



« 90% des 100 sites les plus populaires du Web sont des réseaux sociaux ou des moteurs de recherche. Plus de 47% d'entre eux proposent du contenu généré par l'utilisateur. »

**Websense Security Labs™, 2009**

**Websense®**

## Web Security Gateway

Les technologies Web 2.0 dynamiques et interactives ont transformé l'Internet en une plateforme incontournable d'applications pour les entreprises. Les outils traditionnels de relation clients et de facturation sont désormais disponibles en ligne et interactifs. Les sites de réseaux sociaux sont utilisés au quotidien pour le recrutement, la génération d'opportunités et autres processus métier. Mais cette nouvelle génération du Web engendre de nouveaux risques de sécurité et les outils d'anti-virus et de filtrage d'URL classiques sont incapables de sécuriser le contenu généré par l'utilisateur. De plus, ils n'apportent aucun contrôle sur l'information sensible susceptible d'être publiée sur les sites Web 2.0.

Websense® Web Security Gateway domine le marché des passerelles Web sécurisées en offrant la meilleure protection contre les nouvelles menaces du Web 2.0, au coût total de possession (CTP) le plus bas. C'est la seule solution capable de proposer une prévention performante contre la perte de données et une gestion unifiée des déploiements sur site, en mode SaaS ou hybride. Web Security Gateway permet aux organisations d'exploiter le Web 2.0 sans se soucier des malwares, du contenu indésirable ou de la divulgation de données sensibles.

### Principe de fonctionnement

Websense Web Security Gateway inspecte le contenu entrant et sortant en temps réel, pour protéger les entreprises contre les malwares Web dynamiques, les pertes de données sensibles et pour améliorer la productivité des employés. La technologie de déploiement TruHybrid™ prend en charge les appliances installées sur site, les plateformes SaaS (Security-as-a-Service) et gère l'ensemble de l'environnement via une infrastructure unique de politiques et de reporting. Contrairement aux utilisateurs de solutions alternatives, les clients Websense ont la possibilité de choisir la plateforme ou la sélection de plateformes qui correspond le plus à leurs besoins opérationnels, sans subir les coûts liés à la gestion de multiples systèmes.

L'offre Websense Web Security Gateway :

- **Une prévention contre la perte des données sortantes et des contrôles de conformité** – Une technologie intégrée et globale de prévention contre la perte de données définit les contrôles nécessaires pour autoriser les communications sortantes vers des services de Webmail et des sites de réseaux sociaux. Ainsi, les règles de conformité sont respectées et la publication de l'information sensible est contrôlée.
- **Une protection contre les malwares** – Websense TRITON™ Advanced Classification Engine (ACE) protège les organisations contre les agressions fichiers classiques et contre les attaques dynamiques capables de contourner les solutions anti-virus traditionnelles.
- **Une productivité «Web 2.0» des employés** – TRITON Advanced Classification Engine supprime le contenu indésirable des sites Web 2.0 dynamiques, complexes et protégés par mots de passe ; des sites Web que les solutions de filtrage d'URL classiques sont incapables de classer de façon précise.
- **Le coût total de possession le plus bas (CTP)** – La console TRITON de Websense et la technologie de déploiement TruHybrid réduisent le nombre d'appliances, de systèmes de gestion et de fournisseurs à maintenir à travers l'entreprise.
- **Une couverture globale et homogène** – La technologie TruHybrid unifie les politiques à travers les déploiements sur site et en mode SaaS. Les utilisateurs nomades ou travaillant depuis chez eux bénéficient ainsi d'une mise en application permanente des politiques internes.

« Au cours du premier semestre 2009, plus de 80% des 100 sites les plus populaires du Web ont hébergé du contenu malveillant ou dissimulé une URL de site corrompu.

**Websense Security Labs, 2009**

### Un moteur de classification avancée

Web Security Gateway de Websense comprend l' Advanced Classification Engine (ACE) de TRITON, le moteur d'analyse bidirectionnelle de sécurité le plus performant du marché, combinant l'étude des informations entrantes avec une prévention approfondie de la perte des données sortantes. ACE associe une sécurité traditionnelle aux techniques avancées de classification du contenu (anti-virus, filtrage d'URL, services de réputation, empreintes numériques des données...) pour classer les risques entrants et sortants de façon précise. ACE est soutenu par le réseau ThreatSeeker de Websense ; il analyse le contenu au niveau de la passerelle, à l'aide de scans de sécurité et d'une classification du contenu effectués en temps réel, ainsi qu'une prévention haute performance contre la perte de données.

### Scanning de sécurité en temps réel

La technologie anti-virus ne peut faire face à elle seule aux attaques dynamiques et à base de scripts qui dominent le Web aujourd'hui. Les outils de scanning de sécurité en temps réel développés par Websense analysent ces attaques « zero day » en identifiant le contenu malveillant « à la volée », sans avoir besoin de consulter les bases de données des agressions connues.

### Classification du contenu en temps réel

La majorité des sites les plus visités du Web ne peuvent être classés précisément par les outils de filtrage d'URL classiques. Par exemple, une page Google ou Facebook peut contenir de multiples éléments de contenu de catégories différentes, ce qui rend impossible toute affectation à une seule catégorie. Résultat : de nombreuses organisations sont contraintes de bloquer de précieuses ressources ou d'ignorer les politiques d'utilisation en levant toutes les restrictions d'accès aux sites Web 2.0 dynamiques.

Web Security Gateway propose une classification en temps réel du contenu permettant d'appliquer les politiques d'utilisation aux sites Web 2.0 dynamiques. Les éléments de contenu de chaque page sont classés « à la volée » ; si l'un d'eux s'avère inapproprié, il peut être retiré de la page. L'accès aux autres informations reste autorisé. Cette capacité unique permet d'exploiter le Web 2.0 dans sa globalité, en garantissant la productivité et la conformité aux politiques d'utilisation.

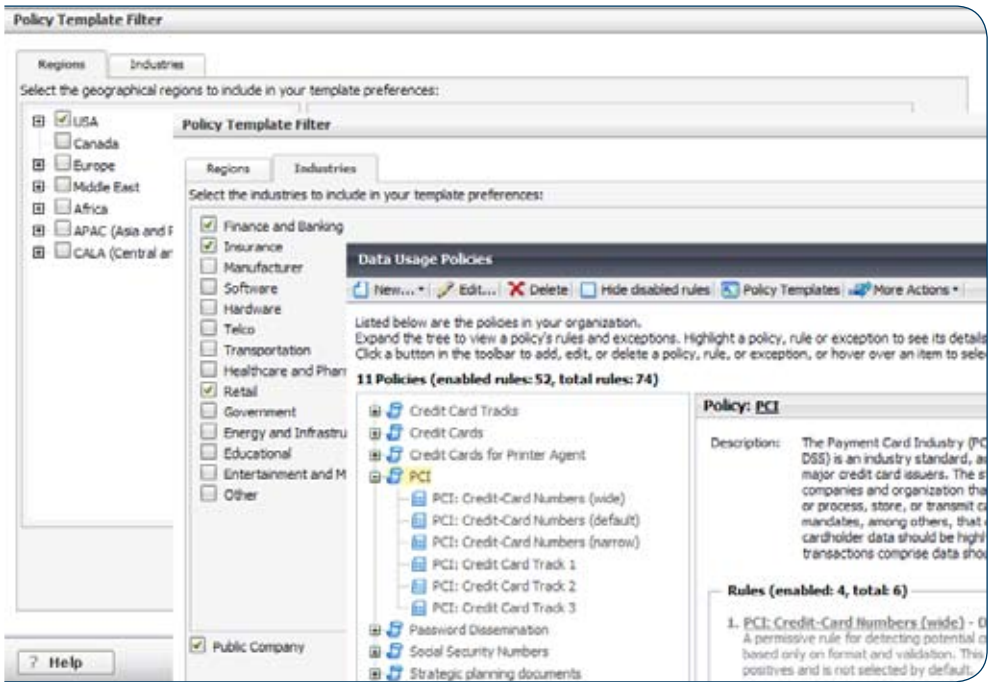
### Prévention globale contre la perte de données

Une technologie intégrée et globale de prévention contre la perte de données (DLP) définit les contrôles nécessaires pour autoriser les communications professionnelles sortantes vers des services de Webmail et des sites de réseaux sociaux. Ainsi, les règles de conformité sont respectées et la publication de l'information sensible est contrôlée. Contrairement aux autres outils disponibles qui proposent des fonctionnalités DLP limitées à des services d'inspection de mots clés ou qui nécessitent des intégrations complexes de solutions tierces, Web Security Gateway bénéficie de toutes les capacités de la solution DLP numéro 1 de Websense pour le trafic réseau http, https et FTP. WSG comprend plus de 800 politiques « out-of-the-box », des services d'empreintes numériques des données pour une inspection avancée du contenu et des fonctions complètes de reporting pour la conformité.

L'intégration de DLP Web avec Web Security Gateway réduit les coûts de façon significative en éliminant le besoin d'équiper tous les bureaux d'une entreprise avec du matériel DLP issu de sociétés tierces. Pour les organisations souhaitant investir à plus long terme dans une solution de prévention contre la perte de données, DLP Web permet d'optimiser votre investissement : une simple mise à jour logicielle suffit pour étendre les fonctions de contrôle au-delà du Web. Tout devient ainsi régulé : le trafic email, la messagerie instantanée, le P2P, les postes

\* <http://www.websense.com/content/tolly-report-reg.aspx>

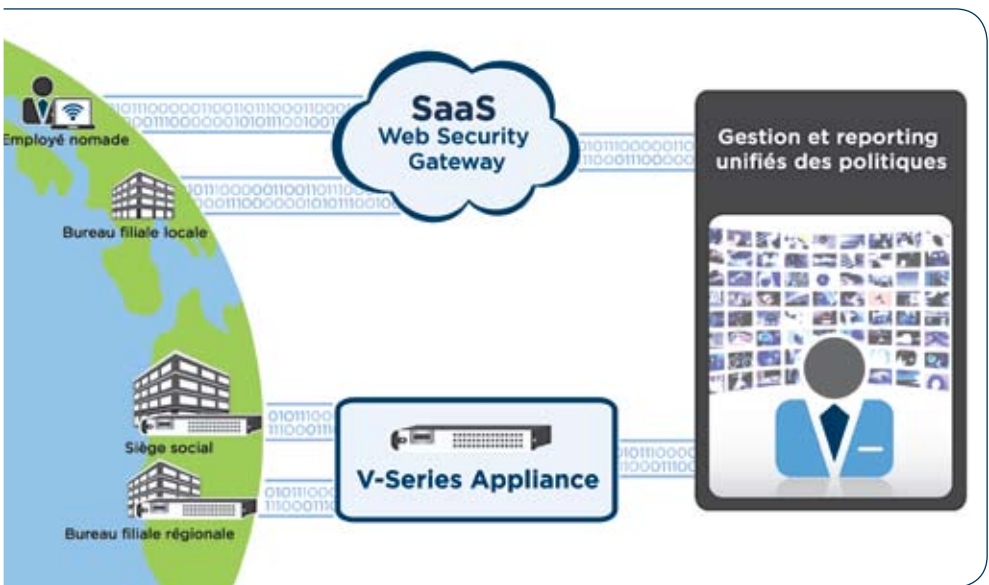
de travail et l'information stockée (bases de données, fichiers partagés, Exchange, SharePoint). En résumé, étendre la couverture de DLP Web à d'autres canaux ne remet pas en cause l'existant ; les politiques et les investissements d'infrastructure sont préservés.



Des assistants de politiques DLP aident les administrateurs à définir rapidement des politiques conformes aux réglementations locales et spécifiques à l'industrie de l'entreprise.

### Déploiement TruHybrid

La technologie de déploiement TruHybrid™ offre un choix de plateformes installées sur site ou disponibles en mode SaaS, et un seul système de gestion unifiée pour l'ensemble de l'environnement. Vous pouvez ainsi étendre votre solution de sécurité aux bureaux des filiales, en optimisant la plateforme SaaS. De plus, vous avez la possibilité de déployer des appliances haute performance à votre siège social, au sein de vos principales succursales ou dans vos centres de données. Quelles que soient les options choisies (SaaS, appliances...) vous bénéficiez d'un système de politiques unique pour toute l'entreprise. Cette approche unifiée permet de minimiser les coûts des déploiements hybrides sur site/ SaaS, et de mettre en place une véritable couverture de sécurité globale.



TruHybrid unifie la gestion des déploiements hybrides sur site/SaaS.

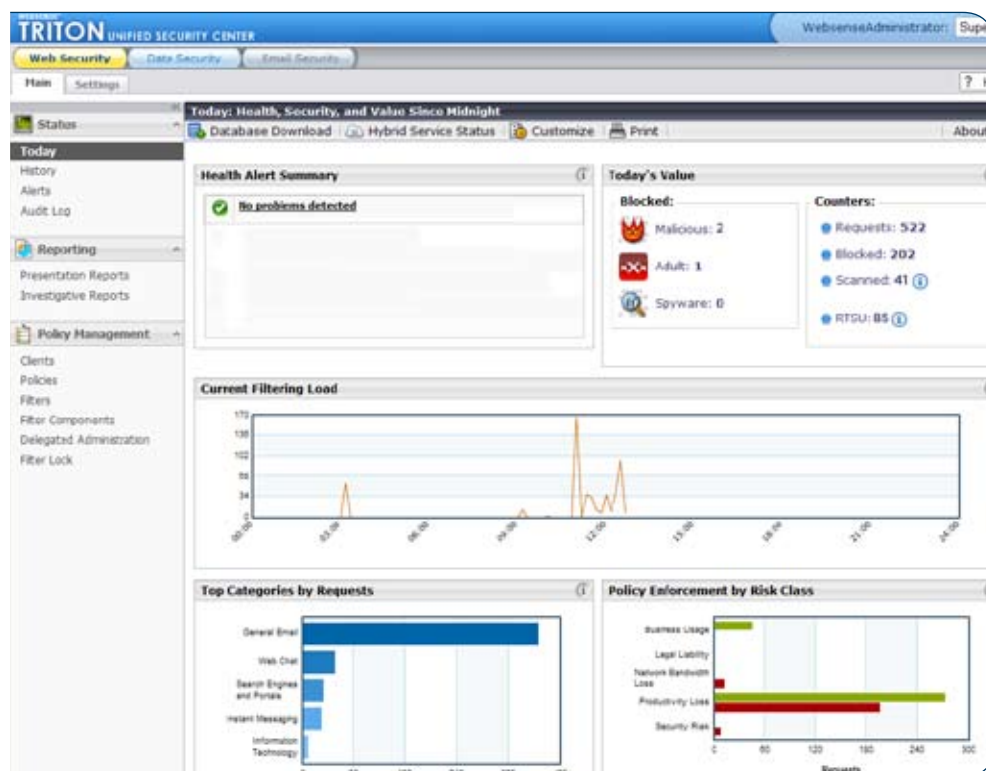
« Nous utilisons l'appliance Web sécurisée V10000™ de Websense pour permettre à notre personnel infirmier d'accéder rapidement aux informations dont ils ont besoin, en toute sécurité. Avec un scanning effectué en temps réel et la possibilité de créer des politiques flexibles d'utilisation de l'Internet, je ne me soucie plus des conséquences liées aux visites de sites Web corrompus par des codes malveillants ou aux détournements accidentels des données confidentielles des patients ».

#### Larry Whiteside

Responsable de la sécurité,  
Visiting Nurse Service  
de New York

“57% des attaques Web incluent un code malveillant destiné à détourner l’information.”

WebSense Security Labs, 2009



Les tableaux de bord interactifs de la Console TRITON offrent un accès instantané aux menaces et aux activités de violation de politiques, dès qu'elles se produisent.

### Visibilité et contrôle SSL

L'augmentation du trafic SSL a créé des zones d'ombre pour les filtres URL classiques, facilitant ainsi la prolifération des menaces et des pertes de données.

Web Security Gateway apporte une visibilité et un contrôle uniques sur le trafic SSL et permet aux entreprises de mettre en place des politiques d'utilisation sur l'ensemble de leurs communications Web.

### Contrôle avancé des applications

La multiplication des applications réseau, telles que la messagerie instantanée et le P2P facilitent l'activité des hackers cherchant à perturber les activités d'une entreprise ou à détourner des données confidentielles. Web Security Gateway contrôle plus de 125 protocoles réseau et des milliers d'applications. Cela permet de minimiser les risques et de prévenir les pertes de données depuis les applications non approuvées. La palette d'actions disponibles s'étend du simple blocage d'application au contrôle granulaire de la bande passante.

### Gestion de la sécurité du contenu et reporting unifiés

La Console TRITON est une caractéristique importante de Web Security Gateway. C'est une exclusivité Websense. Elle permet de consolider la gestion de toutes les solutions de sécurité du Web, de la messagerie et des données de Websense dans une seule interface Web. Son tableau de bord intuitif comprend 55 rapports prédéfinis et de nombreuses possibilités de personnalisation, pour déterminer l'activité des utilisateurs, faciliter la résolution des problèmes et réduire davantage les risques. La charge de travail des administrateurs est allégée et les coûts sont réduits de façon significative par rapport aux solutions concurrentes. Comment ? A l'aide d'outils faciles à utiliser tels que de nombreuses fonctions de contrôles avancés, des assistants de politiques, des modèles de configuration prédéfinis, un système sous-jacent de programmation et des mises à jour automatiques de contenu. De plus, anticipant l'expansion des besoins de sécurité au-delà du Web, les fonctionnalités unifiées de la Console TRITON peuvent être facilement étendues aux outils de gestion email et DLP.

Caractéristiques	Avantages
Déploiement TruHybrid	Réduit le coût total de possession (CTP) et garanti une exécution globale des politiques dans l'entreprise à travers une gestion unifiée des déploiements sur site et en mode SaaS.
Une prévention haute performance contre la perte de données	Prévient la perte des données sortantes et définit les contrôles de conformité appropriés. Réduit le CTP en évitant les déploiements DLP complexes.
Une classification du contenu en temps réel	Sécurise l'utilisation des sites Web 2.0 dynamiques, protégés par mots de passe et aux contenus variés, à l'aide d'un outil de filtrage de contenu « à la volée ».
Un scanning de sécurité en temps réel	Protège les organisations contre les malwares Web en identifiant les menaces dynamiques, inconnues ou à base de scripts « à la volée ».
Console TRITON	Réduit le CTP et les coûts de gestion des fournisseurs à l'aide de solutions unifiées de sécurité du Web, des données et de la messagerie.
Des anti-virus intégrés	Protège contre les attaques de virus en utilisant la technologie avancée anti-virus de Websense et d'autres solutions tierces.
Les outils leaders de filtrage du Web, avec des fonctions avancées d'analyses de réputation	Permet la mise en place de politiques d'utilisation et le blocage des sites Web corrompus connus ; effectue des analyses de réputation multipoints (type, réputation lexicale, messages publiés sur des sites Web 2.0, réputation de recherche, historique, âge et géographie).
Mises à jour du réseau ThreatSeeker en temps réel	Réduit l'exposition aux menaces émergentes en effectuant des mises à jour de sécurité toutes les 5 minutes.
Visibilité SSL	Permet l'inspection du trafic Web crypté à l'aide de proxys SSL et d'une gestion intégrée des certificats.
Contrôle des applications	Minimise les risques, augmente la productivité et réduit les coûts de bande passante en contrôlant l'utilisation des applications et des protocoles réseau.
Des proxys/caches Web haute performance	Améliore la performance et réduit les coûts de bande passante en optimisant le trafic. Soutient les configurations de proxys transparents et explicites.
Une authentification flexible des utilisateurs	Propose un outil d'authentification flexible aux (groupes d') utilisateurs via Active Directory, LDAP, RADIUS, Novell et NTLM v2.
Haute disponibilité et répartition des charges	Permet la redondance des systèmes et l'évolutivité des grandes entreprises via WCCP ou des répartiteurs de charge externes.

## Disponibilité des plateformes de déploiements

Les déploiements sur site peuvent être effectués avec les appliances V-Series de Websense ou avec des logiciels fonctionnant sur des serveurs classiques. Les déploiements SaaS sont soutenus par notre solution Hosted Web Security Gateway.

- Appliances V-Series** Les appliances Websense® V-Series™ offrent une plateforme haute performance et une grande fiabilité pour les déploiements sur site. Conçues pour répondre aux besoins des plus grandes entreprises, les appliances V-Series intègrent des fonctions de redondance performantes et soutiennent de nombreuses fonctionnalités de déploiements, telles que la répartition des charges et la haute disponibilité. Les appliances V-Series sont capables d'anticiper les futures solutions de Websense, sans mises à jour matériel. La durée de vie et la valeur ajoutée de la plateforme sont ainsi optimisées.

Websense est positionné en tant que leader dans la plus récente publication du Carré Magique de Gartner pour les solutions Secure Web Gateway.

### Gartner, Inc.

“Magic Quadrant for Secure Web Gateway”\* par Peter Firstbrook et Lawrence Orans, 8 Janvier 2010

**Websense, Inc.**  
San Diego, CA USA  
tel +1 800 723 1166  
fax +1 858 458 2950  
www.websense.com

**Websense France**  
Paris  
tel +33 1 56 60 58 14  
fax +33 1 56 60 56 00  
www.websense.fr

**Australie**  
websense.com.au

**Brésil**  
websense.com/brasil

**Colombie**  
websense.com/latam

**Allemagne**  
websense.de

**Hong Kong**  
websense.cn

**Italie**  
websense.it

**Japon**  
websense.jp

**Mexique**  
websense.com/latam

**Chine**  
prc.websense.com

**Espagne**  
websense.com.es

**Taiwan**  
websense.cn

**Royaume-Uni**  
websense.co.uk

- **Hosted Web Security Gateway** de Websense transfère les processus d'inspection de sécurité vers 10 datacenters redondants et disponibles dans le monde entier « in the cloud ». Le modèle SaaS permet non seulement d'accélérer les déploiements mais aussi de réduire les coûts opérationnels de façon significative, en supprimant le besoin de support et de maintenance d'équipement sur les principaux sites des entreprises. Les datacenters Websense sont tous certifiés ISO 27001 et conformes aux plus hauts standards de sécurité et de disponibilité. Une performance très difficile et très coûteuse à égaler pour les organisations multi sites. Proposée en « stand alone » et en mode SaaS, Websense Hosted Web Security Gateway offre également l'intégration d'outils SaaS de sécurité de la messagerie en option.



L'appliance V10000™ de Websense

### Les options de Websense Web Security

**Websense Web Security Gateway Anywhere** — Pour des déploiements nécessitant une gestion sur site\*/SaaS, une prévention haute performance contre la perte de données ou le logiciel client Websense Remote Filtering.

**Websense Web Security Gateway** — Pour des déploiements sur site\*.

**Websense Hosted Web Security Gateway** — Pour des déploiements en mode SaaS.

Spécifications techniques minimum requises :

**Système d'exploitation**

Red Hat Linux v4,  
mise à jour 5\* ou Windows Server 2003/  
Server 2008†

CPU: 2 processeurs Dual-core 2.8GHz

**Mémoire**  
4GB RAM

**Disques durs**

2 disques :

\* 100GB pour système d'exploitation,  
applications et informations temporaires,

100GB de mémoire cache\*

\* 100GB (RAID 1 recommandé)†

**Interfaces réseau**

2 x 10/100/1000 interfaces Ethernet

\* Les déploiements sur site peuvent être effectués sur les appliances V-Series de Websense ou en tant que logiciel fonctionnant sur des serveurs classiques.

\*Le Carré Magique est une représentation graphique du marché à un moment donné. Il expose l'analyse de Gartner sur les performances de plusieurs fournisseurs, en fonction de critères définis par Gartner. Gartner ne soutient aucun vendeur, produit ou service présent dans le Carré Magique et ne conseille pas aux utilisateurs de ces technologies de ne sélectionner que les leaders du Carré. Le Carré Magique est un simple outil d'analyse et non un guide d'achat. Gartner réfute toute notion de garantie, expresse ou implicite, relative à cette étude, notamment toute garantie marchande ou d'adéquation à un usage particulier.

Pour une démonstration en ligne ou une évaluation gratuite de Websense Web Security Gateway : [www.websense.fr](http://www.websense.fr)