Symantec® Encryption

Chiffrement du courrier électronique

Présentation

Vecteur de collaboration efficace entre les membres du personnel, le courrier électronique reste un canal de communication essentiel pour les entreprises. Cependant, il est tout aussi essentiel de reconnaître que l'humain est la première source de vulnérabilité du système. Lorsqu'un collaborateur de l'entreprise envoie par inadvertance un fichier contenant des données sensibles, les conséquences peuvent être désastreuses. C'est pourquoi l'entreprise doit s'assurer que ses utilisateurs mettent effectivement en œuvre des mesures afin de préserver les informations critiques qu'ils transmettent par courrier électronique, qu'il s'agisse de dossiers médicaux, de données financières ou encore de documents stratégiques.

D'après une étude récente du Ponemon Institute, 60 % des entreprises ont subi des pertes de données ou des transferts de données non autorisés à la suite d'erreurs commises par des collaborateurs dans le cadre de leur utilisation du courrier électronique au cours de l'année passée. Il est impératif pour le département IT de préserver la sécurité des données sensibles de l'entreprise, que ce soit lors des opérations de transfert, de consultation ou d'utilisation.

Le portefeuille Symantec® Encryption constitue une solution robuste qui vous aide à relever ce défi d'envergure. Notre technologie de chiffrement assure la protection des données sensibles tout au long de leur cycle de vie, lors de leur transfert comme de leur stockage, même dans des systèmes de messagerie basés sur le cloud. Le portefeuille Symantec Encryption protège vos informations de valeur contre les risques de violations et d'utilisation frauduleuse.

Présentation de Symantec Encryption

La variété des solutions incluses dans le portefeuille Symantec Encryption vous permet de disposer de fonctionnalités polyvalentes de protection des données, allant de la sécurité des terminaux au chiffrement du courrier électronique en passant par celui des fichiers et dossiers. Notre portefeuille propose également des fonctionnalités robustes de gestion des clés de sécurité individuelles et de groupe, d'automatisation des contrôles de politiques et de reporting sur la conformité. Le présent document met en avant les fonctionnalités de nos solutions de chiffrement du courrier électronique.

Avantages d'Email Encryption

Prévenir les fuites de données accidentelles

Permettre une collaboration métier sécurisée

Assurer la conformité en termes de confidentialité des données

Les avantages du chiffrement du courrier électronique

Prévenir les fuites de données accidentelles

Symantec Desktop Email Encryption automatise le chiffrement, le déchiffrement, la signature numérique et la vérification des messages, en conformité avec des politiques individuelles ou gérées de façon centralisée. Le processus de chiffrement s'exécute au niveau du client, ce qui permet de garantir que les communications sont sécurisées avant de traverser le réseau interne ou d'être stockées dans des référentiels cloud.

Une solution alternative, Symantec Gateway Email Encryption, permet le chiffrement des messages sur la base de règles hautement personnalisables, et élimine ainsi le besoin de déployer un logiciel côté client. En associant Gateway Email Encryption et Symantec Messaging Gateway, les utilisateurs peuvent exploiter la synergie du chiffrement PGP® et de la solution antivirus, antimalware et de filtrage des spams de Symantec de premier plan. L'intégration des deux solutions permet d'étendre la sécurité des communications électroniques pour les protéger des menaces extérieures.

Permettre une collaboration métier sécurisée

Symantec Gateway Email Encryption facilite l'échange sécurisé de données sensibles en dehors de l'entreprise, éliminant la nécessité d'installer un logiciel ou d'échanger des clés de chiffrement. Cet échange sécurisé est rendu possible par une fonctionnalité appelée Web Email Protection, qui fournit une boîte de réception web sécurisée hébergée sur le serveur passerelle. Les utilisateurs peuvent transmettre des contenus sécurisés à leurs destinataires même s'ils ne disposent pas d'un logiciel PGP. Des copies des messages correspondants sont stockées de façon sécurisée, au format PDF, sur le serveur passerelle. Les destinataires externes peuvent s'inscrire dans la solution pour obtenir l'accès aux messages et les consulter dans des navigateurs Internet courants comme Chrome ou Firefox.

Assurer la conformité en termes de confidentialité des données

À une époque où les répercussions de fuites de données véhiculées par le courrier électronique, que ce soit de façon délibérée ou accidentelle, sont de plus en plus médiatisées, les organismes de régulation et d'audit incitent les entreprises à surveiller et renforcer la sécurité des communications électroniques impliquant des données sensibles. En plus de protéger les communications électroniques, la solution Symantec Email Encryption intègre un module cryptographique compatible avec la norme FIPS 140-2. Ce module aide les entreprises à se mettre en conformité avec un large éventail d'obligations gouvernementales et industrielles, parmi lesquelles les normes CDM, PCI DSS, HIPAA et le RGPD.

L'intégration de Symantec Data Loss Prevention avec les solutions de chiffrement du courrier électronique Symantec offre aux entreprises une couche supplémentaire de sécurité, conforme aux réglementations en matière de confidentialité des données. Tout message électronique sortant est analysé sur la base des politiques de DLP. S'il contient des données sensibles, il peut être réacheminé vers Symantec Gateway Email Encryption avant transmission. Cette intégration stratégique fournit aussi une piste d'audit exhaustive précieuse pour l'audit de conformité.

Pourquoi Symantec Encryption

- **Options de distribution flexibles** – Gestion centralisée des clés et des politiques par utilisateur ou par groupe depuis une console web unique, et synchronisation avec Active Directory.
- **Interopérabilité** – Intégration transparente avec les solutions de chiffrement du courrier électronique standard existantes telles que OpenPGP et S/MIME ; prise en charge des protocoles POP, IMAP, MAPI et SMTP ; compatibilité garantie avec les plates-formes Microsoft Windows et macOS.
- **Portefeuille étendu** – Le portefeuille de solutions de chiffrement le plus complet du marché. Étendez la protection à vos autres canaux de communication avec des solutions de sécurité des terminaux et de chiffrement de fichiers et de dossiers.

EMA-ENC-OT100_FR 26 septembre 2023