KASPERSKY ENDPOINT SECURITY FOR ENTERPRISE

Innovativer Schutz vor hoch entwickelten Bedrohungen, die gezielt Ihre Endpoints und Benutzer angreifen

Die Bedrohungslage hat sich exponentiell verschlechtert: Wichtige Geschäftsprozesse, vertrauliche Daten und finanzielle Ressourcen sind einem ständig steigenden Risiko durch Zero-Day-Attacken 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, sei es ein stationärer oder mobiler Endpoint, wirksam sichern können, ist dies eine starke Grundlage für Ihre gesamte Sicherheitsstrategie.

LEISTUNGSSTARKER SCHUTZ

Die vollständige Absicherung Ihres Endpoints gegen jede Form von bekannter und unbekannter Cyberbedrohung ist eine große Aufgabe. Herkömmliche Virenschutzprogramme können 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.

STARKE LEISTUNG

Der Schutz der Endpoints sollte in jedem Unternehmen selbstverständlich sein.
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 Leistung liefert, ohne dass Konflikte mit Software oder Sicherheitslücken entstehen.

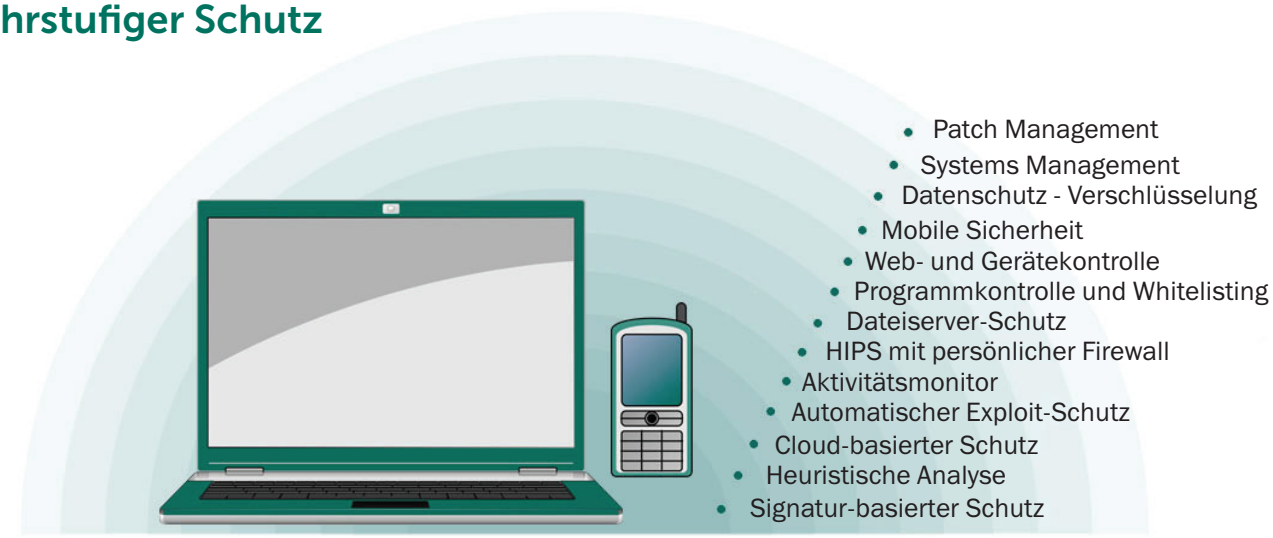
LEISTUNGSSTARKE INFORMATIONEN ZUR BEDROHUNGSLAGE

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.

ZENTRALISIERTE VERWALTUNG

Verwalten Sie eine Vielzahl von Plattformen und Geräten von derselben Konsole aus, über die auch andere Endpoints verwaltet werden, und verbessern Sie Transparenz und Kontrolle ohne mehr Aufwand oder zusätzliche Technologien.

Mehrstufiger Schutz



Abwehr und Eliminierung von Bedrohungen der nächsten Generation

Das Herzstück einer umfassenden Sicherheitsstrategie bildet unsere leistungsstarke und effektive Endpoint Protection. Unabhängige Test bestätigen das regelmäßig.[1]

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

- Heuristische Analyse mit **mehreren Algorithmen** – Erkennt unbekannte Malware und ergänzt herkömmliche **signaturbasierte** Technologien.
- **Cloud-basiertes Kaspersky Security Network (KSN)** – 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.
- **Aktivitätsmonitor** – Blockiert unbekannte Bedrohungen, indem verdächtige Verhaltensmuster erkannt werden, und stellt Schlüsseldateien wieder her, wenn das System beschädigt wurde
- **Hostbasierte Angriffsüberwachung (HIPS)** – Beschränkt Aktivitäten und gewährt Berechtigungen gemäß der Vertrauensstufe der Software
- **Persönliche Firewall** für Beschränkungen der Netzwerkaktivität
- **Network Attack Blocker** stoppt Netzwerk-basierte Angriffe
- **Auch die Dateiserver** sind vollständig geschützt

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 Plug-ins: Zugriffe auf unangemessene Elemente werden identifiziert und blockiert, Zugriffe auf unnötige Elemente reguliert und der Zugriff auf vertrauenswürdige Elemente gefördert.

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

RISIKEN MITHILFE VON PROGRAMMEN MINDERN

Das **dynamische Whitelisting der Programmkontrolle** kann 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.

FLEXIBLES WHITELISTING IN DER CLOUD

Unser internes Whitelisting Lab unterstützt das Default-Deny-Szenario, das in Testbedumgebung 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 MOBILEN 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.

Daten schützen per integrierter Verschlüsselung

Die leistungsstarke, benutzertransparente **Verschlüsselung** schützt vertrauliche Daten unterwegs auf mobilen 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.

---

1 Referenz hier – Top3.

Eliminierung von Schwachstellen durch intelligentes 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. **Der Schutz von Mobilgeräten** 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.

Enthaltene Funktionen

- **Leistungsstarker mehrstufiger Schutz** vor Bedrohungen durch Malware für alle führenden mobilen Plattformen.
- **Anti-Phishing-**Technologie – Blockiert gefährliche Links in Nachrichten und auf Webseiten, der Filter für Anrufe und SMS wendet unerwünschte Kommunikation ab
- **Application Wrapping** – Unternehmensdaten auf den Privatgeräten von Mitarbeitern werden eingekapselt, verschlüsselt und separat gelöscht.
- **Die Programm- und Web-Kontrolle** mit Unterstützung durch KSN blockiert den Zugriff auf unautorisierte Software und Webseiten.
- **Diebstahlschutz-Funktionen** – Löschen, Gerätesperre, Ortung, SIM-Kontrolle, „Fahndungsfoto" und Alarm ermöglichen die schnelle Deaktivierung von Geräten und das Löschen von vertraulichen Daten, wenn ein Gerät verloren oder gestohlen wird.
- **Gerootete oder per Jailbreak entsperrte Geräte** erkennen und melden, sodass eine Maßnahme ergriffen werden kann
- **Zentralisierte Verwaltung** – Inklusive Mobile Device und Applications Management (MDM/MAM). Die Richtlinien können auf unterschiedlichen Geräten auf allen großen Plattformen über eine einzige Schnittstelle bereitgestellt werden.

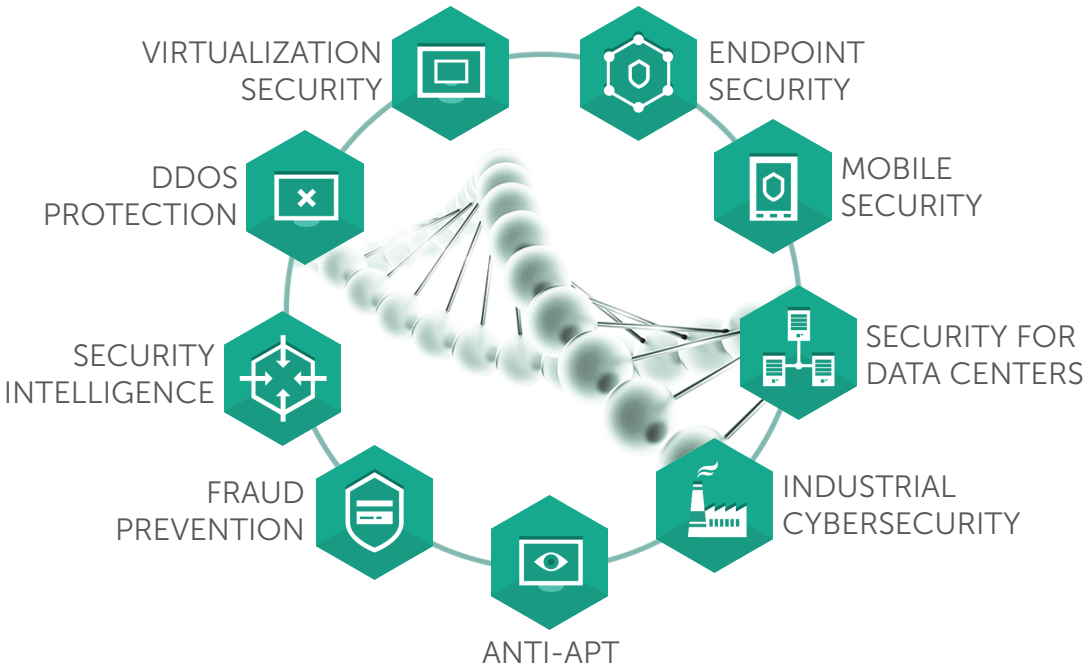
Optimierte Effizienz – Integriertes Management

Kaspersky Endpoint Security for Enterprise 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 zentralisierte Verwaltung über eine einzige Konsole wird durch die rollenbasierte Management-Funktion ergänzt, sodass Zugriffsrechte und Aufgaben wie erforderlich einzelnen Sicherheitsexperten zugewiesen werden können.

Blick auf das Ganze – Sicherheitslösungen für Unternehmen von Kaspersky

Der Schutz von Endpoints ist entscheidend, befindet sich jedoch noch in den Kinderschuhen. Ob Sie auf den Branchenführer vertrauen oder bei Ihrer Sicherheitsstrategie mit nur einem Anbieter arbeiten, 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. Die Lösungen decken **virtualisierte** und **physische Systeme, Server und Infrastrukturen** gleichermaßen ab und werden durch Systeme, die sich auf **branchenspezifische Probleme** wie Finanzbetrug oder Denial-of-Service-Angriffe konzentrieren, sowie durch unser Sortiment an **Security Intelligence Services** ergänzt.



Instandhaltung 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 Lab Sicherheitslösung stets das Maximum herausholen.

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

Kaspersky Enterprise Security for Endpoints/V 1.0/Nov 15/Global