

MailScan

Viren- und Spamschutz und Inhaltssicherheit am Mail-Gateway



MailScan

MailScan ist der hochentwickelteste Echtzeit-Viren- und -Spamschutz der Welt für Mailserver. Er ist verfügbar für Plattformen wie Windows, Unix, Linux, Novell und Solaris. MailScan fungiert als leistungsstarkes und proaktives Sicherheitsgateway zwischen dem Mailserver und Internet, um Ihre E-Mail-Infrastruktur in Echtzeit umfassend zu sichern.

Wie funktioniert MailScan?

MailScan scannt alle E-Mails, bevor diese in die Mailboxen gelangen bzw. über Mailserver hinausgeschickt werden. Daher ist MailScan eine Lösung für totale Sicherheit am Mail-Gateway. Diese Sicherheitslösung kontrolliert den gesamten Innen- und Außenmailverkehr einer Organisation.

Hauptmerkmale von MailScan

Webbasierte Verwaltungskontrolle

Auf die MailScan-Verwaltungskontrolle kann durch den Browser zugegriffen werden. Alle Operationen können mithilfe dieser leistungsstarken webbasierten Konsole konfiguriert und zentral verwaltet werden. Dadurch wird die Fernverwaltung dieser Anwendung aktiviert.

Umsetzung der integrierten Sicherheitsrichtlinie

MailScan befähigt Sie, gemäß den universellen bzw. firmenspezifischen Richtlinien Regelsätze zu erstellen.

Schutz vor (Bilder-)Spam und Phishing

MailScan verwendet eine Kombination von Technologien wie die Realtime-Blackhole-Liste (RBL), Überprüfung der in Echtzeit abfragbaren Schwarzen Liste der URLs der Spamversender (SURBL), MX/A DNS Rekordüberprüfung, Reverse-DNS-Abfrage, X-SPAM-Regelüberprüfung, Sender Policy Framework und Unaufdringliches Lernen (NILP*), um Spam- und Phishing-Mails und Bilderspam zu blockieren.

Echtzeitvirenprüfung am Mail-Gateway

Dieses Modul prüft mittels der leistungsstarken und heuristisch angetriebenen Doppelantivirengines alle E-Mails in Echtzeit auf Viren, Würmer, Trojaner, Spyware, Adware und versteckten bösartigen Inhalt. Dadurch werden Online-Bedrohungen abgewendet, bevor sie über E-Mails in das Netzwerk gelangen. Ausgeklügelte heuristische Scantechnologie wird eingesetzt, um neuere Viren und versteckte Schädlinge proaktiv und präventiv zu blockieren.

Echtzeitinhaltskontrolle

Alle ein- und ausgehenden Nachrichten werden gemäß den Sicherheitsrichtlinien eines Unternehmens in Echtzeit auf anstößige Wörter und Inhalt für Erwachsene (Adult-Content) geprüft, um den Spam zu filtern. Dabei wird die firmeneigene hochentwickelte Technologie namens NILP* (Unaufdringliches Lernen) verwendet. Die-ser Technologie liegt die Intelligenz zugrunde, jede E-Mail zu analysieren und sie gemäß den Verhaltensmustern der Benutzer als Spam bzw. Ham zu klassifizieren.

Graue Liste (Greylisting)

Bei der Methode „Graue Liste“ werden die E-

Mails von unbekanntem Absendern temporär abgewiesen, da die meisten Spamservers nicht versuchen, eine Mail wiederzuschicken, die bereits einmal abgewiesen wurde. Wenn es eine legitime Mail gibt, wird der Quellrechner in meisten Fällen versuchen, sie wiederzuschicken. Dann wird sie angenommen.

LDAP- und POP3-Authentifizierung

MailScan überprüft durch die webbasierte LDAP- und POP3-Authentifizierung die Identität der berechtigten Benutzer und schränkt den unautorisierten Zugang zu den Mails ein.

Weißer Liste der E-Mail-Adressen

Wenn ein lokaler Benutzer eine E-Mail schickt, wird die Adresse des Empfängers automatisch durch das System der Weißen Liste der E-Mail-Adressen hinzugefügt.

Clusterbildung

Verteilung der Mails auf mehrere Computers durch Scannen hilft bei der Lastenteilung des MailScans.

Relaykontrolle

Die Relaykontrolle hindert Spammern daran, die IP-Adresse und den Mailservern Ihrer Firma zum Versenden von Spam zu verwenden.

Archivierung der E-Mails und Anhänge

Die Archivierung der ein- und ausgehenden E-Mails und E-Mail-Anhänge kann individuell angepaßt werden, um deren Inhalt umfassend zu kontrollieren.

E-Mail-Anhänge filtern

Es gibt umfangreiche Möglichkeiten, um das Versenden oder Empfangen bestimmter Anhänge wie EXE, COM, CHM oder BAT zu blockieren.

Benutzerdefinierte Fußtexte

Durch diese Option können benutzerdefinierte Fußtexte einfach allen ausgehenden und internen E-Mails angehängt werden.

TCP-Verbindungen

Diese Option zeigt alle TCP/UDP-Verbindungen wie Prozesse, Protokolle, lokale Adresse, Fernadresse und Status in dem System an.



Ausführliche Reports

MailScan bietet ausgereifte analytische Reports in grafischen und nicht-grafischen Formaten an.

Komprimierte automatische Updates

Viren- und Spamsdatenbanken werden stündlich automatisch aktualisiert, um Benutzer umgehend vor neu entstehenden Gefahren zu schützen.

24x7 Kostenfreier Technischer Dienst

MailScan wird rund um die Uhr durch kostenfreien technischen Dienst per Telefon und Online (per E-Mail, Live Chat und Forums) unterstützt.

Minimale Systemvoraussetzungen:



Prozessor: Pentium II 200 MHz oder höher
RAM: 128 MB (256 MB empfohlen)
Festplatte: 500 MB freier Plattenplatz
Betriebssystem: Windows 2008 / Vista / XP / 2003 (32-/64-Bit) / 2000 / NT / ME / 98
Internet Explorer 5.0
CD-ROM-Laufwerk

*NILP=Non-Intrusive Learning Patterns

Spezielle MailScan-Versionen sind verfügbar für folgende Mailserver:
SMTP ohne Virenschutz, Microsoft Exchange 2000/2003/2007, Lotus Domino, MailServers, CommuniGate Pro, Mail Daemon, VPOP3, Mailtraq, Mailtraq Lite, DMail/SurgeMail, Postmaster Pro, Postmaster Enterprise, Merak, Avirt, Sharemail, Netnow, SpearMail, VOPMail, CMail, GiftMail, MailMax, IAMS, LAN-Projekt, Winroute, WinProxy, 1. UpMailServer und MailServers ohne Virenschutz.