Sécurité Next-Generation

Une plateforme de sécurité pionnière et de classe Enterprise pour les réseaux, le cloud et les terminaux

Réseaux de Palo Alto: les points clés

- Une plateforme de sécurité unique en son genre et hautement intégrée à l'échelle de l'industrie
- Protection transparente pour le réseau, le multi-cloud et les terminaux
- Appliance physique avec hardware optimisé
- Appareils virtuels pour les clouds privés, publics et hybrides
- Analyse en temps réel et en single-pass de l'ensemble du flux de données
- Décryptage et cryptage SSL
- Ouvert et vévolutif
- Gestion centralisée

L'entreprise californienne Palo Alto Networks a été fondée en 2005 par l'expert en sécurité Nir Zuk. Palo Alto Networks est le premier fournisseur mondial de solutions de cybersécurité et est connu pour remettre constamment en question l'état actuel de la sécurité. Ses développements sont axés sur la protection efficace des utilisateurs contre les cyberattaques à l'ère numérique. Les solutions de sécurité de Palo Alto Networks ont la confiance de dizaines de milliers d'entreprises et de leurs clients, administrations publiques et organisations. Cette plateforme de sécurité révolutionnaire protège les utilisateurs grâce à l'innovation continue dans la transformation numérique. Elle combine les dernières avancées en matière de sécurité, d'automatisation et d'analyse.

En fournissant une véritable plateforme et en favorisant un réseau croissant, les clients bénéficient de solutions de cybersécurité hautement efficaces et novatrices pour le cloud, les réseaux et les terminaux. Grâce à ses solutions de sécurité innovantes, Palo Alto Networks a réussi à devenir en quelques années le fabricant de solutions de sécurité qui connaît la croissance la plus rapide. Actuellement, plus de 75 000 clients de diverses industries dans 150 pays comptent sur la «Next Generation Security Platform» de Palo Alto Networks. Plus de 85% des sociétés Fortune 100 et plus de 63% des sociétés Global 2000 font confiance à Palto Alto Networks pour accroître leur cybersécurité.

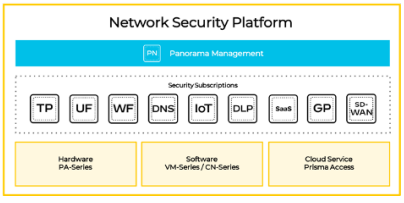
Une sécurité globale pour l'ensemble de l'entreprise

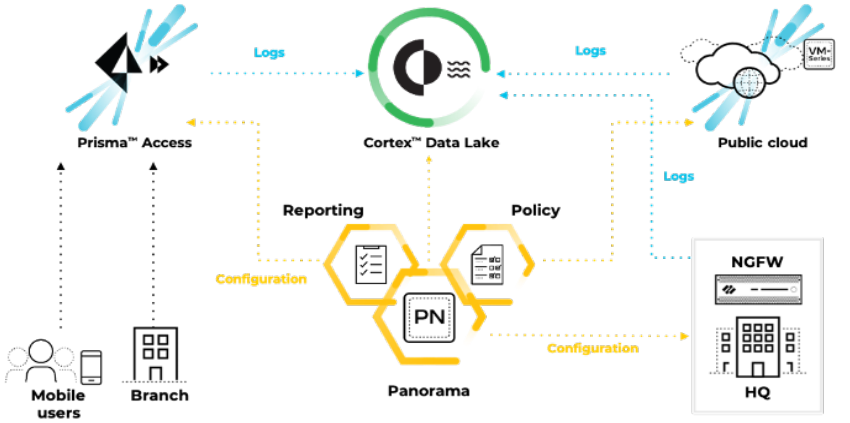
La plateforme de sécurité Next Generation de Palo Alto Networks protège le réseau d'entreprise et tous les services cloud utilisés – qu'ils soient privés, publics ou hybrides – et utilise l'intelligence artificielle pour détecter et défendre automatiquement contre tous les types de cyberattaques.

Secure the Enterprise: Strata Next Generation Firewall

Le pare-feu Next Generation de Palo Alto Networks a été conçu dès le départ pour échapper à l'efficacité limitée du contrôle exclusif des adresses IP et des numéros de port (Stateful Inspection). Grâce à la combinaison de l'identification de l'utilisateur (User ID), de l'identification de l'application (App ID), du contrôle du contenu (Content ID) et de l'identification du nouveau dispositif (Device ID), le trafic peut être analysé et régulé en détail. Même le trafic crypté peut être décrypté et vérifié, les méthodes de dissimulation sont ainsi identifiées.

Le pare-feu Next Generation est disponible sous forme d'Appliance avec différents niveaux de performance et en tant que solution intégrée dans des environnements virtuels tels que VMware.



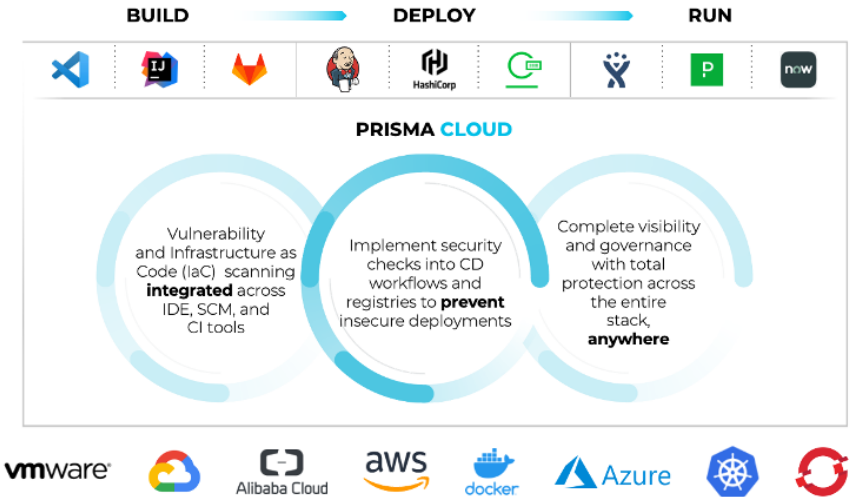


Panorama Management est la plateforme de gestion centralisée pour les appareils, les politiques de sécurité, les changements de configuration, les logs et le monitoring.

Toutes les fonctions sont également disponibles pour toutes les plateformes. Les souscriptions de sécurité sont disponibles pour 1, 3 et 5 ans. Threat Prevention, URL Filtering, WildFire Sandboxing, GlobalProtect pour la protection des appareils mobiles, DNS Security, SD-WAN et Enterprise DLP sont disponibles sous forme de souscriptions complémentaires. IoT Security automatise l'orchestration du cycle de vie de l'IoT et protège contre les vulnérabilités et les menaces. La série VM est une variante virtualisée du pare-feu Next Generation qui peut être déployée dans de nombreux environnements de cloud privés et publics – basés sur des technologies de VMware, Cisco, KVM, OpenStack, Nutanix, Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud et Alibaba Cloud. Les mêmes services de sécurité sont disponibles que pour les versions matérielles du pare-feu.

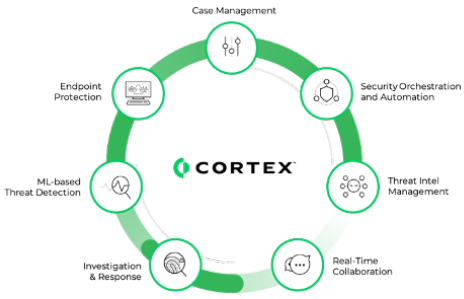
Secure the Cloud: Prisma

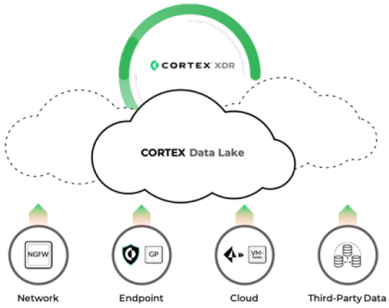
Prisma Cloud est une plateforme de sécurité native du cloud qui offre à la fois des fonctions pour la gestion du Cloud Security Posture Management (CSPM) et de la Cloud Workload Protection (CWP). Les applications et les données sont protégées tout au long du cycle de vie des applications dans des environnements multi-cloud et hybrides. Prisma Cloud couvre les domaines fonctionnels suivants: Visibilité, compliance et gouvernance, sécurité des environnements hôtes, des conteneurs et des environnements sans serveur, sécurité des applications web et des API, détection des menaces, micro segmentation basée sur l'identité, IAM et sécurité des données. Prisma Access SASE (Secure Access Service Edge) fournit à tous les utilisateurs un accès sécurisé aux applications dans le cloud, dans le centre de données et sur Internet, qu'ils soient accessibles depuis une succursale, en déplacement, en home-office ou au siège social.
Avec CloudGenix, une offre SD WAN basée sur le cloud, en plus des critères classiques tels que Jitter, Packet Loss, etc., il inclut également la disponibilité de l'application.
En tant que Cloud Access Security Broker (CASB) basé sur le cloud, Prisma SaaS assure l'utilisation sécurisée des applications et des services cloud.



Secure the Future: Cortex

Cortex est une plateforme de détection, de défense et d'automatisation. La mission de Cortex est triple: «Prévenir tout ce qui est possible, identifier et enquêter rapidement sur ce qui ne peut être évité, automatiser la réponse et apprendre à chaque incident.» Des technologies de pointe telles que le machine learning et l'IA sont utilisées.
Cortex XDR Prevent empêche les menaces connues et inconnues sur les terminaux. Cortex XDR Pro fournit également une enquête automatisée, une analyse basée sur les règles et le comportement, tout cela fournit ainsi une réponse intégrée aux incidents de sécurité des endpoints.





Cortex XSOAR (Security Orchestration, Automation and Response) orchestre et automatise les processus du Security Operations Center. XSOAR intègre d'innombrables sources de données et utilise des playbooks standardisés et automatisés pour accélérer l'analyse et la réponse. XSOAR vise ainsi le juste équilibre entre l'exécution rapide des machines et le contrôle humain progressif. En tant que référentiel, **Cortex Data Lake** collecte, intègre et normalise les données de sécurité des solutions Palo Alto Networks pour le réseau, le cloud et les terminaux, ainsi que les logs de fournisseurs tiers.

Dépliant du fabricant
Palo Alto Networks

La cybersécurité repensée

Les clients de Palo Alto Networks bénéficient de solutions de cybersécurité très efficaces et innovantes pour les clouds, les réseaux et les endpoints.

Next-Generation Threat Intelligence

Les informations sur les menaces provenant de milliers d'appareils et de millions de terminaux, de fournisseurs de Threat-Feed et d'autres partenaires sont automatiquement collectées, regroupées et analysées dans le Threat Intellgence Cloud. La Unit 42, l'équipe Threat-Research de Palo Alto Networks, apprend de ces données comment les attaquants ont évoluer leurs méthodes. Grâce à ces connaissances, de nouvelles mesures de défense sont élaborées et mises à la disposition des clients en quelques minutes. Le degré élevé d'automatisation aide les organisations à répondre de manière adéquate aux menaces modernes et à stopper les attaques sans intervention manuelle.

Zero Trust Network Access

Palo Alto Networks recommande et soutient le Zero Trust Network Access. ZTNA est une stratégie qui contribue à prévenir le vol de données en n'autorisant pas l'accès sans vérification préalable au sein d'une organisation. Basé sur le principe «Ne jamais faire confiance, toujours vérifier», ZTNA protège contre la propagation de codes malveillants dans les réseaux.

Les services de Palo Alto Networks

Palo Alto Networks offre divers services de support et services professionnels. Les utilisateurs peuvent choisir entre un support Premium ou Platinum, fourni par Palo Alto Networks ou par des Authorized Support Center (ASC).

Services de support

Lorsque chaque minute compte, vous pouvez compter sur l'aide rapide des experts de Palo Alto Networks. L'équipe d'assistance mondiale et les vastes ressources aident les clients à éviter les temps d'arrêt, à minimiser les risques et à optimiser les opérations informatiques.

Focused Services

Les Focused Services proposent un support sur mesure par l'intermédiaire d'un gestionnaire de compte dédié. Grâce à ces services, les utilisateurs bénéficient d'une assistance individuelle et personnalisée, de bilans hebdomadaires, d'une analyse des incidents critiques, d'une aide à la planification des mises à niveau et de Business Reviews trimestriels.

BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com

IT Security Distribution