Kaspersky® Secure Mail Gateway

An all-in-one secure mailing system to safeguard your communications

Few businesses today could function without email. Having your own mailing system offers numerous benefits and almost endless opportunities for configuration in a way that suits your business processes perfectly. But there are a number of obstacles in the way, the first being price. A Windows-based solution can be prohibitively expensive, especially for small and medium businesses.

Linux-based solutions are free, yet their administration is considerably more complex. And you still need to think about security – email is the number one malware distribution vector today[1].

Kaspersky Secure Mail Gateway is an all-in-one solution that can help you tackle this complexity, offering a pre-built mailing system in the form of an easy-to-deploy appliance – for the price of security alone.

Delivering reliable protection for corporate email from mass and targeted phishing, spam and all forms of malicious attachment (with ransomware and miner Trojans currently demanding particular attention), Kaspersky Secure Mail Gateway is suitable for a wide range of deployment scenarios, on-premise or in the cloud.

Become a master of your business communications while protecting the business from financial, operational and reputational loss with the world's most tested, most awarded email security, conveniently packed for hassle-free deployment.

Highlights

- Real-time and on-demand next-gen anti-malware protection
- Two-way integration with Kaspersky Anti Targeted Attack Platform (KATA)
- Multi-layered protection against Business Email Compromise (BEC)
- Zero-hour threat protection
- Backed by global threat intelligence from Kaspersky Security Network
- Microsoft Active Directory integration
- Quarantine management for emails and attachments
- Takes care of embedded malicious macros and other objects
- Stops email-distributed ransomware and mining Trojans

Benefits

Email is the no.1 attack vector. Block incoming threats with proven multi-layered protection, before someone clicks and lets them in.
Multiple layers of machine learning-powered security, including multi-factor heuristics, sandboxing and reputation system for emails and attachments combine to provide reliable protection against even the most complex mail-based attacks. Stopping these attacks before they can exploit your users' naivety or curiosity dramatically boosts corporate security levels.

Over half of all emails sent are spam. Increase productivity and reduce threats with cloud-assisted, next-generation spam protection.
Kaspersky Lab's cloud-assisted, next-generation anti-spam detects even the most sophisticated, unknown spam with minimal loss of valuable communication due to false positives. Reducing the time, resources and risks associated with spam by stopping it in its tracks saves system and human resources.

[1] Verizon Data Breach Investigations Report 2017.

Saves valuable man-hours

Conveniently packaged into a ready-to-use appliance, Kaspersky Secure Mail Gateway offers an easy start for your new, now-secure corporate mailing service, freeing up loads of IT staff time for other tasks. Its flexible filtering configuration scenarios ensure a great fit with your business processes, reducing management resources.

Reduces cost of ownership

Besides saving IT staff time, Kaspersky Secure Mail Gateway saves even more by embracing all the benefits of virtualization. The appliance is suitable for deployment with the whole range of the most popular hypervisors, which makes this particular element of your corporate infrastructure less resource-hungry and, at the same time, more flexible, adding to manageability and fault tolerance. Even more, it is available as a workload image in Microsoft Azure marketplace, helping to enable security for your cloud-based mail - at warp speed - without compromising on either protection or management granularity.

Features

HuMachine™-powered, multi-layered malware protection

Kaspersky's next-generation malware protection incorporates multiple proactive security layers, including machine learning and cloud-assisted threat intelligence, to filter out malicious attachments, known and previously unknown malware in incoming mail. Real-time and on-demand scanning are available – the latter is especially useful in migration scenarios.

Global threat intelligence: Kaspersky Secure Mail Gateway's protection utilizes globally acquired data for the latest view of the threat landscape, even as it evolves.

Machine learning: The big data of global threat intelligence is processed by the combined power of machine learning algorithms and human expertise, delivering proven high detection levels with minimal false positives.

Emulative sandboxing

To protect against even the most sophisticated, heavily obfuscated malware, attachments are executed in a safe emulated environment where they are analyzed to ensure dangerous samples aren't let through into the corporate system.

Integration with Kaspersky Security Network / Kaspersky Private Security Network

Having the most up-to-date threat intelligence is key to prompt blocking of emerging types of spam, phishing and malware. Participation in Kaspersky Security Network allows the solution to receive the most up-to-date threat intelligence, processed from globally acquired data using the Kaspersky HuMachine™ framework. For the most privacy-aware organizations, integration with Kaspersky Private Security Network is also available.

Script detection

According to cybersecurity analysts, scripts are increasingly being used for both all kinds of mail-based attacks, including embedding malware into seemingly harmless office files. Kaspersky Secure Mail Gateway deals with script-based threats, including office macros, therefore preventing the execution of deadly malware even before it reaches the recipient.

Archive scanning

Archiving malicious attachments is a common technique used by malware creators. Kaspersky engines can reach into even multi-layered archives to ensure the threat wouldn't evade detection.

Ready-to-use secure mailing system

All-in-one appliance

Everything required for a complete secure mailing system (including Linux OS, Mal Transfer Agent (MTA), Kaspersky Security for Linux Mail Server etc.) is already included into Kaspersky Secure Mail Gateway, with all its components pre-configured to work seamlessly with each other and requiring only minimum additional configuration from the security administrators.

Virtualization platforms support

Kaspersky Secure Mail Gateway is available as a virtual appliance for the most popular virtualization platforms, downloadable as an .OVA or .ISO image and deployed as a public cloud workload. Microsoft Azure users may find it even more convenient to use the image offered in the Azure marketplace.

Robotized spam protection

Next-generation anti-spam system (with content reputation)

Kaspersky's anti-spam system extensively leverages machine learning-based detection models. To minimize the possibility of false positives and adapt to changes in the threat landscape, robotic spam processing is supervised by Kaspersky Lab experts, part of the Kaspersky HuMachine framework. It also utilizes reputation data from Kaspersky Security Network to ensure precise detection of new spam variations immediately after they hit the internet.

Kaspersky Humachine™ Approach

Powered by Big Data threat intelligence, robotic machine learning capabilities and the experience of human experts, Kaspersky HuMachine™ provides multiple benefits and delivers more efficient protection. By combining each element, individual components are enhanced into an even more efficient, effective whole.

Anti-spam quarantine

To ensure no valuable correspondence is lost, an anti-spam quarantine storage is available. The administrator can configure the criteria for quarantining emails and for how long they should be stored; anything of value can be retrieved and forwarded to recipients in its original, intact state.

Advanced anti-phishing

Kaspersky Lab's advanced anti-phishing system is based on Neural Networks analysis for effective detection models. With over 1000 criteria used – including pictures, language checks, specific scripting – this cloud-assisted approach is supported by globally acquired data about malicious and phishing URLs to provide protection from both known and unknown/zero-hour phishing emails.

Authenticated email management

Reliable sender authentication mechanisms such as SPF/DKIM/DMARC help protect against source spoofing. This is especially useful for countering Business Email Compromise (BEC) scenarios.

Specialized business email compromise (BEC) detection

A dedicated heuristic model processes a number of indirect indicators, enabling the system to block even the most convincing fake emails. Given the acuteness of this issue today, detection models are regularly reviewed, and new scenarios added.

Attachment filtering

Some types of attachment are too risky to be let inside the corporate security perimeter. Kaspersky's attachment filtering system allows for the flexible configuration of an attachment delivery policy, and detects multiple types of file disguise commonly used by cybercriminals. These features help reduce the probability of data leaks.

Email categories

Support for a number of pre-configured email categories makes communications filtering easier, again helping to simplify dealing with everyday mail streams and reducing your security risk.

Management and visibility

Convenient web console
An easy-to-use web-based interface enables the administrator to monitor the state of corporate mail security and configure its rules and policies. Separate sets of policies can be configured for each of the managed domains.

SIEM integration
Support for Common Event Format (CEF) allows the export of mail security event information into your corporate SIEM system, tracking email security alerts as part of the whole organization's security context.

Flexible rules configuration system: Finely tuned security policies are key to the solution's effectiveness, configured to be consistent with existing business processes. Kaspersky Secure Mail Gateway offers a flexible yet easy-to-use rules configuration system, which allows for the granular management of your email security while ensuring your administrators don't have to spend too much time learning it.

Role-based access system: Administrators can define a role to restrict administration rights for different administrator categories. This is useful for internal task delegation or for providing the necessary degree of control for serviced clients for Managed Service Providers (MSPs).

Active Directory integration: Kaspersky Secure Mail Gateway can obtain information on corporate domain entities (users, user groups, computers, etc.) to configure its Role-Based Access rules and security policies around known objects operating in a company's IT network. The data describing the objects is constantly synchronized between the Active Directory and the application itself to ensure consistency with the most recent changes in corporate infrastructure.

System health diagnostics
With email being one of the mission-critical services for any business, ensuring its security system's uninterrupted operation is essential. Besides convenient dashboards available in the web console, Kaspersky Secure Mail Gateway integrates with Kaspersky Security Center, providing real-time information about the state of the product's components. In addition, a package of diagnostic data can be generated and sent to Kaspersky Lab's technical support, who will then have the necessary information for effective resolution of the issue in question.

Built-in backup

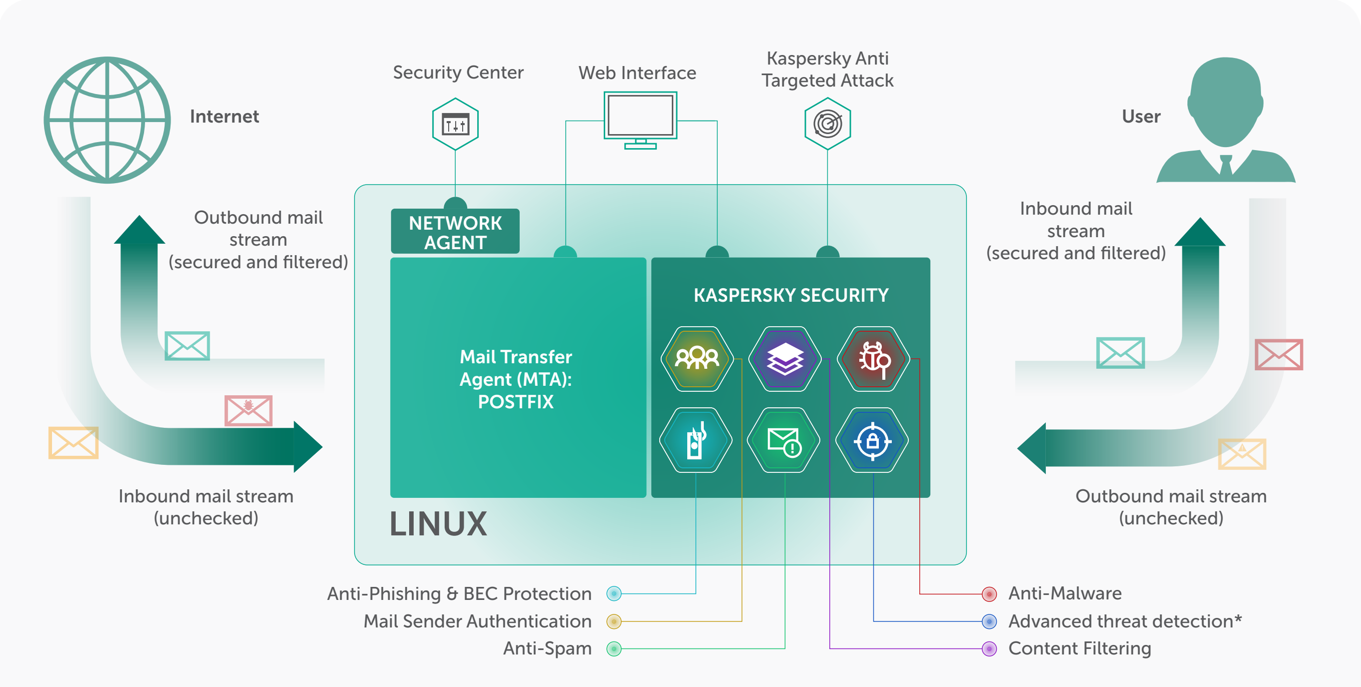
To ensure that no critical data is lost due to disinfection or deletion, original messages can be saved onto backup storage to be processed by the administrator when convenient. Specific rules can be configured for conditional data backup.

Kaspersky Anti-Targeted Attack integration

Two-way integration with Kaspersky's advanced threat detection platform not only enables the use of mail systems as an additional source of information for targeted attack detection, but also, based on the results of deep analysis, can block further messages containing dangerous content. A special quarantine is available to deal with those especially sophisticated malicious emails detected by Kaspersky Anti-Targeted Attack mechanisms.

HOW TO BUY

Kaspersky Secure Mail Gateway is available on an annual license or monthly subscription basis. It can be purchased separately under a Kaspersky Security for Mail Server license, or as a part of Kaspersky Total Security for Business. To help you choose the most suitable product for your business, please consult a Kaspersky reseller or authorized distributor.


Internet
Security Center
Web Interface
Kaspersky Anti Targeted Attack
User
Outbound mail stream (secured and filtered)
Inbound mail stream (secured and filtered)
NETWORK AGENT
Mail Transfer Agent (MTA): POSTFIX
KASPERSKY SECURITY
LINUX
Inbound mail stream (unchecked)
Outbound mail stream (unchecked)
Anti-Phishing & BEC Protection
Mail Sender Authentication
Anti-Spam
Anti-Malware
Advanced threat detection*
Content Filtering

*With Kaspersky Anti Targeted Attack

System requirements

Hardware or virtual equivalent to deploy and run the appliance[2]:

- 4-Core CPU
- 4 GB RAM
- 100+ GB of disk space
- Intel E1000 family network adapter

Supported hypervisors

- VMware ESXi 5.5 Update 2
- VMware ESXi 6.0, 6.5, 6.7
- Microsoft Hyper-V Server 2012 R2

Browsers for the web console:

- Mozilla Firefox version 49 and above
- Internet Explorer version 11 and above
- Google Chrome version 61 and above

[2] These minimum requirements ensure the throughput of up to 10 messages/sec, with average message size about 50kb. For bigger throughput, it’s recommended that you either allocate more resources for your virtual machine, or run more VMs and configure load balancing between them.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com