



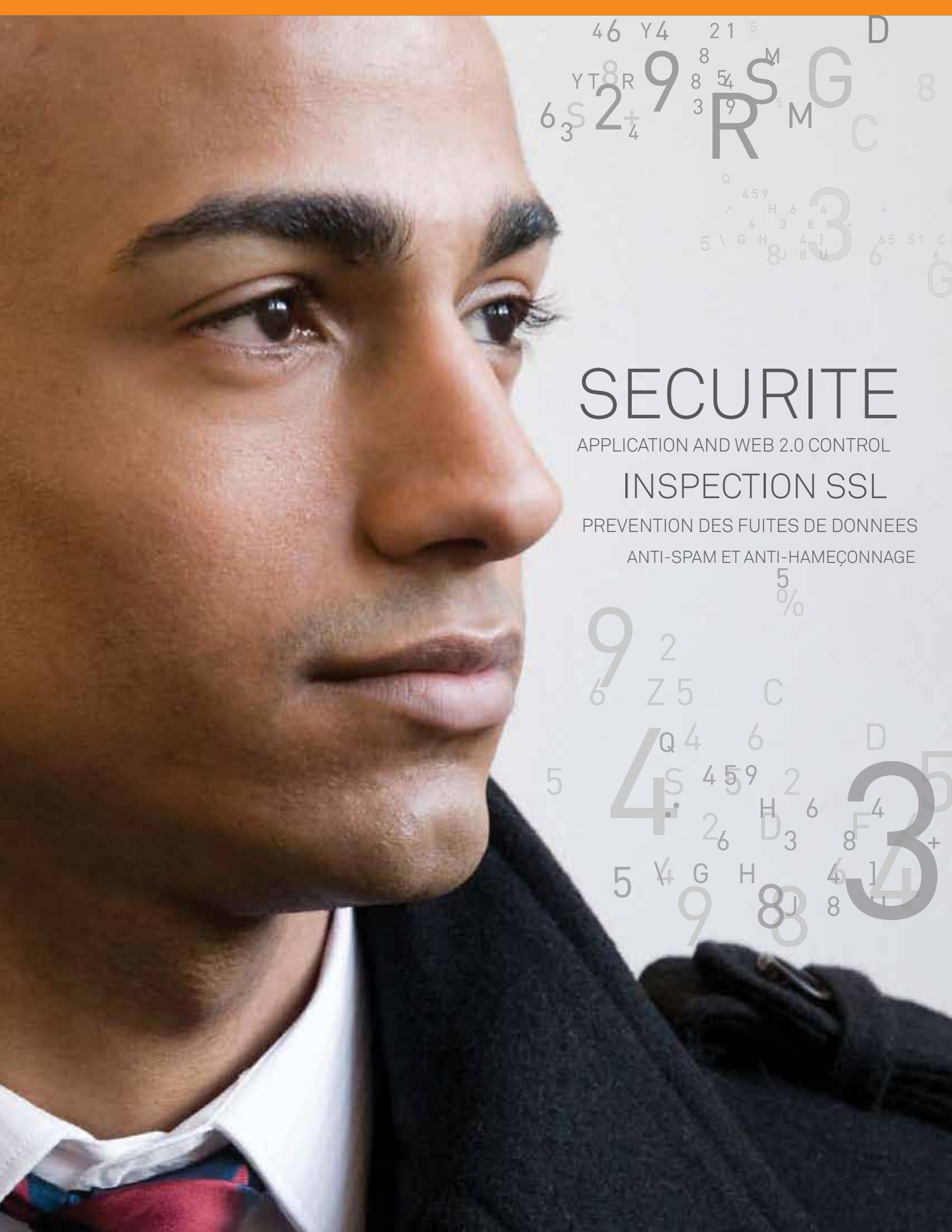
# SafeNet Sécurité des contenus Aperçu sur le produit

Protéger le périmètre du réseau



Depuis le concept jusqu'à l'action, SafeNet protège intelligemment les informations au cours de leur cycle de vie. Grâce au système de chiffrement et de contrôle, les sociétés peuvent continuellement protéger leurs données sensibles pendant leur cycle de vie, qu'elles se trouvent dans le centre informatique ou qu'elles soient transférées vers le point final à la frontière du réseau et dans le Cloud. eSafe fournit des solutions assurant la sécurité des contenus, la maîtrise des données et la prévention des fuites de données (DLP) pour le trafic Internet entrant et sortant à travers les frontières du réseau, y compris le surf sur le web (passerelle sécurité web) et la messagerie (passerelle sécurité mail).





46 Y4 21 S D  
YT8R 9 8 54 S M G 8  
63 2+4 3 9 3 R 5 M C  
Q 459 H 6 4 +  
5 \ G H 8 J 8 U 6 65 51 C  
G

# SECURITE

APPLICATION AND WEB 2.0 CONTROL

## INSPECTION SSL

PREVENTION DES FUITES DE DONNEES

ANTI-SPAM ET ANTI-HAMEÇONNAGE

5%

9 2  
6 Z 5 C

5 4 Q 4 6 D  
S 4 5 9 2  
2 6 D 3 4  
5 V G H 8 J 8 8 3+  
9 8 8 3

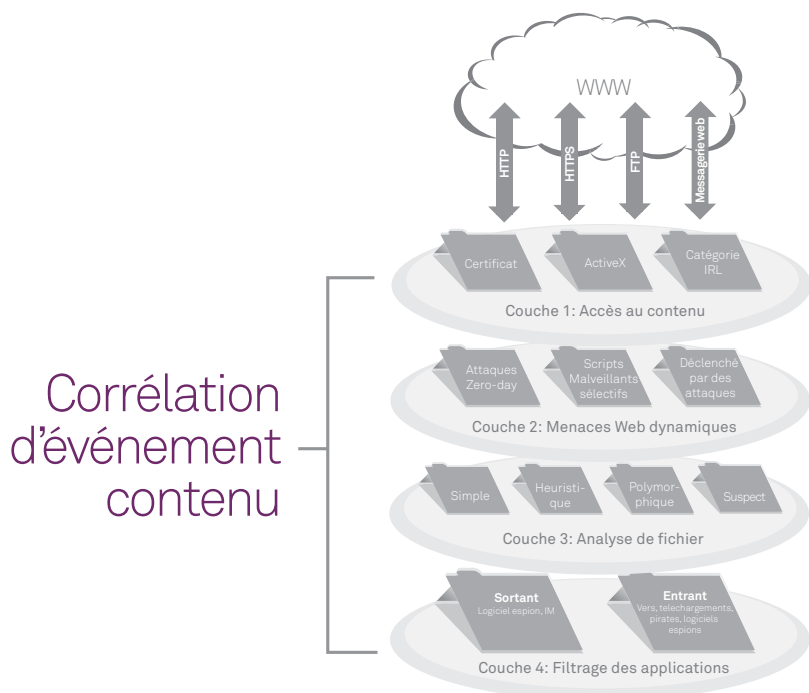
Que vous soyez une PME devant faire face à des menaces précises concernant la sécurité ou une entreprise voulant déployer plus largement son système de sécurité, les solutions et les services eSafe pour les passerelles web et la messagerie protègent le périmètre de votre réseau contre les menaces et violations externes et internes concernant la sécurité.

eSafe fournit la solution la plus complète pour inspecter en temps réel et de manière intelligente tous les trafics web et mail entrants et sortants sur le marché des solutions de sécurité de contenus. eSafe offre les performances et la capacité nécessaires pour que votre société reste souple et productive, il inspecte en détail tous les contenus, y compris les sites légitimes, le trafic chiffré et les applications web, et il le fait à la vitesse d'un circuit câblé comme cela est nécessaire pour une transparence totale.

## Passerelle de sécurité web (Web Security Gateway)

Les passerelles de sécurité web doivent être protégées contre les menaces externes et internes. Face au danger que représente le eCrime (crime électronique), la fuite de données et la baisse de productivité, les sociétés deviennent de plus en plus vulnérables et ont besoin de défenses variées pour protéger leurs données et leur propriété intellectuelle.

Web Security Gateway de eSafe fonctionne en temps réel pour filtrer les contenus malveillants lorsqu'ils pénètrent dans votre réseau, en analysant le trafic http et ftp pour détecter toutes les traces de contenu et d'applications malveillants, inappropriés ou autrement indésirables. De plus, cette passerelle contrôle tous les trafics sortants grâce à des fonctions avancées de prévention de fuite de données (DLP) afin que les informations ne quittent pas la société. Le nouveau moteur d'analyse Web 2.0 Script Analysis Engine de eSafe sait comment traiter les derniers malwares (malicieux) et il est utilisé automatiquement sur le web.



## Passerelle de sécurité mail (Mail Security Gateway)

Les passerelles de sécurité d'emails sont constamment exposées à des menaces évolutives. Que ces menaces se présentent sous la forme de spams, de tentatives de phishing, de logiciels espions, de malwares (malicieux), de fuites de données ou d'autres risques concernant le contenu, les sociétés doivent être vigilantes et s'adapter rapidement pour garantir la sécurité du trafic entrant et sortant à travers les passerelles messagerie.

Mail Security Gateway d'eSafe utilise un double moteur anti-spams avec une technologie de réputation et de reconnaissance de distribution en temps réel pour bloquer les spams, les malwares et les virus, et pour protéger les informations sensibles en prévenant leur fuite.

En assurant en temps réel l'analyse de réputation et l'analyse approfondie de contenu dans un seul système intégré, Mail Security Gateway d'eSafe protège votre société contre les menaces variées résultant de l'utilisation de la messagerie.

# Modules eSafe

## Sécurité: anti-malwares (maliciels), anti-logiciels espions et antivirus

Les modules sécurité d'eSafe utilisent plusieurs technologies pour protéger votre réseau et vos messageries contre les codes malveillants, les logiciels espions et les tentatives d'exploitation des vulnérabilités des applications web conduisant à une infection par des malwares.

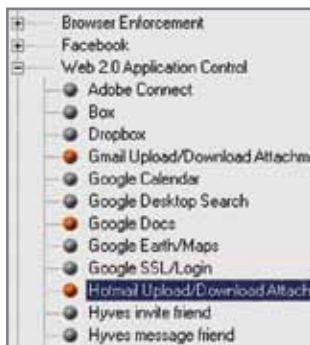
Contrairement aux autres systèmes se concentrant sur l'inspection des fichiers téléchargeables pour détecter les virus, eSafe détecte les malweb (maliciels propres au web) (grâce au moteur Kaspersky). Les malweb sont dissimulés dans les contenus web standard et exploitent les diverses vulnérabilités des applications Internet comme les navigateurs, les plug-ins (modules d'extension) de navigateur, et les autres applications intervenant sur le web.

eSafe peut détecter de manière impérative les tentatives d'exploitation de ces vulnérabilités avant qu'elles ne pénètrent réellement au lieu de détecter les malwares qui sont téléchargés du fait de l'exploitation.

## Application and Web 2.0 Control

Les modules Application and Web 2.0 Control d'eSafe assurent un contrôle granulaire des applications web, régulent l'utilisation d'Internet, et interdisent les opérations non autorisées, indésirables ou dangereuses pouvant conduire à une infection ou à une fuite d'informations.

Le module Web 2.0 Control d'eSafe empêche les applications Web 2.0 de bypasser les mesures de sécurité existantes et de créer des lacunes à travers lesquelles les logiciels espions, les chevaux de Troie, les virus et les autres malwares peuvent attaquer un réseau.



AppliFilter assure une protection complète en temps réel contre les applications malveillantes, dangereuses et indésirables en utilisant plus de 500 protocoles dans plus de 20 catégories d'applications. En contrôlant, maîtrisant et bloquant les applications au niveau de la passerelle, le réseau sera protégé en temps réel en ne laissant passer que les applications autorisées, tout en restant complètement transparent pour les utilisateurs.

Contrairement aux autres solutions, eSafe, en vue d'améliorer la productivité, offre Web Quota Control (gestion de quota), permettant aux administrateurs de contrôler et de faire appliquer la politique de la société par les utilisateurs et les groupes dépassant systématiquement leur quota journalier d'utilisation du web.

## Prévention des fuites de données (Data Leak Prevention DLP)

Le module Data Leak Prevention (DLP) d'eSafe contrôle tous les trafics sortants en bloquant et en maintenant à l'intérieur du réseau les informations pouvant être classées à 100% comme confidentielles de manière certaine. Le module DLP facilite le respect de la réglementation, minimise les fausses détections et fournit des outils complets d'enquête judiciaire et de détection.

Le module DLP d'eSafe inspecte tous les trafics sortants de la société sur Internet (web, messagerie et FTP). Avec plus de 20 dictionnaires immédiatement disponibles pour plus de 150 types de fichiers, et avec la prise en charge de Unicode, le module DLP peut gérer les politiques granulaires devant être suivies par les utilisateurs ou les groupes et peut déclencher des mesures de reporting, de blocage, d'archivage ou d'alerte, et peut aussi générer des rapports pour faciliter le contrôle et l'administration. De plus, les administrateurs peuvent personnaliser de manière très précise les dictionnaires DLP pour les adapter aux besoins de leur société, ou ils peuvent créer leurs propres dictionnaires.

Contrairement aux produits DLP nécessitant une configuration et une mise en œuvre compliquées, le module DLP d'eSafe fournit toutes les fonctions nécessaires pour que les sociétés puissent mieux respecter la réglementation et pour qu'elles puissent gérer facilement le module DLP. Le module DLP d'eSafe fait partie du produit et fournit les fonctions DLP sans coût supplémentaire.

## L'importance de la DLP

Les sociétés veulent protéger leurs informations internes pour qu'elles ne s'échappent pas dans le monde extérieur, et elles doivent mettre en place une protection périphérique robuste pour contrôler le trafic sortant sur Internet afin de faire appliquer les politiques de sécurité.

Dans son étude récente, "Putting the P in DLP," le Aberdeen Group a écrit que l'approche "Ramper, marcher, courir" est un modèle pragmatique pour un déploiement réussi à l'échelle de l'entreprise de tous les projets de sécurité informatique, et le projet DLP ne fait pas exception.

- Inspection de tous les trafics sortants de la société pour aller sur Internet (web, messagerie et FTP)
- Reconnaissance du format de plus de 150 types différents de fichiers, y compris tous les formats MS Office, PDF, et archives
- Enregistrement de tous les événements concernant la distribution de documents, y compris leur horodatage, qui les a envoyés, où ils ont été envoyés, et même les métadonnées du document
- Plus de 20 dictionnaires prédéfinis permettant de détecter les contenus sensibles comme PII, numéros de cartes de crédit, code source, profanation et réglementations comme SOX, PCI, et HIPAA

## Filtrage de contenu (Content Filtering)

Le module Content Filtering d'eSafe interdit l'accès aux sites web non autorisés, inappropriés et malveillants, protégeant ainsi votre société contre des poursuites judiciaires tout en augmentant la sécurité et la productivité. Les administrateurs peuvent identifier les activités de surf sur le web et peuvent adapter de manière précise les politiques web par un contrôle granulaire des utilisateurs et des groupes, et par un contrôle et un reporting complets de l'activité sur le web.

Avec plus de 150 millions de sites web appartenant à 70 catégories, mis à jour 12 fois par jour, eSafe utilise une technologie unique d'intelligence artificielle et de classification du web permettant aux administrateurs de contrôler la diffusion par les médias par catégorie de sites web. eSafe utilise uniquement un cache dynamique local avec des adresses URL communes, supprimant ainsi la nécessité d'une grande base de données locale ou de mises à jour constantes.

## SSL Inspection (inspection SSL)

SSL Inspection d'eSafe protège le réseau contre les codes malveillants tentant de pénétrer sur le trafic chiffré SSL.

eSafe inspecte totalement le trafic web HTTPS/SSL en utilisant la technologie transparente "trusted Man-in-the-Middle" (MitM), pour faire appliquer la politique d'utilisation SSL et pour certifier la validité.

Grâce à la technologie MitM, eSafe peut ouvrir toutes les communications chiffrées puis les chiffrer à nouveau, et il peut aussi contrôler complètement le contenu même lorsqu'il est chiffré, par exemple dans Gmail. De plus, eSafe vérifie que le certificat est signé et vérifie aussi qu'il est valide et n'a pas été résilié. Une inspection SSL transparente est incorporée pour protéger les modes dérivation (pont) et routeur.

## Anti-spam et anti-hameçonnage

Le double moteur anti-spam d'eSafe pour la sécurité de la messagerie assure une protection complète, un contrôle total et une augmentation de la productivité.

En associant les stratégies de réputation et de contenu, le module anti-spam d'eSafe assure en temps réel l'analyse de réputation et l'analyse détaillée de contenu dans un seul système intégré. L'utilisation de deux moteurs permet de détecter 99% de tous les spams et de toutes les tentatives d'hameçonnage, et supprime presque totalement les fausses détections positives, garantissant ainsi que les utilisateurs ne reçoivent que des emails pertinents et fiables.

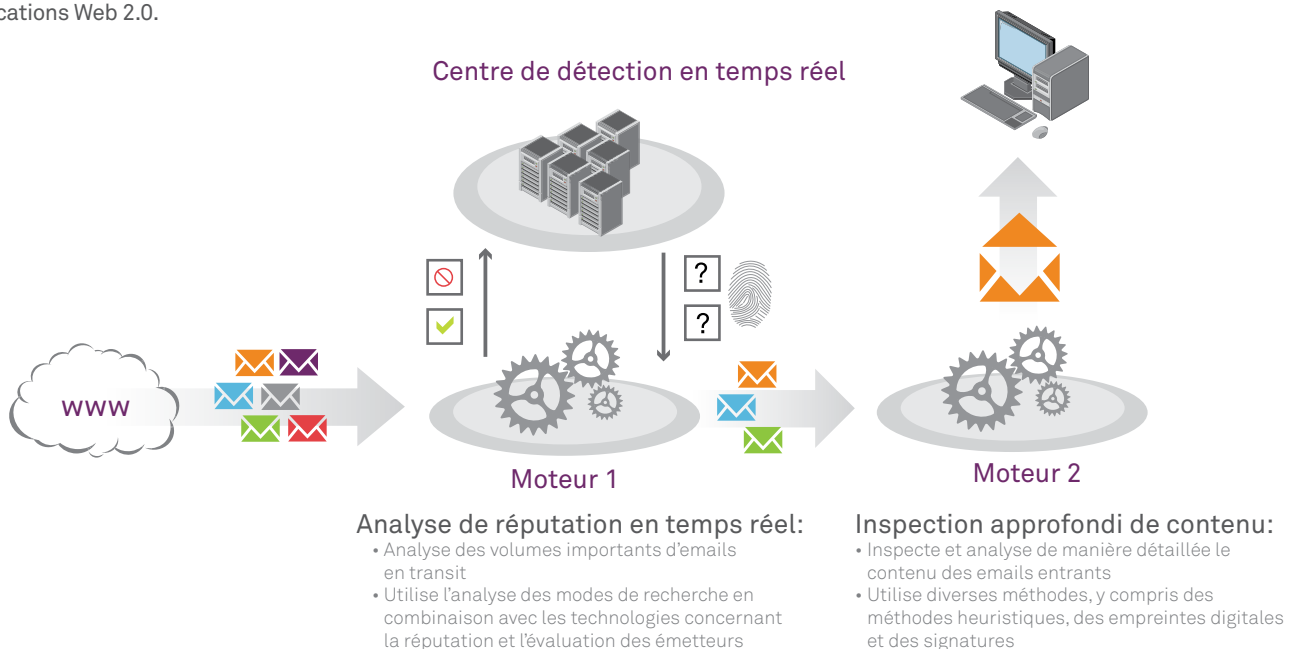
eSafe assure une protection globale contre les tentatives d'hameçonnage sur la messagerie et sur le web, quelle que soit la langue du pays d'origine, et il bloque les attaques d'hameçonnage lorsqu'elles sont dissimulées sur des sites web légitimes ou lorsqu'elles arrivent par des applications Web 2.0.

## Crime électronique (eCrime)

Internet offre aux criminels des opportunités innombrables pour faire de l'argent avec un risque presque nul. Malheureusement le crime électronique est devenu une profession et il a pris des proportions qui auraient été considérées comme de la science-fiction il y a seulement dix ans. Qu'il s'agisse de la recherche des opportunités, de l'analyse des vulnérabilités de la sécurité, du choix des outils et des méthodes d'exploitation, de l'exploitation et de l'utilisation de la chaîne alimentaire (par le blanchiment d'argent) ou de faire de l'argent en envoyant des spams et des emails d'hameçonnage via des ordinateurs infectés, il s'agit d'une course entre des systèmes robustes de sécurité et les professionnels/amateurs du crime électronique, et celui qui aura une longueur d'avance gagnera.

*"L'an dernier, pour la première fois, les revenus fournis par le cybercrime ont été supérieurs aux revenus fournis par la vente des drogues interdites... et la justice ne peut rien y faire."*

**Valerie McNiven,**  
U.S. Treasury Dept.



# Gestion et reporting (Management and Reporting)

Le module Management and Reporting d'eSafe fournit aux administrateurs des fonctions avancées leur permettant de contrôler facilement le réseau et de faire appliquer la politique sécurité de la société dans tout le réseau. Les administrateurs sont au courant de tout ce qui se passe sur le réseau grâce à un aperçu en temps réel du système de sécurité interne de la société et de l'utilisation d'Internet, ce qui leur permet de prendre rapidement les mesures nécessaires lorsque le réseau est menacé ou attaqué, et ce module génère des rapports détaillés et faciles à utiliser concernant l'utilisation d'Internet, rapports destinés à la direction.

Le Centre sécurité d'eSafe constitue la console de gestion permettant aux administrateurs de configurer et de faire appliquer la politique de sécurité de contenu dans tout le réseau.

Le module Management and Reporting d'eSafe fournit aux services de sécurité des outils puissants pour examiner et analyser le trafic sur le réseau, la productivité des employés, et le respect de la politique. eSafe permet aux administrateurs de transmettre facilement les problèmes de sécurité et de justifier de manière rationnelle de nouveaux besoins auprès de la direction générale.



## Distribution

eSafe offre des options de distribution robustes et souples avec plusieurs modes de mise en œuvre. Grâce au mode cluster actif assurant une disponibilité élevée et l'équilibrage de charge et prenant en charge les modes dérivation (pont) et routeur, eSafe assure la redondance et la disponibilité du service Internet sans coûts supplémentaires.

### Mise en œuvre souple

Les deux modules Web Security Gateway et Mail Security Gateway d'eSafe prennent en charge plusieurs modes de déploiement. Grâce à cette souplesse, eSafe peut être mis en œuvre de manière simple et facile sur le réseau du client. Les modes de déploiement d'eSafe sont les suivants:

- Dérivation (pont) en ligne transparente (web et messagerie)
- Routeur (web et messagerie)
- Serveur mandataire (Proxy) avec cache (web)
- Serveur mandataire (Proxy) émetteur (web)
- Serveur mandataire (Proxy) avec support WCCP (web)
- Serveur ICAP (web)
- Relais SMTP (mail)

### Disponibilité élevée / Equilibrage de charge

La technologie eSafe offre divers systèmes assurant une disponibilité élevée et l'équilibrage de charge, notamment les clusters de dérivation (pont) en ligne, les clusters routeurs, et les commutateurs L3-L4 de tiers.

### Entretien et assistance produit

eSafe fournit tous les services d'entretien et d'assistance produit, notamment des programmes de soutien et diverses ressources en ligne, afin de maintenir à niveau le système de sécurité et afin que le service eSafe puisse réagir en temps voulu à toutes les demandes.

Les services comprennent aussi les mises à niveau logicielles, les mises à jour critiques pour la sécurité, et le remplacement des équipements si nécessaire.

*"En tant qu'expert informatique dans un grand collège d'Etat, je devais aller d'un laboratoire à l'autre trois ou quatre fois par jour pour supprimer des infections par virus. J'ai reçu un disque de démonstration pour évaluation et ma vie a changé.*

*Après avoir évalué le produit eSafe et nettoyé les laboratoires de recherche critiques, j'ai présenté le produit au doyen du collège et j'ai aussitôt commandé une licence pour un site, qui est devenue un système de licence à l'échelle de l'entreprise. Je suis entièrement satisfait des services offerts par eSafe!"*

**Eddie G. Holman**  
Informaticien

## Systèmes

Système	Marché visé	Capabilités
XG110	PME et succursales	Jusqu' à 700 utilisateurs
XG210	Entreprises moyennes	Jusqu' à 3 000 utilisateurs
XG300	Grandes entreprises et centres informatiques ISP	Jusqu' à 7 000 utilisateurs
XG1000	Telco, services sécurité ISP et administration	Jusqu' à 100 000 utilisateurs





**Pour nous contacter:** Pour connaître l'emplacement des bureaux et avoir des informations sur les contacts, visitez le site [www.safenet-inc.com](http://www.safenet-inc.com)

**Suivez-nous:** [www.safenet-inc.com/connected](http://www.safenet-inc.com/connected)

©2010 SafeNet, Inc. Tous droits réservés. SafeNet et le logo SafeNet sont des marques de fabrique déposées de SafeNet.

Tous les autres noms de produits sont des marques de fabrique appartenant à leurs détenteurs respectifs. FB (EN)-08.10.10