Kaspersky Security for Microsoft Office 365

So funktioniert's

Kaspersky Security for Microsoft Office 365 setzt Next-Generation-Technologien ein, um Ihr Postfach vor Spam, Business Email Compromise, Phishing, Ransomware und hoch entwickelten Bedrohungen zu schützen.

Und so funktioniert es ... Schnelle und einfache Registrierung Verbinden Sie Office 365 mit der unter cloud.kaspersky.com web-basierten Verwaltungskonsole Auf Seiten von Kaspersky Lab werden keine Daten gespeichert. Schutz wird aktiviert Die Administratoren wählen ihr Rechenzentrum für die Verarbeitung selbst aus. Wie können wir maximalen Schutz gewährleisten? Next-Generation-Sicherheitstechnologien E-Mails treffen in Ihrer Diese Filterung geschieht filtern auch unbekannte Bedrohungen Office 365-Cloud ein schnell und effizient heraus, bevor der Benutzer einen Fehler machen kann. Legitime E-Mails bleiben im Postfach des **Kaspersky Security for Microsoft** Benutzers. Schädliche oder verdächtige E-Mails Office 365 durch sucht die E-Mails werden in einen nicht sichtbaren Ordner gefiltert, nach Bedrohungen den nur der Administrator anzeigen oder bearbeiten kann

Anhangfilterung:

Next-Generation-

durch Fehlalarme.

Mehrschichtige

HuMachine

Erkennung durch

Erkennt selbst unbekannte

Malware. Verdächtige Dateien

können an einem sicheren Ort

ausgeführt werden, bevor sie

zugelassen werden.

Anti-Spam-Technologie

Die auf lernfähigen Systemen

basierenden Erkennungsmodelle

hochentwickelten, unbekannten

Spam und minimieren Zeitverlust

von Kaspersky Lab erkennen selbst

Durch Filtern von Anhängen werden gefährliche Dateien blockiert, bevor sie zu einem Problem werden. Durch Erkennung echter Dateitypen kann gefährlicher und unerwünschter Inhalt herausgefiltert werden. Die auf neuronalen Netzwerken basierende Anti-Phishing-Engine von Kaspersky Lab verwendet über 1000 Kriterien zur Erstellung von Erkennungsmodellen.

Ö.

Next-Generation-Anti-Phishing-Technologie



Lernfähige Systeme

Die lernfähigen Algorithmen sind dafür trainiert, Malware in Datensätzen von über **200 Mio**. schädlichen und über **1 Mrd**. sauberen Dateien zu identifizieren. Diese Erkennungsmodelle filtern bisher unbekannte Zero-Hour-Malware heraus.



Threat Intelligence für Big Data

Globale Cloud-basierte und kontinuierlich aktualisierte Threat Intelligence, betrieben durch das Kaspersky Security Network. Kombiniert mit der menschlichen Expertise von über 200 spezialisierten Bedrohungsexperten.