LIVRE BLANC

Symantec® Data-Centric SASE

Une solution de sécurité économique et compatible avec l'architecture hybride basée sur les principes de vérification systématique (« Zero Trust »)

SOMMAIRE

La transformation numérique de l'entreprise exige une architecture de sécurité moderne

Nombreuses sont les entreprises qui opèrent leur transformation numérique, un processus qui consiste à servir plus de clients en ligne, migrer les applications vers les plates-formes cloud et intégrer les fournisseurs dans les chaînes d'approvisionnement numériques. Elles offrent également à leurs employés un plus large éventail d'options pour travailler depuis leur domicile, dans des bureaux distants ou encore depuis le site d'un client.

Cette transformation passe notamment par l'abandon de modèles de sécurité réseau obsolètes dans lesquels toute la pile de sécurité est hébergée dans des centres de données d'entreprise et à laquelle accèdent les employés dans les locaux de la société. Ces modèles n'ont pas été conçus pour permettre aux travailleurs nomades et distants d'accéder de manière pratique, sécurisée et rapide aux applications et données hébergées sur le cloud, ni pour leur garantir un accès sécurisé à l'infrastructure sur site existante.

Une pile de sécurité délivrée par le cloud constitue certes la méthode de transformation numérique privilégiée, mais cela n'est pas sans poser de problèmes pour les entreprises. Ainsi, elles craignent que la gestion d'un patchwork de services cloud puisse, au final, augmenter les coûts et la complexité de la sécurité du réseau. De nos jours, les entreprises informatiques cherchent à instaurer un nouveau modèle pour fournir des services de sécurité et réseau à faible latence aux employés d'entreprises numériques orientées cloud opérant depuis plusieurs emplacements. À ce titre, l'architecture SASE (Secure Access Service Edge) apparaît comme la candidate idéale, mais l'empreinte d'une grande entreprise en termes de sécurité s'avère souvent particulièrement complexe. Pour implémenter une architecture SASE comme il se doit, il ne faut pas agir dans la précipitation. Surtout, l'entreprise ne doit pas abandonner les principes « Zero Trust » pour atteindre l'efficacité opérationnelle. Ce livre blanc présente l'architecture SASE et explique comment Symantec® by Broadcom met en œuvre les concepts sous-jacents.

Qu'est-ce que SASE ?

Pour obtenir la définition la plus complète de SASE, nous vous invitons à consulter la note de recherche *The Future of Network Security Is in the Cloud* du bureau d'étude de marché Gartner. Cette note, publiée en août 2019, a été rédigée par Neil MacDonald, Lawrence Orans et Joe Skorupa. Comme d'autres fournisseurs et analystes du secteur après eux, ils décrivent SASE comme une combinaison de concepts, de principes et de technologies conçus pour améliorer les performances et la sécurité des réseaux dans un environnement de travail mobile et distant, dans lequel les utilisateurs accèdent à des applications et des données disséminées sur des centres de données d'entreprise et de multiples plates-formes cloud.

LA CONVERGENCE RÉDUIT LE NOMBRE DE PRODUITS, DE FOURNISSEURS ET D'AGENTS DE TERMINAL DISTINCTS À GÉRER, ET OPTIMISE L'UTILISATION DES RESSOURCES RÉSEAU AFIN D'AMÉLIORER LES PERFORMANCES DES APPLICATIONS POUR LES UTILISATEURS.

SASE s'articule autour de plusieurs concepts essentiels :

- Convergence des services réseau hébergés dans le cloud et des solutions de sécurité réseau
- Prise en charge des principes essentiels d'un modèle de sécurité « Zero Trust »
- Points de présence (POP) étendus et appairage pour des performances optimales
- Gestion et surveillance simplifiées

Convergence des services réseau hébergés dans le cloud et des solutions de sécurité réseau

L'un des concepts fondamentaux de SASE est la convergence des services réseau, tels que les réseaux étendus à définition logicielle (SD-WAN), et des technologies de sécurité hébergées dans le cloud, comme la passerelle web sécurisée (Secure Web Gateway, SWG), le courtier en sécurité d'accès au cloud (CASB, Cloud Access Security Broker), la prévention contre les pertes de données (DLP, Data Loss Prevention), l'isolement du navigateur, l'accès réseau « Zero Trust » (ZTNA, Zero Trust Network Access) ou encore l'inspection SSL.

Dans ce contexte, la convergence est synonyme de haut degré d'intégration, de sorte que les services réseau et les solutions de sécurité réseau puissent s'échanger mutuellement des informations, utiliser les travaux réalisés par l'autre partie, et appliquer des politiques de sécurité et réseau de manière cohérente, en temps réel, sur une architecture cloud à hautes performances. La convergence peut, par exemple, permettre la mise en place d'un processus fluide dans lequel le trafic réseau relatif à une application stratégique peut être déchiffré, analysé à la recherche de malwares, identifié comme étant sensible à la latence et acheminé vers une plate-forme cloud en empruntant la voie la plus rapide et la plus fiable.

Au chapitre des avantages de la convergence, citons également l'amélioration des performances et la réduction de la latence en activant une inspection en un seul passage du trafic réseau. Ainsi, au lieu d'avoir plusieurs services de sécurité qui déchiffrent le trafic SSL/TLS provenant d'une application web et le chiffrent à nouveau, le service peut déchiffrer le trafic une seule fois, le rediriger vers plusieurs services de sécurité pour une inspection et une analyse en parallèle, puis le chiffrer à nouveau pour le transmettre aux utilisateurs.

La convergence réduit également le nombre de produits, de fournisseurs et d'agents de terminal distincts à gérer, et optimise l'utilisation des ressources réseau pour améliorer les performances des applications pour les utilisateurs.

Prise en charge du modèle de sécurité « Zero Trust »

Les principes « Zero Trust » viennent parachever l'infrastructure SASE de trois manières différentes :

- Chaque demande d'accès à une ressource d'entreprise doit être évaluée (si possible, de manière transparente pour l'utilisateur) en fonction de plusieurs facteurs, tels que l'identité et le rôle de l'utilisateur, le rôle et l'emplacement de l'appareil, et la sensibilité de l'application et des données demandées.
- L'accès d'un utilisateur aux ressources doit être limité par le niveau de confiance défini dans le cadre de l'évaluation.
- Le niveau de confiance et d'accès aux ressources doit être réévalué en permanence en cours de session sur la base des comportements de l'utilisateur.

La mise en œuvre de l'infrastructure SASE doit prendre en charge la sécurité « Zero Trust » pour s'assurer que les employés et d'autres utilisateurs puissent accéder aisément aux ressources de l'entreprise depuis n'importe où et sur tout appareil, tout en réduisant les risques de violation des données que font peser les personnes malveillantes.

UNE SOLUTION SASE DOIT INCLURE UN RÉSEAU MONDIAL DE POINTS DE PRÉSENCE VERS INTERNET, AINSI QUE DES RELATIONS D'APPAIRAGE AVEC DES FOURNISSEURS D'APPLICATIONS ET DE PLATES-FORMES CLOUD DE PREMIER PLAN AFIN DE RÉDUIRE LA LATENCE ET DE GARANTIR DES PERFORMANCES ÉLEVÉES.

Points de présence étendus et appairage pour une latence optimale

Les analystes de Gartner font également observer que pour offrir aux employés une expérience utilisateur positive et un accès illimité aux ressources cloud, une solution SASE doit comporter un réseau mondial de points de présence vers Internet, ainsi que des relations d'appairage avec des fournisseurs d'applications et de plates-formes cloud de premier plan afin de réduire la latence et de garantir des performances élevées.

Gestion et surveillance simplifiées

Enfin, une infrastructure SASE offre une gestion et une surveillance simplifiées afin de gérer le nombre sans cesse croissant d'appareils et d'utilisateurs mobiles et distants, ainsi que les nombreux services dont ils doivent pouvoir bénéficier à l'échelle locale et dans le cloud. Il doit, par exemple, être possible de proposer davantage de services sur des terminaux client et des appareils périphériques avec moins d'agents. Une seule console de gestion doit être en mesure de consigner et de présenter les informations émanant de plusieurs services réseau et de sécurité du réseau.

Avantages d'une solution SASE axée sur les données

Dans un monde basé sur le cloud, les modèles de sécurité et réseau traditionnels axés sur les centres de données deviennent de plus en plus complexes et coûteux. Dans le même temps, ils complexifient l'expérience utilisateur et réduisent la productivité. Ils limitent également l'évolutivité et la flexibilité. Une architecture SASE axée sur les données (« Data-Centric ») est conçue pour résoudre ces problèmes tout en offrant plusieurs avantages concrets et, au final, la forme de protection des données la plus sûre qui soit.

Amélioration des performances du réseau et des applications

L'intelligence applicative et l'application des politiques à la périphérie du réseau améliorent les performances des applications et des réseaux en permettant aux employés et aux appareils de se connecter directement à Internet. Cela permet de réduire le nombre de sauts jusqu'aux applications et services en exploitant les dorsales des fournisseurs de services plutôt que l'Internet public, et en utilisant des fonctions de gestion du trafic afin d'offrir une qualité de service élevée pour les applications sensibles à la latence.

Une sécurité renforcée et plus homogène

Avec la convergence des services réseau et de sécurité réseau, les politiques de sécurité peuvent être appliquées de manière plus homogène sur plusieurs technologies de sécurité et dans tous les secteurs de l'entreprise, et ce que les données soient hébergées sur site, dans le cloud ou dans des environnements hybrides. L'opération de déchiffrement et d'inspection en un seul passage réduit la latence du réseau et permet de s'assurer que le trafic est analysé par l'ensemble des outils de sécurité (en fonction de la politique).

SASE PERMET AUX ENTREPRISES DE GÉRER LES SERVICES DE SÉCURITÉ ET RÉSEAU DE MANIÈRE CENTRALISÉE ET UNIFIÉE, AVEC UN NOMBRE RÉDUIT D'AGENTS DE TERMINAL.

Activation de l'accès réseau « Zero Trust »

L'un des principaux atouts de l'infrastructure SASE est de permettre aux appareils et employés distants et mobiles d'accéder à des ressources cloud, hybrides et sur site depuis n'importe où, en fonction des autorisations correspondant à leur identité, à leur appareil, et au contexte de leur demande et des données sollicitées, sans avoir recours à de coûteux VPN.

Utilisation plus facile et gestion simplifiée

SASE permet aux entreprises de gérer les services de sécurité et réseau de manière centralisée et unifiée, avec un nombre réduit d'agents de terminal. Cela leur permet aussi de rationaliser le nombre de fournisseurs d'outils de sécurité et réseau afin de simplifier l'administration et la coordination.

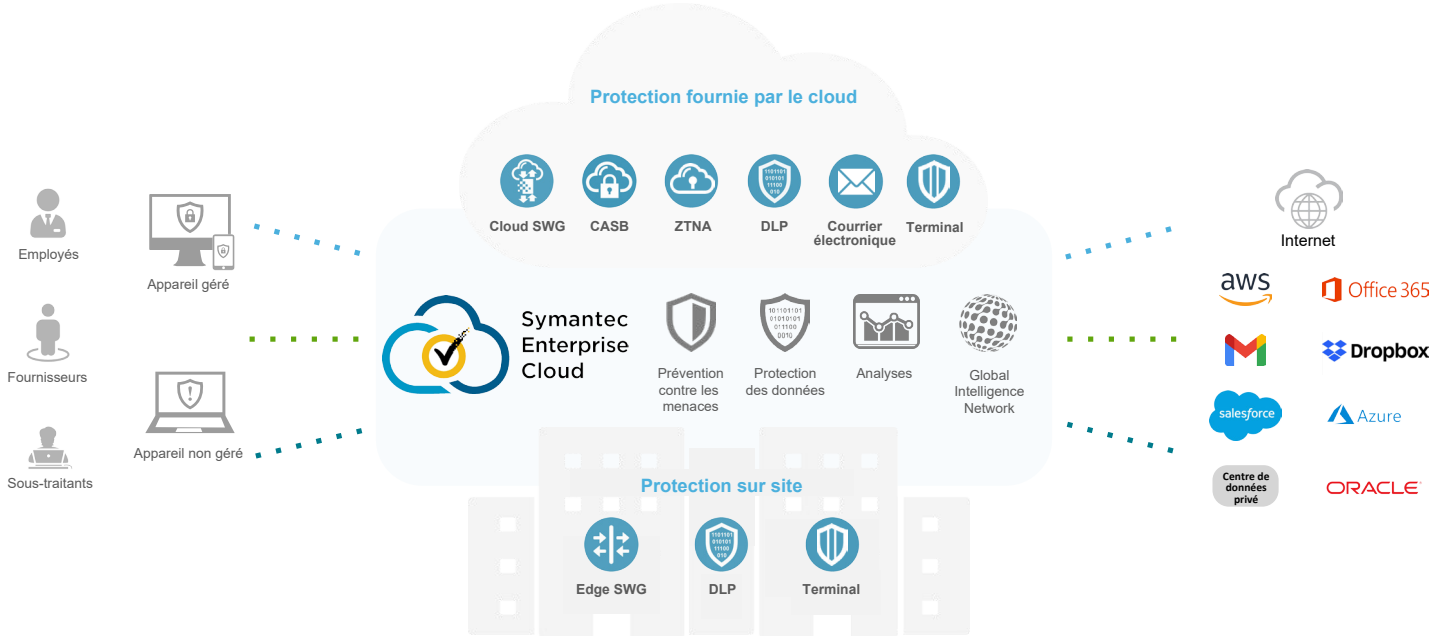
Réduction des coûts et augmentation de la productivité

SASE offre plusieurs axes pour réaliser des économies, dont une réduction de la dépendance vis-à-vis des connexions MPLS onéreuses pour réacheminer le trafic réseau des filiales vers les centres de données. Il permet également aux entreprises de regrouper de nombreux dispositifs de sécurité et de périphérie du réseau au sein d'un plus petit nombre d'appliances physiques et virtuelles. La productivité des équipes en charge du réseau et de la sécurité s'en trouve améliorée, dans la mesure où la gestion et la configuration sont simplifiées. Un accès réseau plus simple et plus uniforme se traduit par une productivité accrue et une meilleure satisfaction des employés.

Symantec Data-Centric SASE : convergence

L'une des principales caractéristiques de SASE est la convergence des services réseau et des technologies de sécurité réseau. L'illustration suivante montre comment Symantec intègre un large éventail de ces technologies.

Illustration 1 : Symantec SASE applique des politiques « Zero Trust » pour les applications sur les plates-formes cloud et dans les centres de données



Secure Web Gateway : un ensemble complet de technologies de sécurité intégrées

Symantec Cloud Secure Web Gateway (SWG) est la pierre angulaire de la solution Symantec SASE. Elle intègre des technologies de sécurité avancées et les rend accessibles dans le cloud. Cloud SWG, au même titre que toute la pile de sécurité Symantec, s'exécute sur la plate-forme cloud mondiale à hautes performances de Google. Optimisé pour la périphérie du réseau, Google Cloud fournit l'une des plates-formes de calcul les plus vastes et les mieux connectées au monde pour les télétravailleurs. Symantec Cloud SWG s'exécute sur l'infrastructure Google et évolue rapidement pour répondre aux exigences des nouvelles charges de travail en réduisant, par exemple, les temps d'intégration de quelques jours ou semaines à seulement quelques heures. L'infrastructure à définition logicielle se répare beaucoup plus rapidement que les précédentes générations d'infrastructure PoP dédiée utilisées par d'autres fabricants, dont l'évolutivité repose sur des composants réseau physiques. Le fait qu'il s'agisse d'une application entièrement « cloud native » permet aux ingénieurs de Symantec de se concentrer sur la sécurité, tandis que Google fournit des performances et une évolutivité de pointe pour optimiser la pile de sécurité de Symantec.

Secure Web Gateway et déchiffrement SSL/TLS

Symantec Cloud SWG s'articule autour d'une plate-forme de sécurité haut de gamme qui filtre le trafic Internet indésirable, détecte les malwares et le code malveillant, et déchiffre le trafic chiffré avec la technologie SSL/TLS pour le partager avec d'autres outils de sécurité. La passerelle extrait et inspecte les fichiers, identifie le trafic en provenance des différentes applications, et applique les politiques de conformité, de sécurité et QoS appropriées à chaque flux d'application.

Cloud SWG repose sur une architecture de proxy de transfert qui garantit que 100 % du trafic web peut être authentifié, déchiffré et analysé avant que les employés puissent y accéder. Cette solution offre également de bien meilleures performances que les pare-feu de nouvelle génération, pour un coût inférieur, lorsque des fonctions telles que le chiffrement et l'extraction de fichiers sont activées[1].

[1] Pour une explication détaillée de l'importance d'une architecture de proxy, consultez le livre blanc : Next Generation Secure Web Gateway : The Cornerstone of Your Security Architecture.

SYMANTEC CLOUD FIREWALL SERVICE (CFS) REPOSE SUR LA TECHNOLOGIE DE POINTE NGFW.

Cloud Access Security Broker (CASB)

Cloud SWG est intégré à la technologie Symantec CloudSOC®, ce qui permet aux entreprises de contrôler l'accès aux données hébergées sur des charges de travail SaaS. Les administrateurs peuvent également détecter et bloquer l'accès au cloud et à d'autres applications non autorisées (Shadow IT), et imposer des contrôles tels que la détection de malwares sur les téléchargements de fichiers.

Cloud Firewall Service

Symantec Cloud Firewall Service (CFS) repose sur la technologie de pointe NGFW. CFS effectue une inspection approfondie et permet aux entreprises d'opérer un contrôle du trafic réseau sur l'ensemble des ports et protocoles, et pas seulement sur quelques-uns. Il identifie le trafic en provenance de différentes applications, et peut appliquer des politiques en fonction des applications, des groupes d'utilisateurs (par le biais d'une intégration étroite des fonctions de gestion des identités des utilisateurs de Cloud SWG) et de facteurs tels que la position des utilisateurs (itinérance ou emplacement spécifique). CFS peut appliquer des règles de pare-feu en fonction du comportement, des autorisations et de la géolocalisation de l'utilisateur. Il permet également de gérer le pare-feu et de créer des rapports de façon centralisée via le portail Cloud SWG.

Web Isolation

Symantec Web Isolation assure une protection contre les ransomwares, les malwares et les attaques par hameçonnage qui ciblent les navigateurs. Les utilisateurs sont autorisés à accéder à des sites non répertoriés et potentiellement dangereux. Cependant, les pages qui y sont hébergées sont exécutées et affichées dans un conteneur distant temporaire et sécurisé. Seul un rendu des informations ne présentant aucun danger est envoyé au navigateur des utilisateurs, de sorte qu'aucun ransomware ou malware ne puisse être installé ni exécuté sur les terminaux des employés. Pour réduire les risques de compromission des informations d'authentification, les pages web peuvent être rendues en lecture seule. Cela évite que les utilisateurs n'envoient les informations d'authentification de l'entreprise ainsi que d'autres données sensibles. Les liens vers des sites web malveillants envoyés dans des messages électroniques sont rendus inoffensifs, de sorte qu'ils ne puissent pas transmettre de malwares ni de ransomwares aux ordinateurs des destinataires.

SYMANTEC WEB ISOLATION ASSURE UNE PROTECTION CONTRE LES RANSOMWARES, LES MALWARES ET LES ATTAQUES PAR HAMEÇONNAGE QUI CIBLENT LES NAVIGATEURS.

Data Loss Prevention

Les solutions Data Loss Protection (DLP) de Symantec surveillent et analysent tout le trafic (qu'il s'agisse du Web, des applications ou du courrier électronique) pour éviter que du contenu sensible ne sorte de l'entreprise, ou que des appareils ou des utilisateurs à risque n'y accèdent. Ce comportement applique des politiques de conformité et de sécurité gérées de manière centralisée, et réduit les risques de fuites de données. La solution DLP de Symantec est capable de détecter les informations envoyées à des applications cloud de type « Shadow IT » et d'analyser les applications cloud afin de détecter les fichiers sensibles chargés par les employées en utilisant des liens externes à l'entreprise (accès hors bande).

Analyse du contenu et des malwares avec Sandboxing

Sandboxing permet d'observer et d'analyser les actions des malwares et des fichiers suspects dans un espace isolé de notre plate-forme cloud. Cette technique révèle les comportements malveillants et expose les menaces exploitant les vulnérabilités existantes (menaces « Zero Day ») sans aucun risque pour vos terminaux et systèmes. Symantec Content Analysis fournit des fonctions avancées, telles que l'utilisation de plusieurs techniques d'analyse (dont l'analyse de règles YARA, comportementale et statique), la détection d'exploits en mémoire, la détection d'évitement du bac à sable (y compris la livraison différée) et l'utilisation d'images de bac à sable personnalisées. Cette solution tire également parti de la vaste base de données de renseignements sur les menaces de Symantec pour identifier et catégoriser rapidement les menaces.

Accès réseau « Zero Trust »

Symantec Zero Trust Network Access (ZTNA) assure une connectivité point à point au niveau de l'application, dissimulant ainsi toutes les ressources auprès des appareils des utilisateurs finaux et d'Internet. La surface d'attaque au niveau du réseau est entièrement supprimée, et les techniques de mouvement latéral et les menaces basées sur le réseau sont bloquées. Symantec ZTNA permet d'appliquer aisément des politiques d'activité et d'accès précises afin d'empêcher tout accès non autorisé aux ressources d'entreprise. Les entreprises peuvent sécuriser l'accès de leurs partenaires et employés, ainsi que l'accès BYOD, en implémentant une autorisation contextuelle continue basée sur la ressource, l'utilisateur ou l'appareil.

Écosystème partenaire SD-WAN

Symantec est intégré aux services réseau et produits SD-WAN de pointe, qui sont testés pour s'assurer que les technologies interagissent avec ses propres solutions de sécurité web.

Avantages de la convergence et de l'intégration

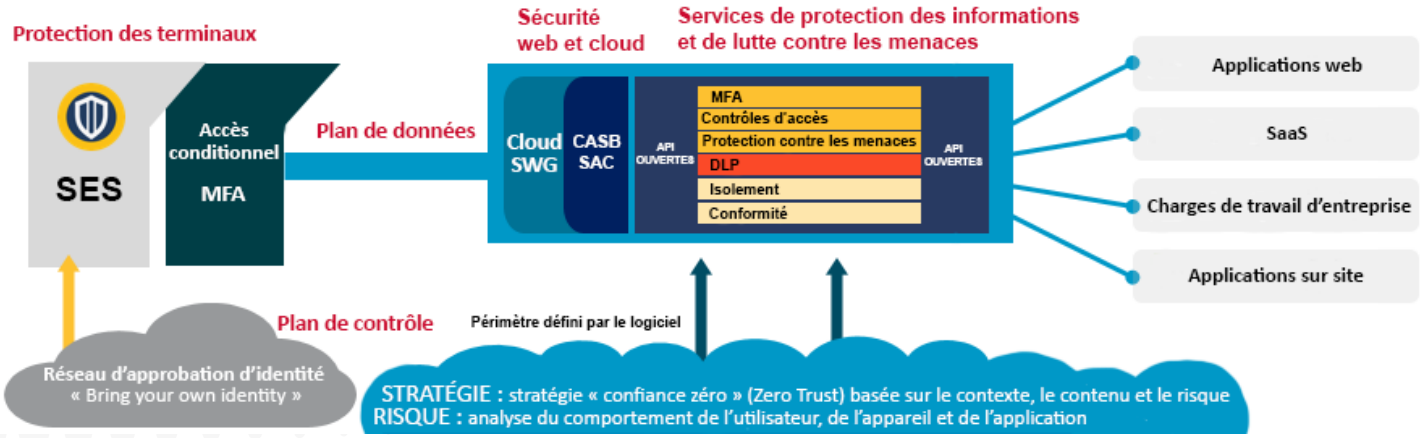
L'intégration des technologies de sécurité et réseau dans la plate-forme cloud de Symantec s'articule autour des principes SASE. Elle permet aux composants de la plate-forme de partager des informations, de renforcer leurs capacités mutuelles et d'appliquer des politiques de sécurité de manière cohérente. Cela garantit également une gestion simplifiée, dans la mesure où les administrateurs peuvent surveiller les activités et définir des politiques de façon centralisée pour les utilisateurs, applications et données, quel que soit leur emplacement. Ajoutons encore que les fonctions de sécurité et réseau peuvent interopérer afin d'améliorer les performances et de réduire les coûts ; par exemple, en acheminant efficacement le trafic lié à la sécurité à l'aide de la plate-forme réseau la plus rapide et la plus fiable via Google Cloud.

Symantec Data-Centric SASE : activation de la surveillance en continu et de la sécurité « Zero Trust »

L'architecture SASE se distingue également par la prise en charge de la sécurité « Zero Trust ». Parmi les principes essentiels, citons notamment l'évaluation de chaque demande d'accès à une ressource de l'entreprise afin de déterminer à quel point elle est fiable, la limitation de l'accès en fonction du degré de confiance et la réévaluation continue du degré de confiance sur la base du comportement de l'utilisateur.

Le schéma ci-dessous illustre notre approche en ce qui concerne l'utilisation de SASE pour la sécurité « Zero Trust ».

Illustration 2 : Approche Symantec concernant l'accès réseau « Zero Trust »



Symantec Endpoint Security (SES) fournit un agent de terminal unique pour la réduction de la surface d'attaque, la prévention des attaques, la prévention des fuites de données et la technologie EDR (Endpoint Detection and Response). Cette solution peut également faire office d'agent « Zero Trust » en recueillant des informations sur l'utilisateur et l'appareil, en prenant en charge l'authentification multifactorielle et en proposant des fonctionnalités d'accès conditionnel et de routage sécurisé.

Symantec ZTNA et CloudSOC CASB sont tous deux des services cloud qui fournissent une gestion des accès granulaire et appliquent des politiques « Zero Trust » pour les applications sur les plates-formes cloud, ainsi qu'au sein des environnements de centre de données sur site. Lorsque le service Symantec ZTNA reçoit des demandes d'accès aux ressources de l'entreprise de la part des terminaux, il analyse les informations relatives à l'utilisateur, à l'appareil, à l'emplacement et à l'authentification, et se connecte à des plates-formes de gestion des identités pour obtenir les rôles assignés aux utilisateurs. Il évalue également la sensibilité des applications et des données consultées, ainsi que les opérations demandées. Symantec ZTNA autorise alors les utilisateurs à se connecter uniquement aux ressources auxquelles ils ont le droit d'accéder. Enfin, il utilise en permanence l'analyse des données pour surveiller les comportements des utilisateurs et réévaluer le degré de confiance. Symantec CloudSOC Mirror Gateway permet d'étendre une protection du même type aux appareils non gérés (BYOD, par exemple) sans qu'un agent soit nécessaire.

Avantages de la prise en charge de ZTNA

Notre méthodologie de prise en charge de la sécurité « Zero Trust » s'accompagne de plusieurs avantages non négligeables :

- Une expérience utilisateur simple et cohérente pour accéder aux ressources de l'entreprise, et la possibilité de se passer des coûteux VPN qui n'ont pas été conçus pour une utilisation à grande échelle par toute la communauté des utilisateurs.
- Une réduction des violations de données, dans la mesure où les entreprises peuvent appliquer des politiques très précises pour contrôler l'accès à leurs ressources en fonction des autorisations et de l'identité des utilisateurs, de l'état et de l'emplacement des appareils, de la sensibilité des ressources et d'autres facteurs qui déterminent le degré de confiance.
- La garantie que tout le trafic réseau, y compris celui provenant des réseaux de bureau, sera surveillé, inspecté et acheminé sur la base de politiques.

Symantec Data-Centric SASE : prise en charge réseau de la sécurité à la périphérie du réseau et dans le cloud

Comme indiqué précédemment, lorsque les employés qui travaillent depuis chez eux et dans des bureaux distants souhaitent se connecter à des applications cloud, cela n'a aucun sens d'acheminer leur trafic réseau vers les centres de données centraux de l'entreprise en vue de l'inspecter et d'y appliquer des politiques. Cette approche nuit à l'expérience utilisateur en exigeant des utilisateurs qu'ils créent une connexion VPN pour chaque action. Elle augmente également la latence des demandes en les acheminant vers le centre de données sur site à l'aide du VPN avant de les envoyer sur Internet.

LES AVANTAGES DE LA SOLUTION SASE DE SYMANTEC SONT INDISCUTABLES : UN DÉBIT 144 % PLUS ÉLEVÉ ET UNE LATENCE 62 % PLUS FAIBLE QUE LE TRAFIC TRANSITANT PAR L'INTERNET PUBLIC.

Pour améliorer l'expérience et la productivité des télétravailleurs, une connexion directe au cloud est nécessaire. Pour ce faire, il convient de placer des services de sécurité sur le chemin direct entre les terminaux et les applications, sans réacheminer le trafic vers un site central.

Quant aux applications sensibles à la latence, telles que la collaboration, le VoIP, le streaming multimédia et la visioconférence, elles exigent une dorsale réseau à hautes performances et à faible gigue qui soit à la fois fiable et évolutive. L'importance des performances et de l'évolutivité augmente encore lorsque les applications IoT passent en production.

Dans les sections précédentes de ce livre blanc, nous avons parlé des solutions Symantec qui assurent la sécurité à la périphérie du réseau : sécurité fournie à partir du cloud, via l'emplacement périphérique le plus proche de la position de chaque utilisateur, que ce soit à domicile ou dans une filiale. Nous avons également mis en avant quelques offres Symantec qui fournissent des services de sécurité sur le terminal proprement dit.

Symantec propose une infrastructure cloud à hautes performances et hautement évolutive basée sur Google Cloud. Cette infrastructure jouit d'une présence mondiale et de relations d'appairage de pointe avec des fournisseurs de réseau de diffusion de contenu (CDN). Tolly Group a testé la pile de sécurité SASE de Symantec exécutée sur Google Cloud par rapport au trafic direct vers Internet n'ayant fait l'objet d'aucune inspection de sécurité. Les avantages de la solution SASE de Symantec sont indiscutables : un débit 144 % plus élevé et une latence 62 % plus faible que le trafic transitant par l'Internet public. Cela signifie que non seulement les clients Symantec bénéficient, comme prévu, d'une inspection complète et d'une protection contre les menaces, mais aussi d'une amélioration sensible des performances.

Avantages de Symantec Security Intelligence à la périphérie du réseau et dans le cloud

L'infrastructure cloud à hautes performances de Symantec offre de nombreux avantages :

- Éviter les pertes de performances et les surcoûts liés à l'acheminement du trafic réseau vers le centre de données à des fins d'inspection et d'application des politiques.
- Améliorer les performances des applications pour tous les utilisateurs, que ce soit au siège de l'entreprise, dans une filiale ou à distance.
- Améliorer sensiblement les performances des applications à l'échelle mondiale en tirant parti de la dorsale réseau de Google, ainsi que de la couverture POP généralisée garantie par les solides partenariats que nous avons noués avec les FAI et les fournisseurs CDN.
- Bénéficier d'une parfaite visibilité des menaces, grâce au réseau civil de renseignements sur les menaces le plus vaste du monde.
- Disposer de l'offre SASE la plus complète proposée par un seul fournisseur, basée sur l'architecture de pointe Secure Web Gateway.
- Tirer parti d'options flexibles autorisant des déploiements hybrides personnalisés, sur site ou intégralement dans le cloud, capables d'évoluer en fonction des besoins de l'entreprise et utilisant une formule de gestion des licences simple basée sur l'utilisateur.

L'UN DES PRINCIPAUX OBJECTIFS DE LA TECHNOLOGIE SASE EST DE SIMPLIFIER CONSIDÉRABLEMENT LA GESTION ET LA SURVEILLANCE DES SERVICES DE SÉCURITÉ ET RÉSEAU.

Symantec et SASE : gestion et surveillance simplifiées

L'un des principaux objectifs de la technologie SASE est de simplifier considérablement la gestion et la surveillance des services de sécurité et réseau.

Pour les administrateurs informatiques, le déploiement et la gestion de plusieurs agents sur chaque terminal constituent un facteur d'aggravation bien connu. Sur de nombreux terminaux, Symantec Enterprise Agent peut réduire le nombre d'agents à un seul. Si d'autres solutions Symantec, telles que ZTNA, peuvent utiliser cet agent, elles peuvent également fonctionner sans, ce qui permet la prise en charge d'appareils non gérés, tout en réduisant sensiblement les coûts de déploiement et de maintenance.

Symantec propose une console de gestion centralisée pour sa solution SASE. Elle permet aux équipes en charge des opérations et de la sécurité de surveiller et de gérer les politiques et l'administration du service SWG, du terminal, ainsi que d'autres composants de sécurité essentiels, ce qui réduit la charge administrative et garantit une protection homogène. De la même manière, Symantec Unified Policy Enforcement (UPE) et l'intégration entre Cloud SWG et CloudSOC permettent aux administrateurs de gérer un ensemble commun de politiques de sécurité des données et web qui sont appliquées aux solutions de sécurité sur site et dans le cloud, simplifiant ainsi les charges de travail des administrateurs de sécurité.

Symantec offre également aux entreprises la possibilité de travailler avec un seul fournisseur pour développer leur propre architecture SASE, et de bénéficier ainsi des ressources et de l'expérience nécessaires pour proposer des produits de sécurité et réseau efficaces dès aujourd'hui, et des concepts novateurs tels que SASE à l'avenir.

Avantages d'une surveillance et d'une gestion simplifiées

Grâce à une surveillance et une gestion simplifiées, les entreprises peuvent réagir plus rapidement aux menaces, et libérer les ressources en charge du réseau et de la sécurité des tâches de routine pour qu'elles puissent se concentrer sur les points importants.

LES TESTS RÉALISÉS PAR TOLLY GROUP ONT MONTRÉ QUE SYMANTEC DISPOSAIT DE TOUS LES COMPOSANTS NÉCESSAIRES POUR OFFRIR UNE SOLUTION SASE COMPLÈTE.

Résumé

SASE a recueilli une large adhésion parmi les entreprises informatiques de premier plan, ainsi qu'au sein de la communauté des analystes du secteur et des experts en sécurité et réseau indépendants. Cette technologie a en effet de quoi séduire : amélioration des performances du réseau et des applications, renforcement de la sécurité, utilisation plus simple, réduction des coûts réseau et informatiques, sans oublier l'agilité commerciale.

Cela fait des années que Symantec occupe le leadership dans le domaine de la sécurité cloud et réseau avec ses services SWG, CASB et DLP en proposant une plate-forme de sécurité et réseau intégrée. Compte tenu de ces technologies de sécurité essentielles et d'autres composants critiques tels que le déchiffrement SSL/TLS, Web Isolation, ZTNA, Content Inspection et Sandboxing, il n'est pas étonnant que Tolly Group ait confirmé que Symantec disposait de tous les composants nécessaires pour offrir une solution SASE complète. Nous ouvrons la voie pour la mise en œuvre des concepts fondamentaux de la technologie SASE, à savoir :

- Convergence des services réseau et des solutions de sécurité réseau
- Prise en charge des principes de sécurité « Zero Trust »
- Prise en charge réseau de la sécurité à la périphérie du réseau et dans le cloud
- Gestion et surveillance simplifiées

Si vous souhaitez en savoir plus sur la façon dont les solutions Symantec peuvent vous aider à évoluer vers une architecture SASE tout en améliorant la sécurité et la conformité, en augmentant la productivité et en réduisant les coûts, contactez votre représentant Symantec ou rendez-vous à l'adresse suivante : www.broadcom.com/SASE

Pour plus d'informations, visitez notre site web à l'adresse suivante : www.broadcom.com

SED-SASE-WP102_FR 4 octobre 2023