kaspersky BRING ON THE FUTURE

Kaspersky Security for Mail Server

Building resilience against the number one attack vector

Email is the primary attack vector threatening business IT security. Attackers have increasingly sophisticated ways to infiltrate organizations through mail-based attacks, resulting in financial, operational and reputational losses. To counter these developments, businesses need to think about resilience as well as protection.
By optimizing your resilience and minimizing your attack surface, you can make your business a less attractive and even unfeasible target for attackers – regardless of whether your company operates an on-prem, cloud or hybrid emailing infrastructure.

Primary vector for data breaches

- According to Verizon's Data Breach Investigation Report (DBIR), Social Engineering is the most common pattern resulting in a data breach.
- The report also states that "...phishing remains one of the top Action varieties in breaches and has done so for the past two years"

Source: Verizon Data Breach Investigation Report

Build up your resilience at the number one entry point for attacks

Kaspersky Security for Mail Server applications help build resilience to mail-based attacks by:

Identifying and filtering out suspicious or unwanted mail at gateway level

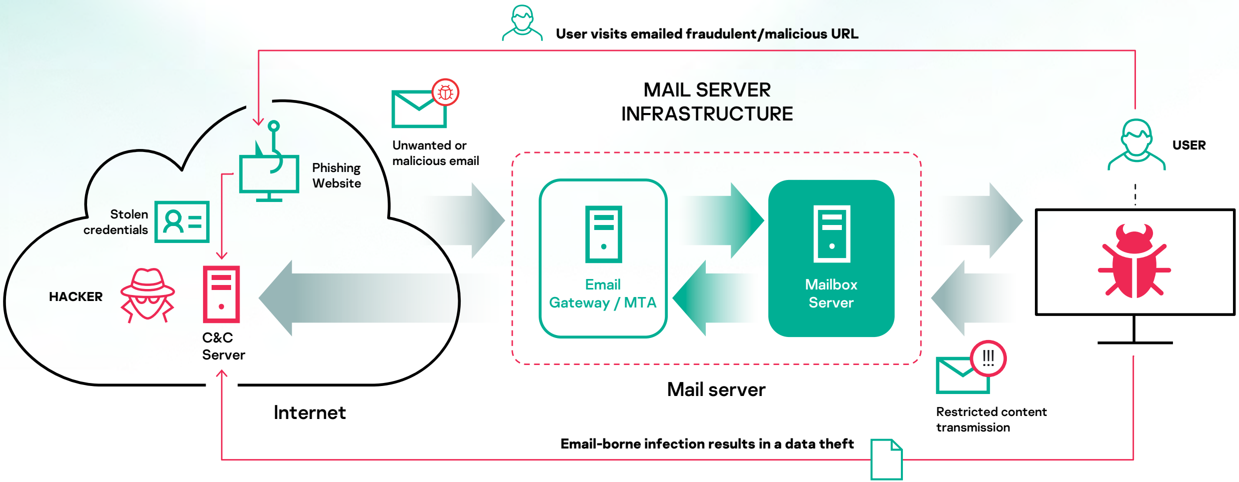
Most mail attacks only begin to activate at endpoint level – Kaspersky Security for Mail Server sets out to stop them long before they get that far. Our award-winning protection strengthens your resilience by detecting and intercepting attacks right at the beginning of the killchain, before they can breach your perimeter and head for your endpoints and users.

Swiftly and accurately processing legitimate emails

The core role that email plays in business communications means that security processing has to be fast, agile and accurate – without impeding legitimate communications. Kaspersky Security for Mail Server offers the most effective protection technologies in the industry against everything from phishing emails and spam to Business Email Compromise (BEC) attacks and ransomware, with near-zero false positives, enabling legitimate emails to travel uninterrupted.

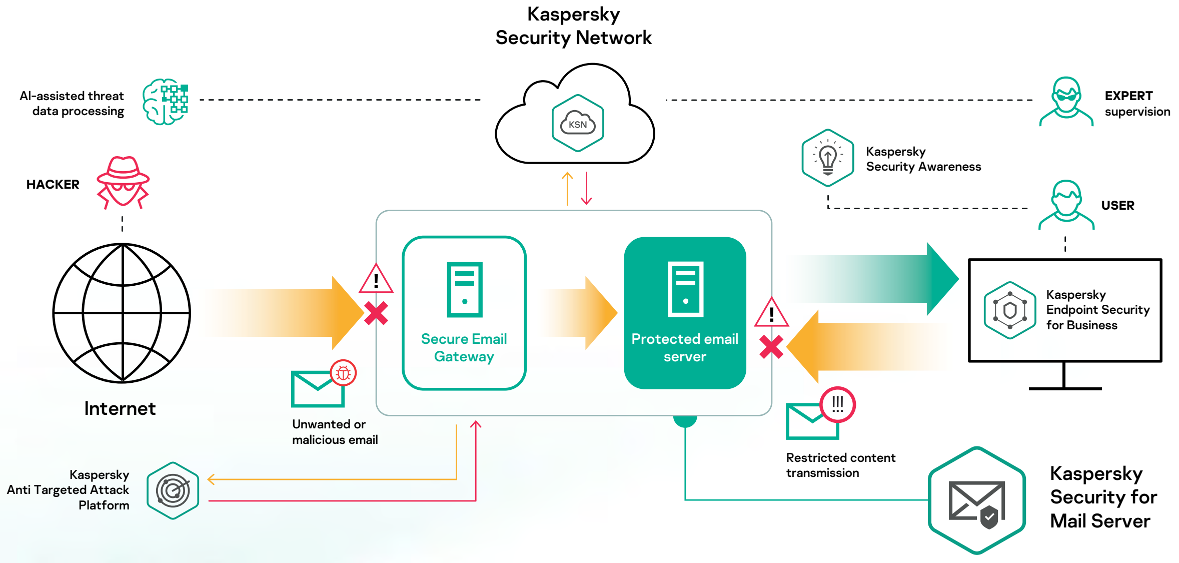
Protecting email beyond the gateway

Kaspersky Security for Mail Server detects malicious or undesirable content not only at the gateway, but also at the level of individual Microsoft Exchange Server mailboxes – or/and Microsoft Exchange Online. Delayed phishing attacks designed to evade gateway level countermeasures, BEC messages generated after account takeovers, and insider threat scenarios that need never pass through the gateway – all these can be identified and eradicated, making server mailbox protection a 'must-have'.


User visits emailed fraudulent/malicious URL
MAIL SERVER INFRASTRUCTURE
Unwanted or malicious email
Phishing Website
Stolen credentials
HACKER
C&C Server
Email Gateway / MTA
Mailbox Server
USER
!!!
Restricted content transmission
Mail server
Internet
Email-borne infection results in a data theft

The email-based threat model

Key features



Kaspersky Security Network
KSN
AI-assisted threat data processing
EXPERT supervision
HACKER
Kaspersky Security Awareness
USER
Internet
Secure Email Gateway
Protected email server
Kaspersky Endpoint Security for Business
Unwanted or malicious email
Restricted content transmission
Kaspersky Anti Targeted Attack Platform
Kaspersky Security for Mail Server

How Kaspersky Security for Mail Server counters email-borne cyberthreats

Multi-layered malware protection

Multiple security layers are capable of stopping the most complex email-borne malware – including spyware, wipers, miners and ransomware- all of which are often spearheaded by targeted phishing. Reputational data from the cloud, precise detection, cloud and on-prem machine learning models, globally acquired threat intelligence and exclusive research data combine to ensure one of the best detection-to-false-positives ratios in the industry.

Breadth of scenarios: one license for all

A single product license covers a unique variety of scenarios – including boosting the protection of your pre-existing emailing infrastructure or building a new, secure one. A range of emailing architectures encompassing Linux- or Windows-based, comprising on-prem, virtualized, cloud or a combination of these, it is all covered in a single Kaspersky product

Automated anti-spam (with content and source address reputation)

Kaspersky's anti-spam system uses smart engines to minimize the possibility of false positives as they continuously adapt to changes in the spammers' techniques. Globally collected reputation data is processed in the cloud and used to feed AI aspects, providing a solid basis for efficient spam detection.

Countering Business Email Compromise (BEC)

A dedicated machine learning-based detection system, with algorithmic models updated regularly with new scenarios, processes a number of indirect indicators, enabling the system to block even the most convincing fake emails. Support for sender authentication mechanisms such as SPF / DKIM / DMARC helps protect against source spoofing – especially helpful for withstanding Business Email Compromise (BEC) scenarios.

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 aren't let through into the corporate system. For Kaspersky Anti Targeted Attack users, integration adds "detonation" in a lifelike external advanced sandbox environment– providing much deeper levels of assessment and dynamic analysis.

Advanced anti-phishing

Kaspersky's advanced anti-phishing system uses Neural Network based analysis to create effective detection models. With over 1,000 criteria used – including pictures, language checks, specific scripting – this cloud-assisted approach is supported by globally acquired data about malicious and phishing URLs and IP addresses to provide protection from both known and unknown/zero-hour phishing emails.

Blocking unsafe content transfers

Kaspersky's configurable attachment filtering system can detect file disguises commonly used by cybercriminals, identifying potentially dangerous attachments. DLP-like functionality allows the administrator to configure complex rules for preventing data leakage, armed with the power of Regular Expressions and benefitting from a plethora of best practices accumulated by the community.

Beyond the gateway – mailbox-level resilience

Mailbox-level technologies include:

Email rescanning – addressing scenarios like delayed phishing URL activation.

Anti-spam shadow quarantine – ideal for low-tolerance environments. Borderline-suspicious emails can be held in temporary quarantine until sufficient evidence has been accumulated by Kaspersky Security Network for a judgement to be made on whether delivery is definitely safe.

Visibility

A clear user-friendly web-based interface enables your administrator to monitor levels of corporate mail protection, with tools including:

- Configurable dashboard.
- Convenient event viewer with powerful Boolean event search.
- Event export to your SIEM system.
- In-console or emailed reports.
- System health monitor.

Scaling and resilience

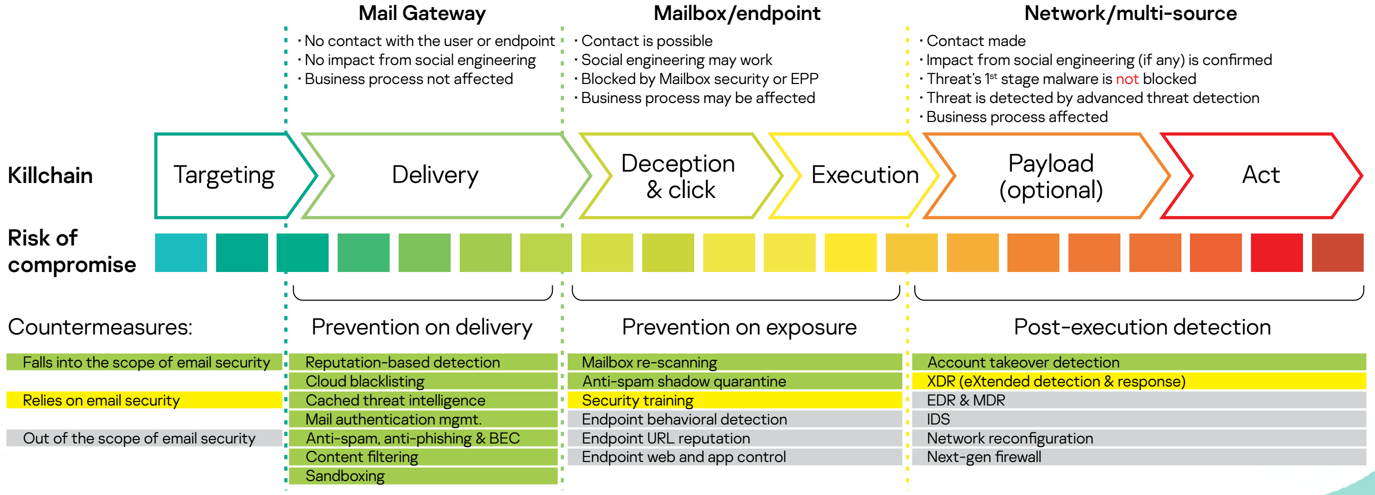
The solution supports clustered architectures in order to tackle growing traffic loads and ensure the resilience of the entire email security system in case of a disaster. To ensure that no critical data is lost due to disinfection, deletion or a technical mishap, original messages can be backed up according to admin-specified criteria, giving risk-free access.

Management and access control

Flexible rules allow the administrator to set up policies combining multiple criteria and to track any violation attempts. For an all-in-one Secure Email Appliance, specialist instruments to configure non-security aspects of the system are offered in the same management console. Role-based Access Control means separate administrators can be allocated to different areas of the business or to different clients.

eXtended Detection & Response

Integration with Kaspersky Anti Targeted Attack gives you access to a stack of expert-level detection technologies comprising an advanced sandbox, mobile threat analyzer, special data feeds containing C&C data and more. After successful detection, a targeted attack can be disrupted by blocking its components through finding and isolating them across different infrastructure layers, using XDR cross-product scenarios.



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

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

Get on board with Kaspersky Security for Mail Server

Kaspersky Security for Mail Server is just one of a range of products and solutions from Kaspersky, developed in-house, drawing on 20+ years of focused expertise, built from a single code base and designed to intermesh seamlessly to provide a comprehensive and unassailable security platform.

If you already use Kaspersky Endpoint Security for Business, installing Kaspersky Security for Mail Server means you can rest assured that your mail gateway protection will deliver the same high-performance standards as the rest of your security.

If you don't, now could be a good time to strengthen your perimeter and build your resilience by installing Kaspersky Security for Mail Server alongside, or instead of, your current email protection.

How to buy

Kaspersky Security for Mail Server is sold as a standalone targeted solution or as an add-on available only to Kaspersky Endpoint Security for Business customers.

Applications inside

- Kaspersky Security for Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Security for Cloud Mail

Licensing

Kaspersky Security for Mail Server is available under:

- Annual license
- Monthly subscription

You may also want to consider...

Kaspersky Security for Internet Gateway — complement your email perimeter protection with equally powerful web gateway security — also included in Kaspersky Total Security for Business.

Kaspersky Endpoint Security for Business — our leading endpoint security solution, delivering the most tested and most awarded endpoint protection on the market.

Kaspersky EDR Optimum — our new flagship Kaspersky endpoint security solution, offering enhanced visibility and detailed information about malware detections, supplemented with root cause analysis and automated response options.

Try Before Buying

Explore Kaspersky Security for Mail Server now with our free 30-day trial.

Request a Call

Still feel you need more information? Please ask us to call you!

Buy From a Trusted Partner

Feel like you're ready to buy? Find a local reseller to help you with your purchase.

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.