Kaspersky® Endpoint Security for Business

Advanced

Ready for GDPR

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. Die Sicherheits- und Verwaltungskonsole steigert die Effizienz, während zusätzliche Verteidigungsebenen Schwachstellen beseitigen und vertrauliche Daten weiter schützen.

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
- Windows Server-Container
- Android und andere mobile Geräte
- Wechseldatenträger

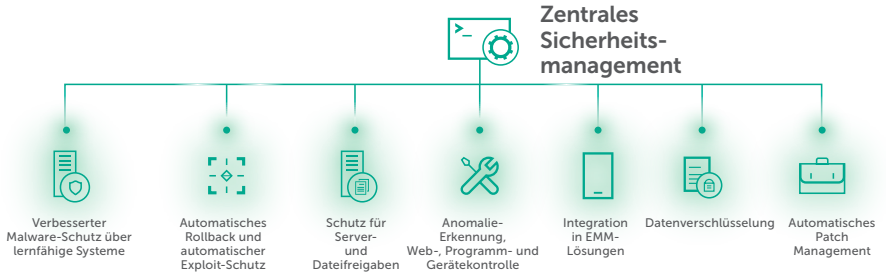
Umfassende Schutzmechanismen gegen

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

Enthaltene Funktionen

- Malware-Schutz erweiterte Funktionalität
- Vulnerability Management
- 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
- Adaptive Anomaly Control neu
- Programm-, Web- und Gerätekontrolle
- Server- und Containerschutz erweiterte Funktionalität
- Schutz für Terminalserver
- Unterstützung für Windows-Linux-Subsysteme neu
- Mobile Threat Defense erweiterte Funktionalität
- Verschlüsselungsmanagement für Betriebssysteme
- Systemkonfiguration und -bereitstellung
- Patch Management erweiterte Funktionalität
- Reporting

Ausführliche Informationen finden Sie hier.



Adaptive Sicherheit mit erweiterten Management- und Datenschutzfunktionen

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 – durch unsere breite 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.

Ein einziges Produkt mit transparenten Kosten

Mit mehreren Sicherheitstechnologien in einem einzigen Produkt gibt es keine versteckten Kosten. Ein Produkt mit lediglich einer Lizenz ist alles, was Sie brauchen, um Ihren IT-Bestand zu schützen.

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

Cloud-basierte Endpoint-Kontrollen

Einzigartige Anomalie- und Anwendungskontrollen
Adaptive Anomaly Control – eine Komponente, die Sicherheitsstufen automatisch auf die höchste Ebene anhebt, die für die Rolle des jeweiligen Benutzers sinnvoll ist – wird von der Anwendungskontrolle sowie topaktuellen Whitelisting-Datenbanken ergänzt.

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

Geräte-, Webkontrolle und mehr

Verschlüsselung und Datenschutz

Umfassende Verschlüsselung
Ihr Sicherheitsteam kann zentral die Verschlüsselung per FIPS 140.2 und Common Criteria auf Datei-, Festplatten- oder Geräteebene durchsetzen und native Verschlüsselungstools wie Microsoft BitLocker und macOS FileVault verwalten.

Einheitliche integrierte Richtlinie
Die einzigartige Integration der Verschlüsselung in Programm- und Gerätesteuerungen sorgt für eine zusätzliche Sicherheitsebene und vereinfacht die Verwaltung.

Wichtige Schutzfunktionen

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 von Containern und Terminalservern
Schützt Windows Server-Container und eine Vielzahl von Remote-Zugriffs-Umgebungen, darunter die Microsoft-Remotedesktopdienste und Citrix XenApp/Xen Desktop. Die Sicherheitskomponente für Datenverkehr bietet Schutz für Web- und E-Mail-Verkehr auf dem Terminalserver.

Exploit-Schutz, Anti-Rootkit-Technologie und mehr

Funktionen von Mobile Threat Defense

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

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

Vulnerability und Patch Management

Patch Management
Die erweiterten Scans zum Finden von Schwachstellen werden durch die automatisierte Patch-Verteilung ergänzt.

Zeitsparende Betriebssystem- und Softwareimplementierung
Erstellen, Speichern und Implementieren von Systemimages von einem zentralen Standort. Dies eignet sich ideal z. B. für ein Upgrade auf Microsoft Windows 10 oder für die Implementierung von 150 gängigen Programmen, die dem Kaspersky Security Network bekannt sind.

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

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.

Kaspersky Lab
Finden Sie einen Partner in Ihrer Nähe:
www.kaspersky.de/partners
Kaspersky for Business: www.kaspersky.de/business-security
IT Security News: www.kaspersky.de/blog/b2b/
Unser einzigartiger Ansatz:
www.kaspersky.de/true-cybersecurity

#truecybersecurity
#HuMachine

www.kaspersky.de