



“La perdita di dati attraverso il Web è quattro volte più probabile che via e-mail.”

Data Loss Open Security Foundation

Websense

Soluzioni di Data Security

Dai danni alla reputazione del brand fino alle sanzioni vere e proprie, le conseguenze negative causate dai furti di dati sono ormai un dato di fatto. È sufficiente un singolo caso di fuga di dati per erodere il vantaggio competitivo di una azienda, indebolire la fiducia dei clienti ed essere esposti ad ammende da parte delle autorità. Il problema si è ulteriormente intensificato con la rapida diffusione di dispositivi mobili, l'uso sempre più diffuso di periferiche e il facile accesso ai software di file sharing, fenomeni che hanno generato nuove cause di perdita di dati. Websense propone soluzioni complete per la sicurezza dei dati che sono in grado di aiutare le aziende a proteggere i propri dati sensibili, fornendo visibilità su quali dati sono sensibili, dove sono archiviati, come vengono trasmessi e chi li sta usando.

Come funziona?

Le soluzioni Websense® per la sicurezza dei dati forniscono protezione alle organizzazioni contro una vasta gamma di scenari di perdita dei dati, con un unico sistema di policy per attività di Data Loss Prevention (DLP) specifiche per la rete e gli endpoint, oltre a funzionalità di localizzazione dei dati sensibili attraverso sistemi di scansione sulla rete e in locale. Queste soluzioni sono disponibili come moduli singoli o integrate in forma di suite, in modo da fornire il massimo livello di flessibilità di implementazione.

I singoli moduli disponibili nelle soluzioni Websense di data security mettono a disposizione funzionalità specifiche di DLP per rispondere ad ogni tipo di necessità delle aziende. Websense Data Security Suite comprende invece tutti i moduli, per fornire una soluzione onnicomprensiva.

Inoltre, la tecnologia DLP Websense di classe enterprise è stata integrata anche nelle soluzioni di sicurezza Web ed email, per consentire alle organizzazioni di adottare in modo semplice una soluzione espandibile e ricca di funzionalità, in grado sia di prevenire le minacce in ingresso che di gestire i rischi associati alla fuga di dati verso l'esterno, rispettando le normative a riguardo. È possibile partire dalle soluzioni di Data Loss Prevention integrate nelle soluzioni di protezione Web ed email di Websense o dall'implementazione di singoli moduli di sicurezza per i dati. In ogni caso, le aziende possono espandere le loro implementazioni per completare Websense Data Security Suite, in modo da garantire la sicurezza su tutti quanti i canali sfruttando le funzionalità complete di prevenzione della perdita dei dati.

Websense Data Security Suite

La soluzione Websense Data Security Suite comprende quattro moduli integrati, gestiti da un unico sistema di policy, che insieme forniscono visibilità e controllo sulla perdita di dati a livello di rete e di endpoint, oltre a una completa attività di ricerca dei dati lungo i sistemi di storage aziendali.

- **Websense Data Monitor:** controlla la perdita di dati in rete (via Web, e-mail, FTP e altro)
- **Websense Data Protect: (comprende Websense Data Monitor)** attiva controlli automatizzati attraverso l'uso di policy per bloccare, mettere in quarantena, deviare su gateway di codifica, verificare e connettere, o inviare una notifica agli autori delle violazioni
- **Websense Data Endpoint:** effettua il monitoraggio e attiva controlli automatizzati attraverso l'uso di policy sui dati in fase di utilizzo da applicazioni e periferiche di endpoint; è in grado di individuare e classificare localmente i dati sensibili
- **Websense Data Discover:** individua e procede alla classificazione dei dati sensibili conservati negli archivi aziendali, con funzionalità di intervento personalizzabili, compresa la rimozione del file

Websense Data Security Suite è l'unica soluzione progettata per coprire il traffico Web (HTTP), Secure Web (HTTPS) ed email (SMTP), rendendo superfluo l'utilizzo di costose soluzioni Proxy aggiuntive di terze parti. Può essere integrata con qualsiasi soluzione Websense di sicurezza Web, in quanto il traffico Web in uscita è indirizzato al modulo Websense Data Monitor per essere analizzato.



“Non abbiamo alcuna visibilità sulla sicurezza dei nostri dati finché non abbiamo ricevuto il primo report dalla soluzione Websense.”

Roger McIlmoyle

Director of technology services
TLC Vision

Websense Data Monitor

Websense Data Monitor è la più efficace soluzione di Data Loss Prevention per monitorare e avere reportistica sulle fughe di dati. A differenza delle soluzioni di altri produttori che sono focalizzate soltanto su quali dati sensibili sono andati perduti, Websense Data Monitor automaticamente fornisce il contesto per identificare i dati di quali clienti sono stati persi e dettagli in tempo reale su chi sta utilizzando i dati sensibili e dove i dati sono stati inviati.

Websense Data Monitor consente:

- **Visibilità senza confronti** sulle applicazioni Web 2.0, per sapere in tempo reale quali dati sono stati inviati e da chi.
- **Identificazione accurata dei dati sensibili** tramite un set completo di tecnologie, che comprende i modelli di policy per i dati regolati e tecniche di fingerprinting dei dati riservati noti.
- **Architettura flessibile** per diminuire i costi di implementazione, compresa l'integrazione con la soluzione Websense Web security.

Websense Data Protect

Basandosi sulle funzionalità di Websense Data Monitor, Websense Data Protect è la più efficace soluzione di prevenzione della perdita di dati in grado di monitorare e fornire protezione automatica. Grazie a livelli di controllo granulari e automatizzati, Websense Data Protect può aiutare a prevenire la perdita dei dati sensibili, richiedendo meno impegno e manutenzione.

Websense Data Protect mette a disposizione:

- **Applicazione automatica delle policy** con funzionalità di blocco, messa in quarantena, rimozione dei file, cifratura, verifica/segnalazione, invii di notifiche agli utenti in tempo reale.
- **Sistema di policy potente ed espandibile** in grado di fornire visibilità e controllo sui dati sensibili presenti nella rete.
- **Websense Data Monitor**, con le sue funzionalità e potenzialità.

Websense Data Endpoint

Websense Data Endpoint estende, al livello degli endpoint, la visibilità e il controllo su quali sono i dati riservati e che dovrebbero essere salvati; chi li sta utilizzando; come sono utilizzati; dove sono trasferiti e quale azione in tempo reale è eseguita per prevenire la fuga dei dati dall'endpoint. Fornendo visibilità senza confronti e controllo delle operazioni di copia-incolla, print screen, stampa e trasferimento su dispositivi portatili, con Websense Data Endpoint è possibile applicare policy nell'ambiente dell'endpoint con il minimo impatto.

Websense Data Endpoint offre:

- **Applicazione automatica delle policy** comprendente funzionalità di blocco, controllo e rimozione delle applicazioni, verifica/segnalazione, conferma, invii di notifiche agli utenti.
- **Visibilità e controllo senza confronti** su azioni di copia-incolla, accesso ai file, print screen e stampa in applicazioni software per client (comprese le applicazioni con comportamenti in rete di difficile controllo e cifrati, come Skype), endpoint (indipendentemente dalla loro ubicazione) e periferiche.
- **Efficienza operativa** con impatto minimo sugli endpoint, compresa la possibilità di interrompere le attività di localizzazione durante il funzionamento con batteria.
- **Individuazione accurata dei dati sensibili** con un set completo di tecnologie.
- **Localizzazione e classificazione** di tutti i dati sensibili presenti sull'endpoint.

Websense Data Discover

Websense Data Discover è una soluzione agent-less che esegue da remoto scansioni selettive di reti di condivisione file, database, server email, archivi e postazioni desktop per localizzare e classificare i dati sensibili. Consente inoltre di applicare automaticamente le policy di protezione dei dati su questi sistemi tramite una serie di azioni come la cifratura, la rimozione e la sostituzione dei file, la notifica, il controllo e la segnalazione di eventuali violazioni delle policy.

Websense Data Discover offre:

- **Localizzazione e classificazione dei dati riservati** conservati in rete in punti conosciuti, attraverso la scansione di particolari range di indirizzi IP noti per contenere dati riservati.
- **Azioni di compensazione automatiche** su informazioni riservate non protette contenute negli archivi.
- **Efficienza operativa con il minimo impatto sulle prestazioni dei server**, grazie alla possibilità di programmare le scansioni in momenti di scarso traffico.
- **Individuazione precisa dei dati riservati** attraverso un set completo di tecnologie che utilizzano modelli di policy per i dati regolati e tecniche di fingerprinting dei dati riservati noti.
- **Sistema di policy espandibile e potente** in grado di fornire visibilità e controllo su tutti i dati riservati.

Costi più bassi e meno complessità

Una protezione DLP completa può richiedere più implementazioni software e hardware, con un costo da aggiungere alla soluzione generale e l'aumento della complessità. E l'aumento di costi e complessità è la principale sfida a cui deve far fronte la maggior parte delle implementazioni DLP. Con le soluzioni Websense di sicurezza dati, le organizzazioni possono iniziare con una piccola ma efficace soluzione DLP, come Websense Web Security Gateway, quindi passare a Data Security Suite non appena l'azienda cresce e aumentano le esigenze.

Non solo. La soluzione completa Data Security Suite è facile da installare e da gestire, e può essere operativa in meno di un'ora. Le caratteristiche di elevata integrabilità delle soluzioni Websense di sicurezza dei dati, inoltre, riducono al minimo la quantità di hardware necessario per implementare una soluzione completa.

Gestione unificata della sicurezza dei contenuti e reportistica

Le funzionalità di gestione e reportistica sono critiche in qualsiasi soluzione di sicurezza implementata. Non solo devono mettere a disposizione interfacce semplici e intuitive ma devono anche consolidare attività diverse, che talvolta riguardano più soluzioni di sicurezza. Le soluzioni Websense di Data Loss Prevention sono gestite da Websense TRITON™ Console. Si tratta di un pannello di controllo che unisce funzionalità di gestione e reportistica per tecnologie Web, email e Data Loss Prevention in una unica interfaccia Web-based, che permette visibilità e controllo di livello superiore. Sono inclusi oltre 55 report integrati, ampie potenzialità di personalizzazione, procedure guidate per la formulazione di policy, modelli di configurazione e altre innovative funzionalità per ridurre i costi e semplificare enormemente le attività di gestione.

Sia con l'implementazione di Websense Data Security Suite, di uno dei moduli di data security, o delle soluzioni di Web security o email security, la Websense TRITON Console mette a disposizione una unica soluzione di gestione per tutte le esigenze di sicurezza, attuali e future.



“[A proposito di violazioni dei dati], i due terzi sono stati il risultato di un’azione deliberata, gli altri casi sono stati involontari.”

Verizon Business
2009 Data Breach



Visibilità e Controllo attraverso l'identificazione della Destinazione

“Il 31% dei casi di fuga di dati rilevati sono riconducibili a furti di laptop, furti di desktop o dispositivi smarriti.”

DatalossDB

Open Security Foundation



Alert della Concorrenza

Dati: PCI & PII
Fonte: 10.14.222.21
Canale: Web
Destinazione: 10.14.222.21





Alert di Websense

Database: PCI & PII, customer database
Fonte: Joe User x1234,
 juser@company.com
 Titolo: Associate
 Dipartimento: Finance
 Manager: Jane Manager x1234
 jmanager@company.com

Canale: Web
Destinazione: mail.google.com
Tipo: Personal webmail site
Posizione: Mountain View, CA

- Contesto non dettagliato
- Più lavoro per gli amministratori IT

Consideriamo un normale avviso di perdita di dati, in cui sono indicati solo l'indirizzo IP e il canale in cui è stata registrata; al manager IT è lasciato il carico di identificare chi deve essere informato e a quali destinazioni specifiche i dati sensibili sono stati inviati.

- Identificazione dell'utente e destinazione
- Tempi di intervento più veloci

Grazie a Websense Data Monitor è semplice vedere che alcuni dati PCI e PII sono stati persi in un canale Web (**come**), tramite un URL webmail specifico (**dove**), da Joe User del dipartimento Finance (**chi**), il che fornisce visibilità in modo *efficace*. Questo avviso è anche attendibile e può avere valore legale, dato che è generato in tempo reale e fornisce i dettagli del contatto, il ruolo e tutto quanto può essere ottenuto tramite l'integrazione con la soluzione Websense Web Security.

Identificazione dell'applicazione e controllo dei dispositivi sugli Endpoint

I dipendenti possono essere fonte di rischio copiando dati su periferiche di storage da applicazioni locali. Quando un dipendente copia dati da una applicazione aziendale ad un client e-mail in locale, Websense registra questa attività includendo dettagli sull'utente, l'endpoint, i dati sensibili, l'applicazione e la destinazione di questi dati. Le altre soluzioni di DLP per endpoint non garantiscono un livello di visibilità sufficiente su dati e applicazioni, con il rischio di bloccare attività che invece dovrebbero essere consentite.

La ricerca ad ampio spettro permette interventi rapidi

Una volta attestato il furto di dati, un immediato inventario delle informazioni trafugate può essere utile a determinare le possibili cause della perdita. Websense Data Discovery utilizza un sistema di scansione attraverso la rete degli archivi di dati per trovare dati sensibili in punti conosciuti, classificare questi dati, e attivare un'azione di intervento che include la codifica o la rimozione dei file. La visibilità sulla gestione dell'incidente si ha attraverso un link al file specifico, la categoria dell'anomalia del file (dati fingerprinted o regulated), il proprietario del file (l'attribuzione dell'incidente per l'intervento), e ogni azione di intervento che è già stata attivata per gestire la violazione. In caso di utilizzo in aggiunta a Websense Data Endpoint, che individua i dati localmente utilizzando un agente software, la soluzione mette a disposizione funzionalità di ricerca complete e scalabili per entrambi i sistemi online e offline.

Funzionalità	Vantaggi
Attivazione automatizzata e in tempo reale su rete, dispositivi endpoint e archivi di dati riconosciuti.	<ul style="list-style-type: none"> • Opzioni di messa in esecuzione flessibile, tra cui la notifica all'utente, verifica/connessione, e altro ancora • Traffico di rete: quarantena, blocco, deviazione su gateway di codifica di terze parti, rimozione del contenuto • Azioni a livello endpoint: blocco di spostamenti, copia e stampa di dati sensibili da applicazioni verso dispositivi esterni, blocco di screen print, notifica all'utente, conferma/verifica/connessione dell'utente • Ricerca: rimozione o sostituzione (con l'utilizzo di credenziali e script automatizzati), codifica (integrazione di terze parti con la codifica di file Voltage) di dati archiviati

Funzionalità	Vantaggi
DLP per applicazioni Security-as-a-Service (SaaS)	<ul style="list-style-type: none"> • Garantiscono che i dati sensibili siano caricati solo su applicazioni SaaS identificate e approvate • Definiscono la tipologia di dati scaricabili in locale dalle applicazioni SaaS
Funzionalità di Smart Detection per individuare le fughe di dati su più comunicazioni	<ul style="list-style-type: none"> • Individua piccole porzioni di dati riservati inviate su più comunicazioni • Individua grandi quantità di dati in fuga dalla somma dei dati riservati inviati in un periodo di tempo specifico
Visibilità su numerosi canali di rete tramite il monitoraggio del traffico passivo	<ul style="list-style-type: none"> • Monitoraggio via rete sui protocolli Web (HTTP), secure Web (HTTPS), e-mail (SMTP), applicazioni IM (AOL, Yahoo, MSN), FTP, attività di stampa (disponibile la funzionalità opzionale per OCR), contenuti dinamici Web 2.0 • Riduce le violazioni del 50% grazie alla funzionalità di notifica all'utente
Visibilità su dispositivi, applicazioni e archivi di contenuti sensibili su sistemi end user	<ul style="list-style-type: none"> • Gestione del rischio di perdita dei dati dovuto a spostamenti e all'uso non consentito di dati da parte dell'utente • Conoscenza dell'ubicazione: consente l'applicazione di policy dentro e fuori rete e in locale • Portabilità: archiviazione di fingerprint in locale con il minimo impatto sui dispositivi di storage • Monitoraggio e controllo di dispositivi di storage portatili, hard drive esterni, operazioni di stampa, masterizzazione CD e DVD, attività di copia, incolla e screen print sulla clipboard, accesso ai file • Monitoraggio delle applicazioni avviate dall'utente, da gruppi di utenti, applicazioni predefinite o gruppi di applicazioni • Classificazione secondo tipologie di dati regolamentati, come i numeri di carta di credito
Ricerca di dati sensibili su archivi di dati in locale e in rete	<ul style="list-style-type: none"> • Ricerca ad ampio spettro: scansioni di rete, in locale (tramite agenti software endpoint); scansioni ad hoc o programmate • Copertura: scansione via rete di database, file share, Exchange, SharePoint; scansioni in locale basate su tipo di file, dimensione e data • Identificazione: più di 400 tipologie di file, tra cui i PST Microsoft Exchange; funzionalità di file fingerprint, modelli di regolamentazione
Comprende funzionalità di identificazione dei dati attraverso la tecnologia brevettata PrecisID™	<ul style="list-style-type: none"> • Identificazione automatizzata e precisa di dati sensibili: keyword, dizionari, fingerprinting, regular expression, soglia, contesto, prossimità e correlazione per dati strutturati e non (per esempio i database) • Identificazione efficace: riduce i falsi positivi e la business disruption non tenendo conto dei dati se non mappati ai dati del cliente (con l'uso di fingerprint) o se sotto soglie specificate
Opzioni di implementazione flessibile, tra cui proxy Web interno e l'integrazione con proxy Web di terze parti	<ul style="list-style-type: none"> • Integrazione con Websense Web Security: instradamento di traffico HTTP, HTTPS, FTP per l'analisi eseguita da Websense Data Security attraverso il protocollo ICAP • Non occorrono soluzioni aggiuntive: attiva su HTTP, SMTP, applicazioni IM, FTP e HTTPS (con Websense Web Security, per proxy Web) • Flessibile e conveniente: (1) modalità monitoraggio o protezione, (2) porta passby/span o inline/tap, (3) con Websense Web Security o qualsiasi proxy Web standard, (4) con Websense Email Security o qualsiasi MTA compatibile con SMTP • Efficace: programma le scansioni di ricerca quando il sistema non funziona con la batteria (endpoint) e fuori dagli orari di punta; copertura basata su rete ma con prestazioni da agente software; dotato di elenchi delle eccezioni di range IP per le ricerche in rete • Implementazione del software sull'endpoint: SMS Microsoft o altri metodi; assenza di conflitto con antivirus o firewall personali; implementazione su fasi secondo i profili degli utenti; attivazione/disattivazione del software • Protezione dell'investimento: implementazione dei moduli a fasi, secondo le necessità



“[Le soluzioni Websense] forniscono un livello di precisione senza confronti, mettendosi automaticamente alla ricerca di contenuti lungo tutta la nostra azienda e identificando dove sono ubicati i nostri dati sensibili.”

**Addison Avenue
Federal Credit Union**
Websense Data
Discover customer

Specifiche Tecniche:

WebSense Data Security Suite: specifiche tecniche

Consultare il manuale utente per maggiori dettagli

DSS Protector (componente di monitoring)

Risorse di sistema

Consultare il documento *Certified Hardware per maggiori dettagli*

Marchi certificati: IBM, HP, Dell, Network Engines
Processore Intel Xeon dual o quad core
1, 2, 4 GB RAM (fully buffered DIM)
Hard drive hot pluggable da almeno 74 GB
NIC 1000/100/10 Mbps

Risorse Software (includere)

Sistema operativo Hardened Linux con Websense Data Monitor o software Data Protect

DSS Server (componente di gestione)

Risorse di sistema

Due processori Intel 2.4 GHz o AMD o superiori
4 GB RAM
Quattro hard drive 74 GB, 15K RPM, SCSI U320 (minimo) in RAID 1+0
NIC 1000/100/10

Risorse Software

Windows 2003 Server standard R2 edition con Service Pack più recente

DSS Endpoint (agente software end point)

Risorse di sistema

Pentium 4 @ 1.8ghz o superiore
• Almeno 512MB RAM su Windows XP,
• 1GB RAM su Windows Vista o Windows Server 2003
• Almeno 100MB di spazio libero su hard drive

Risorse Software

Sistemi operativi supportati:

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

Codice e descrizione

SKU: WDSS-X-XXXX-X

Descrizione: Websense Data Security Suite
Opzioni: # licenze, supporto, printer agent, content gateway, durata delle licenze, acquisto/rinnovo/ulteriori licenze.

WebSense, Inc.

San Diego, CA USA
tel 800.723.1166
tel 858.320.8000
www.websense.com

WebSense Italy

Milan, Italy
tel +39 02 6203 3040
fax +39 02 6203 4000
www.websense.it

Australia
websense.com.au

Italia
websense.it

Brasile
websense.com/brasil

Giappone
websense.jp

Colombia
websense.com/latam

Malesia
websense.com

Francia
websense.fr

Messico
websense.com/latam

Germania
websense.de

Cina
prc.websense.com

Hong Kong
websense.cn

Singapore
websense.cn

India
websense.com

Spagna
websense.com.es

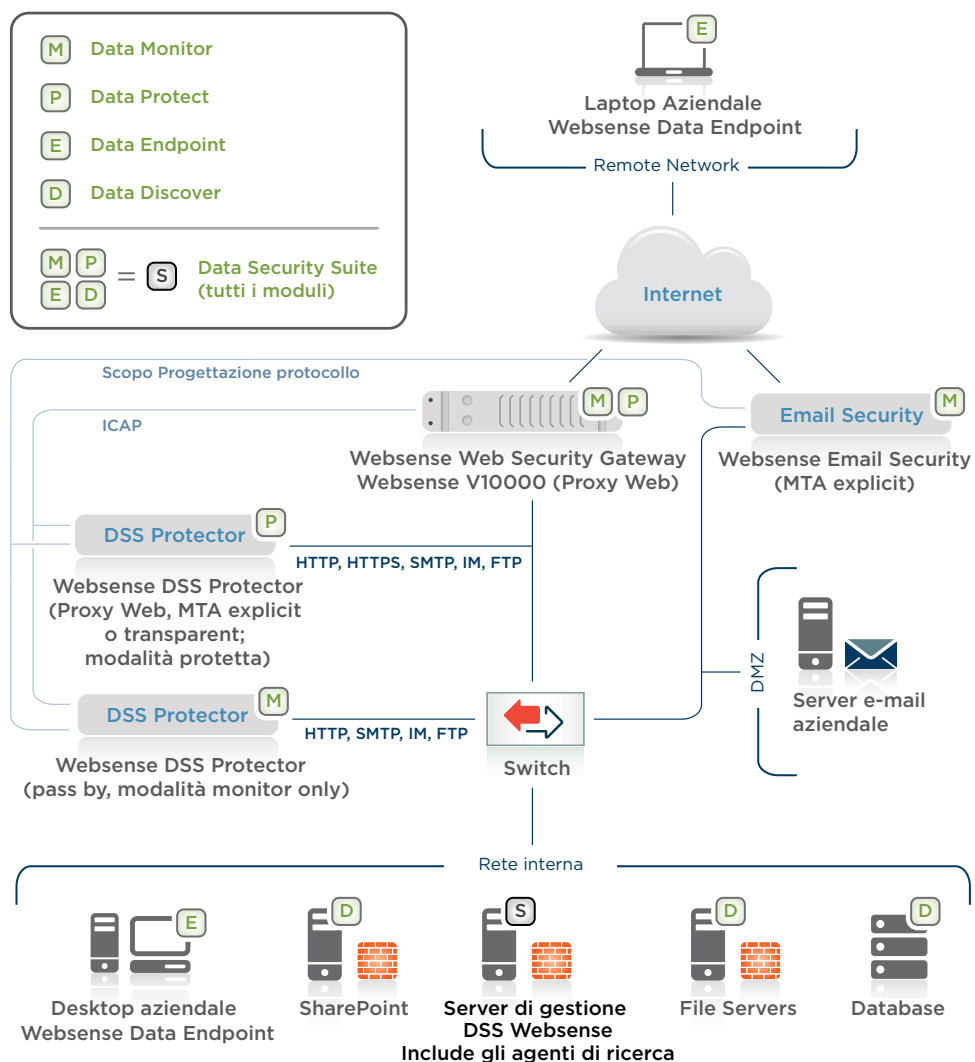
Irlanda
websense.co.uk

Taiwan
websense.cn

Israele
websense.com

UAE
websense.com

Funzionalità	Vantaggi
<p>Template di policy completi e aggiornati, policy centralizzata e gestione e reportistica degli incidenti</p>	<ul style="list-style-type: none"> • Funzionalità integrate per facilitare l'uso: settori, normative regionali (PCI, UK DPA, GLBA, HIPAA, SOX); controlli pre-configurati: PII (personally identifiable Data), PHI (personal healthcare information), PCI (credit card data), PFI (personal financial information). • Permette l'applicazione di policy conformi per la rete, dispositivi endpoint o archivi di dati • Teniamo traccia noi delle normative, al posto tuo: un team dedicato ricerca e aggiorna i template con regolarità • Reportistica integrata per i bilanci e le revisioni aziendali: potrai fornire report in formato non modificabile (PDF) con informazioni sul numero totale di incidenti causati da... • Rete: user group, policy, normativa, attivazione di policy ecc... • Endpoint: canale utilizzato dal dispositivo o dall'applicazione, user group, policy, normativa, procedura mandata in esecuzione ecc... • Ricerca: indirizzo IP, tipologia/nome archivio, dati sensibili (tipologia, file/record specifico), proprietario del dato, azione di intervento



Per una prova gratuita di tutti i prodotti Websense o per seguire le nostre demo online, visita la pagina "Evaluation" del nostro sito www.websense.it