Kaspersky® Security for Mail Server

Sicherer, hochmoderner Schutz für geschäftliche E-Mails

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, lernfähige Systeme und andere Next Generation-Technologien, um E-Mails vor 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.

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

Der Cloud-basierte, hochmoderne 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.

Flexible Zahlungsoptionen für kleine und mittelständische Unternehmen

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

Bequem für Managed Service Provider (MSP)

Da Cybersicherheit für immer mehr MSPs zu einem Mehrwert wird, unterstützt Kaspersky Security for Mail Server mehrmandantenfähige Verwaltungsfunktionen und eine flexible Lizenzierung sowie genau die richtige Art von Reporting für den MSP-Support auf unterster Ebene.

Wichtigste Vorteile

- Echtzeit- und bedarfsorientierter Next Generation-Malware-Schutz
- Beidseitige Integration mit Kaspersky Anti Targeted Attack Platform (KATA)
- Spezieller Schutz vor ausgeklügelten Phishing-Bedrohungen, darunter BEC (Business Email Compromise)
- 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
- Verhindert über E-Mails verteilte Ransomware und kleinere Trojaner

1 Verizon Data Breach Investigation Report 2017.

Funktionen

Durch HuMachine™ unterstützter, 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 neueste Einblicke in eine sich ständig weiterentwickelnde Bedrohungslandschaft.

- **Lernfähige Systeme**
  Die weltweiten Threat Intelligence-Daten werden durch die kombinierte Leistung von maschinellen Algorithmen und menschlicher Expertise verarbeitet und ermöglichen so nachweislich hohe Erkennungsraten mit minimalen Fehlalarmen.
- **Emuliertes Sandboxing:**
  Um Systeme selbst vor hoch entwickelter und schwer erkennbarer Malware zu schützen, werden Anhänge in einer sicher emulierten Umgebung 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 Kaspersky 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- und BEC-Schutz

Das fortschrittliche Anti-Phishing-System von Kaspersky Lab basiert auf der Analyse von neuronalen Netzwerken für effektive Erkennungsmodelle. Mit über 1.000 verwendeten Kriterien – einschließlich Bildern, Sprachprüfungen und speziellen Skriptsprachen – wird dieser Cloud-basierte Ansatz durch weltweit gesammelte Daten zu schädlichen und Phishing-URLs unterstützt. Damit wird ein Schutz vor bekannten und unbekannten/Zero-Hour-Phishing-E-Mails ermöglicht. Spezielle Algorithmen zielen auf BEC-Bedrohungen (Business Email Compromise) ab.

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.

Integriertes Backup

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

Integration von Kaspersky Anti Targeted Attack (KATA)

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.

Enthaltene Programme
- Kaspersky Security for Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Security Center

Hinweise zum Kauf
Kaspersky Security for Mail Server ist als Jahres- oder Monatslizenz erhältlich. Das Programm kann separat erworben werden oder ist als Teil von Kaspersky Total Security for Business verfügbar. Ein Vertriebspartner oder autorisierter Distributor von Kaspersky Lab hilft Ihnen gern bei der Auswahl des für Sie geeigneten Produkts.

www.kaspersky.de
#truecybersecurity