



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

Data Loss Open
Security Foundation

Websense

Data Security-Lösungen

Die negativen Auswirkungen von Datenschutzverletzungen sind offensichtlich: Sie reichen von angeschlagener Markenreputation bis hin zu behördlich auferlegten Geldbußen. Ein einzelnes Datenleck kann die Wettbewerbsvorteile eines Unternehmens untergraben, das Vertrauen der Kunden schwächen und zur Auferlegung von Bußgeldern oder Strafzahlungen durch Behörden führen. Das Problem wird durch die schnelle Ausbreitung mobiler Computer, den verbreiteten Gebrauch von externen Geräten und den einfachen Zugriff auf File-Sharing-Software verschärft – alle diese Faktoren erhöhen das Risiko von Datenverlusten. Websense bietet umfassende Data-Security-Lösungen, mit denen Sie ihre essenziellen Daten schützen können. Die Software macht transparent, welche Daten vertraulich sind, wo diese gespeichert werden, wie sie übertragen werden und wer sie verwendet.

Funktionsweise

Die Data-Security-Lösungen von Websense® schützen Organisationen in unterschiedlichsten Situationen, in denen Daten verloren gehen können. Dabei kommt ein einheitliches Richtlinien-Framework für Data Loss Prevention (DLP) im Netzwerk und an den Endpoints sowie für die Datenerfassung durch lokale und Netzwerkscans zur Anwendung. Diese Lösungen sind als Einzelmodule oder in einer integrierten Suite erhältlich, mit der Sie bei der Bereitstellung den höchstmöglichen Grad an Flexibilität gewinnen.

Die in Data-Security-Lösungen von Websense verfügbaren Einzelmodule bieten spezifische DLP-Funktionen, die die besonderen Anforderungen von Organisationen abdecken. Die Websense

Data Security Suite enthält sämtliche Module und bietet daher die umfassendste Lösung. Zudem ist unsere hochleistungsfähige DLP-Technologie in unsere Web- und E-Mail-Security-Lösungen integriert. So können Organisationen ganz einfach eine erweiterbare und vollständige Lösung implementieren, um externe und interne Bedrohungen in Bezug auf Datenverlust und Compliance abzuwehren. Egal, ob Sie mit den in die Web- oder E-Mail-Lösungen von Websense integrierten Data-Loss-Prevention-Lösungen oder mit einzelnen Data-Security-Modulen beginnen: Sie können jederzeit rasch ein Upgrade auf Websense Data Security Suite durchführen, um weitere Kanäle zu schützen sowie die vollständigen Data-Loss-Prevention-Funktionen zu nutzen.

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

Websense Data Security Suite ist die einzige Lösung mit nativer Durchsetzung von Richtlinien bei Web- (HTTP-), gesichertem Web- (HTTPS-) und E-Mail- (SMTP-) Datenverkehr. So benötigen Sie keine teuren zusätzlichen Proxy-Lösungen von Drittanbietern. Die Software kann in jede Websense Web-Security-Lösung integriert werden, die ausgehenden Web-Datenverkehr zur Analyse an Websense Data Monitor weiterleitet.



„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

Websense Data Monitor

Websense Data Monitor ist die führende Data-Loss-Prevention-Lösung für Netzwerke, die Datenverluste erkennt und meldet. Anders als Lösungen von Wettbewerbern, bei denen lediglich erkannt wird, welche vertraulichen Daten verloren gehen, stellt Websense Data Monitor automatisch den Kontext zum Identifizieren der verloren gegangenen Kundendaten und darüber hinaus Echtzeitinformationen dazu bereit, wer die vertraulichen Daten verwendet und wohin die Daten übertragen werden.

Websense Data Monitor bietet:

- **Unerreichte Transparenz** von Web-2.0-Anwendungen, u. a. durch Echtzeit-Zielerkennung (welche Daten, welches Ziel und durch wen)
- **Präzise Erkennung von vertraulichen Daten** durch umfassende Technologien, u. a. Richtlinienvorlagen für regulierte Daten und Fingerabdrücke bekannter vertraulicher Daten
- **Flexible Architektur**, die die Bereitstellungskosten senkt; dazu gehört die Integration in Websense Web Security

Websense Data Protect

Websense Data Protect beruht auf den Funktionen von Websense Data Monitor und stellt die führende Data-Loss-Prevention-Lösung für Netzwerke dar, die Datenverluste erkennt und automatisch vor diesen schützt. Durch detaillierte und automatisierte Kontrollstufen trägt Websense Data Protect bei geringerem Verwaltungsaufwand und weniger manuellen Eingriffen dazu bei, den Verlust vertraulicher Daten zu vermeiden.

Websense Data Protect bietet:

- **Automatisierte, richtlinienbasierte Durchsetzung** mit Blockierung, Quarantäne, Löschung von Dateien, Verschlüsselung, Prüfung/Protokollierung und Anwenderbenachrichtigung in Echtzeit
- **Erweiterbares und leistungsfähiges Richtlinien-Framework**, das Transparenz und Kontrolle über vertrauliche Daten im Netzwerk sicherstellt
- **Funktionen und Merkmale** von **Websense Data Monitor**

Websense Data Endpoint

Mit Websense Data Endpoint stellen Sie auch an den Endpoints Transparenz und Kontrolle darüber bereit, welche Daten als vertraulich gelten, wie diese gespeichert werden, wer sie verwendet, wie sie verwendet werden, wohin sie übertragen werden und welche Maßnahme in Echtzeit ergriffen wird, um Datenverluste am Endpoint zu verhindern. Durch unerreichte Transparenz und Kontrolle über das Kopieren/Einfügen, Bildschirmabzüge, Druckvorgänge und die Übertragung auf Wechselmedien können Richtlinien mit Websense Data Endpoint bei minimalem Verwaltungsaufwand in der Endpoint-Umgebung durchgesetzt werden.

Websense Data Endpoint bietet:

- **Automatisierte Durchsetzung**, darunter Blockierung, Anwendungskontrolle/-entfernung, Prüfung/Protokollierung, Bestätigung, Anwenderbenachrichtigung
- **Unerreichte Transparenz und Kontrolle** über Kopieren/Einfügen, Dateizugriffe, Bildschirmabzüge und Druckvorgänge für Client-Softwareanwendungen (darunter Anwendungen mit ausweichendem Netzwerkverhalten und Verschlüsselung, z. B. Skype), Endpoints (unabhängig von deren Standort) sowie Peripheriegeräte
- **Betriebliche Effizienz** bei minimalen Auswirkungen auf den Endpoint mit Optionen zum Deaktivieren der Erfassung im Batteriebetrieb
- **Präzise Erkennung von vertraulichen Daten** durch umfassende Technologien
- **Erfassung und Klassifizierung** aller vertraulichen Daten am Endpoint

Websense Data Discover

Websense Data Discover ist eine Lösung ohne Agenten für Remote-Scans angegebener Dateifreigaben, Datenbanken, E-Mail-Server, Daten-Repositorys und Desktops im Netzwerk. Dabei werden vertrauliche Daten erfasst und klassifiziert. Die Richtlinien zum Datenschutz werden in diesen Systemen automatisch durch unterschiedliche Maßnahmen durchgesetzt, u. a. Verschlüsselung, Löschung von Dateien, Ersetzung von Dateien, Benachrichtigungen, Prüfungen und Protokollierung von Richtlinienverletzungen.

Websense Data Discover bietet:

- **Erfassung und Klassifizierung vertraulicher Daten** an bekannten Orten im Netzwerk durch Scannen von angegebenen IP-Adressbereichen, in denen bekanntermaßen vertrauliche Daten gespeichert sind
- **Automatisierte Abhilfemaßnahmen** für nicht geschützte vertrauliche Daten in Daten-Repositorys
- **Betriebliche Effizienz bei minimalen Auswirkungen auf die Serverleistung** durch Planung der Scans für Zeiten mit geringem Datenverkehrsaufkommen
- **Präzise Erkennung von vertraulichen Daten** durch umfassende Technologien, u. a. Richtlinienvorlagen für regulierte Daten und Fingerabdrücke bekannter vertraulicher Daten
- **Erweiterbares und leistungsfähiges Richtlinien-Framework**, das Transparenz und Kontrolle über alle vertraulichen Daten sicherstellt

Geringere Kosten und Komplexität

Eine umfassende DLP-Security-Abdeckung kann sich auf mehrere Software- und Hardware-Bereitstellungen stützen, wodurch die Gesamtkosten der Lösung und deren Komplexität steigen. Dieser Anstieg bei Kosten und Komplexität stellt in den meisten DLP-Bereitstellungen die größte Herausforderung dar. Mit den Data-Security-Lösungen von Websense können Organisationen mit einer kleinen, aber wirksamen DLP-Lösung beginnen, z. B. Websense Web Security Gateway, und bei expandierender Organisation und gestiegenen Anforderungen auf Data Security Suite aufrüsten. Darüber hinaus kann die komplette Data Security Suite sehr einfach bereitgestellt und verwaltet werden – meist dauert die Inbetriebnahme weniger als eine Stunde. Zudem bedeuten die Integrationsfähigkeiten der Websense Data-Security-Lösungen, dass eine umfassende Lösung weniger Hardware für die Bereitstellung benötigt.

Einheitliche Verwaltung und Berichterstellung für Content-Security

Die Verwaltungs- und Berichterstellungsfunktionen sind für jede Security-Lösung von zentraler Bedeutung. Zu den Anforderungen zählt nicht nur eine einfache, intuitiv zu erfassende Anwenderoberfläche – es müssen auch zahlreiche Aufgaben integriert werden, die sich bisweilen auf mehrere Security-Lösungen erstrecken. Data-Loss-Prevention-Lösungen von Websense werden mit der Websense TRITON™-Konsole verwaltet. Diese Konsole vereint die Verwaltungs- und Berichterstellungsfunktionen der Web-, E-Mail- und Data-Loss-Prevention-Technologien unter einer webbasierten Oberfläche. Für Sie bedeutet das größere Transparenz und bessere Kontrolle. In der Konsole sind mehr als 55 integrierte Berichte verfügbar, und umfassende Anpassungsmöglichkeiten, Richtlinienassistenten, Konfigurationsvorlagen und weitere innovative Funktionen tragen zur Kostensenkung und starken Vereinfachung der Verwaltungsaufgaben bei. Unabhängig davon, ob Sie Websense Data Security Suite, eines der Data-Security-Module oder Web- bzw. E-Mail-Security-Lösungen bereitstellen – die Websense TRITON-Konsole bietet schon heute eine vereinheitlichte Verwaltungslösung für Ihre Sicherheitsanforderungen von morgen.



„[Bei internen Verletzungen] waren zwei Drittel das Ergebnis bewusster Handlungen, der Rest war unabsichtlich.“

Verizon Business
2009 Data Breach



„31 Prozent der gemeldeten Fälle von Datenverlust gehen auf gestohlene Laptops, gestohlene Desktops oder verlorene Medien zurück.“

DatalossDB
Open Security Foundation

Transparenz und Kontrolle mit Zielerkennung



Competitor Alert

Daten: PCI & PII
Quelle: 10.14.222.21
Kanal: Web
Destination: 10.14.222.21





Websense-Alert

Datenbank: PCI & PII, customer database
Quelle: Joe User x1234,
 juser@company.com
 Funktion: Mitarbeiter
 Abteilung: Finanzen
 Manager: Jane Manager x1234
 jmanager@company.com

Kanal: Web
Destinazione: mail.google.com
Typ: private Webmail-Site
Ort: Mountain View, CA

- **Eingeschränkter Kontext**
- **Aufwand für IT-Administrator**

Betrachten Sie eine typische Meldung zu einem Datenverlust, die nur die IP-Adresse und den Anwendungskanal enthält. Hierbei muss der IT-Manager ermitteln, wer benachrichtigt werden muss und an welche Ziele die vertraulichen Daten übermittelt wurden.

- **Anwender- und Zielerkennung**
- **Schnellere Abhilfe**

Bei Websense Data Monitor kann schnell erkannt werden, dass PCI- und PII-Daten über den Webkanal (**wie**), an eine spezifische Webmail-URL (**wo**) und durch einen bestimmten Anwender in der Finanzabteilung (**wer**) verloren gegangen sind – so erhalten Sie *effizient* Transparenz. Diese Warnung ist zudem relevant und kann direkt für entsprechende Maßnahmen herangezogen werden, da diese in Echtzeit generiert wird und Kontaktdaten, Stellenbezeichnung und alle weitere Angaben enthält, die aus der Integration mit Websense Web Security bereitgestellt werden.

Anwendungserkennung und Gerätekontrolle an den Endpoints

Wenn Mitarbeiter Daten aus lokalen Anwendungen auf periphere Speichergeräte kopieren, entstehen Risiken. Kopiert ein Mitarbeiter beispielsweise Daten aus einer Unternehmensanwendung in lokale E-Mail-Software, meldet Websense dieses Ereignis mit detaillierten Angaben zu Anwender, Endpoint, vertraulichen Daten, Anwendung und Ziel der Daten. Andere Endpoint-DLP-Lösungen bieten unzureichende Transparenz in Bezug auf die betreffenden Anwendungen und Daten und blockieren Aktionen, bei denen es sich in Wirklichkeit um legitime geschäftliche Aktivitäten handelt.

Umfassende Erfassung ermöglicht effiziente Abhilfe

Wenn eine Datenschutzverletzung aufgetreten ist, lassen sich durch laufende Inventarisierung dieser Daten die mögliche Ursachen des Datenverlusts bestimmen. Websense Data Discover durchsucht Daten-Repositorys mithilfe von Netzwerkskans nach vertraulichen Daten an bekannten Speicherorten. Anschließend werden die Daten klassifiziert, und es werden Abhilfemaßnahmen wie Verschlüsselung oder die Löschung von Dateien eingeleitet. Die Ansicht für die Vorfallsverwaltung enthält einen Link zur entsprechenden Datei, die Kategorie, unter die die darin enthaltenen Daten fallen (mit Fingerabdruck versehene oder regulierte Daten), den Besitzer der Datei (um den Vorfall für Abhilfemaßnahmen zuweisen zu können) sowie sämtliche Abhilfemaßnahmen, die bereits zur Behebung des Problems eingeleitet wurden. In Verbindung mit Websense Data Endpoint, das Daten lokal mithilfe eines Software-Agenten erfasst, bietet die Lösung eine umfassende, skalierbare Erkennung für Online- und Offline-Systeme.

Funktionen	Vorteile
Optionen für die automatisierte Durchsetzung von Richtlinien im Netzwerk, an den Endpoints und in erfassten Daten-Repositories	<ul style="list-style-type: none"> • Flexible Durchsetzungsoptionen mit Anwenderbenachrichtigung, Prüfung/Protokoll usw • Netzwerkdatenverkehr: Quarantäne, Blockierung, Weiterleitung an Verschlüsselungs-Gateways von Drittanbietern, Löschung von Content • Endpoint-Aktivität: Blockieren des Verschiebens/Kopierens/Druckens vertraulicher Daten aus Anwendungen auf externe Geräte, Blockieren von Bildschirmabzügen, Anwenderbenachrichtigung, Anwenderbestätigung/-prüfung/-protokollierung • Erfassung: Entfernung oder Ersetzung (mithilfe von Anmeldeinformationen und automatisierten Skripten), Verschlüsselung gespeicherter Daten (Integration mit Voltage-Dateiverschlüsselung durch Drittanbieter)

Funktionen	Vorteile
DLP für SaaS-Anwendungen (Security-as-a-Service)	<ul style="list-style-type: none"> • Sicherstellen, dass vertrauliche Daten nur in identifizierte und genehmigte SaaS-Anwendungen hochgeladen werden • Durchsetzen von Richtlinien zu den Arten von Daten, die lokal aus der SaaS-Anwendung heruntergeladen werden können
Intelligente Erkennungsfunktionen für Datenverluste, die über mehrere Kommunikationskanäle erfolgen	<ul style="list-style-type: none"> • Erkennung geringer Volumina vertraulicher Daten, die über mehrere Kommunikationskanäle gesendet werden • Erkennung von Datenverlust in großen Mengen anhand des Gesamtumfangs der in einem bestimmten Zeitraum gesendeten vertraulichen Daten
Transparenz zahlreicher Netzwerkkanäle durch passive Datenverkehrsüberwachung	<ul style="list-style-type: none"> • Netzwerküberwachung für Web (HTTP), gesichertes Web (HTTPS), E-Mail (SMTP), IM (AOL, Yahoo, MSN), FTP, Druckvorgänge (optionaler OCR-Agent) und dynamischer Web 2.0-Content • Verringerung der Verstöße um 50 Prozent durch Anwenderbenachrichtigung bei Verstößen
Transparenz bei Geräten, Anwendungen und der Speicherung vertraulicher Daten auf Endanwendersystemen	<ul style="list-style-type: none"> • Verringerung des Risikos von Datenverlusten aufgrund von Anwendermobilität und Datenmissbrauch • Speicherorterkennung: Anwendung von Richtlinien im und außerhalb des Netzwerks, offline • Portabilität: lokale Speicherung von Fingerabdrücken mit minimalem Speicherplatzbedarf • Geräteüberwachung und Kontrolle von Wechselmedien, externen Festplatten, Druckvorgängen, Brennvorgängen auf CDs/DVDs, Kopieren/Einfügen/Erstellen von Bildschirmabzügen in die Zwischenablage und Dateizugriff • Anwendungsüberwachung mit Auslösung durch Anwender, Anwendergruppen oder, vordefinierte Anwendungen • Klassifizierung nach regulierten Datentypen, z. B. Kreditkartennummern
Erfassung vertraulicher Daten in lokalen und Netzwerk-Daten-Repositories	<ul style="list-style-type: none"> • Umfassende Erfassung: Netzwerkscans, lokale Scans (über Software-Agenten an den Endpoints); Ad-hoc-Scans oder geplante Scans • Abdeckung: netzwerkbasierte Scans von Datenbanken, Dateifreigaben, Exchange, SharePoint; lokale Scans auf Grundlage von Dateityp, -größe und -erstellungsdatum • Identifizierung: über 400 Dateitypen, einschließlich Microsoft Exchange-PSTs; Fingerabdrücke für Dateien, Compliance-Vorlagen
Integrierte Datenerkennung mit patentierten Precise ID™-Technologien	<ul style="list-style-type: none"> • Automatisierte und präzise Erkennung vertraulicher Daten: Schlüsselwörter, Wörterbücher, Fingerabdrücke, reguläre Ausdrücke, Grenzwerte, Kontext, Proximität und Korrelation bei unstrukturierten und strukturierten Daten (z. B. in einer Datenbank) • Effektive Erkennung: Verringerung von falsch positiven Treffern und Störungen der betrieblichen Abläufe durch Ignorieren von Daten, wenn keine Zuordnung zu Kundendaten (mithilfe von Fingerabdrücken) erfolgen kann oder der angegebene Grenzwert unterschritten wird
Flexible Bereitstellungsoptionen mit integriertem Web-Proxy und Integration mit Web-Proxies von Drittanbietern	<ul style="list-style-type: none"> • Websense Web Security-Integration: Weiterleiten von HTTP-, HTTPS- und FTP-Datenverkehr zur Analyse durch Websense Data Security über das ICAP-Protokoll • Keine Zusatzlösungen erforderlich: HTTP, SMTP, IM, FTP und HTTPS (mit Websense Web Security, für Web-Proxy) • Flexibel und kostengünstig: (1) Überwachungs- oder Schutzmodus, (2) Bypass/Span-Port oder Inline/Tap, (3) mit Websense Web Security oder einem beliebigen Standard-Web-Proxy, (4) mit Websense Email Security oder einem beliebigen SMTP-kompatiblen MTA • Effizienz: Planung von Erfassungsscans, wenn das System nicht durch einen Akku betrieben wird (Endpoint), zu Zeiten mit geringem Datenverkehrsaufkommen; netzwerkbasierend (Abdeckung) oder agentenbasiert (Leistung), Ausnahmelisten für den IP-Bereich bei der Netzwerkerfassung • Bereitstellung eines Endpoint-Agenten: Microsoft SMS oder andere Methoden; Vermeidung von Konflikten mit Anti-Virus-Funktionen und persönlichen Firewalls; schrittweise Bereitstellung mit Anwenderprofilen; Aktivieren/Deaktivieren des Agenten • Investitionsschutz: schrittweise Bereitstellung der Module nach Bedarf



„[Die Lösungen von Websense] bieten branchenführende Präzision. Sie durchsuchen automatisch den verteilten Content unseres Unternehmens und ermitteln, wo sich unsere vertraulichen Daten befinden.“

**Addison Avenue
Federal Credit Union**
Websense Data
Discover-Kunde

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

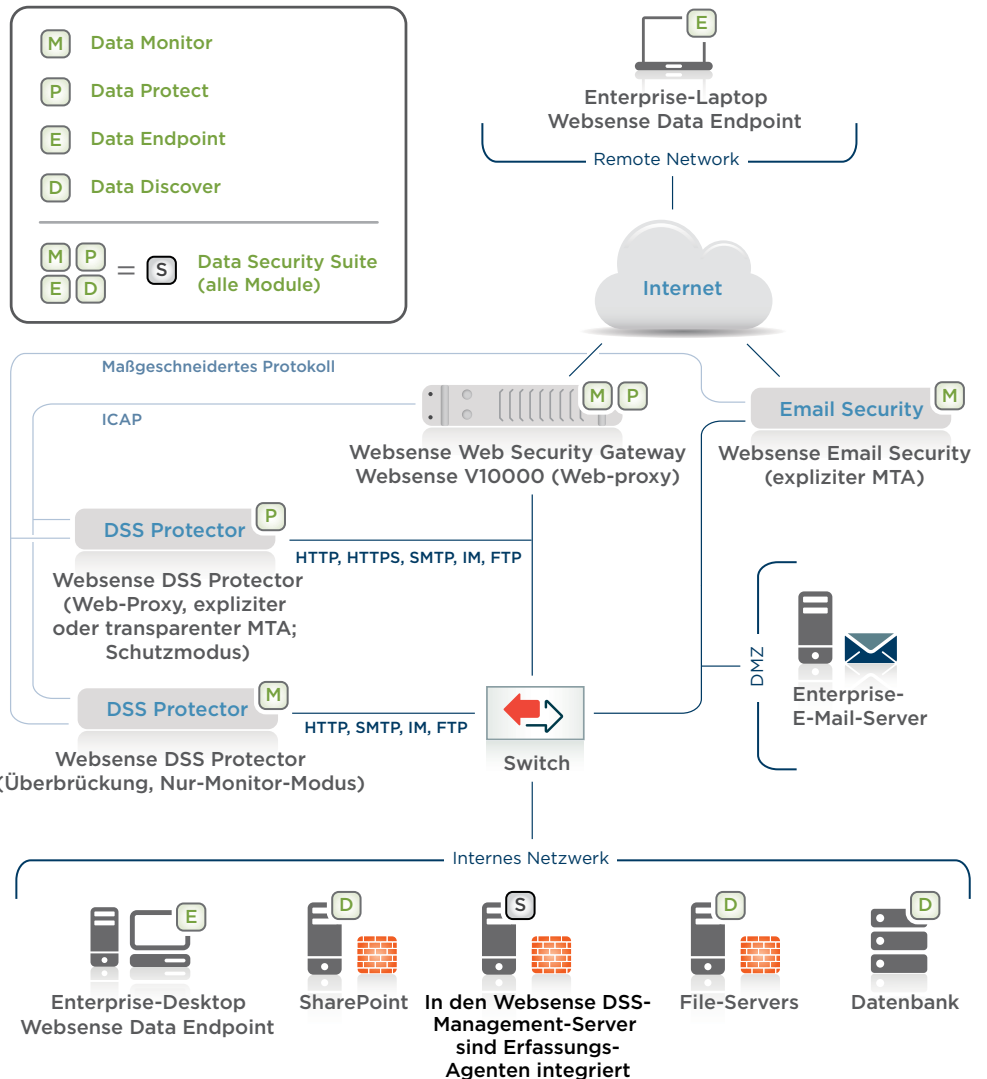
SKU: WDSS-X-XXXX-X

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 Deutschland GmbH Hamburg, Deutschland tel +49 40 3764 4414 fax +49 40 376 44 603 www.websense.de
--	--

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

Funktionen	Vorteile
Umfassende und aktuelle Richtlinienvorlagen, zentrale Richtlinien- und Vorfallsverwaltung und Berichterstattung	<ul style="list-style-type: none"> Vereinfachung durch integrierte Assistenten: Branchenspezifische und regionale Vorschriften (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 Laufende Aktualisierung der Vorschriften: regelmäßige Aktualisierung der Vorlagen durch ein spezielles Team Integrierte Berichte für Auditoren und Führungskräfte: Verteilung fälschungssicherer Compliance-Berichte (PDF) mit Informationen zur Gesamtzahl von Vorfällen nach: Netzwerk: Anwendergruppe, Richtlinie, Vorschrift, Durchsetzungsmaßnahme usw. Endpoint: Gerät/Anwendungskanal, Anwendergruppe, Richtlinie, Vorschrift, eingeleitete Durchsetzungsmaßnahme usw. Erfassung: IP-Adresse, Name/Typ des Repositorys, vertrauliche Daten (Typ, betreffende Datei/Datensatz), Datenbesitzer, Abhilfemaßnahme



Weitere Informationen, eine kostenlose Demoversion der Websense Data-Security-Lösungen oder eine Online-Demonstration finden Sie unter www.websense.com/evaluations.