



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

Data Loss Open Security Foundation

Websense Data Security Suite

Dai danni alla reputazione del brand alle sanzioni vere e proprie, le conseguenze negative dei furti di dati sono ormai note a tutti. Il problema si è intensificato con la diffusione dei dispositivi mobili e l'accesso sempre più facile ai software di file sharing, fenomeni che hanno dato origine a nuove cause di perdita di dati. Websense® Data Security Suite è una soluzione di prevenzione dalla perdita di dati in grado di aiutarti a proteggere le informazioni della tua azienda, fornendo visibilità su quali dati sono sensibili, dove e come sono trasmessi e conservati, e chi li sta usando.

Come funziona?

La soluzione Websense Data Security Suite copre molteplici scenari di perdita di dati, con un unico sistema di policy in ambito Data Loss Prevention (DLP) sia di rete che di endpoint, e l'individuazione dei dati sensibili grazie all'utilizzo di scansioni sia in locale che in rete. Si tratta di un approccio modulare, il che

significa che è possibile decidere che cosa implementare secondo le esigenze della propria azienda.

La suite si integra facilmente con i prodotti Websense di sicurezza e-mail e Web, per attivare controlli autonomamente o attraverso l'integrazione di terze parti.

La soluzione Websense Data Security Suite mette a disposizione:

- **Una completa suite di DLP** per identificare, monitorare e proteggere i dati sensibili lungo la rete, sui desktop e i laptop degli utenti e nei dispositivi connessi in rete in cui i dati sono conservati
- **La possibilità di iniziare con uno solo o più moduli** per dotarsi del sistema di DLP più conveniente
- **Visibilità e controllo senza confronti**, grazie al funzionamento automatizzato in tempo reale sulle applicazioni Web 2.0, dove i contenuti dinamici generati dagli utenti aumentano i rischi
- **Identificazione dei dati sensibili in modo semplice e accurato**, attraverso modelli di policy conformi alle normative di settore e funzionalità di fingerprinting dei file
- **Una solida struttura di policy** in grado di fornire visibilità e controllo su chi (i dettagli dell'utente), come (quali applicazioni), dove (le informazioni sulla destinazione) e cosa (quali dati sensibili) sta transitando sulla tua rete
- **Un'architettura flessibile** per ridurre i costi di implementazione, tra cui l'integrazione con le soluzioni di sicurezza Web di Websense e con altri proxy Web

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

La soluzione Websense Data Security Suite è l'unica progettata per coprire il traffico Web (HTTP), Secure Web (HTTPS) e e-mail (SMTP), rendendo superfluo l'utilizzo di costose soluzioni aggiuntive Proxy di terze parti. Può essere integrata con qualsiasi soluzione Websense di sicurezza Web; il traffico Web in uscita è indirizzato al modulo Websense Data Monitor per l'analisi, il quale genera una regola che indica quale soluzione di sicurezza Web deve mandare in esecuzione la policy.



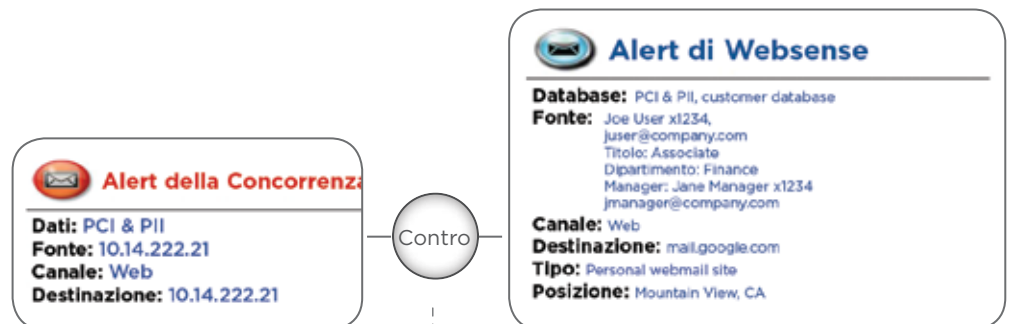
“Non avevamo alcuna visibilità sulla sicurezza dei nostri dati finché non abbiamo ricevuto il primo report dalla soluzione Websense.”

Roger McIlmoyle
Director of technology services, TLC Vision

La soluzione permette visibilità e controllo in tre ambiti:

Area DLP	Copertura Websense	Prodotti Websense
Dati in transito	<p>Visibilità: Web, Secure Web (HTTPS), e-mail, FTP, Instant Messaging, P2P e altro ancora grazie all'identificazione dell'utente e della destinazione sul Web</p> <p>Controllo: attivazione automatizzata e basata su policy con funzionalità di blocco, codifica, quarantena, connessione, notifica all'utente, rimozione del file</p>	Data Monitor Data Protect
Dati in uso	<p>Visibilità: applicazioni client (pre-definite, personalizzate), dispositivi mobili, azioni (copia, incolla, screen print, stampa); ricerca in locale</p> <p>Controllo: attivazione automatizzata e basata su policy con funzionalità di blocco (con l'opzione di helpdesk bypass), connessione, notifica all'utente, rimozione del file</p>	Data Endpoint
Data at Rest	<p>Visibilità: all'interno di database, file shares, Exchange, Share Point tramite ricerca in rete</p> <p>Controllo: attivazione automatizzata e basata su policy con funzionalità di connessione, notifica all'utente, rimozione del file, codifica, modifica dei file permission</p>	Data Discover

Visibilità e Controllo attraverso l'identificazione della Destinazione



- 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/connesione, 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/connesione 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
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 PreciseID™	<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 in tutta la nostra azienda e individuando dove sono ubicati i 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 (include)

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 UK, Ltd.

Reading, Berkshire UK
 tel 0118.938.8600
 fax 0118.938.8697
 www.websense.co.uk

Australia
 websense.com.au

Brasile
 websense.com/brasil

Colombia
 websense.com/latam

Francia
 websense.fr

Germania
 websense.de

Hong Kong
 websense.cn

India
 websense.com

Irlanda
 websense.co.uk

Israele
 websense.com

Italia
 websense.it

Giappone
 websense.jp

Malesia
 websense.com

Messico
 websense.com/latam

Cina
 prc.websense.com

Singapore
 websense.com

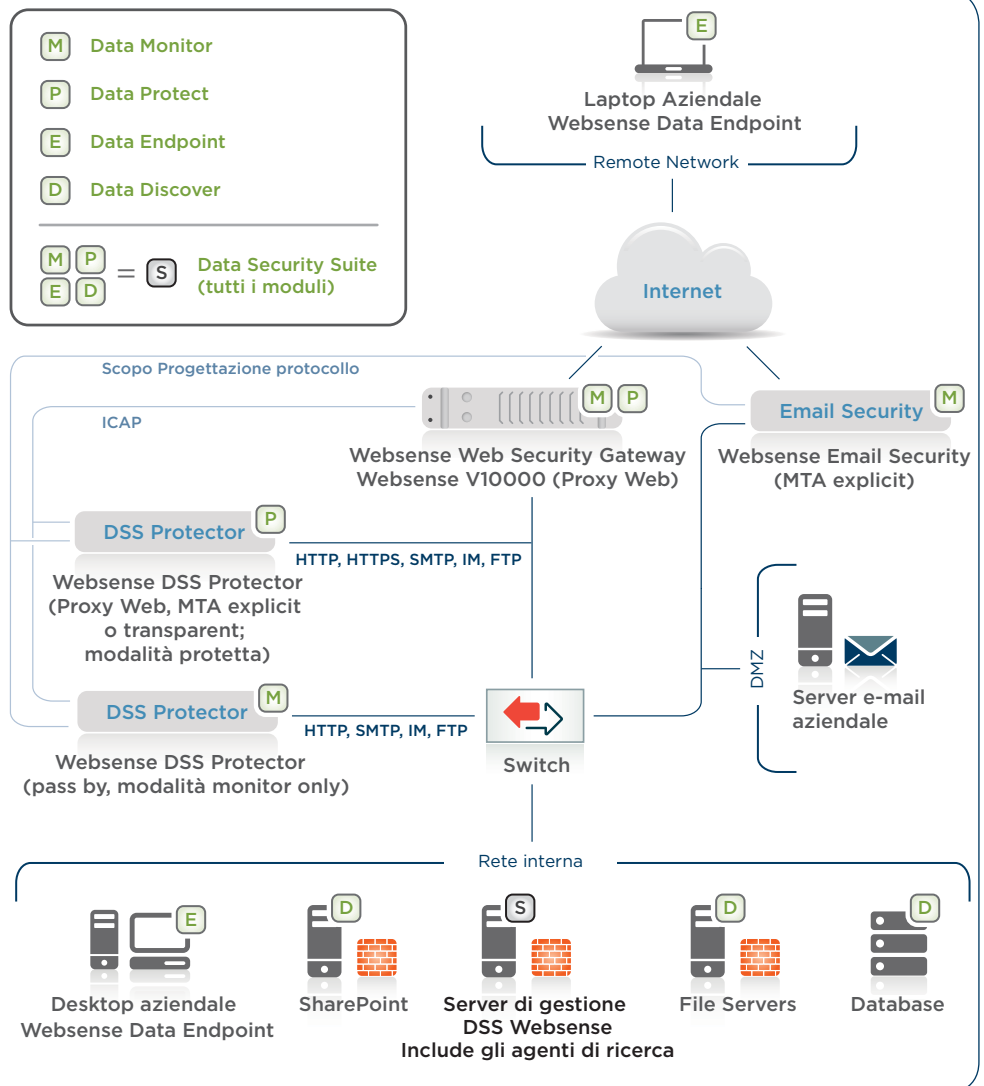
Spagna
 websense.com.es

Taiwan
 websense.cn

UAE
 websense.com

- **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/home archivio, dati sensibili (tipologia, file/record specifico), proprietario del dato, azione di intervento

Template di policy completi e aggiornati, policy centralizzata e gestione e reportistica degli incidenti



Implementazione ottimale di Websense Data Security Suite

Per maggiori informazioni, provare una versione trial gratuita delle soluzioni Web di Websense o visualizzare una demo online, visita il sito www.websense.com/evaluations.