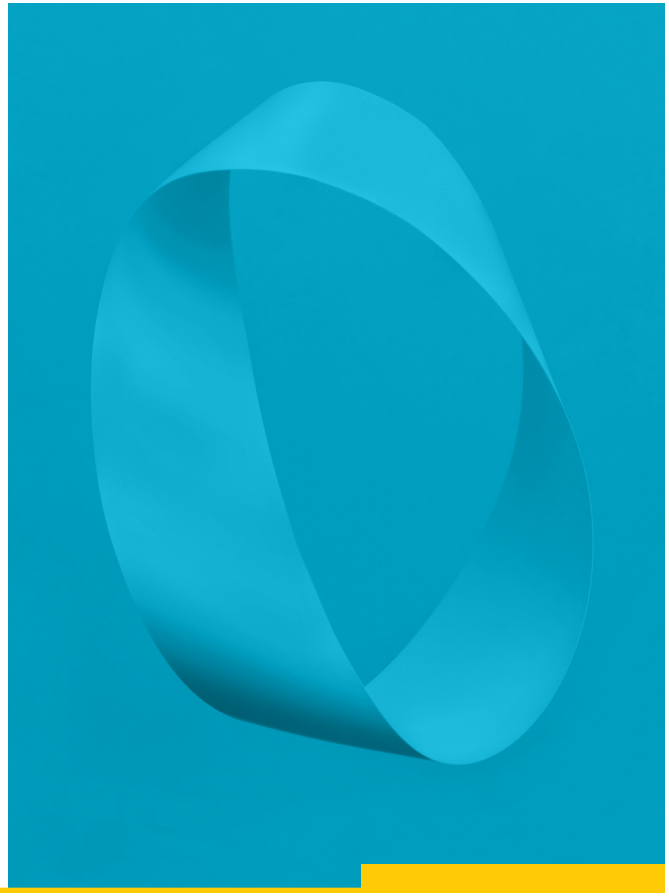
Cloud privé : cinq problématiques de sécurité majeures

Network Security Platform lève les freins à l'implémentation du Zero Trust

paloalto NETWORKS | STRATA BY PALO ALTO NETWORKS



Sommaire

Les clouds privés ont le vent en poupe

Le cloud se décline en deux formes, l'une publique et l'autre privée, qui se distinguent sous bien des aspects. Les fournisseurs de cloud public (CSP) proposent des services de calcul et de stockage qu'ils facturent à l'usage, faisant totalement abstraction de tous les rouages internes (le matériel et les logiciels) qui sous-tendent la plateforme. Tout ce que le client voit, ce sont ses données et ses applications. Côté pile, les avantages sont nombreux : réduction des dépenses d'investissement (CapEx), disparition des cycles de modernisation coûteux, évolutivité quasi illimitée, fiabilité à toute épreuve, agilité métier et sauvegarde fiable des données.

Côté face, le cloud public oblige le client à accepter une certaine perte de contrôle. Sur le plan de la sécurité, vos applications et vos données partagent une infrastructure commune avec d'autres entreprises, ce qui peut s'avérer problématique dans des secteurs sensibles comme la santé ou les services financiers. Par ailleurs, l'abstraction de la plateforme constitue un blocage pour les industries fortement réglementées (matériel médical, pharmaceutique, etc.), qui requièrent une validation dès qu'un changement impacte les workflows, les données ou la logique métier. Pour toutes ces raisons, bon nombre d'entreprises choisissent d'héberger leurs applications et leurs données sensibles dans des clouds privés, tout en faisant appel aux CSP à des fins d'évolutivité et de mise à proximité des services.

Si le cloud public fait aujourd'hui l'objet de toutes les attentions, force est de constater que l'architecture privée a nettement gagné du terrain au cours des dernières années. Pour preuve, les entreprises utilisent en moyenne 2,6 clouds publics et 2,7 clouds privés, tandis que deux fois plus de clouds privés (2,2 contre 1,1) sont aujourd'hui en cours d'expérimentation (cf. tableau ci-dessous). La plupart des organisations misent ainsi sur une combinaison d'architectures publiques et privées, c'est-à-dire un environnement cloud hybride.

	Public	Privé
En usage	2,6	2,7
En cours d'expérimentation	1,1	2,2
Total	**3,7**	**4,9**

Nombre de clouds qu'utilisent en moyenne les entreprises

À suivre : les clouds privés présentent des problématiques de sécurité uniques.

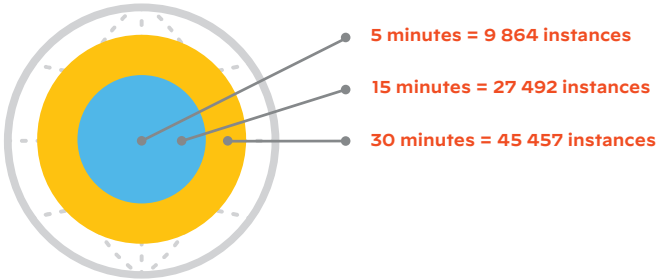
Sécurité du cloud privé : une équation de plus en plus compliquée

En règle générale, la sécurité informatique n'est jamais un long fleuve tranquille. Mais avec le cloud privé, on monte encore d'un cran dans la difficulté, et ce en raison de plusieurs facteurs.

Surface d'attaque élargie – L'émergence du télétravail et de la mobilité multiplie les points d'entrée, ce qui fragilise la sécurité des clouds privés. Quant à la généralisation des supply chains intégrées, elle pose un risque supplémentaire étant donné que chaque intervenant de la chaîne n'applique pas forcément le niveau de sécurité adéquat sur ses terminaux. On estime aujourd'hui que quatre cyberattaques sur dix émanent non pas de l'entreprise victime, mais de sa supply chain étendue.

Menaces plus sophistiquées – Aujourd'hui, les menaces avancées contournent les systèmes de sécurité, en se déclinant par exemple sous la forme de variantes ou en chiffrant le trafic entre le malware et l'attaquant externe qui le pilote. Ces offensives exploitent des vulnérabilités non divulguées ou utilisent des variantes de malwares polymorphes qui échappent aux solutions de détection basées sur les signatures.

Fenêtres d'action réduites – Ces menaces furtives sont aussi plus rapides que jamais. Aujourd'hui, un malware peut commencer à chiffrer vos données à peine quelques minutes après avoir pénétré votre réseau. Résultat : le danger se répand comme une traînée de poudre dans les infrastructures qui font l'impasse sur la segmentation. Au cours d'une étude interne menée récemment par l'équipe Unit 42 de Palo Alto Networks, une menace avancée est parvenue à se répliquer dans plus de 45 000 instances en 30 minutes (voir l'illustration ci-dessous).



À suivre : les réseaux cloud privés redessinent les contours du périmètre traditionnel.

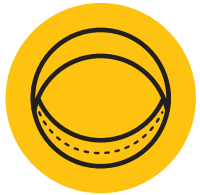
Problématique nº 1 : l'architecture cloud brouille les lignes de démarcation

Le modèle de sécurité classique se fonde sur une frontière nette entre votre environnement interne et le monde extérieur : ce périmètre délimite les zones de confiance, situées à l'intérieur du réseau, par opposition à l'environnement extérieur considéré comme non fiable. Dans une telle perspective, vos informations sensibles sont en sécurité tant que vos défenses couvrent efficacement tous les points d'entrée possibles.

Le problème est que l'architecture cloud estompe la démarcation entre le périmètre intérieur et extérieur. Bureau, télétravail, itinérance : les utilisateurs peuvent se connecter depuis n'importe où. De même, une application hébergée dans le data center local peut très bien traiter des données situées dans le cloud, générant ainsi des flux continus de trafic entrant et sortant.

On pourrait représenter le modèle de sécurité traditionnel par une bande de papier formant une simple boucle. Ici, la face intérieure est bien distincte de la face extérieure : il est impossible de relier les deux côtés en partant d'une ligne droite.

En ce sens, l'architecture cloud équivaut plutôt au ruban de Möbius – une bande fermée, retournée sur elle-même, qui ne présente qu'une seule face. Autrement dit, pour rejoindre son point de départ, votre tracé parcourt nécessairement la surface tout entière. Dans un même ordre d'idée, la sécurité cloud ne fait aucune distinction entre l'intérieur et l'extérieur. Aucun équipement, utilisateur ou application ne peut être jugé fiable avant d'avoir prouvé son identité, son authenticité et sa légitimité.



La boucle simple présente une face intérieure et extérieure.

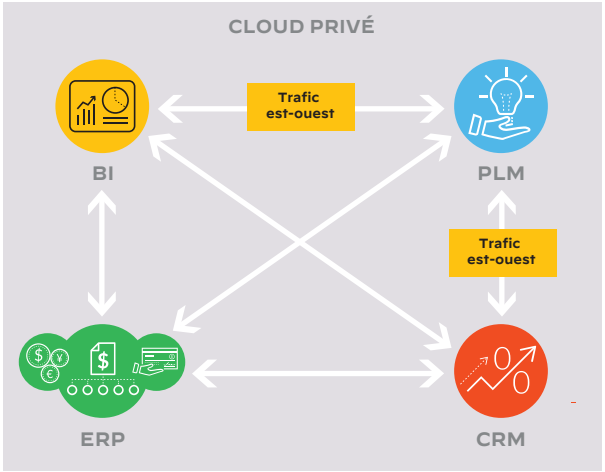
Le ruban de Möbius possède une seule face : l'intérieur et l'extérieur se confondent.

À suivre : les applications métiers intégrées mettent sous pression la sécurité des clouds privés.

Problématique nº 2 : le modèle traditionnel peine face aux applications métiers intégrées

Aujourd'hui, chaque entreprise est par essence une structure numérisée dont l'activité repose sur un socle d'applications métiers indispensables. Le PLM (Product Lifecycle Management), par exemple, régit le cycle de vie complet d'un produit – de la conception à la fabrication – et sert de référentiel centralisé pour la propriété intellectuelle ainsi créée. Les systèmes ERP (Enterprise Resource Planning) gèrent quant à eux les aspects financiers des processus métiers, de l'approvisionnement au traitement des commandes, en passant par la planification de la production et la fabrication de produits finis. Les équipes commerciales et marketing s'appuient pour leur part sur des solutions CRM (Customer Relationship Management) et BI (Business Intelligence) pour cibler et nouer le dialogue avec les clients et prospects de l'entreprise. La liste, si nous devions être exhaustifs, serait encore bien longue.

Or, les applications métiers n'existent pas en vase clos : elles s'intègrent dans une matrice interconnectée qui facilite la collaboration, raccourcit les délais de commercialisation (TTM) et extrait de la valeur à partir du volume massif de données que brasse l'entreprise. Ces intégrations génèrent de ce fait un trafic inter-applicatif important – que l'on qualifie de flux est-ouest en raison de son mouvement latéral –, qu'il faut sécuriser contre les malwares, les menaces ciblées, les campagnes de phishing et autres exploits avancés. Le problème, c'est que les stratégies de sécurité traditionnelles ne sont ni assez flexibles, ni assez puissantes pour mener à bien cette mission.

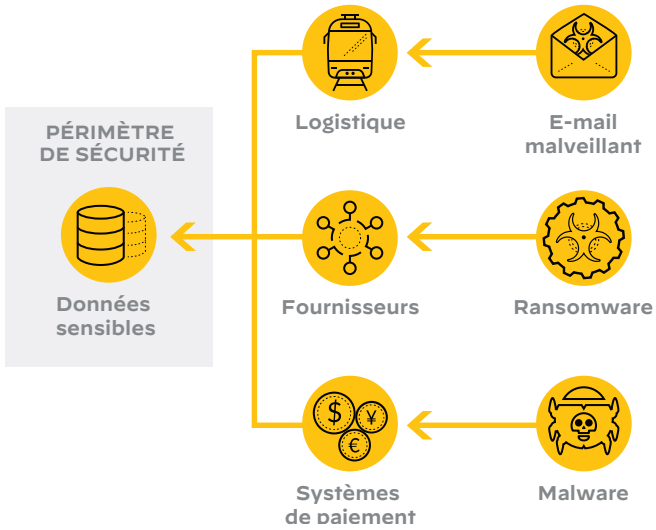


À suivre : les supply chains intégrées créent des vulnérabilités.

Problématique nº 3 : les intégrations externes ouvrent des brèches dans le périmètre de sécurité du cloud privé

Face aux exigences de plus en plus fortes qui émanent à la fois des clients et du marché, les supply chains linéaires traditionnelles prennent désormais la forme de maillages logistiques complexes et interconnectés. Souvent, vos fournisseurs ont un accès direct à certaines parties de votre réseau. Ils disposent eux-mêmes de leurs propres supply chains intégrées, prolongement direct d'un réseau parent. Il existe d'autres vulnérabilités associées aux intégrations externes, notamment en ce qui concerne les systèmes de paiement et la logistique.

Au final, ces intégrations tierces augmentent de façon significative le nombre de nœuds à sécuriser, ce qui non seulement élargit la surface d'attaque dans les mêmes proportions, mais aussi atténue davantage les frontières de la périphérie. Résultat, le risque de compromission augmente considérablement : Accenture estime ainsi qu'environ quatre cyberattaques sur dix émanent non pas de l'entreprise victime, mais de sa supply chain étendue.

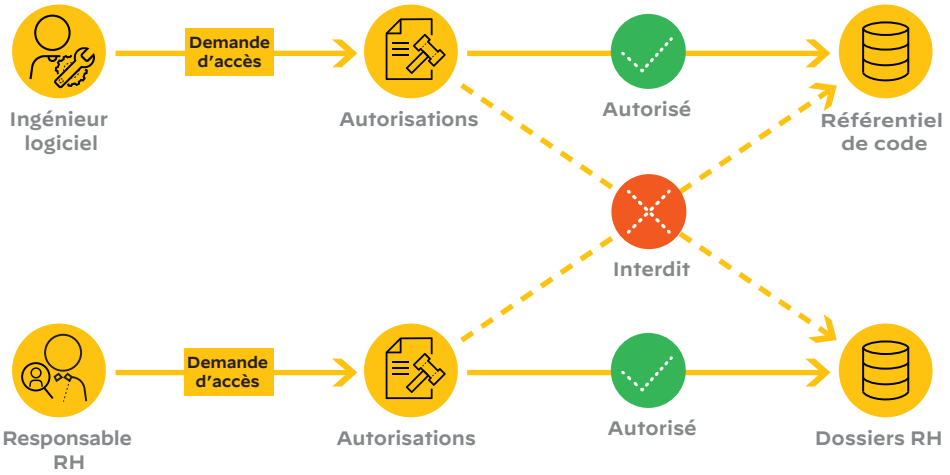


À suivre : les enjeux de conformité du cloud privé.

Problématique nº 4 : les infrastructures cloud mettent les cadres de conformité existants à rude épreuve

Aux États-Unis, les entreprises cotées en bourse doivent se conformer à la loi Sarbanes-Oxley (SOX). Dans les secteurs hautement régulés, le non-respect des normes et régimes réglementaires (par exemple, HIPAA[1] pour la santé, PCI DSS[2] dans le retail, ou encore ACH[3] pour les services bancaires) expose les organisations à des risques considérables. Or, le transfert d'équipements et de données vers le cloud privé peut avoir un effet significatif sur la posture de conformité.

La création d'une stratégie de conformité efficace dans le cloud passe par une modification du système de sécurité. Premier point essentiel, une gestion centralisée qui permet aux responsables sécurité d'harmoniser les politiques à l'échelle de l'environnement hybride. Une autre problématique concerne l'émergence des containers Kubernetes dans le développement d'applications cloud, qui restreignent l'efficacité des pare-feu traditionnels – ces derniers ne pouvant accéder directement aux containers. Enfin, le contrôle des accès doit être resserré à l'aide de politiques basées sur le principe du moindre privilège et de l'authentification multifacteur. Le but est d'attribuer aux utilisateurs les seules autorisations dont ils ont besoin pour accomplir les missions entrant dans le cadre de leurs fonctions. Par exemple, un ingénieur logiciel requiert l'accès au référentiel de code, mais pas aux dossiers RH.



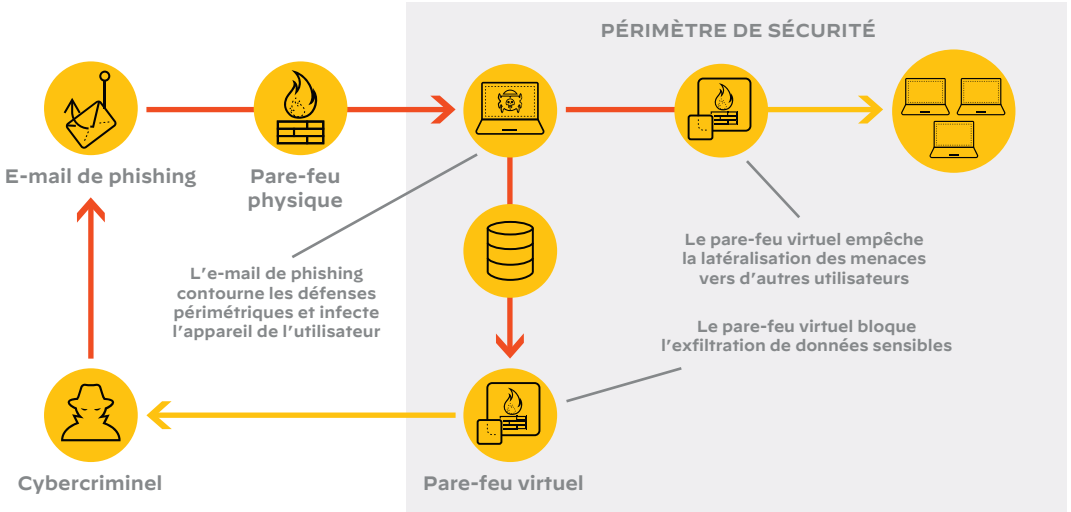
[1] Health Insurance Portability Accountability Act.
[2] Payment Card Industry Data Security Standard.
[3] Automated Clearing House.

À suivre : les environnements virtualisés posent des problèmes bien spécifiques aux pare-feu.

Problématique nº 5 : qui dit environnement virtuel, dit pare-feu virtuel

Les pare-feu nouvelle génération (NGFW) forment aujourd'hui la pierre angulaire de la sécurité réseau. Ils protègent votre infrastructure contre les menaces au niveau des couches L3 et L4 du modèle OSI (réseau et transport, respectivement), ainsi que contre les attaques visant les applications (L7) – notamment les techniques DDoS, le HTTP flood et les injections SQL. Jusqu'à récemment, les NGFW étaient déployés exclusivement sous la forme d'équipements physiques, qui sont par nature difficiles à déplacer au sein de l'architecture. Cette approche, quoiqu'adaptée aux data centers statiques, présente des limites dans les environnements virtualisés dynamiques d'aujourd'hui.

C'est là que les pare-feu virtuels entrent en jeu. Ces NGFW logiciels polyvalents possèdent les mêmes fonctionnalités que leurs pendants traditionnels, avec en prime la capacité à suivre automatiquement les applications et les workloads au sein de l'environnement virtualisé. D'un côté, les pare-feu matériels protègent les données et les applications contre les menaces externes au niveau du périmètre de sécurité ; de l'autre, les pare-feu virtuels sécurisent le trafic entre les équipements et les workloads au sein du périmètre. Les e-mails de phishing, par exemple, esquivent souvent les défenses périmétriques et parviennent jusqu'aux utilisateurs qui, peu méfiants, risquent d'ouvrir un malware.

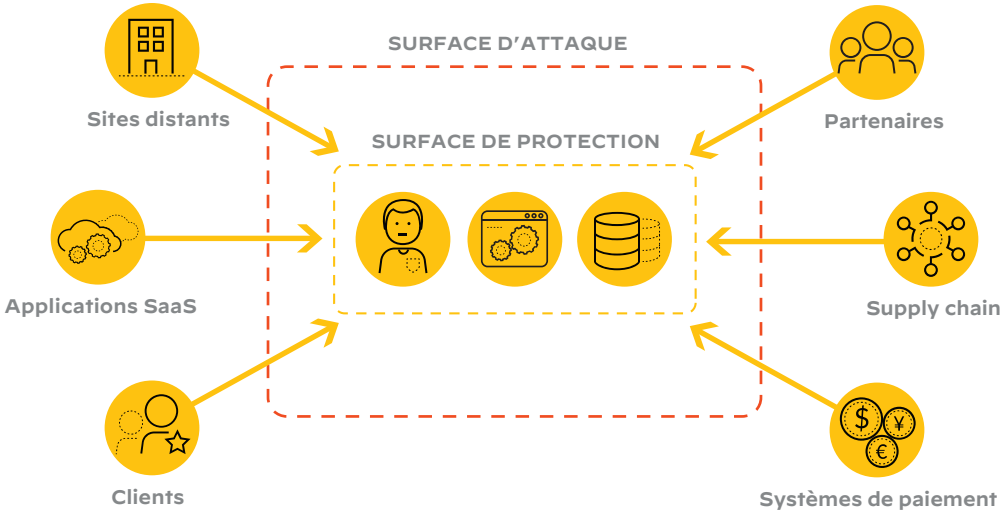


À suivre : la sécurité des environnements cloud privés requiert une approche Zero Trust.

L'approche Zero Trust : ne jamais faire confiance, toujours vérifier

Le Zero Trust désigne un ensemble de pratiques de sécurité éliminant toute notion de confiance implicite, le but étant de prévenir les compromissions de données dans les environnements virtualisés. Fondée sur le principe de « ne jamais faire confiance, toujours vérifier », une architecture Zero Trust protège les environnements numériques en agissant sur quatre leviers : segmentation du réseau, prévention des mouvements latéraux, prévention des menaces sur la couche L7 et simplification du contrôle granulaire des accès utilisateurs.

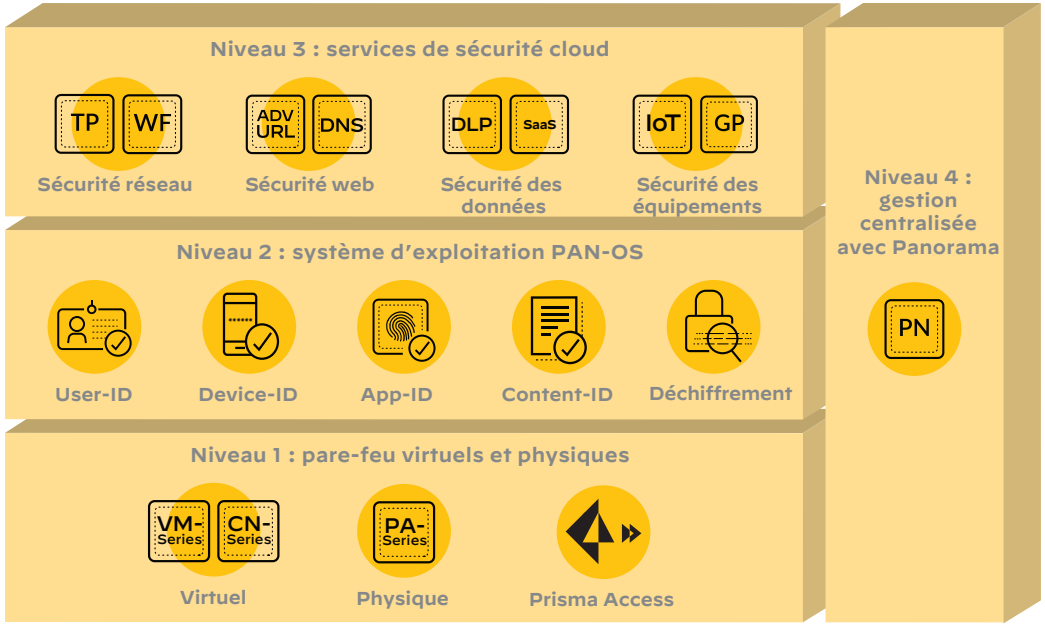
La mise en œuvre d'une stratégie Zero Trust implique tout d'abord un changement fondamental de paradigme. Le modèle de sécurité traditionnel repose sur le concept de surface d'attaque, c'est-à-dire la somme des équipements et des connexions par lesquels un hacker pourrait tenter de percer les défenses réseau. Le Zero Trust renverse cette notion en mettant l'accent sur la surface de protection : autrement dit les données, applications, ressources et services à protéger. Largement plus petit que la surface d'attaque, cet espace est aussi toujours identifiable.



À suivre : l'implémentation du Zero Trust passe par une plateforme conçue pour le Zero Trust.

Network Platform Security : une solution pensée pour le Zero Trust

À l'heure où les entreprises adoptent des architectures cloud hybrides et décentralisent leurs effectifs (sites distants, télétravail et utilisateurs mobiles), les solutions traditionnelles et les produits spécialisés et non intégrés ne sont plus de taille. Dans ce contexte, la mise en place d'une architecture Zero Trust requiert une offre intégrée comprenant des NGFW, un OS de pare-feu, des services de sécurité et une gestion centralisée. C'est justement ce que propose Palo Alto Networks avec Network Security Platform.

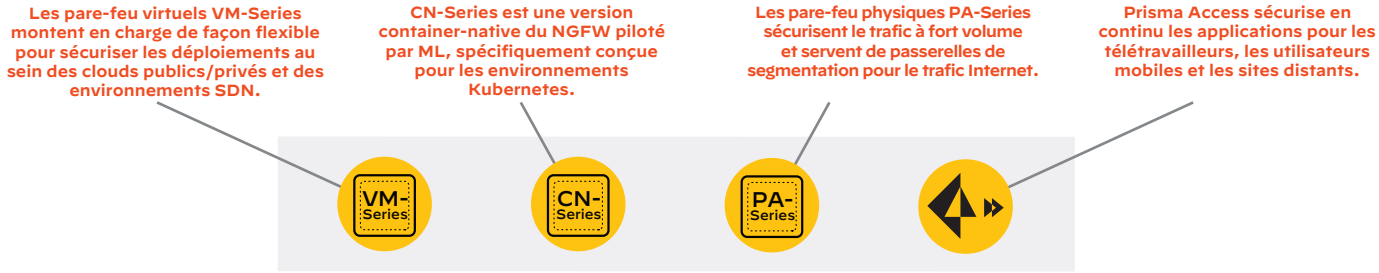


À suivre : la plateforme se compose de quatre niveaux, à commencer par les pare-feu.

Niveau 1 : pare-feu physiques et virtuels

Nos NGFW innovants aident les entreprises du monde entier à sécuriser leur infrastructure face aux attaques avancées. Chez Palo Alto Networks, nous voulons rendre chaque jour un peu plus sûr que le précédent pour nos clients. C'est pour cette raison que nous leur offrons des solutions capables de lutter efficacement contre les dernières menaces émergentes. Disponibles aux formats physique, virtuel, containerisé et cloud, nos NGFW sont plébiscités par les experts du secteur.

En 2021, Palo Alto Networks a figuré pour la dixième année consécutive au rang de Leader du Gartner® Magic Quadrant™ des pare-feu réseau, arrivant même en tête sur les axes « Capacité d'exécution » et « Exhaustivité de la vision ».



À suivre : l'OS de pare-feu joue un rôle central dans la sécurité Zero Trust.

Niveau 2 : système d'exploitation PAN-OS

PAN-OS, le système d'exploitation avancé qui équipe nos pare-feu, mobilise toute la puissance du machine learning et de l'analytique pour identifier efficacement les utilisateurs, les applications, les équipements et le contenu. Il permet également de lutter contre les nouvelles menaces basées sur les empreintes digitales et les signatures. Grâce à la mise à jour constante des modèles ML, PAN-OS détecte les attaques de phishing avec davantage d'efficacité. D'autre part, le système d'exploitation collecte les données télémétriques, mais aussi suggère des politiques et des changements de configuration pour réduire les risques et la probabilité d'erreur humaine. L'illustration ci-dessous décrit les fonctionnalités essentielles de PAN-OS qui assurent la sécurité Zero Trust des environnements cloud privés.

PAN-OS

FONCTIONNALITÉS PAN-OS

User-ID
Valide l'identité des utilisateurs au moyen d'une authentification forte.

Device-ID
Vérifie l'intégrité de chaque workload et équipement du réseau, y compris l'IoT.

App-ID
Applique des politiques du moindre privilège pour interdire les accès non autorisés.

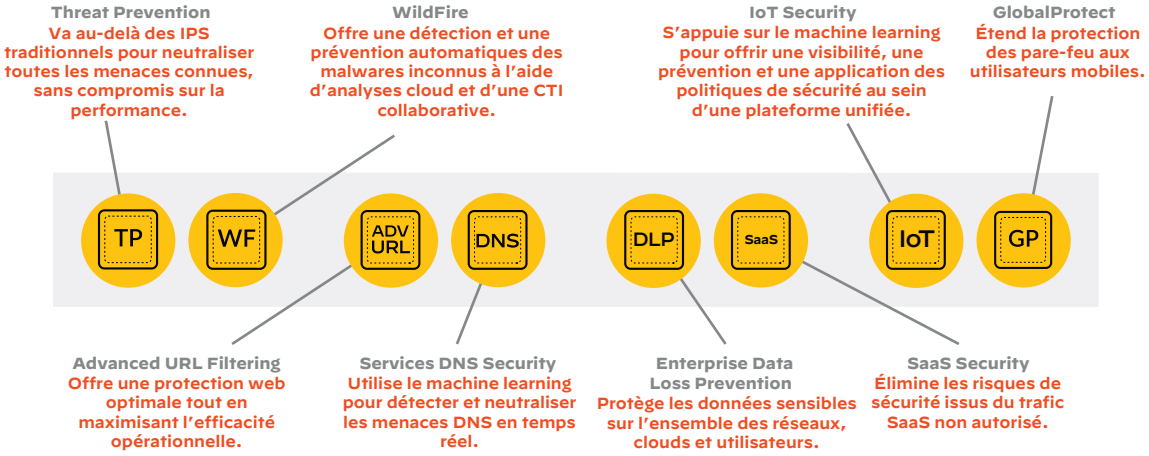
Content-ID
Bloque le transfert non autorisé de fichiers et de données sensibles (p. ex., numéros de CB et de sécurité sociale).

Déchiffrement
Analyse l'ensemble du trafic réseau à la recherche d'activités malveillantes et de vols de données.

À suivre : services de sécurité en mode cloud – un choix à la fois flexible et économique.

Niveau 3 : services de sécurité en mode cloud

Les NGFW virtuels au format logiciel de Palo Alto Networks adoptent une approche unique et efficace des services de sécurité cloud (CDSS). Avec Palo Alto Networks, vous pouvez souscrire uniquement les services dont vous avez besoin à un instant *t*, puis modifier vos choix à la volée à mesure que vos impératifs de sécurité évoluent. Vous bénéficiez à la clé d'une maîtrise optimale sur votre posture de sécurité, doublée d'une flexibilité inégalée pour répondre aux nouvelles menaces.

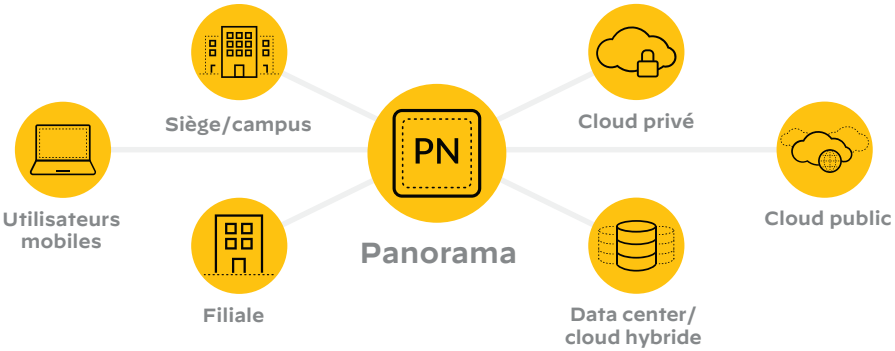


À suivre : la complexité du cloud impose une gestion centralisée.

Niveau 4 : gestion centralisée avec Panorama

Les grandes entreprises déploient généralement plusieurs NGFW sur leurs réseaux, ce qui rend la gestion et la surveillance de ces pare-feu particulièrement contraignante en raison des configurations complexes et de la multiplication des consoles. Cette situation augmente les coûts d'administration et dégrade la posture de sécurité.

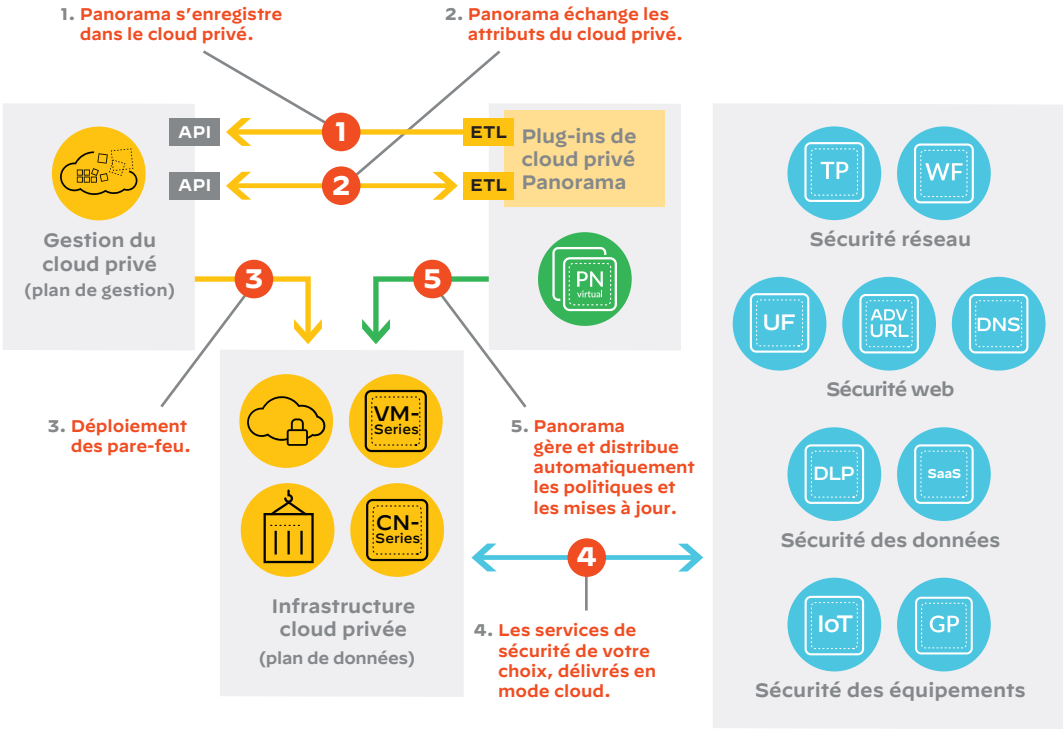
Pare-feu périmétriques, sites distants, environnements cloud et data centers : Panorama™ offre une gestion et une visibilité centralisées pour l'ensemble des pare-feu Palo Alto Networks, peu importe leur format ou leur emplacement. Les administrateurs disposent d'un éclairage approfondi sur les applications, les utilisateurs, les équipements et le contenu pour l'ensemble du trafic réseau et des menaces. Grâce à cette centralisation, Panorama accélère le déploiement et renforce la protection du réseau.



À suivre : découvrez comment fonctionne Network Security Platform.

La plateforme en action

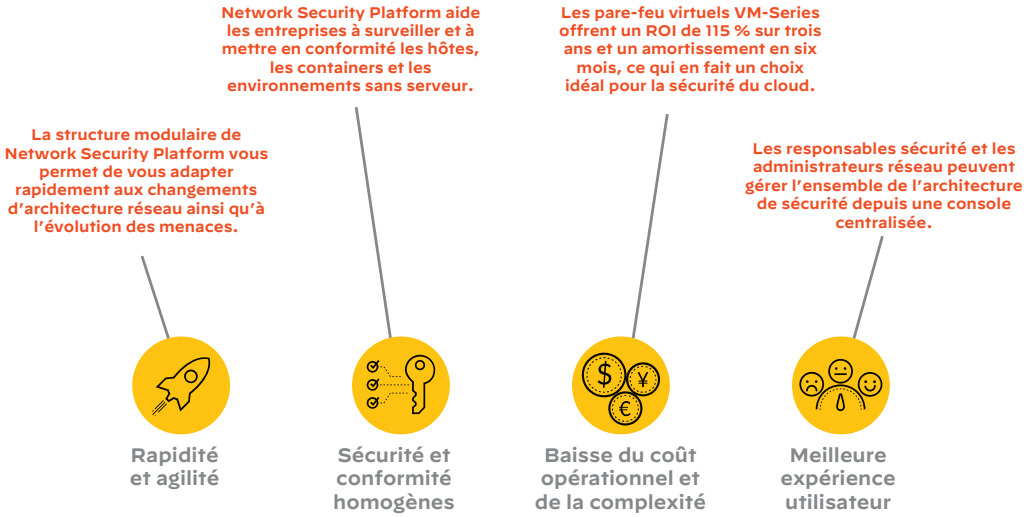
Les pare-feu virtuels de Palo Alto Networks s'intègrent de façon transparente à l'orchestrateur SDN ou au contrôleur de cloud privé pour automatiser le processus de déploiement, de gestion et de mise à jour de votre parc de pare-feu virtuels Palo Alto Networks (VM-Series et CN-Series). Vous passez ainsi moins de temps à gérer les pare-feu, tout en garantissant l'application de politiques homogènes et actualisées sur le réseau.



À suivre : Network Security Platform offre des résultats tangibles.

Des avantages concrets

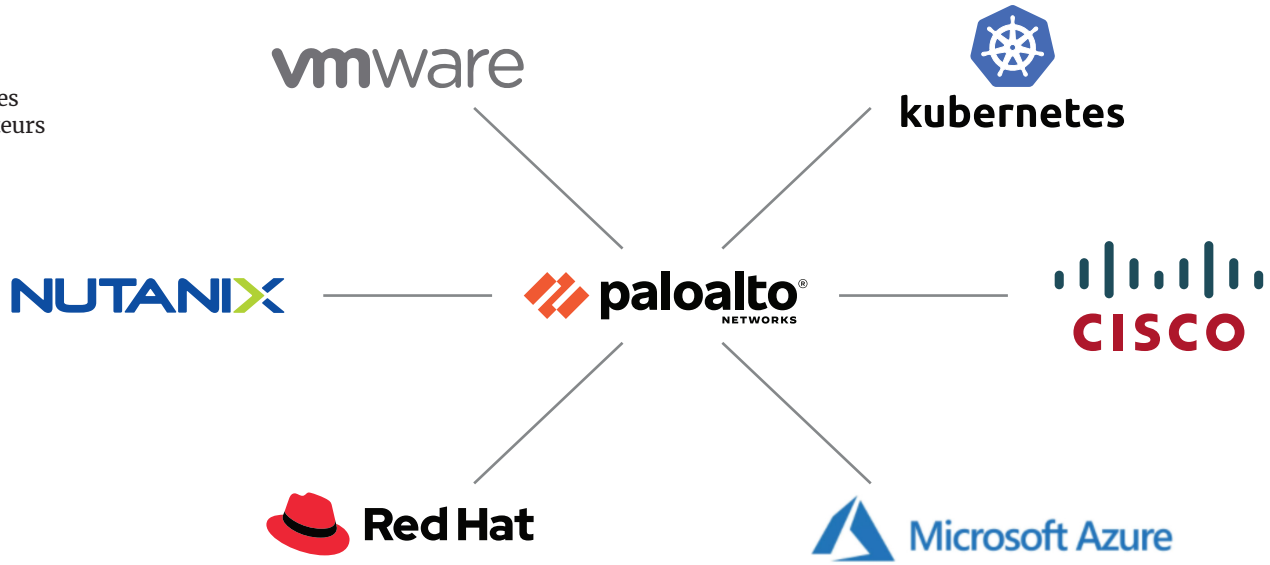
Ce document présente Network Security Platform sous l'angle du cloud *privé*, mais notre solution se prête tout autant à la sécurité des environnements publics et hybrides. Quel que soit votre cas d'usage, vous bénéficiez d'une vitesse et d'une agilité accrues, d'une sécurité et d'une conformité homogènes, d'une réduction des coûts opérationnels et de la complexité, ainsi que d'une meilleure expérience utilisateur.



À suivre : nos pare-feu virtuels prennent en charge un large éventail de systèmes de virtualisation.

Intégration aux principaux systèmes de virtualisation

Pour les systèmes de virtualisation de vos environnements cloud privés, vous n'avez que l'embarras du choix. Cela tombe bien car Network Security Platform prend en charge les solutions de virtualisation des principaux acteurs du marché.



Prêt à passer à la prochaine étape ? Découvrez toutes les options sur la page suivante.

Cap sur la sécurité des clouds privés

Les menaces qui pèsent sur les clouds privés augmentent à la fois en virulence, en volume et en niveau de sophistication. L'approche traditionnelle du périmètre de sécurité, qui consiste à diviser l'environnement en zones de confiance (trusted) et de « non confiance » (untrusted), est inadaptée aux architectures cloud hybrides et aux stratégies de développement cloud-native. Une sécurité cloud efficace passe par des périmètres plus petits et l'implémentation du Zero Trust.

Pour répondre aux enjeux des architectures distribuées, à des menaces de plus en plus virulentes et au rétrécissement des fenêtres de détection et de neutralisation, Palo Alto Networks a créé le NGFW virtuel VM-Series et le NGFW containerisé CN-Series : deux innovations qui garantissent la sécurité des clouds privés, publics et hybrides. Associés aux pare-feu physiques PA-Series, ces produits forment le socle de Network Security Platform, notre solution de sécurité cloud innovante et flexible, à découvrir en cliquant sur les vignettes ci-dessous. Comme nous l'avons souligné dans ce document, l'émergence des environnements cloud privés apporte avec elle des problématiques de sécurité spécifiques, auxquelles votre entreprise doit répondre pour devenir plus compétitive et innovante. Faites confiance à Palo Alto Networks pour vous offrir tous les avantages d'un partenaire de sécurité privilégié.

Jugez par vous-même

Demandez une démo personnalisée

Utilisez VM-Series gratuitement pendant 30 jours

Essayez CN-Series sur QwikLabs

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas

+31 20 888 1883

www.paloaltonetworks.fr