Étendre la sécurité Zero Trust au cloud public

Pare-feu virtuels : une pièce maîtresse de la défense multiniveau

paloalto NETWORKS | STRATA BY PALO ALTO NETWORKS

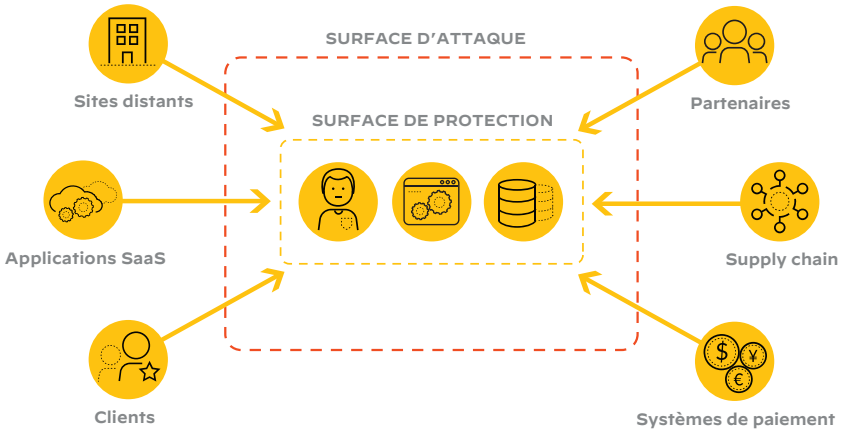
Sommaire

Ne jamais faire confiance, toujours vérifier

La maxime « faire confiance, mais vérifier » a été popularisée par le président américain Ronald Reagan en décembre 1987 à l'occasion de la signature du traité sur les forces nucléaires à portée intermédiaire avec Mikhaïl Gorbatchev. À première vue, l'expression semble contradictoire : si vous accordez votre confiance, pourquoi vérifier ?

Il s'avère que le principe sous-jacent au traité était en fait : « ne jamais faire confiance, toujours vérifier ». C'est sur ce précepte que repose la sécurité Zero Trust. Dans une architecture Zero Trust, l'emplacement du réseau ne fait pas partie des critères essentiels pour la confiance. Par contre, chaque appareil, utilisateur, application et flux de réseau est une menace en puissance qui doit donc être authentifiée et soumise à autorisation[1].

Le Zero Trust marque un tournant majeur dans la stratégie de sécurité. 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, services et l'infrastructure à protéger. Largement plus petit que la surface d'attaque, cet espace est aussi plus facilement identifiable.



Le Zero Trust réduit le nombre de points d'entrée potentiels des cyberattaques

Parlons maintenant du cloud, et spécifiquement des trois déclinaisons du cloud public.

Les déclinaisons du cloud public

On parle souvent du cloud public comme d'un modèle monobloc. En réalité, ce terme recouvre trois modèles : le logiciel en tant que Service (SaaS), la plateforme en tant que service (PaaS) et l'infrastructure en tant que service (IaaS).

Software as a Service (SaaS)

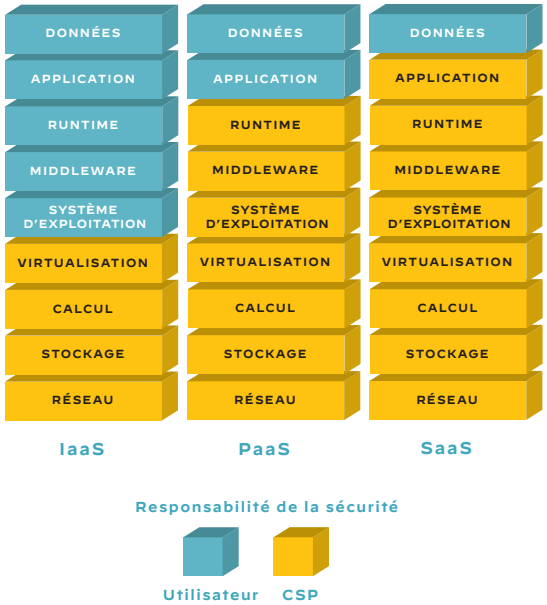
Très répandu dans les entreprises, le SaaS s'illustre dans des applications telles que Salesforce CRM, Adobe Creative Cloud, Google Docs et Microsoft Windows 365. Dans ce modèle de cloud public, le client détient les données, et le fournisseur de services cloud (CSP) gère tout le reste, du réseau jusqu'à l'application.

Platform as a Service (PaaS)

Le modèle PaaS est utilisé essentiellement par les développeurs. Ici, contrairement au SaaS, le client détient les données et l'application. Quelques exemples de services PaaS : AWS Elastic Beanstalk, Windows Azure, Googl App Engine, Red Hat OpenShift.

Infrastructure as a service (IaaS)

L'IaaS est, de loin, le modèle de cloud public le plus courant. Il est proposé par les principaux fournisseurs : AWS, Microsoft Azure, Google Cloud, Alibaba... En mode IaaS, le fournisseur met à disposition les ressources réseau, de stockage et d'infrastructure informatique, tandis que vous êtes chargé d'exécuter et de tenir à jour l'OS, le middleware, le runtime, les applications et les données.



Modèles de sécurité pour les trois déclinaisons du cloud public

Partagée entre deux responsables (le fournisseur cloud et vous), la sécurité du cloud public n'est pas une mince affaire (voir ci-après).

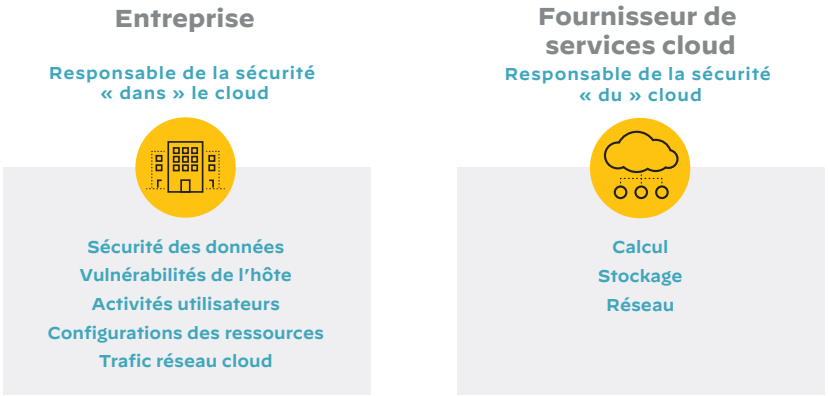
Le modèle de responsabilité partagée

Dans le modèle de cloud sur site ou privé, la totalité de l'environnement vous appartient, du matériel jusqu'aux données, en passant par les applications et tout le reste. Dès lors, aucun doute n'est possible quant à sa sécurité : vous en êtes le seul et unique responsable, à tout moment.

Par contre, tout n'est pas aussi limpide dans le cloud public qui suit un modèle de responsabilité partagée. Le fournisseur de services cloud assure la sécurité de la base de la plateforme. Réseau, stockage, calcul, services de virtualisation… tous les aspects matériels et logiciels sont concernés, jusqu'aux systèmes d'exploitation standard tels que Red Hat Enterprise Linux (RHEL) et Windows Server.

À vous d'assurer la sécurité du middleware, des runtimes, des applications et des données, sans oublier tout système d'exploitation non pris en charge. En somme, le fournisseur est responsable de la sécurité « **du cloud** » ; tandis que la sécurité « **dans le cloud** » incombe au client.

Pour que le partage de responsabilité fonctionne, les deux parties doivent collaborer et ne laisser aucun trou dans le filet, notamment sur les aspects en limite de responsabilité.



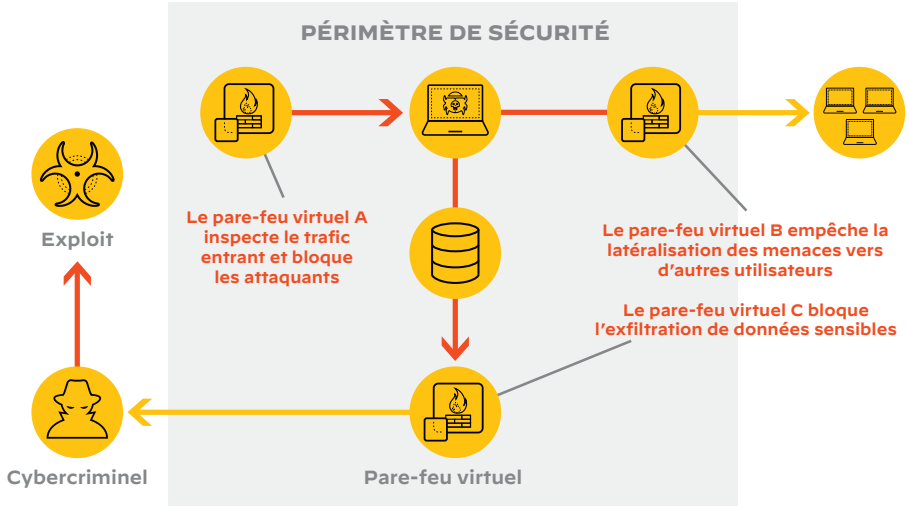
Partage des responsabilités en matière de sécurité dans le cloud public

Attention ! Ni outil ni architecture, le Zero Trust est une série de principes.
À suivre, le rôle majeur des pare-feu virtuels dans l'implémentation d'une architecture Zero Trust.

Pare-feu virtuels : une pièce maîtresse du cloud public

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. Il n'y a pas si longtemps, les NGFW n'étaient déployés que sous forme d'équipements matériels. Cette approche adaptée aux data centers d'application client/serveur physiques traditionnels n'est pas en phase avec le déploiement de matériel dans les environnements multicloud dynamiques actuels où chaque CSP maîtrise sa propre infrastructure.

Les pare-feu virtuels, ou NGFW logiciels, répondent aux besoins de sécurité du cloud public. Ils possèdent les mêmes fonctionnalités que leurs pendants physiques, avec en prime la capacité à suivre automatiquement les applications et les workloads au sein de l'environnement virtualisé.



Les pare-feu virtuels assurent une protection en profondeur contre les cybermenaces

Le besoin de conformité réglementaire est tout aussi important pour le cloud public que pour les déploiements sur site. Mais l'un et l'autre n'empruntent pas la même voie, comme nous allons le voir.

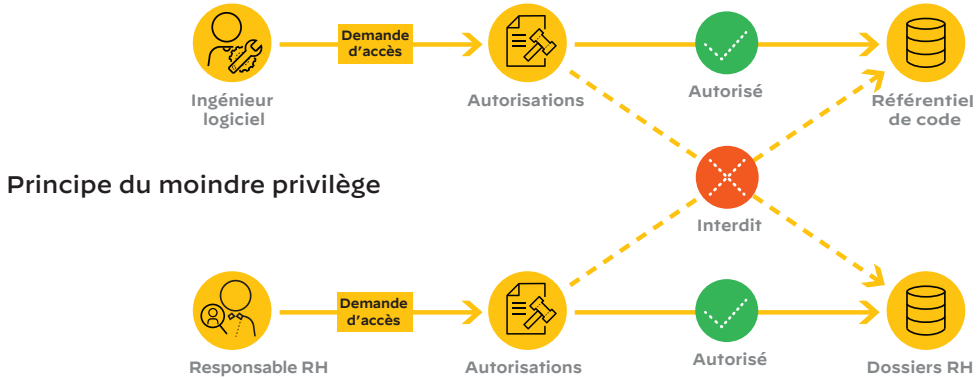
Les infrastructures cloud mettent les cadres de conformité existants à rude épreuve

Dans les secteurs hautement régulés, le non-respect des normes et régimes réglementaires (par exemple, HIPAA pour la santé, PCI DSS2 dans le retail, ou encore ACH3 pour les services bancaires) expose les organisations à des risques considérables. Or, le transfert d'applications et de données vers le cloud public peut avoir un effet significatif sur la posture de conformité.

La bonne nouvelle c'est que les CSP sont prêts à s'investir dans le programme de conformité de votre entreprise. Pour commencer, vous pouvez « hériter » des contrôles de sécurité appliqués par le CSP sur son infrastructure pour renforcer vos propres programmes de conformité et de certification. La majorité des fournisseurs vous autoriseront à utiliser leurs services de surveillance d'activité pour détecter les changements de configuration et les événements de sécurité sur votre système, voire à les intégrer à vos solutions pour faciliter le reporting de conformité.

Indéniablement, la création d'une stratégie de conformité efficace dans le cloud passe par une modification du système de sécurité. Les responsables sécurité doivent appliquer une gestion centralisée pour harmoniser les politiques à l'échelle de l'environnement cloud, et même des déploiements cloud multiples plus complexes. Pour répondre aux exigences réglementaires, les équipes de sécurité doivent pouvoir harmoniser la gestion et la sécurité à l'échelle du cloud public, ce que les CSP ne sont pas en mesure de faire.

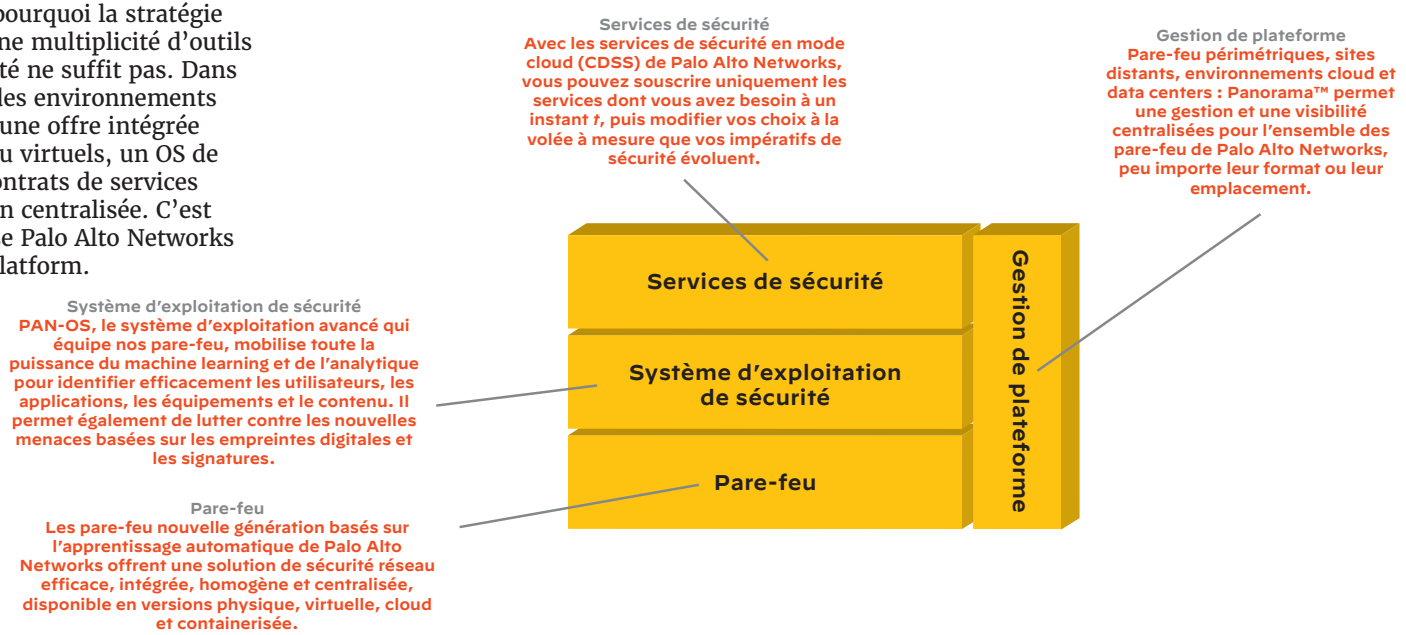
Enfin, le contrôle des accès doit être resserré à l'aide de politiques basées sur le principe du moindre privilège et de l'authentification multifacteur. Le but est d'attribuer aux utilisateurs les seules autorisations dont ils ont besoin pour accomplir les missions entrant dans le cadre de leurs fonctions. Par exemple, un ingénieur logiciel requiert l'accès au référentiel de code, mais pas aux dossiers RH. Et l'inverse est vrai pour les responsables RH.



Face à de tels défis, vous vous demandez sans doute comment mettre en œuvre la sécurité du cloud public. Réponse dans la section suivante…

Architecture de la plateforme de sécurité réseau

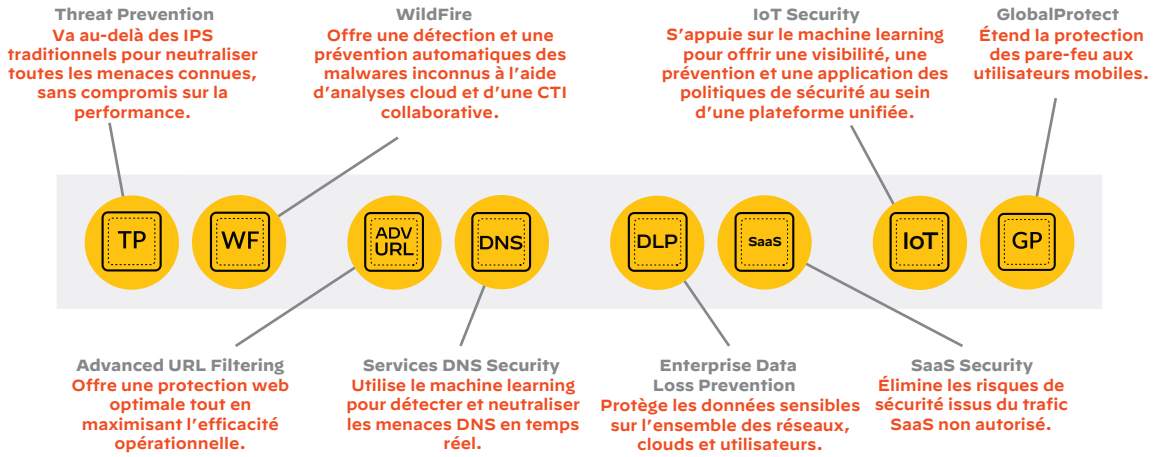
Une fois engagé dans le Zero Trust, vous comprendrez aisément pourquoi la stratégie consistant à combiner une multiplicité d'outils et d'approches de sécurité ne suffit pas. Dans ce contexte, la sécurité des environnements de cloud public requiert une offre intégrée comprenant des pare-feu virtuels, un OS de pare-feu courant, des contrats de services de sécurité et une gestion centralisée. C'est justement ce que propose Palo Alto Networks avec Network Security Platform.



Dans les environnements de cloud dynamiques, les contraintes de sécurité changent souvent. La plateforme de sécurité réseau relève ce défi en intégrant des services supplémentaires, détaillés ci-après.

Services de sécurité cloud pour la plateforme de sécurité réseau

La plateforme de sécurité réseau propose un ensemble de services de sécurité cloud complémentaires pour sécuriser en toute confiance le trafic qui transite sur vos réseaux et vos clouds. Contrairement aux solutions concurrentes qui proposent des services groupés — et vous obligent à acheter des services dont vous n'avez pas l'utilité —, cette plateforme offre une flexibilité totale. Sélectionnez uniquement les services qui vous intéressent dans l'immédiat, puis ajoutez-en et supprimez-en au gré de vos besoins en sécurité.

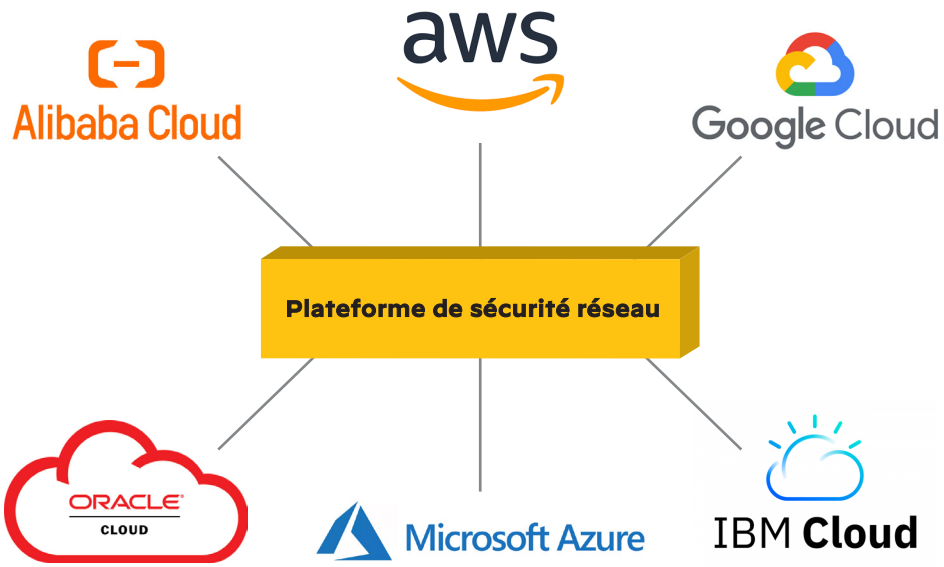


L'engouement pour les environnements multicloud impose de pouvoir combiner des offres de différents CSP, sans enfermement propriétaire. Lire la suite.

Fournisseurs de services cloud pris en charge par la plateforme de sécurité réseau

La Marketplace du cloud public est extrêmement compétitive, voire impitoyable selon le point de vue. Les entreprises les plus au fait peuvent jouer sur cette dynamique, négocier des contrats plus favorables et choisir leur CSP pour accéder plus rapidement aux technologies émergentes.

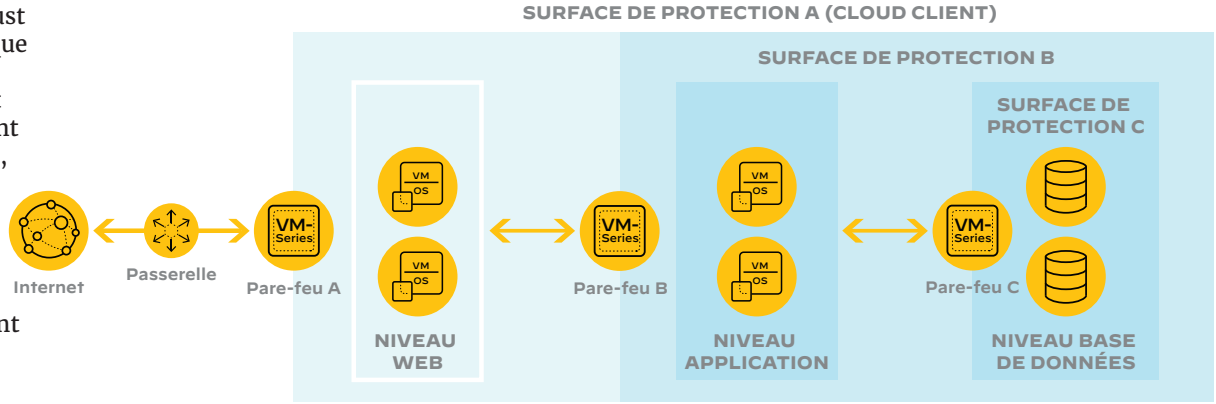
La plateforme de sécurité réseau s'intègre aisément aux principaux fournisseurs de cloud public. Vous pouvez donc choisir le fournisseur – ou plusieurs en cas d'environnement multicloud — le mieux adapté à vos besoins, sachant que Palo Alto Networks vous accompagne pour assumer votre part du modèle de responsabilité partagée, quel que soit l'environnement cloud, multicloud ou hybride.



Il est temps maintenant de rassembler toutes les pièces du puzzle et de découvrir le fonctionnement du Zero Trust sur le terrain.

Sécurité Zero Trust pour la défense en profondeur

Encore une fois, la mise en œuvre du Zero Trust implique le changement d'une surface d'attaque à une surface de protection. Dans l'exemple illustré ci-contre, trois pare-feu VM-Series et des services de sécurité cloud (CDSS) sécurisent une architecture applicative multiniveau (web, application, base de données). Chaque pare-feu crée une surface de protection bien délimitée. Le pare-feu de passerelle inspecte et sécurise le trafic entrant et sortant, tandis que le pare-feu applicatif contrôle l'accès au sous-réseau privé contenant les couches application et base de données. Touche finale de la sécurité en profondeur, la microsegmentation, implémentée par un pare-feu, renforce le niveau de protection entre la base de données et le reste de l'infrastructure.



Protection multiniveau d'applications de cloud public assurée par des pare-feu virtuels VM-Series

Après ce survol de la technologie, entrons dans le vif du sujet et voyons comment la plateforme de sécurité réseau produit de la valeur ajoutée et un ROI remarquable.

Valeur ajoutée : ROI et productivité des équipes

Outre les raisons de sécurité, les entreprises mettent en œuvre le Zero Trust pour ses impacts métiers. La plateforme de sécurité réseau présente quatre avantages majeurs : optimisation du retour sur investissement en sécurité, atténuation des conséquences de la pénurie de talents, accélération de la réponse aux menaces et amélioration de l'expérience utilisateur. Examinons-les dans l'ordre.

ROI rapide

Jusqu'à présent, la protection des investissements en sécurité passait souvent avant les questions financières pour les professionnels de la sécurité. Depuis, les entreprises ont relevé leurs exigences et incitent les RSSI à protéger les données et le parc logiciel de valeur, en optimisant des budgets de sécurité serrés. Selon une étude récente de Forrester Consulting, les pare-feu virtuels VM-Series offrent un ROI de 115 % sur trois ans et un amortissement en six mois[2]. La même étude indique en outre que l'on atteint une posture de sécurité adaptée 30 % plus vite.

115 %

ROI
Période d'amortissement de six mois

30 %

Réduction
Posture de sécurité adaptée atteinte plus vite

Avec le passage au cloud, les dépenses d'exploitation (OpEx) passent devant les dépenses d'investissement (CapEx). Matériel et logiciels ne sont plus achetés, mais loués au CSP. C'est à ce dernier qu'incombent désormais l'acquisition, l'installation, l'exploitation et la maintenance de l'infrastructure, ce qui vous permet d'affecter autrement vos collaborateurs et l'investissement.

Pénurie de compétences en cybersécurité

À l'heure où les professionnels IT, notamment les experts en sécurité, font cruellement défaut dans tous les secteurs, la gestion de la sécurité réseau, par nature laborieuse et chronophage, s'avère un véritable casse-tête. Selon une étude récente, plus de 2,7 millions de postes restent à pourvoir, et il faudrait une augmentation annuelle de 65 % du nombre de collaborateurs pour répondre à la demande[3].

Dans ces circonstances, il n'est pas étonnant que les entreprises, impuissantes à résoudre l'équation, cherchent d'autres moyens de pallier cette pénurie de talents. Et la technologie se hisse en tête : 38 % des entreprises confient la charge de leur infrastructure de data center à des fournisseurs de service cloud pour diminuer le temps d'exploitation, de maintenance et d'actualisation de l'infrastructure informatique en interne[4].

Après le ROI et la productivité des équipes, penchons-nous sur d'autres avantages de la plateforme de sécurité réseau : l'amélioration de la réponse aux menaces et de l'expérience utilisateur.

Valeur ajoutée : réponse aux menaces et expérience utilisateur

Réponse aux menaces : visez l'efficacité

L'évolution perpétuelle des menaces constitue l'un des plus grands défis de la sécurité du cloud public. Les attaquants ne reculent devant rien : non contents d'inventer des attaques toujours plus sophistiquées, ils n'hésitent pas à en modifier d'autres pour contourner les mesures de sécurité connues. Pour les équipes de sécurité, une vigilance de tous les instants est de mise.

Pour assurer des services de sécurité, la plateforme de sécurité réseau suit une approche modulaire en mode cloud, qui permet aux professionnels de la sécurité de répondre sans délai et de façon efficace aux changements dans l'environnement des menaces et dans l'architecture de l'entreprise. Imaginons que vous ayez reçu un signalement d'exfiltration de données confidentielles sur clé USB. Si la menace est sérieuse, votre équipe peut déployer la Prévention des pertes de données (DLP) en quelques minutes seulement pour consolider votre système de défense.

Expérience utilisateur améliorée

Les entreprises sont très exigeantes avec leurs DSI et RSSI, tout comme elles le sont en matière de performances de leurs infrastructures réseau pour permettre à l'ensemble des intervenants (équipes, fournisseurs, sous-traitants, etc.) de travailler. Ralentissements, pannes de réseau, exfiltration de données par exploits, attaques par ransomware… tout ce qui interfère avec l'accès aux applications et données essentielles à l'activité peut miner la productivité, le moral et l'innovation.

Sans oublier l'expérience de la communauté d'utilisateurs hors de l'entreprise. Les clients qui consultent votre site web s'attendent à trouver rapidement l'information et les services précis dont ils ont besoin. Une panne ou un ralentissement du site risque de les faire fuir. Pire encore, si, faute de sécurité adéquate, les visiteurs de votre site sont infectés par un logiciel malveillant ou dépossédés de leurs données personnelles, vous risquez d'être soumis à d'importantes sanctions financières et réglementaires. Quant à votre image de marque, elle sera irrémédiablement entachée.

Le Zero Trust est un formidable antidote à ces problèmes potentiels. La plateforme de sécurité réseau intégrée unifie le traitement de la sécurité : tous les éléments de l'infrastructure de sécurité fonctionnent en coordination pour optimiser la protection et limiter les interruptions. La plupart du temps, les utilisateurs n'ont pas connaissance de son existence, ce qui est le meilleur cas de figure possible.

Félicitations ! Vous venez d'achever cet eBook sur les fondamentaux du Zero Trust dans les clouds publics. Et maintenant, il est temps de passer à l'action. Lisez la suite pour savoir par où commencer.

Sécurité Zero Trust : à vous de jouer

Force est de constater que le transfert de vos informations et applications dans le cloud public crée de nouveaux défis de sécurité. Heureusement, nos solutions sont à votre disposition. Les pare-feu virtuels VM-Series de Palo Alto Networks sont les composants centraux d'une architecture Zero Trust multiniveau qui assure la défense contre les menaces de type « zero-day » et autres, améliore l'expérience utilisateur, génère un ROI appréciable et réduit considérablement les interruptions de service (jusqu'à 67 %)[5].

La migration des applications dans le cloud public n'est pas sans dangers. Or, une architecture Zero Trust modère ces risques et sécurise vos besoins métiers essentiels. Nous vous renvoyons à la lecture de la récente étude Total Economic Impact (TEI) de Forrester Consulting pour plus d'informations sur les différents avantages économiques de nos pare-feu virtuels (ROI et autres). Vous pouvez également calculer les économies potentielles avec l'outil de calcul de ROI des pare-feu virtuels, basé sur l'étude de Forrester Consulting.

Dans tous les cas, n'hésitez pas à nous contacter. Nos experts en sécurité se feront un plaisir de vous proposer une démo personnalisée et de répondre à vos questions sur la sécurité du cloud public. Programmez une démo.

1 « Chapter 1: Zero Trust Fundamentals », dans *Zero Trust Networks*.

2 Étude Total Economic Impact™ pour les pare-feu virtuels VM-Series de Palo Alto Networks, Forrester Consulting pour Palo Alto Networks, 26 octobre 2021

3 « A Resilient Cybersecurity Profession Charts the Path Forward », (ISC)2 Cybersecurity Workforce Study, 2021.

4 Ibid.

5 Étude Total Economic Impact™ pour les pare-feu virtuels VM-Series de Palo Alto Networks, Forrester Consulting pour Palo Alto Networks, 26 octobre 2021

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr