paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

Les 10 piliers d'une solution SASE efficace

Sommaire

Introduction

La pandémie de COVID-19 a changé à jamais le modèle opérationnel des entreprises. Du jour au lendemain, elles ont dû tant bien que mal transformer leurs réseaux dans l'urgence pour offrir à leurs télétravailleurs une connectivité ininterrompue et un accès distant sécurisé aux services, applications et données indispensables au bon fonctionnement de leur activité.

Avant même la crise sanitaire, les entreprises étaient déjà aux prises avec des technologies d'ancienne génération qui limitaient fortement leur capacité à gérer des types de trafic et des menaces de sécurité en évolution permanente. Pour y faire face, elles n'avaient d'autre choix que de déployer une multitude de produits spécialisés : pare-feu, passerelles web sécurisées (SWG), solutions CASB (Cloud Access Security Broker) et réseaux SD-WAN (Software-Defined Wide Area Network), entre autres. La pandémie n'a donc fait qu'exacerber des problèmes existants en obligeant les entreprises à s'engager au pied levé sur la voie du télétravail dans le monde entier, tout en préservant la confidentialité et la sécurité des données.

Le concept de Secure Access Service Edge (SASE) est apparu en 2018. Le SASE (prononcez « sassi »), comme l'a baptisé Gartner, consiste à fournir des services réseau et de sécurité à partir d'une architecture cloud commune pour aider les organisations à adopter les technologies cloud et mobiles en toute sérénité. En ce sens, une solution SASE doit offrir des services de sécurité et d'accès homogènes à tous les types d'applications cloud (public, privé et SaaS) sur un framework commun.

En abandonnant leur patchwork de produits isolés au profit d'une solution SASE dans le cloud, les entreprises réduisent la complexité et rendent leurs télétravailleurs et sites distants très rapidement opérationnels, tout en réalisant des économies substantielles sur leurs ressources techniques, humaines et financières.

Cet eBook vous invite à découvrir les 10 piliers d'un SASE réellement efficace.

Pilier nº 1 – Réseau SD-WAN (Software-Defined Wide Area Network)

PROBLÉMATIQUE

Les entreprises se sont appropriées le SD-WAN (Software-Defined Wide Area Network) pour connecter les sites distants au réseau de leur siège et fournir un « breakout » local vers Internet comme alternative aux coûteuses liaisons MPLS. Les solutions SD-WAN d'ancienne génération posent de nombreuses difficultés dans la mesure où elles obligent à intégrer au forceps le modèle de routage classique, basé sur les paquets, à une architecture cloud. De plus, le manque d'évolutivité de ces anciennes solutions oblige les entreprises à « greffer » après coup des services de sécurité et de visibilité pour les sites distants, augmentant au passage les coûts et la complexité.

APPROCHE SASE

Dans une solution SASE, l'architecture des sites distants est 100 % cloud. En d'autres termes, les fonctions réseau et de sécurité sont assurées intégralement depuis le cloud, ce qui simplifie la gestion WAN et rentabilise l'investissement des entreprises.

À RETENIR

Si vous cherchez à simplifier votre solution SD-WAN, envisagez une solution autonome et en mode cloud de type SASE. Votre solution SD-WAN doit être orientée applications plutôt que basée sur des paquets. Vous pourrez ainsi gagner en visibilité et définir des SLA sur chaque application, notamment SaaS, cloud et UCaaS (Unified Communications as a Service). Par ailleurs, le modèle SASE fait converger les fonctions réseau et sécurité. De fait, une solution SASE réellement efficace doit proposer un SD-WAN intégré et régi par des politiques cohérentes pour former une plateforme homogène. Bref, tout le contraire du patchwork de produits disparates de multiples fournisseurs.

« D'ici à 2024, plus de 60 % des clients SD-WAN auront déployé une architecture SASE (Secure Access Service Edge), contre 35 % environ en 2020. »

Gartner Magic Quadrant 2020 des infrastructures Edge WAN

Pilier nº 2 – Accès réseau Zero Trust (ZTNA)

PROBLÉMATIQUE

Les entreprises ne parviennent toujours pas à appliquer les politiques et mesures de sécurité nécessaires à la protection de leurs données et collaborateurs. Avec le ZTNA, les utilisateurs qui veulent se connecter à une application doivent s'authentifier au préalable via une passerelle. Les administrateurs de sécurité peuvent ainsi identifier les utilisateurs et créer des politiques de restriction des accès, réduire les pertes de données et neutraliser rapidement les menaces potentielles.

Seulement voilà, beaucoup de produits ZTNA s'appuient sur des architectures SDP (Software-Defined Perimeter). Or, celles-ci n'offrent aucune inspection des contenus, ce qui crée des disparités dans le type de protection disponible pour chaque application. Pour homogénéiser le niveau de sécurité, les organisations doivent donc effectuer d'autres contrôles, en complément du modèle ZTNA, et inspecter tout le trafic de toutes les applications.

APPROCHE SASE

Une architecture SASE reprend les principes fondamentaux du modèle ZTNA et les applique à tous ses autres services. L'identification des utilisateurs, des appareils et des applications, indépendamment de leur lieu de connexion, simplifie la création et la gestion des politiques. Toujours dans une perspective de simplification, le SASE incorpore les services réseau au sein d'un seul et même framework cloud unifié pour tirer un trait sur les connexions à une passerelle.

À RETENIR

Une solution SASE doit intégrer un modèle ZTNA de protection des applications et exécuter d'autres services de sécurité pour assurer une application cohérente des politiques de prévention des pertes de données et de prévention des menaces. En tant que tels, les contrôles d'accès sont en effet utiles pour confirmer l'identité d'une personne. Mais d'autres contrôles de sécurité sont aussi nécessaires pour s'assurer que le comportement et les actions de cette personne ne portent pas préjudice à l'organisation. Par ailleurs, les mêmes contrôles d'accès doivent s'appliquer à toutes les applications.

« Beaucoup d'entreprises n'appliquent aucune restriction sur les applications qu'utilisent leurs salariés. Seules 62 % d'entre elles ont interdit l'installation d'applications non approuvées dans leur politique d'utilisation acceptable (PUA). »

Rapport Verizon Mobile Security Index 2020

Pilier nº 3 – Cloud Access Security Broker (CASB)

PROBLÉMATIQUE

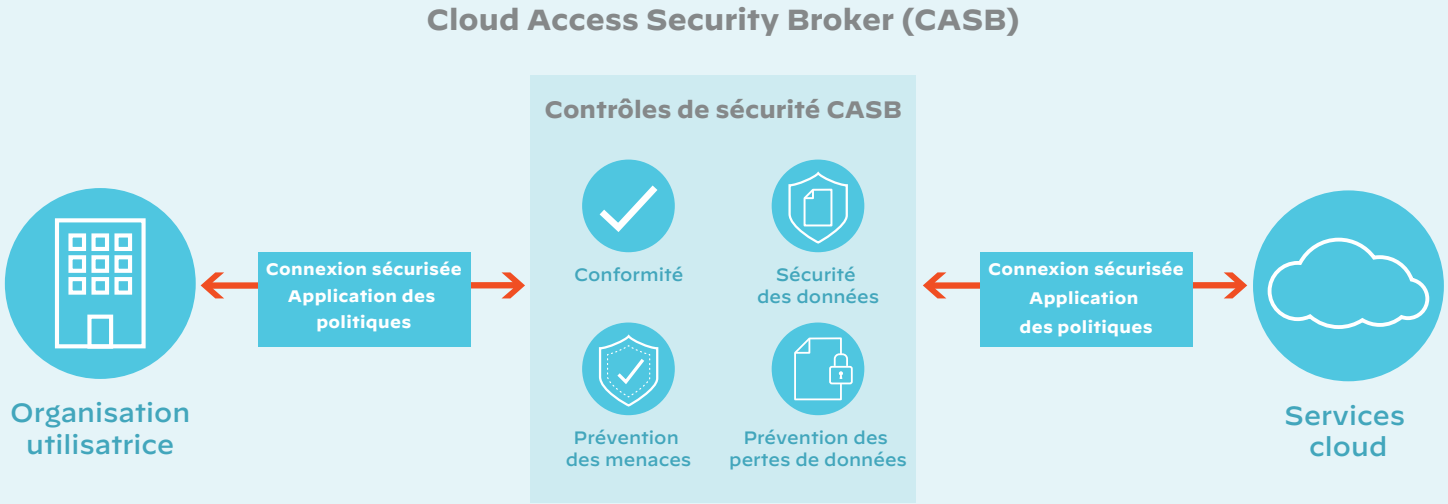
Beaucoup d'entreprises misent sur les CASB (Cloud Access Security Brokers) pour renforcer leur visibilité sur la localisation de leurs données sensibles (notamment dans le cas d'applications SaaS), appliquer des politiques d'accès utilisateurs et se protéger contre les hackers. Les CASB servent à appliquer les politiques de sécurité de votre organisation lors de l'accès de vos collaborateurs à leurs applications SaaS.

APPROCHE SASE

Élément indispensable de votre solution SASE, un CASB offre aux différents acteurs concernés une plateforme centralisée de gestion des contrôles de sécurité pour tous les types d'applications. Une solution SASE vous permet de savoir quelles applications SaaS sont utilisées et où vont les données, quel que soit le lieu de connexion des utilisateurs.

À RETENIR

Votre solution SASE doit intégrer des contrôles SaaS in-line et basés sur des API pour la gouvernance, les contrôles d'accès et la protection des données. Pour améliorer la visibilité, la gestion, la sécurité et la protection contre les menaces zero-day et émergentes, une solution SASE doit combiner des mesures de sécurité in-line et API en parallèle à des contrôles contextuels. Cette combinaison est également appelée CASB multimode.



Pilier nº 4 – Pare-feu sous forme de service (FWaaS)

PROBLÉMATIQUE

Des pare-feu physiques ou virtuels doivent être déployés partout où il existe des applications ou des utilisateurs : au siège, sur les sites distants, dans les data centers ou dans le cloud. Avec l'explosion du télétravail et la prolifération des applications dans toutes sortes d'environnements, les entreprises peinent à gérer les dizaines voire les centaines de pare-feu nécessaires. C'est là que le FWaaS (Firewall as a Service) entre en jeu pour leur offrir des fonctionnalités de pare-feu sous forme de service hébergé dans le cloud. Côté fonctionnalités, les meilleures offres FWaaS ne diffèrent en rien des pare-feu nouvelle génération sur site.

APPROCHE SASE

Dans une solution SASE, le FWaaS fait partie intégrante d'une plateforme unifiée. Elle offre ainsi les mêmes fonctionnalités qu'un pare-feu nouvelle génération, mais en mode cloud. En intégrant le modèle de service FWaaS à un framework SASE, les organisations peuvent facilement gérer leurs déploiements à partir d'une seule et même plateforme.

À RETENIR

Pour assurer une protection comparable à celle des pare-feu nouvelle génération, une solution SASE doit intégrer des fonctionnalités FWaaS qui permettent d'implémenter des politiques de sécurité réseau dans le cloud. Il est également important que votre solution ne fournisse pas uniquement des fonctions basiques de blocage des ports ou de protection par pare-feu. Il vous faut les mêmes fonctionnalités qu'un pare-feu nouvelle génération, avec en plus des fonctionnalités de sécurité dans le cloud comme les services de prévention des menaces et la sécurité DNS.

« D'ici à 2025, 30 % des nouveaux déploiements de pare-feu de sites distants distribués suivront le modèle FWaaS, alors qu'ils ne représentaient que 5 % en 2020. »

Gartner Magic Quadrant 2020 des pare-feu réseau

Pilier nº 5 – Passerelle web sécurisée (SWG)

PROBLÉMATIQUE

Les entreprises s'appuient sur les passerelles web sécurisées (Secure Web Gateway, SWG) pour empêcher leurs utilisateurs et leurs équipements d'accéder à des sites malveillants ou inappropriés. Une SWG avec sécurité DNS peut servir à bloquer du contenu inapproprié (sites pornographiques, sites de paris en ligne, etc.), mais également des sites web que l'entreprise veut rendre inaccessibles au bureau (par ex. les plateformes de streaming comme Netflix). Malheureusement, les SWG sont proposées sous forme de services ou d'équipements autonomes, ce qui entraîne des disparités dans l'application des politiques, selon que les utilisateurs sont sur site ou en télétravail.

APPROCHE SASE

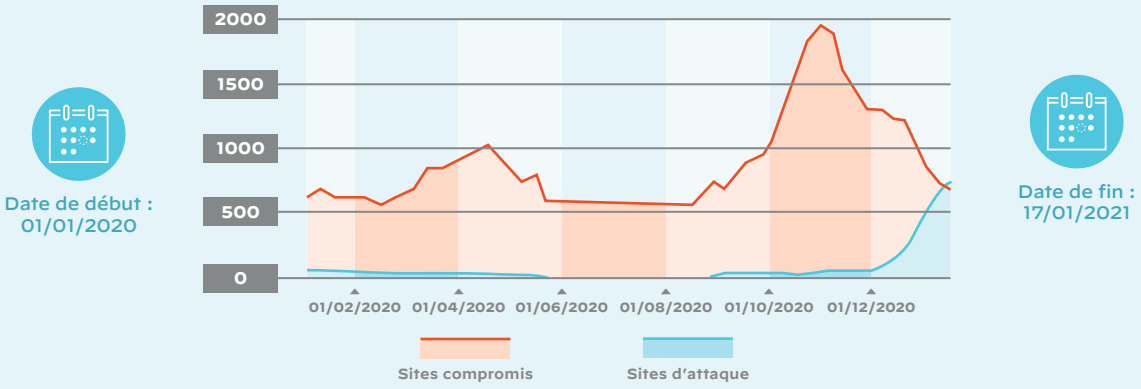
Les passerelles web sécurisées (SWG) ne sont qu'un des nombreux services de sécurité indispensables à une solution SASE. Un service SWG cloud fourni par une plateforme SASE offre une visibilité et un contrôle complets sur l'ensemble du réseau, indépendamment du lieu de connexion de l'utilisateur, pour garantir un usage sécurisé des applications cloud et autres services web. À mesure que les organisations se développent et que leur population d'utilisateurs à distance augmente, le service SWG cloud de la solution SASE monte en charge automatiquement au rythme des besoins.

À RETENIR

Une solution SASE intègre les mêmes services de sécurité qu'une passerelle web sécurisée traditionnelle. Elle permet ainsi aux organisations de contrôler l'accès au web et d'appliquer des politiques de sécurité qui protègent les utilisateurs contre les sites web dangereux ou les contenus inappropriés. Assortie de la sécurité DNS et d'un proxy explicite, une passerelle web sécurisée offre une entrée en matière simple et idéale pour la transition vers une architecture SASE.

Transparence des informations (Google) : Sites hébergeant des malwares, janvier 2020 à janvier 2021

https://transparencyreport.google.com/safe-browsing/overview?hl=fr



Pilier nº 6 – Suivi de l'expérience numérique

PROBLÉMATIQUE

La satisfaction et la productivité des collaborateurs passent par une bonne expérience utilisateur, ce quel que soit le lieu de travail. Au niveau du réseau et des terminaux, les équipes informatiques sont confrontées à des problèmes de visibilité qui les obligent à passer énormément de temps à résoudre manuellement le moindre problème.

APPROCHE SASE

La fonction de suivi autonome de l'expérience numérique (ADEM) offre toute la visibilité et les détails indispensables pour créer une expérience utilisateur fluide. Intégrée à la plateforme SASE, l'ADEM fournit des analyses par segment sur tout le parcours de livraison des services, avec en prime une analyse du trafic réel et synthétique qui permet aux entreprises d'automatiser la résolution des problèmes d'expérience numérique dès qu'ils surviennent.

À RETENIR

L'optimisation de l'expérience utilisateur devient un enjeu crucial depuis qu'une grande partie des collaborateurs est passée en télétravail. Pour que votre solution SASE soit tout aussi bénéfique aux utilisateurs qu'aux équipes informatiques, elle doit intégrer l'ADEM pour profiter d'une visibilité complète, d'une résolution automatique et d'informations approfondies sur la performance des terminaux, du Wi-Fi, des chemins réseau et des applications.

« Les responsables IT devront rendre compte des indicateurs d'expérience utilisateur pour 70 % des initiatives technologiques lancées par leur entreprise en 2025, contre 15 % en 2019 d'après Gartner. »

Guide Gartner 2020 du suivi des expériences numériques

Pilier nº 7 – Prévention des menaces

PROBLÉMATIQUE

Dans un monde où sévissent des compromissions de toute envergure et où des attaques par ransomware se produisent au quotidien, la prévention des menaces est devenue en enjeu essentiel pour protéger les données et les salariés de votre entreprise. Anti-malware, prévention des intrusions, blocage de fichiers… il existe toute une variété d'outils qui permettent de prévenir et bloquer les menaces. Toutefois, ces produits fonctionnent indépendamment les uns des autres, ce qui non seulement complique leur gestion et leur intégration, mais aussi ralentit l'identification et le traitement des menaces.

APPROCHE SASE

Avec une solution SASE, tous ces produits et services sont intégrés au sein d'une seule et même plateforme cloud. Vous simplifiez ainsi la gestion et la surveillance de toutes les menaces et vulnérabilités qui pèsent sur votre réseau et vos environnements cloud. Une solution SASE doit aussi inclure des fonctionnalités de machine learning permettant de neutraliser les menaces inconnues en quasi-temps réel et d'étendre la visibilité et la sécurité à tous les appareils, y compris les objets IoT non répertoriés.

À RETENIR

Pour protéger vos collaborateurs et données contre les exploits et malwares, vous devez pouvoir vous appuyer sur un référentiel de Threat Intelligence à jour. De même, votre solution SASE doit intégrer des outils de prévention des menaces pour vous permettre de répondre et remédier rapidement aux menaces, ainsi que des fonctions de machine learning in-line pour contrer instantanément les menaces inconnues à base de fichiers et issues du web. En parallèle, des recommandations automatiques de politiques peuvent faire gagner du temps et réduire le risque d'erreur humaine.

Pourquoi est-il plus difficile de détecter et répondre aux menaces aujourd'hui ?

Résultats de l'enquête ESG Master sur la détection et la réponse aux menaces

Pilier nº 8 – Internet des objets

PROBLÉMATIQUE

Souvent non gérés par l'entreprise, les objets connectés (IoT) n'en sont pas moins rattachés à son réseau. Or, ces appareils contiennent souvent des vulnérabilités et n'apportent aux équipes informatiques qu'une visibilité limitée sur les ressources auxquelles ils accèdent, sans compter que leurs mises à jour doivent s'effectuer manuellement. Il en résulte des failles dans lesquelles les cybercriminels peuvent facilement s'engouffrer. Certes, il existe des capteurs et équipements de sécurité IoT. Mais outre leur coût, ils n'apportent qu'une solution partielle au problème et créent des lourdeurs et des difficultés opérationnelles.

APPROCHE SASE

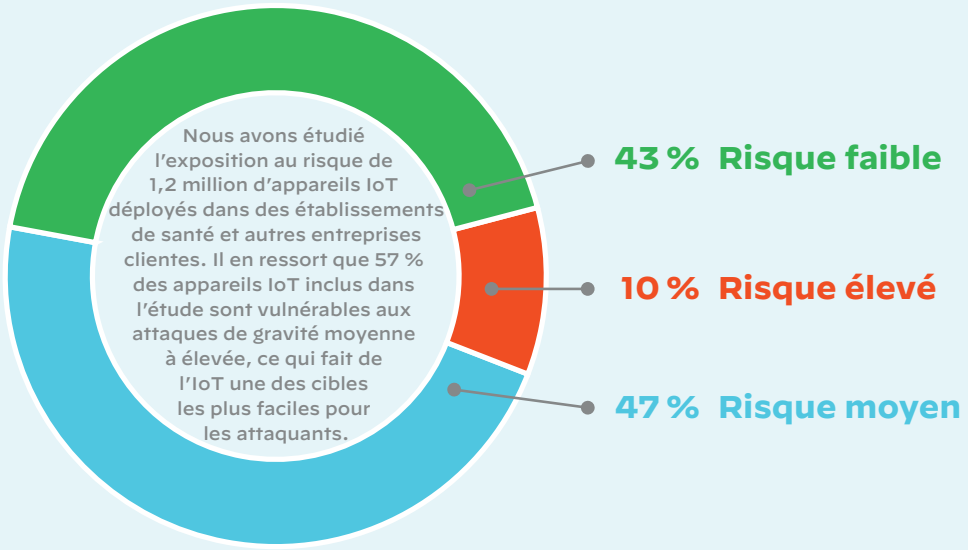
Avec une solution SASE, la sécurité IoT doit être intégrée à la plateforme pour protéger les sites distants et les télétravailleurs en mode cloud. Le cloud permet en effet de détecter avec précision les appareils IoT pour obtenir une visibilité complète et appliquer des politiques de sécurité sur l'ensemble du réseau, le tout sans ajout d'autres solutions de sécurité IoT.

À RETENIR

Les entreprises s'approprient les objets connectés au moment même où des technologies séculaires se transforment en objets du futur, à l'image des thermostats intelligents ou des systèmes d'éclairage connecté. Ce ne sont donc plus seulement les smartphones, les montres connectées et autres tablettes qu'il faut protéger sur le réseau d'entreprise, mais tout un éventail d'objets divers et variés. Une solution SASE doit intégrer des fonctions de machine learning et d'IA, gage d'autonomie pour identifier et contrer rapidement les menaces.

« 57 % des objets connectés sont vulnérables aux attaques de gravité moyenne à élevée, faisant de l'IoT une des cibles les plus faciles pour les attaquants. »

Rapport 2020 d'Unit 42 sur les menaces IoT, Palo Alto Networks



Pilier nº 9 – Prévention des pertes de données (DLP)

PROBLÉMATIQUE

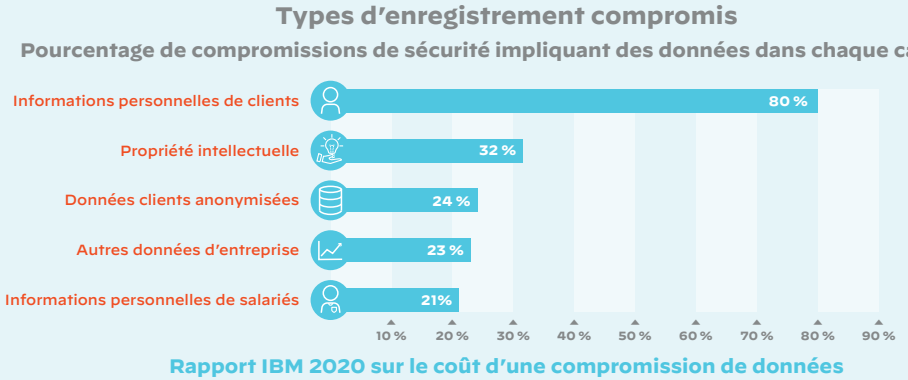
Les outils de prévention contre la perte de données (Data Loss Prevention, DLP) protègent les données sensibles et veillent à ce qu'elles ne subissent ni perte, ni vol, ni utilisation abusive. Ces solutions composites surveillent les données dans les environnements où elles sont déployées (réseaux, terminaux, clouds, etc.) et au niveau de leurs points de sortie. Elles alertent également les principaux acteurs concernés en cas de violation d'une politique. Compte tenu des différentes exigences de conformité en place (HIPAA, PCI DSS, RGPD, etc.), les outils DLP sont absolument essentiels à la sécurité des données et au respect des réglementations. Les outils DLP d'ancienne génération reposent sur des technologies initialement conçues pour les environnements sur site. Ils ont par la suite été étendus, puis adaptés aux applications cloud. Toutefois, la multitude des fonctionnalités et l'hétérogénéité des politiques et des configurations de ces outils les rendent extrêmement coûteux, complexes et difficiles à déployer à grande échelle. La transformation numérique et les nouveaux modèles d'usage des données exigent une nouvelle approche de la protection des données.

APPROCHE SASE

Avec une solution SASE, les outils DLP convergent en une seule solution cloud axée sur les données, quel que soit l'endroit où elles résident. Les mêmes politiques sont appliquées uniformément à toutes les catégories de données (sensibles, stockées, en transit, en cours d'utilisation, etc.), peu importe leur emplacement. Dans une architecture SASE, les outils DLP ne forment plus une solution autonome : ils sont intégrés aux points de contrôle existants de l'organisation. Plus besoin de déployer et gérer plusieurs outils. Grâce au SASE, les organisations ont enfin la possibilité d'exploiter une solution complète de protection des données qui 1) repose sur une architecture simple et évolutive, et 2) exploite les accès au trafic global pour renforcer l'efficacité des fonctions de machine learning.

À RETENIR

Les outils DLP sont essentiels pour protéger les données sensibles et respecter les réglementations en vigueur. Ils doivent donc appartenir au noyau dur d'une solution SASE. Le SASE fait de la prévention contre la perte des données un service cloud intégré permettant d'identifier, de surveiller et de protéger efficacement les données sensibles dans tous les points de l'environnement (réseaux, clouds, utilisateurs).



Pilier nº 10 – Extensibilité de la plateforme

PROBLÉMATIQUE

L'ajout et l'intégration de multiples services cloud de divers fournisseurs est une opération souvent complexe pour les entreprises. Comme il n'existe pas d'outil universel capable de répondre à toutes les problématiques, les différentes solutions doivent pouvoir communiquer entre elles pour éliminer les failles de sécurité. Malheureusement, il existe peu de solutions cloud capable de s'intégrer en toute transparence à des services tiers, sans compter que les fournisseurs se montrent souvent réticents à l'idée d'accompagner les entreprises dans ce parcours.

APPROCHE SASE

Une solution SASE doit être capable d'intégrer les services d'autres fournisseurs, facilement de surcroît pour simplifier le travail des administrateurs. Une plateforme d'intégration permet aux entreprises d'ajouter rapidement les services dont elles ont besoin, tout en bénéficiant d'une assistance totale de leur fournisseur SASE.

À RETENIR

Une solution SASE extensible permet aux entreprises d'ajouter facilement des services à la plateforme pour répondre à tous les cas d'usage possibles. Débarrassées du problème des solutions disparates et non intégrées, les entreprises peuvent continuer à utiliser leurs services tiers existants pour renforcer leurs capacités et répondre à leurs besoins.

« Les responsables de la gestion du risque et de la sécurité doivent réduire la complexité en choisissant un seul fournisseur pour les fonctions SWG, CASB, DNS, ZTNA et d'isolement de navigateur à distance. »

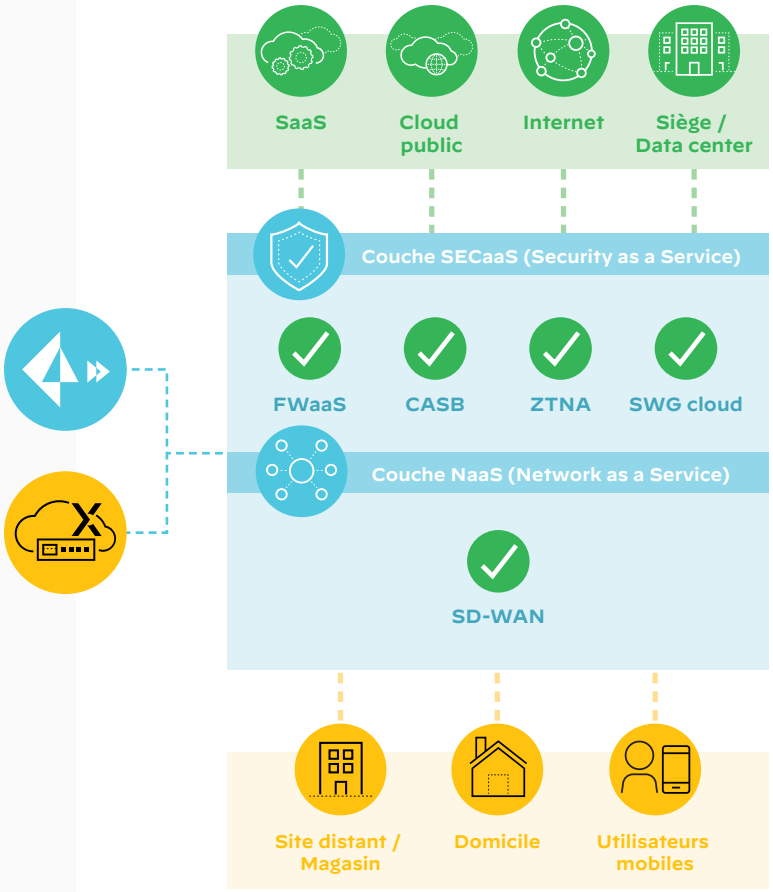
L'avenir de la sécurité des réseaux se joue dans le cloud, Gartner, 2019

Palo Alto Networks vous accompagne

Palo Alto Networks propose la solution la plus complète du marché au travers de ses produits Prisma® Access et CloudGenix® SD-WAN. Prisma Access fournit des fonctions de sécurité en mode cloud pour prévenir les cyberattaques. Pour ce faire, elle protège tout le trafic, de toutes les applications et sur tous les ports. CloudGenix SD-WAN de Palo Alto Networks est la première solution nouvelle génération exploitant le machine learning et l'automatisation pour simplifier les opérations réseau et de sécurité, tout en offrant une expérience utilisateur incomparable.

Grâce à l'intégration étroite de Prisma Access à CloudGenix SD-WAN, les entreprises peuvent étendre leur couverture de sécurité et de connectivité à leurs télétravailleurs et à leurs sites distants. Au lieu de cumuler des produits spécialisés qui créent un patchwork de technologies monofonctionnelles mal intégrées, Prisma Access s'appuie sur une infrastructure cloud commune qui fournit de multiples types de services de sécurité. Ensemble, Prisma Access et les services réseau de CloudGenix SD-WAN forment une solution complète. En prime, les clients peuvent bénéficier d'une Threat Intelligence complète alimentée par des données CTI provenant de Palo Alto Networks et de centaines de sources tierces.

Prisma Access et CloudGenix SD-WAN : la solution SASE la plus complète du marché



Conclusion

Alors que le télétravail et la transition vers le cloud se poursuivent dans les entreprises, nous vous encourageons à étudier la possibilité d'une solution SASE complète pour répondre à vos besoins de services réseau et de sécurité. Le SASE offre trois avantages essentiels à votre entreprise :

1

SIMPLIFICATION DE LA GESTION ET DES OPÉRATIONS

- Convergence des fonctions réseau et de sécurité au sein d'un même service cloud géré depuis une console centralisée.
- Automatisation des déploiements et de la gestion courante des sites distants.
- Recours au machine learning et à la science des données pour simplifier les opérations réseau et réduire fortement les tickets d'incident réseau.

2

ÉVOLUTIVITÉ ET PERFORMANCE ILLIMITÉES

- Architecture cloud-native permettant une parfaite élasticité des charges sur un réseau mondial haute performance comptant plus de 100 points de présence.
- Livraison des services aux sites distants en mode cloud, synonyme d'une simplification de la gestion WAN et d'un ROI pouvant atteindre 243 %.
- Visibilité orientée applications en couche L7 pour améliorer les politiques et définir des chemins réseaux plus efficaces.

3

EXPÉRIENCE UTILISATEUR IRRÉPROCHABLE

- Homogénéité de la sécurité et de la conformité, indépendamment du lieu de connexion des utilisateurs.
- Respect des SLA pour toutes les applications, y compris cloud, SaaS et UCaaS.

En résumé, une solution SASE efficace doit à la fois offrir une vue holistique de tout le réseau et offrir une protection et des performances avancées depuis une seule et même plateforme cloud unifiée.

Pour en savoir plus sur les produits SASE de Palo Alto Networks : Prisma Access • CloudGenix SD-WAN

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