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.

L'approche plateforme, pour une gestion simple

Zero Trust Network Security
Plateforme complète pour la visibilité réseau

- **Strata Hardware** — *NGFW, PA-Series*
- **Strata Software** — *VM & CN-Series AI Runtime Security*
- **Prisma SASE** — *Prisma Access & Prisma SD-WAN*
- **ZTNA** — *Private & Secure App Access*
- **Real-Time Analysis** — *Cloud-Delivered Security Subscriptions*
- **Visibilité complète** — *Strata Cloud Manager*
- **Prisma Access Brower** — *Secure Enterprise Browser*
- **IoT & OT Security** — *Protection de l'environnement OT & IoT*
- **Data Security** — *NG-CASB, DLP, AI Access Security*

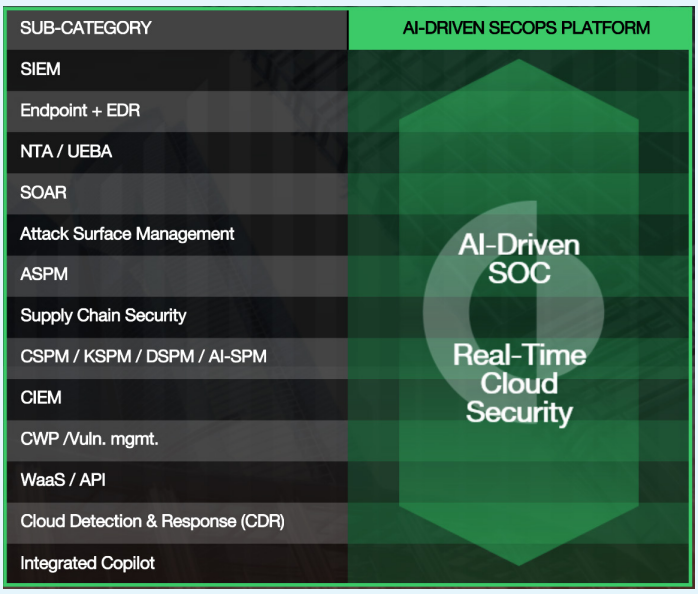
Real-Time Cloud Security
Plateforme cloud-native pour sécuriser tout ce qu'il y a dans le cloud

- **DevSecOps** — *Sécurité du développement dans le cloud*
- **CNAPP** — *Sécuriser les Cloud-Natives Applications*
- **CSPM** — *Gérer la posture de sécurité cloud*
- **Policy as Code** — *Gérer les règles de sécurité dès la programmation*
- **Cloud Workload Security** — *Protection des Workloads cloud*
- **DSPM** — *Gestion de la donnée*
- **Container Security** — *Sécurité des environnements type Kubernetes, Docker, etc.*
- **CIEM** — *Gestion des droits de l'infrastructure cloud*

AI-Driven SOC
Data, Analytics & Automatisation réunis dans une seule et unique plateforme de SOC nouvelle génération

- **EPP** — *Protection des endpoints*
- **IR** — *Réponse aux incidents et transformation du SOC*
- **MDR** — *Gestion de la détection et réponses aux cyberattaques*
- **XDR** — *Protection avancée et étendues des endpoints, du réseau et du cloud*
- **SOAR** — *Automatisation et orchestration de la réponse aux incidents*
- **SIEM** — *Corrélation d'événements*
- **Attack Surface Management** — *Réduction de la surfave d'attaque et l'exposition sur Internet*
- **Autonomous SOC** — *XSIAM pour mettre l'IA au coeur du SOC*

Une plateforme en perpétuelle évolution



MIEL

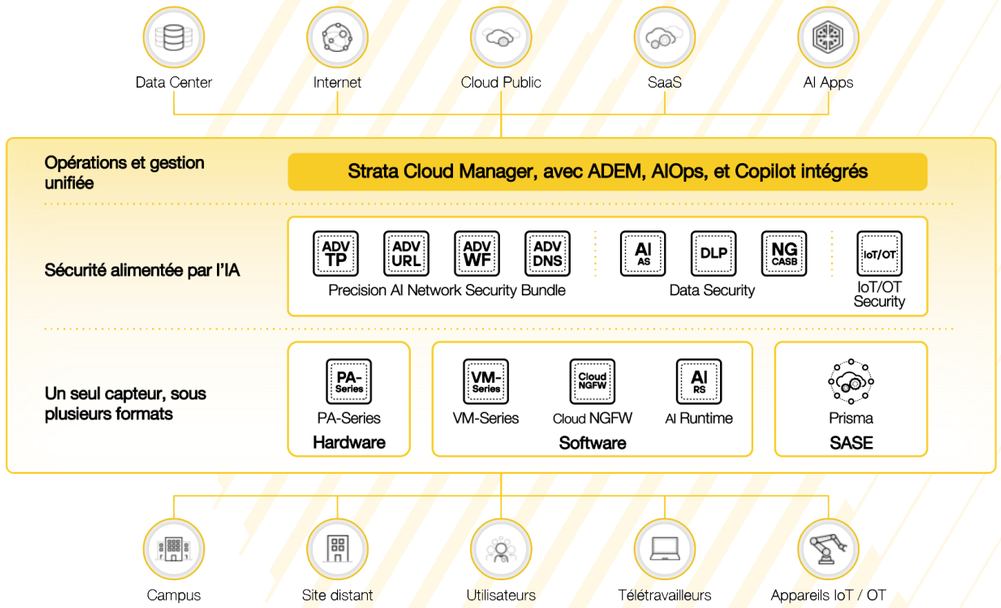
Distribué en france par Miel
www.miel.fr/palo-alto-networks.fr - 01 60 19 34 52

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.

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 nativement plusieurs fonctionnalités :

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.

Les souscriptions de sécurité

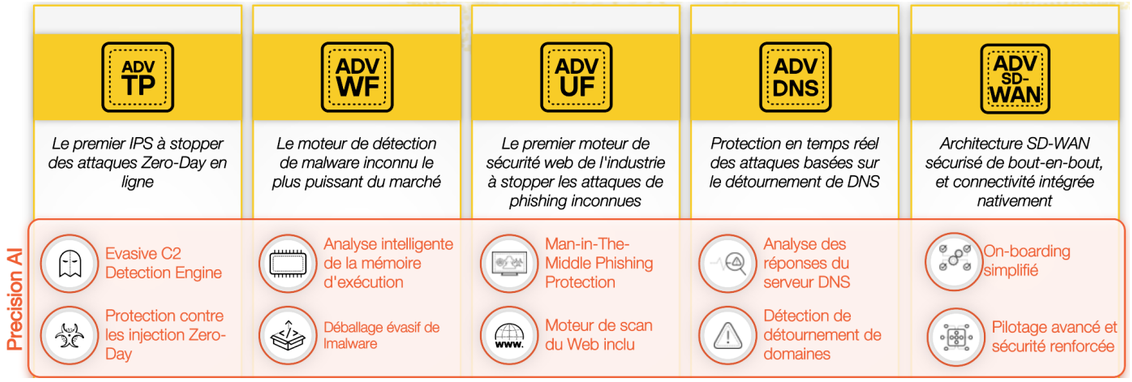
Les cyberattaques dans le domaine des réseaux sont de plus en plus redoutables, notamment parce qu'elles se basent sur l'IA pour augmenter les dégâts.

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.

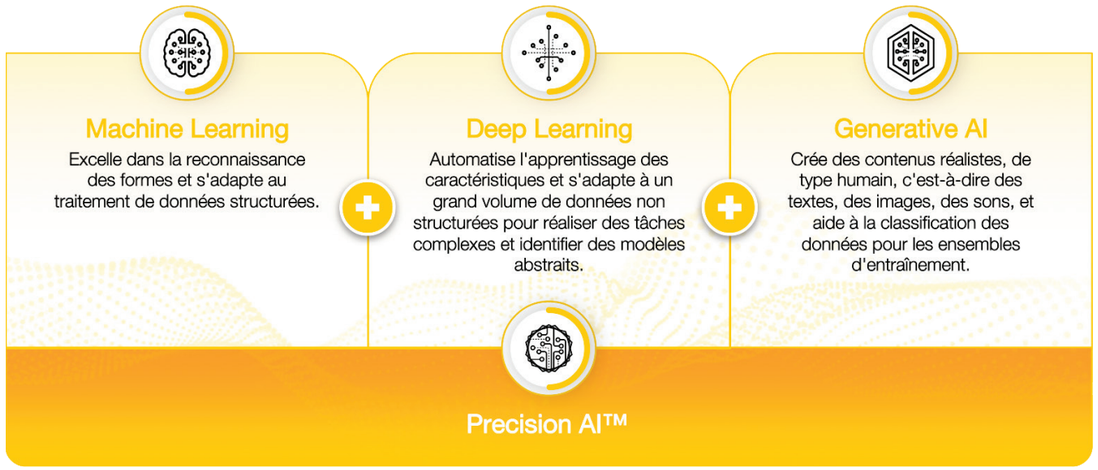
Pour répondre à ces problématiques, Palo Alto Networks a développé une suite de souscriptions, utilisant le moteur **Precision AI** pour bloquer toutes les attaques les plus sophistiquées en temps réels.

SOUSRIPTIONS	DESCRIPTION
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
SD-WAN	Optimiser de la bande passante entre les sites, et sécuriser l'interconnexion des sites
Global Protect	Améliorer les politiques VPN, contrôler l'intégrité des postes, et faire du VPN sans agent
IoT Security	Détecter, classifier, et stopper les menaces venant de l'IoT et machines inconnues sur le réseau
Enterprise Data Loss Prevention	Détecter, classifier la donnée sensible, et limiter les fuites de données sensibles
NG-CASB	Voir et sécuriser toutes les applications SaaS, avec des classificateurs avancés, DLP intégré, et surveillance d'Apps

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



Le système d'IA de Palo Alto Networks exploite les capacités du Machine Learning, du Deep Learning et de l'IA générative avec des données de haute fidélité pour former des modèles de sécurité afin de détecter et de prévenir les menaces qui évoluent rapidement, le tout en temps réel.



Ultimate Test Drive (UTD)

Mettez-vous aux commandes de la plateforme de cybersécurité Palo Alto Networks grâce aux ateliers technniques **Ultimate Test Drive** (UTD)

Découvrez la liste des UTD
et contactez notre équipe !
reseausecu@miel.fr

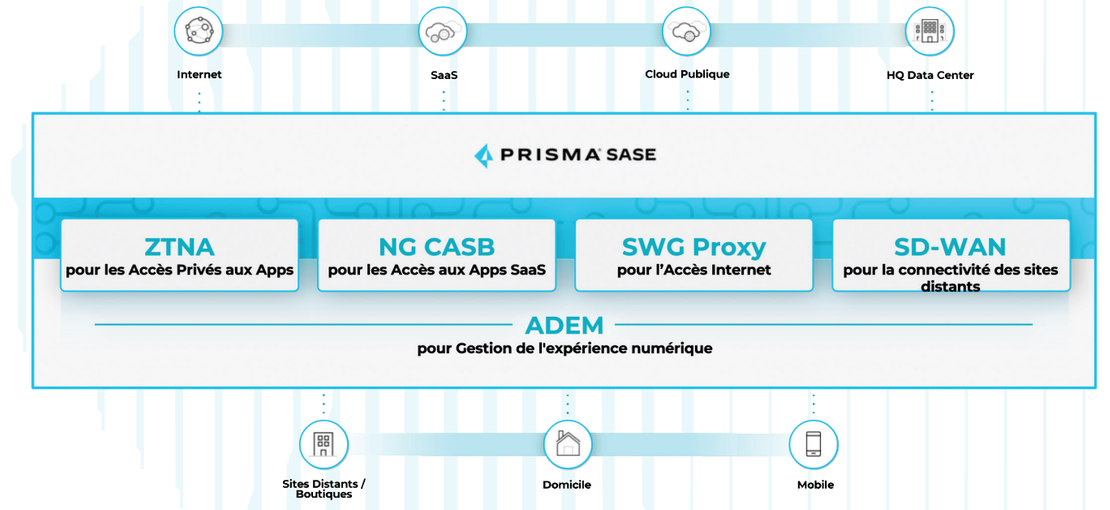
PRISMA® SASE
BY PALO ALTO NETWORKS

La solution SASE la plus complète du marché

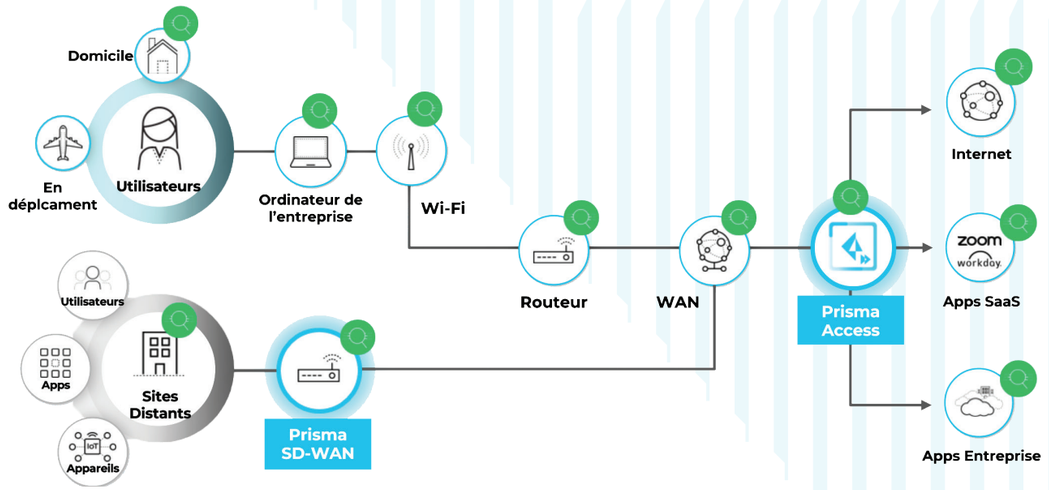
Prisma SASE (**Prisma Access + Prisma SD-WAN**) est l'offre de Palo Alto Networks qui converge les fonctionnalités de réseaux et de sécurité en une seule et même plateforme délivrée depuis le Cloud.

Prisma Access est la plateforme 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.



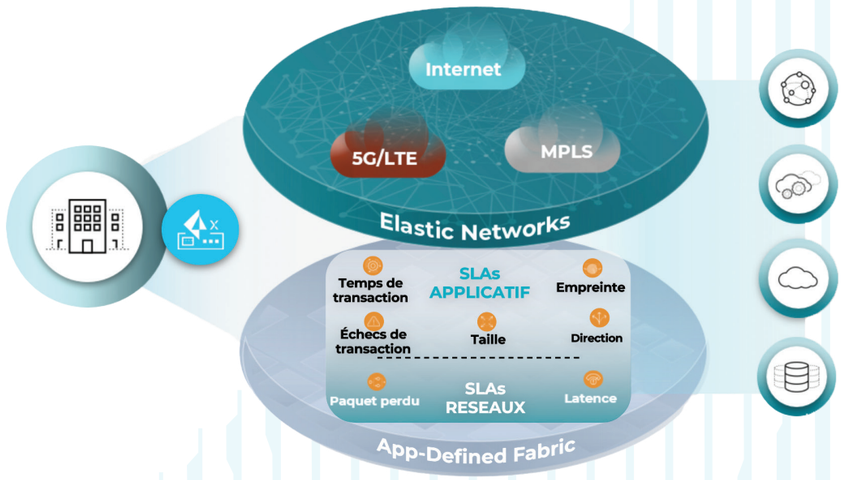
ADEM (Autonomous Digital Experience Management) : L'option ADEM de Prisma SASE permet d'avoir une observabilité de bout en bout, depuis le poste utilisateur vers la destination (application, internet, SaaS, Cloud etc.)



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® ACCESS BROWSER
BY PALO ALTO NETWORKS

Le seul navigateur d'entreprise sésurisé 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 Access 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 Access 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

Prisma Access Browser permet de répondre à de nombreux cas d'usages, allant au-delà des attentes d'un navigateur classique.

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 cours 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 (ex.: QUIC, SLA de Microsoft 265 etc.) • Utilisation des applis de GenAI • Menaces internes et surveillance via le navigateur • Forensic et conformité • Donner un accès à un tiers

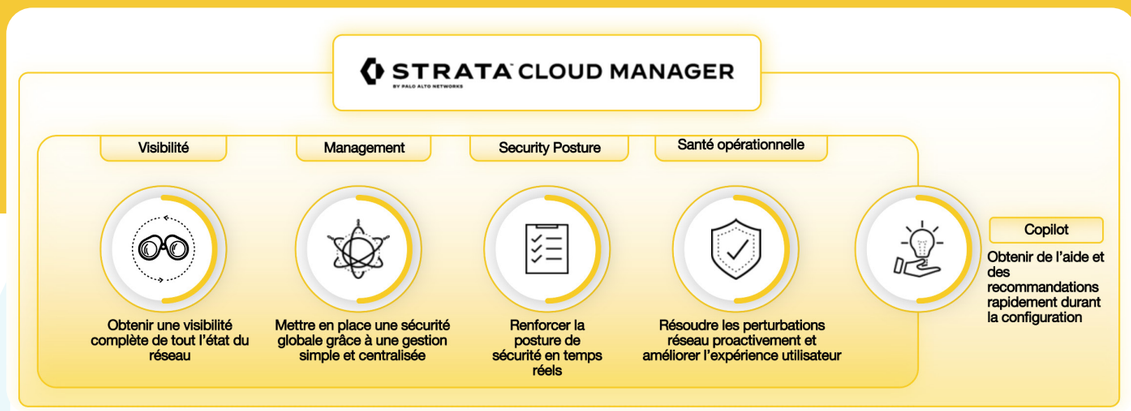
Strata Cloud Manager

Une seule console, pour tous les cas d'usages de la sécurité réseau

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 ou encore Prisma SD-WAN.

La gestion des '*Best practices*', l'analyse de la compliance et la prédiction des problèmes réseaux sont intégrés via la souscription AIOps.

La gestion autonome de l'expérience utilisateur est également intégrée via l'ADEM, disponible dans l'offre Strata Cloud Manager Pro.



CORTEX®
BY PALO ALTO NETWORKS

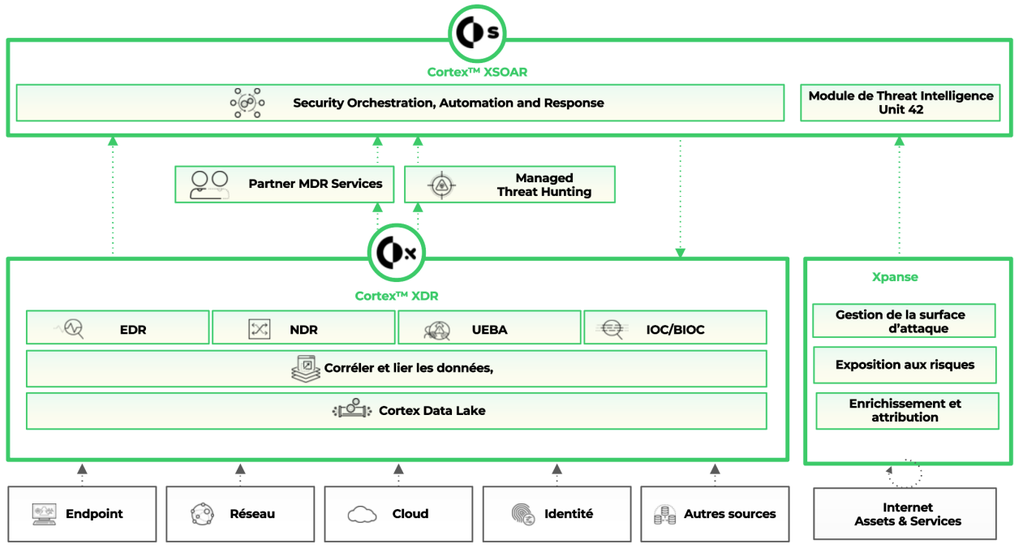
La plateforme Security Operations

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.

Réinventer la sécurité opérationnelle

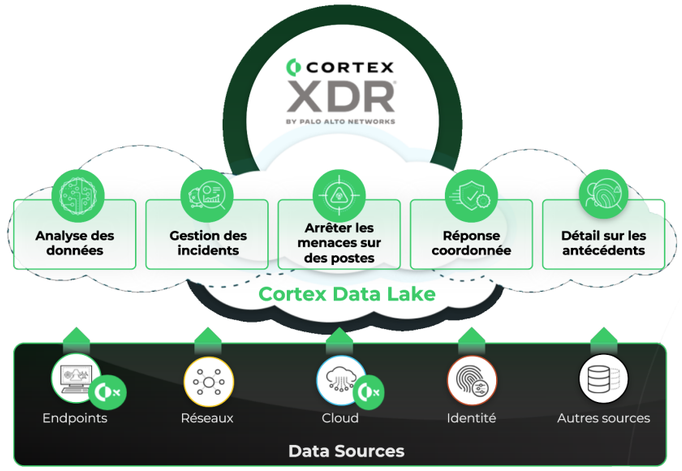
La plateforme Security Operations propose un ensemble de produits visant à détecter et répondre toujours plus efficacement et rapidement aux cyberattaques de demain.



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



L'outil d'eXtended Detection & Response le plus abouti du marché

Les évaluations MITRE ATT&CK® Enterprise constituent le test le plus rigoureux du secteur en matière de sécurité des terminaux. Elles mesurent la capacité d'une solution à se défendre contre les acteurs malveillants avancés grâce à des simulations d'attaques en conditions réelles.

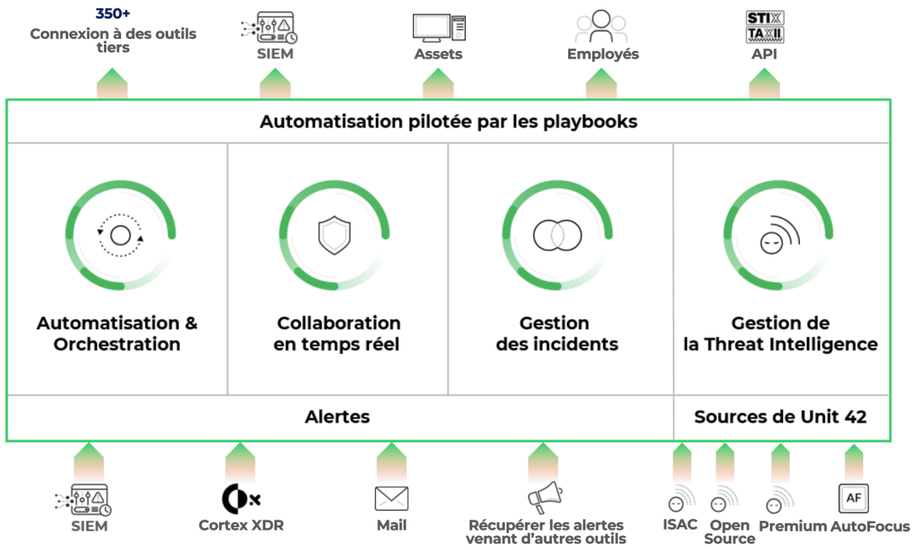
Lors de la sixième édition, MITRE ATT&CK® Enterprise a placé la barre plus haut, en proposant l'évaluation la plus exigeante et la plus réaliste à ce jour. Celle-ci comprenait des attaques étendues sur les plateformes Linux et macOS® et l'introduction de tests de faux positifs pour la première fois.

Palo Alto Networks a relevé le défi et obtenu les meilleurs résultats du secteur :

- Le premier fournisseur à atteindre une **couverture de détection de niveau technique à 100 %** sans délai ni modification de configuration.
- Couverture de **détection à 100 %** sur les surfaces d'attaque étendues de **macOS et Linux**.
- Le **taux de prévention le plus élevé avec zéro faux positif** susceptible de perturber les opérations critiques.

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 350 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

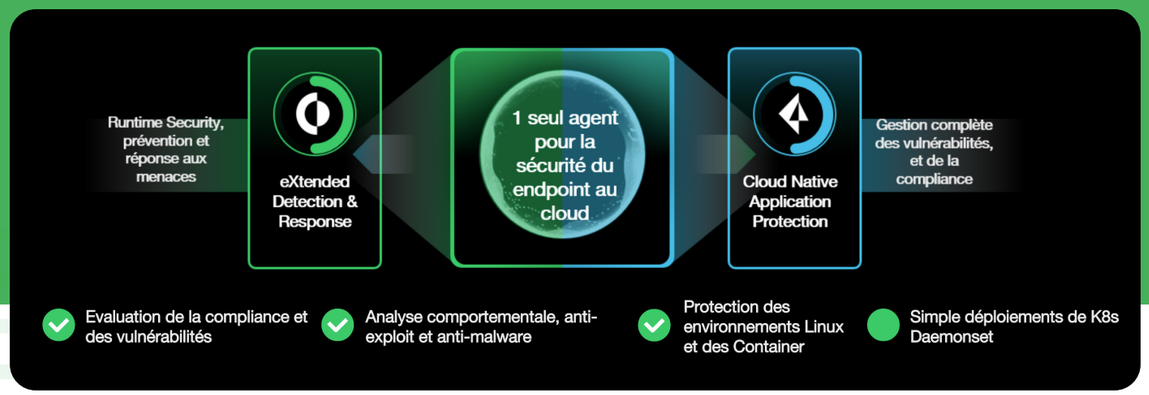
CORTEX XSIAM®
BY PALO ALTO NETWORKS

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) est une solution qui 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 ainsi en productivité tout en se consacrant à des besoins SecOps plus stratégiques.

Cortex Cloud
Quand Cortex et Prisma Cloud fusionnent !

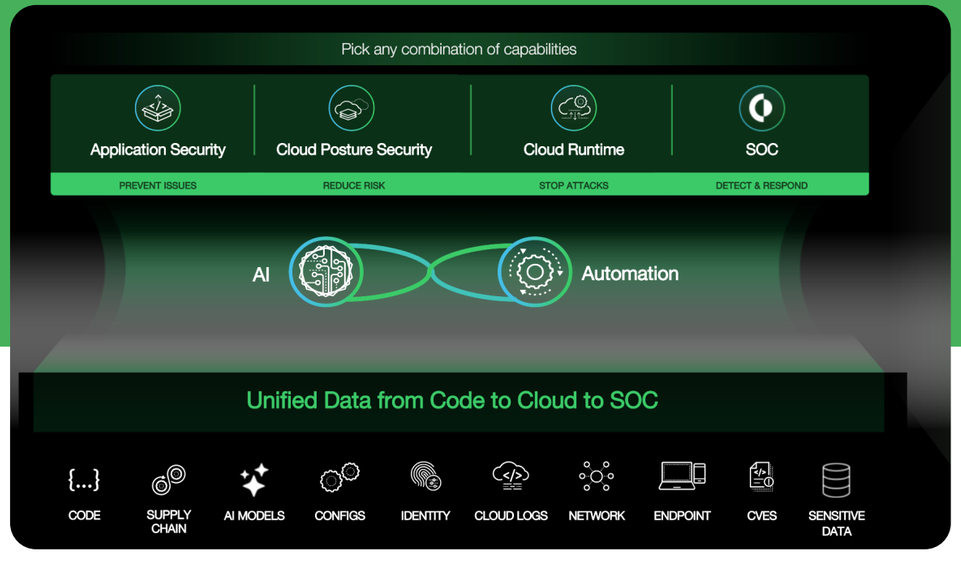
Avec l'introduction de **Cortex Cloud,** Palo Alto Networks fusionne sa plateforme Prisma Cloud avec la plateforme Security Operations.
Les outils connus tels que **CNAPP**, le **Code to Cloud**, le **CSPM**, ou encore le **CWPP**, sont tous concentrés dans la console de **SOC Cortex**, pour pouvoir répondre à tous les cas d'usages du CDR (**Cloud Detection & Response**)

Cortex permet de tirer parti des données de l'IA et des méthodes d'automatisations connues du SOC.



En convergeant les 2 plateformes de sécurité, Palo Alto Networks permet aux analyses SOC et DevOps de fonctionner de manière transparente du Code, au Cloud, au SOC, tout en se servant de l'IA et de l'automatisation.

Cortex Cloud propose 1 agent, 1 modèle de données, 1 interface, et 1 flux de travail, le tout dans 1 seule console.



Contactez-nous

Horaires d'ouverture :
9h-12h15 et 14h-18h CET
Du lundi au vendredi

Appelez le
+33 1 60 19 34 52

Visitez
www.miel.fr →

MIEL

/company/miel

/c/mielfrance

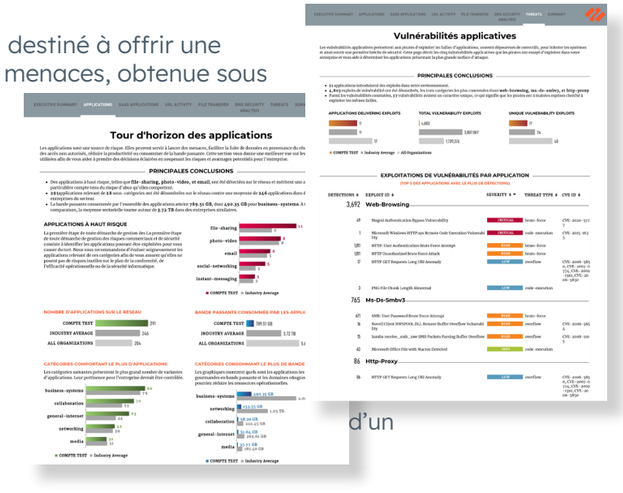
SLR : Security Lifecycle Review

Montrez la puissance de la plateforme Palo Alto Networks

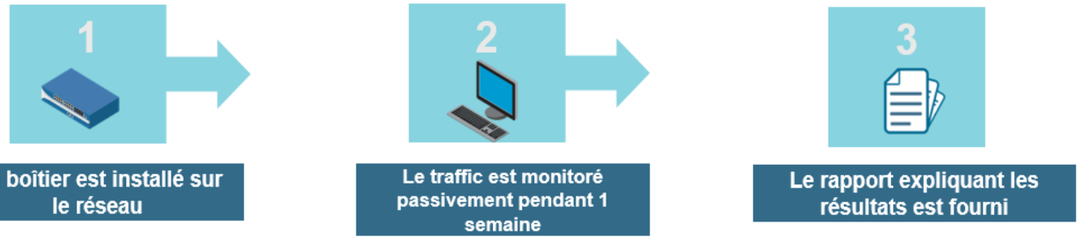
Le SLR (Security Lifecycle Review) est un outil destiné à offrir une visibilité sur les applications, les risques et les menaces, obtenue sous la forme d'un rapport généré sur la base d'informations recueillies par le firewall nouvelle génération grâce à une mise en place non intrusive.

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 partenaire en récupérant un fichier de logs.



d'un



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

AIOps : Artificial Intelligence for IT Operations

Renforcer la posture de sécurité grâce à des recommandations sur les meilleures pratiques et éliminer les risques

Suivre le cycle de vie de l'adoption des fonctions et services de sécurité configurés
Maximiser le retour sur investissement des NGFW en utilisant toutes les fonctionnalités disponibles et proposer des recommandations sur les meilleures pratiques

Remédier aux mauvaises configurations
L'analyse en direct des politiques détecte et suggère des remèdes aux anomalies qui dégradent la posture de sécurité

Améliorer de manière proactive la posture de sécurité
Corriger les mauvaises configurations, et mettre en place les meilleures pratiques avant les Commit

Résoudre les perturbations du pare-feu pour maintenir une santé et des performances optimales

Éviter de manière proactive les perturbations du pare-feu
Détecte les problèmes de santé et de performance du pare-feu jusqu'à 7 jours à l'avance avec des recommandations pour y remédier.

Relever les principaux défis opérationnels des FW
Résoudre les problèmes liés à l'utilisation des ressources, aux matériels, logiciels, à l'épuisement de la mémoire, aux logs, au trafic, à la surcharge, à la détection des vulnérabilités spécifiques aux fonctionnalités, etc.

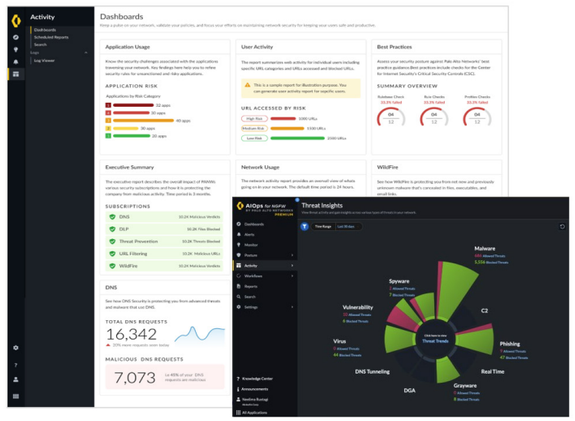
Planifier les mises à jour et minimiser les temps d'arrêt
Conseils sur les versions logicielles les mieux adaptées à votre environnement en fonction des fonctionnalités activées, des modèles NGFW et des vulnérabilités connues.

Une vue unifiée de l'efficacité de la sécurité

Connaître l'efficacité de votre sécurité
Voir les menaces les plus dangereuses et les plus récentes du réseau, celles qui ont été empêchées et celles qui requièrent une attention particulière

Comprendre l'évolution d'une menace
Exploiter le réseau partagé et les renseignements sur les menaces pour obtenir une visibilité sur les menaces avancées potentielles avec des mesures correctives actionnables pour arrêter les risques de sécurité émergents

Vue unifiée des artefacts de sécurité
Vue centralisée de l'activité à travers les applications, les menaces, les réseaux, les utilisateurs et les souscriptions de sécurité



Expedition

Migrez intelligemment et rapidement vers une configuration Palo Alto Networks

Expedition est un outil open-source qui va permettre d'accélérer la migration de configuration de firewalls traditionnels vers les technologies de firewall nouvelle génération Palo Alto Networks, donnant ainsi accès aux meilleurs processus et aux meilleures pratiques de protections contre les menaces.

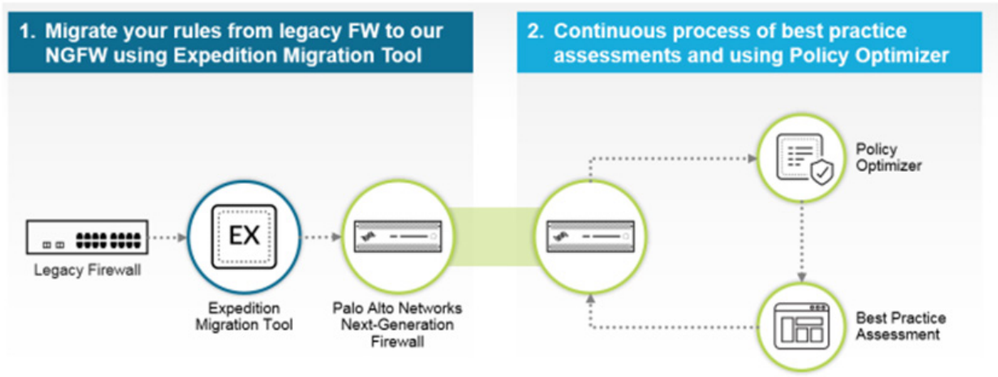
Expedition transpose facilement les règles de sécurité à la couche 3/4 des firewalls tiers vers des règles à la couche 7, améliorant ainsi la protection. Expedition aide à l'implémentation de ces règles à travers les technologies App-ID™, User-ID™ et Content-ID™ de Palo Alto Networks.

Expedition permet d'importer automatiquement les configurations des firewalls

- Cisco
- Fortinet
- Check Point
- Forcepoint
- Juniper
- IBM XG.

Les configurations d'autres types de firewalls peuvent être migrés par l'intermédiaire d'Expedition avec l'aide de scripts.

Expedition va automatiquement mettre à jour vos règles existantes. Il va également utiliser l'analytique pour générer et implémenter de nouvelles règles et des recommandations de configuration. L'objectif sera d'améliorer les contrôles de sécurité tout en optimisant les processus.



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.

Formations disponibles

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

- Formation mixte
- Durée : 35 heures (5 jours)
- Accessible

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

- Formation mixte
- Durée : 14 heures (2 jours)
- Accessible

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

- Formation mixte
- Durée : 14 heures (2 jours)
- Accessible

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

- Formation mixte
- Durée : 35 heures (5 jours)
- Accessible

Formation Palo Alto Networks PAN-EDU-260 : Palo Alto Networks Cortex™ XDR - Prevention and Deployment

- Formation mixte
- Durée : 21 heures (3 jours)
- Accessible

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

- Formation mixte
- Durée : 14 heures (2 jours)
- Accessible

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

- Formation mixte
- Durée : 28 heures (4 jours)
- Accessible

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

- Formation mixte
- Durée : 28 heures (4 jours)
- Accessible

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

- Formation mixte
- Durée : 21 heures (3 jours)
- Accessible

Formation Palo Alto Networks PAN-EDU-380 : Palo Alto Networks Cortex XDR : Automation and Orchestration

- Formation mixte
- Durée : 28 heures (4 jours)
- Accessible

Détails des formations, dates et pré-inscriptions
01 60 19 16 27