



“Datenverluste  
über das Internet  
sind viermal  
wahrscheinlicher als  
per E-Mail.”

**Data Loss Open  
Security Foundation**

## Websense

# Data Security Suite

Die negativen Auswirkungen von Datenschutzverletzungen sind offensichtlich: Sie reichen von angeschlagener Markenreputationen bis zu Bußgeldern für Regelverletzungen. Verschärft wird das Problem durch mobile Endgeräte und den einfachen Zugriff auf File-Sharing-Software, die das Risiko eines Datenverlusts erhöhen. Websense® Data Security Suite ist eine Data-Loss-Prevention-Lösung, die Ihnen hilft Ihre essentiellen Daten zu schützen. Sie bietet eine Übersicht, wer die Daten verwendet, welche Daten vertraulich sind, wo und wie sie verschickt, verwendet oder gespeichert werden.

### Funktionsweise

Websense Data Security Suite deckt problemlos alle Datenrisikoszenarien mit Hilfe eines einzigen Richtlinien-Frameworks zur Data Loss Prevention (DLP) für Netzwerke und Endpoints sowie zur Erkennung vertraulicher Daten ab. Dabei stützt sie sich sowohl auf lokale als auch auf Netzwerk-Scans. Der Ansatz

ist modular, d. h. Sie können je nach den Unternehmensanforderungen selbst entscheiden, wie Sie sie einsetzen.

Die Suite ist eng in die Websense Web- und E-Mail-Security-Lösungen eingebunden und unterstützt eine integrierte oder über Dritt-Integration erzielte Durchsetzung.

Die Websense Data Security Suite bietet:

- **Eine vollständige DLP-Suite** zur Identifizierung, Überwachung und Schutz vertraulicher Daten im Netzwerk, auf Desktop- und Laptop-Computern von Anwendern und im Netzwerk angebundene Datenspeicher
- **Die Option, mit einem oder mehreren Modulen zu starten**, im Interesse einer kosteneffizienten DLP
- **Beispiellose Übersicht und Kontrolle** mit automatisierter Richtlinienumsetzung in Echtzeit bei Web 2.0 Anwendungen, bei denen dynamischer, usergenerierter Content ein zunehmendes Risiko darstellt.
- **Präzise Identifizierung vertraulicher Daten** mit Vorlagen für Branchen-Richtlinien und File-Fingerprinting
- **Leistungsstarkes Richtlinien-Framework**, das Transparenz und Kontrolle darüber bietet, wer (Informationen über den Anwender), wie (Anwendungen), wo (Destination-Awareness) und was (vertrauliche Daten) in Ihrem Netzwerk überträgt
- **Flexible Architektur** zur Reduzierung von Implementierungskosten einschließlich Integration mit Websense Web Security und andere Web-Proxy-Lösungen

### Die Websense Data Security Suite

Die Websense Data Security Suite umfasst vier – unter einem einzigen Richtlinien-Framework verwaltete – Module, die gemeinsam für die Transparenz und die Kontrolle über Datenverluste im Netzwerk und an Endpoints sowie für eine umfassende Datenerfassung in Enterprise-Speichersystemen sorgen.

- **Websense Data Monitor:** wacht über Datenverluste im Netzwerk (Web, E-Mail, FTP, Sonstige)
- **Websense Data Protect:** (beinhaltet Websense Data Monitor) setzt automatisierte, richtlinienbasierte Kontrollen um und blockiert Daten, verschiebt sie in Quarantäne, routet sie zum Verschlüsselungs-Gateway, überprüft und protokolliert sie oder informiert die Anwender über Richtlinienverstöße
- **Websense Data Endpoint:** überwacht und erzwingt automatisierte, richtlinienbasierte Kontrollen für die Datennutzung durch Anwendungen und Peripheriegeräten an Endpoints und erfasst und klassifiziert vertrauliche Daten
- **Websense Data Discover:** ermittelt und klassifiziert vertrauliche Daten, die in Datenspeichern im Netzwerk vorliegen und generiert individuell anpassbare Maßnahmen, u. a. das Entfernen von Dateien

Die Websense Data Security Suite ist die einzige Lösung mit nativer Richtlinienumsetzung von Web- (HTTP), Secure-Web- (HTTPS) und E-Mail-(SMTP) Traffic. Damit erübrigen sich zusätzliche, kostspielige Proxy-Lösungen von Drittanbietern. Sie ist in jede Websense Web-Security-Lösung integrierbar, die ausgehenden Web-Traffic zur Analyse an den Websense Data Monitor routet und eine Disposition zurücksendet, auf deren Grundlage die Web-Security-Lösung Richtlinien umsetzt.



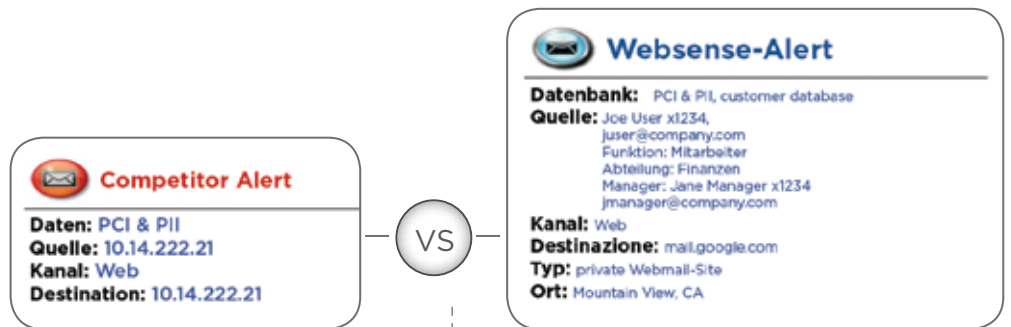
„Unsere Maßnahmen zur Datensicherheit waren völlig intransparent, bis wir den ersten Bericht über die Websense-Lösung erhielten.“

**Roger McIlmoyle**  
Director of technology services, TLC Vision

## Die Lösung bietet Transparenz und Kontrolle in drei Bereichen:

DLP-Bereich	Websense-Absicherung	Websense-Produkte
Data-in-Motion	<p><b>Transparenz:</b> Web, Secure-Web (HTTPS), E-Mail, FTP, IM, P2P und weitere (z. B. mit dem Web verbundene Anwender/Bestimmungsorte)</p> <p><b>Kontrolle:</b> automatisierte, richtlinienbasierte Umsetzung mit Blockierung, Verschlüsselung, Sperrung, Protokollierung, Information der Anwender, Löschen von Dateien</p>	Data Monitor Data Protect
Data-in-Use	<p><b>Transparenz:</b> Kundenanwendungen (vordefiniert, maßgeschneidert), Wechseldatenträger, Aktionen (Kopieren, Einfügen, Bildschirmausgabe, Ausdruck), lokale Erfassung</p> <p><b>Kontrolle:</b> automatisierte, richtlinienbasierte Umsetzung mit Blockierung (mit Helpdesk-Überbrückungsoption), Protokollierung, Information der Anwender, Entfernen von Dateien</p>	Data Endpoint
Data-at-Rest	<p><b>Transparenz:</b> von Datenbanken, File-Sharing, Exchange, Share-Point durch Netzwerk-Erfassung</p> <p><b>Kontrolle:</b> automatisierte, richtlinienbasierte Umsetzung mit Protokollierung, Information der Anwender, Entfernen von Dateien, Verschlüsselung, Änderung von Dateirechten</p>	Data Discover

## Transparenz und Kontrolle durch Destination-Awareness



- Begrenzter Kontext
  - Mehr Aufwand für den IT-Administrator
- Anwender- und Destination-Awareness
  - Abhilfe in kürzerer Zeit

Denken Sie an einen typischen Alert bei Datenverlust, bei dem nur die IP-Adressen und die Anwendungskanäle angegeben werden und so dem IT-Manager die Arbeit aufgebürdet wird, zu bestimmen, wer zu benachrichtigen ist und welche besonderen Bestimmungsorte vertrauliche Daten erhalten sollen.

Websense Data Monitor bietet effiziente Transparenz. Die Lösung erkennt, dass PCI- und PII-Daten über einen Internetkanal (wie), über eine bestimmte Webmail-URL (wo) und durch „Anwender xy“ in der Abteilung Finanzen (wer) verloren gingen. Der Alarm erfolgt in Echtzeit und liefert Kontaktdaten, Funktion und alle anderen Informationen, die dank der Integration in Websense Web Security übergeben werden.

## Application-Awareness und Device-Kontrolle an Endpoints

Risiken entstehen dadurch, dass Mitarbeiter Daten von lokalen Anwendungen auf periphere Speichergeräte kopieren. Wenn ein Mitarbeiter Daten von einer Business-Anwendung in eine E-Mail-Software kopiert, meldet Websense diesen Vorgang mit detaillierten Angaben zu Anwender und Endpoint, zu den vertraulichen Daten sowie der Anwendung und dem Ort dieser Daten. Andere DLP-Lösungen für Endpoints machen Anwendungen und Daten nur unzureichend transparent und blockieren Funktionen, die durchaus auch legitime Geschäftsaktivitäten sein können.

## Umfassende Erfassung ermöglicht effiziente Abhilfemaßnahmen

Sobald ein Verstoß gegen den Datenschutz erfolgt ist, lassen sich mit Hilfe eines aktuellen Bestandsverzeichnisses dieser Daten die möglichen Ursachen des Datenverlustes ermitteln. Websense Data Discover nutzt einen Netzwerk-Scan der Daten-Repositorys, um vertrauliche Daten an bekannten Speicherorten zu finden, sie zu klassifizieren und Maßnahmen wie Verschlüsselung und Entfernen der Datei einzuleiten. Die Incident-Management-Übersicht umfasst einen Link zu der betreffenden Datei, die Kategorie, in die diese Daten fallen (regulierte oder Fingerprint-Daten), den Dateibesitzer (zur Markierung des Vorfalls für Gegenmaßnahmen) sowie jede Maßnahme, die bereits umgesetzt wurde, um gegen den Verstoß vorzugehen. Wird diese Lösung zusammen mit Websense Data Endpoint zur lokalen Ermittlung der Daten mit Hilfe eines Software-Agenten eingesetzt, bietet sie eine umfassende, skalierbare Erfassung in Online- und Offline-Systemen.

Funktionen	Vorteile
Optionen zur automatisierten Richtlinienumsetzung in Echtzeit im Netzwerk, an Endpoints und erfassten Daten-Repositories	<ul style="list-style-type: none"> <li>• <b>Flexible Umsetzungsoptionen</b> mit Information der Anwender, Überprüfung/Protokoll usw.</li> <li>• <b>Netzwerk-Traffic:</b> Verschiebung in Quarantäne, Blockierung, Routen zum Verschlüsselungs-Gateway von Drittanbietern, Entfernen von Content</li> <li>• <b>Endpoint-Aktivität:</b> blockweise Verschiebung/Kopie/Ausdruck vertraulicher Daten von Anwendungen zu externen Geräten, blockweise Bildschirmausgabe, Anwender-Information, Anwender-Bestätigung/Überprüfung/Protokollierung</li> <li>• <b>Erfassung:</b> Entfernen oder Ersetzen (mit Hilfe von Credentials und automatisierten Skripten), Verschlüsselung (Integration in Drittanbieter-Dateiverschlüsselung Voltage) gespeicherter Daten</li> </ul>
Transparenz zahlreicher Netzwerkkanäle durch passives Traffic-Monitoring	<ul style="list-style-type: none"> <li>• <b>Netzwerk-Monitoring</b> Web (HTTP), Secure-Web (HTTPS), E-Mail (SMTP), IM (AOL, Yahoo, MSN), FTP, Ausdruck (optionaler OCR-Agent), dynamischer Web 2.0 Content</li> <li>• <b>Die Zahl der Verstöße reduziert</b> sich um 50 Prozent, wenn die Anwender über Verstöße informiert werden</li> </ul>
Transparenz in Bezug auf Gerät, Anwendung und Speicherung vertraulicher Dateninhalte auf Endanwender-Systemen	<ul style="list-style-type: none"> <li>• <b>Verwaltet das Risiko von Datenverlusten</b> aufgrund von Anwender-Mobilität und Datenmissbrauch</li> <li>• <b>Location-Awareness:</b> Richtlinienanwendung „on/off network“, offline</li> <li>• <b>Portabilität:</b> lokale Fingerabdruckspeicherung mit minimalem Speicherplatzbedarf</li> <li>• <b>Device Monitoring und Kontrolle von Wechseldatenträgern,</b> externen Festplatten, Ausdrucken, Brennen auf CDs/DVDs, Kopieren / Einfügen / Bildschirmausgabe in Zwischenablage, Dateizugriffen</li> <li>• <b>Anwendungs-Monitoring wird ausgelöst durch Anwender, Anwender-Gruppe, vordefinierte Anwendung oder Anwendungsgruppen</b></li> <li>• <b>Klassifizierung nach regulierten</b> Datentypen wie Kreditkartennummern</li> </ul>
Erfassung vertraulicher Daten in lokalen und Netzwerk-Daten-Repositories	<ul style="list-style-type: none"> <li>• <b>Umfassende Erfassung:</b> Netzwerk-Scans, lokale Scans (<b>über Endpoint-Softwareagenten</b>), Ad-hoc-Scans oder geplante Scans</li> <li>• <b>Absicherung:</b> netzwerkbasierter Scan von Datenbanken, File Sharing, Exchange, Share-Point; lokaler Scan nach Dateityp, -größe und -alter</li> <li>• <b>Erfassung:</b> über 400 Dateitypen, einschließlich Microsoft Exchange PSTs; Datei-Fingerprints, Compliance-Vorlagen</li> </ul>
Integrierte Datenerfassung mit Hilfe patentierter Precise ID™-Technologien	<ul style="list-style-type: none"> <li>• <b>Automatisierte, präzise Erfassung vertraulicher Daten:</b> Keywords, Wörterbücher, Fingerprinting, reguläre Ausdrücke, Schwellenwerte, Kontext, Proximität und Korrelation bei unstrukturierten oder strukturierten Daten (z. B. Datenbank)</li> <li>• <b>Effektive Erkennung:</b> Reduziert False Positives und Betriebsstörungen durch Nichtbeachtung von Daten, wenn sie Kundendaten nicht (durch Fingerprints) zugeordnet werden können oder den festgelegten Schwellenwert unterschreiten</li> </ul>
Flexible Einsatzmöglichkeiten, u.a. integrierter Web-Proxy und Integration von Web-Proxys von Drittanbietern	<ul style="list-style-type: none"> <li>• <b>Integration von Websense Web Security:</b> Routet den HTTP-, HTTPS-, FTP-Traffic zur Analyse durch die Websense Data Security über ICAP-Protokoll</li> <li>• <b>Keine Zusatzlösungen notwendig:</b> HTTP, SMTP, IM, FTP und HTTPS (mit Websense Web Security, für Web-Proxy)</li> <li>• <b>Flexibel und kostengünstig:</b> (1) Monitor- oder Schutzmodus, (2) Überbrückung/Span-Port oder Inline/Tap, (3) mit Websense Web Security oder einem beliebigen Web-Proxy, (4) mit Websense Email Security oder einem beliebigen SMTP-konformem MTA</li> <li>• <b>Leistungsfähigkeit:</b> Planung von Erfassungs-Scans, wenn das System nicht von einem Akku gespeist wird (Endpoint); in aktivitätsarmen Zeiten; netzwerkbasierter (Anwendungsbereich) oder agentenbasiert (Performance); Ausnahmelisten im IP-Bereich zur Netzwerkerfassung</li> <li>• <b>Einsatz des Endpoint-Agenten:</b> Microsoft SMS oder andere Verfahren; Vermeidung von Konflikten mit Antivirenprogramm, privaten Firewalls; schrittweiser Einsatz mit Anwender-Profilen; Aktivierungs-/Deaktivierungsagent</li> <li>• <b>Investitionsschutz:</b> schrittweiser Einsatz der Module nach Bedarf</li> </ul>



„[Websense-Lösungen] bieten eine branchenweit führende Präzision, sie durchsuchen automatisch Content in unserem gesamten Unternehmen und ermitteln, wo sich unsere sensiblen Daten befinden.“

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

## Technische Daten:

### Websense Data Security Suite, Technische Daten

Detaillierte Informationen finden Sie im Anwender-Handbuch

#### DSS Protector (Monitoring-Komponente)

##### Systemressourcen

Detaillierte Informationen finden Sie im Dokument über zertifizierte Hardware

Zertifizierte Anbieter: IBM, HP, Dell, Network Engines  
 Duale oder Quad-Core Intel Xeon-Prozessoren  
 1, 2, 4 GB RAM (voll gepufferte DIMM-Speicher)  
 Mindestens 74 GB, Hot-Plug-fähige Festplatten  
 NIC 1000/100/10 Mbps

#### Software-Ressourcen (im Lieferumfang enthalten)

Abgesichertes Linux-Betriebssystem mit der Software Websense Data Monitor oder Data Protect

#### DSS Server (Management-Komponente)

##### Systemressourcen

Zwei 2.4 GHz Intel oder AMD Prozessoren oder besser  
 4 GB RAM  
 Vier 74 GB, 15K RPM, SCSI U320 Festplatten (mindestens) in RAID 1+0  
 NIC 1000/100/10

#### Software-Ressourcen

Windows 2003 Server Standard R2 Edition, neuester Service-Pack

#### DSS Endpoint (Endpoint-Softwareagent)

##### Systemressourcen

Pentium 4 @ 1.8 Ghz oder höher  
 • Mindestens 512 MB RAM bei Windows XP, 1 GB RAM bei Windows Vista oder Windows Server 2003  
 • Freier Festplattenspeicher von mindestens 100 MB

#### Softwareressourcen

Unterstützte Betriebssysteme

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

#### Teilenummern und Beschreibung

SKU: WDSS-X-XXXX-X

Beschreibungen: Optionen von Websense Data Security Suite: Anzahl der Arbeitsplätze, Support, Drucker-Agent, Content-Gateway, Subskriptionsdauer, neue/verlängerte/zusätzliche Arbeitsplätze.

#### 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

#### Australien

websense.com.au

#### Italien

websense.it

#### Brasilien

websense.com/brasil

#### Japan

websense.jp

#### Kolumbien

websense.com/latam

#### Malaysia

websense.com

#### Frankreich

websense.fr

#### Mexiko

websense.com/latam

#### Deutschland

websense.de

#### China

prc.websense.com

#### Hong Kong

websense.cn

#### Singapur

websense.com

#### Indien

websense.com

#### Spanien

websense.com.es

#### Irland

websense.co.uk

#### Taiwan

websense.cn

#### Israel

websense.co.uk

#### UAE

websense.com

#### • Integrierte Assistenten erleichtern die Anwendung:

Branchen- bzw. regionale Regelungen (z. B. PCI, UK DPA, GLBA, HIPAA, SOX); vordefinierte Kontrollen: PII (personenbezogene Daten), PHI (persönliche Gesundheitsdaten), PCI (Kreditkartendaten), PFI (persönliche finanzielle Daten).

#### • Anwendung konsistenter Richtlinien: Netzwerk, Endpoint, Daten-Repositorys

• Wir aktualisieren stets die Regelungen, damit Sie keine speziellen Nachforschungen und keine regelmäßigen Updates der Vorlagen vornehmen müssen

#### • Integrierte Reports für Prüfer und leitende Angestellte:

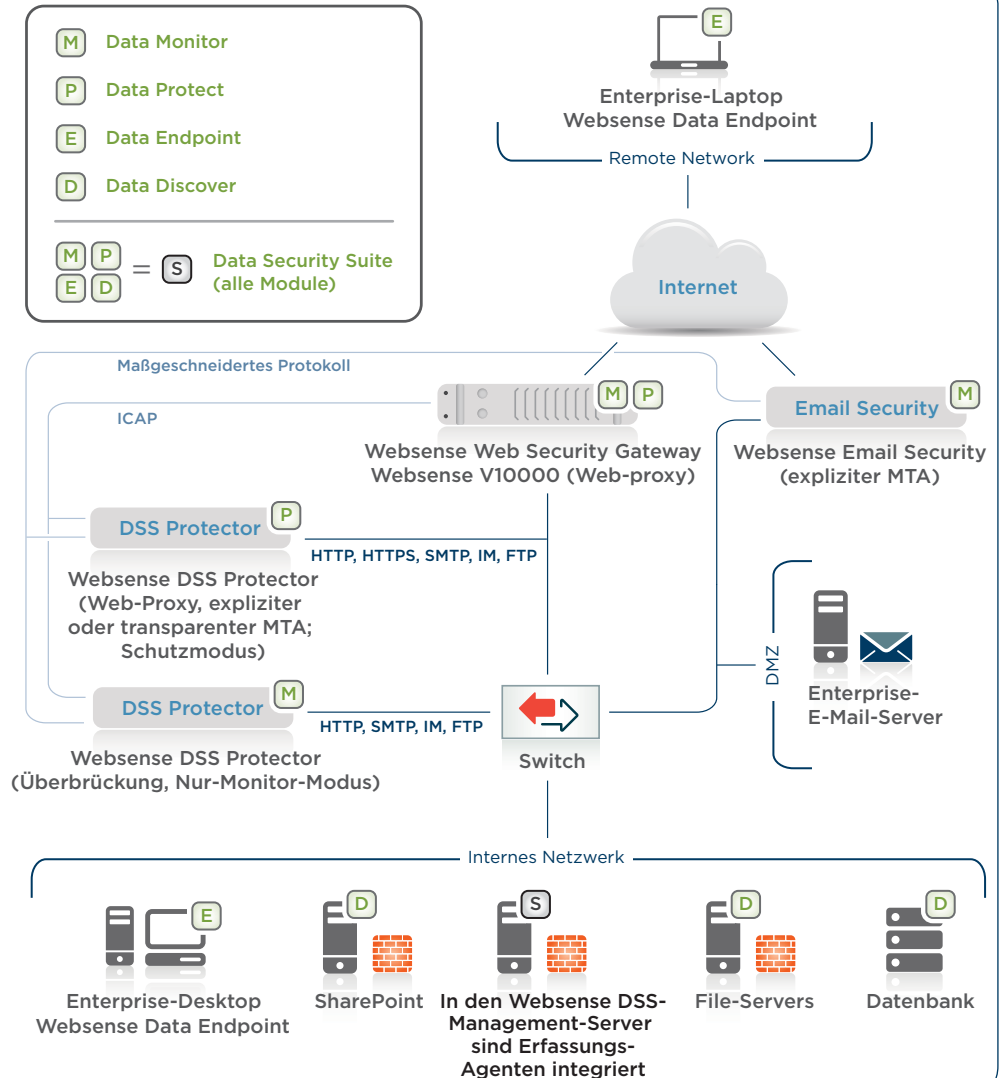
Versand von fälschungssicheren (PDF) Compliance-Reports mit Informationen über die Gesamtzahl der Vorfälle nach ...

• **Netzwerk:** Anwender-Gruppe, Richtlinie, Regelung, Umsetzungsaktion usw.

• **Endpoint:** Geräte-/Anwendungskanal, Anwender-Gruppe, Richtlinie, Regelung, durchgeführte Umsetzungsaktion usw.

• **Erfassung:** IP-Adresse, Repository-Typ/-Name, vertrauliche Daten (Typ, spezifischer File/Datensatz), Dateneinhaber, Abhilfemaßnahme

Umfassende und aktuelle Richtlinien-Vorlagen, zentralisiertes Richtlinien- und Vorfall-Management und Reporting



Optimaler Einsatz der Websense Data Security Suite

Weitere Informationen, eine kostenlose Testversion von Websense Internetlösungen und eine Online-Demo finden Sie unter [www.websense.com/evaluations/Default.aspx?l=de](http://www.websense.com/evaluations/Default.aspx?l=de)