

Solutions Proofpoint Messaging Security Gateway



Service hébergé à la demande Proofpoint et logiciel de serveur de protection Proofpoint



Les solutions Proofpoint Messaging Security Gateway™, le service Proofpoint on Demand™ et le logiciel Proofpoint Protection Server® ont pour mission de vous défendre contre les attaques par courriels entrants, de prévenir les fuites de données confidentielles, de chiffrer vos messages et d'analyser l'infrastructure de votre système de messagerie. Leur architecture unifiée, leurs défenses modulaires et leur interface d'administration de politiques de sécurité protègent votre organisation contre tous les types de risques de messagerie, et ce, aux portes mêmes de votre entreprise.

protéger, prévenir, chiffrer et analyser

Pourquoi encore acheter une autre solution ne réalisant qu'une seule fonction? Cette plateforme unifiée de sécurité de messageries et de prévention de pertes de données offre une protection globale à la fois contre les attaques externes et contre les risques auxquels sont exposées les données envoyées, et l'architecture modulaire Proofpoint vous permet de déployer facilement de nouvelles défenses en fonction de l'évolution de vos besoins.

Toutes les fonctions Proofpoint, y compris les fonctions anti-pourriel, antivirus, de sécurité de contenus sous protocoles multiples, de chiffrement fondé sur une politique déterminée et de production de rapports sont gérées de façon centralisée à partir d'une interface graphique d'administration unique et déployées sur une architecture de systèmes unifiée. Chaque fonction peut être déployée dans presque toutes les configurations possibles et imaginables afin de répondre aux besoins spécifiques de votre organisation.

Que votre déploiement implique un unique serveur Proofpoint ou une série de systèmes répartis aux quatre coins du globe, toutes les tâches de gestion de politique et administratives sont contrôlées à partir d'une console d'administration Proofpoint unique, centrale et Internet.

options de déploiement flexibles

Les solutions de sécurité de messageries et de prévention de pertes de données sont proposées sous un éventail de formes différentes qui vous offre une flexibilité de déploiement maximale.

- **Service hébergé** : Proofpoint on Demand offre un ensemble de fonctions de protection de messageries et de prévention de pertes de données Proofpoint sous la forme d'un service économique, hautement personnalisable et à la demande qui ne nécessite aucune installation de matériel ou de logiciels sur votre site.
- **Matériel** : le système Proofpoint Messaging Security Gateway est un appareil à châssis renforcé, sécurisé, d'un déploiement aisé et qui s'installe en quelques minutes. Une gamme de modèles différents est proposée afin de satisfaire toutes les entreprises, quelle que soit leur taille.
- **Systèmes virtuels** : le système Proofpoint Messaging Security Gateway—Virtual Edition offre le même type de protection supérieure que le matériel Proofpoint, mais avec les nombreux avantages offerts par la virtualisation, y compris en termes de réduction de coûts, de déploiement et d'avantage accélérés, de gestion de changements facilitée et de procédures de sauvegarde et de reprise simplifiées. Le système virtuel fonctionne sur n'importe quel ordinateur de bureau x86 ou serveur doté de VMware Server ou VMware Infrastructure.
- **Logiciel** : Proofpoint Protection Server est une plateforme de sécurité de messagerie Proofpoint sous forme logicielle destinée aux systèmes d'exploitation Enterprise Linux de Red Hat.

Sûr. Performant. Facile à déployer.

Voilà quelques-uns des commentaires ou expressions (ce ne sont pas les seuls) couramment utilisés pour décrire la plateforme unifiée de protection de messageries et de prévention de pertes de données Proofpoint. C'est aujourd'hui la solution la plus puissante sur le marché, proposée sous la forme d'un système, d'un outil virtuel ou d'un logiciel conçu spécifiquement pour les entreprises et offrant les atouts suivants :

- Capacité de détection de pourriels et de gestion de connexions imbattable
- Protection de premier rang contre les virus et les épidémies
- Prévention contre les pertes de données et protection de contenus complète et compatible avec de nombreux protocoles
- Chiffrement de courriels en fonction de la politique de l'entreprise
- Fonctions de production de rapports et fonctions analytiques avancées
- Administration unifiée de la politique
- Performance professionnelle
- Déploiement et avitaillement rapides
- Architecture modulaire optimale

« Pacific Sunwear a testé un grand nombre de produits anti-pourriel, antivirus et de scannage de contenu, et Proofpoint est la première entreprise à proposer une plateforme permettant de résoudre tous les problèmes de courriels et de messagerie à l'aide d'une solution unique, facile à déployer et encore plus facile à utiliser. Messaging Security Gateway a complètement rétabli notre système de messagerie, ce qui veut dire qu'il en a fait un canal de communication stratégique pour l'entreprise, et non pas une simple porte pivotante de protection contre les attaques par courriels. »

Ron Ehlers

Vice-président des systèmes d'information
Pacific Sunwear

Proofpoint Messaging Security Gateway et Proofpoint Protection Server

protection intégrale

Technologie MLX Proofpoint

Apprentissage automatique avancé

La puissance des solutions de messagerie d'entreprise Proofpoint résulte de la technologie Proofpoint MLX, un système d'apprentissage automatique avancé dont la demande de brevet est en instance et qui a été développé par les chercheurs du Centre Proofpoint de réponse aux attaques. Basée sur des techniques statistiques avancées, y compris la régression logistique et l'analyse de gains d'informations, la technologie MLX de Proofpoint permet d'effectuer une classification et une identification très précises de contenus non structurés, tels que ceux que l'on trouve couramment dans les courriels et d'autres documents.

Précision sans équivalent

MLX est à la base de la précision anti-pourriel exceptionnelle offerte par le module Proofpoint Spam Detection. Grâce à MLX, Proofpoint analyse des centaines de milliers de contenus structurels, d'images et d'attributs de réputation afin de distinguer avec précision entre le pourriel et les messages authentiques. Les solutions anti-pourriel traditionnelles évaluent uniquement un nombre limité d'attributs et sont incapables de classer le pourriel de manière décisive, ce qui réduit considérablement leur efficacité et entraîne un nombre d'erreurs important.

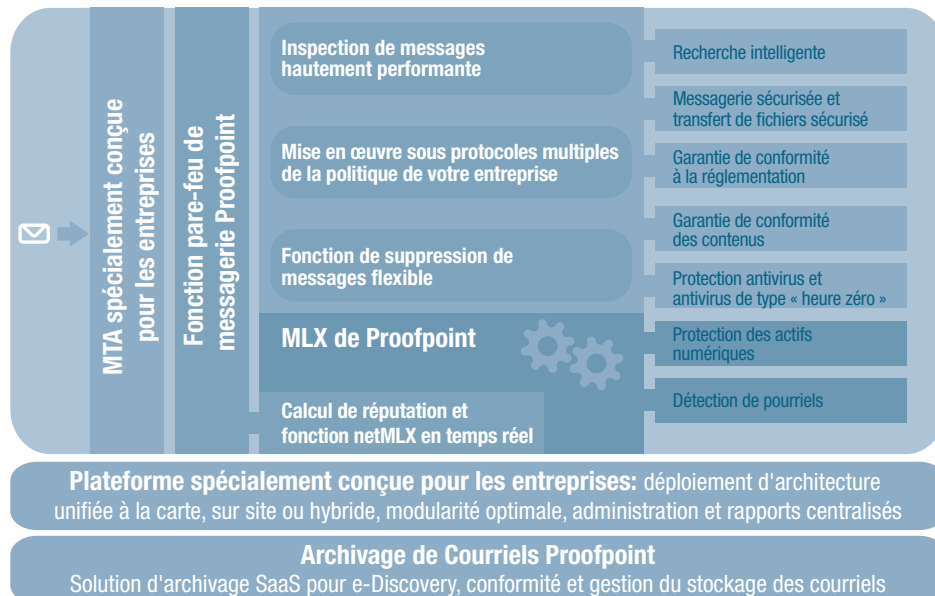
Intelligence à toute épreuve pour le futur

La technologie anti-pourriel intelligente de Proofpoint se maintient en permanence à jour afin de protéger vos systèmes contre les nouvelles formes de pourriel. Un certain nombre de techniques d'apprentissage automatique et de nouvelles techniques mises au point par les chercheurs de Proofpoint permettent à MLX d'anticiper et de s'adapter aux nouvelles formes de pourriel dès leur première apparition. Les mises à jour de MLX sont automatiquement envoyées à tous nos clients plusieurs fois par jour.

Par conséquent, MLX Proofpoint affiche un taux de réussite égal ou supérieur à 99,8 %, même contre les formes de pourriel les plus redoutables, y compris celles sous forme d'images, de fichiers PDF, de pièces jointes, de messages de rétrodiffusion (« backscatter ») et en langues étrangères.

À l'inverse des autres solutions anti-pourriel disponibles sur le marché, la capacité de Proofpoint à vous protéger contre les attaques de pourriel ne diminue pas avec le temps et chaque mise à jour du moteur anti-pourriel de MLX est automatiquement et régulièrement envoyée à votre entreprise. MLX de Proofpoint évolue en permanence afin de contrer toutes les nouvelles menaces, ce qui permet de garantir que l'infrastructure de votre messagerie soit également protégée contre les pourriels qui émergeront à l'avenir.

MLX est par ailleurs le moteur des fonctions de protection de contenu avancées du module Proofpoint Digital Asset Security, ainsi que celui des fonctions de protection de périmètre intelligentes du service Proofpoint Email Firewall and Dynamic Reputation. Proofpoint est le seul développeur à appliquer ces techniques puissantes d'apprentissage automatique à la protection de messageries et la prévention contre les pertes de données.



protection contre les attaques externes

Détection de pourriel avancée et optimisée grâce à Proofpoint MLX™

Optimisé par notre technologie d'apprentissage automatique Proofpoint MLX (brevet en instance), le module **Proofpoint Spam Detection™** examine des centaines de milliers d'attributs au sein de chaque courriel, y compris dans les en-têtes et la structure de l'enveloppe du message, les propriétés des images, les données de réputation de l'expéditeur ainsi que le contenu non structuré figurant dans le corps du message, et ce afin de bloquer la plupart des pourriels, les pourriels à base d'images et les attaques de type « phishing », tout en s'adaptant automatiquement aux nouveaux types d'attaque au fur et à mesure qu'ils apparaissent. Quant à **Proofpoint Dynamic Update Service™**, il actualise automatiquement votre protection anti-pourriel afin de garantir une efficacité maximale en toutes circonstances. Le système de notation de pourriel et de contenu pour adultes, contrôlé individuellement, vous permet de mettre en œuvre une politique de tolérance zéro contre les pourriels à caractère pornographique. Les fonctions anti-phishing bloquent la dissémination de ce type de messages et autres attaques de vol d'identité visant à dérober les informations personnelles de vos employés. Des techniques anti-spam intégrées, y compris « Bounce Address Tag Validation » (BATV), permettant de bloquer la totalité des messages de rétrodiffusion indésirables (messages d'avis de non-livraison).

Proofpoint Spam Detection est une fonction multilingue et offre une précision exceptionnelle contre les pourriels en toutes langues, y compris contre ceux dans des langues à caractères composés d'octets multiples, qui sont plus difficiles à analyser, telles que le japonais et le chinois. Les mesures anti-pourriel peuvent être personnalisées au niveau mondial, au niveau de chaque groupe ou au niveau individuel, avec intégration totale sous LDAP ou Active Directory afin de simplifier l'administration du système au quotidien.

Protection pare-feu intégrée de messageries

Le système **Proofpoint Email Firewall™** représente une première ligne de protection dynamique contre le pourriel et les connexions malignes en testant de nombreux points de données au niveau de la connexion, y compris les DNS, la vérification de fichiers MX, SPF, la vérification du destinataire, les informations de type « Proofpoint Dynamic Reputation » et les données netMLX optionnelles.

Gestion de connexions innovante

Proofpoint Dynamic Reputation™, optimisé par Proofpoint netMLX™, ajoute les fonctions de gestion de connexions les plus puissantes de l'industrie à votre déploiement de la plateforme Proofpoint. Il s'agit du seul service de vérification de réputation de courriels utilisant une combinaison de données locales de comportements prévisibles et de données de réputation internationale analysées par des algorithmes d'apprentissage automatique puissants, ce qui permet de bloquer les tentatives de connexion provenant d'adresses IP malignes.

Proofpoint Messaging Security Gateway et Proofpoint Protection Server

Protection contre les attaques externes (suite)

Chaque déploiement de matériel et de logiciels Proofpoint commence par une analyse intégrée et prédictive du comportement du trafic IPC local qui répond en temps réel, afin d'éliminer les crêtes de trafic de messages causées par des attaques ciblées et de bloquer ou d'asphyxier les connexions malignes émanant de réseaux « botnets » (réseaux zombies).

Nos clients dont les messageries voient transiter des volumes de courriels très élevés peuvent renforcer la protection de leurs systèmes déployés grâce à Proofpoint netMLX, qui permet de réduire le volume de connexions externes de 80 %, voire davantage. Proofpoint netMLX représente la base de données de réputation d'adresses IP envoyant des courriels sur l'Internet la plus précise et la plus actualisée de l'industrie. Chaque minute, des centaines de points de données de toutes les adresses IP sont analysées à l'aide d'algorithmes d'apprentissage automatique avancés, afin de générer une note qui représente la réputation de l'expéditeur. Proofpoint Dynamic Reputation utilise ensuite ces notes, combinées à des données de comportement locales, pour prendre des décisions intelligentes en matière d'acceptation, d'asphyxie ou de rejet de courriels entrants.

Protections contre les virus et antivirus heure-zéro

Grâce à un plusieurs partenariats stratégiques établis avec quelques-uns des plus importants fournisseurs de produits antivirus, **Proofpoint Virus Protection™** offre une fonctionnalité complète de détection de virus par scanage. Les moteurs de détection de virus sont totalement intégrés à la plateforme Proofpoint, permettant ainsi de gérer l'ensemble des mesures de protection contre les virus à partir d'une console centralisée et conviviale dotée de la même interface que celle utilisée pour gérer les pourriels et la détection de contenus. Les messages sont minutieusement scannés afin d'y déceler toute forme de virus, de pourriel et de contenu malin et de protéger les utilisateurs finaux contre les virus, les vers et autres codes malins. De plus, le module **Proofpoint Zero-Hour Anti-Virus™** vous protège contre les virus émergents dès qu'ils commencent à proliférer, ce qui permet de les stopper bien avant que les produits concurrents ne commencent à se mettre au travail.

protection contre les fuites d'information intervenant entre différents protocoles

Les fonctions de protection avancées contre les pertes de données Proofpoint permettent de protéger les courriels sortants et les flux de messages additionnels, y compris les courriels Internet, les affichages de blogs, les affichages de tableaux de messages et autres activités HTTP ou FTP.

Conformité des contenus : permet de mettre facilement en œuvre votre politique en matière d'utilisation acceptable des systèmes

Proofpoint Content Compliance™ facilite l'élaboration et la mise en œuvre de votre politique en matière d'utilisation acceptable concernant le contenu des messages et de leurs pièces jointes. Notre interface conviviale à base de clics simplifie le processus de définition de règles complexes concernant les types de fichiers, la taille des messages et le contenu des messages. Ces fonctions peuvent être utilisées pour identifier et prévenir un large éventail d'infractions liées à des messages entrants ou sortants, y compris en ce qui concerne les contenus désobligeants, le harcèlement, le partage de fichiers et les infractions aux réglementations externes.

Conformité à la réglementation : protection des données privées

De nos jours, les entreprises ont plus que jamais besoin de protéger les données de leurs clients et de leurs personnels. Le module **Proofpoint Regulatory Compliance™** permet de mettre en œuvre les meilleures pratiques connues en matière de protection de données privées et contre les risques potentiels d'amendes ou de poursuites en cas d'infraction à une réglementation ou une autre dans ce domaine, telles que les règles de l'HIPAA (Health Insurance Portability and Accountability Act ; Loi américaine sur la portabilité et la responsabilité des assurances médicales), de la GBLA (Gramm-Leach-Bliley Act ; Loi américaine Gramm-Leach-Bliley), du PCI (Payment Card Industry Security Standards Council ; Conseil des normes de sécurité de l'industrie des cartes de paiement), de la SEC (Securities and Exchange Commission ; Autorité des marchés financiers américains) et autres. Le module utilise des règles personnalisables, des dictionnaires gérés et des « identifiants intelligents » (smart identifiers) pour scanner automatiquement les messages à la recherche de toute information non-publique, telles que des données médicales ou financières personnelles, et pour rejeter ou chiffrer les messages inappropriés.

Ces identifiants intelligents sont bien plus sophistiqués que de simples expressions ordinaires. En effet, ils sont capables de déterminer si le nombre de chiffres ou de caractères est correct, mais également d'exécuter des algorithmes complexes qui permettent d'atteindre un très haut niveau de précision en matière de détection, tout en minimisant les erreurs de détection positive.

Protection de données numériques : documents confidentiels

Le courriel, les messageries Internet et autres systèmes de messagerie sont devenus les outils de communication les plus importants de nos jours, mais ils sont également devenus des systèmes exposant au grand jour des informations confidentielles. Le module Proofpoint Digital Asset Security™ permet de protéger les actifs les plus précieux et les données confidentielles de votre entreprise contre une quelconque fuite par le biais de courriels et autres protocoles de messagerie. La technologie puissante d'apprentissage automatique MLX analyse et trie vos documents confidentiels et continue de les surveiller (ou à en surveiller certaines parties) afin de déterminer s'ils apparaissent dans le flux de messages sortants, afin de stopper toute infraction à la sécurité avant qu'elle ne se produise.

Administration centralisée

Gestion de la politique sur l'Internet, administration et contrôle de l'utilisateur final

La console Proofpoint Messaging Security Console™ est l'interface d'administration centralisée passant intégralement par l'Internet du cadre de gestion de politiques unifiée Proofpoint qui permet de garantir une application homogène et systématique de votre politique de messagerie. Cette console facilite la surveillance et le contrôle de votre infrastructure de messagerie, ainsi que l'élaboration de votre politique de messagerie. Vous pouvez même définir et mettre en œuvre différentes politiques pour différents groupes d'utilisateurs finaux. Quels que soient les modules Proofpoint que vous ajoutez à votre plateforme, vous continuerez à gérer vos politiques à l'aide de la même interface conviviale.

Cette interface fondée sur Ajax vous permet de personnaliser vos rapports, vos informations d'état, vos sources RSS et autres modules affichés par de simples opérations de « glisser-déposer ». Vous pouvez même créer des mélanges d'informations (« mashups ») à partir de sources externes.

Et même les utilisateurs finaux bénéficient de la convivialité du système Proofpoint. Les rapports et les contrôles, faciles à comprendre, tels que le rapport de l'utilisateur final Proofpoint, la mise en quarantaine par l'Internet et les listes de sécurité et de blocage personnalisées sont autant de moyens permettant à l'utilisateur de contrôler complètement ses préférences en matière de pourriel.

Fonction de production de rapport à toute épreuve

La Console vous permet par ailleurs de consulter plus de 60 rapports et des messages d'alerte graphiques en temps réel, ce qui vous donne une visibilité complète de la situation de votre messagerie d'entreprise. Les rapports peuvent aisément être envoyés par courriel ou affichés en HTML/XML. Les rapports « actifs » de Proofpoint vous fournissent toutes les informations essentielles, et permettent également aux administrateurs de prendre immédiatement des mesures si nécessaire (en cliquant simplement sur un lien pour bloquer un expéditeur abusif).

Administration zéro

Protection mise à jour en permanence, administration facilitée à l'extrême

L'installation et la notification automatiques de modules facilitent hautement l'administration du système au quotidien. Le service Proofpoint Dynamic Update Service permet de garantir que votre réseau bénéficie en toutes circonstances du meilleur niveau de protection possible contre les attaques par courriels. Il met continuellement à jour chacun des modules de votre logiciel ou plateforme Proofpoint, y compris le système d'exploitation renforcé et MTA, les moteurs anti-pourriel et antivirus, les lexiques (tels que les dictionnaires utilisés par le module de conformité à la réglementation Proofpoint Regulatory Compliance), les modules d'applications et les réparations à chaud personnalisées.

Proofpoint Messaging Security Gateway et Proofpoint Protection Server

chiffrement d'informations confidentielles

Le module **Proofpoint Secure Messaging™** offre une haute capacité de chiffrement sensible au contenu à votre plateforme Proofpoint en chiffrant automatiquement tous les messages en fonction de la politique spécifique de votre entreprise dans ce domaine. Il applique automatiquement et systématiquement votre politique en matière de chiffrement de données, sans nécessiter la moindre intervention de la part de l'utilisateur final. La technologie IBE (identity based encryption ; chiffrement fondé sur l'identité) est très puissante, d'une utilisation facile et qui élimine tous les problèmes liés à la gestion de clés et de certificats que l'on rencontre avec les solutions de nos concurrents. Le matériel et les outils virtuels Proofpoint sont par ailleurs compatibles avec les certificats numériques et permettent à la fois d'effectuer des transferts entre passerelles en toute sécurité et de recevoir des courriels à l'aide du protocole TLS (Transport Layer Security ; sécurité de la couche transport).

optimisation de l'infrastructure de votre messagerie

Déployez votre plateforme Proofpoint grâce à une palette de perfectionnements qui améliorent la convivialité et la gestion de l'infrastructure de votre messagerie. Le module **Proofpoint Smart Search™** renforce les fonctions intégrées de journalisation et de production de rapports dotées de capacités de traçage des messages, d'analyse de puits de données et d'analyse du journal de messages avancées qui offrent une visibilité claire et en temps réel des flux de messages à travers toute l'infrastructure de votre système de messagerie. Vous pouvez ainsi rechercher, analyser et exporter toutes vos listes de messages à partir d'une interface graphique conviviale et facile à utiliser, même si votre plateforme est déployée à l'échelle internationale. **Proofpoint Secure File Transfer™** ajoute une capacité de transfert de fichiers de grande taille à votre plateforme Proofpoint. Elle permet aux utilisateurs finaux d'envoyer rapidement et facilement des fichiers de grande taille (ou des fichiers nécessitant une sécurité supérieure) ; tout en réduisant l'impact des pièces jointes importantes sur l'infrastructure de votre messagerie. La solution à la carte **Proofpoint Email Archiving™** prend en charge la gestion du stockage des courriels, les besoins de la recherche d'éléments à des fins légales et la conformité réglementaire sans les frais qu'implique la gestion d'un archivage de messagerie en entreprise.

haute performance, déploiement aisé et modularité optimale

Proofpoint a été spécialement conçu pour répondre aux besoins particuliers des grandes entreprises, des fournisseurs de services Internet, des universités et des administrations publiques. Il offre toutes les fonctions de performance, de flexibilité, d'extensibilité, de personnalisation et de contrôle dont l'utilisateur final a besoin dans le contexte d'un déploiement à grande échelle de cette plateforme.

Chacun des modules du système Proofpoint a été conçu de manière à satisfaire les exigences de performance propres aux entreprises. Qu'il s'agisse du système d'exploitation renforcé à messages optimisés utilisé par le matériel Proofpoint ou de l'architecture unique et sans file d'attente de Proofpoint grâce à laquelle toutes les fonctions de filtrage de messages sont effectuées dans la mémoire, les systèmes Proofpoint vous fourniront le très haut niveau de performance que vous recherchez, notamment dans un contexte de déploiement complexe.

Le matériel Proofpoint est modulable à l'infini afin de pouvoir gérer des millions de messages par jour. Il est aisément déployé dans des configurations de type maître/agent afin de permettre la gestion de centres de données complexes ou éloignés géographiquement les uns des autres et ainsi fournir une protection de la redondance à 100 %, combinée à l'agrément de pouvoir travailler avec une seule interface administrative. Proofpoint autorise même les déploiements hybrides de matériel et d'outils virtuels intégrés les uns aux autres.

L'architecture de modularité optimale Proofpoint vous permet de gérer tous les serveurs agents à partir d'une seule et même console générale. La propagation automatique de configurations, la mise en quarantaine centralisée de messages et la production de rapports centralisée simplifient votre travail de maintenance et réduisent votre coût de propriété global.

Proofpoint permet de réduire encore davantage votre coût de propriété global grâce à la facilité avec laquelle le système s'intègre à tous les types d'infrastructure IT, quelle que soit la façon dont elle est répartie à travers votre pays ou à travers le monde. Une console de contrôle de type LDAP à interface graphique et une compatibilité intégrale avec Microsoft Active Directory® facilitent hautement l'intégration de serveurs d'annuaire. Proofpoint est également compatible avec les solutions de serveurs de messagerie sur-utilisés, tels que Microsoft Exchange® et Lotus Notes®, et minimise également leurs charges de travail.

essayez Proofpoint gratuitement dès aujourd'hui!

Faites vous-même l'expérience de la puissance du système Proofpoint. Rendez-vous sur le site www.proofpoint.com/trial et inscrivez-vous afin de télécharger une version d'essai de Proofpoint Messaging Security Gateway — Virtual Edition pleinement opérationnelle, valide 45 jours. Le déploiement ne prend que quelques minutes. Ou bien rendez-vous sur le site www.proofpoint.com/trypod et inscrivez-vous pour un essai gratuit de la solution de sécurisation de la messagerie SaaS à la carte.

Proofpoint parle votre langue

Outre les excellentes performances anti-pourriel dans toute les langues, la politique et les moteurs de filtrage de Proofpoint détectent et « comprennent » les textes dans toutes les langues, y compris les langues composées de caractères à plusieurs octets. Les politiques de prévention de perte des données peuvent faire correspondre des mots-clés et des termes d'un dictionnaire écrits dans des jeux de caractères internationaux comme le japonais, le chinois et le cyrillique. Les administrateurs peuvent créer des politiques qui se déclenchent d'après la langue détectée dans le contenu d'un courriel. Par exemple, envoyez une pièce jointe contenant des avis de non-responsabilité propres à une langue à un message sortant, selon la langue dans laquelle il a été écrit.

Des interfaces pour l'utilisateur final pour le traitement des messages et la mise en quarantaine sont disponibles en version chinoise, néerlandaise, anglaise, allemande, finlandaise, française, italienne, japonaise, portugaise, russe, espagnole et suédoise.

L'interface graphique d'administration, la documentation du produit et l'aide en ligne de Proofpoint sont actuellement disponibles en version japonaise et anglaise. Tout comme avec les interfaces utilisateur final de Proofpoint, les administrateurs peuvent programmer leurs préférences linguistiques individuellement.

Versions matériel

L'unité Proofpoint Messaging Security Gateway est proposée en de nombreuses configurations de matériel différentes afin de satisfaire toutes les tailles de déploiement de plateforme. Pour de plus amples renseignements concernant les différents modèles de matériel Proofpoint, veuillez consulter :

www.proofpoint.com/products/msg.php

Navigateurs compatibles

Toutes les procédures de configuration et d'administration, que ce soit pour le matériel, pour les outils de virtualisation ou pour les logiciels, sont effectuées sous l'interface de navigateur de Proofpoint. Navigateurs compatibles :

Microsoft® Internet Explorer 6.0 ou supérieur

Mozilla Firefox 2.0 ou supérieur

©2008 Proofpoint, Inc. Proofpoint Protection Server est une marque déposée de Proofpoint, Inc. aux États-Unis et dans les autres pays. Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Email Firewall, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Dynamic Update Service, Proofpoint MLX, Proofpoint Dynamic Reputation, Proofpoint netMLX, Proofpoint Smart Search, Proofpoint Messaging Security Console et Proofpoint on Demand sont des marques déposées de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques figurant dans ce document appartiennent à leurs propriétaires respectifs. 09/08