KASPERSKY lab

KASPERSKY SECURITY MICROSOFT OFFICE 365

Funktionsliste

KURZBESCHREIBUNG

Kaspersky Security for Microsoft Office 365 ist ein neues SaaS-Produkt zum Schutz der E-Mail-Komponente der Microsoft Office 365-Suite: Exchange Online. Es verwendet erweiterte Heuristiken, Sandbox-Umgebungen, maschinelles Lernen und andere Next-Generation-Technologien zum Schutz der E-Mail-Komponente vor Ransomware, schädlichen Anhängen, Spam und Phishing (einschließlich Business E-Mail Compromise, BEC) wie auch unbekannten Bedrohungen. Genau wie Microsoft Office 365 wird es in der Cloud gehostet. Wie alle Kaspersky-Lösungen beruht es auf der Sicherheitssoftware, die weltweit eine der am häufigsten getesteten und ausgezeichneten ist.

Kaspersky Security for Microsoft Office 365 wird über den **Kaspersky Business Hub** verwaltet, die gleiche einfache, intuitive Cloud-Konsole wie für **Kaspersky Endpoint Security Cloud**.

Beide Produkte können unter https://cloud.kaspersky.com als Testversionen heruntergeladen werden.

Standardmäßig dient die von der Firmenzentrale erstellte Funktionsliste nur internen Zwecken!

INHALT

INTEGRATION

Funktion	Beschreibung	Vorteile/Anwendungsfall
Exchange Online-Integration	Integration von Exchange Online unter Verwendung von Exchange Web Services, Exchange Online-Commandlets und anderen von Microsoft zugelassenen Technologien.	Native Integration, keine Konfiguration zusätzlicher Integrationsparameter in Exchange Online notwendig.

ADMINISTRATION UND VERWALTUNG

Funktion	Beschreibung	Vorteile/Anwendungsfall
Kaspersky Business Hub	Kaspersky Security for Microsoft Office 365 ist Teil des Kaspersky Business Hub: Mit nur einer Konsole kann der Schutz Ihres Unternehmens verwaltet werden. Die folgenden Produkte werden im Kaspersky Business Hub verwaltet: • Kaspersky Endpoint Security Cloud • Kaspersky Security for Microsoft Office 365	Intuitive Oberfläche, einfache Verwaltung und hervorragender Schutz für verschiedene Geräte und Produktivitätstools, alles über eine einzige Konsole verwaltet. Keine Notwendigkeit mehr für Kunden oder Partner, zwischen verschiedenen Verwaltungskonsolen zu wechseln, während sie die Sicherheit für Endpoints und Exchange Online verwalten.
Mehrmandaten-fähigkeit	Sie können mehrere Workspaces von Kaspersky Security for Microsoft Office 365 über nur ein Konto verwalten.	MSP-Administratoren können über dieselbe Konsole mit mehreren verschiedenen Organisationen zusammenarbeiten, immer vom selben Konto aus.
Auswahl zu schützender Posteingänge	Sie können spezifische Posteingänge auswählen, um die Lösung vor dem Rollout zu testen oder um sie auf alle Posteingänge innerhalb einer Organisation anzuwenden.	Ist sich der Administrator über die richtigen Einstellungen unsicher und möchte die Lösung an einigen wenigen Posteingängen testen, kann er dies durch Auswahl bestimmter Posteingänge tun. Alternativ können alle Posteingänge gewählt werden, sodass der Schutz auf die gesamte Organisation angewendet wird.
Einfache Konfiguration	Alle Schutzeinstellungen sind auf einem Bildschirm zusammengefasst. Durch Wechseln der Registerkarten können Sie durch die verschiedenen Schutztechnologien navigieren.	Die Schutzeinstellungen können sehr einfach konfiguriert und geprüft werden.

Dashboard	Intelligentes Dashboard mit Informationen für die tägliche oder wöchentliche Überwachung. Das Dashboard zeigt den Echtzeitstatus für die Module der Lösung sowie Statistiken an. Administratoren können tägliche, wöchentliche oder monatliche Statistiken nach Erkennungen, nach Benutzern mit den meisten Spamnachrichten/Viren und nach den Details der letzten Erkennungen einsehen.	Überblick über die tägliche, wöchentliche oder monatliche Überwachung und den Status
Berichte	Detailliertes, flexibles Reporting im PDF-Format Steuerung und Überwachung der Anwendung von Sicherheitsrichtlinien sowie Statistiken zur detaillierten Analyse des Sicherheitsstatus	Tägliche, wöchentliche oder monatliche Berichte oder Berichte für zufällig gewählte Zeitspannen zu Verwaltungszwecken.
Benachrichtigungs-system	Informiert Systemadministratoren und Absender/Empfänger von Nachrichten über Richtlinienverstöße in Form von Viren, Phishing oder unerwünschten Anhängen, sodass sofortige Maßnahmen ergriffen werden können.	Ermöglicht dem Administrator die schnelle Reaktion auf Sicherheitsvorfälle.
Backup	Die originalen Nachrichten werden nach der Löschung im Backup gespeichert. Administratoren können im Backup gespeicherte Nachrichten abfragen, sie löschen, auf Festplatte speichern oder bei Bedarf an Empfänger weitersenden. Das Backup wird in der Exchange Online-Installation beim Kunden gespeichert.	Minimiert das Risiko verlorener Nachrichten bei Fehlalarmen.
Anzeige von Microsoft-Quarantäne-elementen im Backup-Abschnitt	Sie können Nachrichten anzeigen und wiederherstellen, die innerhalb der Kaspersky Security for Microsoft Office 365-Konsole durch Microsoft Online Protection gelöscht wurden.	Keine Notwendigkeit mehr zum Suchen gelöschter Nachrichten in mehreren Konsolen; die Suche nach fehlenden Nachrichten erfolgt in nur einer einfachen Konsole.
Mehrere Administratoren	Der Zugriff auf die Verwaltungskonsole kann mehr als einem Administrator gewährt werden (durch KES Cloud).	Die Lösung kann von mehreren Administratoren verwaltet werden, die verschiedene Konten verwenden.

ANTI-MALWARE

Funktion	Beschreibung	Vorteile/Anwendungsfall
Mehrschichtige Bedrohungs-erkennung durch HuMachine	Die preisgekrönte Erkennungs-Engine für Bedrohungen setzt sich aus mehreren proaktiven Sicherheitsebenen zusammen, die schädliche Anhänge aus eingehenden E-Mails herausfiltern. Unsere Erkennungsmodelle, die auf maschinellem Lernen basieren, können sowohl bekannte als auch bisher unbekannte komplexe Malware herausfiltern.	Fähigkeit zur Erkennung und Beseitigung schädlicher Anhänge und Objekte im Text einer Nachricht.
Kaspersky Security Network	Nahezu in Echtzeit ermöglicht die umfangreiche datenbasierte Threat Intelligence vom KSN unmittelbare Reaktionen auf Veränderungen in der Bedrohungslandschaft.	Die sofortige Bereitstellung einer praktisch umsetzbaren Threat Intelligence sorgt für schnelle Reaktionen selbst auf die komplexesten Bedrohungen.

ANHANGFILTERUNG

Funktion	Beschreibung	Vorteile/Anwendungsfall
Nachrichten mit unerwünschten Anhängen löschen oder mit Tags versehen	Nachrichten mit unerwünschten Anhängen können entweder gelöscht oder in der Betreffzeile mit einem benutzerdefinierten Tag versehen und zugelassen werden.	Dies hilft, die richtige Nutzungsrichtlinie für E-Mails durchzusetzen und die Unternehmenshaftung zu verringern (z. B. bei Benutzern, die illegale Musik oder Video-Dateien über E-Mails verbreiten). Außerdem trägt es dazu bei, rechtliche oder Reputationsrisiken in Bezug auf die Verteilung illegaler Inhalte (z. B. Musik oder Video-Dateien) zu vermeiden.
Erkennung echter Dateitypen	Erkennt echte Dateitypen und Attribute, auch wenn versucht wird, sie zu verschleiern.	Blockiert potentiell schädliche Dateien (z. B. Programmdateien), selbst wenn diese als harmlose Dateien getarnt werden.
Anhangfilterung nach Erweiterungen	Auf Nachrichten, deren Anhänge unerwünschte Erweiterungen aufweisen, können Sie Aktionen anwenden.	Sie können die Sicherheit erhöhen, indem Sie unerwünschte Dateitypen entweder mittels Regeln filtern oder mit Tags versehen.

Erkennung von Office-Dateien mit Makros	Sie können Aktionen auf Nachrichten anwenden, an denen Office-Dateien mit Makros angehängt sind.	Einige Viren werden über Makros in Office-Dokumenten (Excel, Word usw.) verbreitet. Sie können die Sicherheit erhöhen, indem Sie Office-Dateien, die Makros enthalten, mittels Regeln filtern oder mit Tags versehen.
Flexible Ausschlüsse durch Anhangfilterung	Sie können Anhänge durch Filtern entweder nach Typ oder nach Absender-/Empfängername ausschließen.	So kann u. U. vermieden werden, dass fälschlicherweise wertvolle E-Mails herausgefiltert werden.

SPAM-SCHUTZ

Funktion	Beschreibung	Vorteile/Anwendungsfall
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, wird die automatisierte Spam-Verarbeitung durch Experten von Kaspersky Lab im Rahmen von Kaspersky HuMachine betreut.	Effektive Erkennung selbst raffiniertester unbekannter Spam-Mails bei minimalem Verlust wertvoller Nachrichten aufgrund von Fehlalarmen.
Unterstützung autorisierter E-Mails	Das Sender Policy Framework (SPF) wird unterstützt, um den Empfang von Spoof-E-Mails zu vermeiden.	Das Senden von Spoof-E-Mails ist eines der wichtigsten Werkzeuge von betrügerischem und böswilligem Spam im Kontext von Social Engineering. Mittels autorisierter E-Mails können ihre Auswirkungen erheblich reduziert werden.
Kaspersky Security Network	Das KSN erfasst Informationen über neuen Spam aus der ganzen Welt, verarbeitet sie mit dem Ansatz der Kaspersky HuMachine und gibt sie umgehend an den Kunden weiter.	Dies ermöglicht sofortige Reaktionen auf unbekannten Spam, einschließlich „Zero-Hour“ und neuer Epidemien, automatisch und ohne dass das IT-Personal eingreifen muss. Es trägt dazu bei, Überschwemmungen mit E-Mails und Infektionen zu verhindern.

Massen-E-Mails	Nachrichten aus einer vertrauenswürdigen Quelle können einige Spam-Attribute enthalten, sind aber kein wirklicher Spam. Solche E-Mails können als Massen-E-Mails gekennzeichnet oder in den Junk-Ordner/Posteingang verschoben werden. (Zu dieser Art von Nachrichten gehören Newsfeeds, Werbe- oder Marketing-E-Mails.)	Massen-E-Mails können von einigen Benutzern als nützlich betrachtet oder sogar zu Arbeitszwecken verwendet werden. So können Massen-E-Mails im Posteingang des Benutzers verbleiben, jedoch mit einem Tag an der Betreffzeile, um den Benutzer zu sensibilisieren.

PHISHING-SCHUTZ

Funktion	Beschreibung	Vorteile/Anwendungsfall
Auf neuronalen Netzwerken basierende Anti-Phishing-Engine	Das proaktive Anti-Phishing-System von Kaspersky Lab basiert auf neuronalen Netzwerken und setzt sich aus effektiven Erkennungsmodellen zusammen. Mehr als 1000 Kriterien werden verwendet, einschließlich Bildern, Sprachprüfungen und der Verwendung von bestimmtem Skriptsprachen.	Dies schützt Ihr Unternehmen gegen unbekannte oder „Zero-Hour“-Phishing-E-Mails und verhindert den Verlust von Anmeldeinformationen oder Datenschutzverletzungen.
URL-Datenbanken für Malware und Phishing	Die kontinuierlich aktualisierten Datenbanken von Kaspersky Lab für Malware- und Phishing-URLs profitieren sowohl von automatisch ermittelten Daten als auch von den Ergebnissen einer ausgereiften Bedrohungsforschung. Diese werden durch das Kaspersky Security Network zur Verfügung gestellt.	Dadurch werden Drive-by- und Waterholing-Angriffe, die zu möglichen Infektionen und nachfolgendem Datenverlust führen könnten, sowie Betrugsversuche verhindert.
Phishing-Nachrichten löschen oder mit Tags versehen und in den Junk-Ordner verschieben	Phishing-Nachrichten können entweder gelöscht oder in den Junk-Ordner verschoben werden. Im Junk-Ordner kann den Phishing-Nachrichten ein benutzerdefinierter Tag angefügt werden.	Dies trägt zur Steigerung der Produktivität bei, indem einfach tagbasiert gefiltert werden kann, ohne potentiell nützliche Massen-E-Mails zu verlieren.