Kaspersky® Endpoint Security for Business

Select

Kaspersky Endpoint Security for Business – Select bietet HuMachine™-basierten Next Generation-Schutz für eine Vielzahl von Plattformen, einschließlich Linux-Servern und Endpoints. Es liefert mehrschichtige Sicherheit, die verdächtiges Verhalten erkennt und Bedrohungen blockiert, einschließlich Ransomware. Cloud-basierte Kontrollen reduzieren Ihre Angriffsflächen. Mobile Verwaltungstools helfen Ihnen, mobile Plattformen zu schützen.

Alle Schutz- und Verwaltungsfunktionen, die Sie benötigen

Kaspersky Lab hat leistungsfähige auf große Unternehmen abgestimmte Funktionen in seine fortschrittlichen, aufeinander aufbauenden Angebote integriert. Wir haben dafür gesorgt, dass die Nutzung der Technologie für Unternehmen jeder Größenordnung unkompliziert und einfach ist.

Welche Stufe ist die richtige für Sie?

- **SELECT**
- ADVANCED
- TOTAL

Mehrere Schutzstufen für

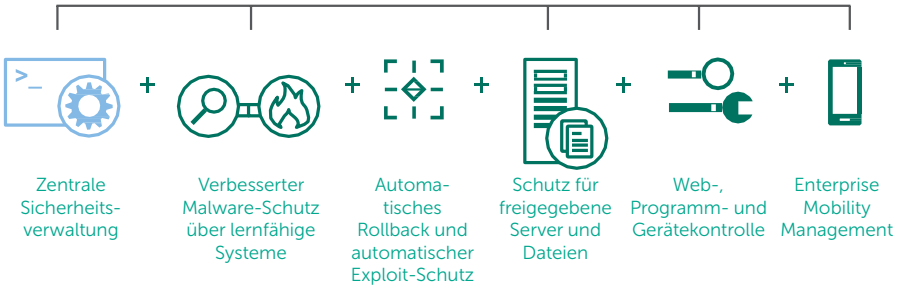
- Windows, Linux und Mac
- Windows- und Linux-Server
- Android und andere mobile Geräte
- Wechseldatenträger

Umfassender Schutz gegen

- Software Exploits
- Ransomware
- Malware für Mobilgeräte
- Hoch entwickelte Bedrohungen
- Dateilose Bedrohungen
- Powershell- und Skript-basierte Angriffe
- Webbedrohungen

Enthaltene Funktionen

- Malware-Schutz verbessert
- Statisches maschinelles Lernen
- Dynamisches maschinelles Lernen neu
- Prozessisolierung
- Firewall
- Verwaltung der Betriebssystem-Firewall neu
- Cloud-basierter Schutz
- Integrierter EDR-Agent neu
- Programmkontrolle verbessert
- Dynamische Whitelists
- Web-Kontrolle
- Gerätekontrolle verbessert
- Serverschutz verbessert
- Schutz für Terminalserver verbessert
- Enterprise Mobility Management verbessert
- Mobile Endpoint Security verbessert
- Reporting verbessert



Next Generation-Schutz und Kontrolle für jeden Endpoint

Eine Verwaltungskonsole

Über die zentrale Verwaltungskonsole können Administratoren die gesamte Sicherheitslandschaft im Blick behalten und verwalten und Ihre gewählten Sicherheitsrichtlinien auf jeden Endpoint Ihres Unternehmens anwenden. Dies hilft Ihnen bei der schnellen Bereitstellung der Sicherheit mit minimalem Aufwand oder Unterbrechungen – durch unsere breite Palette an vorkonfigurierten Szenarien.

Flexible Sicherheit

Das Produkt wurde für die Anwendung in sämtlichen IT-Umgebungen entwickelt. Es nutzt eine Reihe alt bewährter sowie Next Generation-Technologien. Integrierte Sensoren und die Integration in Endpoint Detection & Response (EDR) ermöglichen die Erfassung und Analyse großer Datenvolumen und gewährleisten damit die Erkennung hochentwickelter Cyberangriffe.

Ein einziges Produkt – keine versteckten Kosten

Mit mehreren Sicherheitstechnologien in einem einzigen Produkt gibt es keine versteckten Kosten. Ein einziges Produkt mit lediglich einer Lizenz ist alles, was Sie brauchen, um Ihre Endpoints zu schützen.

Hauptfunktionen

Funktionen für den zukunftsorientierten Schutz vor Bedrohungen

Exploit-Schutz
Verhindert die Ausführung von Malware und unautorisierte Nutzung von Software und bietet damit eine zusätzliche Schutzstufe gegen unbekannte Zero-Day-Bedrohungen.

Verhaltenserkennung und automatisches Rollback
Identifiziert und bietet Schutz vor hoch entwickelten Bedrohungen, einschließlich Ransomware, dateilosen Angriffen und Übernahmen von Administratorkonten. Die Verhaltenserkennung blockiert Angriffe, während das automatische Rollback alle bereits vorgenommenen Änderungen rückgängig macht.

Schutz vor Verschlüsselung freigegebener Ordner
Einzigartiger Anti-Cryptor-Mechanismus, der die Verschlüsselung von Dateien auf freigegebenen Ressourcen durch den schädlichen Prozess auf einem anderen Rechner im selben Netzwerk blockiert.

Schutz vor Bedrohungen im Netzwerk
Malware, die bei einem Angriff mit Pufferüberläufen zum Einsatz kommt, kann einen Prozess, der bereits im Speicher ausgeführt wird, modifizieren und auf diese Weise den schädlichen Code ausführen. Der Schutz vor Bedrohungen für das Netzwerk erkennt Netzwerkangriffe und Exploits und stoppt sie in ihrer Ausführung.

Anti-Rootkit-Technologie
Angreifer nutzen Rootkits und Bootkits, um ihre Aktivitäten vor den Sicherheitslösungen zu verbergen. Die Anti-Rootkit-Technologie hilft, auch gut versteckte Infektionen zu erkennen und zu neutralisieren.

Funktionen für mobile Sicherheit

Innovative Anti-Malware-Technologien
Die Kombination von signaturbasierter, proaktiver und Cloud-basierter Erkennung ermöglicht Echtzeitschutz. Ein sicherer Browser sowie bedarfsabhängige und geplante Scans erhöhen die Sicherheit.

„Over the Air"-Bereitstellung (OTA)
Diese Funktion bietet die Möglichkeit, Programme zentral über SMS, E-Mail und PC im Voraus zu konfigurieren und bereitzustellen

Remote-Tools zum Diebstahlschutz
SIM-Überwachung, externe Sperrung, Löschung und Suche dienen dazu, nicht autorisierten Zugriff auf Unternehmensdaten zu verhindern, wenn ein mobiles Gerät verloren geht oder gestohlen wird.

Programmkontrolle für mobile Geräte
Die Programmkontrolle stellt Daten auf installierter Software bereit und ermöglicht Administratoren das Erzwingen der Installation und Nutzung bestimmter Programme.

Cloud-basierte Endpoint-Kontrollen

Programmkontrolle
Reduzieren Sie Ihre Angriffsflächen durch die vollständige Kontrolle darüber, welche Software möglicherweise wann auf den Computern ausgeführt wird, ermöglicht durch dynamische Whitelists aus unserem internen Labor. Default Allow- und Default Deny-Szenarien werden unterstützt.

Dynamische Whitelists
Für eine bessere Programmkategorisierung kann die Programmkontrolle die Datenbank für dynamische Whitelists verwenden, die von Kaspersky Lab durch systematische Zusammenstellung der Kenntnisse über legitime Software entwickelt wurde.

Gerätekontrolle
Diese Funktion gestattet es Benutzern, Datenrichtlinien zur Kontrolle von Wechseldatenträgern und sonstigen Peripheriegeräten festzulegen, zeitlich zu planen und durchzusetzen – ganz gleich, ob die Verbindung über USB oder sonstige Schnittstellen erfolgt.

Host Intrusion Prevention
Reguliert den Zugriff auf sensible Daten und Aufzeichnungsgeräte durch Anwendung der lokalen und einer Cloud-basierten (Kaspersky Security Network) Reputationsdatenbank, ohne die Leistung von genehmigten Programmen zu beeinträchtigen.

Instandhaltung und Support

Unsere professionellen Serviceteams in über 200 Ländern an 35 Standorten weltweit sind immer in Bereitschaft und stellen sicher, dass Sie aus Ihrer Kaspersky-Sicherheitsinstallation den maximalen Nutzen ziehen.

Gratis testen

Finden Sie heraus, wie nur True Cybersecurity die benutzerfreundliche Flexibilität mit **HuMachine™**-Informationen kombiniert und Ihr Unternehmen so vor jeder Art von Bedrohung schützt. Besuchen Sie diese Seite und sichern Sie sich die kostenlose 30-tägige Testversion der Vollversion von **Kaspersky Endpoint Security for Business**.

Kaspersky Lab
Informationen zu Partnern in Ihrer Nähe finden Sie hier:
https://www.kaspersky.de/partners
Kaspersky for Business: **www.kaspersky.de/business-security**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**
Unser einzigartiges Konzept: **https://www.kaspersky.de/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.de