Kaspersky® Security for Internet Gateway

Stärken Sie Ihre erste Verteidigungslinie

Allein im zweiten Quartal 2018 haben Kaspersky-Lösungen über 960 Millionen Angriffe abgewehrt, die von Internetressourcen in 187 Ländern ausgegangen sind. Dies ist nicht überraschend, wenn man bedenkt, wie stark Unternehmen auf das Internet angewiesen sind. Wenn Ihr Unternehmen jedoch auf das Internet angewiesen ist, ist es unerlässlich, es abzusichern.

Endpoints sind das häufigste Ziel von Angriffen. Hier greifen Benutzer auf Webressourcen zu und hier können Angreifer die Handlungen von Menschen durch Social Engineering beeinflussen. Nutzer klicken oftmals auf Links, ohne genauer darüber nachzudenken. Dies kann sogar den besten Endpoint-Schutz aushebeln. Infektionen zu verhindern, bevor sie den Benutzer erreichen, ist nun wichtiger denn je.

Wichtigste Vorteile

- Malware- und Phishing-Schutz in Echtzeit auf Basis maschinellen Lernens
- Wehrt Ransomware ab, bevor sie in das Unternehmensnetzwerk gelangt
- Steigert die Erkennungsraten, ohne dabei zusätzliche Fehlalarme zu erzeugen
- Inhaltsfilterung zur Abwehr potentiell gefährlicher Dateien und zur Verhinderung von Datenlecks
- Webkontrolle zur Überwachung der Webressourcennutzung
- Sichere SSL-verschlüsselte Überwachung des Datenverkehrs
- Skalierbar für Netzwerke mit hoher Auslastung
- Schutz vor Zero-Hour-Bedrohungen
- Unterstützt durch globale Threat Intelligence von Kaspersky Security Network
- Mehrmandantenfähigkeit für MSPs und Unternehmen mit einem breit gefächerten Portfolio

Dadurch, dass 95 % der eingehenden Bedrohungen auf der Gateway-Ebene aufgehalten werden und die Endpoints gar nicht erst erreichen, reduziert Kaspersky Security for Internet Gateways die potentiellen Auswirkungen auf Benutzer und ihre Workstations deutlich. Durch die Integration von Kaspersky Security for Internet Gateways in den vorhandenen Schutz Ihrer Infrastruktur wird das Risiko einer Infektion erheblich reduziert und die Geschäftskontinuität sichergestellt.

Merkmale und Vorteile

Wehrt eingehende Malware und Ransomware ab

Mit mehreren sich überschneidenden Erkennungsebenen, die durch maschinelles Lernen unterstützt werden, verhindert Kaspersky Security for Internet Gateway, dass fortschrittliche Malware und Ransomware in Ihre IT-Infrastruktur eindringt und geschäftskritische Prozesse beeinträchtigt. Die Effizienz der Kaspersky Engines wird kontinuierlich durch Bestnoten in unabhängigen Tests belegt.

Wirkt den Auswirkungen von Internet-Phishing entgegen

Phishing wird genutzt, um Benutzer dazu zu bringen, zu glauben, dass eine betrügerische Ressource legitim ist. Wenn der Benutzer den Köder schluckt, kann dies zum Verlust personenbezogener und sogar finanzieller Daten führen. Das fortschrittliche Cloud-basierte Anti-Phishing-System von Kaspersky nutzt weltweit gesammelte Daten zu schädlichen URLs und Phishing-URLs, um Sie vor bekannten und unbekannten Zero-Hour-Phishing-URLs zu schützen, die in heruntergeladenen Dateien enthalten sind.

Verhindert potentiell gefährliche Dateiübertragungen

Effektive Funktionen zur Inhaltsfilterung reduzieren das Risiko von Infektionen und Datenlecks, indem sie den gesamten Inhalt, der sich durch das Netzwerk bewegt, auf Basis verschiedener von Administratoren festgelegter Parameter filtern.

Reduziert Risiken und steigert die Produktivität durch Überwachung der Internetnutzung

Administratoren können benutzerdefinierte Regeln für Webkontroll-Szenarien konfigurieren und erstellen, um die Verwendung bestimmter Arten von Webressourcen einzuschränken. So wird das Risiko von Infektionen durch Webressourcen reduziert – das sich mit der Ausbreitung von Malware-Websites voraussichtlich verdoppeln wird – und Ablenkungen durch Online-Inhalte werden minimiert. So wird die Produktivität erheblich gesteigert.

Mehrstufiger Schutz vor Bedrohungen durch HuMachine™

Der Next Gen-Malware-Schutz von Kaspersky umfasst mehrere proaktive Sicherheitsebenen, darunter Ebenen auf Basis von Algorithmen für maschinelles Lernen, die von Cloud-basierten Mechanismen unterstützt werden.

Die neuesten Bedrohungen werden mithilfe des **Kaspersky Security Network** schnell und präzise erkannt – es entstehen keine Wartezeiten für Updates, während denen Sie gefährdet sind.

- **Globale Threat Intelligence:** Kaspersky Security for Internet Gateway verwendet global gesammelte Daten, wodurch stets aktuelle Einblicke in die sich stetig wandelnde Bedrohungslandschaft gewährleistet werden können.
- **Lernfähige Systeme:** Die weltweiten Big-Data-Bedrohungsinformationen werden durch die kombinierte Leistung von maschinellen Algorithmen und menschlicher Expertise verarbeitet und ermöglicht so sichere und hohe Erkennungsraten mit minimalen Fehlalarmen.

Ergänzt die Überwachung des Datenverkehrs mit Sicherheitsfunktionen

Die Architektur der Lösung ermöglicht eine einfache Implementierung der Überwachung des Unternehmensdatenverkehrs (auch „SSL-Bumping" genannt). Da SSL-verschlüsselter Webverkehr sich zum De-facto-Standard für die Internetkommunikation entwickelt, ist diese Funktion essentiell.

Skalierbar für Ihr Unternehmen

Kaspersky Security for Internet Gateways ist für Systeme mit hoher Auslastung vollständig skalierbar und erleichtert so die Verwaltung mehrerer Nodes sowie eine hierarchische Verteilung.

Erleichtert die Abwehr von web-basierten Bedrohungen durch flexible Verwaltung und vollständige Transparenz

Kaspersky Security for Internet Gateways bietet ein flexibles und dennoch benutzerfreundliches Verwaltungssystem.

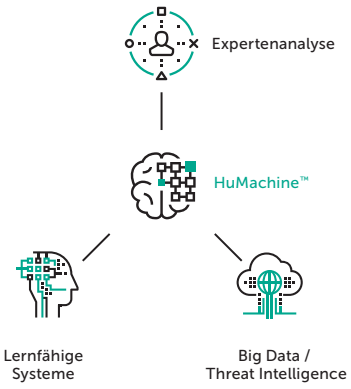
- Über die neue Webkonsole bietet es Ihren Sicherheitsadministratoren vollständige Transparenz und eine flexible Verwaltung.
- Über ein praktisches Dashboard bietet es einen schnellen und effektiven Überblick über Ihre Gateway-Sicherheit, einschließlich der Vorfälle.
- Administratoren können mithilfe eines flexiblen Regelkonfigurationssystems effektive Schutzszenarien für die fein abgestufte Verwaltung der Gateway-Sicherheit einrichten.
- Durch den rollenbasierten Zugriff auf die Verwaltungskonsole werden Fehlerquellen minimiert. Dies ist besonders nützlich für größere Unternehmen mit mehreren Sicherheitsadministratoren, die auf unterschiedlichen Zuständigkeitsebenen tätig sind, ebenso wie für MSPs, die mit mehreren Mandanten arbeiten.
- Die Integration mit Active Directory ermöglicht die Erstellung von Regeln für die Internet-Nutzung basierend auf vorhandenen Benutzer- und Gruppeninformationen.
- Dank der Integration in vorhandene SIEM-Systeme (Security Information Event Management) kann durch Anzeige von Vorfällen auf Gateway-Ebene ein noch klareres Bild der Unternehmenssicherheit erzielt werden.

Ermöglicht die zentrale Verwaltung mehrerer Systeme

Kaspersky Security for Internet Gateways unterstützt mehrmandantenfähige Verwaltungsfunktionen und flexible Lizenzierung und ermöglicht die Delegierung eines entsprechenden Maßes an Kontrolle an die Administratoren der Mandanten. Deshalb ist es ideal für MSPs und Unternehmen mit einem breit gefächerten Portfolio.

Bekämpft fortschrittliche Bedrohungen

Kaspersky Security for Internet Gateway kann in Verbindung mit Kaspersky Anti Targeted Attack eingesetzt werden und erweitert so den Schutz vor komplexen, zielgerichteten Cyberangriffen, die Ihr Unternehmen gefährden.



Ihr Team von Kaspersky

Neues über Cyberbedrohungen: **https://de.securelist.com**
IT Security News: **www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de