Kaspersky® Endpoint Security for Business

Advanced

Kaspersky Endpoint Security for Business – Advanced kombiniert mehrschichtige Sicherheit mit erweiterten Kontrolltools und bietet damit eine flexible Sicherheitslösung, die sich schnell an neue Bedrohungen anpasst. Zusätzliche Verteidigungsebenen helfen Unternehmen, Schwachstellen zu beseitigen und noch mehr für den Schutz sensibler Daten zu tun. Alle Funktionen werden über eine einzelne, einfach zu handhabende Verwaltungskonsole gesteuert.

Alle Schutz- und Verwaltungsfunktionen, die Sie benötigen

Kaspersky Lab hat leistungsfähige, auf größere Unternehmen zugeschnittene Funktionen in seine fortschrittlichen, aufeinander aufbauenden Produkte 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

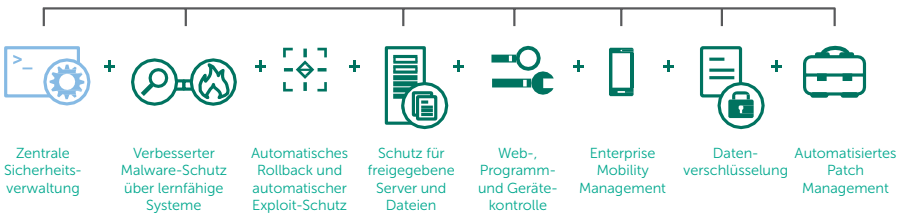
- Windows, Linux und Mac
- Windows- und Linux-Server
- Windows Server-Container
- Android und andere mobile Geräte
- Wechseldatenträger

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
- Vulnerability Management
- 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
- Verschlüsselung
- Verwaltung der Betriebssystem-Verschlüsselung verbessert
- Systemkonfiguration und -bereitstellung verbessert
- Patch Management verbessert
- Reporting verbessert



Erhöhte Sicherheit mit erweiterten Management- und Datenschutzfunktionen

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 Ihren IT-Bestand zu schützen.

Führend und anerkannt

Allein 2017 haben die Sicherheitsprodukte von Kaspersky Lab an 86 unabhängigen Tests und Bewertungen teilgenommen – mit 72 Siegen und 78 Top-3-Platzierungen. Unsere Endpoint-Lösung wird durch führende globale Analysten anerkannt.

Hauptfunktionen

Cloud-basierte Endpoint-Kontrollen

Verbesserte Programmkontrolle
Reduzieren Sie Ihre Angriffsflächen auf Servern, mobilen Geräten und Computern durch die vollständige Kontrolle darüber, welche Software möglicherweise wann ausgeführt wird. Dies wird durch dynamische Whitelists aus unserer internen Forschungsabteilung ermöglicht. Default Allow- und Default Deny-Szenarien werden unterstützt.

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.

Geräte- und Web-Kontrolle und mehr ...

Verschlüsselung und Datenschutz

Umfassende Verschlüsselung
Sicherheitsteams können FIPS 140-2-zertifizierte Verschlüsselung auf Datei-, Festplatten- oder Geräteebene zentral durchsetzen und native Verschlüsselungstools wie Microsoft BitLocker und macOS FileVault verwalten.

Erstellung eindeutiger, integrierter Richtlinien
Die einzigartige Integration der Verschlüsselung in Programm- und Gerätekontrollen sorgt für eine zusätzliche Sicherheitsstufe und eine einfache Verwaltung.

Funktionen für den zukunftsorientierten Schutz vor 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 von Containern und Terminalservern
Schützt Windows Server-Container und eine Vielzahl von Fernzugriffsumgebungen, darunter Microsoft Terminal Services und Citrix XenApp/Xen Desktop. Die Sicherheitskomponente für Datenverkehr bietet Schutz für Web- und E-Mail-Verkehr auf dem Terminalserver.

Exploit Prevention, Anti-Rootkit und mehr ...

Funktionen für mobile Sicherheit

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

„Over the Air"-Bereitstellung (OTA) und mehr ...

Systeme, Vulnerability & Patch Management

Patch Management
Erweiterte umfassende Schwachstellen-Scans in Kombination mit automatischer Patch-Verteilung.

Zeitsparende Betriebssystem- und Softwareimplementierung
Erstellen, Speichern und Implementieren von Systemimages von einem zentralen Standort. Dies eignet sich ideal z. B. für die Migration auf Microsoft Windows 10 oder für die Implementierung von 150 gängigen Programmen, die vom Kaspersky Security Network identifiziert wurden.

Hardware-, Software- und Lizenzverwaltung
Hardware- und Software-Bestandsberichte unterstützen die Erfüllung von Software-Lizenzverpflichtungen. Sparen Sie Kosten durch eine zentrale Bereitstellung von Software-Rechten.

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-Lab-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