Kaspersky®
Security for
Internet Gateway

Securing your first line of defense

In Q2 2018 alone, Kaspersky Lab solutions blocked over 960-million attacks launched from Internet resources located in 187 countries. This is not surprising when you consider how heavily businesses rely on the Internet. But if your business can't get by without the Internet, you can't get by without securing it...

The endpoint is the no. 1 target of attack. It's where web resources are consumed by users and where attackers can influence peoples' actions through clever use of social engineering. The human tendency to click without thinking can undermine even the best endpoint protection. Dealing with an infection before it reaches the user has never been more important...

Highlights

- Real-time anti-malware and anti-phishing protection powered by machine learning
- Blocks ransomware before it enters the corporate network
- Boosts detection rates without generating additional false positives
- Content filtering to block risky files and prevent data leaks
- Web control to govern web resource use
- Secure SSL-encrypted traffic monitoring
- Scalable for high-load networks
- Zero-hour threat protection
- Backed by global threat intelligence from Kaspersky Security Network
- Multitenancy for MSPs and diversified businesses

By stopping 95% of incoming threats at gateway level and preventing them from reaching your endpoints, Kaspersky Security for Internet Gateways significantly reduces their potential impact on users and their workstations. Adding Kaspersky Security for Internet Gateways to your existing protective infrastructure substantially reduces the risk of compromise, ensuring business continuity.

Features and benefits

Blocks incoming malware and ransomware

With multiple overlapping detection layers powered by machine learning, Kaspersky Security for Internet Gateway prevents even advanced malware and ransomware from entering your IT infrastructure and disrupting business-critical processes. The efficiency of Kaspersky Lab's engines is constantly proven by receiving top marks in independent tests.

Helps negate the effects of online phishing

Phishing is used to trick users into believing that a fraudulent resource is legitimate – if the user takes the bait, it may result in loss of personal and even financial data. Kaspersky's advanced, cloud-assisted anti-phishing system uses globally acquired data about malicious and phishing URLs to protect against known and unknown, zero-hour phishing URLs contained in downloaded files.

Helps prevent risky file transmissions

Effective content filtering capabilities reduce the risks of infection and data leaks by filtering all content that moves through the network, based on various parameters set by administrators.

Reduces risks and boosts productivity by governing internet usage

Administrators can configure and create custom rules for web control scenarios to restrict the use of specific types of web resources. This reduces the risk of infection from web resources more likely to double as malware sites and minimizes online distractions – and boosts productivity.

Arms your traffic monitoring with security capabilities

The solution's architecture allows for easy implementation of corporate traffic monitoring (also known as 'SSL bumping'). With SSL-encrypted web traffic becoming the de-facto standard for internet communications, this is an essential feature.

Scales to fit your business

Kaspersky Security for Internet Gateways is fully scalable for high-load systems, facilitating multiple node management and hierarchical deployment.

Makes fighting web-based threats easier with flexible management and full visibility

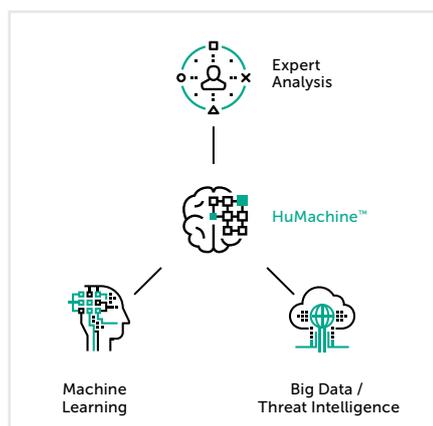Kaspersky Security for Internet Gateways features a flexible yet easy-to-use management system.

- It offers complete visibility and flexible management for your security administrators via the all-new web console.

- It offers a quick and effective overview of your gateway security situation, including events, from a convenient dashboard.

- It enables admin to set up effective protection scenarios using a flexible rules configuration system, for granular management of your gateway security.

- It minimizes administrative error risks by using role-based access to the management console. This is especially useful for bigger businesses with multiple security administrators all with different levels of responsibility, and for MSPs working with multiple serviced tenants.

- Integration with Active Directory enables the creation of web usage rules based on existing user and group information.

- It enriches the corporate security picture with gateway-level events through integration with existing Security Information Event Management (SIEM) systems.

Enables centralized management of multiple systems

Kaspersky Security for Internet Gateways supports multi-tenant management capabilities and flexible licensing, and allows the appropriate degree of control to be delegated to the tenants' administrators. This makes it ideal for MSPs and diversified businesses.

Helps fight advanced threats

Kaspersky Security for Internet Gateway can operate in conjunction with Kaspersky Anti Targeted Attack, adding an extra dimension to protection against the most complex, focused cyberattacks threatening your business.

Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence