Kaspersky® Endpoint Security

Die zuverlässige mehrschichtige Endpoint Protection, basierend auf True Cybersecurity-Technologien

Die Bedrohungslage hat sich exponentiell verschlechtert: Wichtige Geschäftsprozesse, vertrauliche Daten und finanzielle Ressourcen sind einem ständig steigenden Risiko durch Zero-Day-Angriffe ausgesetzt. In den vergangenen 12 Monaten waren mehr als 38 % aller Unternehmen Risiken durch Malware ausgesetzt. Um das Risiko für Ihr Unternehmen zu verringern, müssen Sie smarter, besser gewappnet und besser informiert sein als die Cyberkriminellen, die es auf Ihr Unternehmen abgesehen haben.

Fakt ist: Die Mehrheit der Cyberangriffe auf Unternehmen werden über Endpoints initiiert. Wenn Sie jeden Endpoint im Unternehmen, ob physisch oder virtuell, stationär oder mobil, wirksam sichern können, ist dies eine starke Grundlage für Ihre gesamte Sicherheitsstrategie.

Die Technologien und Threat Intelligence von Kaspersky Lab werden ständig weiterentwickelt, damit Unternehmen selbst vor den neuesten und raffiniertesten Bedrohungen und Exploits sowie zielgerichteten Angriffen geschützt sind.

Dieser verzögerungsfreie Schutz vor bekannten und unbekannten Bedrohungen wird durch leistungsstarke Kontroll- und Datenschutztools ergänzt, darunter integrierte Verschlüsselung, automatisiertes Patching und Schutz von mobilen Endpoints, die alle gemeinsam über das Kaspersky Security Center verwaltet werden.

Bedrohungsprävention

Unsere führende Engine zur Bedrohungsprävention, die auf HuMachine™-Informationen basiert, schützt Sie vor Ransomware, Schwachstellenausnutzung und sogar den höchstentwickelten Cyberbedrohungen.

Fortschrittliche Endpoint-Kontrolle

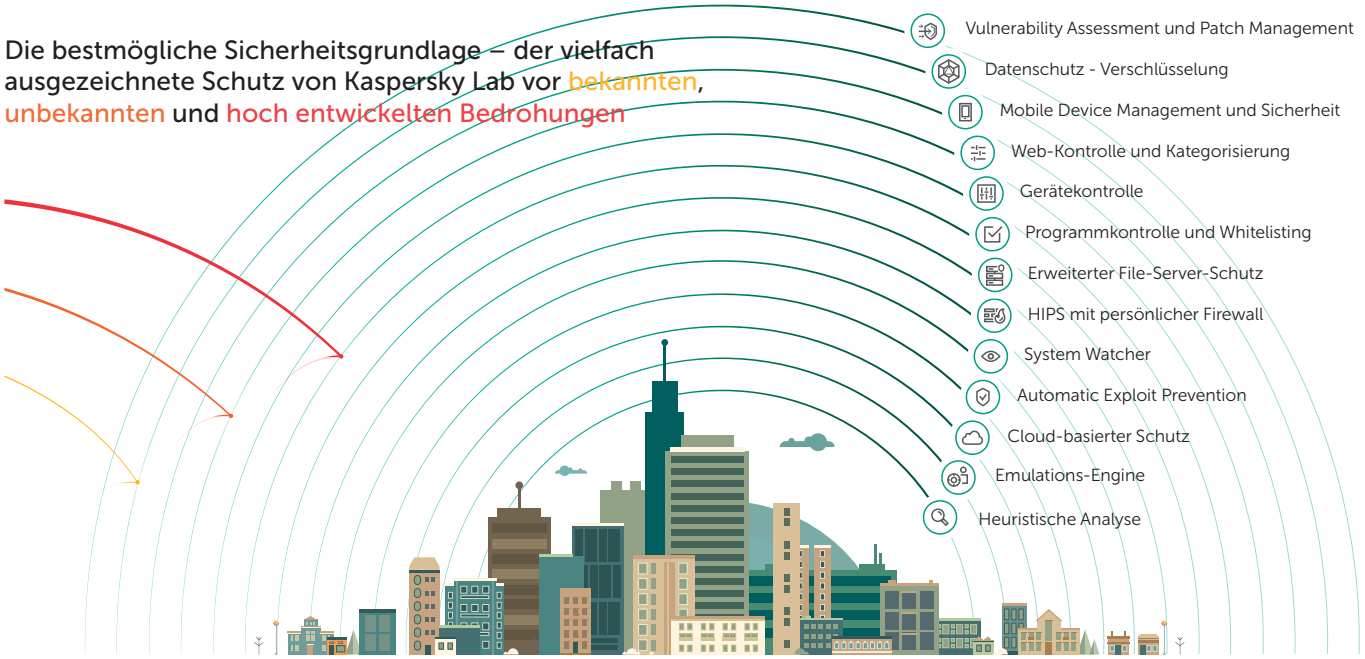
Einfache und effektive Kontrollen für Internet, Geräte und Anwendungen reduzieren die Angriffsfläche und sorgen für die Sicherheit Ihrer Benutzer.

Datenschutz

Mithilfe der FIPS-140.2-zertifizierten Full-Disk-Verschlüsselung können Sie vertrauliche Daten auf stationären und mobilen Geräten umfassend schützen.

Mehrstufiger Schutz

Die bestmögliche Sicherheitsgrundlage – der vielfach ausgezeichnete Schutz von Kaspersky Lab vor bekannten, unbekannten und hoch entwickelten Bedrohungen



EFFIZIENTER, MEHRSTUFIGER SCHUTZ VOR ALLEN ARTEN VON CYBERBEDROHUNGEN

Zuverlässige Sicherheit auf der Basis von lernfähigen Systemen

Die vollständige Absicherung Ihrer Endpoints gegen jede Form von bekannter und unbekannter Cyberbedrohung ist eine große Aufgabe. Herkömmlicher Malware-Schutz kann das nicht leisten. Nur die Nutzung einer modernen Sicherheitsplattform mit einem mehrstufigen Ansatz kann dafür sorgen, dass Sie jeden einzelnen Endpoint innerhalb und außerhalb Ihres Perimeters schützen können.

Hohe Leistung

Die integrierte Sicherheitsplattform von Kaspersky Lab ist kontinuierlicher Pulsgeber im Herzen Ihrer IT-Infrastruktur und bietet leistungsstarken Schutz für Ihre Endpoints, wobei die Geschwindigkeit und die Ressourcen nur minimal beeinträchtigt werden. Komplett im eigenen Haus entwickelt ist diese Lösung eine voll skalierbare integrierte Plattform, die optimale Systemleistung liefert, ohne dass Konflikte mit Software oder Sicherheitslücken entstehen.

Leistungsstarke Informationen zur Bedrohungslage

Auf der Basis von stets aktuellen Bedrohungsinformationen in Echtzeit entwickeln wir unsere Technologien kontinuierlich weiter. So schützen wir auch Ihr Unternehmen zuverlässig vor den Bedrohungen von heute und morgen. Auch vor Zero-Day-Exploits. Mit Kaspersky Lab setzen Sie auf einen der weltweit führenden Anbieter und auf innovative Lösungen, die Ihr Unternehmen zuverlässig schützen. Für Ihr Unternehmen kann es keine bessere Sicherheitslösung geben.

Einheitliche und zentrale Verwaltung

Verwalten Sie Multi-Plattformen und Geräte von derselben Konsole aus, über die auch andere Endpoints verwaltet werden, und verbessern Sie Transparenz und Kontrolle ohne Mehraufwand oder zusätzliche Technologien.

Zuverlässige Abwehr und Eliminierung von Bedrohungen der nächsten Generation (Next Gen Threats)

Im Kern Ihrer Sicherheitsstrategie steht eine der leistungsfähigsten und effektivsten Engines zum Schutz von Endpoints, was immer wieder durch unabhängige Tests bestätigt wird. [1]Diese Lösung basiert auf weltweit führenden Sicherheitsdaten und Technologien für lernfähige Systeme und maschinelles Lernen.

Schicht um Schicht verzahnen sich vorausschauende und intelligente Schutzfunktionen zu einer leistungsstarken und zuverlässigen Verteidigung gegen die ausgefeiltesten bekannten, unbekannten und modernsten Cyberbedrohungen.

- **Heuristische und Bedrohungs-Emulationsanalyse** mit mehreren Algorithmen – erkennt unbekannte Malware und ergänzt herkömmliche **signaturbasierte** Technologien.
- **Cloud-basierter Schutz (Kaspersky Security Network)** – erleichtert die Identifizierung und Blockierung von neuen Malware-Bedrohungen in Echtzeit, sobald diese auftreten.
- **Automatischer Exploit-Schutz** – hält durch Blockierung von Exploits, die von Cyberkriminellen genutzt werden, auch die höchstentwickelten Bedrohungen ab.
- **System Watcher** – blockiert unbekannte Bedrohungen durch Erkennung verdächtiger Verhaltensmuster und stellt wichtige Dateien wieder her, wenn das System beeinträchtigt wird. Dies bietet zuverlässigen Schutz vor Ransomware.
- **Hostbasierte Angriffsüberwachung (HIPS)** – beschränkt Aktivitäten und gewährt Berechtigungen gemäß der Vertrauensstufe der Software.
- **Persönliche Firewall** für Beschränkungen der Netzwerkaktivität.
- **Network Attack Blocker** stoppt netzwerkbasierte Angriffe.

[1] www.kaspersky.com/de/top3

Anti-Ransomware- und Anti-Exploit-Schutz

Mit Kaspersky System Watcher halten Sie Ihre Daten geschützt und vermeiden es, Cyberkriminelle durch Lösegeldzahlungen zu finanzieren. Mit Kaspersky Security for Windows Server schützen Sie freigegebene Ordner vor modernen Crypto Lockern. Außerdem können Sie mit unseren Automatic Exploit Prevention-Technologien Endpoints vor den neuesten Exploits schützen.

Senken Sie das Angriffsrisiko über Anwendungen

Dynamische Whitelists und die Programmkontrolle können das Risiko von Zero-Day-Angriffen erheblich reduzieren, indem Sie die vollständige Kontrolle darüber erhalten, welche Software ausgeführt werden darf. Programme auf der Blacklist werden blockiert, während jene, die verdächtiges oder unangemessenes Verhalten zeigen, mithilfe des Aktivitätsmonitors und HIPS erkannt, analysiert und anschließend blockiert oder beschränkt werden. Ihre genehmigten und vertrauenswürdigen Anwendungen laufen unterdessen reibungslos weiter.

Nutzen Sie Cloud-Empowered Flexible Whitelisting

Whitelisting durch unser eigenes Labor unterstützt ein **Default-Deny**-Szenario, das in jeder Umgebung ausgeführt werden kann.

Risiken beim Surfen beseitigen

Die Web-Kontrolle überwacht, filtert und kontrolliert, welche Webseiten der Endbenutzer am Arbeitsplatz verwenden darf, und erhöht die Produktivität, während Ihre Schwachstellen gegenüber Systempenetration und Infiltrierung über Webseiten und Social Media abgemildert werden.

Kontrolle über die Nutzung von tragbaren Geräten

Die Gerätekontrolle schützt vor den schädigenden Folgen des Verlustes von Unternehmens- und Kundendaten auf nicht genehmigten oder unverschlüsselten Mobilgeräten sowie vor dem Hochladen von infizierten Daten von einem Gerät.

Stellen Sie erweiterten Schutz für Ihre Unternehmensserver bereit

Application Launch Control auf Servern bietet zuverlässige Sicherheit durch konfigurierte Regeln, die zulassen bzw. unterbinden, dass ausführbare Dateien, Skripte und MSI-Pakete gestartet oder DLL-Module auf den Server geladen werden.

Jeder Endpoint unter Ihrer Kontrolle

Begrenzen Sie das Risikopotential für Endpoints und erhöhen Sie zugleich die Produktivität. Kontrollieren Sie den Zugriff einzelner Endpoints auf Programme, Webseiten und Geräte: Zugriffe auf unangemessene Elemente werden identifiziert und blockiert, Zugriffe auf unnötige Elemente reguliert und der Zugriff auf vertrauenswürdige Elemente gefördert.

Alle Kontrolltools lassen sich in die Active Directory integrieren, und die vereinfachte, anpassbare oder automatisierte Erstellung von Richtlinien und deren Durchsetzung können je nach Präferenz zentralisiert oder rollenbasiert erfolgen.

Schutz von Daten durch integrierte, FIPS 140-2-zertifizierte Verschlüsselung

Die leistungsstarke, benutzertransparente Verschlüsselung schützt vertrauliche Daten unterwegs auf tragbaren Geräten und vor Ort. Integrierte Technologie bedeutet, dass Sie die Verschlüsselung der Unternehmensdaten auf Ebene der Datei, Festplatte oder des Geräts zentral erzwingen können, indem Sie Sicherheitsrichtlinien einrichten, die sich auf Gruppen von Endpoints oder auf einzelne Geräte beziehen. Dies erfolgt über die gleiche zentrale Konsole, mit der die gesamte Endpoint-Sicherheitslösung von Kaspersky Lab verwaltet wird. Außerdem kommt native Betriebssystemverschlüsselung zum Einsatz, darunter Microsoft BitLocker.

Eliminierung von Schwachstellen durch automatisiertes Patching

Die Ausnutzung von unerkannten Schwachstellen in einem vertrauenswürdigen Programm ist einer der üblichsten Wege, um Zugriff auf die IT-Infrastruktur über einen einzigen Endpoint zu erlangen. Die Priorisierung und Verwaltung des zeitnahen und effizienten Patchings erfordert ein tiefgreifendes Verständnis für die Schwachstellen, ihrer Verhaltensstrukturen und ihrer Ziele. Die **automatisierte Bewertung von Schwachstellen und das Patch Management** von Kaspersky Lab basierend auf globalen Informationen zu Exploit-Aktivitäten in Echtzeit halten das kritische Patching auf dem neuesten Stand, ohne dass die laufenden Systeme und Benutzer beeinträchtigt werden.

Sicherheit für Mobilgeräte jenseits Ihres Perimeters

Auf Unternehmensdaten kann inzwischen über Smartphones und Tablets von überall und zu jeder Zeit zugegriffen werden, wobei Ihr IT-Perimeter frei passiert wird. **Mobile Sicherheit** schützt vor Bedrohungen, die speziell auf vertrauliche Daten auf mobilen Geräten abzielen, sowie vor jenen, die nach Sicherheitslücken auf unternehmenseigenen oder privaten Geräten suchen, um so die Systeme infiltrieren zu können.

Optimierte Effizienz – integriertes Management

Kaspersky Endpoint Security gibt Ihren Sicherheitsteams volle Transparenz und Kontrolle über jeden Ihrer Endpoints, stationär oder mobil, unabhängig von Ort und Aktivität. Die Lösung ist nahezu ins Unendliche skalierbar und bietet Zugriff auf Bestandslisten, Lizenzierung, Remote-Troubleshooting und Netzwerkkontrollen, die alle über eine Konsole zugänglich sind, das **Kaspersky Security Center**.

Die zentrale Verwaltung über eine einzige Konsole wird durch rollenbasierte Verwaltungsfunktionen ergänzt, sodass Zugriffsrechte und Aufgaben wie erforderlich einzelnen Sicherheitsexperten zugewiesen werden können.

Der Blick auf das große Ganze – Sicherheitslösungen für Unternehmen von Kaspersky Lab

Der Schutz von Endpoints ist entscheidend, stellt aber nur einen Teil des großen Ganzen dar. Egal, ob Sie eine Single- oder Multi-Vendor-Strategie umsetzen, Kaspersky Lab bietet eine **große Bandbreite an Unternehmenslösungen**, die sich gegenseitig ergänzen oder unabhängig arbeiten, sodass Sie frei sind, ohne auf Leistung oder Wahlfreiheit verzichten müssen. Unsere Lösungen schützen **virtuelle und Cloud-basierte Systeme** sowie **physische Endpoints, Server und Infrastrukturen**. Außerdem bieten wir dedizierte Cybersecurity-Lösungen für einige **vertikale Branchen**, darunter Finanzdienstleistungen Gesundheitswesen und Behörden.

Anti Targeted Attack

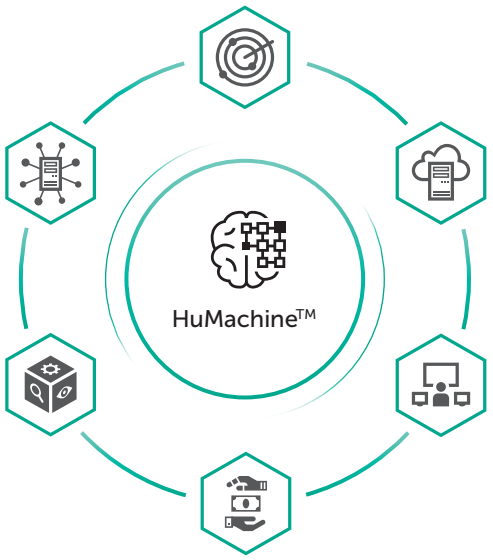
Umfassende Erkennung verschiedener Vektoren und Risikominimierung bei fortschrittlichen Bedrohungen und zielgerichteten Angriffen

Endpoint Security

Die zuverlässige mehrschichtige Endpoint Ptotection-Plattform, basierend auf True Cybersecurity-Technologien

Cloud Security

Perfekt für Ihre Hybrid-Cloud



Cybersecurity Services

Mit Bedrohungsinformationen, Sicherheitsschulungen, Vorfallsreaktion und Assessments

Security Operations Center

Versorgt Ihr SOC mit den Tools und Informationen zur effizienten Erkennung und Abwehr von Bedrohungen

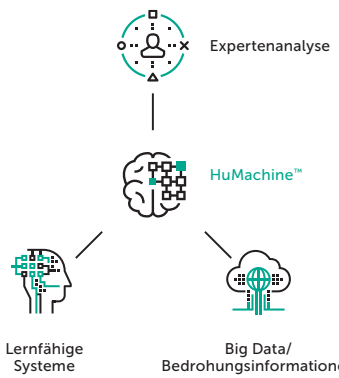
Fraud Prevention

Frühzeitige Erkennung plattformübergreifender Betrugsversuche in Echtzeit

Maintenance und Support

Wir sind in mehr als 200 Ländern in 34 Niederlassungen weltweit tätig und bieten Ihnen exzellenten Support – rund um die Uhr an jedem Tag im Jahr. Dieses Engagement spiegelt sich in unseren speziellen **Maintenance Service Agreement (MSA)-**Support-Paketen wider. Unsere **professionellen Serviceteams** sind immer in Bereitschaft und stellen sicher, dass Sie aus Ihrer Kaspersky-Sicherheitslösung stets das Maximum herausholen.

Kontaktieren Sie das Kaspersky Lab Enterprise Sales Team, um mehr über die effektive Sicherung Ihrer Endpoints zu erfahren.



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **https://de.securelist.com/**
IT-Sicherheitsnachrichten: **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.de