



« La perte de données via le Web est 4 fois plus probable que via la messagerie »

Fondation « Data Loss Open Security »

Websense

Solutions de sécurité des données

Réputation ternie, pénalisation financière... les impacts négatifs des violations des données sont éloquentes. Un simple incident de perte de données peut avoir des répercussions importantes sur la compétitivité d'une entreprise et sur la confiance de ses clients. Un problème exacerbé par la prolifération des périphériques mobiles et par la facilité d'accès aux logiciels de partage de fichiers ; deux situations propices à la perte de données. Websense offre des solutions complètes de sécurité des données capables de sécuriser l'information essentielle de votre entreprise en identifiant vos données confidentielles, leur emplacement, leur mode de transmission et la personne qui les utilise.

Principe de fonctionnement

Les solutions de sécurité des données de Websense protègent les organisations contre de nombreux scénarios de perte de données avec une plateforme de politiques unique, pour une meilleure protection contre la perte de données (DLP) sur le réseau et les postes de travail. Une détection précise de l'information confidentielle est également proposée à l'aide de scans effectués en local et sur le réseau.

Les différents modules disponibles dans les solutions de sécurité des données de Websense offrent des fonctionnalités DLP spécifiques pour répondre aux besoins de chaque organisation. La suite Data Security de Websense inclut tous les modules, proposant ainsi une solution

globale. De plus, nous avons incorporé notre technologie DLP haute performance dans nos solutions de sécurité du Web et de la messagerie. Les entreprises bénéficient d'une solution facile à adopter, extensible et performante, pour prévenir les menaces entrantes et gérer les risques associés aux pertes de données et à la conformité réglementaire. Pour commencer, une organisation peut opter pour des outils DLP incorporés dans les solutions Web ou email de Websense ou pour des modules individuels de sécurité des données. Ensuite, il est possible d'évoluer rapidement vers la suite Websense Data Security pour sécuriser les autres canaux de communication et tirer parti de toutes les fonctionnalités de prévention contre la perte de données.

Websense Data Security Suite

Websense Data Security Suite se compose de 4 modules intégrés et gérés à l'aide d'une plateforme de politique de sécurité unique. Cela permet d'obtenir une visibilité et un contrôle plus efficaces de la perte de données sur le réseau et les postes de travail, ainsi qu'une localisation détaillée de l'information à travers les systèmes de stockage.

- **Websense Data Monitor:** contrôle la perte de données sur le réseau (Web, email, FTP ou autres)
- **Websense Data Protect: (qui comprend Websense Data Monitor)** applique des contrôles automatisés de politiques dans le but de protéger, de mettre en quarantaine, de rediriger vers la passerelle d'encryption, de vérifier mais aussi d'alerter les utilisateurs en cas de violation
- **Websense Data Endpoint:** analyse et applique des contrôles automatisés de politiques sur l'information traitée, via les applications et les périphériques installés sur les postes de travail. Localise et hiérarchise les données confidentielles
- **Websense Data Discover:** Localise et hiérarchise l'information essentielle se trouvant dans les répertoires de stockage de l'entreprise. Les options de résolution sont personnalisables et incluent la suppression de fichier

Websense Data Security Suite est la seule solution proposant des outils natifs capables de réguler le Web (HTTP), le Web sécurisé (HTTPS) et la circulation des emails (SMTP). Les solutions de proxy supplémentaires, et coûteuses, deviennent inutiles. Cette suite logicielle s'intègre à n'importe quelle solution de sécurité du Web de Websense, ce qui permet de rediriger le trafic Web sortant vers Websense Data Monitor pour l'analyser.



« Nous n'avons aucune visibilité concernant la sécurité de nos données, jusqu'à la publication du premier rapport de notre solution Websense. »

Roger McIlmoyle

Director of technology services
TLC Vision

Websense Data Monitor

Websense Data Monitor est la solution leader de prévention contre la perte de données réseau. Elle est capable de surveiller et de signaler toute perte d'informations. Alors que les solutions concurrentes se concentrent uniquement sur la nature des données perdues, Websense Data Monitor fournit le contexte permettant d'identifier les informations perdues, ainsi que des renseignements en temps réel sur l'utilisateur et la destination de ces données confidentielles.

Websense Data Monitor propose :

- **Une visibilité inégalée** des applications Web 2.0, incluant une sensibilisation à la destination en temps réel : quelle information est envoyée, où et par qui ?
- **Une identification précise de l'information confidentielle** à l'aide de nombreux outils tels que des modèles prédéfinis de politiques pour les données réglementaires et des empreintes numériques des fichiers utilisés.
- **Une architecture flexible** pour réduire les coûts de déploiement incluant une intégration avec les outils Web Security de Websense.

Websense Data Protect

S'appuyant sur les fonctionnalités de Websense Data Monitor, Websense Data Protect est la solution leader de prévention contre la perte de données réseau. Elle est capable de surveiller et de signaler toute perte d'informations. Avec des contrôles granulaires et automatisés, Websense Data Protect prévient la perte de données sensibles, sans effort et sans intervention humaine.

Websense Data Protect offre :

- **Une mise en application automatisée des politiques** avec options de blocage, mise en quarantaine, suppression des fichiers, encryption, audit/log et notification de l'utilisateur en temps réel.
- **Une plateforme de politiques extensible et performante**, apportant visibilité et contrôle sur l'information confidentielle présente sur votre réseau.
- Les caractéristiques et fonctionnalités de **Websense Data Monitor**.

Websense Data Endpoint

Websense Data Endpoint étend la visibilité et le contrôle des données confidentielles aux postes de travail ; par qui et comment elles sont utilisées ; où elles sont transférées et le type d'action à prendre en temps réel pour prévenir la perte de données au niveau de ces postes de travail. En apportant une visibilité et un contrôle inégalés sur le copier-coller, la capture d'écran, l'impression et le transfert de fichiers vers des supports amovibles, Websense Data Endpoint permet d'appliquer les politiques aux environnements de postes de travail sans charge de travail supplémentaire.

Websense Data Endpoint propose :

- **Une mise en application automatisée**, incluant le blocage, le contrôle et/ou la suppression des applications, l'audit/log, la confirmation et la notification de l'utilisateur.
- **Une visibilité et un contrôle inégalés** sur le copier-coller, l'accès fichier, la capture d'écran et l'impression pour les applications des logiciels clients (y compris les applications au comportement réseau évasif et crypté, comme Skype par exemple), les postes de travail (quelle que soit leur localisation) et les équipements périphériques.
- **Une efficacité opérationnelle**, avec un impact minimum sur les postes de travail et la possibilité de désactiver les services de découverte en cas d'utilisation de l'ordinateur sur batterie.
- **Une identification précise de l'information confidentielle** à l'aide de nombreuses technologies.
- **Découverte et classification** de toute l'information confidentielle sur les postes de travail.

Websense Data Discover

Websense Data Discover est une solution dite « agent-less » capable de scanner à distance des échanges de fichiers réseau spécifiques, des bases de données, des serveurs de messagerie, des répertoires de données et des postes de travail, pour découvrir et classer l'information confidentielle. Les politiques de protection des données sont appliquées automatiquement sur ces systèmes, via des technologies telles que l'encryption, la suppression de fichiers, le remplacement de fichiers, la notification, et l'audit/log des violations.

Websense Data Discover offre :

- **Une découverte et une classification** de l'information confidentielle stockée et connue sur le réseau, à l'aide d'un scanning des adresses IP réputées pour héberger des données confidentielles.
- **Une résolution automatisée** des problèmes liés à l'information confidentielle dans les répertoires de données.
- **Une efficacité opérationnelle**, avec un impact minimum sur la performance des serveurs ; les scans sont effectués en dehors des heures de pointe.
- **Une identification précise de l'information confidentielle** à l'aide de nombreux outils, tels que des modèles prédéfinis de politiques pour les données réglementaires et les empreintes numériques des informations confidentielles.
- **Une plateforme de politiques extensible et performante**, apportant visibilité et contrôle sur toute l'information confidentielle.

Un coût et une complexité réduits

Une couverture globale de sécurité DLP peut engendrer de multiples déploiements de logiciels et d'équipement, ce qui augmente le coût total de la solution et accroît sa complexité. L'exacerbation des coûts et la complication de l'environnement sont les deux principaux challenges des déploiements DLP. Avec les solutions de sécurité des données de Websense, les organisations ont la possibilité de débiter avec une solution DLP modeste, mais performante, telle que Websense Web Security Gateway et d'opter ensuite pour Data Security Suite en fonction de l'évolution de leurs besoins. De plus, Data Security Suite est facile à déployer et à utiliser et peut être opérationnelle en moins d'une heure. La forte capacité d'intégration des solutions de sécurité des données de Websense minimise également l'équipement nécessaire au déploiement d'une telle solution.

Une gestion et un reporting unifiés pour la sécurité du contenu

Les fonctionnalités de gestion et de reporting sont primordiales dans tout déploiement de solution de sécurité. Elles doivent proposer des interfaces faciles d'utilisation et intuitives, et aussi consolider de nombreuses tâches, susceptibles de couvrir de multiples solutions de sécurité. Les solutions de prévention contre la perte de données de Websense sont opérées par notre console TRITON™. Cette console rassemble les fonctionnalités de gestion et de reporting pour les technologies Web, email et DLP en une seule interface Web ; elle apporte ainsi une plus grande visibilité et un meilleur contrôle. La console TRITON inclut 55 rapports prédéfinis, une personnalisation approfondie des fonctionnalités, des assistants intégrés de politique, de nombreux modèles de configuration et d'autres outils innovants pour réduire les coûts et simplifier la gestion des tâches quotidiennes. Que vous souhaitiez déployer Websense Data Security Suite, un des modules de sécurité des données, ou des solutions de sécurité du Web/email, la console TRITON de Websense vous offre un outil de gestion unique pour tous vos besoins de sécurité actuels et futurs.



“Concernant les failles de sécurité internes, les deux tiers sont dues à des actions délibérées, les autres sont involontaires.”

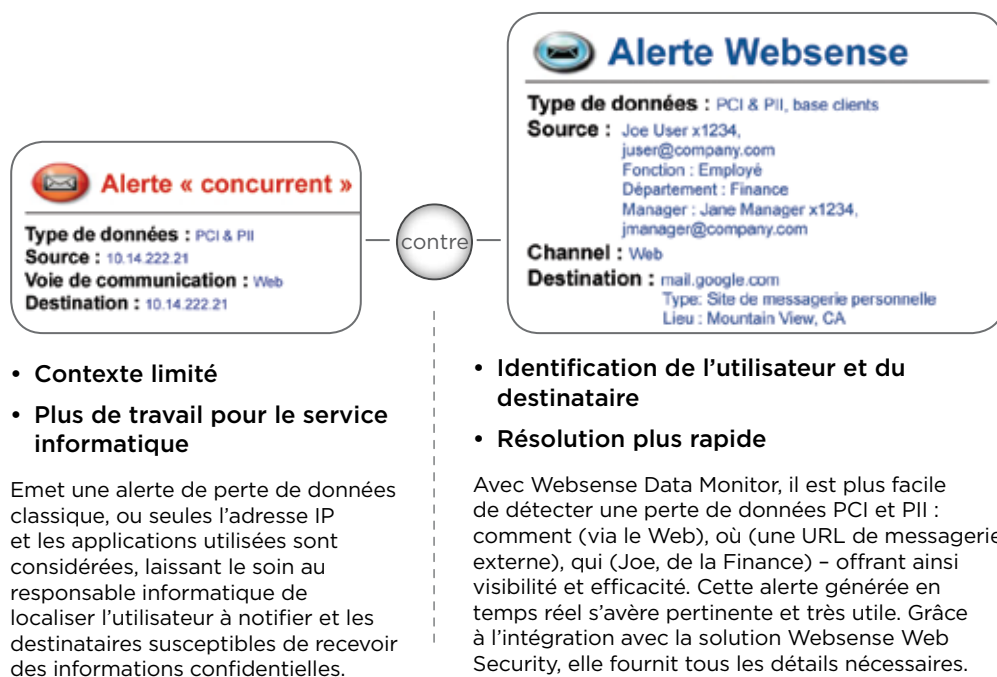
Verizon Business
2009 Data Breach



Visibilité et contrôle avec identification de la destination

“31% des incidents de perte de données signalés sont dus à un vol d'ordinateur portable ou fixe, ou à la disparition d'un autre support.”

Fondation « Data Loss Open Security »



Identification des applications et contrôle des périphériques installés sur les postes de travail

Les employés prennent un risque en copiant des données sur des périphériques de stockage via des applications internes. Si, par exemple, un utilisateur transfère des informations d'une application métier vers un logiciel de messagerie interne, Websense détecte les détails de l'employé et de son poste de travail, les données confidentielles transférées (et leur destination), ainsi que l'application utilisée. Les autres solutions DLP de postes de travail, faute d'offrir une visibilité suffisante pour fournir ce type de renseignements, bloquent parfois des opérations tout à fait légitimes.

Une localisation détaillée pour une résolution rapide

Dès qu'une violation de l'information se produit, un inventaire détaillé des données permet de déterminer les origines possibles de la perte. Websense Data Discover analyse les répertoires de stockage du réseau, afin d'identifier et de classer les informations confidentielles. Une résolution du problème est ensuite initiée (encryption, suppression du fichier...). Un lien direct vers le fichier en question est disponible dans la fenêtre de gestion des incidents. Sont aussi signalés : la catégorie à laquelle appartient l'information détectée (données classiques ou à empreintes numériques), le nom du détenteur du fichier et toutes les actions nécessaires favorisant une résolution rapide de l'incident. Combinée avec Websense Data Endpoint (capable de localiser l'information à l'aide d'un agent logiciel) Websense Data Discover offre des fonctionnalités de localisation détaillées et flexibles, « online » et « offline ».

Caractéristiques	Bénéfices
Mise en application automatisée et en temps réel des politiques sur le réseau, les postes de travail et les répertoires de stockage	<ul style="list-style-type: none"> • Option de mise en application flexible avec notification, identification et vérification de l'utilisateur... • Trafic réseau : mise en quarantaine, blocage, redirection vers une passerelle d'encryption externe, suppression du contenu • Postes de travail : bloque le transfert, le copiage et l'impression des données confidentielles entre des applications et des périphériques externes. Bloque les impressions écran, notifie et effectue un audit des utilisateurs • Localisation : suppression ou déplacement (à l'aide d'autorisations spécifiques et de scripts automatisés), encryptage de l'information stockée (s'appuyant sur la technologie Voltage)

Features	Bénéfices
DLP pour applications SaaS (Security-as-a-Service)	<ul style="list-style-type: none"> • Autorise le téléchargement des données sensibles sur des applications SaaS identifiées et approuvées uniquement • Définit le type d'information qui peut être téléchargé localement, à partir d'applications SaaS
Outils de Smart Detection, pour détecter les données perdues à travers de multiples canaux de communication	<ul style="list-style-type: none"> • Détecte les faibles quantités de données confidentielles envoyées vers de multiples canaux de communication • Détecte de larges volumes d'informations perdues à partir du total des données envoyées au cours d'une période spécifique
Visibilité des différents réseaux à travers un contrôle passif du trafic	<ul style="list-style-type: none"> • Le réseau contrôle le Web (HTTP), le Web sécurisé (HTTPS), les emails (SMTP), la messagerie instantanée (AOL, Yahoo, MSN), FTP, l'impression (agent logiciel OCR en option) et le contenu dynamique Web 2.0 • Réduit les violations de données de 50% avec notification de l'utilisateur
Visibilité des périphériques, applications et répertoires de stockage de données confidentielles, au niveau des postes de travail	<ul style="list-style-type: none"> • Gère les risques de perte de données engendrés par la mobilité des utilisateurs et la mauvaise utilisation de l'information • Localisation : gestion de la mise en application des politiques réseau, « offline » • Portabilité : stockage local des empreintes numériques (avec impact minimal sur la capacité de stockage) • Suivi et contrôle des périphériques de stockage, disques durs externes, impression, graveurs de CD/DVD, copies écran • Contrôle des applications ouvertes par les utilisateurs ou groupes d'utilisateurs (applications prédéfinies ou groupes d'applications) • Classification par type de données (numéros de cartes de crédit...)
Localisation de l'information confidentielle dans les répertoires de stockage locaux et réseau	<ul style="list-style-type: none"> • Localisation détaillée : analyse réseau, analyse locale (via l'agent logiciel du poste de travail), analyse ponctuelle ou programmée • Protection : analyse réseau des bases de données, fichiers partagés, Exchange, SharePoint, analyse locale basée sur le type du fichier, sa taille et son ancienneté • Identification : plus de 400 types de fichiers (Microsoft Exchange PST inclus) ; empreintes numériques de fichiers et modèles prédéfinis de conformité
Identification intégrée des données à l'aide de la technologie brevetée Precise ID™	<ul style="list-style-type: none"> • Identification précise et automatisée des données confidentielles : mots clés, dictionnaires de contenu, empreintes numériques, expressions courantes, seuil d'utilisation maximum, contexte, proximité et corrélation de données structurées ou non (exemple : base de données) • Détection performante : réduit le nombre de faux positifs et les interruptions de fonctionnement de l'entreprise en ignorant les données non conformes aux critères (à l'aide d'empreintes numériques) ou sous un seuil fixé
Options d'installation flexibles, incluant un proxy Web intégré et l'intégration de proxys Web tierces	<ul style="list-style-type: none"> • Intégration Websense Web Security : Redirige le trafic HTTP, HTTPS, FTP pour en permettre l'analyse à l'aide de Websense Data Security, via le protocole ICAP • Aucune autre solution n'est nécessaire : HTTP, SMTP, messagerie instantanée, FTP et HTTPS • Flexible et abordable : (1) mode de contrôle ou de protection, (2) port passby/span ou inline/tap, (3) avec Websense Web Security ou n'importe quel Web Proxy standard, (4) avec Websense Email Security ou n'importe quel MTA compatible SMTP • Efficacité : déclenche des analyses de localisation lorsque le périphérique fonctionne sur secteur (poste de travail) ; hors heures de pointe ; listes d'exception IP pour la localisation réseau • Agent logiciel d'installation poste de travail : Microsoft SMS ou autres méthodes ; évite les conflits avec les outils antivirus, les pare-feu ; installation progressive en fonction des profils d'utilisateurs ; agent logiciel «on/off » • Protection de l'investissement : pour déployer les modules d'une solution en fonction des besoins



« Les solutions Websense nous apportent la plus grande précision du marché, en cherchant automatiquement le contenu dans toute notre organisation et en localisant nos données confidentielles »

Addison Avenue
Federal Credit Union
 Client Websense
 Data Discover

Caractéristiques techniques :

Caractéristiques techniques de Websense Data Security Suite

Voir guide des utilisateurs pour plus d'information

DSS Protector (outil de contrôle)

Ressources système

Voir document de certification hardware pour plus d'information

Fournisseurs certifiés : IBM, HP, Dell,
Moteurs de recherche réseau
Processeur Dual ou « quad core » Intel Xeon 1, 2, 4 GB RAM (mémoire DIM avec tampon total)
Minimum 74 GB, disques durs « hot plug »
NIC 1000/100/10 Mbps

Ressources logiciel (incluses)

Système d'exploitation Linux renforcé avec Websense Data Monitor ou Data Protect

DSS Server (outil de gestion)

Ressources système

Deux processeurs 2.4 GHz Intel, AMD ou autre
4 GB RAM
Quatre disques durs 74 GB, 15K RPM, SCSI U320
RAID 1+0 (minimum)
NIC 1000/100/10

Ressources logiciel

Windows 2003 Server, édition standard R2, nouveau Service Pack

DSS Endpoint (agent logiciel poste de travail)

Ressources système

Pentium 4 @ 1.8ghz ou plus
• Mémoire RAM 512MB minimum avec Windows XP, 1GB RAM avec Windows Vista ou Windows Server 2003
• Espace disque dur requis : 100MB minimum

Ressources logiciel

Systèmes d'exploitation compatibles

- Windows XP (32 bit)
- Windows Vista (32 bit)
- Windows Server 2003 (32 bit)

Références et description

SKU: WDSS-X-XXXX-X

Description : Websense Data Security Suite
Options : nombre de postes de travail, service support, agent logiciel d'imprimante, passerelle de contenu, durée de souscription, ajout de postes de travail (nouveaux, renouvelés ou additionnels).

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

Japon

websense.jp

Brésil

websense.com/brasil

Mexique

websense.com/latam

Colombie

websense.com/latam

Chine

prc.websense.com

Allemagne

websense.de

Espagne

websense.com.es

Hong Kong

websense.cn

Taiwan

websense.cn

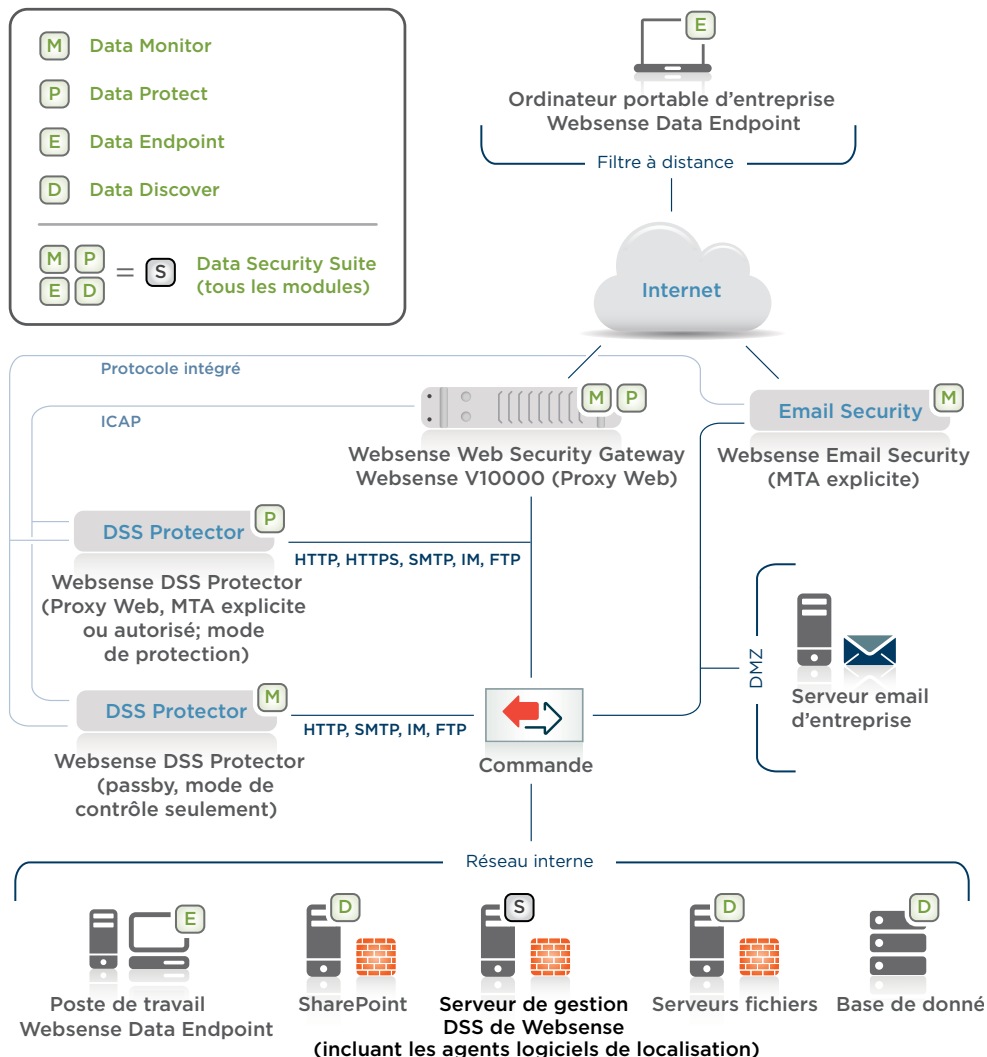
Italie

websense.it

Royaume-Uni

websense.co.uk

Caractéristiques	Bénéfices
Modèles prédéfinis de politiques précis et actualisés, gestion et reporting centralisés des politiques et des incidents	<ul style="list-style-type: none"> • Assistants intégrés disponibles pour faciliter l'utilisation : réglementations nationales (PCI, GLBA, HIPAA, SOX...). Vérifications prédéfinies : PII (données personnelles identifiables), PHI (information médicale personnelle), PCI (données de cartes de crédit), PFI (informations financières personnelles) • Application de politiques cohérentes : réseau, postes de travail, répertoires de stockage • Nous suivons l'évolution des réglementations en permanence et effectuons les mises à jour nécessaires : inutile de dédier une équipe pour le faire • Création de rapports intégrés destinés aux auditeurs et responsables de la société : publication de rapports de conformité non modifiables (PDF) comprenant le nombre total d'incidents par : <ul style="list-style-type: none"> • Réseau : groupe d'utilisateurs, politiques, réglementations en vigueur, mise en application des actions, etc. • Postes de travail : voie de communication des périphériques et applications, groupe d'utilisateurs, politiques, réglementations en vigueur, mise en application des actions, etc. • Localisation : adresse IP, type et nom du répertoire de stockage, données confidentielles (type, fichier spécifique...), détenteur des données, résolution



Pour en savoir plus, pour évaluer les solutions de sécurité des données de Websense, ou pour une démonstration en ligne : www.websense.fr