



Websense

Web Security Gateway

Sichere und kontrollierte Nutzung des Web 2.0

Das Web 2.0 verändert unsere Arbeits- und Interaktionsweisen grundlegend. Mehr als 90 der Top-100-Webseiten werden als Social Networking Seiten oder Such-Webseiten kategorisiert, die dynamische oder nutzergenerierte Inhalte unterstützen. Viele Unternehmen nutzen das Web als geschäftliche Plattform. Durch Web-2.0-Technologien wie Blogs, Wikis, Social Networking Seiten und RSS Feeds werden herkömmliche Sicherheitstechnologien wie Antivirenprogramme, Web-Reputation oder einfache URL-Filterung jedoch unwirksam.

Das Web 2.0 kann für Unternehmen von enormem Nutzen sein, zum Beispiel um die Kundenbeziehung und -zufriedenheit zu optimieren sowie bei der Etablierung von Wettbewerbsvorteilen. Es birgt jedoch auch neue Risiken – für Sicherheit, Produktivität und gesetzliche Haftung. Dennoch können Unternehmen von Web-2.0-Technologien beträchtlich profitieren. Ob sie es gutheißen oder nicht: Ihre Mitarbeiter nutzen diese neuen Tools und ebenso webbasierte Anwendungen greifen, von IT- und Network-Security-Teams unbemerkt, darauf zu.

Das Websense® Web Security Gateway ist eine der branchenweit genauesten und effizientesten Lösungen für Web-2.0-Content-Filtering und Schutz vor Bedrohungen. Dadurch können Unternehmen ihren Geschäftsverkehr beschleunigen, ohne sich um Sicherheit, Produktivität und Haftungsrisiken wie böartigen, unsachgemäßen Content und Datenverlust sorgen zu müssen.

Das Websense Web Security Gateway bietet:

- Transparenz und Kontrolle über dynamischen Web-Content und den Verlust ausgehender Daten einschließlich SSL-verschlüsseltem Datenverkehr
- Schutz vor Web-2.0-Bedrohungen wie z.B. dynamischen Scripts
- Hochentwickelte Anwendungskontrollen für IM, P2P etc.
- bedienerfreundliches, zentralisiertes Management und Reporting
- Integrierter Web-Proxy und Caching

Schutz vor dynamischen Web-2.0-Bedrohungen

Das heutige Web ist reich an dynamischem Content. Das Content-Scanning in Echtzeit ist die einzige Möglichkeit einer effizienten Kontrolle dynamischer Web-Bedrohungen, die herkömmliche Sicherheitsmethoden umgehen. Die Websense V10000 Appliance nutzt zur Analyse des Web-Contents proprietäre Analyse Engines, die von den Websense Security Labs entwickelt wurden. Diese hochentwickelte Kontrolle wird durch verschiedene in das Gateway integrierte Techniken wie Virenschutz, Websense Web Antivirus, Web-Reputationsanalysen, Verhaltensanalysen und Web-Filtering auf Basis der Websense URL-Datenbank erweitert. Dieser fortschrittliche Schutz bietet bestmögliche Absicherung und höchste Präzision, damit die Kunden die Vorzüge des Web 2.0 sicher nutzen können.

Kontrolle über dynamischen und nutzergenerierten Content

Websense hat die moderne Analytik und die Echtzeit-Content-Überwachungs- und Klassifizierungstechnologien des Websense ThreatSeeker™ Network in das Websense Web Security Gateway eingebettet. Diese eingebetteten Technologien garantieren den „spontanen“ Schutz vor zuvor nicht kategorisiertem bzw. unbekanntem Web-Content. Das Websense Web Security Gateway kategorisiert spezifischen Webseiten-Content, wie Mashups und nicht einfach nur die Webseiten selbst. Dadurch können IT-Manager den Zugriff auf Web-2.0-Seiten ermöglichen, während ihre Unternehmen gleichzeitig vor den Bereichen der Seiten geschützt sind, die unsachgemäßen oder unerwünschten Content enthalten. Websense analysiert mit Hilfe des einzigartigen

„In der zweiten Jahreshälfte 2008 hosteten 70 % der Top-100-Seiten böartigen Content oder enthielten eine versteckte Umleitung auf eine illegale Webseite.“

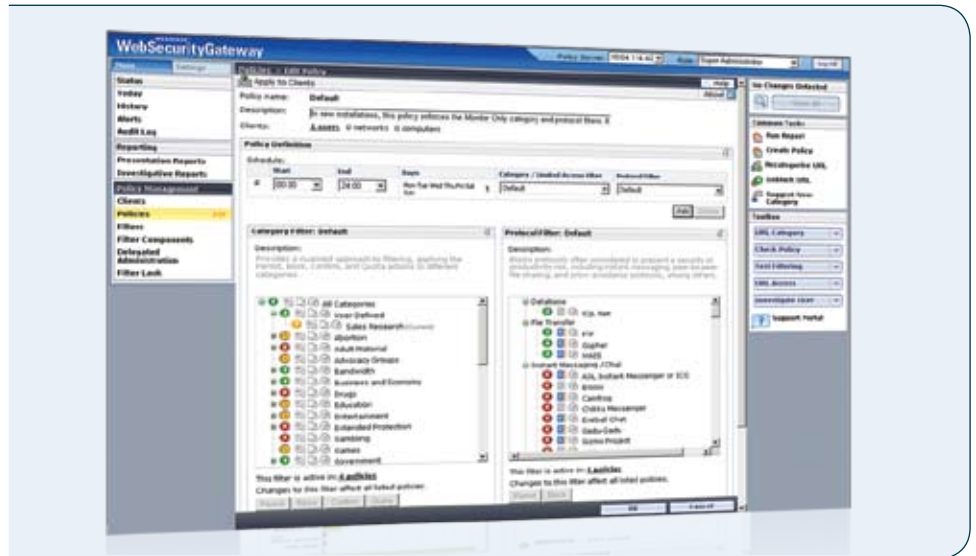
Websense Security Labs

„Das Echtzeit-Scanning von Websense Web Security Gateway gestattet uns, auf Web-2.0-Seiten zuzugreifen und stellt gleichzeitig sicher, dass kein bösartiger Content eindringen und unsere vertraulichen Daten nicht nach außen gelangen können.“

Henry Parker

Senior Security Architect
Addison Avenue

Web 2.0-Früherkennungs- und Schutzsystems an Web 2.0, Social Networking und Blogger-Netzwerke geposteten Content sobald dieser online ist. So sind die Kunden vor Gefahren geschützt, noch bevor sie sich ausbreiten können.



Websense Policy Management

Hochentwickelte Anwendungskontrollen

Die zunehmende Menge von Netzwerkanwendungen, wie IM und P2P, bietet Hackern die Möglichkeit, Geschäftsprozesse zu unterbrechen und vertrauliche Daten zu stehlen. Mit dem Websense Web Security Gateway können mehr als 130 Netzwerkprotokolle für eine Vielzahl von Anwendungen kontrolliert werden; das senkt die Sicherheitsrisiken und schützt vor Datenverlust infolge nicht autorisierter Anwendungen.

Integrierter Web-Proxy und Cache

Das Websense Web Security Gateway basiert auf einer Enterprise-Class-Web-Proxy- und Cache-Plattform. Diese Plattform sorgt für ein besseres Management sowie eine detailliertere Kontrolle und ermöglicht Echtzeit-Content-Analysen des Internetverkehrs. Der integrierte Proxy und Cache kann ebenso für eine Konsolidierung bereits vorhandener Web-Proxy-Systeme genutzt werden, wodurch Reaktionszeit und Leistung verbessert werden. Darüber hinaus spart diese Lösung gegenüber dem Kauf und der Wartung separater Systeme viel Zeit und schont die Ressourcen.

Transparenz und Kontrolle für eine sichere Web-Kommunikation

Das Websense Web Security Gateway ermöglicht eine sichere Web-Kommunikation. Die zunehmende Nutzung von SSL-Datenverkehr und FTP gegenüber HTTP produziert „Schlupflöcher“ für herkömmliche URL-Filter und öffnet eine Hintertür für Bedrohungen und Datenverlust. Das Websense Web Security Gateway bietet eine vollständige Transparenz des SSL-Verkehrs und erlaubt den Unternehmen damit eine effiziente Richtlinienpolitik für die gesamte Web-Kommunikation anzuwenden.

Intuitive Management- und Reporting-Schnittstelle

Das Websense Web Security Gateway bietet eine zentralisierte, aufgabenbasierte Management- und Reporting-Schnittstelle, die eine granulare Richtlinienkontrolle mit detailliertem Reporting kombiniert. Das intuitive, nutzerfreundliche Dashboard ermöglicht den Kunden die einfache Erstellung prozessfähiger Berichte und umfasst über 55 integrierte Reports über Anwenderaktivitäten und Risikoreduktion. Die Verwaltung des Gateways erfordert wenig Aufwand und spart so Zeit und Geld bei gleichzeitig besserer Transparenz und Kontrolle sowie präziseren, granularen Richtlinienkontrollen.



Websense Management und Reporting

„Über 45 Prozent der Top-100-Webseiten unterstützen dynamischen oder nutzergenerierten Content.“

„Immerhin 39 Prozent der bösartigen Web-Angriffe enthalten einen Code für Datendiebstahl.“

Websense Security Labs

| Funktionen | Vorteile |
|--|--|
| <p>Web-2.0-Content-Kontrolle in Echtzeit</p> | <ul style="list-style-type: none"> • Ermöglicht die sichere Nutzung und Kontrolle der neuesten Web-2.0-Technologien • Bietet die Möglichkeit, neue Web-2.0-Technologien zu nutzen und schützt sowohl vor bekannten wie auch neu entstehenden Bedrohungen • Erhöht die Produktivität der Mitarbeiter und dehnt die Web-Nutzungsrichtlinien in Echtzeit auf unbekannte, dynamische Seiten aus • Senkt die IT-Kosten und erhöht die Effizienz durch Zusammenfassung mehrerer einzelner Produkte zu einer ganzheitlichen, nutzerfreundlichen Lösung, die ebenso vor bekannten wie vor neu entstehenden Bedrohungen schützt |
| <p>Web 2.0 Security Scanning in Echtzeit mit Analyse Engines wie Antivirenprogramme, Web-Antivirensoftware, Web-Reputationsanalysen, Verhaltensanalysen und anderen zur Erkennung und Blockierung dynamischer Bedrohungen</p> | <ul style="list-style-type: none"> • Verhindert potenzielle Infektionen und Datenverlust durch Erkennung und Blockierung dynamischer Bedrohungen, wie z.B. Cross-Site-Scripting, die herkömmlichen Schutz unterlaufen • Bietet Ihnen die Präzision und Granularität, die für die Verwaltung und den Schutz Ihres Unternehmens im Rahmen von Web 2.0 erforderlich sind |
| <p>Umfassende Anwendungskontrollen: Eine hybride Proxy- und Network-Protocol-Engine kontrolliert über 130 Protokolle und eine Vielzahl von Einzelanwendungen</p> | <ul style="list-style-type: none"> • Minimiert die Sicherheitsrisiken und schützt vor Datenverlust, indem die Mitarbeiter an der Nutzung nicht autorisierter Anwendungen gehindert werden • Reduziert die Kosten für die Netzwerkinfrastruktur durch Kontrolle von Art und Umfang des Netzwerkverkehrs |
| <p>Enterprise-Class-Web-Proxy und Cache zur Überprüfung, Optimierung und Kontrolle des Internetverkehrs einschließlich SSL</p> | <ul style="list-style-type: none"> • Ermöglicht Kontrollen von ein- und ausgehendem Content und sogar von SSL-verschlüsseltem Datenverkehr • Verbessert die Web-Performance und -Reaktionszeit • Reduziert Kosten- und Verwaltungsaufwand, der für herkömmliche Proxy-Lösungen entsteht |
| <p>Zentralisiertes, anwenderfreundliches Management und Reporting</p> | <ul style="list-style-type: none"> • Spart Zeit und Geld bei der Verwaltung der Internetsicherheit • Verbessert Transparenz und Reporting und erhöht damit die Internetsicherheit • Löst Web-Security-Vorfälle schneller und einfacher • Implementiert Kontrollen per Mausclick - ohne kompliziertes Scripting |

Websense Deutschland GmbH
 München, Deutschland
 tel +49 89 5908 2357
 fax +49 89 5908 1361
 www.websense.de

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 86981
 www.websense.co.uk

Australien Israel
 websense.com.au websense.com

China Italien
 prc.websense.com websense.it

Frankreich Japan
 websense.fr websense.jp

Deutschland Niederlande
 websense.de websense.com

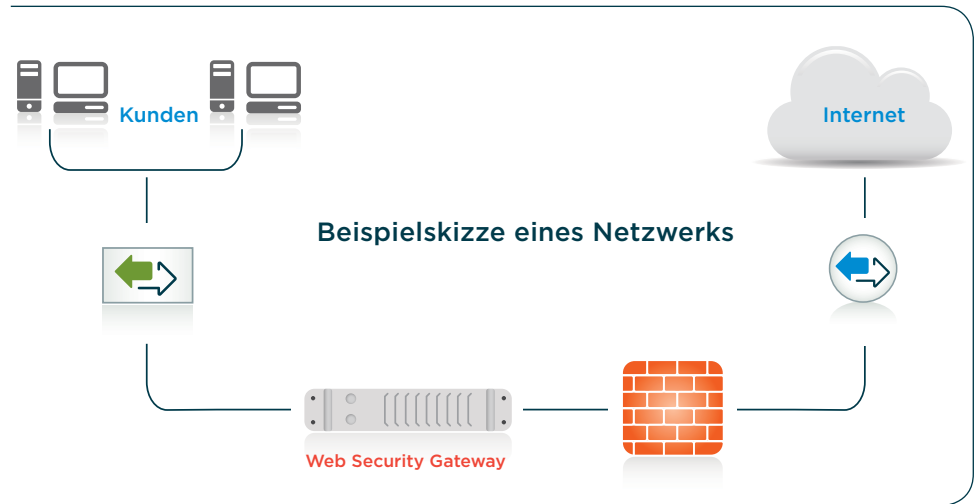
Hong Kong Singapur
 websense.cn websense.com

Indien Spanien
 websense.com websense.com.es

Irland UAE
 websense.co.uk websense.com

Einsatzoptionen zur freien Auswahl

Das Websense Web Security Gateway ist als Software oder im Rahmen der Websense V10000™ Appliance lieferbar. Die reine Softwarelösung bietet sich Unternehmen an, die eine Standardisierung auf bestimmten Hardwareplattformen wünschen. Den Unternehmen, die eine Appliance bevorzugen, bietet Websense V10000 vereinfachte Einsatzmöglichkeiten, einfaches Management, automatische Updates und „Zukunftssicherheit“.



Websense Web Security Gateway

Technische Daten

Das Websense Web Security Gateway kann als Software oder Appliance-basierte Lösung eingesetzt werden.

Appliance:

Websense V10000

Server-Mindestanforderungen:

Betriebssystem

Red Hat Linux v4,
Update 5* oder Windows Server 2003/
Server 2008†
CPU: 2 Dual-Core-Prozessoren 2,8 GHz
processors

Datenspeicher

4GB RAM

Festplattenlaufwerk

Zwei physikalische Discs:
- 100 GB für OS und Anwendungs- und
temporäre Daten, 100 GB für Cache*
- 100 GB (empfohlen: RAID 1)†

Netzwerkschnittstellen

Zwei Ethernet-Schnittstellen 10/100/1000

Hochverfügbarkeit

WCCP, Externer Loadbalancer

Proxy-Unterstützung

Transparent, explizit

SSL

Voll funktionsfähiger SSL-Proxy mit
integriertem Zertifikat-Management

Echtheitsprüfung

Active Directory, LDAP, RADIUS, Novell,
NTLM v2

* Für Websense Content Gateway und/oder
Websense Web Filter/Web Security v7

† Für Websense Web Filter/Web Security
v7 und/oder Reporting

Weitere Informationen erhalten Sie unter www.websense.com/evaluations.