KASPERSKY SECURITY FOR LINUX® MAIL SERVER

Kaspersky Security for Linux Mail Server bietet internen und Remote-Benutzern (Laptops, Tablets und Smartphones) Spam- und Phishing-Schutz sowie Schutz vor generischen und hochentwickelten Malware-Bedrohungen.

WICHTIGSTE VORTEILE:

- EINE DER BRANCHENWEIT HÖCHSTEN SPAM-ERKENNUNGSRATEN
- VERBESSERTER ECHTZEIT-SCHUTZ VOR MALWARE UND EXPLOITS, INKLUSIVE ZERO-HOUR-SCHWACHSTELLEN
- GEMEINSAMES MANAGEMENT MIT IHRER ENDPOINT-SICHERHEIT ÜBER EINE ZENTRALE KONSOLE

SCHUTZ VOR SPAM

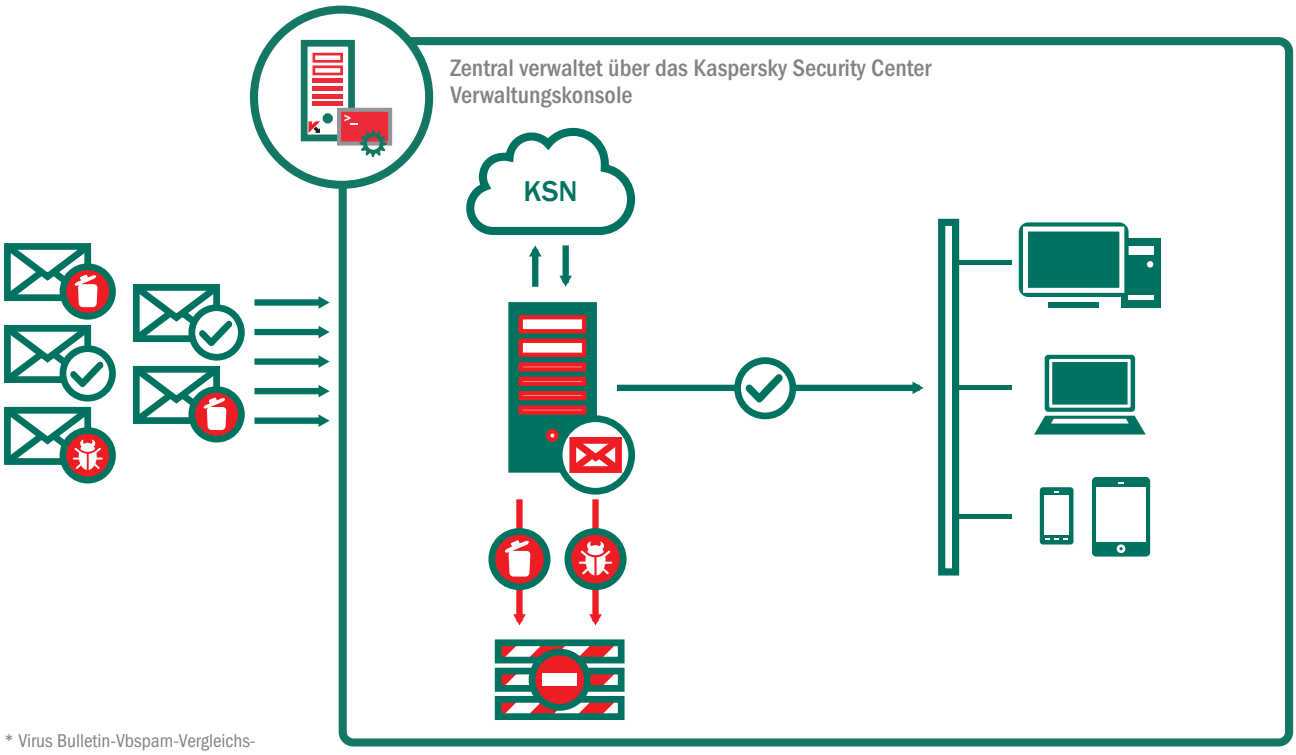
Die von Kaspersky Lab intern entwickelte Spam-Schutz-Engine blockiert bis zu 99,92 %* des zeitraubenden Spam-Verkehrs, wobei Fehlalarme (False-Positives) auf ein Minimum reduziert werden. Dies wird durch einen kombinierten technologischen Ansatz erreicht:

- **Obligatorische Anti-Spam-Updates** – Verwendung der Push-Technologie, um Updates zur Echtzeit-Spam-Identifizierung direkt aus der Cloud bereitzustellen. So wird die Sicherheit immer gewährleistet.
- **Reputationsfilterung** – Schutz vor Spam durch Isolation und erneute Analyse von verdächtigen E-Mails anhand neuester Spam-Informationen.
- **Phishing-Schutz** – Echtzeit-Zugriff auf die Informationen im Kaspersky Security Network, um E-Mails mit Phishing-Links zu erkennen und unmittelbar zu blockieren.
- **Erkennung von Massen-E-Mails** – Identifizierung von Massen-E-Mails, die blockiert werden, bevor sie den Endbenutzer erreichen.

SCHUTZ VOR MALWARE-BEDROHUNGEN

Kaspersky Security for Linux Mail Server verwendet einen mehrschichtigen Anti-Malware-Ansatz, der drei leistungsstarke Schutztechnologien kombiniert:

- **Vielfach ausgezeichnete Anti-Malware-Engine von Kaspersky Lab** – wird in Echtzeit vom cloudbasierten Kaspersky Security Network unterstützt.
- **ZETA Shield** – vorausschauender Schutz vor Exploits einschließlich Zero-Hour-Schwachstellen.
- **URL-Filter** – identifiziert und blockiert E-Mails, die Links zu schädlichen Webseiten und Dateien enthalten.



* Virus Bulletin-Vbspam-Vergleichstest – November 2013

MANAGEMENT UND ÜBERWACHUNG

Verschiedene Management-Optionen über eine integrierte Konsole und eigenständige Web-Oberfläche.

Kaspersky Security for Linux Mail Server wird über ein einziges intuitives Web-Dashboard verwaltet und sorgt für eine optimale Effizienz und nahtloses Deployment. Die Verteilung des E-Mail-Verkehrs in Ihrem E-Mail-System wird auf einen Blick angezeigt.

In komplexen Infrastrukturen mit Gruppen von Mail-Servern, die von verschiedenen Programmen geschützt werden, kann die Sicherheit zentral über Kaspersky Security Center verwaltet werden. Diese Konsole wird ebenfalls für das Management der Sicherheit physischer und mobiler Geräte sowie virtualisierter Endpoints verwendet. So wird der Arbeitsaufwand für Ihre IT-Mitarbeiter so gering wie möglich gehalten.

VOR- UND BENUTZERDEFINIERTES WHITE- UND BLACKLISTING

White- und Blacklists für E-Mails können auf globaler und persönlicher Ebene erstellt und flexibel mit IPv4, IPv6, Wildcards und regulären Ausdrücken verwaltet werden.

ANHANGSFILTER UND FORMATANALYSE

Kategorien von E-Mail-Anhängen können anhand des Dateityps, -namens oder der Dateigröße analysiert, gefiltert und ggf. blockiert werden.

GLOBALE UND PERSÖNLICHE QUARANTÄNEN

Verdächtige E-Mails können in Quarantäne verschoben werden. Benutzer können über das Internet auf ihre persönlichen Quarantänen zugreifen, wenn LDAP verwendet wird, und so die Belastung des HelpDesks reduzieren.

INTEGRATION MIT LDAP-SERVICES

Der Administrator kann mit LDAP-Server-Benutzerkonten und -gruppen arbeiten (OpenLDAP oder Microsoft Active Directory) und spezielle Verarbeitungsregeln für die E-Mail-Verwaltung im Unternehmen erstellen.

DIE HELPDESK-ROLLE

Experten vom technischen Support können Untersuchungen und Troubleshooting durchführen, ohne von Systemadministratoren eingeleitete Vorgänge zu behindern, indem sie direkt auf ihre persönlichen Black- und Whitelists zugreifen und diese verwalten.

AUSFÜHRLICHES REPORTING UND DETAILLIERTE BENACHRICHTIGUNGEN

Detaillierte Berichte stellen Informationen bereit, die für die Überwachung und Analyse von Sicherheitsereignissen benötigt werden, während das Benachrichtigungssystem Administratoren und Dokumenteigentümer vor Richtlinienverletzungen warnt. Darüber hinaus werden Lizenzen verwaltet und Warnungen ausgegeben.

INTEGRATION UND SUPPORT

INTEGRATION IN DIE UNTERNEHMENS-E-MAIL-STRUKTUR

Kaspersky Security for Linux Mail Server unterstützt die Integration in die gängigsten Linux-basierten Mail Transfer Agents.
Das Produkt unterstützt außerdem die AMaViS-Oberfläche und ermöglicht den reibungslosen Ersatz von AV-Scannern.

SYSTEMSPEZIFIKATIONEN

EINES DER FOLGENDEN BETRIEBSSYSTEME (32 ODER 64 BIT):

- Red Hat Enterprise Linux 6.4 Server
- SUSE Linux Enterprise Server 11 SP3
- CentOS 6.4
- Ubuntu Server 10.04.4 LTS/12.04 LTS
- Debian GNU/Linux 6.0.5/7.1
- FreeBSD 8.4/9.1
- Novell Open Enterprise Server 11 (nur x64)

UNTERSTÜTZTE MAIL-SERVER:

- Exim 4.71 oder höher
- Postfix 2.5 oder höher
- Qmail 1.03
- Sendmail 8.14 oder höher
- CommunigatePro 6

Weitere Informationen zu Kaspersky Security for Linux Mail Server finden Sie unter www.kaspersky.de/business-security