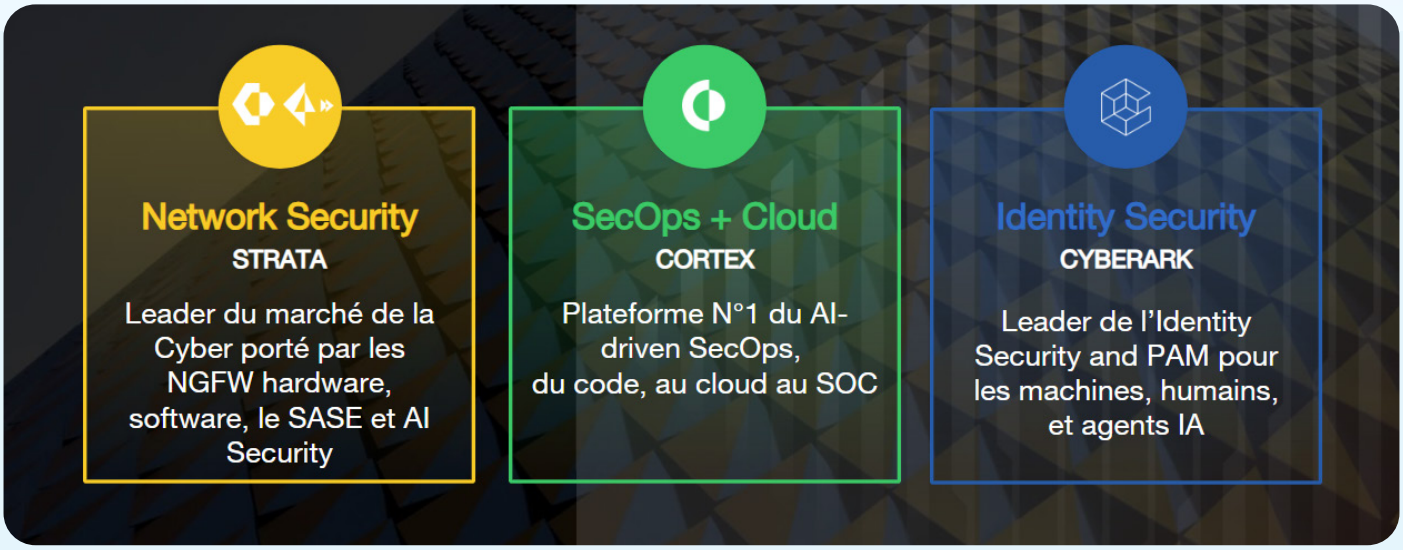
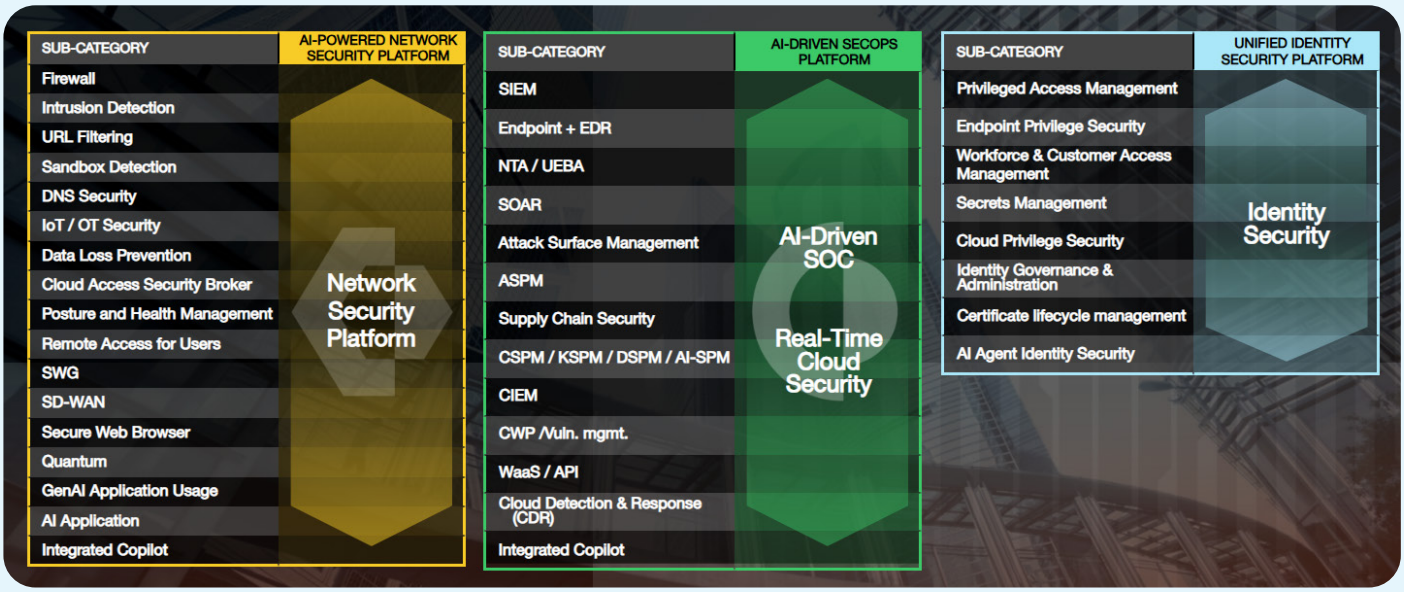
Leader incontesté de la cybersécurité

Depuis 2005, Palo Alto Networks révolutionne le monde de la Cybersécurité, en s'attaquant à des problèmes de sécurité complexes, et en changeant le status quo.

La Plateformisation adresse un défi critique à travers l'innovation et l'intégration



Une approche en perpétuelle évolution



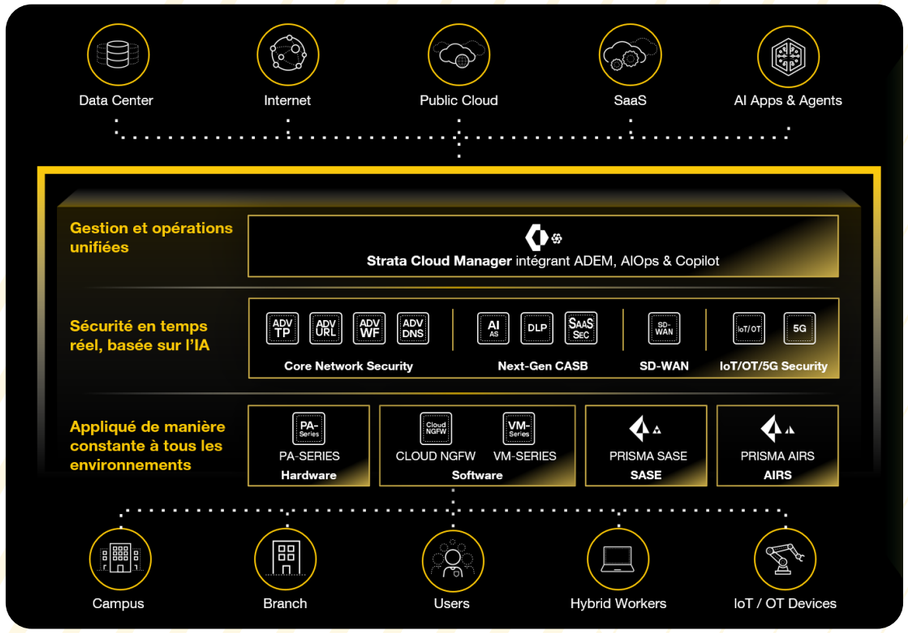
MIEL

Distribué en france par Miel
www.miel.fr/palo-alto-networks.fr - 01 60 19 34 52

NETWORK SECURITY

La Plateforme Zero Trust Network Security

La plateforme Zero Trust Network Security donne la priorité à la prévention et l'intégration d'innovations faciles à déployer. Tous les cas d'usages de la sécurité réseaux sont abordés, via les plateformes physiques, virtuelles, et SASE ou le navigateur sécurisé.



Grâce à un contrôle granulaire des applications, des utilisateurs, des contenus, et une intelligence Cloud partagée, Palo Alto Networks repousse les limites de la protection du réseau, et bloque les menaces les plus sophistiquées.

Strata Hardware & Software NGFW, et Prisma SASE

Qu'il soit physique (PA-Series), virtuel (VM-Series, CN-Series, Cloud NGFW, AI Runtime, via les Software NGFW Credits), ou SASE, tous sont alimentés par le PAN-OS, qui embarque plusieurs fonctionnalités nativement :

APP-ID : détermine l'identité d'une application indépendamment du port, du protocole, du cryptage SSH / SSL ou de toute autre tactique d'évasion que l'application peut utiliser.

USER-ID : permet d'identifier l'utilisateur par son identité, indépendamment de son adresse IP, grâce à plusieurs technologies combinant un mapping avec les annuaires ou le monitoring du trafic d'authentification.

CONTENT-ID : permet une analyse complète de tout le contenu du trafic autorisé comprenant les malwares, tous les types d'exploit, les catégories Web, et les fichiers par catégorie ou type de contenu. L'ensemble sera utilisé comme critère de contrôle.

DEVICE-ID : identifie tous les appareils et objets connectés sur le réseau et applique les politiques de sécurité sur la population IoT / OT.

Single Pass Parallel Processing : modèle breveté par Palo Alto Networks, permettant d'analyser le trafic en un seul passage. Ce moteur permet d'assurer une sécurité à haut débit, et d'intégrer toutes les fonctionnalités avancées sur les NGFW sans dégrader leur performance, et d'assurer la pérennité du matériel.

Strata Hardware NGFW

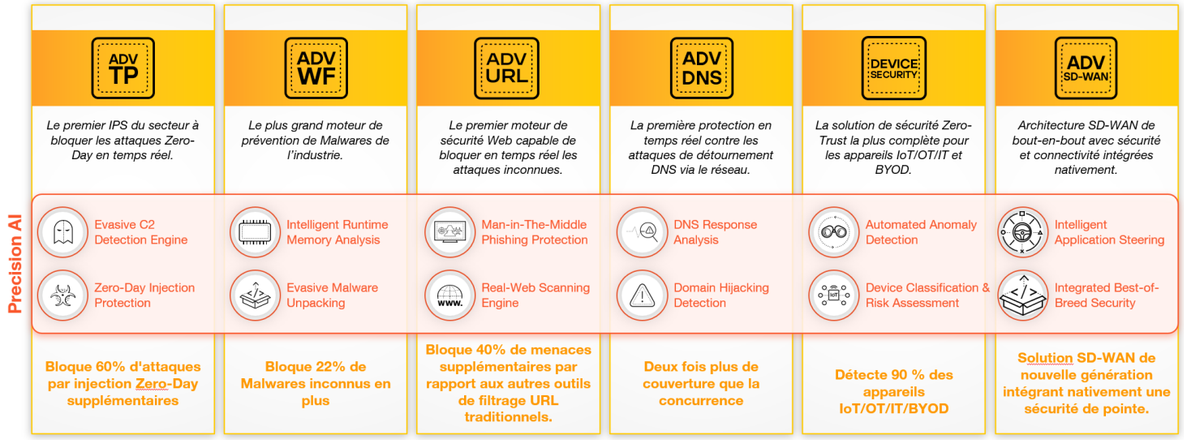
Les 5ème génération de Next-Gen Firewalls de Palo Alto Networks redéfinissent la sécurité réseau pour l'ère hybride et cloud. Propulsés par l'IA et le machine learning, ils bloquent les menaces en temps réel avec une précision inégalée. Leur nouvelle architecture offre des performances multi-gigabit sans compromis sur l'inspection. Plus intelligents, plus rapides, plus proactifs : la nouvelle référence du NGFW.

Les souscriptions de sécurité

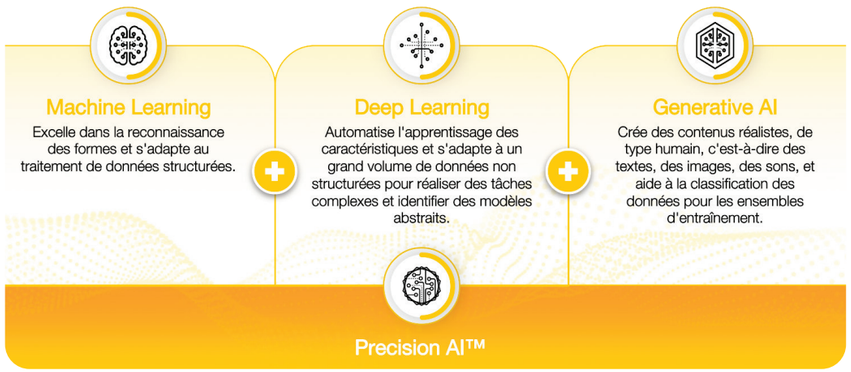
Les cyberattaques dans le domaine des réseaux sont de plus en plus redoutables, notamment parce qu'elles se basent sur l'IA pour augmenter les dégâts. Pour s'en prémunir, les systèmes de protection doivent évoluer, en se dotant de moteurs d'IA capables d'agir en temps réel sur les menaces, et de se former à partir de données riches et variées. L'IA doit être partagée dans la plateforme pour l'améliorer en permanence. Pour répondre à ces problématiques, Palo Alto Networks a développé une suite de souscriptions, utilisant le moteur **Precision AI** pour bloquer toutes les attaques les plus sophistiquées en temps réels.

	SOUSRIPTIONS	DESCRIPTION
Core Network Security	Advanced Threat Prevention	Prévenir les attaques C2 connues et inconnues et les attaques par injection de type Zero-Day
	Advanced URL Filtering	Garantir un accès sécurisé au Web et stopper les attaques de phishing connues et inconnues
	Advanced Wildfire	Moteur d'analyse basé sur l'IA pour prévenir les malwares inconnus basés sur des fichiers
	Advanced DNS Security	Prévenir les menaces sophistiquées utilisant le DNS, y compris le détournement de DNS
Connectivité et sécurité	SD-WAN	Optimiser de la bande passante entre les sites, et sécuriser l'interconnexion des sites
	Prisma Access Agent	Mettre en place une sécurité Zero trust, appliquer la DLP, contrôler l'intégrité des postes, l'authentification et renforcer le Always-On via l'agent VPN.
Sécurité des appareils connectés	Device Security	Détecter, classifier, et stopper les menaces venant de l'IoT et machines inconnues sur le réseau
Next-Gen CASB	Enterprise Data Loss Prevention	Détecter, classifier la donnée sensible, et limiter les fuites de données sensibles
	SaaS Security	Voir et sécuriser toutes les applications SaaS (inline et via API), avec des classificateurs avancés, DLP intégré, et surveillance d'Apps. Contrôle de la posture de sécurité SaaS.
	AI Access	Contrôler l'accès, l'usage, et appliquer la DLP aux apps de Gen-AI

Precision AI : L'IA qui redéfinit la cybersécurité



Le Bundle Precision AI est disponible sur toutes les plateformes NGFW physiques de Palo Alto Networks.



Prisma AIRS : Sécuriser l'IA d'aujourd'hui. Maîtriser l'innovation de demain

Prisma AIRS est conçue pour protéger les applications IA tout au long de leur cycle de déploiement. Elle découvre l'ecosystème AI complètement, évalue les risques et protège contre les menaces pour tous les composants IA : Agents, modèles, datasets, applications que ce soit en développement, en déploiement ou à l'exécution.

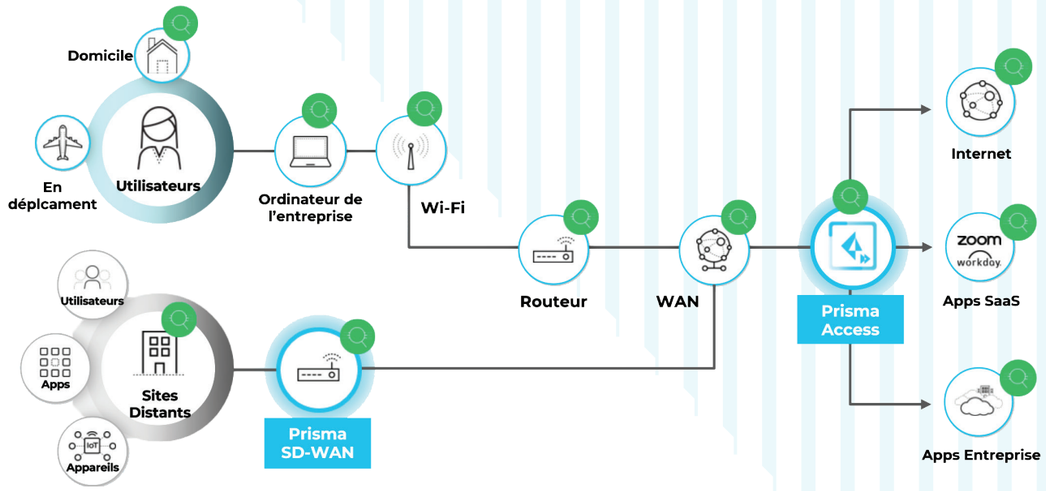
PRISMA® SASE
BY PALO ALTO NETWORKS

Prisma SASE (**Prisma Access + Prisma SD-WAN**) est l'offre de Palo Alto Networks qui converge les fonctionnalités de réseaux et de sécurité en une seule et même plateforme délivrée depuis le Cloud.

Prisma Access est la plate-forme de service de sécurité Cloud qui propose toutes les fonctions et souscriptions de la plateforme Network Security. La disponibilité et la montée en charge du service sont gérées et garanties par Palo Alto Networks.

Prisma SASE propose un ensemble de licences permettant de sécuriser les utilisateurs mobiles et/ou les sites distants de manière unifiée, vers tout type d'application.

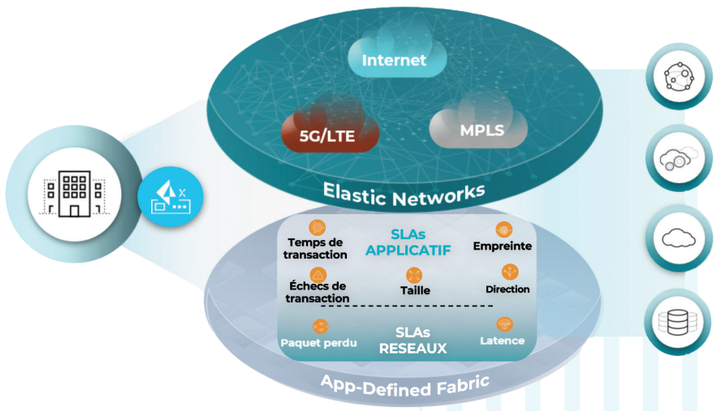
ADEM (Autonomous Digital Experience Management) : L'option ADEM de Prisma SASE permet d'avoir une observabilité de bout en bout, depuis le poste utilisateur vers la destination (application, internet, SaaS, Cloud etc.)



PRISMA® SD-WAN
BY PALO ALTO NETWORKS

La connexion des sites distants simple et sécurisée

Prisma SD-WAN est la première solution de SD-WAN nouvelle génération du marché capable d'assurer un retour sur investissement allant jusqu'à 243%. Prisma SD-WAN simplifie les opérations réseau grâce au Machine Learning, élimine 99% des tickets de support réseaux, et améliore l'expérience des utilisateurs avec une bande passante WAN décuplée pour un coût inférieur à celui des architectures classiques.



PRISMA BROWSER™
BY PALO ALTO NETWORKS

Le seul navigateur d'entreprise sécurisé pour tous les users, tous les appareils et toutes les applications

Avec la généralisation des applications Web et SaaS, le navigateur est devenu l'espace de travail principal. Cependant, la dépendance croissante au navigateur a également révélé une faille critique dans la sécurité des entreprises. Le navigateur sécurisé **Prisma Browser** de Palo Alto Networks étend la sécurité du SASE à tous vos appareils gérés et non gérés, en toute transparence, sans problème de déchiffrement pour vous offrir contrôle, agilité et protection. Prisma Browser disponible en standalone, s'installe sans droit d'admin sur n'importe quel poste, en quelques minutes et est compatible avec tous les OS.

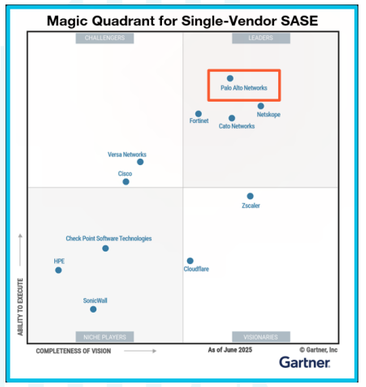
- Basé sur Chromium
- Expérience Utilisateur Intuitive
- Pas besoin de droits d'admin
- Visibilité unifiée, une seule politique

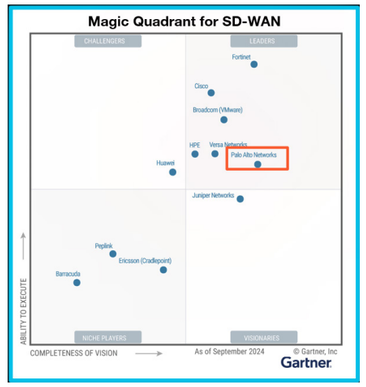
Disponible sur

iOS

Partenaires et Contractuels	BYOD	Nouveaux cas d'utilisation sur tout type d'appareil
• Fusions et Acquisitions • Centres d'appels • Travailleurs de première ligne sur le terrain • Réduction des coûts d'envoi de laptops • Réduction de l'utilisation du VDI	• Agilité de la force de travail • Liberté de choix de l'appareil • Possibilité d'utiliser le mobile	• Support pour le trafic non déchiffrable (QUIC, SLA de M365…) • Utilisation des applis de GenAI • Menaces internes et surveillance via le navigateur • Forensic et conformité • Donner un accès à un tiers

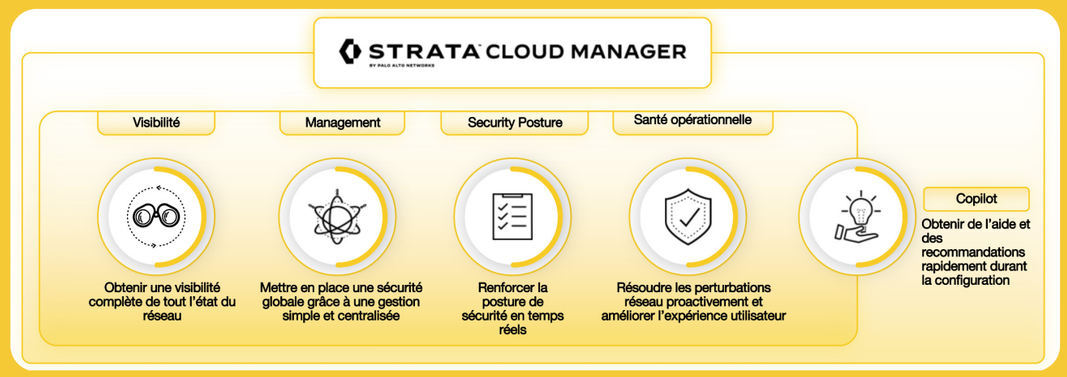
Le SEUL éditeur du marché LEADER en SSE, SD-WAN et SASE



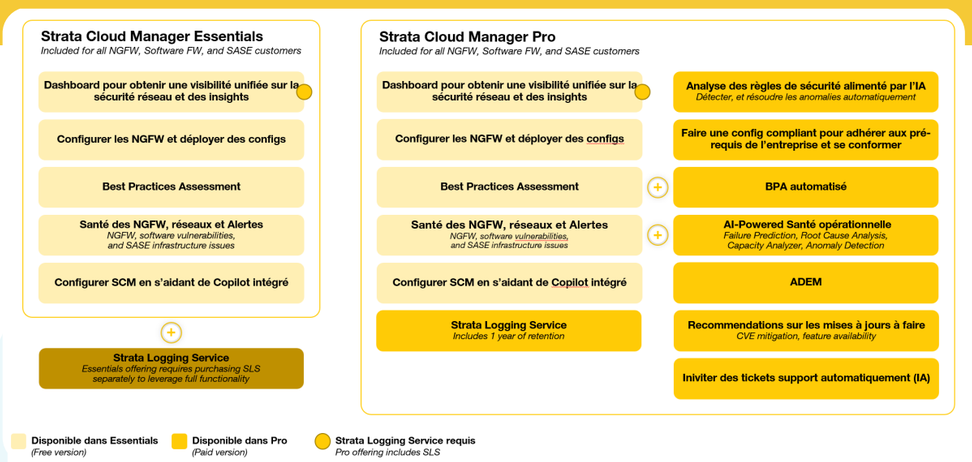


Strata Cloud Manager

Strata Cloud Manager est la console de gestion centralisée de Palo Alto Networks délivrée depuis le Cloud. Elle permet d'avoir une visibilité de tout l'environnement Network Security Platform incluant, entre-autres, les NGFW physiques, virtuels, Prisma Access, Prisma SD-WAN ou encore Prisma Browser.



Strata Cloud Manager Essentials est disponible nativement et redéfinit les standards du pilotage sécurité en offrant une gestion centralisée d'une puissance inégalée. **Avec Strata Cloud Manager Pro**, nous passons dans une autre dimension : automatisation intelligente à grande échelle, visibilité totale, contrôle stratégique multi-plateformes et innovation continue portée par le leader mondial incontesté de la cybersécurité.



Détails des fonctionnalités Essentials et Pro

MIEL

paloalto NETWORKS

CORTEX®
BY PALO ALTO NETWORKS

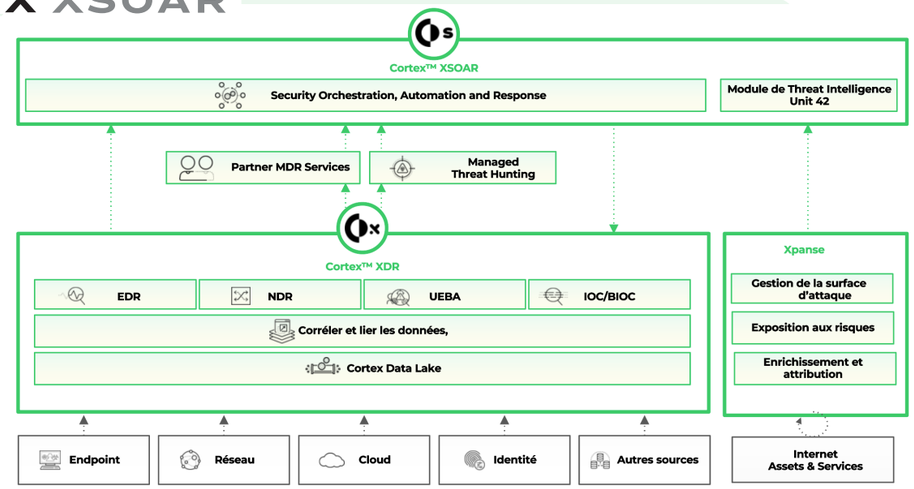
La plateforme Security Operations

Lors d'une cyberattaque, les menaces traversent plusieurs environnements et génèrent des informations, que nous pouvons retrouver sur le Cloud, le réseau, et les endpoints. Dans tous les cas, la vitesse de détection (MTTD) et de réponse (MTTR) à l'attaque sont des critères essentiels pour se protéger contre les menaces les plus sophistiquées. Palo Alto Networks a conçu la plateforme Security Operations pour répondre à ce défi, en proposant une plateforme pilotée par l'IA, permettant d'unifier la donnée du Code au Cloud, puis, au SOC, et de répondre aux nouvelles attaques en autonomie et en temps réel.

La plateforme Security Operations propose un ensemble de produits visant à détecter et répondre toujours plus efficacement et rapidement aux cyberattaques de demain.

CORTEX XSOAR®
BY PALO ALTO NETWORKS

Cortex XSOAR analyse les alertes venant de Cortex XDR et des autres outils de sécurité, pour réduire les incidents et répondre automatiquement aux attaques.



Cette plateforme d'orchestration, d'automatisation et de réponse de sécurité (SOAR) permet aux équipes de sécurité opérationnelles de piloter de manière unifiée la gestion d'incident, l'automatisation, la collaboration temps réel et la gestion des sources de Threat Intelligence. La réponse est coordonnée avec plus de 850 éditeurs de sécurité différents.

CORTEX XPANSE®
BY PALO ALTO NETWORKS

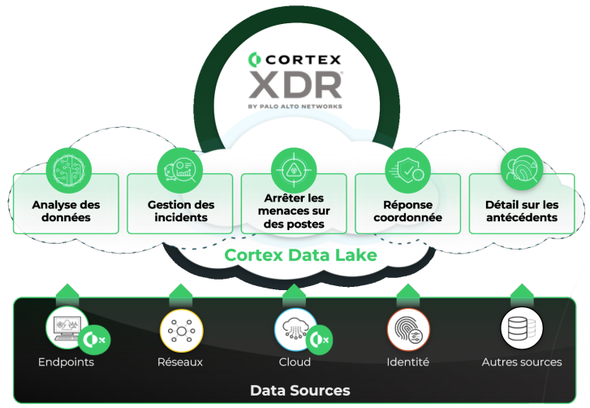
Cortex XPANSE scanne Internet pour découvrir l'exposition de l'entreprise, réduire et protéger sa surface d'attaque.

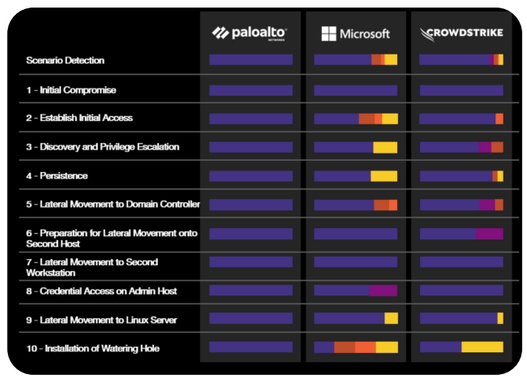
- Découverte de tous les systèmes connectés et les services exposés relatif à l'entreprise
- Attribution des actifs basée sur le Machine Learning et hiérarchisation automatisée des risques pour une réponse immédiate
- Création des playbooks automatisés alimentés par l'IA pour identifier les propriétaires de services et remédier au problème en temps réels

CORTEX XDR®
BY PALO ALTO NETWORKS

Cortex XDR détecte les menaces venant des endpoints, du réseau et du Cloud. L'**eXtended Detection & Response** permet de répondre aux attaques avec précision.

- Découverte des menaces par un Machine Learning continu
- Management unifié dans une seule console
- Reprise les informations venant des NGFW Palo Alto Networks et autres
- Nativement Intégré à Cortex XSOAR





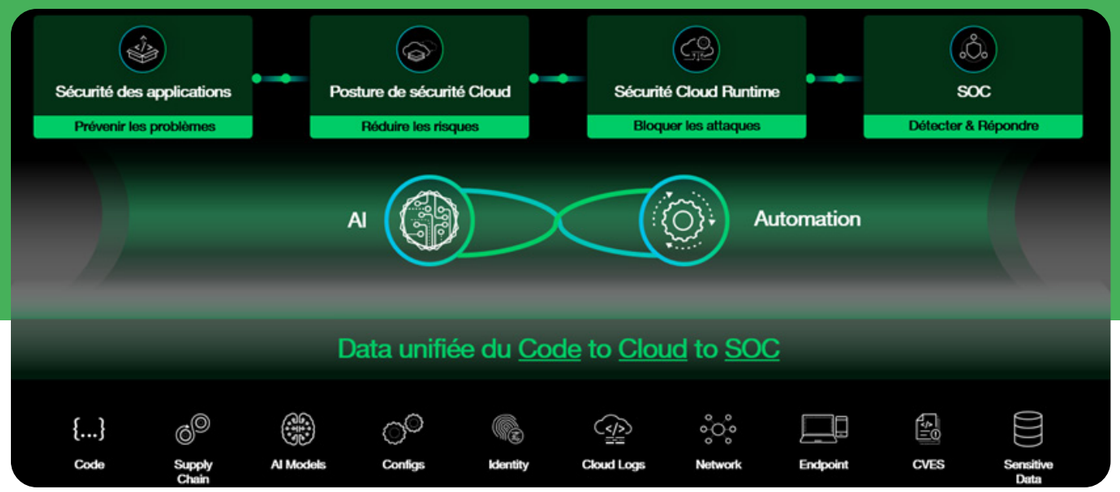
Cortex XDR est le numéro 1 du marché dans les évaluations MITRE ATT&CK® Enterprise !

CORTEX XSIAM®
BY PALO ALTO NETWORKS

Cortex XSIAM est la fusion de tous les produits Cortex en une seule plateforme, le tout alimenté par l'IA. Cortex XSIAM (eXtended Security Intelligence and Automation Management) rassemble la télémétrie de l'infrastructure, la Threat Intelligence et les données ASM au sein d'une base de données intelligente, garante d'une détection et d'une réponse plus efficace et entièrement automatisée. Cortex XSIAM permet de ne plus perdre de temps sur les tâches répétitives et sur l'analyse de gros volumes de données. Les analystes gagnent en productivité tout en se consacrant à des besoins SecOps plus stratégiques.

Cortex Cloud : Quand Cortex et Prisma Cloud fusionnent !

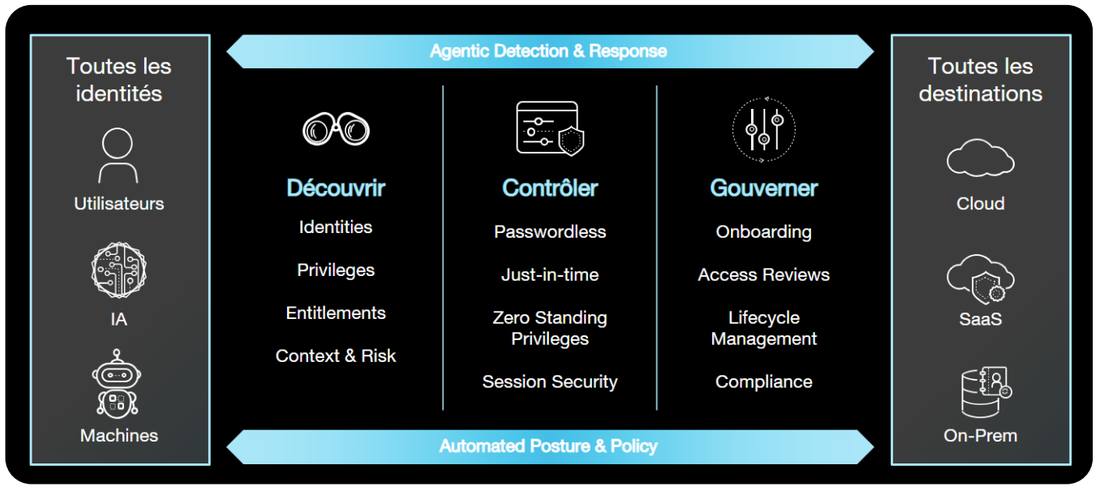
Avec **Cortex Cloud**, Palo Alto Networks redéfinit la sécurité cloud en unifiant Prisma Cloud et Security Operations dans **une plateforme unique et puissante**. Grâce à **l'IA et à l'automatisation avancée**, Cortex Cloud connecte enfin DevOps et SOC de manière fluide. Du code, au cloud, au SOC avec la remédiation. **Un agent. Un modèle de données. Une interface. Un workflow.**



Unified Identity Security

Avec l'acquisition de CyberArk, Palo Alto Networks repoussent les limites de la plateformisation, en intégrant la gestion de la sécurité des identités : **Une solution unique, native de l'IA, qui découvre, analyse et protège en continu chaque identité humaine, machine et IA.**

- **Découvrir :** Découverte automatique de toutes les identités, droits et privilèges dans les environnements. Création d'un graphe d'identités dynamique enrichi de données de risque et de contexte.
- **Contrôler :** Appliquer des contrôles dynamiques. Changer les authentifications SSO & MFA basiques, par des accès sans mots de passe, sans privilèges permanents, et Zero-Trust en continu.
- **Gouverner :** Donner aux équipes SOC et RSSI une vision globale, et la capaciter d'appliquer l'IA et la sécurité proactive directement dans les identités.



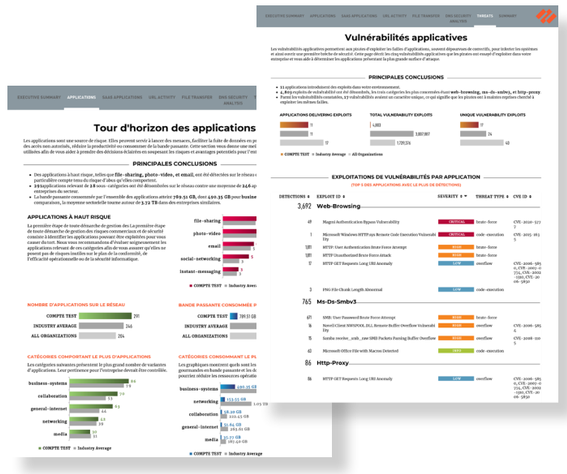
SLR : Security Lifecycle Review

Montrez la puissance de la plateforme Palo Alto Networks

Le SLR (Security Lifecycle Review) est un outil destiné à offrir une visibilité sur les applications, les risques et les menaces, obtenue sous la forme d'un rapport généré sur la base d'informations recueillies par le firewall nouvelle génération grâce à une mise en place non intrusive.

Le SLR est une évaluation sur mesure des risques comprenant l'exposition réelle aux menaces, le comportement utilisateur, l'utilisation des applications, pour comprendre les risques "cyber" de l'entreprise.

Le SLR est généré par l'intermédiaire d'un partenaire en récupérant un fichier de logs.



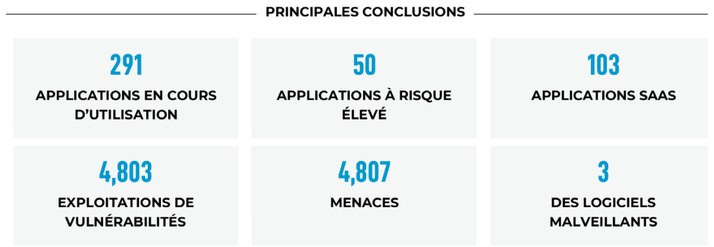
1 → Un boîtier est installé sur le réseau

2 → Le traffic est monitoré passivement pendant 1 semaine

3 → Le rapport expliquant les résultats est fourni

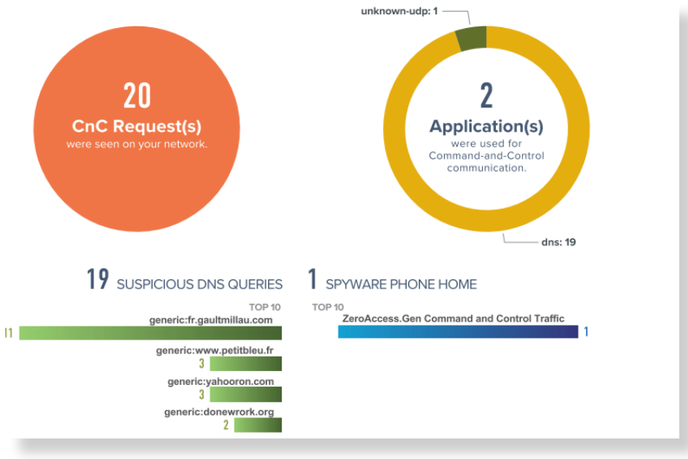
Que fait le SLR ?

- Identification et usage des applications
- Identification et usage des applications SaaS
- Comportement des utilisateurs
- Rapport sur les risques et les menaces



SLR : Dans quel cas ?

- Construire un cas d'usage Palo Alto Networks pour les architectes, les managers et les décisionnaires.
- Montrer comment restaurer la visibilité et le contrôle sur les applications, les utilisateurs et le contenu
- Prouver la nécessité d'une telle solution dans le réseau
- Gérer le cycle d'évaluation et mettre un cadre autour de l'évaluation/POC



Miel Academy : Centre de Formation

Miel est **centre de formation ATP** (Autorized Training Partner) Palo Alto Networks depuis près de 10 ans. Nos formateurs ont tous une très solide expérience avant-vente et après-vente afin de délivrer la formation la plus pertinente possible. Nos sessions inter-entreprises se déroulent à Paris, à Bièvres (91) et ponctuellement en région.

Nous proposons aussi des sessions sur-mesure en « intra » pour un minimum de 3 participants. Il est également possible de suivre des formations virtuelles avec formateurs, en ligne, pour toutes les dates sur Paris et Bièvres.

Palo Alto Networks PAN-EDU-210 : Firewall - Configuration & Management

MIXTE | 35 HEURES (5 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-220 : Panorama - Centralized Network Security Administration

MIXTE | 14 HEURES (2 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-220 : Panorama - NGFW Management

MIXTE | 14 HEURES (2 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-238 : Prisma SD-WAN - Design and Operation

MIXTE | 35 HEURES (5 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-260 : Cortex XDR - Security Operations and Integration

MIXTE | 21 HEURES (3 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-262 : Cortex XDR - Investigation and Analysis

MIXTE | 14 HEURES (2 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-270 : Cortex XSIAM - Security Operations, Integration, and Automation

MIXTE | 21 HEURES (3 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-272 : Cortex XSIAM - Investigation and Analysis

MIXTE | 14 HEURES (2 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-318 : Prisma Access SSE - Configuration and Deployment

MIXTE | 28 HEURES (4 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-330 : Firewall - Troubleshooting

MIXTE | 21 HEURES (3 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-380 : Cortex XSOAR - Engineering Security Automation Solutions

MIXTE | 28 HEURES (4 JOURS) | ACCESSIBLE

Palo Alto Networks PAN-EDU-PAB : Prisma Access Browser

MIXTE | 7 HEURES (1 JOUR) | ACCESSIBLE

Détails des formations,
dates et pré-inscriptions
01 60 19 16 27
formation@miel.fr

Miel élu Meilleur Centre de formation Palo Alto Networks d'Europe, pour la 2ème année consécutive.

MIEL

Distribué en france par Miel
contact@miel.fr - 01 60 19 34 52