



„90 % der Top-100-Websites sind als Social Networking oder Suchmaschinen klassifiziert, und mehr als 47 % davon unterstützen von Anwendern erstellten Content.“

Websense Security Labs™, 2009

Websense®

Web Security Gateway-Lösungen

Dynamische und interaktive Web 2.0-Technologien haben das Web in eine zentrale Plattform für Unternehmensanwendungen verwandelt. Kundenbeziehungen können heutzutage ebenso wie Lohn- und Gehaltsabrechnungen interaktiv im Web bearbeitet werden. Anwendungen wie social Networking werden tagtäglich für die Personalbeschaffung, Leadgewinnung und andere Geschäftsprozesse verwendet. Das Web 2.0 bringt jedoch auch neue Risiken mit sich, und dynamischer sowie von Anwendern erstellter Content machen herkömmliche Security-Technologien wie Virenschutz und URL-Filterung wirkungslos. Darüber hinaus bieten sie keinerlei Kontrolle über ausgehende vertrauliche Daten, die im Web 2.0 veröffentlicht werden.

Websense® Web Security Gateway-Lösungen sind Marktführer bei Secure-Web-Gateways. Sie bieten ein Höchstmaß an Schutz gegenüber modernen Bedrohungen im Web 2.0, weisen aber gleichzeitig die niedrigsten Gesamtbetriebskosten (TCO) auf. Nur mit unseren Lösungen verfügen Sie über hochleistungsfähige Data-Loss-Prevention-Funktionen und können hybride Vor-Ort- und cloud-basierte Bereitstellungen zentral verwalten. Dank unserer Web Security Gateway-Lösungen können Unternehmen alle Chancen nutzen, die das Web 2.0 bietet, ohne sich um Malware, ungeeigneten Content oder die Offenlegung vertraulicher Daten sorgen zu müssen.

Funktionsweise

Web Security Gateway-Lösungen überwachen eingehenden und ausgehenden Content von Unternehmen und schützen so vor dynamischer Web-Malware, beugen dem Verlust ausgehender vertraulicher Daten vor und steigern die Mitarbeiterproduktivität. Die Websense TruHybrid™-Bereitstellung unterstützt Appliances vor Ort sowie Security-as-a-Service (SaaS)-Plattformen und verwaltet die gesamte Umgebung aus einer einzelnen Infrastruktur für Richtlinien und Berichterstattung. Im Gegensatz zu anderen Ansätzen profitieren Websense-Kunden von einer umfassenden Flexibilität. Sie wählen anhand ihrer Anforderungen eine Plattform aus oder kombinieren unterschiedliche Plattformen, ohne dass Kosten für die Verwaltung mehrerer Systeme auflaufen.

Vorteile der Websense Web Security Gateway-Lösungen:

- **Data Loss Prevention bei ausgehenden Daten und Compliance-Kontrollen** – Die integrierte hochleistungsfähige Data-Loss-Prevention-Technologie sorgt für die erforderliche Kontrolle ausgehender Daten an Webmail- und Social-Networking-Sites, während Compliance-Anforderungen im Hinblick auf die Offenlegung vertraulicher Daten durchgesetzt werden.
- **Schutz vor Malware** – Die Websense TRITON™ Advanced Classification Engine (ACE) schützt vor herkömmlichen dateibasierten Angriffen ebenso wie vor dynamischen skriptbasierten Angriffen, mit denen traditionelle Antiviruslösungen umgangen werden.
- **Mitarbeiterproduktivität im Web 2.0** – Die TRITON Advanced Classification Engine entfernt ungeeigneten Content aus komplexen, dynamischen und kennwortgeschützten Web 2.0-Websites, die von herkömmlichen URL-Filterlösungen nur unzureichend erkannt werden.
- **Niedrigste Gesamtbetriebskosten (TCO)** – Durch die Websense TRITON-Konsole und die TruHybrid-Bereitstellung wird die Anzahl der Appliances, Verwaltungssysteme und Anbieter reduziert, die im Unternehmen unterstützt werden müssen.
- **Einheitliche Security im ganzen Unternehmen** – Die TruHybrid-Bereitstellung vereinheitlicht die Durchsetzung von Richtlinien für die Bereitstellung vor Ort und als Security-as-a-Service (SaaS). Dies stellt eine einheitliche Durchsetzung spezifischer Richtlinien für jeden Anwender sicher – ob unterwegs oder vor Ort.

Im ersten Halbjahr 2009 hosteten über 80 % der Top-100-Websites böartigen Content oder enthielten verborgene Weiterleitungen auf illegitime Websites.“

WebSense Security Labs, 2009

Advanced Classification Engine

WebSense Web Security Gateway-Lösungen nutzen die WebSenseTRITON Advanced Classification Engine (ACE), das präziseste* Security-Analysemodul, das eine detaillierte Untersuchung eingehender Daten mit umfassender Data Loss Prevention ausgehender Daten verbindet. ACE bietet herkömmliche Security-Funktionen sowie eine hochentwickelte Methodik zur Klassifizierung von Content, beispielsweise durch Antivirusbefreiungen, URL-Filter, Reputationsdienste und Fingerabdrücke. Risiken bei ein- und ausgehenden Daten lassen sich so präzise und zuverlässig einstufen. Content, der das Gateway passiert, wird von ACE unter Rückgriff auf das WebSense ThreatSeeker® Network analysiert. Dabei kommen Security-Scans in Echtzeit, eine Content-Klassifizierung in Echtzeit sowie die hochleistungsfähige Data-Loss-Prevention-Technologie zum Einsatz.

Security-Scans in Echtzeit

Webbasierte Angriffe gehen mehrheitlich auf dynamische und skriptbasierte Angriffe zurück. Durch den Einsatz von Antivirustechnologie alleine kann dieser Bedrohung kaum Einhalt geboten werden. Die Technologie von WebSense schützt Sie vor so genannten Zero-Day-Bedrohungen, indem schädlicher Content in Echtzeit erkannt wird, ohne dass Datenbanken mit früheren Angriffsmustern benötigt werden.

Content-Klassifizierung in Echtzeit

Viele der am häufigsten besuchten Websites lassen sich mit herkömmlichen URL-Filterlösungen nur unzureichend klassifizieren. Eine einzelne Google- oder Facebook-Seite kann beispielsweise eine Mischung von Content aus den unterschiedlichsten Kategorien enthalten und lässt sich so unmöglich in nur eine Kategorie einstufen. Viele Unternehmen sehen sich daher gezwungen, wertvolle Ressourcen pauschal auszuschließen, oder lassen den uneingeschränkten Zugriff auf dynamische Web 2.0-Websites zu und umgehen dadurch die Richtlinien für akzeptable Nutzung.

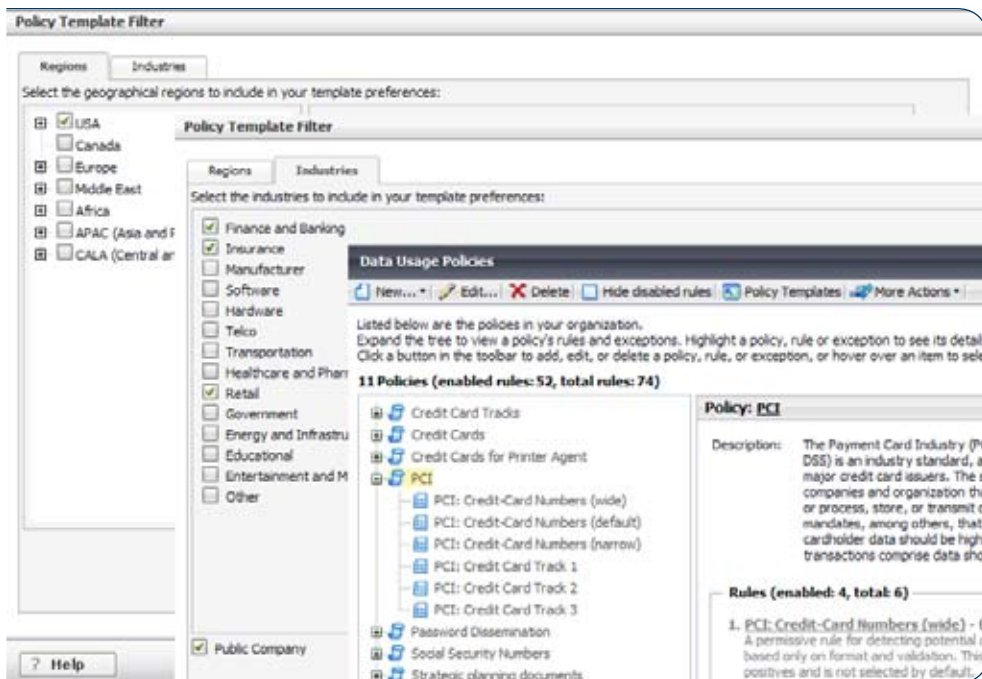
Mit den Web Security Gateway-Lösungen kann Content nun in Echtzeit klassifiziert werden. Dies ermöglicht die Anwendung von Richtlinien für die akzeptable Nutzung auf dynamischen Content im Web 2.0. Content-Elemente, die gegen diese Nutzungsrichtlinien verstoßen, können von einer Seite entfernt werden, während erlaubter Content zugänglich bleibt. Dank dieser einzigartigen Technologie erhalten Sie umfassenden Zugang zum Web 2.0, ohne an Produktivität einzubüßen und gegen die Richtlinien zur akzeptablen Nutzung zu verstoßen.

Hochleistungsfähige Data-Loss-Prevention-Technologie

Die integrierte hochleistungsfähige Data-Loss-Prevention-Technologie (DLP) sorgt für die erforderliche Kontrolle ausgehender Geschäftsdaten an Webmail- und Social-Networking-Sites, während Compliance-Anforderungen im Hinblick auf die Offenlegung vertraulicher Daten durchgesetzt werden. Web Security Gateway-Lösungen bieten die umfassende Funktionalität der marktführenden DLP-Lösung von WebSense für HTTP-, HTTPS- und FTP-Netzwerkverkehr und heben sich so von anderen DLP-Lösungen ab, die sich auf die Untersuchung von Schlüsselwörtern beschränken oder die komplexe Integration von Drittanbietern erforderlich machen. Unsere Lösung umfasst über 800 Standardrichtlinien sowie Fingerabdrücke für detaillierte Content-Analysen und ermöglicht eine umfassende Compliance-Berichterstattung.

Dank der Integration von Web-DLP in die Web Security Gateway-Lösungen entfällt die Notwendigkeit für dedizierte DLP-Hardware von Drittanbietern an den einzelnen Unternehmensstandorten, und die Gesamtbetriebskosten (TCO) werden erheblich gesenkt. Unternehmen mit längerfristigen Data-Loss-Prevention-Strategien profitieren von Web-DLP auch durch soliden Investitionsschutz: ein einfaches Softwareupgrade genügt, um die Kontrolle über das Web hinaus auszudehnen und anderen Datenverkehr (E-Mail, IM, P2P), andere Endpoints sowie ruhende Daten (z. B. Datenbanken, Dateifreigaben, Exchange und Share Point) zu berücksichtigen. Restrukturierungen zur Ausdehnung der Web-DLP-Abdeckung auf andere Kanäle sind nicht erforderlich. Die Investitionen in Richtlinien und Infrastruktur gehen nicht verloren.

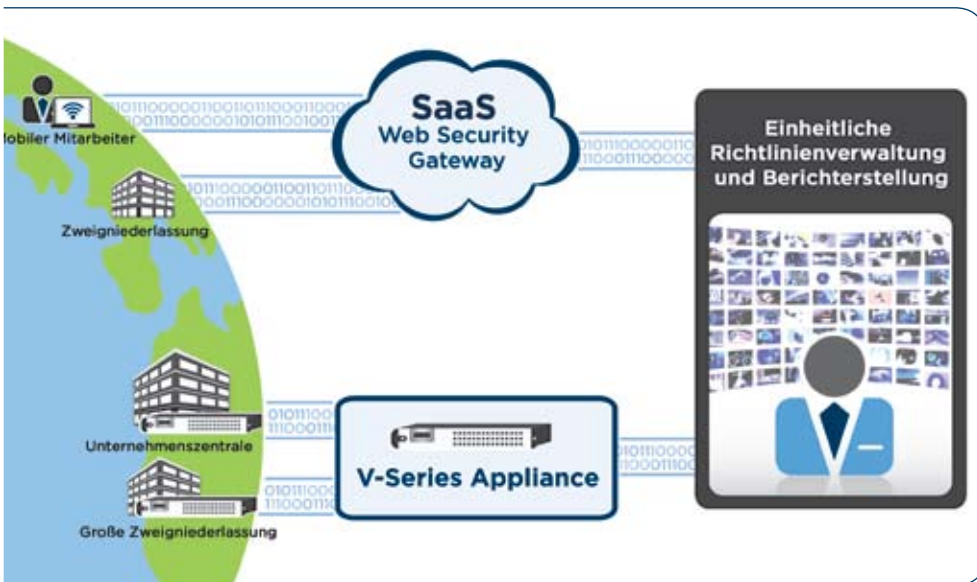
* <http://www.websense.com/content/tolly-report-reg.aspx>



Einfache DLP-Richtlinienassistenten unterstützen Administratoren beim Festlegen von Richtlinien für bewährte Verfahren, die regionale und branchenspezifische regulatorische Anforderungen erfüllen.

TruHybrid-Bereitstellung

Die TruHybrid-Bereitstellung ermöglicht eine flexible Kombination aus Vor-Ort- und SaaS-Bereitstellungsplattformen, während die gesamte Umgebung über ein einzigartiges zentrales Verwaltungssystem gesteuert wird. Mithilfe der SaaS-Plattform kann der Schutz auch auf Zweigniederlassungen und mobile Anwender erweitert werden. Gleichzeitig können Sie hochleistungsfähige Appliances an Unternehmensstandorten sowie in Zweigniederlassungen oder Rechenzentren bereitstellen. Unabhängig von den gewählten SaaS- und Applianceoptionen können Sie zentral eine einheitliche Richtlinie für das gesamte Unternehmen festlegen. Dieser einheitliche Ansatz senkt nicht nur die Verwaltungskosten hybrider Bereitstellungen vor Ort und als SaaS, sondern stellt auch die durchgehende Security in allen Umgebungen sicher.



TruHybrid ermöglicht eine zentrale Verwaltung von hybriden Bereitstellungen vor Ort und als SaaS.

„Wir verlassen uns auf die Websense V10000™ Web Gateway Appliance, weil sie unseren Pflegekräften schnellen und sicheren Zugriff auf die benötigten Daten bietet. Dank der Scans in Echtzeit und flexibel festlegbaren Richtlinien muss ich mir keine Sorgen darüber machen, dass vertrauliche Daten durch manipulierte Websites gestohlen werden oder versehentlich in die falschen Hände gelangen, wenn unsere Pflegekräfte von unterwegs über das Internet auf Patientendaten zugreifen.“

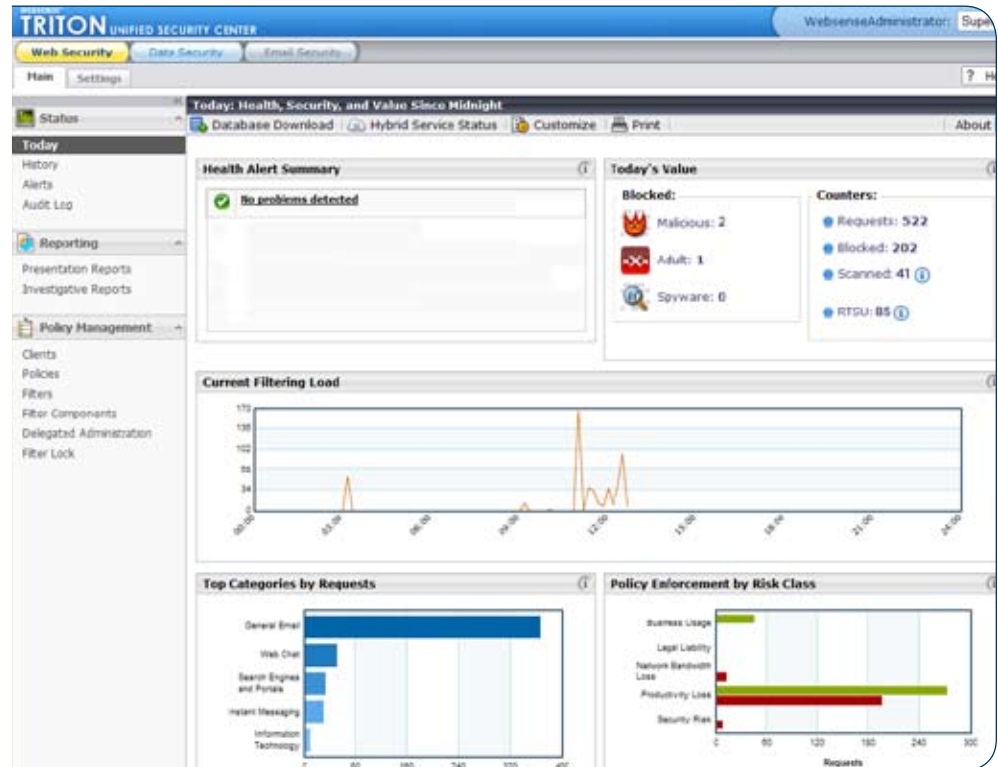
Larry Whiteside

Chief Security Officer

Visiting Nurse Service of New York

„Bis zu 57 % der böswilligen Angriffe im Web umfassen Code für den Datendiebstahl.“

WebSense Security Labs, 2009



Die interaktiven Dashboards der TRITON-Konsole bieten direkten Zugriff und ermöglichen es, aktive Bedrohungen und Richtlinienviolationen unmittelbar zu erkennen.

SSL-Transparenz und -Kontrolle

Infolge des zunehmenden SSL-Datenverkehrs sind blinde Flecken für ältere URL-Filter und Schlupflöcher für Bedrohungen und Datenverlust entstanden. Web Security Gateway-Lösungen bieten Transparenz und Kontrolle für SSL-Datenverkehr und ermöglichen Unternehmen so, die gesamte webbasierte Kommunikation über Richtlinien zu kontrollieren.

Erweiterte Anwendungskontrolle

Die zunehmende Nutzung von netzwerkbasierenden Anwendungen wie Instant Messaging und Peer-to-Peer-Netzen bietet Hackern eine Angriffsfläche, um Unternehmensabläufe zu stören oder sich vertrauliche Daten zu beschaffen. Die Web Security Gateway-Lösungen kontrollieren mehr als 125 Netzwerkprotokolle und Tausende von Anwendungen. Potenzielle Risiken werden so entschärft, und Datenverlust durch nicht autorisierte Anwendungen wird vorgebeugt. Mögliche Richtlinienaktionen reichen von der einfachen Sperrung von Anwendungen bis hin zur detaillierten Bandbreitensteuerung.

Einheitliche Verwaltung und Berichterstattung für Content-Security

Die TRITON-Konsole ist eine wichtige Komponente, die ebenfalls für Web Security Gateway-Lösungen und exklusiv von Websense erhältlich ist. Sie ermöglicht die zentrale Verwaltung aller Web-, Daten- und E-Mail-Security-Lösungen von Websense über eine webbasierte Oberfläche. Im intuitiv zu bedienenden Dashboard sind mehr als 55 Berichte verfügbar, und umfassende Anpassungsmöglichkeiten unterstützen das Nachverfolgen von Anwenderaktivitäten, erleichtern die Problembehandlung und helfen, Risiken zu entschärfen. Verglichen mit Lösungen der Wettbewerber fallen Verwaltungsaufwand und Kosten deutlich geringer aus, da eine Vielzahl an anwenderfreundlichen Funktionen wie detaillierte Drill-Down-Berichte, Richtlinienassistenten, Konfigurationsvorlagen, ein Planungs subsystem und automatische Content-Aktualisierungen zur Verfügung stehen. Da sich die Anforderungen an Content Security nicht auf Web Security beschränken, können auch die zentralen Verwaltungsfunktionen der TRITON-Konsole problemlos erweitert werden, um E-Mails und vollständige DLP zentral zu steuern.

Funktionen	Vorteile
TruHybrid-Bereitstellung	Senkt die Gesamtbetriebskosten (TCO) und stellt die einheitliche Durchsetzung von Richtlinien im Unternehmen durch die zentrale Verwaltung von Vor-Ort- und SaaS-Bereitstellungen sicher.
Hochleistungsfähige Data-Loss-Prevention-Technologie	Verhindert den Verlust von ausgehenden Daten und kontrolliert die Einhaltung der Compliance-Anforderungen. Senkt die TCO durch Vereinfachung der DLP-Bereitstellung.
Content-Klassifizierung in Echtzeit	Sichert die Verwendung von webbasiertem Content mit dynamischen, kennwortgeschützten und gemischten Elementen durch Filterung von Web-Content in Echtzeit ab.
Security-Scans in Echtzeit	Schützt Unternehmen vor Web-Malware durch Erkennung von dynamischen, skriptbasierten und unbekanntem Bedrohungen in Echtzeit.
TRITON-Konsole	Senkt die TCO und die Kosten für das Anbietermanagement durch die einheitliche Verwaltung von Web-, Daten- und E-Mail-Security-Lösungen.
Integrierter Virenschutz	Schützt vor dateibasierten Virenangriffen mit Komponenten von Drittanbietern und leistungsstarken Antivirusbereitstellungen von Websense.
Marktführende Web-Filterung mit erweiterter Reputationsanalyse	Setzt grundlegende Richtlinien zur akzeptablen Nutzung durch und blockiert bekannte böse Websites. Die Mehrpunktreputationsanalyse berücksichtigt Eigenschaftstyp, lexikalische Reputation, Veröffentlichungen im Web 2.0, URL-Kategorie, den nächsten Nachbar, Suchreputation, Verlauf, Alter und Geographie.
Aktualisierungen durch das ThreatSeeker Network in Echtzeit	Reduziert die Angriffsfläche gegenüber neuen Bedrohungen durch Security-Updates alle fünf Minuten.
SSL-Transparenz	Ermöglicht die Untersuchung von verschlüsseltem Web-Datenverkehr mit vollständigem SSL-Proxy und integrierter Zertifikatsverwaltung.
Anwendungskontrolle	Minimiert das Risiko, steigert die Produktivität und senkt die Bandbreitenkosten durch die Verwaltung der Nutzung von Netzwerkprotokollen und Anwendungen.
Hochleistungsfähiger Web-Proxy/-Cache	Steigert die Leistung und senkt die Bandbreitenkosten durch Optimierung des Datenverkehrs. Unterstützt sowohl transparente als auch explizite Proxykonfigurationen.
Flexible Anwenderauthentifizierung	Ermöglicht Richtlinien auf der Grundlage von Anwendern und Anwendergruppen durch die flexible Authentifizierung über Active Directory, LDAP, RADIUS, Novell und NTLM 2.
Hohe Verfügbarkeit und Lastverteilung	Ermöglicht Systemredundanz und Skalierbarkeit für große Unternehmen durch die Nutzung von WCCP oder externen Modulen zur Lastverteilung.

Gartner stuft Websense in seinem jüngsten Magic Quadrant für Secure Web Gateways als Leader ein.

Gartner, Inc.

“Magic Quadrant for Secure Web Gateway”* by Peter Firstbrook and Lawrence Orans
January 8, 2010

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

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

Verfügbarkeit von Bereitstellungsplattformen

Bereitstellungen vor Ort können mit Websense V-Series™ Appliances oder mit Software auf allgemeinen Servern implementiert werden. SaaS-Bereitstellungen werden durch die Websense Hosted Web Security Gateway-Lösung unterstützt.

- **V-Series Appliances** V-Series Appliances sind hochleistungsfähig sowie äußerst zuverlässig und bieten eine einfache Bereitstellung vor Ort. Sie haben sich in Fortune-100-Unternehmen bewiesen und verbinden eine Redundanz auf Komponentenebene mit vielfältigen Funktionen für die Bereitstellung in Unternehmen, z. B. Lastverteilung und Hochverfügbarkeit. V-Series Appliances sind außerdem für zukünftige Lösungen von Websense gerüstet, ohne dass eine Aufrüstung der Hardware erforderlich wäre. Dies steigert die Lebensdauer und den Wert der Plattform.
- **Hosted Web Security Gateway** Websense Hosted Web Security Gateway-Lösungen verteilen Security-Kontrollverfahren auf 10 weltweit verfügbare und redundante Rechenzentren in der Cloud. Dieses SaaS-Modell beschleunigt die Bereitstellung und kann zu einer erheblichen Senkung der Betriebskosten beitragen, da in den einzelnen Zweigniederlassungen keine Hardwareunterstützung mehr erforderlich ist. Websense-Rechenzentren sind nach ISO 27001 zertifiziert und erfüllen strenge Security- und Verfügbarkeitsstandards, die für einzelne Unternehmen allein, insbesondere wenn es sich um Remote-Niederlassungen handelt, nur mit sehr viel Aufwand einzuhalten wären. Bei der Bereitstellung als eigenständige reine SaaS-Lösung bietet Websense Hosted Web Security Gateway darüber hinaus den Vorteil der integrierten E-Mail-Security für SaaS.



The Websense V10000™ Appliance

Optionen für Websense Web Security Gateway-Lösungen

Websense Web Security Gateway Anywhere – Bereitstellungen vor Ort* oder als SaaS, die TruHybrid-Verwaltung benötigen, hochleistungsfähige Data-Loss-Prevention-Technologie für das Web oder für den Websense Remote Filtering-Client

Websense Web Security Gateway – Für Bereitstellungen vor Ort*

Websense Hosted Web Security Gateway – Für SaaS-Bereitstellungen

Mindestanforderungen für den Server bei Softwarebereitstellungen:

Betriebssystem
Red Hat Linux 4, Update 5*,
oder Windows Server 2003/2008†
Prozessor: 2 Dual-Core-Prozessoren
mit 2,8 GHz
Arbeitsspeicher
4GB RAM

Festplattenlaufwerk
Zwei physische Festplatten:
* 100 GB für Betriebssystem, Anwendungsdaten und
temporäre Daten sowie 100 GB für den Cache*
* 100GB (RAID 1 empfohlen)†
Netzwerkschnittstellen
Zwei 10/100/1000-Ethernet-Schnittstellen

* Bereitstellungen vor Ort können in Websense V-Series Appliances oder als Software auf allgemeinen Servern implementiert werden.

**Der Magic Quadrant ist eine grafische Darstellung eines Markts zu einem bestimmten Zeitpunkt und für einen bestimmten Zeitraum. Er stellt die Bewertung von Anbietern gemäß der von Gartner für einen Markt definierten Kriterien dar. Gartner empfiehlt weder die im Magic Quadrant dargestellten Anbieter, Produkte oder Dienstleistungen, noch rät Gartner Technologieanwendern dazu, ausschließlich solche Anbieter zu wählen, die darin als „Leader“ eingestuft werden. Der Magic Quadrant dient ausschließlich als Analyseinstrument und soll keine Handlungsaufforderung sein. Gartner schließt jegliche ausdrückliche oder implizite Haftung in Bezug auf diese Studie aus, ebenso jegliche Gewährleistung der Gebrauchstauglichkeit oder Eignung für einen bestimmten Zweck.

websense[®]
ESSENTIAL INFORMATION PROTECTION™

Eine Produktdemonstration oder eine kostenlose Testversion von Websense Web Security erhalten Sie auf unserer Website unter www.websense.com/evaluations.

©2010 Websense, Inc. alle Rechte vorbehalten. Websense, das Websense Logo, Threatseeker und TRITON, TruContent, V-Series und Essential Information Protection sind registrierte Handelsmarken in den USA und anderen internationalen Märkten. Websense hat zahlreiche registrierte und nicht registrierte Handelsmarken in den USA und weltweit. Alle anderen Handelsmarken sind Eigentum der entsprechenden Inhaber. WSG_DS_DE_Feb10