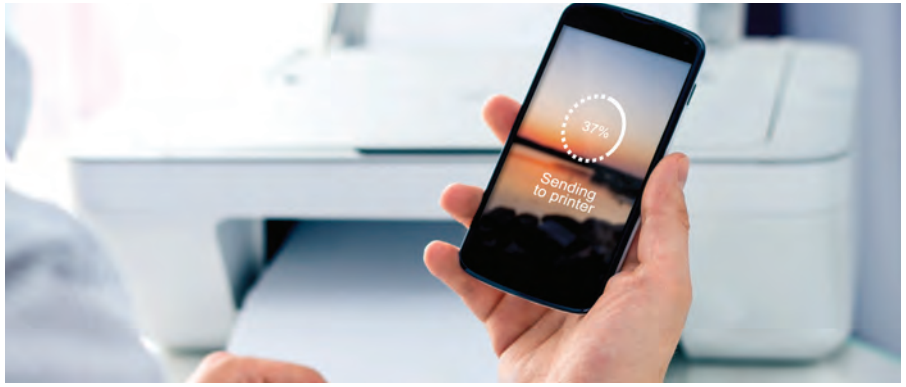


Arguments de vente

- Compatible avec tout type de postes
- Fonctionne directement sur les serveurs d'applications ou sur des serveurs d'impression dédiés
- Fonctionne avec des imprimantes locales ou réseaux
- La plupart des terminaux du marché ont un client ThinPrint embarqué
- Coûts d'utilisation réduits
- Support direct des protocoles ICA et RDS

Imprimez depuis n'importe quel device, n'importe où et en toute sécurité

Dans le contexte actuel de mobilité et de BYOD, où les utilisateurs ont accès à leurs données depuis n'importe où et n'importe quel device, **Uniprint** est la solution idéale pour gérer les impressions en toute sécurité. Basée sur la technologie brevetée par Uniprint de pilote d'impression Universel PDF, Uniprint Infinity simplifie la gestion des impressions et des imprimantes en entreprise. Cette solution permet également de retrouver et finaliser le travail d'impression sur n'importe quelle imprimante, n'importe où, n'importe quand.



Gamme

- Uniprint Infinity embarque toute la technologie Uniprint.
- Le système de licencing se fait par utilisateur concurrent.

Technologies

- Driver Universel PDF
- Compression
- Pull Printing

Besoins clients

- Réduire les coûts d'impression
- Sécuriser les impressions
- Pouvoir imprimer n'importe où
- Pouvoir imprimer à partir de n'importe quel device
- Imprimer rapidement
- Éliminer les drivers côté serveur

Arguments de vente

- Administration simplifiée des impressions
- Indépendant vis-à-vis du constructeur
- Impression de haute qualité rapide et fiable
- Travaux d'impression en attente accessibles de partout
- Support direct des protocoles ICA/HDX et RDP
- Réduire ses coûts d'impression de 35%
- Gérer les impressions dans un contexte de BYOD et mobilité

Maitrise de la sécurité des emails

Vade est le leader de la protection de la messagerie contre tous les types de menaces, y compris les attaques les plus ciblées. Sa technologie unique de filtre heuristique permet de lutter de manière efficace et innovante contre le phishing, le spear phishing, les malwares en général et les ransomwares en particulier. Au-delà de la protection de la messagerie et de la lutte contre les spams, Vade Secure propose une gestion simple du graymail (publicités, notifications de réseaux sociaux et newsletters) par une classification automatique des emails non prioritaires ainsi que la désinscription en 1 clic par l'utilisateur. Les différents modèles de déploiement s'adaptent aussi bien aux entreprises qu'aux fournisseurs de services.

Gamme

- Service Cloud
- Gateway
- Solution Office 365 et Gmail

Besoins clients

- Anti-Spam
- Protection contre les cyber-attaques ciblées par messagerie
- Fourniture de services managés de protection de la messagerie
- Lutte contre les malwares, ransomwares et le phishing

Arguments de vente

- 600 millions de boites aux lettres protégées.
- 95% de renouvellement
- Supporte tout type de messagerie
- Solution intégrée nativement à Microsoft O365 (API)
- Vient renforcer la solution de sécurité native d'O365 (EOP)
- Déploiement en quelques minutes avec O365 (Pas de redirection MX)
- Pas de Sandboxing grâce au traitement des e-mais en temps-réel (Pas de délai supplémentaire pour la réception des e-mails)

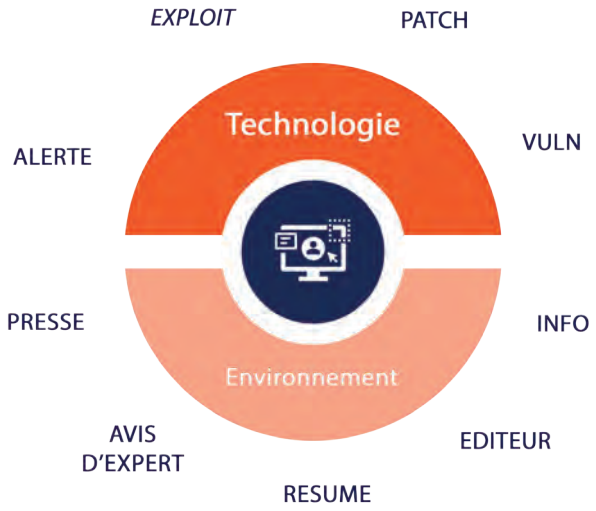
Technologies

- Anti-Malware (Protection multi couche, Fingerprint, analyse structurelle et comportementale)
- Anti-Phishing (filtrage entrant, BrandAlert, exploration de page web, Fermeture automatique des sites)
- Anti-Spear Phishing (filtrage entrant, BrandAlert, exploration de page web, Fermeture automatique des sites)
- Anti-Spam et Graymail management (Visibilité, Inbox zero, gestion des e-abonnements, 99,999% d'efficacité)

Ligne Directe 01 60 19 02 30

Service personnalisé de veille cyber

Chaque jour, les analystes du **CERT-XMCO** collectent et synthétisent des centaines de sources d'information. Les services IT peuvent souscrire à l'abonnement Yuno pour recevoir les bonnes informations en fonction de leur périmètre technique ou de la criticité au sein du portail de suivi d'actions et sous la forme de bulletins quotidiens.



Gamme

- Souscription 1 an renouvelable, tarif en fonction de la taille de l'entreprise
- Packs de tickets de support pour la mise en œuvre et la formation

Technologies

- **CERT (Computer Emergency Response Team)** reconnu et approuvé
- Portail web pour définir les périmètres et consulter les informations
- Format de diffusion mail, plateforme, SMS et API
- Injection possible dans les outils de ticketing

cert by xmco

Besoins clients

- Diminuer le temps passé à se renseigner sur l'actualité cybersécurité qui les concernent
- Aider à la décision sur les priorités de remédiation à entreprendre
- Compléter le renseignement en continu d'un SOC

Arguments de vente

- Collecte exhaustive : Plus de 1500 technologies et éditeurs suivis. 1000+ sources d'information
- Diffusion personnalisée
- Bulletins en français et en anglais
- Recommandations directement exploitables
- Elimination des faux positifs

Ligne Directe 01 60 19 16 74

Matrice des fonctionnalités Virtual Apps & Desktop

ANNEXE 1

	Virtual Apps Standard	Virtuals Apps Advanced	Virtuals Apps Premium	Virtual Desktop Standard	Virtual Apps & Desktop Advanced	Virtual Apps & Desktop Premium
Server-based Virtual Applications (Server-based hosted apps)	■	■	■		■	■
Server-based virtual desktops	■	■	■		■	■
VDI				■	■	■
Remote PC Access					■	■
DesktopPlayer (Add-on*)					■	■
VM hosted applications		■	■		■	■
Enhanced security through centralization and access control						
FIPS compliant			■			■
Common Criteria certified			■			■
Credential Guard compliant	■	■	■	■	■	■
Strengthened IT security	■	■	■	■	■	■
Multi-Factor authentication	■	■	■	■	■	■
Federated Authentication Service	■	■	■	■	■	■
Smart Card Integration	■	■	■	■	■	■
App security risk assessment			■			■
Accelerated Logon for Smart Card Users	■	■	■	■	■	■
App security risk assessment			■			■
ICA Proxy	■	■	■	■	■	■
SmartAccess			■			■
SSL VPN			■			■
Session watermarking	■	■	■	■	■	■
Intelligent session recording			■			■
Citrix Content Collaboration integration	■	■	■	■	■	■
Increase employee productivity with high performance anywhere access						
HDX™ user experience optimization	■	■	■	■	■	■
Optimized Skype for Business		■	■		■	■
Optimized Web-based Microsoft Teams	■	■	■	■	■	■
Browser content redirection	■	■	■	■	■	■
Unified Communications optimization	■	■	■	■	■	■
HDX 3D Pro™	■	■	■	■	■	■
Citrix Casting			■			■
Workspace Environment Management (WEM)		■	■		■	■
Citrix X1 Mouse	■	■	■	■	■	■
HDX Seamless local apps			■			■
HDX User Experience Templates	■	■	■	■	■	■
Superior User Experience for graphic rich Apps	■	■	■	■	■	■
WAN Optimization	■	■	■	■	■	■
Citrix SD-WAN for WAN optimization						■
Citrix SD-WAN plug-in						■

Matrice des fonctionnalités Virtual Apps & Desktop (Suite)

ANNEXE 1

	Virtual Apps Standard	Virtuals Apps Advanced	Virtuals Apps Premium	Virtual Desktop Standard	Virtual Apps & Desktop Advanced	Virtual Apps & Desktop Premium
Simplify support and enable choice of BYO device						
Any device access	■	■	■	■	■	■
Enterprise app store (StoreFront)	■	■	■	■	■	■
Self-service password reset			■			■
Clientless HTML5 Access	■	■	■	■	■	■
Universal printing services	■	■	■	■	■	■
Reduce cost and complexity of app and desktop management						
App Health Monitoring			■			■
Citrix App Layering	■	■	■	■	■	■
Citrix App Layering with Advanced Configuration			■			■
Citrix App Layering with User Layers Writable			■			■
Citrix App Layering with Office 365 User Layers	■	■	■	■	■	■
Unified Management Console	■	■	■	■	■	■
Citrix Director	■	■	■	■	■	■
Director Historical Reporting and Trend Analysis	■	■	■	■	■	■
Director Premium Edition			■			■
End-to-end environment visibility			■			■
Custom delegated administration (Studio)		■	■		■	■
Configuration logging (Studio)		■	■		■	■
User experience network analysis			■			■
Robust high-availability	■	■	■	■	■	■
Application compatibility and migration with AppDNA			■			■
Hybrid cloud provisioning	■	■	■	■	■	■
Microsoft Azure integration	■	■	■	■	■	■
Amazon Web Services integration	■	■	■	■	■	■
Oracle Cloud Platform	■	■	■	■	■	■
Citrix Provisioning for Citrix Virtual Apps	■	■			■	■
Citrix Provisioning for virtual desktops				■	■	■
Citrix Machine Creation	■	■	■	■	■	■
Microsoft App-V integration	■	■	■		■	■
Integrated profile management	■	■	■	■	■	■
Enterprise scalability	■	■	■	■	■	■
Hypervisor Agnostic	■	■	■	■	■	■
Hyper-V with System Center Virtual Machine Manager (SCVMM)	■	■	■	■	■	■
Citrix Hypervisor	■	■	■	■	■	■
VMware vSphere integration	■	■	■	■	■	■
Nutanix AHV	■	■	■	■	■	■
Microsoft System Center Configuration Manager (SCCM) integration		■	■	■	■	■
Citrix Connector for System Center Configuration Manager			■			■
Citrix ADC load-balancing	■	■	■	■	■	■
The Citrix ITSM Adapter for ServiceNow			■			■

End User Experience	Citrix Workspace Essentials	Citrix Workspace Standard	Citrix Workspace Premium	Citrix Workspace Premium Plus
Unified app store	■	■	■	■
Citrix Workspace app		■	■	■
Unified Admin Experience				
Single pane of glass	■	■	■	■
Unified Endpoint Management				
Device and OS management			■	■
Application Management			■	■
Business class productivity apps			■	■
BYOD solution			■	■
Workspace Environment Management (WEM)			■	■
Micro-VPN			■	■
Microsoft EMS/Intune integration			■	■
Citrix Access Control				
Cloud App Control		■	■	■
Single Sign-on	■	■	■	■
Web filtering			■	■
MFA		■	■	■
Content Collaboration				
Securely share and collaborate		■	■	■
Connectors			■	■
Encryption			■	■
Information Rights Management (IRM)			■	■
Structured workflow			■	■
Storage flexibility		■	■	■
Drive Mapper		■	■	■
Virtualized Apps and Desktops Service				
Open architecture				■
Centralized image management				■
App Layering technology				■
Advanced monitoring & analytics				■
Common Criteria and FIPS compliance				■
Unified communication				■
High definition user experience				■
Analytics				
User behavior security analytics			■	■
App performance analytics			■	■
Operations usage analytics			■	■
Advanced analytics for Access Control			■	■
Data security analytics			■	■
Unified Endpoint Management analytic			■	■
Virtual apps and desktop analytics				■
Workspace intelligence		■	■	■

Migrez à votre rythme vers le Cloud grâce à Citrix

On-premises' ou hébergé dans le Cloud, en tant que service Citrix Cloud ou avec un service provider, on peut choisir jusqu'à quel point gérer l'infrastructure soi-même et où placer les charges applicatives.

1. Mode hybride

Citrix Virtual Apps and Desktops Service vous laisse le choix de mettre les charges applicatives soit dans votre data center, soit dans un cloud public ou chez un provider. L'administration et la responsabilité des évolutions restent chez vous.

2. Hébergé

Toute l'infrastructure nécessaire, y compris les charges serveurs, est portée dans un cloud public (Azure, AWS, Google, Oracle). L'administration et les évolutions restent à la charge de l'entreprise. Les utilisateurs se connectent directement à ce Cloud.

3. Service Cloud complet

L'infrastructure Citrix n'est plus qu'un service auquel vous êtes abonné et dans lequel vous ajoutez et administrez juste vos charges applicatives. Citrix s'occupe de faire évoluer les composants et d'assurer la disponibilité.

'On-premises'

Déployez Citrix Virtual Apps ou Citrix Virtual Apps and Desktops dans votre propre environnement et centralisez l'administration et les mises à jour dans votre data center. Citrix met à disposition des modèles de déploiement et vous pouvez vous faire aider par un partenaire Citrix Solutions Advisor (CSA).

Service DaaS avec un CSP

Pour obtenir les bénéfices de Citrix Virtual Apps and Desktops comme un simple service clé-en-main, vous pouvez également vous tourner vers un des nombreux partenaire Citrix Solution Providers (CSP) qui propose des offres Desktop-as-a-Service tout intégrées.

Matrice des fonctionnalités Citrix ADC

Application availability	Premium	Advanced	Standard
L4 load balancing and L7 content switching	■	■	■
Microsoft SQL MYSQL	■	■	■
AppExpert rate controls	■	■	■
IPv6 support	■	■	■
Traffic domains	■	■	■
Subscriber-aware traffic steering	■	■	■
Global server load balancing (GSLB)	■	■	■
Carrier-Grade Network Address Translation (CGNAT)	■	■	
Dynamic routing protocols	■	■	
Surge protection and priority queuing	■	■	
Triscale Clustering	■	■	
Application acceleration			
Client and server TCP optimizations	■	■	■
Cache Redirection	■	■	■
Citrix® AppCompress™	■	■	■
Citrix® AppCache™	■	■	
Application security			
L4 DoS defenses	■	■	■
L7 DoS defenses	■	■	■
L7 rewrite and responder	■	■	■
Citrix Gateway Connector for Exchange Express	■	■	
XenMobile NetScaler Connector	■	■	
AAA for traffic management	■	■	
Citrix Web App Firewall with XLM security	■	■	
Factor authentification	■	■	
IP Reputation	■	■	
Content Inspection	■	■	
SSL Forward Proxy	■		
Cloud Connector for Citrix Networking	■		
Simple manageability			
Citrix Application Delivery Management	■	■	■
AppExpert visual policy builder	■	■	■
ActionAnalytics	■	■	■
AppExpert service callouts, templates and visualizers	■	■	■
Role-based administration and AAA for administration	■	■	■
Configuration wizards	■	■	■
Comtrade Management Pack for Citrix ADC	■		
Native Citrix web interface	■	■	
Front-end Optimization			
Content layout	■	■	
Domain sharding	■	■	
Image optimization	■	■	
Style sheets and JavaScript optimization	■	■	
TCP Protocol Optimization			
Multi-path TCP	■	■	■
BIC and cubic TCP	■	■	■
Citrix Gateway			
Federated Identity	■	■	
One URL/SSO using SAML 2.0	■	■	
Centralized Policy Management (SmartControl)	■		
Stateless RDP proxy	■	■	
PCoIP support	■	■	■
Cluster for IC A proxy (Striped)	■	■	
Monitor Citrix Virtual Apps & Desktop traffic (Real time)	■	■	
Monitor Citrix Virtual Apps & Desktop traffic (Historical)	■		
Monitor Citrix Gateway (real time)	■	■	
Monitor Citrix Gateway (historical)	■		
Broad client support for plugins	■	■	■
Customizable web portal	■	■	■
SSL VPN remote access	■	■	■
IC A proxy to Citrix Virtual Apps & Desktop	■	■	■
Contextual policies for Citrix Virtual Apps & Desktop	■	■	■
Endpoint Analysis	■	■	■
Secure browser-only access (CVPN)	■	■	■
Always-On	■	■	■
Integration with StoreFront	■	■	■

■ standard

Support Technique

Support technique Miel gratuit et illimité pour les revendeurs techniciens formés par Miel

Support téléphonique Miel disponible pour les clients finaux ayant souscrit à un contrat annuel de support Miel via leur partenaire

Gamme de contrats et support direct chez l'éditeur payants pour les partenaires et clients finaux formés

infoline 01 60 19 87 70

Centre de formation et de compétence

Centre de formation officiel

Citrix Authorized Learning Center depuis 20 ans

Elite Training Center Palo Alto Networks

Instructeurs certifiés et expérimentés

Conventionné pour les prises en charge par les organismes possibilité de suivre les formations à distance

Sessions intra- et inter-entreprises

Tous les cursus, dates et pré-inscriptions sur
www.miel.fr/formation

infoline 01 60 19 16 27

Venir chez MIEL

Parc Burospace 5
91571 BIEVRES Cedex
FRANCE
01 60 19 34 52

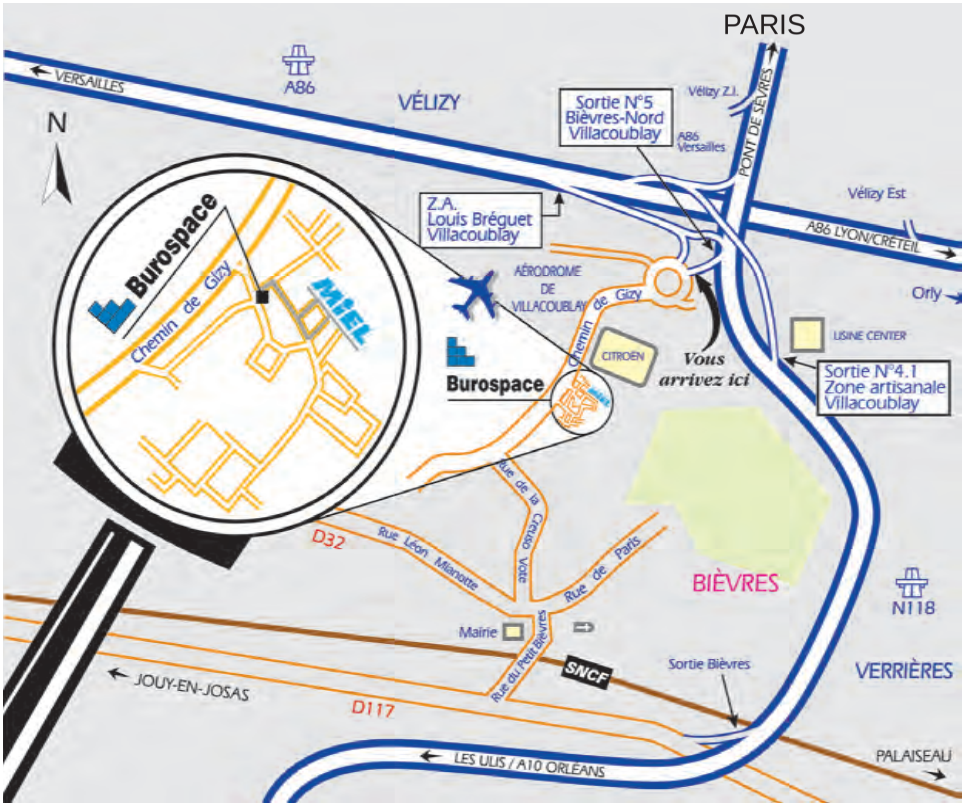
En voiture :

GPS : 48°45'58 N et 2°13'03 E

A86 de Versailles ❯ Sortie Villacoublay
A86 de Créteil ❯ Sortie 30 Petit-Clamart
N118 de Paris ❯ Sortie 4.1 Villacoublay
N118 d'Orléans ❯ Sortie 4.1 Villacoublay

En transport :

RER C ❯ Bièvres ❯ Bus 33
RER C ❯ SNCF ❯ Chaville Vélizy ❯ Bus
RER ❯ SNCF ❯ Versailles Chantier ❯ Bus 22
Métro Pont de Sèvres ❯ Bus 42
Tramway T6 ❯ l'Onde - Maisons des Arts ❯ Bus 42



MIEL

www.miel.fr

01 60 19 34 52