Kaspersky® Security for Mail Server

Zuverlässiger Schutz für Mail Server

E-Mails sind der größte Angriffsvektor für Malware – und damit auch die größte Schwachstelle für die IT-Sicherheit von Unternehmen.[1]
Kaspersky Security for Mail Server nutzt hoch entwickelte, heuristische Analysen, Sandboxing, maschinelles Lernen und andere Next-Generation-Technologien, um E-Mails vor Ransomware, schädlichen Anhängen, Spam, Phishing und unbekannten Bedrohungen zu schützen.

Schützen Sie Ihr Unternehmen vor finanziellen und betrieblichen Verlusten sowie Imageschäden durch E-Mail-basierte Angriffe – mit unserer vielfach getesteten und ausgezeichneten Sicherheitslösung.

Vorteile

Mehr als die Hälfte aller versendeten E-Mails sind Spam. Steigern Sie Ihre Produktivität und reduzieren Sie Bedrohungen mit einem Cloud-basierten und hochentwickeltem Spam-Schutz.

Der Cloud-basierte, hochentwickelte Spam-Schutz von Kaspersky Lab erkennt sogar raffiniertesten und unbekannten Spam – und hält den Verlust wichtiger Kommunikationen aufgrund von Fehlalarmen gering. Je geringer der Zeitaufwand, die Ressourcen und Risiken durch Spam, desto mehr kann bei IT-Mitarbeitern und -Systemen eingespart werden.

Reduzierte Betriebskosten

Kaspersky Security for Mail Server kombiniert Verwaltbarkeit und Benutzerfreundlichkeit, sodass Ihr IT-Team mehr Zeit für andere Aufgaben hat. Flexible Filterkonfigurationsoptionen stellen sicher, dass sich das Programm perfekt in Ihre Geschäftsprozesse eingliedern lässt und so die Verwaltungsressourcen verringert werden.

Compliance und Schutz von vertraulichen Unternehmensdaten

Durch die Identifizierung von Geschäfts-, Finanz-, persönlichen und anderen vertraulichen Daten in ausgehenden E-Mails und Anhängen auf Microsoft-Exchange-Servern und die Kontrolle dieses Informationsflusses sorgt Kaspersky Security for Mail Servers mit optionaler DLP-Funktion dafür, dass vertrauliche Daten Ihres Unternehmens, Ihrer Partner und Ihrer Kunden stets geschützt sind und Sie die gesetzlichen Datenschutzauflagen erfüllen. Durch komplexe Analysetechniken wie die Suche nach strukturierten Daten und unternehmensspezifische Glossare können verdächtige E-Mails identifiziert und blockiert werden, und die entsprechenden Mitarbeiter (z. B. Datenschutzbeauftragte) warnen.

Flexible Zahlungsoptionen für kleine und mittelständische Unternehmen

Kaspersky Security for Mail Server ist als Jahres- oder als praktische Monatslizenz erhältlich.

Komfort für Managed Service Provider (MSP)

Für immer mehr MSPs wird Cybersicherheit zum Mehrwert, weshalb Kaspersky Security for Mail Server mehrmandantenfähige Verwaltungsfunktionen unterstützt und eine flexible Lizenzierung sowie genau die richtige Art von Reporting, die ein MSP-Support auf unterster Ebene benötigt, anbietet.

Wichtigste Vorteile

- Echtzeit- und bedarfsorientierter, hochmoderner Malware-Schutz
- Beidseitige Integration mit Kaspersky Anti Targeted Attack Platform (KATA)
- Authentifizierte E-Mail-Verwaltung bekämpft Business Email Compromise (BEC).
- Als Monatslizenz für Endnutzer und MSPs erhältlich.
- Schutz vor Zero-Hour-Bedrohungen
- Unterstützt durch globale Threat Intelligence von Kaspersky Security Network
- LDAP/Microsoft Active Directory Support
- Quarantäne-Verwaltung für E-Mails und Anhänge
- Bearbeitet eingebettete schädliche Makros und andere Objekte
- Blockiert durch E-Mails verbreitete Ransomware
- Verhindert Datenlecks (für Nutzer von MS Exchange)

1 Verizon Data Breach Investigation Report 2017.

Funktionen

HuMachine™ – mehrschichtiger Malware-Schutz

Der hochmoderne Malware-Schutz von Kaspersky beinhaltet zuverlässige Sicherheitsschichten, darunter lernfähige Systeme und Cloud-basierte Bedrohungsinformationen, und filtert so nach schädlichen Anhängen sowie nach bekannter und bisher unbekannter Malware in eingehenden E-Mails. Echtzeit- und bedarfsorientierte Scans sind verfügbar. Letztere sind besonders in Migrationsszenarien hilfreich.

- **Globale Threat Intelligence:**
  Kaspersky Security for Mail Server verwendet global gesammelte Daten für die neuesten Einblicke in die Bedrohungslandschaft, auch während sie sich weiterentwickelt.
- **Lernfähige Systeme:**
  Die weltweiten Big-Data-Bedrohungsinformationen werden durch die kombinierte Leistung von maschinellen Algorithmen und menschlicher Expertise verarbeitet und ermöglicht so sichere und hohe Erkennungsraten mit minimalen Fehlalarmen.
- **Emuliertes Sandboxing:**
  Um seine Systeme auch vor hoch entwickelten und schwer erkennbarer Malware zu schützen, werden Anhänge in einer sicher emulierten Umgebungen ausgeführt. Dort werden sie analysiert, um sicherzustellen, dass gefährliche Proben nicht ins Unternehmenssystem eindringen.

Automatisiertes Anti-Spam-System (mit Inhaltsreputation)

Das Anti-Spam-System von Kasperky Lab nutzt Erkennungsmodelle, die auf lernfähigen Systemen basieren. Um Fehlalarme zu minimieren und sich den Entwicklungen in der Bedrohungslandschaft anzupassen, unterstützt Kaspersky die Experten im Rahmen von Kaspersky HuMachine™.

Fortschrittlicher Phishing-Schutz

Das fortschrittliche Anti-Phishing-System von Kaspersky Lab basiert auf der Analyse von neuronalen Netzwerken für effektive Erkennungsmodelle. Mit über 1000 verwendeten Kriterien – einschließlich Bilder, Sprachprüfungen und speziellen Skriptsprachen – wird dieser Cloud-basierte Ansatz durch weltweit gesammelten Daten zu schädlichen und Phishing-URLs unterstützt. Damit wird ein Schutz vor sowohl bekannten als auch unbekannten/ Zero-Hour-Phishing-E-Mails ermöglicht.

Authentifizierte Verwaltung von E-Mails

Zuverlässige Mechanismen zur Sender-Authentifizierung wie z. B. SPF / DKIM / DMARC bieten zusätzlichen Schutz vor Quell-Spoofing. Dies ist besonders nützlich für „Business Email Compromise"-Szenarien (BEC).

Filtern von Anhängen

Einige Arten von Anhängen sind zu gefährlich, um sie ins Sicherheitssystem des Unternehmens zu lassen. Das Filtersystem für Anhänge von Kaspersky Lab ermöglicht die flexible Konfiguration einer Richtlinie für Anhänge, und erkennt verschiedene Arten von getarnten Dateien, die häufig von Cyberkriminellen genutzt werden. Diese Funktionen reduzieren das Risiko von Datenlecks.

Datenlecks verhindern (DLP, Data Leak Prevention)

Benutzer von Microsoft Exchange können vertrauliche Informationen in E-Mails und Anhängen mithilfe von Kategorien (personenbezogene Daten und Kreditkarteninformationen), Glossaren (sofort einsatzbereite Compliance Packs) und gründlichen Analysen, die strukturierte Daten verwenden (DLP nur für Microsoft-Exchange-Servern) ,verwalten.

Integriertes Backup

Damit während einer Desinfektion oder Löschung keine wichtigen Daten verloren gehen, können Originalnachrichten auf einem Backup-Speicher gespeichert werden, die vom Administrator an einem passenderen Zeitpunkt bearbeitet werden. Es können bestimmte Regeln für eine bedingte Sicherung von Daten konfiguriert werden.

Integration von Kaspersky Anti Targeted Attack

Die beidseitige Integration der leistungsstarken Anti-APT/ EDR-Lösung ermöglicht nicht nur die Nutzung des E-Mail-Systems als zusätzliche Informationsquelle für zielgerichtete Angriffserkennung, sondern blockiert darüber hinaus Nachrichten mit gefährlichen Inhalten.

Ansatz von Kaspersky HuMachine™

Unterstützt durch Big-Data-Bedrohungsinformationen, Funktionen lernfähiger Robotersysteme und der Erfahrung menschlicher Experten bietet Kaspersky HuMachine™ zahlreiche Vorteile und einen effizienteren Schutz. Durch die Kombination aller Elemente wird jede einzelne Komponente zu einem noch effizienteren und effektiveren Ganzen optimiert.

2 Die optionale Funktion von Data Leak Prevention für Kaspersky Security for Microsoft Exchange Server muss separat erworben werden.

Enthaltene Programme

- Kaspersky Security for Linux Mail Server
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Anti-Virus for Lotus Notes/Domino
- Kaspersky Security Center

Hinweise zum Kauf

Kaspersky Security for Mail Server ist als Jahres- oder Monatslizenz erhältlich. Es kann separat oder als Teil von Kaspersky Total Security for Business erworben werden.[2]
Ein Vertriebspartner oder autorisierter Distributor von Kaspersky Lab hilft Ihnen bei der Auswahl des für Sie geeigneten Produkts.

www.kaspersky.de
#truecybersecurity