kaspersky BRING ON THE FUTURE

Kaspersky Secure Mail Gateway

Defending your perimeter and safeguarding your communications

Email remains the primary attack vector for the vast majority of cyberattacks, and nearly all email-borne threats use social engineering to gain the recipient's trust and make them do something they shouldn't do, but which the attacker needs.

Kaspersky Secure Mail Gateway is an all-in-one SEG (Secure Email Gateway) which identifies and blocks harmful emails from reaching their primary targets – users – and preventing infections and data leaks, while saving on the resources required to bounce off unwanted emails.

Kaspersky Secure Mail Gateway Highlights

- Real-time advanced anti-malware protection
- Deep integration with Kaspersky Anti Targeted Attack Platform
- Multi-layered protection against Business Email Compromise (BEC)
- Zero-hour threat protection
- Backed by global threat intelligence from Kaspersky Security Network or Kaspersky Private Security Network
- Microsoft Active Directory integration
- Role-based Access Control
- Takes care of embedded malicious macros and other objects
- Stops email-distributed ransomware and mining Trojans
- Flexible scaling according to load and organization size
- Quarantine management for emails and attachments across all cluster nodes
- Clustered architecture to tackle growing email traffic loads

Block email threats before they reach their target

Kaspersky Secure Mail Gateway provides reliable protection against phishing, business email compromise, ransomware and even advanced email based threats. Applying effective countermeasures this early in the killchain, before threats have become incidents and well before any damage can be done, reduces your risk as well as the workload on your hard-pressed team. Using data science applied through layers of machine learning-powered security, including ML models, sandboxing and our cloud-assisted reputation system, we let all the right stuff in, while keeping the wrong stuff out.

Increase productivity by doing away with spam

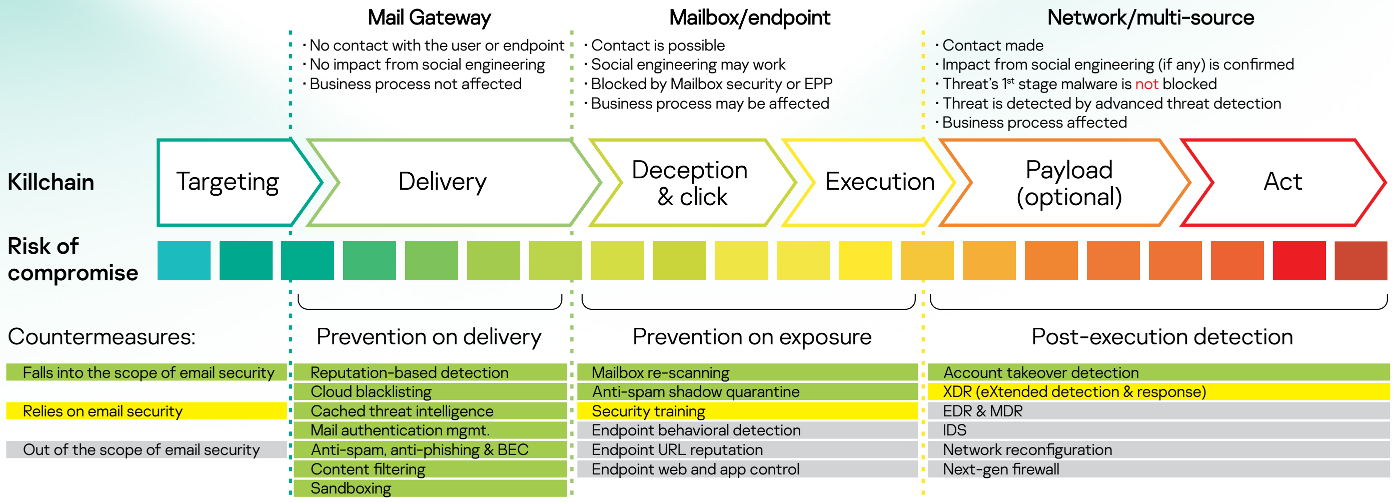
Our cloud-assisted, machine-learning based anti-spam technology detects even the most sophisticated, unknown spam with minimal loss of valuable communication due to false positives. Reducing the time, resources and risks associated with spam by stopping it in its tracks saves system resources as well as time.

Enhance your protection with minimum hassle

Whether you're looking to add a SEG solution to your existing email infrastructure, or boost the performance of your current installation, you'll find installing and configuring our pre-built mailing system in the form of an easy-to-deploy appliance remarkably straightforward.

Let your security grow with you

The scalable clustered architecture of Kaspersky Secure Mail Gateway means it can grow together with your business, so you can continue benefitting from solid email traffic protection without compromising on performance.



Mail Gateway
- No contact with the user or endpoint
- No impact from social engineering
- Business process not affected

Mailbox/endpoint
- Contact is possible
- Social engineering may work
- Blocked by Mailbox security or EPP
- Business process may be affected

Network/multi-source
- Contact made
- Impact from social engineering (if any) is confirmed
- Threat's 1st stage malware is not blocked
- Threat is detected by advanced threat detection
- Business process affected

Killchain: Targeting → Delivery → Deception & click → Execution → Payload (optional) → Act

Risk of compromise

Countermeasures:

🟩 Falls into the scope of email security

🟨 Relies on email security

⬜ Out of the scope of email security

Prevention on delivery
- Reputation-based detection
- Cloud blacklisting
- Cached threat intelligence
- Mail authentication mgmt.
- Anti-spam, anti-phishing & BEC
- Content filtering
- Sandboxing

Prevention on exposure
- Mailbox re-scanning
- Anti-spam shadow quarantine
- Security training
- Endpoint behavioral detection
- Endpoint URL reputation
- Endpoint web and app control

Post-execution detection
- Account takeover detection
- XDR (eXtended detection & response)
- EDR & MDR
- IDS
- Network reconfiguration
- Next-gen firewall

The role of Mail Security at different stages of the cyberattack killchain

Key features

Multi-layered anti-malware protection

Kaspersky's advanced anti-malware protection incorporates multiple proactive security layers, including machine learning and cloud-assisted threat intelligence, to filter out malicious attachments, and known and previously unknown malware in incoming mail.

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 and behavioral sandboxing: To protect against even the most sophisticated, heavily obfuscated malware, attachments are executed in a safe emulated environment where they're analyzed to ensure that dangerous samples can't get through into your corporate system.

Kaspersky Security Network / Private Security Network: Having the most up-to-date threat intelligence is key to blocking emerging types of spam, phishing and malware promptly. Participation in Kaspersky Security Network means your security solution receives the most up-to-date threat intelligence, distilled from globally acquired detection telemetry, insights from expert threat research, information exchange partnerships, and more. For the most privacy-aware organizations, integration with Kaspersky Private Security Network allows users to benefit from the incoming threat data stream without a single bit of data moving out of the infrastructure.

Script detection: According to cybersecurity analysts, scripts are increasingly used for 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, preventing the execution of deadly malware 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 no threat can evade detection.

Rooted in globally renowned expertise

Kaspersky experts are recognized worldwide for their extensive experience with novel threats and groundbreaking discoveries. These Include criminal and nation-state sponsored campaigns like Carbanak and Stuxnet, Duqu and Equation, Lazarus and MosaicRegressor. Most use tools carried by email, and these tools are meticulously dissected and analyzed by our experts. The results of this work are fundamental to advancing Kaspersky's detection technologies. These technologies undergo both regular rigorous internal and external, independent testing – and we consistently out-perform our competitors.

See **https://www.kaspersky.com/top3**

Ready-to-use

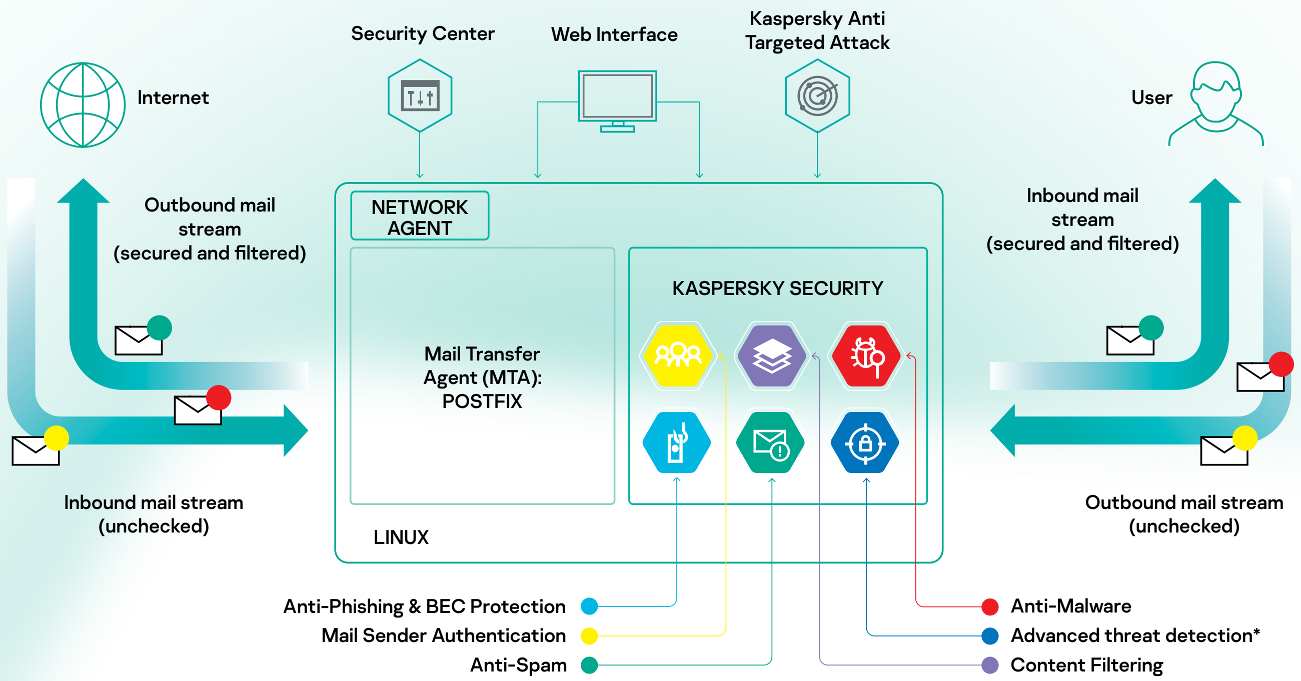
All-in-one appliance: Everything required for a complete secure mailing system (including Linux OS, Mal Transfer Agent (MTA), Kaspersky security application, etc.) is included in Kaspersky Secure Mail Gateway, with all its components pre-configured to work seamlessly with each other and requiring only a few additional configuration steps from your 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.

Spam protection (without losing any good stuff)

Next-generation anti-spam system (with content reputation-based filtering): Kaspersky's anti-spam system makes extensive use of machine learning-based detection models. To minimize false positives and adapt to changes in the threat landscape, automated spam processing is supervised by Kaspersky experts. It also utilizes reputation data from Kaspersky Security Network to ensure the accurate detection of new spam variations as soon as they hit the internet.

Anti-spam quarantine: Anti-spam quarantine storage is available to ensure that no important emails are lost. You administrator can configure the criteria for quarantining emails and the length of time they should be stored – anything of value can be retrieved and forwarded to recipients in its original state.


Security Center
Web Interface
Kaspersky Anti Targeted Attack
Internet
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

[1]Cousin domains

Using a 'cousin' or lookalike domain name is typical of "From" field spoofing. A specially registered domain that looks as similar as possible to a legitimate, trusted one is used. Symbols from the UNICODE typeset can be swapped with those that look very close to the originals. Third-level domain names – kaspersky.xxx.com, for example – can also be used, abusing peoples' trust in popular brand names or business partners.

[2]Mailsploit

'Mailsploit' is a collection of exploits for vulnerabilities identified in specific aspects of popular emailing clients and OSs which can be used to spoof and manipulate the sender's address in the "From" field.

Email client vendors were informed about the vulnerabilities, but not all of them fixed their software, claiming that some of these apparent vulnerabilities were features rather than deficiencies, and that the issues identified should be addressed at the gateway level.

The researcher who assembled the Mailsploit collection eventually opened the source code to the broader public and, not unexpectedly, Mailsploit have become part of the arsenal that spammers and hackers use against unpatched and unprotected systems.

Advanced anti-phishing

Kaspersky'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.

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 seriousness of this issue today, detection models are regularly reviewed, and new scenarios added. Among the notable BEC types that the solution detects are those involving cousin[1] domain usage, a takeover of a legitimate account, the use of the Mailsploit[2] kit and others.

Authenticated email management

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

Email categories

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

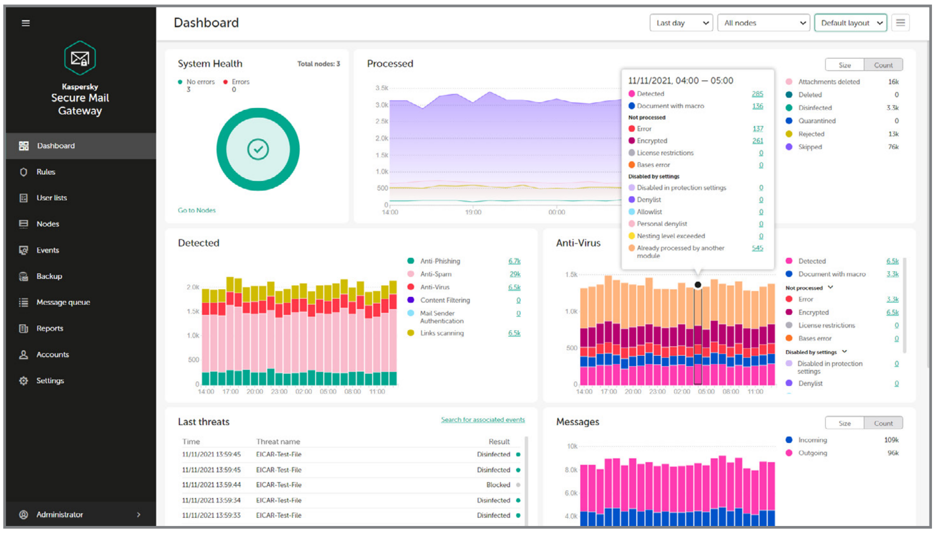
Spear-phishing as a technique of choice

One of the most prolific and sophisticated APT actors, Sofacy (aka APT28 or Fancy Bear), is known for using spear-phishing & BEC in its attacks, employing the widest variety of phishing scenarios – from shortened URLs leading to credential-harvesting websites to zero-day exploits embedded in attached Office documents.

Source: Securelist

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 disguises commonly used by cybercriminals. These features help reduce data leaks.



Dashboard

System Health — Total nodes: 3

No errors	Errors
3	0

Processed

11/11/2021, 04:00 — 05:00

Detected	285
Document with macro	136
Not processed	
Error	137
Encrypted	261
License restrictions	0
Bases error	0
Disabled by settings	
Disabled in protection settings	0
Denylist	0
Allowlist	0
Personal denylist	0
Nesting level exceeded	0
Already processed by another module	545

Attachments deleted	16k
Deleted	0
Disinfected	3.3k
Quarantined	0
Rejected	13k
Skipped	76k

Detected

Anti-Phishing	6.7k
Anti-Spam	29k
Anti-Virus	6.5k
Content Filtering	0
Mail Sender Authentication	0
Links scanning	6.5k

Anti-Virus

Detected	6.5k
Document with macro	3.3k
Not processed	
Error	3.3k
Encrypted	6.5k
License restrictions	0
Bases error	0
Disabled by settings	
Disabled in protection settings	0
Denylist	0

Last threats

Time	Threat name	Result
11/11/2021 13:59:45	EICAR-Test-File	Disinfected ●
11/11/2021 13:59:45	EICAR-Test-File	Disinfected ●
11/11/2021 13:59:44	EICAR-Test-File	Blocked ●
11/11/2021 13:59:34	EICAR-Test-File	Disinfected ●
11/11/2021 13:59:33	EICAR-Test-File	Disinfected ●

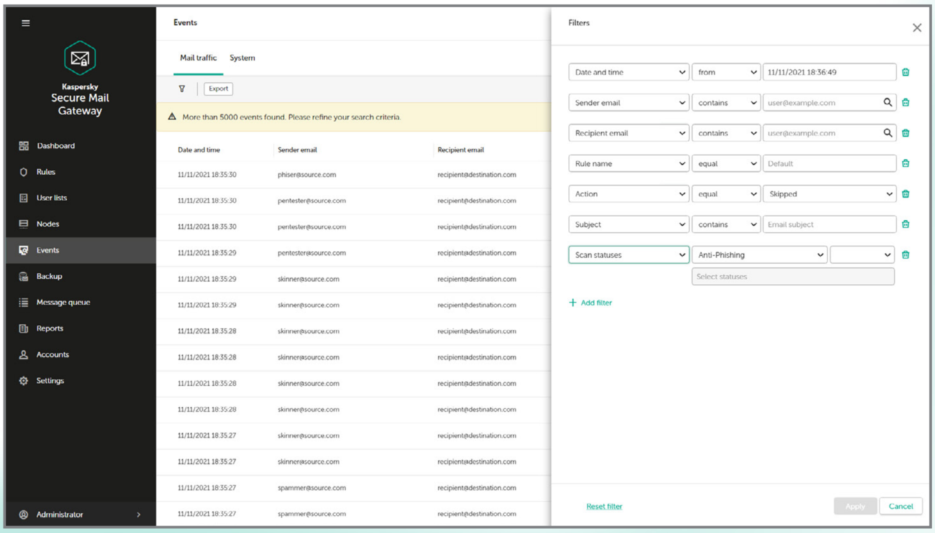
Messages

Incoming	109k
Outgoing	96k

Management and visibility

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

Versatile event management: The event viewer displays the exact information your security administrator needs. This is made possible by creating the criteria of any level of complexity, using logical (Boolean) operators to specify what's needed.



Events

⚠ More than 5000 events found. Please refine your search criteria.

Date and time	Sender email	Recipient email
11/11/2021 18:35:30	phiser@source.com	recipient@destination.com
11/11/2021 18:35:30	pentester@source.com	recipient@destination.com
11/11/2021 18:35:30	pentester@source.com	recipient@destination.com
11/11/2021 18:35:29	pentester@source.com	recipient@destination.com
11/11/2021 18:35:29	skinner@source.com	recipient@destination.com
11/11/2021 18:35:29	skinner@source.com	recipient@destination.com
11/11/2021 18:35:28	skinner@source.com	recipient@destination.com
11/11/2021 18:35:28	skinner@source.com	recipient@destination.com
11/11/2021 18:35:28	skinner@source.com	recipient@destination.com
11/11/2021 18:35:28	skinner@source.com	recipient@destination.com
11/11/2021 18:35:27	skinner@source.com	recipient@destination.com
11/11/2021 18:35:27	skinner@source.com	recipient@destination.com
11/11/2021 18:35:27	spammer@source.com	recipient@destination.com
11/11/2021 18:35:27	spammer@source.com	recipient@destination.com

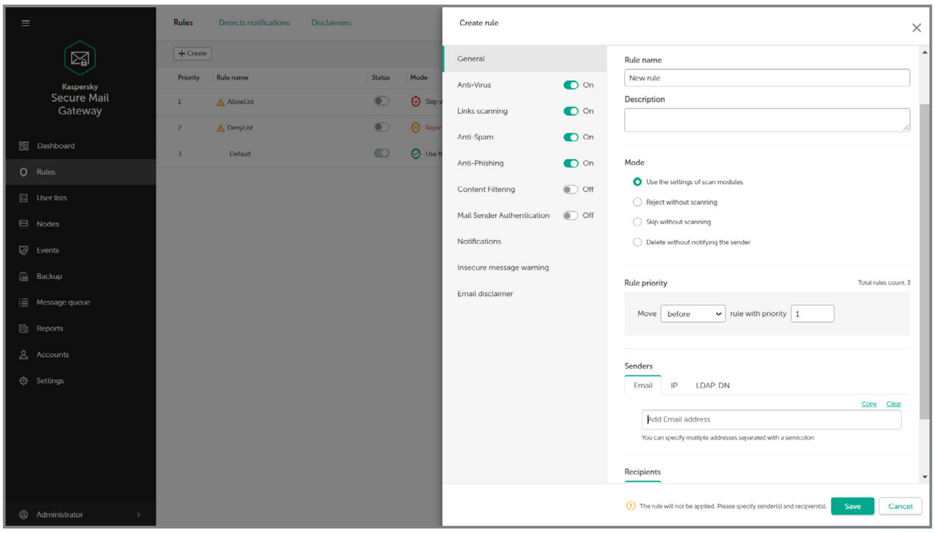
Filters

Date and time	from	11/11/2021 18:36:49
Sender email	contains	user@example.com
Recipient email	contains	user@example.com
Rule name	equal	Default
Action	equal	Skipped
Subject	contains	Email subject
Scan statuses	Anti-Phishing	
	Select statuses	

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 your overall security context.

Role-based access system: Roles can bedefined to restrict administration rights for different administrator categories. This is useful for internal task delegation and, if you're a Managed Service provide (MSP) this provides a crucial degree of control for your serviced clients.

Flexible rule configuration system: Finely tuned security policies are key to the solution's effectiveness, configured to be consistent with your 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.



Priority	Rule name	Status	Mode
1	AllowList		Skip w
2	DenyList		Rejec
3	Default		Use th

General

Anti-Virus On

Links scanning On

Anti-Spam On

Anti-Phishing On

Content Filtering Off

Mail Sender Authentication Off

Notifications

Insecure message warning

Email disclaimer

Rule name: New rule

Description

Mode

● Use the settings of scan modules
○ Reject without scanning
○ Skip without scanning
○ Delete without notifying the sender

Rule priority — Total rules count: 3

Move before rule with priority 1

Senders

Email IP LDAP: DN

Copy Clear

Add Email address

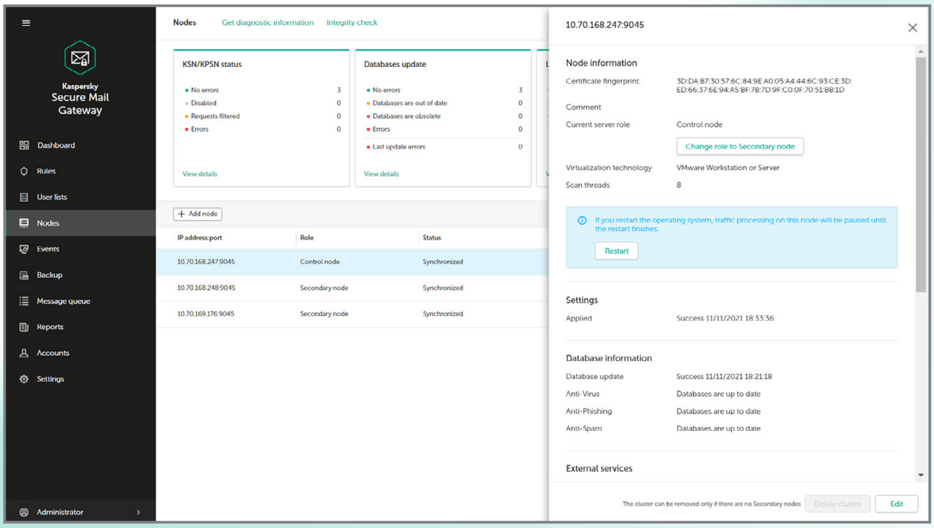
You can specify multiple addresses separated with a semicolon

Recipients

The rule will not be applied. Please specify sender(s) and recipient(s).

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 your 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 your corporate infrastructure.

Clustered architecture: To tackle changing conditions in your emailing infrastructure functioning – such as business growth and increases in traffic intensity – the solution has been designed with a clustered architecture which can be resized according to changing traffic loads.



KSN/KPSN status	
No errors	3
Disabled	0
Requests filtered	0
Errors	0

Databases update	
No errors	3
Databases are out of date	0
Databases are obsolete	0
Errors	0
Last update errors	0

IP address:port	Role	Status
10.70.168.247:9045	Control node	Synchronized
10.70.168.248:9045	Secondary node	Synchronized
10.70.169.176:9045	Secondary node	Synchronized

10.70.168.247:9045

Node information

Certificate fingerprint:	3D:DA:B7:30:57:6C:84:9E:A0:05:A4:44:6C:93:CE:3D: ED:66:37:6E:94:A5:BF:7B:7D:9F:C0:0F:70:51:BB:1D
Comment	
Current server role	Control node
Virtualization technology	VMware Workstation or Server
Scan threads	8

If you restart the operating system, traffic processing on this node will be paused until the restart finishes.

Settings

Applied	Success 11/11/2021 18:33:36

Database information

Database update	Success 11/11/2021 18:21:18
Anti-Virus	Databases are up to date
Anti-Phishing	Databases are up to date
Anti-Spam	Databases are up to date

External services

The cluster can be removed only if there are no Secondary nodes

Kaspersky Anti-Targeted Attack integration

Two-way integration with Kaspersky's advanced threat detection platform enables the use of mail systems as an additional source of information for targeted attack detection and, depending on the results of deep analysis, can also block further messages containing dangerous content. A special quarantine is available to deal with those particularly sophisticated malicious emails detected by Kaspersky Anti Targeted Attack mechanisms.

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. Backup is managed centrally from the administration console.

Features list and system requirements

Detection of malicious objects

- Multi-layered anti-malware combining precise detection and machine learning models to detect unknown threats
- File, URL and IP address reputation system
- Script detection
- File type recognition (sees the real attached file type despite disguises)
- Detection of encrypted objects
- Archives filtering and analysis
- APT-grade attack elements detection blocking using Kaspersky Anti Targeted Attack integration

Anti-spam technologies

- Intelligent spam detection – leverages both on-prem and cloud-running machine learning (ML) models
- Reputation-based spam filtering
- Anti-spam shadow quarantine -briefly withholds emails yielding low-confidence detection to receive clarification from the cloud infrastructure.
- Enforced Anti-Spam Updates Service (EASUS) – pushes critical information about spam waves
- Snowshoe spam detection
- Spoofed domains detection
- Protection against Unicode spoofing
- Emails categorization
- Detection of mass mailings (including marketing mail-outs)
- OCR-based spam detection – detects spams using graphic elements with drawn text

Visibility and Manageability

- Web-based management console
- Configurable dashboard – displays everything the administrator needs
- Role-based access control system
- SSO (Single Sign-on) support for Active Directory users
- Clustered architecture
- Unified email backup system
- User's personal email backups
- User's personal allow/deny lists
- User backup digest, with sending scheduling
- Event viewer with filters and Boolean searches
- Notification system, with customizable templates
- Configurable disclaimers – can be added to outgoing in ingoing emails
- CLI (command line interface) – based management
- Reporting system
- Flexible email processing rules
- Configurable updating timetable

Hardware requirements

We recommend that 1 VM instance (cluster node) is allocated not less than the following resources:

- 8 processor cores 16 GB of RAM 200 GB of disk space

DLP-like functionality (advanced content filtering)

- Attachment filtering (based on multiple criteria)
- True format recognizer – see through file type disguises and apply content filtering rules

Cloud-based intelligence support

- Kaspersky Security Network (GDPR & the like compliant)
- Kaspersky Private Security Network (cloud intel with no data shared)
- Anti-phishing technologies
- Multi-factor, ML-assisted anti-phishing system
- Specialized business email compromise (BEC) protection
- Authenticity of senders checking – SPF/DKIM/DMARC support
- Cousin (lookalike) domain detection
- Sender source IP reputation
- Mailsploit usage detection

Integrations

- Active Directory Integration
- SIEM integration
- Log collector
- Existing email gateway integration
- Kaspersky Anti-Targeted Attack integration

Licensing

- Based on either the number of mailboxes, the volume of traffic, or, if used inside Kaspersky Total Security for Business, on the number of protected nodes multiplied by a factor 1.5

Software requirements

The virtual machine image can be deployed on the following hypervisors:

- VMware ESXi 6.7 Update 3b.
- VMware ESXi 7.0 Update 1.
- Microsoft Hyper-V Server 2016 (Generation 1 only).
- Microsoft Hyper-V Server 2019

To run the web interface, one of the following web browsers must be installed on the computer:

- Mozilla Firefox version 82.
- Internet Explorer version 11.
- Google Chrome version 86.
- Microsoft Edge version 86.

Software requirements for configuring integration with an LDAP server:

- Windows Server 2012 R2 Standard.
- Windows Server 2016 Standard.
- Windows Server 2019 Standard.

How to buy

Kaspersky Secure Mail Gateway is available on an annual license or a 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.

Try Before Buying

Try Kaspersky Security for Embedded Systems now with our free 30-day trial.

Request a Call

Still need more information? We'd be delighted to give you a call – just ask!

Buy From a Trusted Partner

Feel like you're ready to buy? Find a reseller in your region.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Kaspersky technologies: kaspersky.com/technowiki
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.