



## Kaspersky<sup>®</sup> Security for Microsoft Office 365

# Pro Sekunde werden 3,5 Millionen E-Mails versendet. Eine einzige davon kann ausreichen, um Ihr Unternehmen lahmzulegen.

Kaspersky Security for Microsoft Office 365 verwendet erweiterte Heuristiken, Sandbox-Umgebungen, lernfähige Systeme und andere Next-Generation-Technologien zum Schutz der E-Mail-Komponente vor Ransomware, schädlichen Anhängen, Spam und Phishing, Business E-Mail Compromise (BEC) wie auch unbekanntem Bedrohungen. Wie Microsoft Office 365 wird es in der Cloud gehostet. Und wie alle Kaspersky-Lösungen beruht sie auf der Sicherheitssoftware, die weltweit eine der am häufigsten getesteten und ausgezeichneten ist.<sup>1</sup> Mit Kaspersky Security for Microsoft Office 365 wehren Sie Cyberbedrohungen ab, ohne die Kommunikation zu beeinträchtigen.

### Steigerung der Produktivität und Reduzierung der Bedrohungen mit Next-Generation-Spam-Schutz

50 % des E-Mail-Verkehrs sind Spam. Verringern Sie Zeitaufwand, Ressourcen und Risiken durch Spam, indem Sie solche E-Mails stoppen, bevor sie zugelassen werden. Die Next-Generation-Spam-Erkennung und -Analyse von Kaspersky Lab beruht auf maschinellem Lernen und der Cloud-basierten Echtzeit-Intelligenz des Kaspersky Security Network.

### Malware-Schutz durch die Cloud

99 % der Malware wird mit E-Mails oder über Web-Server gesendet, und 66 % wird über schädliche Anhänge installiert.<sup>2</sup> Verhindern Sie die Entwicklung von E-Mail-Angriffen, während Sie unbekannte und Zero-Day-Malware in Word-, Excel-, PowerPoint- und anderen Anwendungsdateien blockieren.

### Stoppen Sie Ransomware, Phishing und andere Bedrohungen

Alle 40 Sekunden wird ein Unternehmen mit Ransomware angegriffen<sup>3</sup>, und E-Mail-Phishing ist ein beliebter Vektor zum Starten solcher Angriffe. 78 % der Nutzer geben an, ihnen seien die Risiken von unbekanntem E-Mails bekannt. Dennoch klickt jeder zweite Benutzer darauf<sup>4</sup>. Kaspersky Security for Microsoft Office 365 verwendet Sandbox-Umgebungen und maschinelles Lernen, um Bedrohungen herauszufiltern, bevor der Benutzer einen Fehler machen kann.

### Datenschutz, Integrität und Kontrolle

Keine Sorge um den Schutz persönlicher Daten: Gleich bei der Einrichtung wählt der Administrator das Rechenzentrum aus, dem die Bearbeitung der E-Mails zugewiesen werden soll. Kunden-E-Mails werden von Kaspersky Lab nicht gespeichert. Verdächtige E-Mails werden in einem Ordner im Office 365-Posteingang des Benutzers abgelegt, auf den nur der Administrator Zugriff hat. Nur der Administrator kann diesen Ordner über die Verwaltungskonsole von Kaspersky Security for Microsoft Office 365 anzeigen und darauf zugreifen.

### Verringerung von Fehlalarmen – keine verschwundenen E-Mails mehr

Viele Benutzer haben das Problem, dass legitime E-Mails mit Spam verwechselt werden. Mit weniger Fehlalarmen und Administratorkontrolle über das, was mit verdächtigen E-Mails geschieht, reduziert Kaspersky Security for Microsoft Office 365 die Wahrscheinlichkeit solcher Vorfälle erheblich. Gelöschte E-Mails werden in Backups hinterlegt und können dort gesucht und wiederhergestellt werden – keine „verschwundenen“ E-Mails mehr.

### Benutzerfreundlich und kostengünstig

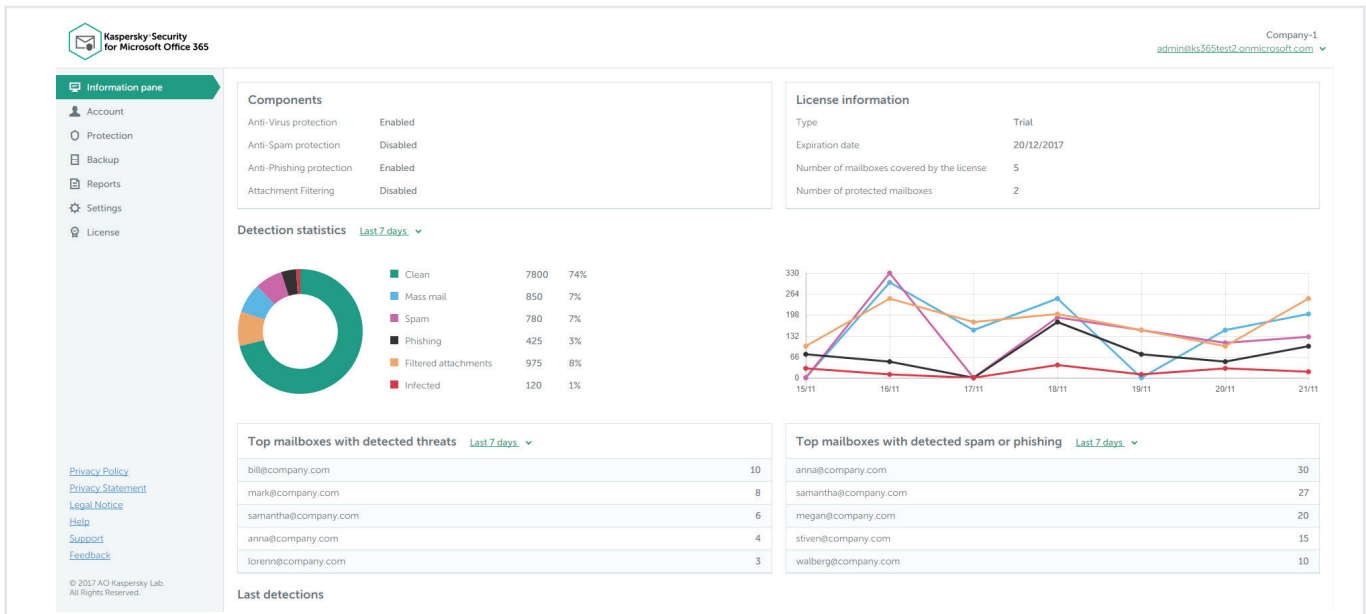
Eine intuitive, leicht zu bedienende Schnittstelle bedeutet, dass keine zusätzlichen Mitarbeiterschulungen notwendig sind. Nur eine Verwaltungskonsole kümmert sich um alles und bietet eine einzige Ansicht der erkannten Bedrohungen und Statistiken. Eine einzige, leicht zu verwendende Richtlinie ermöglicht sofortigen Schutz. Für den Start muss nicht in zusätzliche Infrastruktur investiert werden, und es ist keine Installationsdatei erforderlich.

<sup>1</sup> Im Jahr 2016 haben die Produkte von Kaspersky Lab an 78 unabhängigen Tests und Bewertungen teilgenommen. Unsere Produkte waren 55 Mal auf Platz 1 und 70 Mal unter den Top 3. <https://www.kaspersky.de/top3>

<sup>2</sup> Verizon Data Breach Investigation Report 2017

<sup>3</sup> Kaspersky Security Bulletin 2016: Die Revolution der Ransomware

<sup>4</sup> Friedrich-Alexander-Universität: „Die Forscher der FAU untersuchen das Benutzerverhalten beim Online-Empfang von unbekanntem Nachrichten.“



## Next-Generation-Technologien

### Basierend auf dem Kaspersky Security Network

Reputationsfilterung und Anti-Phishing auf Basis von Bedrohungsdaten, die das Kaspersky Security Network aus den neuesten Spam-Bedrohungen ermittelt. Durchsuchen des E-Mail-Verkehrs nahezu in Echtzeit, um die neuesten Bedrohungen, darunter Ransomware und Zero-Day-Angriffe, zu erkennen, zu blockieren und zu löschen.

### Heuristik und lernfähige Systeme

Ein Heuristik-basiertes automatisches Erkennungssystem sorgt dafür, dass auch unbekannte Malware erkannt wird. Ein lernfähige System ermöglicht die schnelle Erkennung von Ausführungssequenzen, die auf einen Angriff hindeuten. Mit Sandbox-Protokollen kombiniert, sorgt dies für neue Erkennungsindikatoren, an denen ständig weiter gefeilt wird. So wird optimaler Schutz vor den neuesten Bedrohungen sichergestellt, aber auch Fehlalarme werden minimiert.

Die kostenlose Testversion finden Sie unter [cloud.kaspersky.com](https://cloud.kaspersky.com)

## Kombiniert noch besser

**Kaspersky Business Hub** – Verwaltung für den Schutz Ihres Unternehmens über nur eine Konsole. Intuitive Oberfläche, einfache Verwaltung und hervorragender Schutz für verschiedene Geräte und Produktivitätstools, alles von einem einzigen Ort aus verwaltet.

Die folgenden Produkte werden im **Kaspersky Business Hub** verwaltet:

- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365

### Funktionen von Kaspersky Security for Microsoft Office 365

- Zentralisierte Verwaltung
- Leicht zu verwendende Richtlinie
- Bedrohungs-Dashboard für Einblicke und Berichte
- Löschen unerwünschter Anhänge
- Erkennen echter Dateitypen: genaue Erkennung des Dateityps, unabhängig von der Dateierendung
- Anti-Spam, Malware-Schutz, Anti-Phishing
- Keine Notwendigkeit für zusätzliche Infrastruktur

Kaspersky Lab

Neues über Cyberbedrohungen: [de.securelist.com](https://de.securelist.com)

IT-Sicherheitsnachrichten:

<https://www.kaspersky.de/blog/b2b/>

#truecybersecurity

#HuMachine

[www.kaspersky.com](https://www.kaspersky.com)

© 2017 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.

