kaspersky BRING ON THE FUTURE

Kaspersky Security for Microsoft Exchange Server

Comprehensive protection against the no. 1 threat vector for the leading emailing platform

Kaspersky Security for Microsoft Exchange Server protects corporate IT networks from the most frequent mode of attack– which is also used for unscrupulous marketing, mass malware and phishing campaigns and focused, highly complex targeted attacks. Benefitting from API-based integration with the most popular emailing platform, Kaspersky Security for Microsoft Exchange Server covers the broadest range of scenarios where reliable protection is essential.

Highlights

- Multi-layered anti-malware and anti-phishing protection
- Zero-hour threat protection
- Intelligent, cloud-assisted spam protection
- Advanced content filtering
- Ransomware blocking
- Dedicated BEC protection
- Backed by global threat intelligence from Kaspersky Security Network
- Role-based access to admin and web usage
- Microsoft Active Directory and Database Access Group (DAG) support
- Monthly subscription licensing option

Counters a broader range of threats via an API-integrated technology stack

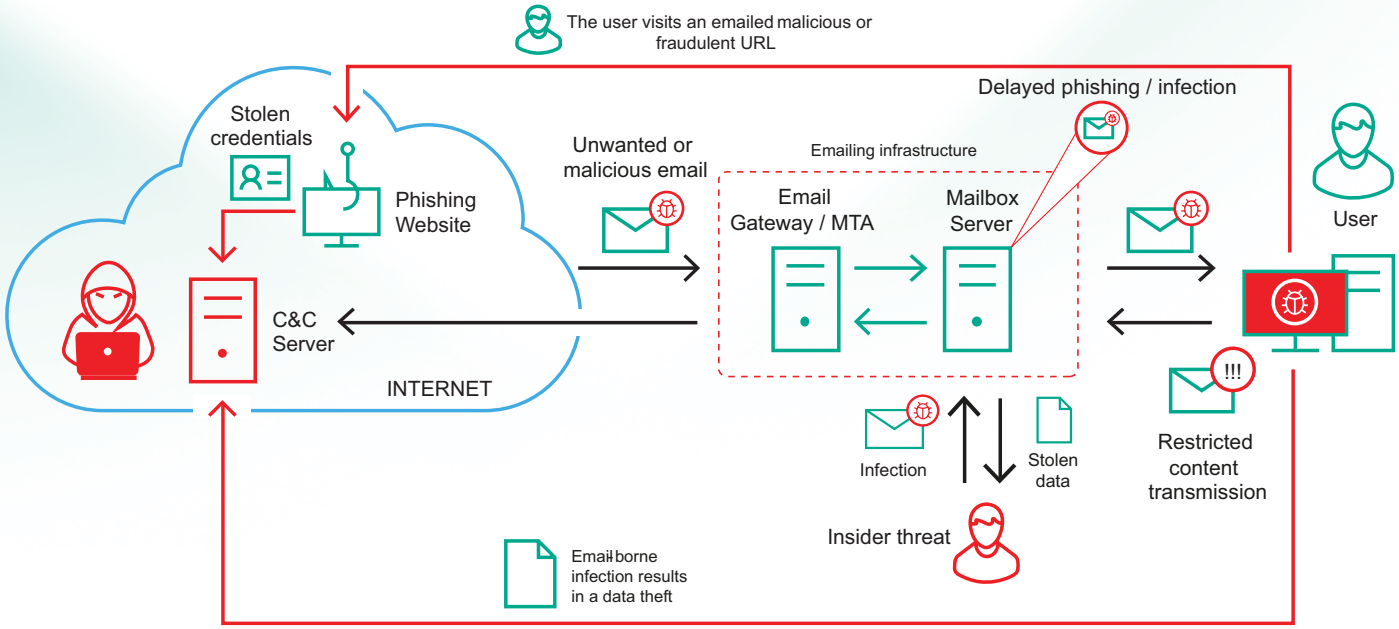
Kaspersky Security for Microsoft Exchange Server protects against email-borne threats at both gateway and mailbox level, reducing the risks from social engineering-based attacks and endpoint vulnerability exploitation. It lets you control risky transmissions to minimize user error-based incidents, including infections, scams and data leaks.

Increases productivity and reduces risks with cloud-assisted, intelligent spam protection

Kaspersky's machine learning-powered anti-spam capabilities detect even the most sophisticated, unknown spam with minimal loss of valuable communications due to false positives. Cloud-assisted, intelligent spam protection reduces the risks associated with spam by stopping it in its tracks, saving system and human resources.

Complements your infrastructure-wide defenses

With one of the most powerful stacks of protective technologies in the industry, superior detection rates and near-zero false positives, Kaspersky Security for Microsoft Exchange Server integrates seamlessly with other Kaspersky solutions – or can be used as a powerful component of your existing multi-vendor defenses.



The email-based threat model

Did you know?
... Some email-based attack scenarios involve intra-corporate communications, sleeping implants, delayed phishing and other schemes that can render one-time checking by a secure email gateway ineffective. To counter the full breadth of these scenarios, a mailbox-level solution is a convenient and effective option.

Features

Multi-layered threat protection and control, powered by data science

Kaspersky's next-generation malware protection and control incorporates multiple proactive security layers, including:

- **Anti-malware:** Proactive machine learning-powered detection, analysis and filtering technologies identify and block malware threats including spyware, financial Trojans, ransomware, miners and wipers.
- **Real-time detection of new threats:** The Kaspersky Security Network, powered by constantly updated intelligence from tens of millions of users and our own world-leading research, supports real-time detection of potential threats even as they emerge, with minimal false positives.
- **Emulative sandboxing:** Attachments are executed and analyzed in a safe emulated environment, protecting against even the most sophisticated, heavily obfuscated malware.
- **Script detection:** Identifies and deals with scripts embedding malware into apparently harmless files heading for your endpoints, and those used in drive-by web-based attacks.
- **Reputation-based filtering:** File and address reputations delivered by the Kaspersky Security Network cloud databases can help stop suspicious or unwanted files and internet resources on the spot, without the need for deeper analysis.
- **Advanced anti-phishing:** Neural network-based analysis supported by real-time cloud-based sender domain and URL checking protects against even the most convincing email phishing. This includes Business Email Compromise, where trust of business associates and companies is abused to make targeted phishing even more credible.
- **Source spoofing detection:** Cyberattackers use various techniques to spoof or disguise an email's source information in order to trick the recipient into believing it comes from a trusted sender. Kaspersky's threat expertise sees through all these techniques, leaving no chance for human error.
- **Mailsploit detection:** A number of email client applications (especially those that haven't been updated) may contain vulnerabilities which allow attackers to affect the way sender information is displayed, effectively spoofing the email source, Kaspersky's anti-phishing engine detects these attempts and uses them against the attacker, blocking their phishing emails.
- **Business Email Compromise (BEC) protection:** BEC phishing involves the abuse of trust between an employee and a colleague (usually of a higher rank) or a business associate (supplier, business partner, etc.) by cyberattackers who pretend to be a trusted sender asking something of the recipient. Kaspersky Security for Microsoft Exchange Server puts together multiple indicators, such as sender data, URL reputations, linguistic analysis of email text and so on, to detect these kinds of attempts.

Intelligent spam protection

Masses of unwanted emails devour resources and employees' attention – and may contain something less harmless than just annoying. Kaspersky Security for Microsoft Exchange Server studies all aspects of a communication, including its service data, sender information, size, attachments, contained URLS and so on. Depending on the item, a range of intelligent technologies are used to detect even polymorphic or image-based spam.

- **KSN integration:** The solution can check with Kaspersky's cloud database to obtain real-time information about the newest spam variations.
- **Reputation filtering:** The administrator has the option of using reputation filtering, an additional anti-spam scanning service that increases the accuracy of spam detection and reduces the probability of false positives.
- **Blocklist integration:** For additional protection against spam, messages are scanned using a DNSBL lists of spammers' addresses and SURBL technology to detect spammer URLs in the message.
- **Multi-language support:** The application carries out anti-spam scanning of messages written in different languages, including Asian language sets.

Unparalleled threat intelligence
Constantly updated global threat data acquisition, continuous research by the world's best security experts, and renowned data scientists who work to transform data into actionable intelligence to counter even zero-hour threats. This is what underpins Kaspersky Security for Microsoft Exchange Server.

Full control over sensitive communications

Despite the trend of migrating corporate productivity infrastructure – including email – into public clouds, many companies prefer to keep their assets on-premises. These are usually due to concerns about handling sensitive data, and compliance issues. Add the sometimes blurred boundaries of 'shared responsibilities' between cloud provider and tenant, and it's not hard to understand why C-level management takes a cautious approach.

Powerful email traffic control

By failing to prepare, you're preparing to fail – so the saying goes. Kaspersky Security for Microsoft Exchange Server offers powerful ways to control your email communications, resulting in a significant reduction of risks.

Content filtering[UPDATED]**:** File types known to be potentially problematic or irrelevant can be prohibited from transmitting, based on parameters including name, size, MIME type (video, images, etc.), hash and extension/type (Format Recognizer is used to spot files with spoofed extensions). For more granular filtering and prevention of potential data leaks, complex text search criteria can be applied to the content.

Message classification: An administrator can configure separate processing rules for each category of unsolicited mail to prevent any loss of information. For instance, messages that are known to be spam can be blocked; suspicious mail can be directed straight to the unwanted mail folder; and formal messages such as message delivery and message-read confirmations can go directly to the Inbox.

Trusted/untrusted lists: Individual users can create their own trusted and untrusted sender lists based on their emails, domain names or sender SMTP name / IP address. A trusted list can also be created using the recipient's SMTP address. Messages from a sender on the trusted list aren't scanned and are delivered straight to the recipient. However, if the address is on the untrusted list, the message will be tagged with a special heading and processed according to the rules configured by the administrator.

Pre-defined mail categories: Category-based email tagging allows more convenient email sorting and helps tackle some security risks.

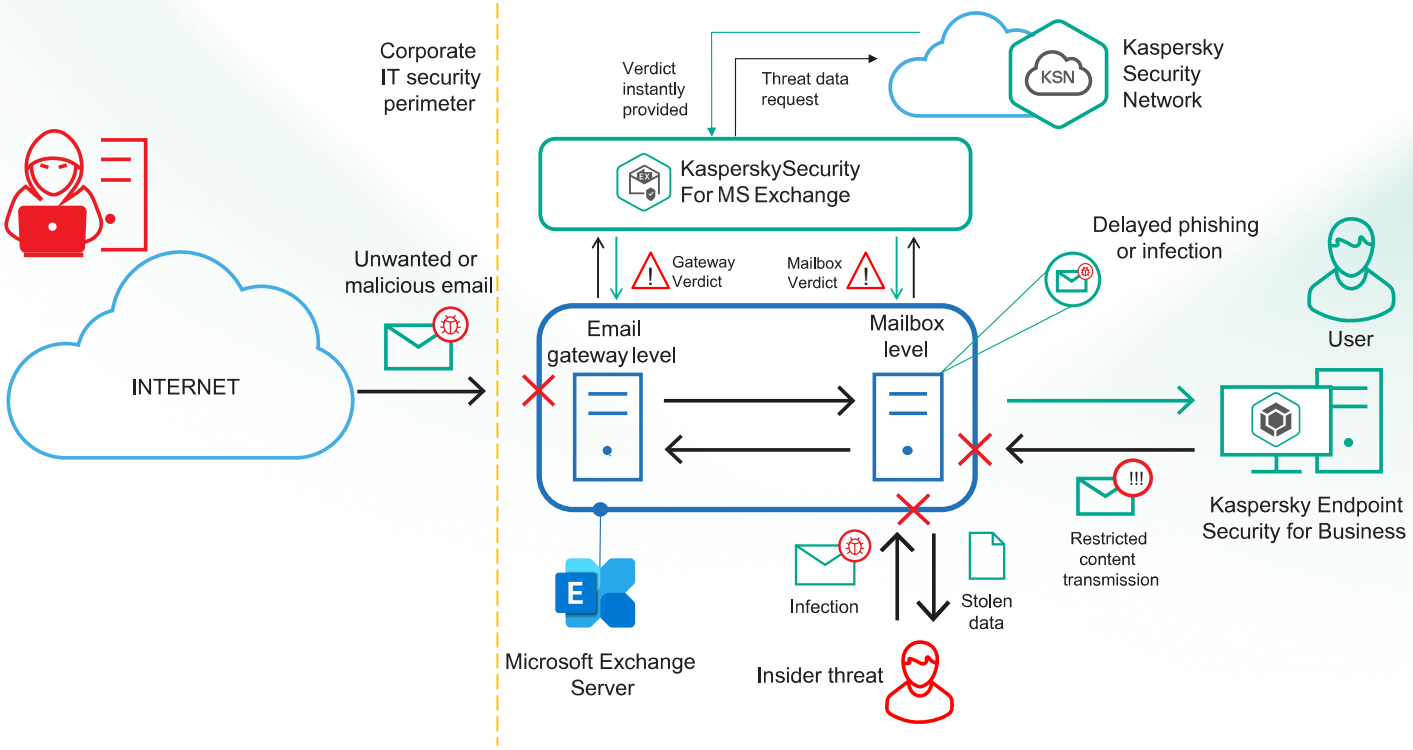
Architecture, deployment and application management

Kaspersky Security for Microsoft Exchange Server relieves the pressure on security administrators through a wide range of useful functions.

Gateway and Mailbox protection in one solution: Kaspersky Security for Microsoft Exchange benefits from full API-level integration, providing both gateway- and mailbox-level email protection. This covers significantly more attack scenarios compared to a Secure Email Gateway (SEG)-class solution.

CLI-based management[NEW]**:** It's possible to install, update, restore, and remove the application via the command line without using the graphical user interface.

Microsoft solutions-based infrastructure integration: The application integrates with Microsoft Active Directory for a more convenient configuration process and is compatible with DAG (Database Availability Group), delivering all the benefits of DAG-provided disaster resilience.



How Kaspersky Security for Microsoft Exchange Server counters email-based threats

How to buy:
The Kaspersky Security for Microsoft Exchange Server can be activated in the following products and solutions:

- Kaspersky Security for Mail Server
- Kaspersky Total Security for Business

Hardware and software requirements

MINIMUM HARDWARE AND SOFTWARE REQUIREMENTS

For the application to run properly, the computer should meet the following minimum requirements:

1. Installing Security Server with the full set of modules:

Hardware requirements:
- Processor – according to the hardware requirements for the protected Microsoft Exchange server;
- At least 2 GB of free RAM;
- 6 GB of available disk space. Additional disk space may be required depending on the application settings and operation mode.

Operating system:
- Microsoft Windows Server 2019 Standard or Datacenter (Desktop Experience);
- Microsoft Windows Server 2019 Core;
- Microsoft Windows Server 2016 Standard or Datacenter;
- Microsoft Windows Server 2012 R2 Standard or Datacenter.

Mail server:
- Microsoft Exchange Server 2019 deployed in at least one of the following roles: Mailbox or Edge Transport;
- Microsoft Exchange Server 2016 deployed in at least one of the following roles: Mailbox or Edge Transport;
- Microsoft Exchange Server 2013 SP1 deployed in at least one of the following roles: Mailbox, Hub Transport, or Client Access Server (CAS).

Database management system:
- Microsoft SQL Server 2019 Express, Standard or Enterprise;
- Microsoft SQL Server 2017 Express, Standard or Enterprise;
- Microsoft SQL Server 2016 Express, Standard or Enterprise;
- Microsoft SQL Server 2014 Express, Standard or Enterprise;
- Microsoft SQL Server 2012 Express, Standard or Enterprise.

Additional software:
- Microsoft .NET Framework 4.5.

2. Installing only the Management Console:

Hardware requirements:
- Intel Pentium 400 MHz or faster processor (1000 MHz recommended);
- 256 MB free RAM;
- 500 MB disk space for the application files.

Operating system:
- Microsoft Windows Server 2019 Standard or Datacenter (Desktop Experience);
- Microsoft Windows Server 2019 Core;
- Microsoft Windows Server 2016 Standard or Datacenter;
- Microsoft Windows Server 2012 R2 Standard or Datacenter;
- Microsoft Windows Server 2012 Standard or Datacenter;
- Microsoft Windows 10;
- Microsoft Windows 8.1;
- Microsoft Windows 8;
- Microsoft Windows 7 SP1 Professional, Enterprise or Ultimate.

Additional software:
- Microsoft Management Console 3.0;
- Microsoft .NET Framework 4.5.

3. Installing the administration plug-in:
- Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1;
- Kaspersky Security Center 10 Service Pack 2 Patch a;
- Kaspersky Security Center 10 Service Pack 3.

4. Monitor the application's operation via System Center - Operations Manager:
- System Center 2012 Operations Manager;
- System Center 2012 R2 Operations Manager.
- Additional software:
- Windows PowerShell 3.0 or higher.

Efficient security management

The more effective and convenient tools you have at your disposal, the stronger your company's security will be. Kaspersky Security for Microsoft Exchange Server offers efficiency and convenience with a host of security management tools.

Role-based access control[UPDATED]**:** A new set of roles lets you manage user access for individual application profiles. This enables the administrator to restrict administrators in other departments to access specific security servers only, if required.

Detailed reports: You can monitor the operation of the application and the protection status using the detailed HTML reports or by viewing the Windows event log. You have complete control over the frequency with which reports are generated and the information to be included in them. All reports can be stored on the hard drive or sent via email.

Centralized management and monitoring: A single administrative console with centralized reporting and backup helps to control all your Exchange servers. Kaspersky Security for Microsoft Exchange is integrated with Kaspersky Security Center, enabling you to monitor the protection status, important events and consolidated statistics for your entire organization in a single console.

On-demand and on-schedule background scanning: All folders and messages stored on the server are scanned in the background to ensure that all objects are processed using the latest threat intelligence data. Set up a flexible background schedule or run on-demand scanning for any specific mailbox at any time. All with minimal impact on server load and business productivity.

Customized configuration: You can configure the application based on your company's IT security policy and hardware capabilities. For example, you can exclude certain file types from scanning and configure the spam-intensity level. You can also configure antivirus and anti-spam processing scenarios for different message categories, and create trusted and untrusted lists according to senders' or receivers' addresses.

Security updates flexibility: Updates to databases and ML models are available on demand or can be completed automatically according to a schedule. You can either download updates directly from the Kaspersky website or from a local server.

Convenient administration: The administrative interface is based on the popular Microsoft Management Console, and remote administration is possible.

Logging and notification system: Events related to application's operation are recorded to the Windows event log on behalf of the KSE source. The events are displayed in the application logs and service logs in the Kaspersky Security for Exchange Servers section. The administrator can also subscribe to email notifications about any critical events in the application's operation.

Flexible licensing: Choose from flexible monthly licensing with scalable and pay-as-you-go options or fixed annual licensing. For Managed Service Providers, it's easy to manage security remotely for multiple clients using the multi-tenant console.

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 tomorrow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.