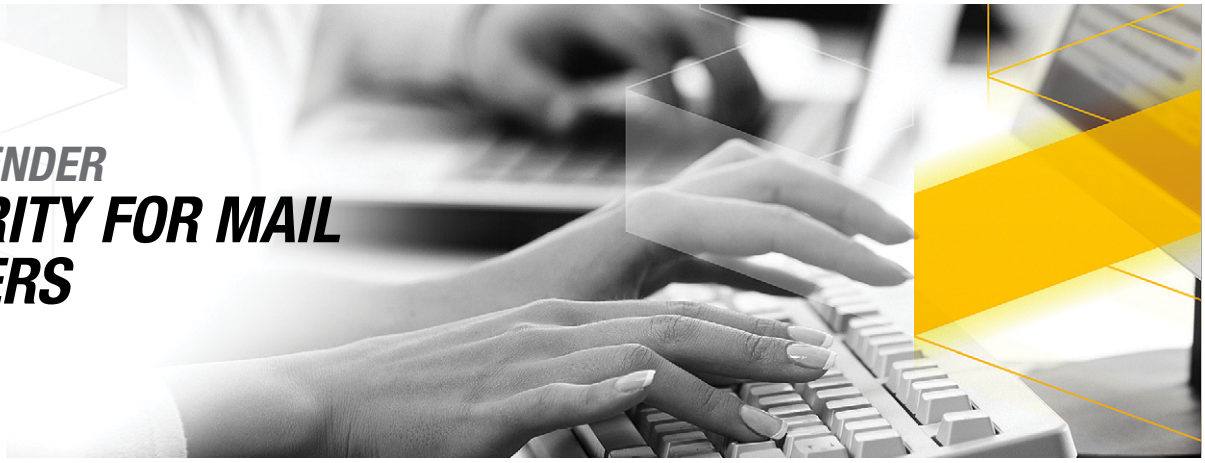


BITDEFENDER SECURITY FOR MAIL SERVERS

SICHERE POSTEINGÄNGE OHNE SPAM

Die E-Mail ist zu einem unverzichtbaren Dienst geworden, den Unternehmen um jeden Preis schützen müssen. Fällt der E-Mail-Server aus, so gilt dies auch für die Mitarbeiter. Die Auswirkungen von Produktivitätsverlusten in Kombination mit einer kritischen Vireninfektion per E-Mail können ein Unternehmen in die Knie zwingen. Viele Unternehmen wägen zwar die internen Folgen von Vireninfektionen per E-Mail ab, doch ernst zu nehmen sind auch die Gefahren für das Image des Unternehmens und die möglichen Schäden, sollte ein Mitarbeiter versehentlich eine infizierte E-Mail an Partner oder Kunden versenden. Gerade die Schäden am Unternehmens-Image sind häufig irreparabel.

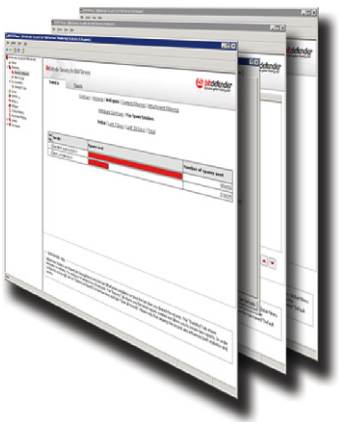
Das E-Mail-System eines Unternehmens stellt einen der Haupteingangs- und -ausgangspunkte für Malware-Verbreitung und Datenlecks des Netzwerks dar. Daher sollten E-Mail-Lösungen in der Lage sein, mit den zahlreichen Bedrohungen umzugehen, die auf die E-Mail-Systeme von Unternehmen abzielen – darunter:

- Versand oder Empfang von Schad-Software über E-Mail-Anhänge
- Unerwünschte Kommunikation in Form von Spam
- Phishing-Versuche, um an vertrauliche Informationen zu gelangen
- Legitime Benutzer, die vertrauliche Daten per E-Mail zugänglich machen
- Dictionary Harvesting Attacks (DHA)

Die Mechanismen zur Verbreitung von Malware per E-Mail werden immer virulenter – es kann zu spät sein, die Malware erst auf dem Desktop zu stoppen. Vielmehr bietet sich eine Lösung an, die im Außenbereich des Netzwerks und auf dem Mail-Server selbst eingesetzt wird und die Auswirkungen von Malware minimiert, indem sie infizierte Dokumente reinigt und das wichtigste Unternehmenskapital schützt – die Kommunikation der Mitarbeiter.

SICHERE E-MAIL-DIENSTE MIT BITDEFENDER

BitDefender Security for Mail Servers mit preisgekrönten Antiviren-, Antispyware-, Antispam-, Antiphishing- sowie Inhalts- und Anhangfiltertechnologien schützt Windows- oder Unix-basierte Mail-Server vor bekannten und neuen Sicherheitsrisiken. Die Lösung schützt die E-Mail-Dienste von Unternehmen und ermöglicht außerdem Produktivitätssteigerungen, indem sie Spam blockiert und gemeinsame zentrale Management-Tools bietet.



BitDefender Security for Mail Servers prüft E-Mails auf verschiedenen Ebenen. Zunächst wird untersucht, ob der Mail-Server des Absenders verdächtig ist oder blockiert wird, dann werden Inhalte und Anhänge auf Malware geprüft und mit Spam-Regeln abgeglichen.

HAUPTMERKMALE UND -VORTEILE

- Prüft den eingehenden E-Mail-Verkehr und bietet so Echtzeitschutz vor Malware und minimiert das Ausbreitungsrisiko von Viren im Netzwerk
- Prüft ausgehende E-Mails, um zu verhindern, dass Sicherheitsrisiken Ihre Partner und Kunden erreichen
- Prüft jede E-Mail einmalig mit einer ausgewählten Methode, um die Server-Last zu minimieren
- Inhaltsfilter sowohl für eingehende als auch für ausgehende E-Mails, die spezifische vom Administrator definierte Schlüsselwörter wie z. B. Kreditkartendaten erkennen
- Antispam- und Antiphishing-Präzisionsfilter mit heuristischer NeuNet-Technologie
- Schutz der Benutzerverzeichnisse vor Harvesting-Angriffen von Spammern, die mit gewaltsamen Techniken legitime E-Mail-Adressen an sich bringen wollen
- Ermöglicht über den zentralen BitDefender Management Server die Remote-Konfigurationen von einem beliebigen Unternehmens-Computer aus
- Reduzierte Ressourcenkosten und Aufwendungen führen zu gesteigerter Geschäftsproduktivität
- Minimierte Ausfallzeiten des Netzwerks für mehr operative Effizienz

Bitdefender

BITDEFENDER TECHNOLOGIEN

b-have Sämtliche Lösungen von BitDefender beinhalten B-HAVE, eine zum Patent angemeldete Technologie, die das Verhalten potenziell schädlicher Codes in einem virtuellen Computer analysiert, falsch positive Ergebnisse eliminiert und die Erkennungsraten neuer bzw. unbekannter Schad-Software signifikant erhöht.

NeuNet Um neuen Spam besser in den Griff zu bekommen, hat das BitDefender Lab den leistungsstarken Spamfilter NeuNet geschaffen. NeuNet wird im Antispam-Labor mithilfe einer Vielzahl von Spam-Nachrichten trainiert und lernt so, neuen Spam anhand von Ähnlichkeiten mit den bereits untersuchten Nachrichten zu erkennen.

UMFASSENDER SCHUTZ

BitDefender Security for Mail Servers ist nur ein Element einer umfassenden Suite von Lösungen, die Rund-um-Netzwerkschutz vom Gateway bis zum Desktop bieten. Die proaktiven Multi-Plattform-Produkte erkennen und stoppen Viren, Spyware, Adware und Trojaner, die die Integrität Ihres Netzwerks bedrohen.

SYSTEMANFORDERUNGEN

Windows-basierte Betriebssysteme:

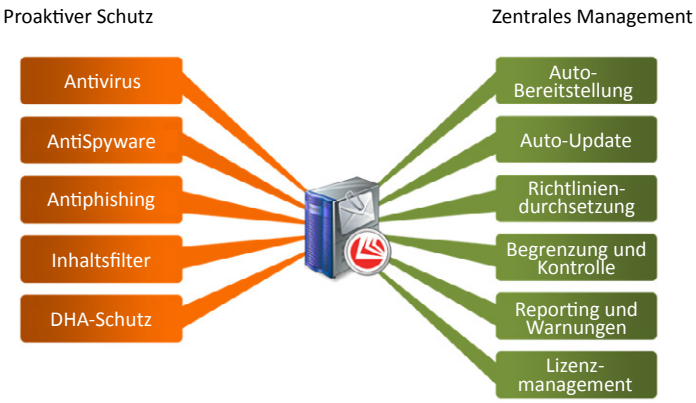
- Windows Server 2000 SP4 + Update Rollup 1
- Windows Server 2003 mit SP1, Windows Server 2003 R2
- Windows Server 2008, Windows Server 2008 R2, Windows Small Business Server (SBS) 2008
- Internet Explorer Version 6.0 oder höher

UNIX-basierte Betriebssysteme:

- Linux, FreeBSD, Solaris
- Linux-Kern: 2.6.18 oder höher
- glibc: 2.3.1 oder höher, libstdc++ von gcc 4 oder höher

Unterstützte Distributionen:

- Debian GNU/Linux 3.1 oder höher
- Fedora Core 1 oder höher
- FreeBSD: 5 (oder höher mit compat5x)
- Mandrake/Mandriva 9.1 oder höher
- Novell SuSE Linux Enterprise Server 9, Linux 8.2 oder höher
- OpenSolaris 2008 oder 2009 (x86-Plattform)
- Oracle Linux 5 oder höher
- RedHat Enterprise Linux 3, Linux 9 oder höher
- Slackware 9.x oder höher
- Solaris 9 oder 10 (x86-Plattform)



BitDefender Security for Mail Servers bietet proaktiven Schutz und zentrales Management von E-Mail-Diensten

INNOVATIVE PROAKTIVE ERKENNUNG UND SCHUTZFUNKTION

Die preisgekrönten Prüf-Engines von BitDefender wurden von führenden Zertifizierungsbehörden wie ICSA Labs, Virus Bulletin und West Coast Labs wegen ihres unschlagbaren proaktiven Schutzes vor Malware ausgezeichnet. BitDefender bietet mehrfachen Schutz durch hochentwickelte Technik.

Antivirus – Zusätzlich zur signaturbasierten Erkennung bietet BitDefender auch heuristische Erkennungsmethoden, die einen virtuellen „Computer im Computer" simulieren und hier alle Dateien und Software auf schädliches Verhalten hin überprüfen. Diese Technik liefert weniger falsch positive Ergebnisse und hat deutlich bessere Erkennungsraten bei Zero-Day- und unbekannten Bedrohungen.

Antispam – Unter Verwendung ständig aktualisierter schwarzer und weißer Listen bekannter Spam-Sites bilden Bayessche Lernprozesse eine weitere Erkennungsmethode, die sich an die Änderungen von Spammern zur Umgehung von statischen Spamfiltern anpasst.

Antispyware – BitDefender spürt bekannte Spy- und Adware über Dateiprüfmethoden auf, um Infektionen mit Spyware und damit verbundene Risiken von Datenlecks nach außen zu unterbinden.

Antiphishing – Phishing-Sites werden zwar eher als persönliche Bedrohung denn als Gefahr für Unternehmen betrachtet, können aber sehr wohl Daten von den Mitarbeitern Ihres Unternehmens „ernten". Mit einer Kombination von ständig aktualisierten schwarzen und weißen Listen, verhindert BitDefender, dass Benutzer auf bekannte Phishing-Seiten zugreifen und verhindert somit eine Beeinträchtigung.

Inhaltsfilterung – Inhaltsfilter erkennen vordefinierte Informationen wie Kreditkarten- oder Namen von Kundendatenbanken etc. und dass sie den Kontrollbereich des Unternehmens verlassen. Die Inhaltsfilterung verwendet auf Web- oder FTP-Serveradresse, Schlüsselbegriffen und Inhaltsgröße basierende, anpassbare Beschränkungen.

Schutz vor Directory Harvesting-Angriffen (DHA) – Spammer versuchen, gültige und bestehende E-Mail-Adressen aufzuspüren. Directory Harvrsting ist besonder geeignet die E-Mail-Adressen von Unternehmen in Erfahrung zu bringen, da diese oft standardisiert sind. Die so generierten E-Mails können den Spam-Filter umgehen, da sie an tatsächliche Anwender adressiert sind.

Weiße und schwarze Listen – Dienen dem Ausschluss spezifischer E-Mail-Server oder der impliziten Wertung von E-Mail-Servern als vertrauenswürdig mit der Option, ihre IP-Adressen zu validieren und mit der Domäne des Absenders abzugleichen.

KONFIGURIEREN SIE DIE SCAN-OPTIONEN

BitDefender Security for Mail Servers bietet Continuous-, On-Request-, Transport- und Full-Scanning-Methodologien, um Schad-Code aufzuspüren und die Integrität der E-Mail-Dienste zu gewährleisten. Jede E-Mail wird nur ein einziges Mal anhand der gewählten Methode geprüft und kann mit einer frei konfigurierbaren Signatur gekennzeichnet werden. Zusätzliche Inhaltsprüfmethoden können konfiguriert werden, um zu verhindern, dass vertrauliche Informationen von bestimmten Benutzergruppen versehentlich versendet werden.

vb 100 VIRUS virusbtn.com

vb VERIFIED SPAM virusbtn.com

Bitdefender