FICHE PRODUIT

Symantec® Email Security.cloud

Sécurité complète du courrier électronique pour la génération cloud

EN BREF

- **Protégez-vous efficacement contre les ransomwares, la fraude au président et les nouvelles menaces.**
  Bloquez les nouvelles menaces sophistiquées (ransomwares, spear phishing, fraude au président…) à l'aide de la solution de sécurité du courrier électronique la plus efficace et la plus précise du marché.
- **Mettez en place une défense solide pour vous protéger contre le spear phishing.**
  Protégez votre entreprise contre le spear phishing grâce à un mécanisme de défense robuste offrant plusieurs couches de protection, un isolement à toute épreuve, une visibilité approfondie et une sensibilisation dynamique à la sécurité.
- **Réagissez plus rapidement aux menaces avec la plate-forme Integrated Cyber Defense.**
  Endiguez les attaques et orchestrez une réponse sur les différentes passerelles web et de sécurité des terminaux en résolvant les attaques, en plaçant les menaces sur liste rouge et en corrélant les analyses de sécurité.
- **Garantissez une adoption sécurisée du cloud grâce aux contrôles les plus robustes du marché.**
  Sécurisez complètement Office 365 et G Suite à l'aide des solutions Email Security.cloud, Cloud Access Security Broker (CASB) et Data Loss Prevention de Symantec®.

La sécurité du courrier électronique : un enjeu majeur

Pourquoi le courrier électronique est-il un vecteur de menaces dont il faut se soucier ? Le courrier électronique est un canal très prisé des cybercriminels pour lancer et distribuer des menaces. Selon l'édition 2023 du rapport d'investigations sur les violations de données (DBIR) de Verizon, le courrier électronique est le principal vecteur d'action pour distribuer des ransomwares, et il se classe en deuxième position en ce qui concerne les violations de données et les incidents. Dans l'édition 2022 du rapport sur la cybercriminalité (Internet Crime Report), le FBI explique que la compromission de courriers électroniques professionnels telle que la fraude au président représente 2,7 milliards de dollars de pertes déclarées, soit 26 % de toutes les pertes déclarées attribuables à la cybercriminalité.[1]

À mesure que le nombre de ces attaques augmente, leur niveau de sophistication s'aiguise. Les menaces avancées et de type « Zero Day » sont beaucoup plus difficiles à détecter et à bloquer que les malwares traditionnels, tandis que les outils anti-malware basés sur des signatures se sont révélés largement inefficaces pour les combattre. Les pirates informatiques privilégient désormais le spear phishing (ou harponnage), en particulier sous la forme de fraudes au président. Particulièrement dangereuses et difficiles à saisir, ces attaques ciblées utilisent des méthodes sophistiquées, dont l'usurpation d'adresse IP et l'obfuscation de liens malveillants incorporés dans des messages électroniques.

Dans le même temps, les entreprises font migrer leur messagerie électronique depuis les serveurs sur site vers des systèmes cloud tels que Microsoft Office 365 et Google G Suite. Malheureusement, la sécurité de base intégrée dans ces systèmes n'assure pas une protection suffisante contre les menaces par courrier électronique. Les solutions de sécurité du courrier électronique traditionnelles s'avèrent tout aussi inefficaces. Leurs moyens de défense rudimentaires ne parviennent pas à stopper les nouvelles attaques sophistiquées, tandis que leur conception cloisonnée de la sécurité permet aux menaces avancées de passer entre les mailles du filet. Avec ces deux types de sécurité, les entreprises ne disposent que d'une visibilité limitée et de fonctions analytiques élémentaires, ce qui leur permet difficilement de faire face aux menaces.

Pour compliquer davantage encore la situation, les éditeurs proposent une foule de produits dédiés qui ne traitent qu'une partie du problème de sécurité. Ces produits disparates (pour la sécurité du courrier électronique, la prévention contre les pertes de données, la protection des terminaux, la sécurité sur le Web, etc.) nécessitent de coûteuses intégrations personnalisées ainsi que de gros efforts en termes de gestion. Une fois encore, une défense hétéroclite s'avère perméable. Ajoutez à cela un manque de personnel de sécurité informatique qualifié, et les entreprises se retrouvent face à des défis opérationnels toujours plus importants et à une vulnérabilité accrue.

Enfin, alors que les utilisateurs partagent toujours plus d'informations sensibles par courrier électronique, les entreprises peinent à empêcher l'exposition des données confidentielles. La fuite de données réduit la capacité d'une entreprise à respecter ses obligations légales et en termes de conformité. Outre une dégradation de son image de marque, cela peut donner lieu à des amendes réglementaires et, au final, entraîner des pertes financières.

1. Édition 2022 du rapport annuel sur la cybercriminalité (Internet Crime Report) de l'Internet Crime Complaint Center (IC3), hébergée sur le site web d'IC3 à l'adresse suivante : www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Élimination d'un vecteur de menaces critique

Symantec Email Security.cloud est une solution de sécurité complète qui permet de protéger les systèmes de messagerie cloud tels qu'Office 365, G Suite et sur site (comme Microsoft Exchange). Elle bloque les nouvelles menaces sophistiquées par courrier électronique, telles que les ransomwares, le spear phishing et la fraude au président, grâce à une défense multicouche et aux renseignements émanant du plus grand réseau d'intelligence civile au monde.

Symantec Email Security.cloud repousse les attaques par spear phishing au moyen d'un mécanisme de défense complet alliant diverses techniques : protection, isolement, visibilité, authentification de l'expéditeur et sensibilisation de l'utilisateur. Cette solution permet également de répondre plus rapidement aux attaques grâce à des analyses qui offrent une visibilité approfondie sur les campagnes ciblées. Symantec Information Centric Analytics met en corrélation la messagerie, d'autres flux de sécurité et l'analyse du comportement des utilisateurs pour proposer une vision encore plus approfondie.

Email Security.cloud fait également partie de la plate-forme de cyberdéfense intégrée de Symantec (Symantec Integrated Cyber Defense Platform) qui assure, entre autres, la sécurité sur le Web et les terminaux, l'analyse des menaces, ainsi que l'automatisation et l'orchestration de la sécurité.

Prévention

Symantec Email Security.cloud booste la sécurité intégrée des systèmes de messagerie sur site et dans le cloud en repoussant un maximum d'attaques par courrier électronique et de malwares avec un minimum de faux positifs. Cette solution basée sur le cloud repousse les attaques par courrier électronique sophistiquées, telles que les ransomwares, le spear phishing et les fraudes au président, grâce à plusieurs technologies de détection avancées et aux données télémétriques du Symantec Global Intelligence Network. Elle améliore également la productivité de l'utilisateur en bloquant le spam et les autres messages indésirables, comme les bulletins d'informations et les courriers marketing.

Prévention contre les menaces émergentes

- **Sandboxing** bloque les attaques ciblées et avancées en exécutant les fichiers inconnus dans des environnements physiques et virtuels. Cela permet de repérer les menaces qui ne présentent pas de comportement suspect dans les environnements virtuels. Le bac à sable Symantec imite le comportement humain pour mettre au jour les attaques dont le caractère malveillant n'apparaît qu'en présence d'humains. De plus, notre bac à sable utilise l'apprentissage automatique pour détecter les menaces furtives et persistantes en analysant le code à la recherche de caractéristiques suspectes. Il a également recours à l'analyse du trafic réseau pour identifier les malwares qui appellent des serveurs de commande et de contrôle.
- L'**analyse du comportement** bloque les nouveaux ransomwares cachés en examinant toutes les caractéristiques de courrier électronique, dont le comportement de remise, les attributs du message, les pièces jointes et les techniques d'ingénierie sociale. Elle bloque également les nouvelles variantes de ransomware en déterminant si un courrier contient du code malveillant recyclé. Enfin, elle utilise des techniques de décomposition de fichiers pour détecter et extraire les ransomwares qui se cachent dans des pièces jointes.

Illustration 1 : La protection la plus complète du marché

Défense contre le phishing

- La **protection des liens** examine et évalue les liens en temps réel avant la remise du courrier électronique et, une nouvelle fois, au moment du clic, contrairement aux solutions de sécurité traditionnelles qui reposent sur des signatures et des listes rouges réactives pour bloquer uniquement les liens de harponnage connus. Cette fonction suit les liens jusqu'à leur destination finale, même si les pirates tentent de contourner la détection au moyen de techniques sophistiquées. Par ailleurs, il est d'usage que les cybercriminels réutilisent du code dans leurs nouvelles attaques. C'est pourquoi nous utilisons une détection avancée des variantes de phishing (ou hameçonnage) pour repérer et bloquer les attaques par spear phishing qui présentent des similitudes avec les attaques par de phishing connues.
- Les **contrôles d'emprunt d'identité** fournissent une protection absolue contre les fraudes au président et autres attaques par usurpation. Cela passe par l'utilisation d'un moteur d'emprunt d'identité sophistiqué qui bloque les menaces qui usurpent l'identité d'un utilisateur bien précis ou se font passer pour un domaine de messagerie légitime de votre entreprise.
- L'**isolement des menaces** ouvre les liens de site web inconnus ou potentiellement dangereux en lecture seule afin de mettre les utilisateurs à l'abri des attaques par phishing.
- La **protection contre la fraude** automatise l'authentification des expéditeurs en veillant à ce que l'identité de votre domaine ne puisse pas être usurpée, éliminant ainsi les risques de fraude pour les destinataires internes et externes.

Protection contre les malwares et contre le spam

- La **défense contre les malwares et contre le spam** bloque le spam et les malwares en inspectant les liens et les pièces jointes au moyen de technologies telles que l'analyse de la réputation, des moteurs antivirus et des signatures antispam.
- La **protection au niveau de la connexion** réduit les risques d'attaques de spam et de malware en ralentissant et en coupant les connexions SMTP « anormales ».
- L'**isolement des menaces** empêche les ransomwares et autres malwares d'infecter les utilisateurs en isolant les pièces jointes suspectes. Cette technologie isole également les liens de courrier électronique inconnus ou potentiellement dangereux qui hébergent des malwares, et protègent ainsi les utilisateurs et appareils contre les virus contenus dans les fichiers téléchargés.

Symantec Global Intelligence Network

Les **renseignements sur les menaces** émanant du plus vaste réseau civil au monde permettent d'avoir une vision globale de l'état des menaces et garantissent de meilleurs résultats en matière de sécurité. Pour cela, le réseau GIN utilise les données télémétriques fournies par 175 millions de terminaux, 80 millions d'utilisateurs proxy web et 57 millions de détecteurs d'attaques répartis dans 157 pays, et analyse quotidiennement 8 milliards de menaces.

Isolement

Symantec Email Threat Isolation protège les utilisateurs contre les attaques par courrier électronique avancées telles que le spear phishing, le vol d'informations d'authentification et les ransomwares en isolant les pièces jointes et les liens suspects. Dans le même temps, cette fonction bloque le vol d'informations d'authentification en effectuant un rendu sécurisé des pages web à risque. Email Threat Isolation fait passer la prévention au niveau supérieur en créant un environnement d'exécution cloisonné entre les utilisateurs et les liens envoyés par courrier électronique, en effectuant un rendu des liens suspects à distance et en ne présentant aux utilisateurs que le contenu web inoculé, tout en analysant les téléchargements potentiellement infectés avant la remise du courrier. De ce fait, les attaques censées être menées par le biais de liens malveillants sont purement et simplement neutralisées.

Symantec Email Threat Isolation bloque également les attaques de phishing des informations d'authentification. Lorsqu'un lien ouvre un site suspecté de phishing, ce dernier est affiché en lecture seule, ce qui empêche les utilisateurs de saisir des informations sensibles, telles que des mots de passe professionnels.

Dans le cas des attaques sophistiquées qui utilisent des pièces jointes pointant vers des ransomwares et autres malwares, les pièces jointes sont mises à l'écart pour empêcher toute infection virale. En cas de détection d'une pièce jointe potentiellement dangereuse, les fonctionnalités d'isolement des menaces par courrier électronique effectuent le rendu de ces documents dans un environnement distant sécurisé, ce qui crée un *air gap* virtuel entre les fichiers et les appareils des utilisateurs. Par conséquent, les ransomwares et les autres attaques avancées qui dissimulent des malwares dans des pièces jointes ne peuvent pas infecter les utilisateurs.

- Protection contre les attaques par spear phishing en isolant les téléchargements et les liens malveillants
- Prévention du vol d'informations d'authentification en effectuant un rendu des pages web en lecture seule
- Isolement des pièces jointes suspectes pour empêcher les ransomwares et autres malwares d'infecter les utilisateurs

Réponse aux attaques

Symantec Email Security.cloud permet de répondre plus rapidement aux attaques grâce à des données analytiques qui confèrent une visibilité totale sur les campagnes d'attaques ciblées et sophistiquées. Vous disposez ainsi d'informations portant à la fois sur les courriers sûrs et malveillants, mais aussi d'un nombre d'indicateurs de compromission (plus de 60 points de données comprenant des URL, des hachages de fichier et des informations sur les attaques ciblées) plus élevé que n'importe quel autre éditeur. Ces données peuvent être transmises à votre centre des opérations de sécurité au moyen d'une intégration API dans des systèmes SIEM (Security Information and Event Management) tiers, Symantec Information Centric Analytics ou Symantec Integrated Cyber Defense Exchange.

Réponse aux attaques (suite)

Cela vous permet de traquer les menaces au sein de votre environnement, et de déterminer rapidement la gravité et la portée d'une attaque. Utilisée parallèlement à Symantec Endpoint Detection and Response (EDR) et à la gamme Secure Web Gateway pour détecter les menaces avancées, cette solution vous permet de corréler automatiquement les événements sur tous les points de contrôle. Vous pouvez ensuite neutraliser les menaces et orchestrer une réponse en contenant les attaques et les plaçant sur une liste rouge à l'échelle de votre environnement de sécurité.

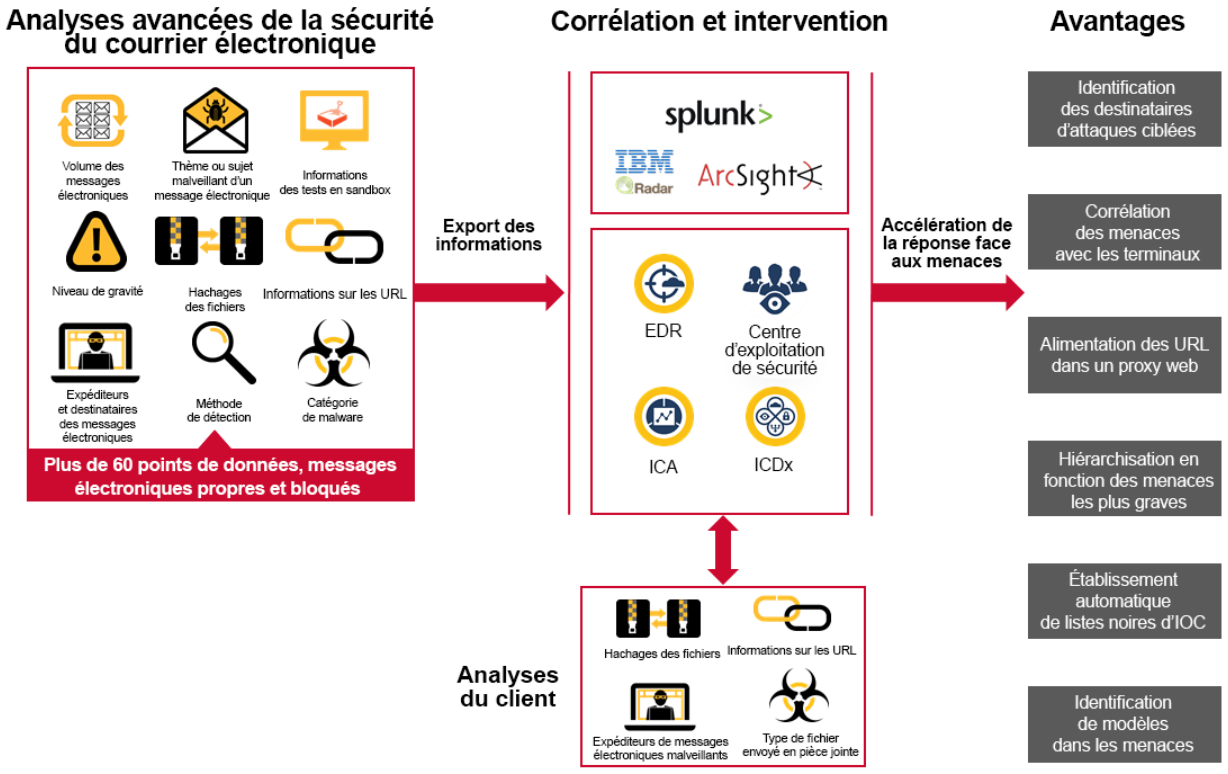
- Réponse plus rapide aux attaques
- Traque des menaces à l'échelle de l'environnement
- Neutralisation des menaces et organisation de la réponse

Préparation

La solution Symantec Email Security.cloud s'accompagne de puissants outils de formation et de sensibilisation à la sécurité qui réduisent les risques pour l'entreprise. Ainsi, elle prépare les utilisateurs à identifier les attaques par phishing et aide les entreprises à considérer comme prioritaire la protection des utilisateurs les plus vulnérables. Vous pouvez évaluer l'état de préparation des employés au moyen d'enquêtes de sécurité qui imitent des menaces réelles qu'il est possible de personnaliser facilement pour répondre aux besoins de votre entreprise. Les tableaux de bord de haut niveau et les rapports détaillés ouvrent une fenêtre sur le comportement des utilisateurs et permettent ainsi d'évaluer le niveau de sensibilisation à la sécurité au sein de votre entreprise. Quant aux évaluations répétées, elles permettent de dégager des tendances en comparant les résultats à ceux obtenus lors de cycles précédents. Les administrateurs peuvent même élaborer des profils de risque et donner la priorité aux utilisateurs à risque en combinant ces informations aux analyses de sécurité des courriers électroniques de Symantec ou en corrélant le comportement des utilisateurs à l'aide d'Information Centric Analytics. Pour sensibiliser les employés à la problématique de la sécurité, et les préparer à identifier et signaler les attaques par courrier électronique les plus récentes, Symantec Email Security.cloud leur envoie des notifications de formation.

- Évaluer l'état de préparation des employés au moyen de simulations réelles
- Effectuer le suivi de la progression grâce à des évaluations répétées et à des rapports détaillés
- Apprendre aux utilisateurs à identifier les attaques par courrier électronique

Illustration 2 : Une visibilité totale sur les attaques sophistiquées par courrier électronique



Intégration

Simplifiez votre pile de sécurité et augmentez votre retour sur investissement en intégrant la sécurité du courrier électronique dans votre infrastructure de sécurité globale. Cela inclut des contrôles de chiffrement et DLP, ainsi que la sécurité du cloud, du réseau et des terminaux.

Symantec Email Security.cloud empêche les fuites de données, et permet de respecter les exigences en termes de confidentialité et de conformité grâce à des contrôles de chiffrement basés sur les politiques et à des contrôles DLP intégrés. Les politiques DLP flexibles identifient et contrôlent les courriers sensibles à l'aide d'une centaine de listes prédéfinies de dictionnaires de mots-clés, d'expressions régulières et de listes de types MIME. Les contrôles de chiffrement basés sur les politiques assurent la confidentialité des courriers électroniques en les chiffrant automatiquement au moyen d'un PDF protégé par mot de passe, ce qui garantit une expérience de chiffrement de type « push » adaptée aux appareils mobiles.

La solution Email Security.cloud fait partie de la plate-forme Integrated Cyber Defense Platform de Symantec. Elle bénéficie ainsi d'un renforcement de ses contrôles DLP intégrés via l'intégration de Symantec Data Loss Prevention, un produit qui empêche la perte de données dans tout votre environnement (systèmes de stockage, courrier électronique, terminaux, réseau, cloud, appareils mobiles, etc.). Vous pouvez en outre répondre à des besoins de chiffrement bien précis et bénéficier d'une personnalisation accrue grâce à Symantec Policy-Based Encryption Advanced, un service additionnel basé sur le cloud.

Symantec Email Security.cloud s'intègre également dans d'autres produits Symantec afin de protéger les terminaux, les applications web et les applications de messagerie, et de renforcer ainsi votre stratégie de sécurité globale. Vous pouvez l'utiliser parallèlement à Symantec Endpoint Security pour répondre plus rapidement aux nouvelles menaces. Par exemple, les renseignements recueillis à la suite d'attaques ciblant le canal de courrier électronique peuvent être transmis sous la forme de listes rouges à l'ensemble des terminaux, et empêcher ainsi que tout votre environnement soit infecté. La protection est ainsi étendue aux applications de productivité et de messagerie les plus récentes (tant dans le cloud que sur site) telles que Slack, Salesforce et Box.

Modules additionnels pour Symantec Email Security.cloud

Les modules additionnels suivants renforcent le niveau de protection offert par la solution Symantec Email Security. cloud de base :

- **Email Threat Detection Response and Isolation :** ce module additionnel assure une protection contre les menaces avancées, tout en permettant d'analyser en détail les campagnes d'attaques cibles et d'y répondre rapidement. Il s'accompagne également d'outils de formation et de sensibilisation à la sécurité Phishing Readiness. La fonction d'isolement vous permet d'ouvrir les pièces jointes et les liens dans un conteneur isolé, et d'interagir ainsi avec des fichiers, des téléchargements et des sites web potentiellement dangereux, tout en bloquant les attaques de malwares et par phishing.
- **Email Fraud Protection :** ce module additionnel simplifie et automatise le processus d'authentification des expéditeurs, ainsi que sa gestion, afin de prendre en charge diverses normes (comme DMARC, DKIM et SPF).

Une efficacité opérationnelle élevée pour un faible coût total de possession

Symantec Email Security.cloud est une solution facile à déployer et simple d'emploi qui évolue au même rythme que le volume de messagerie. Grande efficacité, haut niveau de précision, contrats de service robustes, plate-forme Integrated Cyber Defense Platform de Symantec… Vous avez toutes les cartes en main pour réduire la complexité opérationnelle de votre entreprise, diminuer le coût total de possession et bénéficier d'une protection inégalée contre toutes les attaques par courrier électronique, même les plus sophistiquées.

BROADCOM®
connecting everything®

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

SED-email-security-cloud-PB101_FR 30 novembre 2023