kaspersky BRING ON THE FUTURE

Kaspersky Security for Mail Server

Building resilience against the number one attack vector

Email is the primary attack vector currently threatening business IT security. Attackers are finding ever more sophisticated ways to infiltrate organizations through mail-based attacks, resulting in financial, operational and reputational loss. To counter these developments, business needs to be thinking in terms of resilience as well as protection. By optimizing your resilience and minimizing your attack surface, you can render yourself a less attractive and even a non-feasible target for attack. And the best point at which to deploy resilience-enhancing countermeasures is before unwanted emails come into contact with the user and their endpoint.

In 2018, we blocked **nearly half a billion attempted phishing attacks – double the number** for the previous year.

Securelist, Spam & Phishing in 2018

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 emails at gateway level

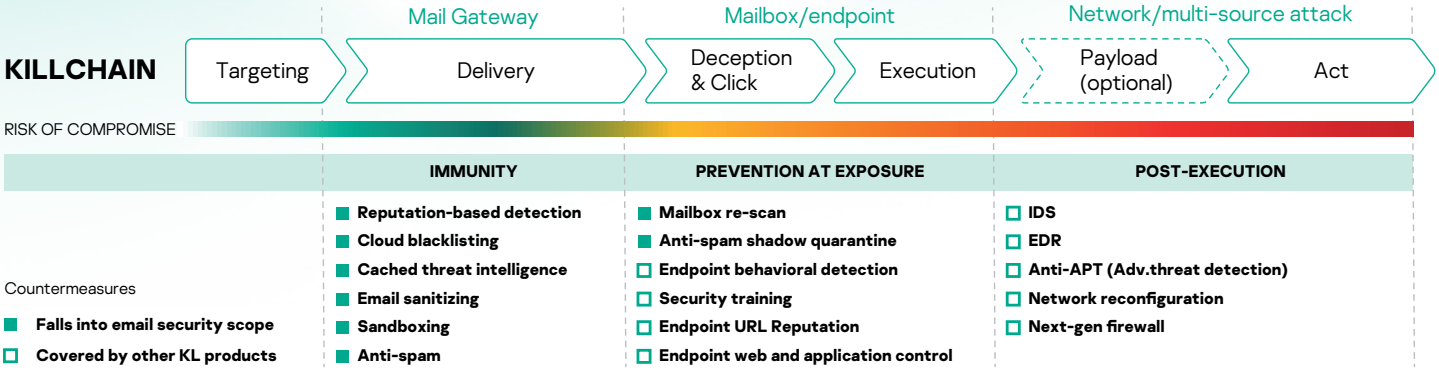
Most mail attacks only begin to activate at endpoint level – Kaspersky Security for Mail Server sets out to stop them long before they get that far. Our award-winning protection strengthens your resilience by detecting and intercepting attacks, right at first base, before they can breach your perimeter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

Swiftly and accurately processing those that are wanted

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[1] 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, while enabling legitimate emails to travel uninterrupted.

Taking email protection beyond the gateway

User must be protected, including from themselves – and the business must be protected from the consequences of user ignorance or error. Kaspersky Security for Mail Server detects the presence of malicious or undesirable content at individual inbox and outbox level on Microsoft Exchange Servers - including malware, phishing emails and potentially dangerous attachments, as administrator-configured policies dictate. In order to contain account takeover or insider threats, protection at the mailbox server level is highly recommended.



[1] https://www.kaspersky.co.uk/top3

Key features

Multi-layered malware protection

Multiple security layers applied through deep learning neural networks halt even most complex mail-based malware, including spear-phishing and targeted ransomware, in its tracks. Behavioral analysis, reputational data from the cloud and signature based engines, heuristics and signature databases combine with human expertise to deliver layer upon layer of award-winning detection and prevention levels, with minimal false positives.

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. For Kaspersky Anti Targeted Attack owners, full integration supports physical detonation in an external sandbox environment – providing much deeper levels of assessment and dynamic analysis. A targeted attack can then be disrupted by blocking its components' delivery.

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

Kaspersky Lab's anti-spam system uses smart engines to minimize the possibility of false positives and to adapt to changes in the threat landscape, under the supervision of human experts. Globally collected reputation data is processed in the cloud to provide a solid basis for efficient spam detection.

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 and IP addresses to provide protection from both known and unknown/zero-hour phishing emails.

The most used mail-borne malware

The most frequent detection verdict that Kaspersky customers have seen last year was Win32.CVE-2017-11882, an exploit for well-known MSOffice vulnerability.

Securelist,
Spam & Phishing in 2018

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.

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.

Preventing unsafe content transfers

Kaspersky's configurable attachment filtering system can detect file disguises commonly used by cybercriminals, to identify potentially dangerous attachments. Content filtering functionality allows the administrator to configure specialized rules for preventing data leakage.

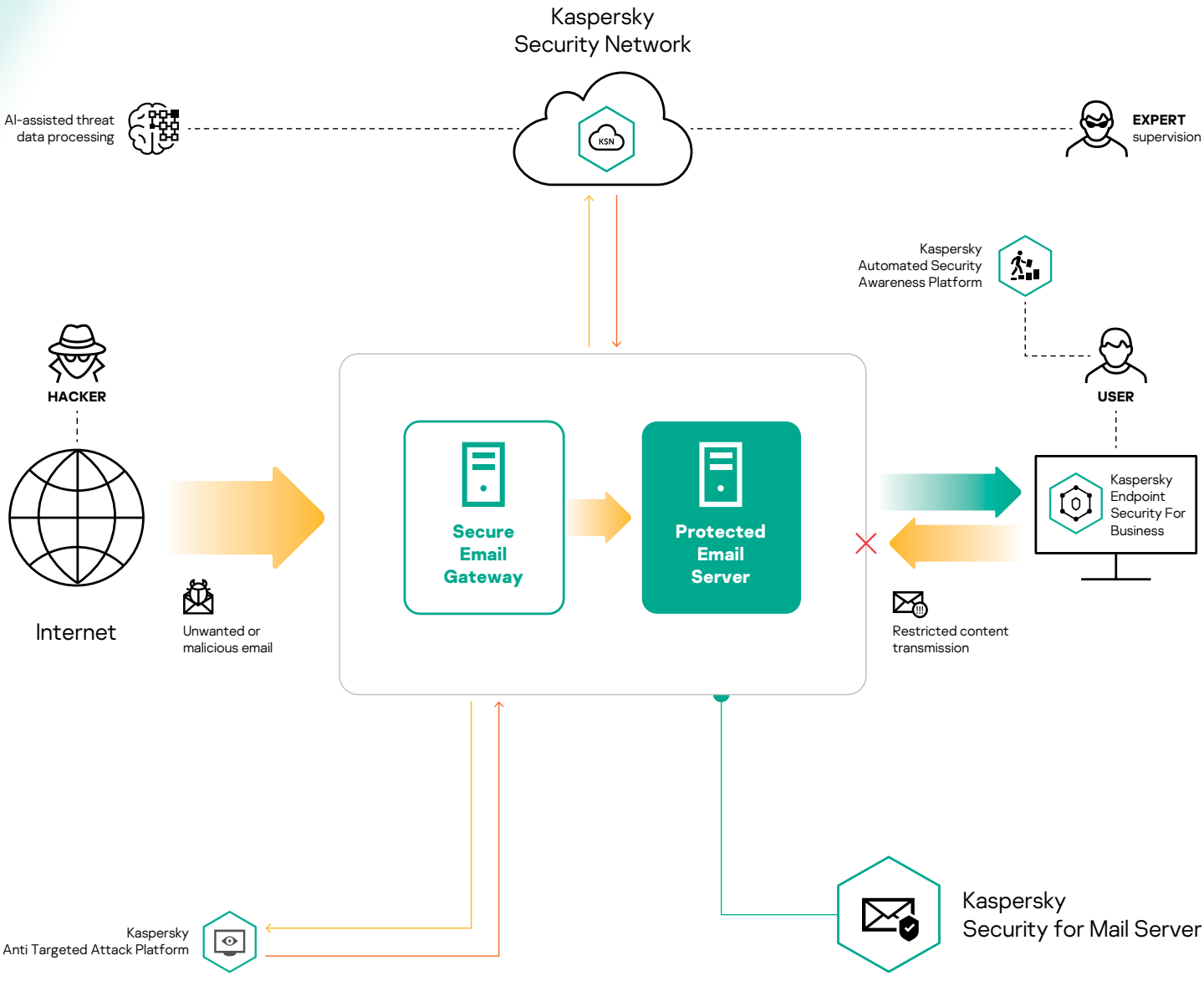
Built-in backup

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.

Management and visibility

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

- Flexible but easy-to-use rules and policy configuration.
- Active Directory integration.
- Event export to your SIEM system.
- Systems health diagnostic.



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 Lab, originated in-house, drawing on 20+ years of single-minded expertise, built from a single code base and designed to intermesh seamlessly to provide a comprehensive and unassailable security platform.

If you already use security solutions such Kaspersky Endpoint Security for Business, installing Kaspersky Security for Mail Server means you can rest assured that your mail gateway protection operates to the same unequalled 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

Licensing

Kaspersky Security for Mail Server is available under:

- Annual license
- Monthly Subscription

You may also want to consider....

Kaspersky Security for Microsoft Office365 — specifically designed to fill the security gaps in Microsoft's cloud-based offering, including Outlook 365.

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 flagship endpoint security solution, delivering the most tested and most awarded endpoint protection on the market today.

Try Before Buying

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

Request a Call

Still feel you need more information? Request a call to clarify everything you require!

Buy Via a Trusted Partner

Feel like you are ready to buy? Find a reseller in your geography to help you with your purchase!

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
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.