kaspersky BRING ON THE FUTURE

Kaspersky® Endpoint Security for Business

Select

Ready for GDPR

Kaspersky Endpoint Security for Business Select bietet HuMachine™-basierten Schutz für eine Vielzahl von Plattformen, einschließlich Linux-Servern und -Endpoints. Die Lösung liefert mehrschichtige Sicherheit, die verdächtiges Verhalten erkennt und Bedrohungen blockiert, einschließlich Ransomware. Cloud-basierte Kontrollen reduzieren die Angriffsfläche für Cyberbedrohungen und Mobile-Device-Management-Funktionen unterstützen Sie beim Schutz von Mobilgeräten.

Alle Schutz- und Verwaltungsfunktionen, die Sie benötigen

Enterprise-Class Funktionalität für Unternehmen jeder Größe. Wählen Sie entsprechend der Größe und den Schutzanforderungen Ihres Unternehmens zwischen drei verschiedenen Versionen der Endpoint Security for Business Produktfamilie.

Welche Produktversion ist die richtige für Sie?

- **SELECT**
- ADVANCED
- TOTAL

Mehrschichtiger Schutz für

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

Umfassende Schutzmechanismen gegen

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

Enthaltene Funktionen

- Malware-Schutz erweiterte Funktionalität
- Vulnerability Assessment
- Security Policy Adviser
- KI-basierte Algorithmen
- AMSI-Unterstützung neu
- Scans von verschlüsseltem Datenverkehr neu
- Prozessisolierung
- Exploit-Schutz und -Rollback
- Firewall plus Verwaltung der nativen Firewall
- Cloud-basierter Schutz
- Integrierter EDR-Agent
- SIEM-Integration über Syslog neu
- Anwendungskontrolle
- Web- und Gerätekontrolle
- Server- und Containerschutz erweiterte Funktionalität
- Unterstützung für Windows-Linux-Subsysteme neu
- Mobile Threat Defense erweiterte Funktionalität
- Reporting

Ausführliche Informationen finden Sie hier.

Next Generation-Schutz und Kontrolle für jeden Endpoint

Eine zentrale 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 – dank unserer breiten Palette an vorkonfigurierten Szenarien.

Flexible, adaptive Sicherheit

Das Produkt wurde für die Anwendung in IT-Umgebungen jeglicher Art entwickelt. Es bietet viele bewährte und Next Generation-Technologien, um erkannte Angriffe abzuwehren. Darüber hinaus ermöglichen integrierte Sensoren und die Integration in Endpoint Detection & Response (EDR) die Erfassung großer Datenvolumen und gewährleisten damit die Erkennung hoch entwickelter Cyberangriffe.

Cybersicherheit, auf die Sie sich verlassen können.

Unternehmen sind auf Neutralität und Datenhoheit angewiesen – unsere Produkte scannen Daten zwar, sie sammeln sie jedoch nicht. Die statistischen Daten werden zur Gewährleistung der geopolitischen Neutralität in der Schweiz verarbeitet.

Hauptfunktionen

Kernfunktionen

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

Schutz vor Verschlüsselung freigegebener Ordner
Ein einzigartiger Anti-Cryptor-Mechanismus blockiert die Verschlüsselung von Dateien in gemeinsam genutzten Ressourcen, um die Ausführung schädlicher Prozesse auf anderen Geräten im Netzwerk zu verhindern.

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.

Webkonsole
Um die Fehlertoleranz zu optimieren, können Sie unsere Webkonsole implementieren, um physische wie auch virtuelle Geräte in den Cloud-Umgebungen von Amazon und Microsoft Azure zentral zu verwalten.

Funktionen für mobile Sicherheit

Innovative Anti-Malware-Technologien
Die Kombination von ML-basierter, proaktiver und Cloud-basierter Erkennung ermöglicht Echtzeitschutz. Der Webschutz steigert gemeinsam mit manuellen und geplanten Scans die Sicherheit.

„Over the Air"-Bereitstellung (OTA)
Bietet Ihnen die Möglichkeit, Anwendungen zentral per SMS, E-Mail und PC im Voraus zu konfigurieren und bereitzustellen.

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

Anwendungskontrolle für mobile Geräte
Die Anwendungskontrolle schützt Daten in installierter Software und ermöglicht es Administratoren, die Installation und Nutzung bestimmter Programme zu erzwingen.

Cloud-basierte Endpoint-Kontrollen

Andwendungskontrolle
Dynamisches Whitelisting ermöglicht eine granulare Kontrolle über Anwendungen, die auf Ihren PCs ausgeführt werden dürfen.

Dynamische Whitelists
Für eine bessere Programmkategorisierung nutzt die Anwendungskontrolle eine dynamische Whitelisting-Datenbank, die von Kaspersky basierend auf den Kenntnissen zu legitimer Software entwickelt wurde.

Gerätekontrolle
Mit dieser Funktion können Benutzer Datenrichtlinien zur Kontrolle von Wechseldatenträgern und sonstigen Zubehörgeräten festlegen, zeitlich planen und durchsetzen – ganz gleich, ob die Verbindung über USB oder andere Schnittstellen erfolgt.

Host Intrusion Prevention System (HIPS)
Reguliert den Zugriff auf vertrauliche Daten und Aufnahmegeräte mithilfe unserer lokalen und Cloud-basierten (Kaspersky Security Network) Reputationsdatenbanken, ohne die Leistung erlaubter Programme zu beeinträchtigen.

Support und Professional Services

Unsere Professional Services stehen jederzeit für Sie bereit. Mit 34 Niederlassungen in mehr als 200 Ländern weltweit bieten wir Ihnen das ganze Jahr über durchgängigen Support (24x7x365). Holen Sie mit unseren Premium Support-Paketen (MSA) oder mit unseren Professional Services das Beste aus Ihrer Kaspersky-Sicherheitslösung heraus.

Sehen Sie selbst

Erleben Sie True Cybersecurity selbst! Auf dieser Seite **können Sie die vollständige Version** von Kaspersky Endpoint Security for Business testen.

Neues über Cyberbedrohungen:
https://de.securelist.com
IT Security News: https://www.kaspersky.de/blog/b2b/
Cybersicherheit für KMUs: kaspersky.de/business
Cybersicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.com/transparency

Getestet.
Transparent.
Unabhängig.