



Zusätzliche Webkategorien für die Websense Enterprise®-Software bieten besseren Schutz gegen Sicherheitsprobleme bei der Internetnutzung. Premium Gruppen ermöglichen es, neue Gefahren wie etwa bandbreitenintensive Internetdienste, Malicious Mobile Code (MMC), Phishing-Angriffe und Spyware, die ein Produktivitäts-, Ressourcen- und Sicherheitsrisiko für Ihr Unternehmen darstellen können, zu erkennen und diesen Problemen mit entsprechenden Richtlinien zu begegnen.

Schutz vor MMC, Phishing-Angriffen und Spyware mit Websense Enterprise Security-PG™

Erweitert Netzwerke um eine zusätzliche Schutzschicht, die Mitarbeiter beim Surfen vor Phishing-Angriffen und einer unwissentlichen Infektion mit MMC oder Spyware schützt. Wenn Desktop-PCs bereits mit Spyware verseucht sind, kann Security-PG die Übermittlung vertraulicher Informationen an Spyware-Hostserver unterbinden.

Spyware ist auf einem Computer installierte Software, die ohne Wissen des Nutzers Daten sammelt und an Werbetreibende oder andere Interessenten weiterleitet. Spyware kann Informationen wie Tastatureingaben, Surfgewohnheiten, Passwörter, E-Mailadressen und mehr sammeln und übermitteln. Spyware verbraucht für die Erfassung und Übertragung von Daten Systemressourcen und Bandbreite. Darüber hinaus kann Spyware ernste Probleme in Bezug auf die Datensicherheit, den Datenschutz und die Einhaltung rechtlicher Vorschriften verursachen.

Security-PG verhindert den Kontakt mit Spyware durch eine Zugriffssperre für Websites, die Spyware verbreiten. In einem zweiten Schritt wird die Übertragung von Nutzer- und Netzwerkdaten an Host-Sites unterbunden. Dank proprietärer Prozesse und der WebCatcher™-Funktionalität, die noch nicht klassifizierte Webseiten anonymisiert von Kunden zur Überprüfung an Websense meldet, kann Websense Spyware-Server erkennen und eine Backchannel-Kommunikation über Port 80 verhindern.

Phishing-Sites und andere betrügerische Angebote sind häufig den Webseiten kommerzieller Anbieter nachempfunden, und fordern den Benutzer zur Eingabe von Kreditkartendaten, persönlichen Zugangsdaten usw. auf. Security PG bietet Schutz vor Phishing-Angriffen, denn ein Zugriff auf die Internetadresse bekannter Phishing-Websites wird wirkungsvoll unterbunden.

Bei Malicious Mobile Code handelt es sich um Programme, die dazu entwickelt wurden, von Computer zu Computer und von Netzwerk zu Netzwerk übertragen zu werden und auf infizierten Rechnern Schaden anzurichten oder Computersysteme zu verändern. Die Quelle des MMC kann eine harmlos erscheinende Webseite sein, die Mitarbeiter zu Einkäufen oder für ihre Reiseplanung besuchen. Eine Infektion bleibt häufig unbemerkt. MMC kann aus dem Internet auch per Virus, Trojaner, Wurm, Skriptangriff und Rogue Internet Code eingeschleust werden. Dies war z.B. beim Nimda-Wurm der Fall.

Websense® verwendet proprietäre Data Mining-Technologien, um eine mehrere Millionen Seiten umfassende URL-Datenbank nach potentiell gefährlichen Programmen einschließlich ActiveX-Befehlen, Visual Basic-Programmen, JavaScript und Java Applets zu durchsuchen. Websense klassifiziert diese mit MMC infizierten Seiten unter Verwendung ausgereifter Algorithmen nach Kategorien und verhindert so die ungewollte Infizierung von Mitarbeiter-PCs.

Websense Enterprise® Premium Gruppen™

Aktuelle Statistiken zeigen, dass ...

- 90% aller mit dem Internet verbundenen PCs mit Spyware infiziert sind.
- 45% der bei Kazaa erhältlichen, ausführbaren Dateien Mobile Malicious Code beinhalten.
- die Zahl der Malicious Mobile Code-Angriffe, die häufig für den Diebstahl vertraulicher Daten eingesetzt werden, im letzten Jahr um fast 50% gestiegen ist.
- 66% aller IT-Manager schon mindestens einmal bemerkt haben, dass Mitarbeiter Freeware über einen Firmen-PC herunterladen.
- 44% der Mitarbeiter in Großunternehmen Streaming Media-Anwendungen nutzen.

Vorteile der Verwendung von Premium Gruppen

Sicherheits-, Produktivitäts- und Bandbreitenprobleme innerhalb eines Unternehmens können durch folgende Maßnahmen bekämpft werden:

- Verhinderung einer Datenübertragung von Spyware an Spyware-Hosts, wirksamer Schutz gegen den Verlust vertraulicher Daten.
- Minimierung des Risikos von Malicious Mobile Code-Angriffen am Arbeitsplatz einschließlich über das Internet übertragbarer Viren, Trojaner, Würmer, Script-Angriffe und Rogue Internet Code.
- Filterung störender Bannerwerbung
- Erhöhung der Produktivität durch eine Zugangskontrolle zu Instant Messaging-Anwendungen
- Vermeidung von Haftungsrisiken und Bandbreitenmissbrauch durch Zugangskontrolle zu Peer-to-Peer-Anwendungen



Premium Gruppen-Kategorien sind nahtlos in den Websense Enterprise Manager integriert.

SiteWatcher™ ist ein in Websense Security-PG enthaltener Dienst, der Unternehmen bei Infektion der eigenen Webseite mit MMC alarmiert, damit sofort Maßnahmen ergriffen werden können, um eine Verbreitung von MMC beim Besuch der Webseite durch Kunden, Interessenten und Partner zu verhindern.

Steigerung der Mitarbeiterproduktivität

Mit Hilfe der Produktivitäts-PG können Unternehmen die Produktivität ihrer Mitarbeiter spürbar verbessern, indem sie den Zugriff auf Webseiten unterbinden, deren Inhalte gerne von „Cyber-Faulenzern“ genutzt werden und die als geschäftlich nicht relevant klassifiziert sind.

Die Produktivitäts-PG hilft, den Zugriff durch Mitarbeiter auf folgende Kategorien zu regulieren:

- Werbung
- Onlineforen & Clubs
- Freeware- & Softwaredownloads
- Online-Brokerage & Wertpapierhandel
- Instant Messaging (IM)
- kostenpflichtige Dienste

Verwaltung der Bandbreite im Netzwerk

Bandbreite ist in allen Netzwerken eine nur beschränkt verfügbare Ressource. Bestimmte Internetaktivitäten von Mitarbeitern wie z.B. der Zugriff auf Streaming Media-Dienste, die Übertragung persönlicher Dateien oder Fotos in eine virtuelle Festplatte und das Herunterladen urheberrechtlich geschützter Musik und sonstiger Daten verringert die für betriebswichtige Anwendungen verfügbare Bandbreite, und kann zu Haftungsrisiken und Urheberrechtsverletzungen führen.

Websense Enterprise Bandbreiten-PG™ ist ein leistungsfähiges Softwarewerkzeug für das Bandbreitenmanagement.

Die Bandbreiten-PG reguliert die Internetnutzung in folgenden Bereichen:

- Streaming Media-Inhalte
- Internetradio und Internet-TV
- virtuelle Festplatten & persönliche Datensicherung im Internet
- Internettelefonie
- Peer-to-Peer-Anwendungen

Wie funktioniert die Zusammenarbeit zwischen Premium Gruppen und Websense Enterprise?

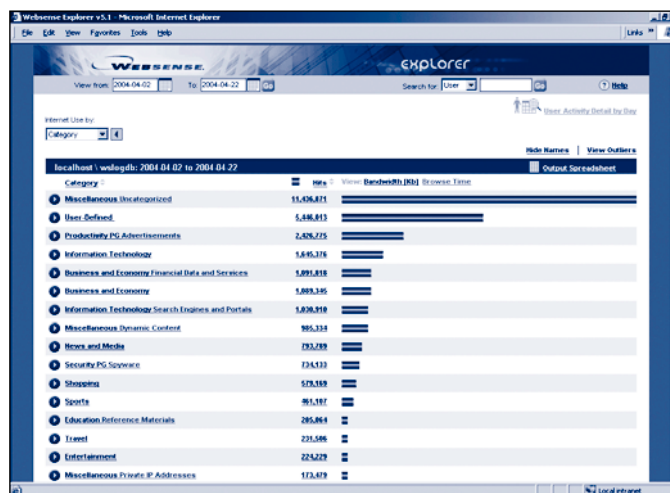
Alle Premium Gruppen-Produkte können nahtlos in die bestehende Websense Enterprise-Umgebung integriert werden.

Nach der Installation aktivieren Premium Gruppen zusätzliche Kategorien im Websense Manager und ergänzen die Websense Enterprise Datenbank. Unternehmen können auf Benutzer oder Benutzergruppen abgestimmte Richtlinien definieren und Berichte erstellen.

Premium Gruppen-Kategorien sind nahtlos in den Websense Enterprise Manager integriert.



Richtlinien für Premium Gruppen gewährleisten eine Zugangskontrolle für Kategorien mit hohem Sicherheitsrisiko.



Premium Gruppen-Kategorien sind nahtlos in den Websense Enterprise Manager integriert.

Download der kostenfreien, voll funktionsfähigen 30 Tage Testversion unter www.websense.de

Websense Inc.
San Diego, CA USA
Tel.: 800.723.1166
Tel.: 858.320.8000
www.websense.com

Websense UK Ltd
Chertsey, UK
Tel.: +44 (0)1932. 796001
www.websense.co.uk

Websense France SARL
Paris, Frankreich
Tel.: +33 (0)15660. 5814
www.websense.fr

Websense Deutschland GmbH
München, Deutschland
Tel.: +49 (0)89 24445. 4005
www.websense.de

Websense Japan
Tokio, Japan
Tel.: +813.5322.1335
www.websense.co.jp

Websense Australia
Sydney, Australien
Tel.: +61 2 9006. 1621
www.websense.com.au

Websense Greater China
Hong Kong
Tel.: +852.2855.8811
www.chinese.websense.com
www.prc.websense.com

Websense Latin America
Sao Paulo, Brasilien
Tel.: +55.11.4612.0798
www.espanol.websense.com
www.portugues.websense.com