Symantec by Broadcom

LIVRE BLANC

À la tête des futures innovations en matière de sécurité

LIVRE BLANC

À la tête des futures innovations en matière de sécurité

Symantec by Broadcom

SOMMAIRE

Résumé

La division Symantec de Broadcom est-elle à la pointe de l'innovation ? C'est une question que l'on est en droit de se poser, surtout quand il est facile de conclure que les nouvelles technologies ne sont créées que par de jeunes startups. Ses 40 ans d'histoire, l'accent mis sur la sécurité intégrée et le fait que ses solutions fonctionnent dans des environnements aussi bien locaux que cloud font que Symantec peut ne pas être considérée comme une *entreprise innovante*. Depuis son acquisition par Broadcom en 2019 et la redéfinition de ses priorités (vente de logiciels aux organisations les plus exigeantes du monde), il est facile de voir Symantec comme une des entreprises qui, parmi tant d'autres, se contente d'attendre son tour pour innover avec une technologie disruptive.

Pourtant, au sens large, Symantec a toujours innové, que ce soit en créant, en sélectionnant, en acquérant, en développant et en intégrant des technologies de sécurité, ou en anticipant et en adoptant les cadres de sécurité tels que Zero Trust et Secure Access Service Edge (SASE). Symantec continue à innover de différentes façons :

- En **restructurant** des logiciels de sécurité qui fonctionnent à présent sur Google Cloud, le premier réseau périphérique hautes performances et à faible latence au monde
- En **optimisant ses produits** pour répondre aux problèmes de conformité, d'intégration, de télétravail et d'environnement multi-cloud auxquels les entreprises internationales sont confrontées
- En **proposant des innovations commerciales**, telles qu'une tarification simplifiée consolidée pour offrir aux clients Symantec une flexibilité de déploiement maximale à un prix attractif basé sur l'utilisateur
- En **participant à des innovations en matière de normes** en collaboration avec le secteur, le gouvernement et les organismes de réglementation pour représenter les intérêts des clients et développer des solutions interopérables

Symantec® Enterprise Cloud (SEC) est l'innovation la plus récente. Cette solution de cloud hybride consolidée offre des fonctionnalités de protection des données et de protection contre les menaces qui s'appuient sur le réseau mondial de centres d'exploitation de sécurité de Symantec. Surensemble de la fonctionnalité Secure Service Edge qui intègre les principes Zero Trust, SEC est une solution de sécurité de bout en bout conçue pour les réseaux d'entreprise les plus complexes et les plus étendus.

Symantec continue à innover et son objectif de longue date de consolidation des agents est à présent à portée de main. Un agent Symantec unique couvrira l'ensemble des technologies, plates-formes et environnements pour une gestion cohérente de la conformité, de la sécurisation du télétravail et de la couverture de cybersécurité, sans lacunes ni chevauchements.

SYMANTEC A TOUJOURS INNOVÉ EN CRÉANT, EN ACQUÉRANT, EN INTÉGRANT ET EN ÉTENDANT DES SOLUTIONS DE CYBERSÉCURITÉ, AINSI QU'EN ANTICIPANT ET EN ADOPTANT DES CADRES DE SÉCURITÉ COMME ZERO TRUST ET SASE.

L'innovation selon Symantec

Symantec est depuis plus de 40 ans un leader reconnu dans le domaine de la cybersécurité, avec à son actif un long palmarès de réalisations. Depuis son rachat par Broadcom, Symantec a redéfini sa stratégie en privilégiant non plus les revenus trimestriels provenant de la vente de produits, mais les partenariats à long terme avec les plus grandes entreprises internationales. Ces clients ont de grandes attentes à l'égard de Symantec, mais l'innovation en fait-elle partie ?

Ce livre blanc démontrera que Symantec a toujours innové en créant, en acquérant, en intégrant et en étendant des solutions de cybersécurité, ainsi qu'en anticipant et en adoptant des cadres de sécurité tels que Zero Trust et SASE. Depuis son acquisition par Broadcom en 2019, la division Symantec Enterprise a continué d'affiner et d'intégrer des technologies de sécurité clés, tout en recentrant l'ensemble de son offre de sécurité sur l'infrastructure Google Cloud et en augmentant ses dépenses en R&D. Elle innove en mettant en place des processus métier qui étendent, regroupent et tarifent les offres en fonction des exigences des clients importants dont l'activité est disséminée sur plusieurs sites. En collaboration avec les gouvernements, les régulateurs et les organismes de normalisation, l'entreprise innove et façonne les technologies à l'échelle mondiale. Elle rassemble les technologies dans l'offre complète Symantec Enterprise Cloud, conçue pour fournir une sécurité multiplateforme orientée données pour les grandes entreprises.

L'innovation par l'acquisition : l'histoire de Symantec, de 1989 à 2019

Fondée en 1982 et cotée en Bourse depuis 1989, Symantec a développé ses activités de cybersécurité en identifiant et en acquérant des sociétés qui avaient développé des technologies de sécurité de niche prometteuses. Ces startups n'ayant généralement pas les ressources nécessaires, Symantec a entrepris de développer leurs produits spécifiques pour les convertir en solutions complètes commercialisables, compatibles avec d'autres technologies de sécurité ou intégrées à ces dernières. Les points forts de la stratégie d'*achat, de développement et d'intégration* de Symantec sont présentés dans le Tableau 1.

Comme le montre ce tableau, ces acquisitions sont plus que des solutions dédiées choisies pour augmenter le chiffre d'affaires. Intégrées à des produits plus larges ou étendues sur plusieurs plates-formes, elles continuent d'ajouter de la valeur longtemps après avoir perdu leur statut de produits autonomes.

Tableau 1 : Acquisition de Symantec et évolution des technologies acquises, de 1989 à 2019

Société	Technologie	Évolution
Certus	Antivirus	Mise à jour, étendue et intégrée à Symantec Endpoint Security Complete, Radicati Group's Top Player pendant sept années consécutives.
Vontu	Prévention contre les pertes de données	Fondation des solutions Core et Cloud de Symantec Data Loss Prevention, première place du classement Forrester Wave 2021 dans leurs segments respectifs.
Elastica	Cloud Access Security Broker	Mise à jour, étendue et intégrée en tant que point de contrôle dans Data Loss Prevention Cloud.
Blue Coat	Passerelle web sécurisée	Disponible en tant que service de sécurité réseau cloud avec une large gamme d'options et d'intégrations, leader de longue date dans la technologie SWG.
Skycure	Défense contre les menaces mobiles	Intégrée à Symantec Endpoint Protection Mobile pour une défense mobile prédictive et multicouche qui respecte la productivité des utilisateurs.

Société	Technologie	Évolution
Fireglass	Isolement web	Intégrée à Symantec Cloud Secure Web Gateway, permet aux appareils non gérés d'accéder aux applications cloud de façon sécurisée.
Javelin	Active Directory Threat Defense	Intégrée à Symantec Endpoint Security Complete afin de renforcer Active Directory et d'obfusquer pour arrêter le vol d'informations d'identification d'administrateur.
Luminate	ZTNA	Disponible dans Symantec ZTNA, passerelle cloud sécurisée permettant d'accéder aux applications privées.
Bay Dynamics	Information Centric Analytics	Élargie et intégrée en tant que fonctionnalité d'analyse des risques dans les solutions Symantec DLP Core et DLP Cloud.

Cadres et architectures

Symantec a acquis, développé et intégré des technologies de sécurité pour faire face aux menaces émergentes (violations de données, ransomware) et protéger les nouvelles plates-formes (mobiles, cloud). Dans le même temps, les cabinets d'analyse codifiaient ces nouveaux environnements informatiques et recommandaient des architectures et des cadres pour leur protection. Ces approches commerciales et analytiques étant mises en œuvre pour résoudre une même problématique, leur convergence n'a rien d'étonnant : les technologies Symantec s'alignent sur le travail des analystes, voire l'anticipent parfois. L'architecture de sécurité Zero Trust et la technologie SASE en sont deux parfaits exemples.

SYMANTEC A ACQUIS, DÉVELOPPÉ ET INTÉGRÉ DES TECHNOLOGIES DE SÉCURITÉ POUR FAIRE FACE AUX MENACES ÉMERGENTES ET PROTÉGER LES NOUVELLES PLATES-FORMES.

Zero Trust

L'adoption des plates-formes informatiques mobiles et cloud a progressivement affaibli le modèle de cyberdéfense basé sur un *périmètre sécurisé*. Celui-ci a été remplacé par une architecture de sécurité Zero Trust orientée données sans périmètre. L'approche Zero Trust repose sur l'authentification d'une personne, d'un appareil ou d'une charge de travail tentant d'accéder aux données, quel que soit son emplacement physique, son adresse réseau ou sa méthode d'accès, puis sur l'attribution des seuls privilèges d'accès associés à l'entité authentifiée. Elle nécessite une automatisation et une orchestration permettant aux technologies constitutives de fonctionner ensemble, ainsi que de la visibilité et des analyses pour surveiller, contrôler et gouverner l'architecture.

Bien avant l'introduction du modèle Zero Trust par Forrester Research en 2009, Symantec avait déjà assemblé, développé et proposé chacune des technologies nécessaires à la mise en œuvre de l'architecture, soutenues par des solutions de gouvernance et d'administration des identités permettant d'automatiser la vérification et la certification de l'accès des utilisateurs.

Avant que le National Institute of Standards and Technology ne l'officialise sous le nom SP 800-207, Symantec avait pris de nouvelles mesures pour fusionner les technologies Zero Trust dans son portefeuille de solutions cloud émergentes :

- **Symantec ZTNA**, solution Zero Trust Network Access (ZTNA) permettant de gérer l'accès aux applications déployées dans les centres de données ou les clouds IaaS/PaaS
- **Symantec VIP**, qui fournit des informations d'identification multifacteur basées sur le cloud et une analyse contextuelle des risques pour les appareils non gérés
- **Fonctionnalités orientées données Zero Trust**, intégrées aux solutions Symantec Secure Web Gateway, CASB, Endpoint et Email, activées par l'offre intégrée Symantec DLP

Technologie Secure Access Service Edge (SASE)

Codifié par les analystes de Gartner en 2019, SASE regroupe des fonctions de sécurité des réseaux et des données sous forme de services cloud fournis directement aux utilisateurs à la périphérie du réseau. La technologie SASE promet d'améliorer les performances du réseau et des applications, de renforcer la sécurité, ainsi que de réduire la complexité et les coûts. Elle fournit un avantage majeur, à savoir qu'elle évite les coûts et la latence liés à la transmission de l'ensemble du trafic via des centres de données centralisés, comme dans le cas des réseaux privés virtuels, par exemple. En 2021, Gartner a défini Secure Services Edge (SSE) comme un sous-ensemble produit de SASE pouvant être fourni sous forme de solution complète.

Comme avec le modèle Zero Trust, les technologies incluses étaient déjà disponibles dans les produits Symantec au moment où le modèle SASE a été codifié. Le Tableau 2 illustre la façon dont les technologies Symantec respectent le cadre SASE de Gartner, tel que validé par un tiers, Tolly Enterprises, LLC.

LES MODÈLES ZERO TRUST ET SASE ÉTAIENT DÉJÀ DISPONIBLES CHEZ SYMANTEC AU MOMENT DE LEUR CODIFICATION.

Lorsque le cadre n'est pas parfaitement respecté, c'est souvent parce que Symantec inclut une technologie (comme la protection des données au repos) ou un environnement (local par exemple) sous-représenté dans le cadre d'origine.

Tableau 2 : Technologies SASE de Symantec

Composant du cadre défini par Gartner	Domaine fonctionnel	Solution Symantec actuelle
Passerelle web sécurisée	Passerelle web sécurisée • Prévention et classification des menaces URL • Analyse de contenu avancée (sandboxing de malware)	Symantec Web Protection
CASB	Cloud Application Security Broker (CASB)	Symantec DLP Cloud
ZTNA/VPN	ZTNA	Symantec ZTNA
FWaaS	Pare-feu cloud	Symantec Web Protection
Isolement web	Isolement web	Symantec Web Protection
Déchiffrement	Inspection SSL	Symantec Web Protection
Prévention contre les pertes de données	Prévention contre les pertes de données	Symantec DLP Cloud

Source : Tolly Enterprises LLC, rapport n° 222122, juillet 2022

Acquisition de Symantec Enterprise par Broadcom

En novembre 2019, Broadcom a fait l'acquisition de l'activité Sécurité d'entreprise de Symantec Corporation, notre but déclaré étant « … d'étendre notre empreinte de logiciels d'infrastructure stratégiques au sein de notre base de clients Global 2000 ».

Séparée de son portefeuille grand public Norton et de son portefeuille destiné aux petites entreprises, l'activité Sécurité d'entreprise de Symantec était et reste étroitement alignée avec l'orientation stratégique de Broadcom qui est de cibler les plus grandes entreprises mondiales. Comme le montre l'encadré, les produits Symantec bénéficient d'une excellente pénétration sur ce segment haut de gamme et il leur reste encore une large marge de développement.

PÉNÉTRATION SUR LE MARCHÉ DE SYMANTEC ENTERPRISE

- **195** SOCIÉTÉS DU CLASSEMENT FORTUNE 500
- **697** SOCIÉTÉS DU CLASSEMENT GLOBAL 2000
- **13 SUR 13** DES MEILLEURES BANQUES
- **8 SUR 10** DES MEILLEURES ENTREPRISES DE TÉLÉCOMMUNICATIONS
- **7 SUR 10** DES MEILLEURS FABRICANTS D'AUTOMOBILES
- **+ DE 150 MILLIONS** D'UTILISATEURS PROFESSIONNELS DANS LE MONDE

Acquisition de Symantec Enterprise par Broadcom (suite)

L'acquisition a eu des effets spectaculaires sur la stratégie de Symantec, qui a recentré son attention sur la croissance à long terme plutôt que sur les revenus trimestriels, et a réalloué ses dépenses vers le conseil et le soutien aux clients existants plutôt que le développement de nouveaux comptes.

Tout comme les ressources en marketing et en ventes, l'innovation a été mobilisée pour promouvoir les intérêts de la base de clients mondiaux de Broadcom, en se concentrant sur les domaines les plus importants pour ces clients :

- **Conformité** : ce moteur majeur pour les grandes multinationales connaît une croissance rapide à mesure que de nouvelles autorités de régulation s'affirment et que les anciennes se fragmentent au niveau régional.
- **Intégration** : une priorité pour les grandes entreprises, à présent renforcée par les opportunités d'intégration des solutions Symantec avec Broadcom® ValueOps™, AIOps et d'autres logiciels d'entreprise.
- **Télétravail** : fait acquis depuis la pandémie et qui constitue un défi de taille pour créer une expérience utilisateur sécurisée et productive sur une infrastructure qui n'a pas été conçue en ce sens.
- **Environnements hybrides et multi-cloud** : l'infrastructure locale est obsolète, mais les inquiétudes en lien avec la résidence des données et la sécurité empêchent la plupart des multinationales de se lancer à 100 % dans le cloud.

Suite à l'acquisition par Broadcom, le rythme des annonces de nouveaux produits et des communiqués de presse s'est ralenti, et de nombreux analystes pensaient que Symantec *s'était détournée* de l'innovation. Mais cette période a en fait été l'une des plus chargées, productives et innovantes de son histoire, car Symantec a recréé l'intégralité de son infrastructure de sécurité dans le cloud pour répondre aux besoins de ses clients mondiaux.

Innovation post-acquisition

Après l'acquisition par Broadcom, il est rapidement devenu évident que Symantec devait restructurer son portefeuille cloud pour servir les entreprises clientes depuis le cloud avec des niveaux de performances élevés.

Partenariat stratégique avec Google

Comme nous l'avons vu plus haut, une architecture SASE fournit des services de sécurité directement aux appareils situés à la périphérie du réseau, évitant ainsi la perte de temps que représentait la nécessité de *communiquer* avec le centre de données local pour chaque transaction. Mais la vitesse et la latence sont toujours importantes dans le cloud : si le réseau périphérique est limité en bande passante ou physiquement éloigné de l'appareil d'un utilisateur, la latence augmentera et les performances en souffriront.

Pour réduire ces contraintes au maximum, Broadcom a repensé et restructuré l'ensemble de son offre (plus de 80 produits et services, y compris toutes les solutions Symantec) en tant que solutions Software-as-a-Service sur l'infrastructure Google Cloud, dans des environnements conteneurisés sous orchestration Kubernetes.

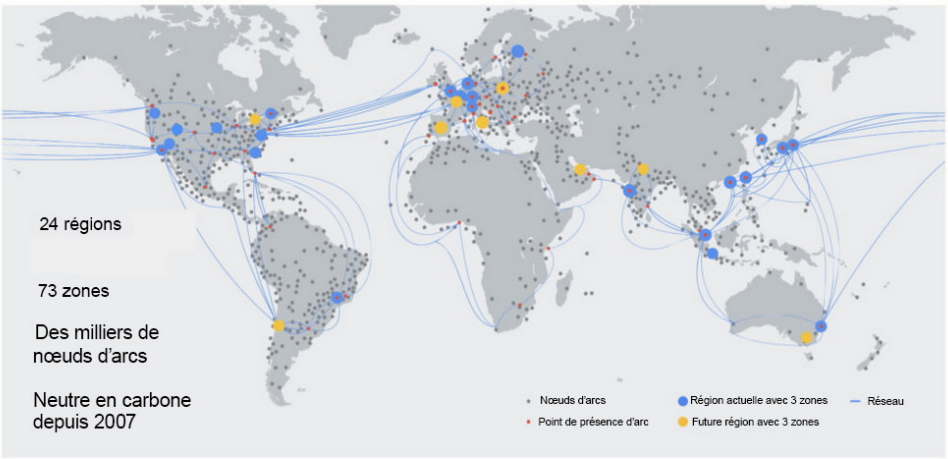
Partenariat stratégique avec Google (suite)

Google offre à présent les avantages suivants aux utilisateurs de Broadcom et de Symantec :

- **Portée globale** interconnectant les FAI, les fournisseurs de contenu et les utilisateurs sur un réseau privé à haut débit
- **Points de présence à la périphérie** sur plus de 180 échanges Internet et sur plus de 160 installations d'interconnexion dans le monde (voir l'Illustration 1 ci-dessous), ce qui permet de réduire les coûts et la latence
- **Routage efficace** sur la dorsale privée de Google, réduisant ainsi au maximum le trafic sur l'Internet public
- **Échelle inégalée**
- **Élasticité** en réponse aux changements imprévisibles
- **Stabilité** et résilience face aux perturbations

Malgré l'impact incontestable de la migration de 18 mois sur ses clients, Symantec offre à présent une sécurité cloud à des niveaux de performances supérieurs, validée par des tiers. Par rapport à l'Internet public, Symantec SASE sur Google Cloud a fourni un débit 144 % supérieur avec une latence inférieure de 62 % pour le trafic chiffré, et un débit supérieur de 14 % avec une latence inférieure de 19 % pour le trafic non chiffré. L'avantage de Symantec en termes de temps total de transaction s'est accru en même temps que la distance physique entre les parties, avec une amélioration de 21 % par rapport à l'Internet public pour les transactions dans la même ville, et une amélioration de 62 % pour les transactions entre la Californie et Singapour.

Illustration 1 : The Network Edge, tel que défini par Google Cloud, février 2021



Source : Blog Google Cloud

La dorsale de Google Cloud profite à Broadcom ainsi qu'à ses clients : les utilisateurs s'intègrent plus rapidement et les technologies les plus récentes garantissent de hauts niveaux de service en continu. Symantec a également collaboré avec Google pour créer des zones de localisation : celles-ci permettent de garantir que le contenu web est localisé pour le pays d'où provient la demande, même lorsque le FAI est situé en dehors de ses frontières. Pour son initiative et son assistance, Broadcom a reçu le prix Client Google Cloud de l'année en 2021.

L'innovation par gamme de produits

Cela n'indique en aucun cas que l'innovation produit s'est arrêtée dans la période qui a suivi l'acquisition de Symantec par Broadcom. Broadcom est, après tout, une entreprise qui réinvestit par principe chaque année plus de 20 % de son chiffre d'affaires dans la R&D. Le Tableau 3 présente un échantillon des innovations produits introduites par Symantec après son acquisition par Broadcom, y compris au plus fort de ses efforts de migration vers Google Cloud.

Tableau 3 : Innovations post-acquisition par Symantec

Les innovations de Symantec par gamme de produits
SÉCURITÉ DES TERMINAUX
• Adaptive Security consolide les informations provenant d'agents répartis dans une zone géographique, un service ou une autre entité pour répondre aux conditions locales, et non à un dénominateur commun mondial. • De nouveaux tableaux de bord mettent en évidence les comportements inhabituels sur les applications à haut risque telles que PowerShell, Net.exc, etc., pour contrecarrer les ransomwares et les attaques ciblées. • La console de gestion des terminaux a été migrée vers le cloud. • Régionalisation des solutions pour répondre à la souveraineté des données et à d'autres problèmes régionaux. • Threat Defense for Active Directory (TDAD) protège l'intégrité d'Active Directory, obfusque AD et neutralise le vol d'informations d'identification et la migration latérale typiques des attaques par ransomware. • Consolidation de l'agent : agent unique pour intégrer le pilotage du trafic nécessaire pour Cloud SWG.
SÉCURITÉ DES INFORMATIONS
• Développement continu de Data Loss Prevention de la version 15 à la version 16 (version 17 en cours). • De nouvelles politiques basées sur l'évaluation des risques utilisant Information Centric Analytics, basées sur les fonctionnalités UEBA, mais utilisables par les unités commerciales. • Consolidation des événements pour une gestion plus facile. • Mise en quarantaine organisée à l'aide de l'intégration de ServiceNow, réduisant ainsi le besoin de surveillance. • Innovations en matière de conformité au RGPD, par exemple l'obfuscation permet aux administrateurs de consulter les événements sans enfreindre les règles de confidentialité. • CASB propose à présent la gestion Oracle via la version cloud d'Enforce. • CASB a ajouté des solutions API, Securlet et Gateway pour la confiance dans les données et les données en mouvement.
SÉCURITÉ RÉSEAU
• Secure Web Gateway est désormais proposé sous forme de machines virtuelles ou de service cloud avec une console unique pour tous les facteurs de forme. • Plusieurs fonctionnalités réseau sont désormais disponibles sous la forme d'une solution SWG unique notamment Cloud SWG, Edge SWG, Cloud SWG, Edge SWG, Isolation, Content Analysis, SSL Inspection, App Visibility and Control, Intelligence Service et Centralize Management & Reporting. • Lancement et ajout de la nouveauté Service Cloud Firewall à tous les clients SWG. • Pilotage sélectif du trafic intégré à Secure Web Gateway et à l'agent consolidé de sécurité des terminaux de Symantec Enterprise Security Complete. • La fonctionnalité ZTNA avec et sans agent est désormais une alternative au VPN, avec un coût inférieur, moins de problèmes de sécurité et moins de complexité.
PLATES-FORMES ET ENVIRONNEMENTS
• Un unique agent Symantec Enterprise Security Complete consolidant les fonctionnalités Secure Web Gateway, ZTNA, CASB et Endpoint. • Migration vers la plate-forme hybride, et non uniquement cloud, dont les grandes multinationales ont besoin. • Extension de l'analyse du comportement des utilisateurs et des entités (UEBA) locale vers CloudSOC CASB et DLP Cloud. • Présentation de la technologie Mirror Gateway qui permet à des appareils totalement non gérés, sans agents d'aucune sorte, d'accéder de façon sécurisée aux réseaux d'entreprise. • Extension de l'agent DLP pour couvrir macOS et Linux. • Création de zones de localisation pour localiser le contenu web en fonction de l'origine géographique d'une demande, quel que soit l'emplacement du FAI.

Bon nombre de ces innovations constituent des intégrations ou des extensions d'une technologie aussi bien en local que dans des clouds privés/hybrides et publics. L'objectif de longue date de Symantec, qui était de proposer un agent et une console uniques dans Symantec Enterprise Cloud, est à portée de main et existe déjà pour le cloud. L'entreprise s'oriente également vers une console unique, ce qui lui permettra de réduire de façon substantielle les frais de gestion.

Innovations commerciales

Tout comme elle investit pour améliorer la facilité d'administration de ses produits, Symantec innove afin de rationaliser et d'accélérer ses propres processus métier au profit des entreprises clientes. Des centaines de références classées par fonction, environnement informatique, plate-forme, etc. sont à présent disponibles. Elles bénéficient d'une tarification annuelle par utilisateur consolidée et simplifiée qui offre un accès illimité à une catégorie de sécurité (terminal client, identité, réseau, données, etc.). Les entreprises clientes qui détiennent à l'heure actuelle vingt ou trente contrats avec Symantec (avec diverses conditions et dates d'expiration) peuvent à présent bénéficier de la protection complète offerte par Symantec Enterprise Cloud avec seulement quatre contrats. Elles obtiennent les avantages suivants :

- Accès à tout l'éventail de solutions dans une gamme de produits, pour une protection sans faille
- Coûts annuels prévisibles, même en cas d'augmentation de l'utilisation
- Réduction des coûts globaux de la cybersécurité
- Flexibilité accrue pour essayer de nouvelles technologies de cybersécurité sans risque financier
- Simplification des processus de maintenance, de mise à niveau et de renouvellement
- Propositions de service client dédiées pour aider les clients à tirer le meilleur parti des solutions
- Possibilité pour le client de choisir le format souhaité pour déployer ou redéployer les fonctionnalités de sécurité : logiciel, matériel, virtuel sur IaaS ou SaaS, dans le cadre d'un contrat unique.

Ces plans tarifaires sont disponibles pour la plupart des produits logiciels Broadcom et permettront de proposer des contrats simplifiés à l'échelle de l'entreprise couvrant la cybersécurité, l'automatisation, le DevOps et d'autres technologies Broadcom.

Innovations communautaires et normatives

Dans la mesure où le respect des réglementations et des normes occupe une place importante dans les processus décisionnels des multinationales, il est important pour ces dernières d'avoir des relations commerciales avec une entreprise qui comprend les enjeux et les impacts commerciaux probables de ces décisions. C'est le rôle qu'assume Symantec depuis plusieurs années, en conseillant le gouvernement américain, l'Union européenne, les Nations unies et divers organismes techniques, en préconisant des politiques visant à protéger ses clients sans imposer de charges inutiles sur leurs opérations. L'encadré ci-dessous détaille certains des exemples les plus importants.

INNOVATIONS COMMUNAUTAIRES ET NORMATIVES DE SYMANTEC

- Symantec est le premier fournisseur de cybersécurité présent au sein de l'Internet Engineering Task Force (IETF) et de l'Union internationale des télécommunications (UIT), la communauté des Nations Unies qui définit l'avenir des télécommunications et des technologies de l'information et des communications. Au cours des dernières années, Symantec a contribué aux efforts suivants :
  - Participation au groupe de travail ITU-T Study Group 17–Security pour développer des **standards de sécurité globaux**. La société a récemment détaché un employé de Symantec au poste de vice-président du groupe d'étude.
  - Apport de son schéma de cyberdéfense intégrée au projet Open Cybersecurity Schema Framework (OCSF) dans le but de briser les silos de données et de normaliser les données entre les solutions de cybersécurité pour une analyse plus rapide des données. Cet **article de blog** et cet **article du magazine Forbes** décrivent l'importance de cette innovation.
  - A été à l'avant-garde des efforts de déchiffrement TLS 1.3 pour répondre aux besoin de ses clients d'inspecter le trafic à la recherche de malwares pouvant être masqués par un chiffrement avancé. **Ce billet de blog** souligne les problématiques rencontrées.
  - A préparé ses solutions pour Encrypted Client Hello (ECH), une extension TLS qui comble la dernière lacune dans le chiffrement de bout en bout de la couche de transport. Symantec a identifié un problème (toujours lié à l'inspection) qui expose ses clients à un risque réglementaire, et s'emploie à définir une solution.
  - A contré l'*hyper-régionalisation* des standards Internet, à mesure que les réglementations et les normes se croisent pour créer des îlots de plus en plus petits de réglementation cohérente, avec des frontières qui ne peuvent être franchies sans tests de conformité ni intervention possible.
- Symantec est représenté et actif à Bruxelles alors que la présidence du Conseil de l'Union européenne et le Parlement européen définissent le Digital Operational Resilience Act (DORA). Grâce à sa participation, les produits Symantec seront conformes à cette législation avant même son entrée en vigueur.
- Symantec participe au Comité européen de la protection des données en tant que leader des logiciels de protection des données. Symantec a récemment identifié un risque dans le processus d'audit de conformité et l'a corrigé en obfusquant les informations personnelles identifiables lors de l'examen administratif.

Le prochain cycle d'innovation

Symantec continue d'innover dans des cadres et architectures de sécurité, dans le but de réduire la complexité de la gestion et de la conformité, ainsi que les lacunes et les chevauchements qui affectent les architectures de sécurité disparates. Symantec a introduit une solution à l'échelle de l'entreprise qui étend le cadre SASE de Gartner pour se concentrer sur la protection des données, la conformité et la veille sur les menaces.

Symantec Enterprise Cloud

Cette solution, Symantec Enterprise Cloud (SEC), est basée sur les principes suivants :

- **Consolidation :** plusieurs agents de terminal épuisent les ressources des clients, ajoutent de la complexité et augmentent les coûts. L'agent unique de SEC pour tous les terminaux client (ordinateurs portables, ordinateurs de bureau, tablettes, téléphones, serveurs et charges de travail cloud) met fin à la prolifération des agents, réduit la complexité et donne aux responsables une vue unique sur tous les terminaux. Consolidé avec Cloud Secure Web Gateway, l'agent fournit la sécurité des terminaux et du réseau aux terminaux itinérants.
- **Cloud hybride :** de nombreuses organisations doivent maintenir un centre de données d'entreprise pour des raisons commerciales, juridiques ou réglementaires : leur migration vers le cloud se fera toujours vers un environnement cloud hybride. Pour ces entreprises, la solution Symantec Enterprise Cloud peut être déployée comme une entité unique couvrant des environnements locaux et cloud gérés de façon unifiée. Elle peut également être déployée en tant que solution 100 % locale avec un point d'application local, ou en tant qu'implémentation 100 % cloud avec le point d'application dans le cloud.
- **Combinaison de la protection des données et de la protection contre les menaces :** Symantec Enterprise Cloud combine la prévention contre les pertes de données (DLP), visant à protéger les données qui transitent par les réseaux, les passerelles et les terminaux, avec la protection contre les menaces, qui permet d'identifier et d'atténuer les attaques. Les capacités de détection des menaces sont alimentées par les équipes de détection de Symantec et par le Symantec Global Intelligence Network, qui utilise l'intelligence artificielle pour convertir plus de neuf pétaoctets de données en informations exploitables sur les menaces.
- **Intégrations des SOC :** l'intégration dans les outils de cybersécurité permet à notre équipe de détection des menaces hautement qualifiée d'évaluer les informations sur les menaces, d'identifier des modèles, de bloquer les attaques et de dialoguer avec les clients pour optimiser leurs opérations SOC.
- **Conformité :** SEC applique et gère les contrôles de conformité de manière cohérente dans toutes les organisations. Une seule équipe de gouvernance peut gérer les risques liés aux données et effectuer des audits à partir d'une seule plate-forme, localement ou dans le cloud.
- **SSE :** la prise en charge de Secure Service Edge (SSE) fait partie de l'architecture de sécurité hybride et orientée données de Symantec.

Que réserve l'avenir ?

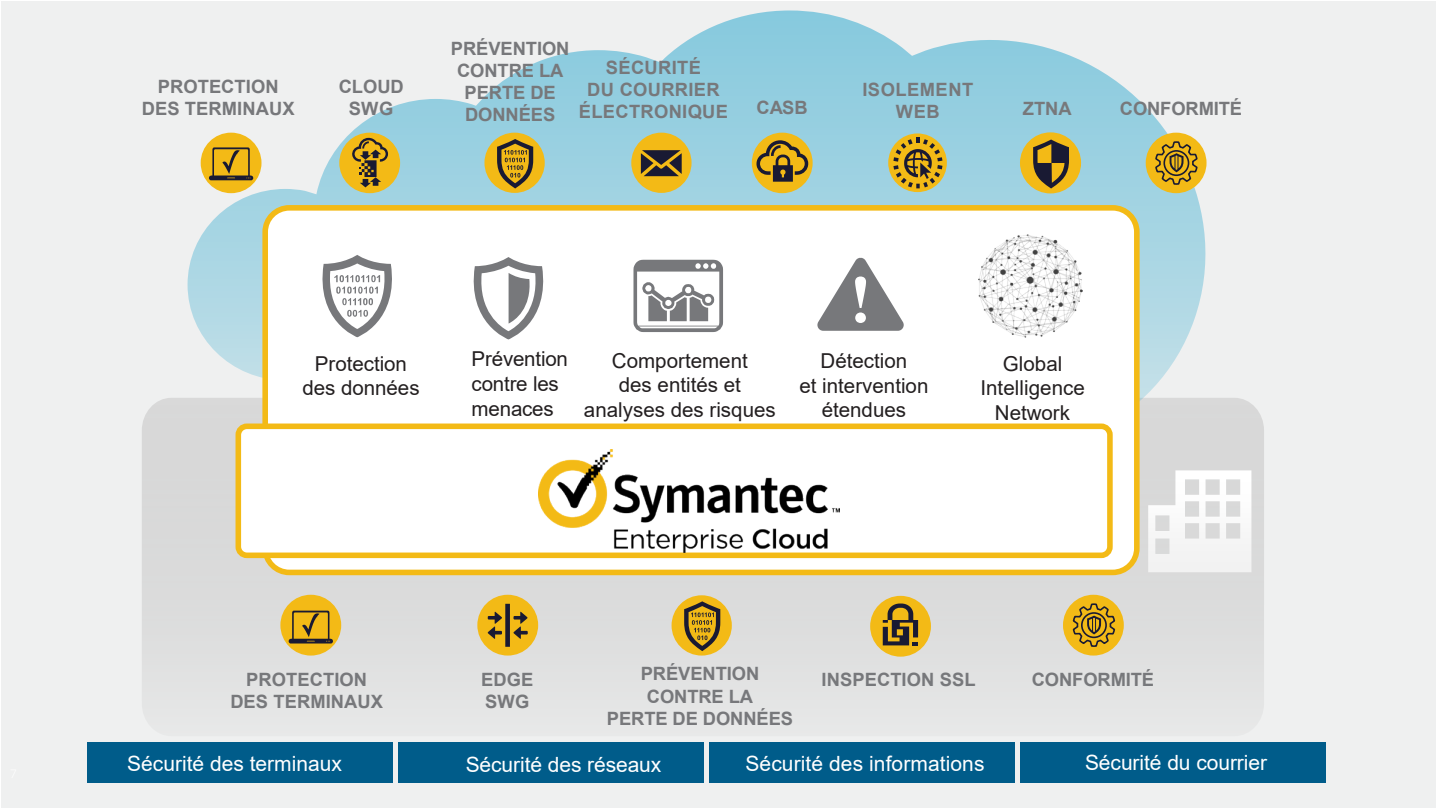
Au cours des prochaines années, les produits Symantec s'intégreront parfaitement les uns aux autres, car l'entreprise continue d'affiner et de mettre en œuvre sa vision pour Symantec Enterprise Cloud. Les clients auront accès aux avantages suivants :

- Agent Symantec unique pour l'ensemble des technologies, plates-formes et environnements : cet objectif de longue date en matière de cybersécurité est à présent à portée de main
- Gestion cohérente de la conformité, sécurisation du télétravail, protection des données et protection contre les menaces dans l'ensemble de l'environnement de l'entreprise
- Capacités fournies dans des mises à niveau de produits couvertes par les contrats de licence en vigueur

Que réserve l'avenir ? (suite)

La consolidation est la clé de la simplicité, d'une gestion efficace, d'une conformité cohérente, d'une expérience utilisateur améliorée et d'une utilisation plus efficace des données internes (journaux) et externes (veille). Symantec Enterprise Cloud, qui offre tous ces avantages, est disponible à un simple tarif annuel par utilisateur couvrant les solutions de sécurité des terminaux, des réseaux, des informations et de la messagerie à l'échelle de l'entreprise.

Illustration 3 : Symantec Enterprise Cloud



Conclusions

Une vision étroite de l'innovation se concentre sur le développement de produits de niche par les startups. Elle favorise les tendances telles que les solutions 100 % cloud disponibles de nos jours. Une vision plus large prend en compte toutes les façons dont les entreprises innovent : par le biais d'acquisitions, en faisant preuve d'un leadership éclairé, en alignant les solutions sur les besoins des clients et en façonnant les environnements commerciaux et réglementaires.

Au cours de son histoire, Symantec est restée à la pointe de toutes ces formes d'innovation en cybersécurité. En tant que division de Broadcom, Symantec continue d'innover dans ses produits, ses modèles commerciaux et ses efforts communautaires au nom de ses clients.

BROADCOM
connecting everything

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

SYM-SI-WP102_FR 20 novembre 2023