McAfee Security for Email Servers

Leistungsfähiger Schutz für Inhalte auf Microsoft Exchange- und Lotus Domino-Servern

McAfee® Security for Email Servers erkennt und filtert Viren, Würmer, Trojaner sowie weitere potenziell unterwünschte Programme. Die Lösung ist mit Microsoft Exchange- und Lotus Domino-Servern kompatibel, blockiert Spam und filtert Nachrichten, damit unangemessene oder sensible Informationen weder in Ihr Netzwerk gelangen noch Ihr Netzwerk verlassen können. Dadurch wird die Einhaltung von Richtlinien und Compliance-Anforderungen vereinfacht.

McAfee verbindet Inhaltsprüfung, Reputationsanalyse und Malware-Schutz, um Ihre E-Mails zu schützen. Unsere Lösung bietet mehrstufige Sicherheitsmaßnahmen sowie verschiedene Optionen für die Umsetzung des E-Mail-Schutzes: Edge-Transport an der Netzwerkperipherie, Hub-Transport-Server und Mailbox-Server.

Hauptvorteile

- *Gewährleistung, dass Ihr System aktiv ist und ausgeführt wird:* Verhindern Sie, dass Viren und Würmer über E-Mails in Ihr Netzwerk gelangen oder sich per Microsoft Exchange oder Lotus Domino intern verbreiten.
- *Garantiert produktive Mitarbeiter:* Blockieren Sie Spam und Phishing-Angriffe.
- *Verwaltung über eine einzige Konsole:* Dank der Software McAfee ePO steht Ihnen eine leistungsstarke, zentrale Verwaltungskonsole zur Steuerung, Verwaltung und Dokumentation zur Verfügung.
- *Schutz kritischer Daten:* Filtern Sie ein- und ausgehende E-Mails, um Ihre Informationen zu schützen und dank DLP- sowie Reputationstechnologien (für IP-Adressen, Nachrichten und Dateireputation) das Haftungsrisiko für das Unternehmen zu senken.
- *Intuitive grafische Benutzeroberfläche:* Über die einfach zu bedienende Benutzeroberfläche stehen umfangreiche Berichtsmöglichkeiten, Diagramme und Echtzeitstatistikdaten zum E-Mail-Verkehr zur Verfügung.

McAfee Security for Email Servers bietet mehrstufigen Schutz für ein- und ausgehende E-Mails. Der Funktionsumfang reicht dabei von On-Demand-Malware-Scans bis zur Durchsetzung von Richtlinien zum Schutz vor Datenverlust oder Missbrauch vertraulicher Daten.

- *Branchenweit führender Schutz:* Nutzt die preisgekrönte Funktion für speicherinterne und inkrementelle On-Demand-Scans zur Erkennung sowie Entfernung von Viren, Würmern, Trojanern und anderen Bedrohungen aus ein- bzw. ausgehenden E-Mails.
- *Starke interne Schutzmaßnahmen:* Entdeckt Bedrohungen, die unbemerkt an Ihren Peripherie-Abwehrmaßnahmen vorbei oder über infizierte Laptops sowie interne E-Mails in Ihr Netzwerk gelangt sind. Außerdem wird Spam mit dem Spam-Schutzmodul blockiert.
- *Leistungsstarke Inhaltsfilterung:* Erzwingt Unternehmensrichtlinien für die E-Mail-Nutzung, indem unzulässige Dateitypen sowie anstößige Inhalte gefiltert und Kompromittierungen sensibler Daten verhindert werden.
- *Verwaltung über eine einzige Konsole:* Verwendet die Plattform McAfee ePolicy Orchestrator® (McAfee ePO™) zur Bereitstellung und Verwaltung von Sicherheitsmaßnahmen sowie zur Darstellung detaillierter grafischer Berichte.

Mehrstufiger E-Mail-Schutz

Umfassender Malware-Schutz

Ein wichtiger Bestandteil von McAfee Security for Email Servers stellt das Malware-Schutzmodul zur Echtzeit-Dateireputationsbewertung dar, mit dem neu aufkommende Bedrohungen erheblich zuverlässiger erkannt werden können. Mithilfe der Cloud-basierten McAfee Global Threat Intelligence™-Technologie (McAfee GTI™) sendet McAfee einen Fingerabdruck jeder verdächtigen Datei zur sofortigen Untersuchung an die McAfee Labs. Wird der Fingerabdruck als bekannte Malware identifiziert, erhält der Server innerhalb weniger Millisekunden die Information, dass die fragliche Datei blockiert oder isoliert werden muss. Die Reputation für E-Mail-Nachrichten und Absender wird vom umfassenden, in Echtzeit funktionierenden und Cloud-basierten Reputationsdienst McAfee GTI ermittelt, durch den McAfee-Produkte vor bekannten und neuen nachrichtenbasierten Bedrohungen wie Spam schützen können.

E-Mail-Reputation

Die E-Mail-Reputation lässt sich mit Faktoren wie Spam-Versandmustern und IP-Verhalten kombinieren, um die Wahrscheinlichkeit böswilliger Inhalte in der betreffenden Nachricht zu ermitteln. Die Einstufung basiert auf mehreren Faktoren: einerseits auf den von Sensoren (sie richten Anfragen an die McAfee-Cloud) gesammelten Informationen und den von McAfee Labs durchgeführten Analysen, andererseits auf der Korrelation von vektorübergreifenden Informationen zu Bedrohungen aus dem Internet, aus E-Mails und Netzwerken.

IP-Reputation

Erkennen Sie Bedrohungen in E-Mails basierend auf der IP-Adresse des Servers, der die E-Mail gesendet hat. Die IP-Reputation unterstützt Sie dabei, gefährliche E-Mails bereits am Gateway zu blockieren und damit Schäden sowie Datenkompromittierungen zu verhindern.

Schutz für Ihre Server rund um die Uhr

Prüfen Sie ein- und ausgehende E-Mail-Nachrichten auf Viren, Würmer, Trojaner sowie andere Malware. Außerdem haben Sie die Möglichkeit, alle internen E-Mails zu prüfen und dadurch die interne Verbreitung von Würmern zu verhindern. McAfee Security for Email Servers lädt automatisch die neuesten Virusdefinitionen (DAT-Dateien) über HTTP, FTP, Netzwerkdateifreigaben oder die zentrale Verwaltungskonsole McAfee ePO herunter.

Umsetzung von Compliance-Vorschriften

Filtern Sie Nachrichten auf Grundlage ihrer Größe, der Nachrichteninhalte oder der Anhanginhalte. Blockieren oder isolieren Sie Nachrichten, die vorher definierte Inhalte in der Betreffzeile, im Nachrichtentext oder in Anhängen enthalten.

Spezifikationen

McAfee Security for Email Servers trägt dem steigenden E-Mail-Aufkommen und dem wachsenden Umfang gemeinsam genutzter Daten auf E-Mail-Servern Rechnung. Daher unterstützt die Lösung sowohl Microsoft Exchange- als auch Lotus Domino-Umgebungen, damit Ihre Mitarbeiter produktiv bleiben und die Aufrechterhaltung Ihres Geschäftsbetriebs rund um die Uhr gewährleistet werden kann.

Anforderungen für McAfee Security for Microsoft Exchange

Anforderungen an das Betriebssystem

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

Anforderungen an den Microsoft Exchange-Server

- Exchange Server 2003 (einschließlich 32-Bit-Version)
- Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013
- Exchange Server-Cluster-Umgebungen werden unterstützt

Anforderungen für McAfee Security for Lotus Domino on Windows

- Windows Server 2008 und 2008 R2
- Unterstützung für Lotus Domino 8.5.x (32- und 64-Bit-Versionen)

Anforderungen für McAfee Security for Lotus Domino on Linux

- Novell SUSE Linux Enterprise Server (SLES) 10 und 11
- Red Hat Enterprise Linux (RHEL) 5.x und 6.x
- Lotus Domino 8.5 (32- und 64-Bit-Versionen)

Verringerter Zeit- und Ressourcen-Aufwand

Die standardmäßig im Produkt enthaltenen Inhaltsfilter vereinfachen die Erstellung und Durchsetzung von Richtlinien. Sie können Regeln auf globaler Basis erstellen und bei Bedarf Ausnahmen für einzelne Personen oder Abteilungen definieren. Die Verwaltung erfolgt über die integrierte HTML-Schnittstelle oder die McAfee ePO-Plattform.

Inhaltsfilterung

Sie können Inhalte und den Text in der Betreffzeile oder im Textteil einer E-Mail-Nachricht sowie im E-Mail-Anhang prüfen. Für die Erstellung eigener Inhaltsfilter-Regeln können Sie reguläre Ausdrücke (Regex) nutzen.

Schutz vor Datenverlust und Gewährleistung der Compliance

Mit der Funktion zum Schutz vor Datenkompromittierung (Data Loss Prevention, DLP) wird gewährleistet, dass versendete (bewegte) oder ruhende E-Mails den Vertraulichkeits- und Compliance-Vorschriften entsprechen, die für Ihr Unternehmen gelten. Dank der vorinstallierten Wörterbücher für unternehmens- und landesspezifische Compliance-Regeln wird die Einrichtung erheblich vereinfacht. Der integrierte Workflow leitet isolierte E-Mails automatisch zur Überprüfung an Prüfer weiter.

Spam-Filter und Produktivitätssteigerung

Mit dem Spam-Schutzmodul können Sie Spam- sowie Phishing-E-Mails abfangen und damit die Produktivität Ihrer Mitarbeiter gewährleisten. Gleichzeitig sparen Sie wertvollen Speicherplatz auf dem E-Mail-Server. Benutzer können eigene White- und Blacklists erstellen. Durch die zentrale Quarantäne, die gemeinsam mit anderen Gateway-E-Mail-Lösungen von McAfee verwendet wird, können Benutzer einfach auf eine Quarantäne-Quelle zugreifen.

Benachrichtigungen über den Produktzustand

McAfee Security for Email Servers sendet Benachrichtigungen über den Produktstatus an den festgelegten Administrator. Diese Benachrichtigungen können entsprechend Ihren Anforderungen konfiguriert und geplant werden.

Aktualität mit geringem Aufwand

Nutzen Sie automatische Aktualisierungen, und halten Sie sich mit den neuesten Sicherheitsinformationen von McAfee Labs, dem weltweit besten Forschungszentren für Bedrohungen, auf dem Laufenden.

Zentralisierung und Isolierung der E-Mail-Quarantänen

Der in McAfee Security for Email Servers enthaltene McAfee Quarantine Manager konsolidiert die Quarantäne- und Spam-Schutz-Verwaltung in einer Lösung. McAfee Quarantine Manager ist einfach in der Verwaltung, ermöglicht die Einsendung von Proben an McAfee Labs und bietet detaillierte Verwaltungsfunktionen, automatische Benutzersynchronisierung von LDAP-Servern, Verwaltung von global oder für Benutzer geltenden Black- und Whitelists sowie umfassende Berichterstellung. Diese Funktionen werden vollständig über die McAfee ePO-Plattform verwaltet.

Unterstützung aller Ihrer Server

Der Schutz steht für E-Mail-Server mit den wichtigsten Betriebssystemen einschließlich Windows und Linux auf 32-Bit- und 64-Bit-Plattformen zur Verfügung.

Prüfung und Schutz des E-Mail-Speichers

McAfee Security for Email Servers unterstützt geplante On-Demand-Scans und ermöglicht detaillierte Konfigurationen, damit Sie nicht nur herkömmliche komplette Scans, sondern auch Schnell-Scans durchführen können. Sie können dabei wählen, ob nur E-Mails mit Anhängen, ungelesene E-Mails, Betreffzeilen, Absender, Empfänger, CC-Empfänger, die Nachrichten-ID oder solche E-Mails geprüft werden sollen, die innerhalb eines bestimmten Zeitraums erhalten wurden oder eine bestimmte Größe haben.

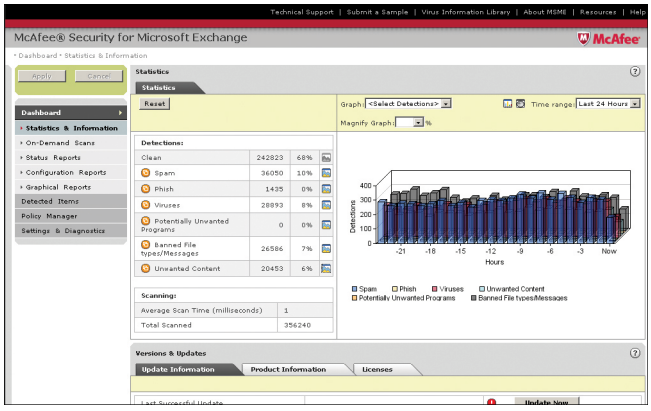

Abbildung 1: Die einfach zu bedienende Benutzeroberfläche stellt umfangreiche Berichtsmöglichkeiten, Diagramme und Echtzeitstatistikdaten zum E-Mail-Verkehr zur Verfügung.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

McAfee, das McAfee-Logo, ePolicy Orchestrator, McAfee ePO, McAfee Global Threat Intelligence und McAfee GTI sind Marken oder eingetragene Marken von McAfee, Inc. oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2013 McAfee, Inc.
60079ds_security-email-servers_0213_fnl_ASD