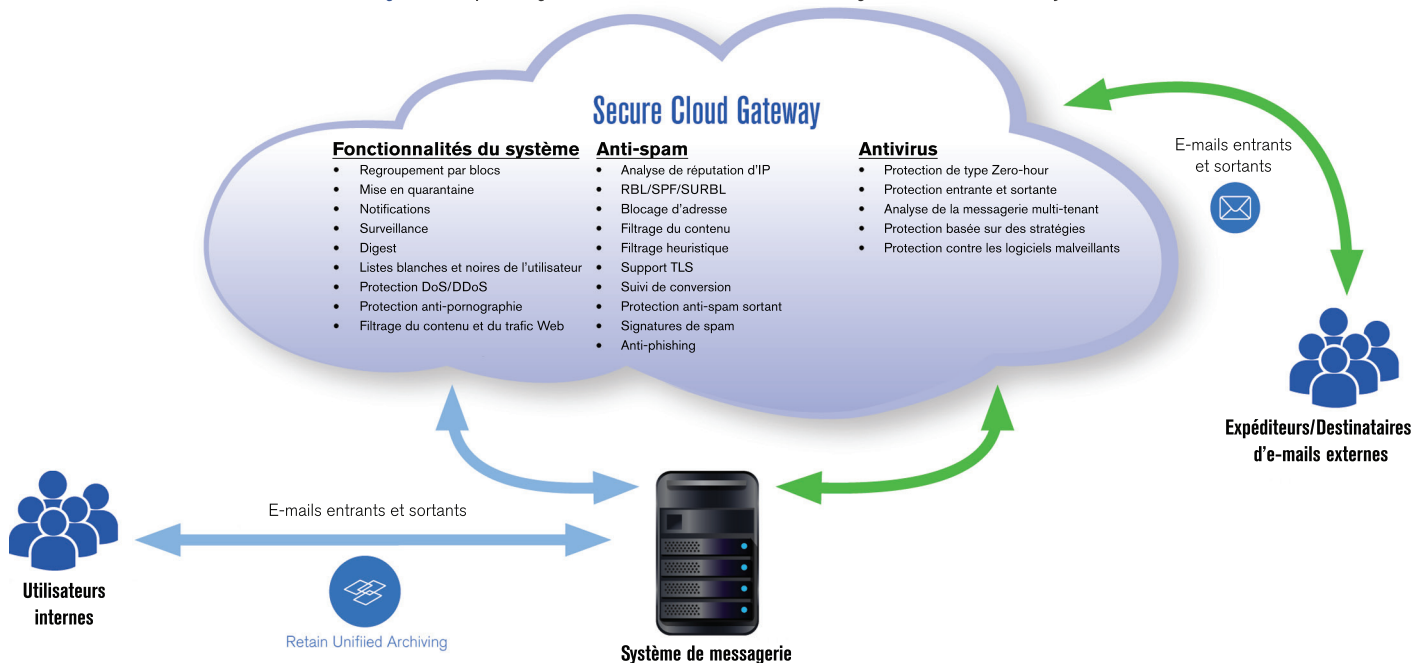


Micro Focus Secure Cloud Gateway

La solution Micro Focus® Secure Cloud Gateway offre une protection antivirus et anti-spam de type Zero-hour basée sur des signatures dans le cloud. Cette solution utilise les technologies les plus récentes afin de garantir que votre système de messagerie et votre réseau sont exempts de virus, de logiciels malveillants et de spams. Elle surveille également le trafic réseau afin de bloquer les images pornographiques et l'accès à du contenu ou des sites Web malveillants, et offre une protection contre la cybercriminalité et les attaques de service distribué (DoS/DDoS).

Traitement des messages : un simple changement de DNS insère la sécurité de messagerie Secure Cloud Gateway dans le flux SMTP



Points forts du produit

Micro Focus protège les réseaux professionnels et les données de communication pour des milliers d'organisations à travers le monde, notamment dans les secteurs de l'éducation, du gouvernement, des services financiers, de la santé et des affaires.

Fonctionnalités du produit

Support multi-système : la solution Micro Focus Secure Cloud Gateway peut filtrer la messagerie dans le cadre de n'importe quel système de collaboration ou de messagerie normalisé basé sur Internet. Cela comprend des plates-formes telles que Microsoft Exchange,

Office 365, Gmail, Micro Focus GroupWise®, Vibe, Lync ou Lotus Domino.

Administration des utilisateurs basée sur les rôles : octroyez l'accès aux utilisateurs en fonction de rôles spécifiques, directement dans Secure Cloud Gateway. La nouvelle liste

de contrôle d'accès vous permet de gérer l'accès des utilisateurs aux fonctionnalités et fonctions de Secure Cloud Gateway en fonction des rôles que vous avez définis. Les utilisateurs désignés peuvent désormais accéder à certaines fonctionnalités d'administration sans disposer de tous les droits d'administration.

Conception évolutive : lorsque votre système approche la capacité maximale ou est sous pression, vous pouvez ajouter de nouvelles ressources (serveurs supplémentaires Secure Cloud Gateway) afin d'équilibrer la charge sur votre système Micro Focus.

Configuration tolérante aux pannes : la solution Secure Cloud Gateway peut être installée sur plusieurs serveurs. Cela permet à votre système de continuer à fonctionner même en cas de panne d'un ou de plusieurs serveurs.

Notifications personnalisables, ad-hoc, faciles à configurer : créez les notifications spécifiques dont vous avez besoin. Les types de notification que vous pouvez créer sont presque illimités. Ces notifications peuvent être déclenchées par des mots-clés, des pièces jointes, du contenu, des images illicites, des virus, des spams ou d'autres catégories. De plus, toutes les notifications peuvent être localisées, ce qui vous permet de fournir des versions localisées de tous les e-mails générés par Micro Focus.

Protection antivirus

Protection Zero-hour : la solution Secure Cloud Gateway fournit la meilleure protection antivirus de type Zero-hour disponible, tant pour le trafic entrant que sortant. Les virus sont arrêtés avant qu'une menace ne se déclare, ce qui économise des milliers de dollars en perte de temps et de données.

Protection entrante et sortante : les virus et les logiciels malveillants sont des menaces qui peuvent pénétrer votre réseau à partir de nombreux points d'entrée. Grâce à l'analyse du trafic entrant et sortant, Secure Cloud Gateway fournit une protection unique en garantissant que les menaces et les dommages sont réduits au minimum.

Configuration multi-tenant basée sur les stratégies : Micro Focus vous permet de créer

et de configurer des stratégies de message individuel basées sur les informations de distribution de chaque message. Utilisez des critères tels que le destinataire, l'adresse source et la direction pour créer plusieurs stratégies pour les e-mails entrants et sortants, pour chaque utilisateur, chaque domaine ou plusieurs ensembles d'utilisateurs. Secure Cloud Gateway prend également en charge l'analyse complète de la messagerie multi-tenant via des passerelles de messagerie uniques. Grâce au contrôle basé sur les stratégies, les partenaires et les fournisseurs de services peuvent utiliser Secure Gateway en tant que solution hébergée.

Analyse antivirus : la solution Secure Cloud Gateway recherche des virus dans l'objet, le corps et les pièces jointes d'un email. Si la pièce jointe contient un virus, l'e-mail est arrêté au niveau de la passerelle. De plus, si le corps ou l'objet de l'e-mail contient un lien malveillant ou un virus, l'e-mail est bloqué.

Analyse multi-thread hautes performances : activez l'analyse de messagerie hautes performances via le threading des processus d'analyse de manière asynchrone sur toutes les ressources disponibles du serveur.

Correspondance des modèles : la solution Secure Cloud Gateway prend en charge les expressions régulières normalisées pour la mise en correspondance des modèles. En outre, Micro Focus vous permet d'appliquer des modèles et d'analyser l'ensemble du domaine. Par exemple, *companydomain.com (domainesociété.com) sera appliqué à toutes les adresses électroniques utilisant ce domaine, afin de rechercher des modèles dans le contenu des e-mails.

Protection anti-spam

Protection multicouche : la solution Secure Cloud Gateway assure une protection multicouche contre les spams pour protéger les e-mails et maintenir le trafic indésirable à l'écart de votre système de collaboration.

Analyse de défense périmétrique : l'unité logicielle Secure Cloud Gateway détecte les spams au sein du périmètre avant qu'ils n'atteignent votre système de messagerie. Les fonctions anti-spam comprennent le blocage

d'adresse, le filtrage de contenu, le filtrage heuristique, la technologie SURBL, l'analyse de réputation d'IP, le suivi de conversion et le support TLS. L'élimination du spam assure que Micro Focus fonctionne correctement et efficacement.

Réduction de faux positifs : le moteur anti-spam est constamment mis à jour avec de nouvelles signatures de spam. Cette technologie innovante garantit la détection des faux positifs. Les e-mails dont vous avez besoin se retrouvent dans votre boîte de réception et seul le spam est filtré.

Filtrage du contenu robuste : la solution Secure Cloud Gateway filtre le contenu des e-mails en fonction des critères suivants : adresse électronique, objet, en-tête, corps, contenu MIME brut, empreintes, fichiers joints, noms des fichiers joints, images (via Image Analyzer), listes blanches et noires, taille du message et adresse IP.

Contrôle de filtrage directionnel : Micro Focus vous permet de créer des filtres basés sur la direction des messages (entrants ou sortants). Appliquez des filtres différents au trafic entrant et au trafic sortant.

Filtrage d'enveloppe : la solution Secure Cloud Gateway vous permet d'effectuer un filtrage basé sur l'authentification des utilisateurs. Si un utilisateur est authentifié dans le système et qu'il envoie un message électronique, la solution peut gérer le message d'une façon spécifique. Par exemple, Secure Cloud Gateway peut bloquer les messages envoyés par un utilisateur qui n'est pas authentifié.

Protection anti-spam sortant : les postes de travail des utilisateurs peuvent être menacés par des virus qui pénètrent les défenses périmétriques. Ces postes de travail peuvent alors transférer le spam via votre réseau en transformant votre système en une source de milliers de spams sortants. La solution Secure Cloud Gateway permet d'éviter les risques de spam sortant tels qu'une adresse IP bloquée, une réputation compromise, une perte de ressources et des systèmes de messagerie défaillants.

Anti-simulation via l'analyse SPF : la solution Secure Cloud Gateway propose une fonction d'analyse SPF (Sender Policy Framework) pour arrêter la simulation des e-mails. L'analyse SPF examine le domaine trouvé dans la partie « mail from: » du fichier MIME, puis vérifie les enregistrements SPF du domaine pour s'assurer que le domaine signalé par l'e-mail correspond aux serveurs de messagerie qui envoient ce domaine. L'analyse SPF permet à Secure Cloud Gateway d'identifier les messages qui sont autorisés ou pas à utiliser le nom de domaine dans les commandes SMTP HELO et MAIL FROM, en fonction des informations publiées dans une stratégie d'expéditeur du propriétaire du domaine.

Protection du réseau

Protection contre la cybercriminalité : la cybercriminalité, le cyberterrorisme et les logiciels malveillants représentent de graves menaces pour votre organisation. Micro Focus fournit plusieurs couches de protection spécialisée afin d'empêcher les cybercriminels d'utiliser la messagerie électronique comme moyen d'attaque contre votre infrastructure.

Protection anti-pornographie : Micro Focus Image Analyzer analyse la composition réelle des images et des vidéos pour en garantir la précision. Son moteur de probabilité sophistiqué analyse les images entrantes et sortantes

en faisant la distinction de manière fiable entre le contenu pornographique et non pornographique, puis empêche le contenu inapproprié d'entrer dans votre système de messagerie ou d'en sortir.

Protection DoS ou DDoS : évitez les attaques par déni de service (DoS) et les attaques de service distribué (DDoS) sur le serveur SMTP ; elles risquent d'endommager votre serveur de messagerie. Ces attaques entraînent des défaillances du système ou des interruptions de service, ce qui représente une perte de temps et d'argent pour votre organisation en raison de la baisse de productivité.

Listes blanches et noires de l'utilisateur : responsabilisez les utilisateurs, et réduisez le temps et les coûts d'administration. La solution Secure Cloud Gateway dispose d'une interface permettant aux utilisateurs de signaler des domaines et des adresses électroniques. Les utilisateurs peuvent inscrire des adresses électroniques individuelles ou des domaines entiers sur leur liste noire ou blanche, autorisant ou interdisant ainsi le transfert des messages en fonction de cette liste.

Avantages du cloud

Fonctionnalité de cloud : le support multi-tenant de Micro Focus permet à plusieurs instances indépendantes de ses configurations

d'analyse d'être exécutées sur le même serveur. Cela vous permet de disposer de toutes les fonctionnalités de Secure Cloud Gateway tout en prenant en charge de nombreux clients à partir d'un système. La solution cloud sécurise votre système de messagerie en évitant les coûts supplémentaires, les risques et la complexité propres aux systèmes de sécurité de messagerie sur site. Laissez Micro Focus prendre en charge les coûts de support système, informatique et matériel.

Déploiement rapide : réduisez les coûts d'implémentation en pointant simplement vos serveurs de messagerie vers Secure Cloud Gateway pour devenir opérationnels.

Packages de protection prédéfinis : utilisez les règles prédéfinies de Secure Cloud Gateway pour une protection maximale. De plus, ces règles peuvent être personnalisées afin de répondre à vos besoins spécifiques.

Support exceptionnel : la solution Micro Focus Cloud inclut l'accès à des techniciens certifiés 24 heures sur 24, 7 jours sur 7.

Accès évolutif : utilisez et payez uniquement pour les services dont vous avez besoin. La solution Micro Focus Cloud offre une disponibilité d'utilisation de serveur et de réseau à la demande.

« Lorsque j'indique (hormis aux administrateurs)
la quantité de spams que nous bloquons par mois
grâce à la solution Micro Focus Secure Gateway,
les gens n'en reviennent pas. »

ROY DRAGOTTA
Network Engineer
Long Island Rail Road

www.microfocus.com



Micro Focus
France

+33 (0) 1 55 70 30 13

Micro Focus
Siège social au Royaume-Uni

Royaume-Uni
+44 (0) 1635 565200

www.microfocus.com