Kaspersky®
Endpoint Security
for Business

Schutz vor Cyberbedrohungen

Jede Sicherheitslösung ist nur so effektiv wie die Engine zur Bedrohungsprävention, auf der sie basiert. Patch Management, Verschlüsselung, Programmkontrollen – all diese Technologien bieten wertvolle zusätzliche Sicherheit, können aber keine grundlegenden Mängel im Schutz vor Bedrohungen kompensieren.

Der Schutz vor Bedrohungen steht im Mittelpunkt aller unserer Sicherheitslösungen, Produkte und Dienstleistungen. Unser mehrschichtiger, anpassungsfähiger Ansatz basiert auf einem Spektrum von Komponenten, von denen viele einzigartig sind und entwickelt wurden, um verschiedenen Formen der Cyberbedrohung auf verschiedenen Ebenen entgegenzuwirken. Das Ergebnis sind defensive und vorausschauende Next Generation-Technologien, die gemeinsam dafür sorgen, dass modernste und fortgeschrittenste Bedrohungen, auch künftige Bedrohungen, schnell erkannt, abgemildert und aufgehalten werden können.

Mit Erfahrung und Forschung gegen Bedrohungen

Der Next Generation-Schutz basiert auf unserem einzigartigen HuMachine™-Ansatz und nutzt dabei die kombinierten Stärken des maschinellen Lernens, der menschlichen Erfahrung und umfassender Bedrohungsinformationen. Kaspersky Lab war im Bereich der Threat Intelligence stets einer der Vorreiter: Wir haben mehr APTs als andere Anbieter aufgedeckt, und unsere Bereitschaft, auch zukünftig in Ihren Schutz zu investieren, zeigt sich in der Größe und dem weltweiten Ruf unserer Forschungsteams.

Threat Hunting mit Kaspersky EDR

Die Integration mit Kaspersky Endpoint Detection and Response bietet automatisierte Funktionen für die Vorfallsreaktion. Dieser umfassende Ansatz für EDR erhöht die Transparenz Ihrer gesamten IT-Infrastruktur und ermöglicht SOC-Teams fundierte Entscheidungen dazu, wie Malware mit niedriger Priorität sowie neueste Bedrohungen optimal abgewehrt werden können. EPP und EDR-Funktionen arbeiten über einen einzigen Agenten zusammen.

Mehrstufiger Schutz durch fortschrittliche Technologien

Multidimensionaler Schutz durch eine Kombination von Technologien zur Bedrohungsprävention, basierend auf Algorithmen des maschinellen Lernens. Hoch entwickelte Endpoint-Kontrollen und Systemhärtung, einschließlich Programmkontrolle und Whitelisting, Verhaltenserkennung, automatisierte Beseitigung, Exploit Prevention und Anti-Ransomware-Schutz sind in unsere Endpoint-Sicherheitsplattformen integriert. Auch Schutz vor PowerShell- und dateilosen Angriffen ist enthalten.

Einfache Verwaltung für Großunternehmen

Die Verwaltung von Hunderten und Tausenden Endpoints über eine einheitliche Konsole ermöglicht die präzise Kontrolle und bietet eine umfassende Übersicht Ihrer gesamten Infrastruktur – sowohl vor Ort als auch in der Cloud. Zu den Szenarien für Großunternehmen zählen die automatisierte Implementierung, Zustandsprüfungen und automatisierte Berichte sowie die vollständige Unterstützung von hierarchischen und Air-Gap-Umgebungen.

Funktionen

Essenzieller Schutz vor Bedrohungen

Schutz vor Bedrohungen durch Dateien

Ein obligatorisches Element des Malware-Schutzes, der ein komplettes Spektrum von Schutztechnologien gegen dateibasierte Bedrohungen implementiert. Beinhaltet WSL-Scans (Windows Subsystem for Linux).

Schutz vor Bedrohungen für E-Mails

E-Mails zählen zu den Schwachstellen, die am häufigsten von Cyberkriminellen ausgenutzt werden. Der Schutz vor Bedrohungen für E-Mails scannt eingehende und ausgehende E-Mails auf gefährliche Objekte.

Schutz vor Bedrohungen aus dem Web

Um eine sichere Arbeit mit Internetressourcen zu gewährleisten, werden eingehende und ausgehende Daten geschützt und URLs anhand von Listen mit bösartigen oder Phishing-Webadressen überprüft. Die Komponente „Web Threat Protection" scannt den HTTPS-Datenverkehr, um die neuesten Bedrohungen, wie z. B. Botnet-Agenten, Malware-Dropper, Ransomware usw., frühzeitig abzufangen.

Schutz vor Bedrohungen im Netzwerk

Scannt eingehenden Netzwerkverkehr auf Aktivitäten, die auf Netzwerkangriffe hindeuten. Der Schutz vor MAC-Spoofing steigert die Sicherheit Ihrer Infrastruktur weiter, indem Angriffe, bei denen Adressänderungen zur Infektion von Endpoints zum Einsatz kommen, erkannt und blockiert werden und der Datenverkehr an andere Netzwerkgeräte abgefangen wird.

Firewall

Schränkt die Netzwerkaktivität des geschützten Nodes ein. Vordefinierte Regeln decken die Filterung von Netzwerkpaketen und Datenströmen sowie softwarebasierte Netzwerkinteraktionen ab.

Schutz vor BadUSB-Angriffen

Einige Viren modifizieren die Firmware von USB-Geräten, damit das Betriebssystem das entsprechende Gerät als Tastatur erkennt. Der Schutz vor BadUSB-Angriffen implementiert einen Prozess zur Tastaturautorisierung, um infizierte USB-Geräte zu erkennen, die Tastaturen emulieren. Das Programm ermöglicht die Verwendung autorisierter Tastaturen und blockiert nicht autorisierte.

AMSI-Schutzanbieter (Anti-Malware Scan Interface)

Ermöglicht Kaspersky Endpoint Security das Scannen von Objekten, die von Malware-Analyseprogrammen von Drittanbietern gesendet werden. Die Ergebnisse werden dann an das anfordernde Programm weitergeleitet, das anhand der Informationen das entsprechende Objekt blockieren oder löschen kann.

Erweiterter Schutz vor Bedrohungen

Kaspersky Security Network (KSN)

Eine komplexe Cloud-Infrastruktur erfasst und analysiert Cybersicherheitsdaten von Millionen freiwilligen Teilnehmern auf der ganzen Welt, um Malware zu erkennen und schnellstmöglich auf neue Bedrohungen zu reagieren.

Verhaltenserkennung

Bietet proaktiven Schutz, bei dem Technologien wie maschinelles Lernen zum Einsatz kommen, um verdächtige Verhaltensmuster zu erkennen und zu extrahieren und Ihr System so effektiv vor Ransomware zu schützen. Sowohl schädliche lokale Dateiverschlüsselungen als auch Remote-Verschlüsselungen von freigegebenen Ordnern über das Netzwerk können erkannt, gestoppt und abgewehrt werden.

Exploit-Schutz

Schützt speziell vor Malware, die Software-Schwachstellen in beliebten Programmen ausnutzt, indem sie typische bzw. verdächtige Verhaltensmuster erkennt und den Exploit aufhält, bevor schädlicher Code ausgeführt werden kann.

Host Intrusion Prevention System (HIPS)

Weist jedem Programm basierend auf KSN-Daten eine von vier standardmäßigen Vertrauensgruppen zu. Programme der vertrauenswürdigsten Gruppe werden der Whitelist hinzugefügt und können ohne Einschränkungen ausgeführt werden. Die übrigen Programme können mit eingeschränkten Berechtigungen ausgeführt werden und erhalten nur beschränkten Zugriff auf kritische Systemressourcen.

Remediation Engine

Erfasst Daten zu verdächtigen Aktivitäten und ermöglicht es Kaspersky Endpoint Security so, Aktionen rückgängig zu machen, die Malware im Betriebssystem ausgeführt hat.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **https://de.securelist.com**
IT Security News: **www.kaspersky.de/blog/b2b/**
Unser einzigartiger Ansatz:
www.kaspersky.de/true-cybersecurity

#truecybersecurity
#HuMachine

www.kaspersky.de