

# Une sécurité complète du courrier électronique au plus haut niveau

Une sécurité complète du courrier électronique doit offrir plus qu'un simple anti-spam et un antivirus. Le Secure E-Mail Gateway (SEG) FortiMail combine la prévention des menaces et la protection des données à la pointe de la technologie. La solution FortiMail s'intègre parfaitement à Office 365 et est disponible en différentes versions (physique, virtuelle ou en tant que service SaaS depuis FortiCloud).

La sécurité des e-mails est essentielle dans les entreprises de toutes tailles, car les courriers électroniques sont le vecteur d'attaque le plus utilisé par les cybercriminels. Selon le «2019 Data Breach Investigations Report» de Verizon, 32% des fuites de données sont liées au phishing et pas moins de 94% des malwares pénètrent dans le réseau de l'entreprise par courrier électronique. Cela s'applique aussi bien aux attaques générales qu'aux attaques ciblées sur des collaborateurs individuels.

La sécurité et la fiabilité des communications par e-mail sont aujourd'hui essentielles pour les entreprises. Il est donc important de s'assurer que la négligence d'une seule personne ne paralyse pas toute une entreprise. Compte tenu des méthodes d'attaque de plus en plus sophistiquées, un système de sécurité des e-mails basé uniquement sur la détection des malwares par signature et l'anti-spam classique ne suffit plus. Les services de courrier électronique basés sur le cloud sont de plus en plus fréquemment utilisés – par exemple: Office 365 ou le service G-Suite de Google. Selon les études de marché de Gartner, environ 70% des entreprises s'appuieront sur de telles offres d'ici 2021. Une solution de sécurité des e-mails doit donc également pouvoir interagir avec les solutions bureautiques cloud.

## Une excellente sécurité des e-mails pour votre entreprise

La solution de sécurité du courrier électronique FortiMail de Fortinet comprend d'une part les fonctions de sécurité classiques de l'anti-malware et de l'anti-spam, d'autre part les fonctions de pro-



Le Secure E-Mail Gateway (SEG) de Fortinet est synonyme de la plus haute sécurité du courrier électronique.

tection des données telles que le cryptage du courrier électronique basé sur l'identité, l'archivage et la protection contre la perte de données (DLP). En outre, plusieurs technologies avancées de prévention des menaces sont incluses. Dans leur ensemble, ces fonctionnalités garantissent le plus haut niveau de sécurité pour le trafic de courrier électronique.

Une prévention efficace des menaces commence par la détection des usurpations d'identités (Impersonation and Cousin Domain Detection). Il s'agit d'e-mails supposés provenir d'un expéditeur connu, souvent utilisé pour des attaques ciblées. Le Sandboxing, souvent intégré comme un service cloud, vérifie les pièces jointes et les liens suspects dans un environnement virtuel fermé et empêche la distribution au destinataire en cas de comportement malveillant. La fonction Virus Outbreak Protection réduit encore plus le risque d'infection causé par les cycles de mises à jour des signatures différés. Dans le monde entier, des senseurs traitent des millions

de requêtes par minute sur les e-mails/URL et les pièces jointes – bonnes et mauvaises, connues et inconnues. Fortinet utilise le Machine Learning et l'intelligence artificielle pour identifier des modèles à partir de requêtes, compare cette information avec celle des partenaires technologiques et crée des listes de réputation de hash de fichiers et d'URL. Cela permet d'identifier rapidement les nouvelles menaces et de contenir ou de prévenir les attaques.

Le Content Disarm & Reconstruction est une autre fonction importante de sécurité: tout le code actif, tel que les macros Office, est supprimé des e-mails/pièces jointes reçus sur la base de règles. L'utilisateur reçoit une version nettoyée des documents qu'il peut consulter et modifier en toute sécurité. Click Protect offre une protection supplémentaire: lors de la lecture d'un courriel, les liens contenus dans l'e-mail sont vérifiés en temps réel par une analyse de réputation et bloqués en cas de destination douteuse.

Fortinet propose la solution FortiMail dans différents formats: des machines physiques et virtuelles sont disponibles pour être déployées dans un cloud privé ou public. Troisième option, la solution FortiMail Cloud, un service SaaS idéal pour les PME grâce à un modèle de licence attrayant et à des coûts fixes par utilisateur et par mois.

## Bonne cohabitation avec Office 365

Dans la nouvelle version 6.4, FortiMail est parfaitement compatible avec Office 365. FortiMail utilise l'API native d'Exchange Online pour l'intégration et peut être implémenté off-path. De cette façon, les e-mails nuisibles déjà délivrés peuvent être supprimés de la boîte de réception (Post-Delivery Clawback).

## FortiMail: les points clés

- Excellente détection anti-spam et anti-phishing
- Certifié par des laboratoires d'essai indépendants (SE Labs, ICASA, NSS Labs, Virus Bulletin)
- Protection étendue contre les attaques ciblées
- Intégration Office 365 grâce à des APIs
- Disponible en différentes variantes (physique, virtuelle ou service SaaS)

**BOLL**  
IT Security Distribution

**BOLL Engineering SA**

En Budron H15  
1052 Le Mont-sur-Lausanne  
Tél. 021 533 01 60  
vente@boll.ch | www.boll.ch