kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Security for Business
Select

Kaspersky Endpoint Security for Business Select provides intelligent protection for a wide range of platforms – including Linux servers and endpoints. Multi-layered security that detects suspicious behavior and blocks threats, including ransomware, combines with cloud-enabled controls to reduce your exposure to attacks – while mobile management features help you to protect data on mobile devices.

The protection and management capabilities you need
Kaspersky has built powerful enterprise-class features into the progressive tiers of our products. We've made sure that the technology is uncomplicated and flexible enough for any growing business to use.

Multiple protection layers for
- Windows, Linux and Mac
- Windows and Linux servers
- Windows Server containers
- Android and other mobile devices
- Removable storage

Unparalleled defense against
- Software exploits
- Ransomware
- Mobile malware
- Advanced threats
- Fileless threats
- PowerShell & script-based attacks
- Web threats

Features included
- Anti-Malware
- Vulnerability Assessment
- Security Policy Adviser
- Process isolation
- Exploit Prevention and Rollback
- Firewall and OS firewall management
- Cloud-assisted protection
- Full integration with Kaspersky EDR Optimum NEW
- Full integration with Kaspersky Sandbox NEW
- SIEM integration via Syslog
- Application Control
- Web and Device Controls
- Server and container protection
- Remote Data Wipe NEW
- Mobile Threat Defense
- Reporting
- Cloud console NEW
- Web and MMC based consoles

See our webpages for details here.

Advanced protection and control

Agile, adaptive security

Kaspersky Endpoint Security for Business Select is designed to secure any IT environment. A full stack of proven and innovative technologies addresses even advanced and unknown threats, reducing your risk and keeping your organization, your data and your users safe.

Seamless integration with new Kaspersky EDR Optimum and Kaspersky Sandbox makes it easy to add powerful automated detection and response capabilities to this security armory.

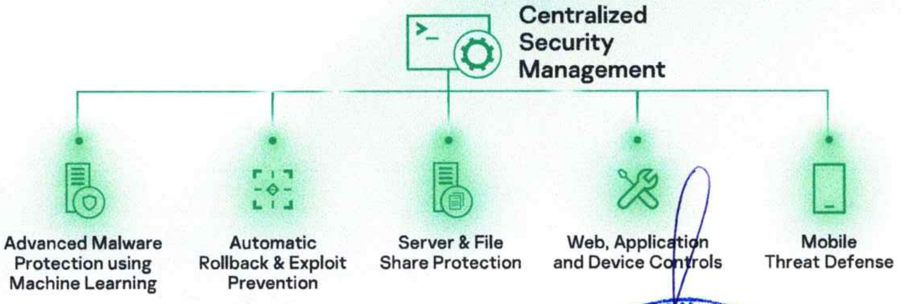
Central management console – the best of both worlds

In the cloud, on-premises or both? You decide - and we'll provide unified management via a cloud console, or traditional console deployment on-premises, in AWS or Azure cloud environments.

Whichever option you choose, our 'single pane of glass' console lets you view and manage your entire security landscape and deploy your chosen security policies to every endpoint rapidly and with minimum fuss, using a wide range of preconfigured scenarios.

Most tested, most awarded

Year after year our products top the charts in independent tests and reports. We're proud of this remarkable track-record and all the industry recognition that goes with it. And we're even more proud that our customers feel the same way, consistently expressing outstanding levels of satisfaction with our products and our performance.


Centralized Security Management
Advanced Malware Protection using Machine Learning
Automatic Rollback & Exploit Prevention
Server & File Share Protection
Web, Application and Device Controls
Mobile Threat Defense

Digitally signed by Gnidaş Bogdan
Date: 2022.09.02 13:08:11 EEST
Reason: MoldSign Signature
Location: Moldova

SOCIETATEA CU RĂSPUNDERE LIMITATĂ, REPUBLICA MOLDOVA, mun. CHIŞINĂU
S.R.L. "BTS PRO"
Nr. 3
IDNO 1008600061565

Key features

Essential protection

Our essential threat protection components form the foundation of effective security against common threats. These include File, Web and Mail Threat Protection, Firewall, Network Threat Protection, BadUSB Attack Prevention and AMSI Protection Provider.

Advanced, ML-driven threat protection

Advanced protection components including **Kaspersky Security Network, Behavior Detection,** Anti-Ransomware Protection and Exploit Prevention, can detect and repel even new and unknown threats. Powered by both static and dynamic machine learning, Behavior Detection analyzes process activity in real time to detect the most sophisticated threats, like fileless malware or script-based attacks. Once a malicious process is identified and flagged, it's terminated, and the Remediation Engine rolls back any changes.

Cloud-enabled controls for policy refinement and breach prevention

Host Intrusion Prevention and centralized **web, device** and **application controls** reduce your attack surface and help keep users safe and productive. Kaspersky has its own dedicated Dynamic Whitelisting laboratory, maintaining a constantly monitored and updated database of more than 2.5-billion trusted programs.

Flexible 360° management

Kaspersky Security Center is a central management console that makes it easier for administrators to configure, deploy, update and manage their security. It simplifies the application of group tasks, policies and policy profiles and the generation of reports.

Windows, Mac, Linux - all covered

Protection for Windows and Linux endpoints and servers, and for Mac for workstations, are all administered from the same console – ideal for mixed environments.

Mobile management and protection

Powerful anti-malware combined with cloud-assisted threat intelligence protects against the latest threats. Web control and anti-phishing capabilities ensure reliable, safe web filtering to block access to malicious and other undesirable websites. Mobile device management capabilities and integration with EMM systems simplify compliance, enablement and overall management.

Integration for advanced prevention, detection and response NEW

Kaspersky Endpoint Security for Windows is designed to integrate with Kaspersky Sandbox and Kaspersky EDR Optimum for advanced automated detection and response.

Experience it for yourself

Why not experience adaptive protection against advanced threats targeting your business for yourself? Visit this page for a free 30-day trial of Kaspersky Endpoint Security for Business.

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.

SOCIETATEA CU RĂSPUNDERE LIMITATĂ, REPUBLICA MOLDOVA mun.CHIŞINĂU
S.R.L.
"BTS PRO"
Nr. 8
IDNO 1008600081565

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

kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Take your endpoint defenses to the next level and tackle evasive threats head-on – with no hassle.

It's time to step up a level. You're ready not just to protect your organization with mainstream anti-malware technologies, but to identify, analyze and effectively neutralize those threats deliberately designed to evade traditional protection, and to bury themselves deep in your systems, ready to do their worst.

Legitimate system tools are used in about **30% of successful attacks** to launch scripts and programs, download payloads, scan networks or get remote access to the infected host.
Incident response analyst report, Kaspersky, 2020

The challenges

Worse disruption

Malware, ransomware, financial spyware and other threats are becoming smarter at evading detection, and attacks are becoming cheaper to mount. So the risk of a serious attack is greater than ever, as are the levels of damage and disruption involved.

Complex infrastructures

Today, the vast majority of IT managers and security professionals have to protect a whole range of different endpoints – laptops, servers, virtual and cloud environments and remote workstations – while coping with barely manageable levels of IT complexity

Finding a balance

Cybersecurity is for the most part about finding the optimal balance between your available resources and the highest level of protection that's realistically achievable. And your IT specialist's time is one of the scarcest resources of all.

The answer

Kaspersky Endpoint Detection and Response (EDR) Optimum helps you identify, analyze and neutralize evasive threats by providing easy-to-use advanced detection, simplified investigation and automated response.

Even in successful attacks, financial losses were **32% lower** if a breach was responded to rapidly.
Incident response analyst report, Kaspersky, 2020

Fully armed and prepared

Based on advanced detection mechanisms, including machine learning and enhanced behavior analysis, Kaspersky EDR Optimum gives you deep visibility into threats, straightforward analysis and investigation tools and automated response. You'll be able to see the threat, understand it, reveal its full scope and instantly respond, preventing business disruption.

A single solution

Kaspersky EDR Optimum brings advanced detection, analysis and response capabilities to the Kaspersky security ecosystem, enhancing defenses across a whole spectrum of endpoints, including laptops, servers, cloud workloads and virtual environments. Centralized deployment and unified management of Kaspersky EDR Optimum are available from the cloud or on-premise.

Simple and efficient

Kaspersky EDR Optimum is built for smaller cybersecurity teams with limited resources who are looking to upgrade their incident response capabilities. Performance is optimized for maximum efficiency and minimum human input, making the most of your security specialists' time with automation and centralization of all administration and streamlining workflows.

Key benefits

- Protect yourself against more frequent and more disruptive evasive threats
- Defend every endpoint: laptops, servers, cloud workloads
- See the full scope of any threat over the whole network
- Understand the root cause of the threat and how it actually occurred
- Avoid further damage with rapid automated response
- Save time and resources with a simple and automated tool

SOCIETATEA CU RĂSPUNDERE LIMITATĂ, REPUBLICA MOLDOVA, mun.CHIŞINĂU
S.R.L.
"BTS PRO"
Nr.3
IDNO 1008600081565

Crucial EDR use cases

Advanced detection

Advanced detection is necessary to discover evasive threats:

- Behavior Threat detection and Exploit prevention powered by machine learning (ML)
- Heuristics, smart records, ML-based technologies
- Built-in Emulator for pre-execution detection of malicious behavior
- Sandbox for enhanced behavior analysis (available with Kaspersky Sandbox)
- Global threat intelligence data collected and analyzed in-lab by AI-based systems and experts

Answer vital questions

Evasive threats often hide in plain sight and should be investigated to be fully eradicated. EDR helps by finding answers to these questions:

- Am I under attack right now?
- Has this industry-wide attack reached my infrastructure?
- Where did this threat come from?
- What has it managed to do on my hosts?
- Are there any hidden layers to this threat?
- Are other endpoints affected?

Respond rapidly

Respond to threats with a single click or with an automated response as soon as they're discovered:

- Prevent the malicious file from running and spreading throughout the network during or after your investigation
- Automatically quarantine files associated with evasive threats on all endpoints
- Automatically isolate infected hosts on finding an Indicator of Compromise (IoC) associated with a fast- spreading threat

Now you can do so much more

Now you can understand the full scope of any threat attacking you and how it's developed on your endpoints, taking advantage of advanced machine learning-based detection and visibility into detects. And you can ensure that each threat has been fully dealt with – nothing's still burrowing away somewhere inside your system, working out how much harm it can do.

Defend hybrid infrastructures

Hybrid infrastructures bring unique security challenges as well as significant benefits. Now you can enhance your data and infrastructure protection for virtual and physical servers, VDI deployments and public cloud workloads with essential EDR functionality.

Avoid alert fatigue and make full use of your resources with centralized management across all your hybrid endpoints and workloads and streamlined EDR workflow from the cloud or on-premise.

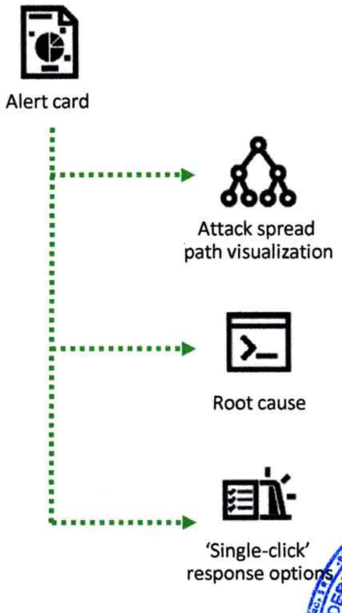
Multiple-level endpoint protection

EDR technologies don't exist in a vacuum – they can only function effectively from a solid base of strong endpoint protection. Multiple-level endpoint protection ensures that you're not distracted by handling commodity threats and incidents which should already have been dealt with by automated anti-malware software. That's why Kaspersky EDR Optimum operates in conjunction with one of our our most tested, most awarded[1] endpoint protection platforms: Kaspersky Endpoint Security for Business and Kaspersky Hybrid Cloud Security.

Analyze threats

In a single incident card, enriched data on the detect and a drill-down attack spread-path are gathered to perform quick analysis and make informed decisions for a 'single-click' or automated response.

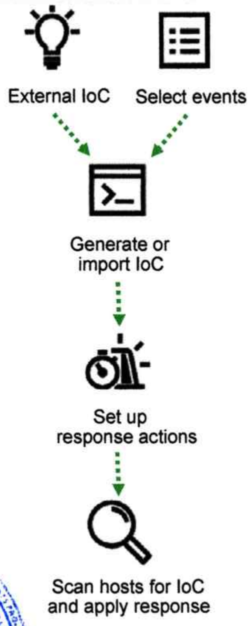
IoCs can be imported from trusted sources or generated based on the investigation in order to discover evasive threats lurking on endpoints across your infrastructure.


Alert card
Attack spread path visualization
Root cause
'Single-click' response options

Automate your response

Instantly respond to threats during the investigation with 'single-click' options available in the incident card or set up automated responses upon discovery based on IoC scans. Response actions include:

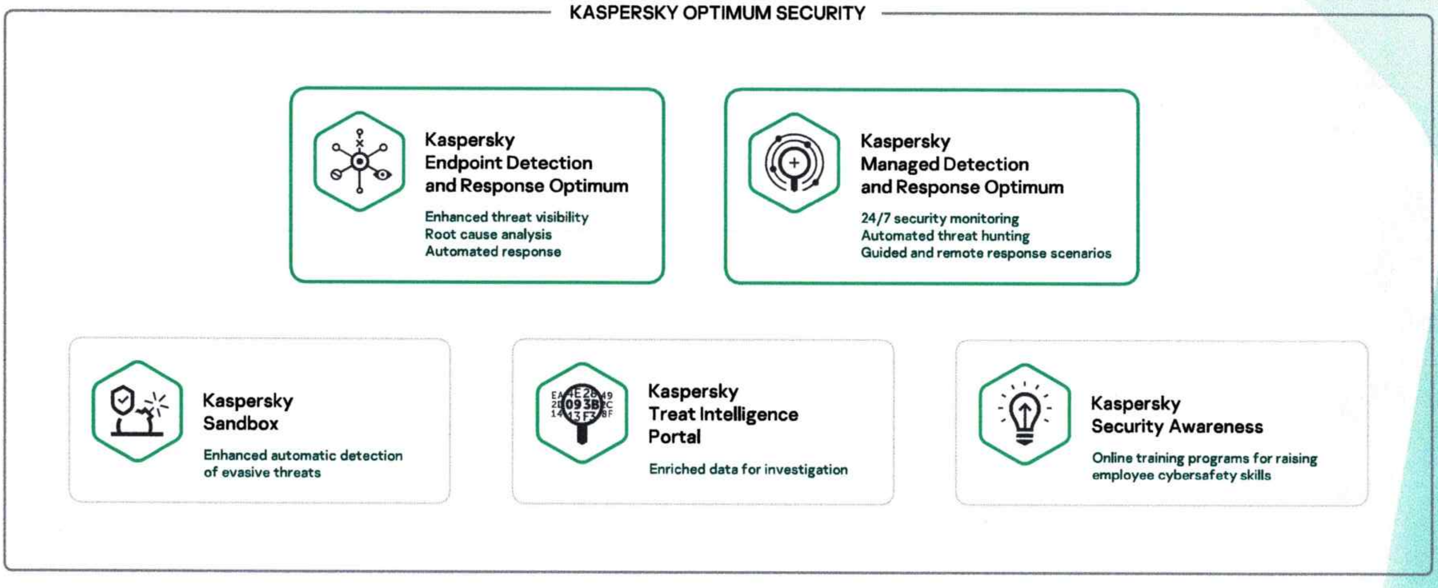
- Isolate host
- Quarantine file
- Prevent execution
- Launch critical areas scan



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

Your Kaspersky Optimum Security platform

EDR is part of an ecosystem spanning multiple technologies, tools and services: Kaspersky EDR Optimum is they key component of Kaspersky Optimum Security, a wider solution strengthening multiple aspects of your defenses against evasive threats, while being easy on your resources:



KASPERSKY OPTIMUM SECURITY

Kaspersky Endpoint Detection and Response Optimum
Enhanced threat visibility
Root cause analysis
Automated response

Kaspersky Managed Detection and Response Optimum
24/7 security monitoring
Automated threat hunting
Guided and remote response scenarios

Kaspersky Sandbox
Enhanced automatic detection of evasive threats

Kaspersky Treat Intelligence Portal
Enriched data for investigation

Kaspersky Security Awareness
Online training programs for raising employee cybersafety skills

A stage-by-stage approach

Kaspersky Optimum Security builds on Kaspersky Security Foundations. If and when you're ready to do so, you can choose to grow smoothly into the application of powerful tools that protect against the most advanced threats, with Kaspersky Expert Security.

Kaspersky Security Foundations

Automatically block the vast majority of threats.

- Multi-vector automated prevention of incidents caused by commodity threats – the vast majority of all cyberattacks
- The foundation stage for organizations of any size and complexity in building an integrated defense strategy
- Reliable endpoint protection for those with small IT teams and emerging security expertise

Kaspersky Optimum Security

Build up your defenses against evasive threats. Ideal for businesses with:

- Have a small IT security team with basic cybersecurity expertise
- An IT environment growing in size and complexity, increasing the attack surface
- A a lack of cybersecurity resources – in contrast to a need for enhanced protection
- A growing need to develop an incident response capability

Kaspersky Expert Security

Readiness for complex and APT-like attacks. For businesses with:

- Complex and distributed IT environments
- A mature IT security team, or an established Security Operations Center (SOC)
- A low appetite for risk due to higher costs of security incidents and data breaches
- And where regulatory compliance is a concern

To find out more about how Kaspersky Endpoint Detection and Response Optimum addresses cyberthreats while going easy on your security team and resources, visit http://www.kaspersky.com/enterprise-security/edr-security-software-solution.

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

www.kaspersky.com

SOCIETATEA CU RĂSPUNDERE LIMITATĂ, REPUBLICA MOLDOVA, mun. CHIȘINĂU
S.R.L.
"BTS PRO"
Nr. 3
IDNO 1008600061565

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

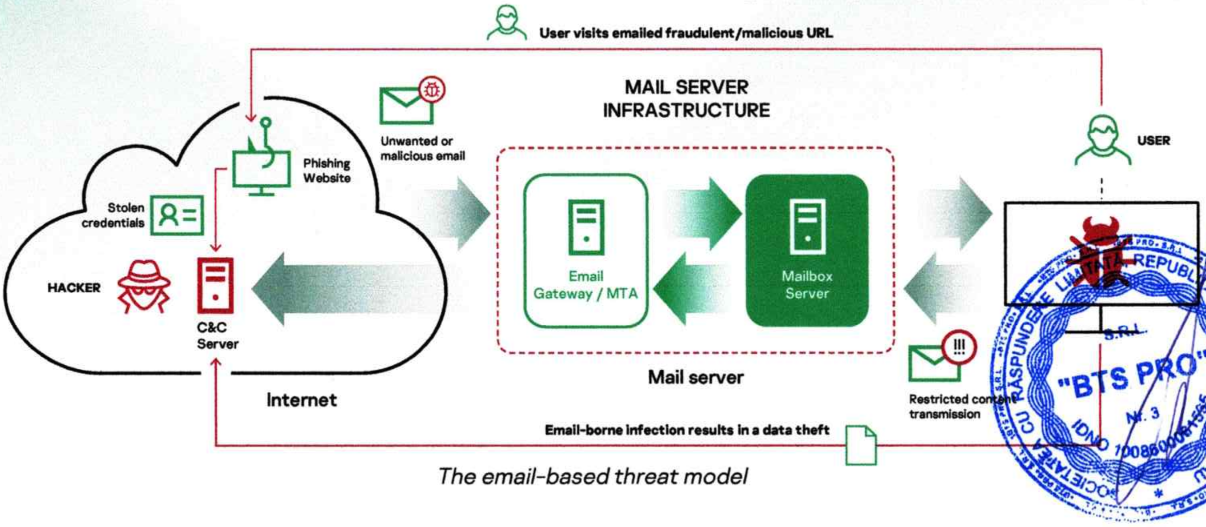
Most mail attacks only begin to activate at endpoint level – Kaspersky Security for Mail Server sets out to stop them long before they get that far. Our award-winning protection strengthens your resilience by detecting and intercepting attacks right at the beginning of the killchain, before they can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

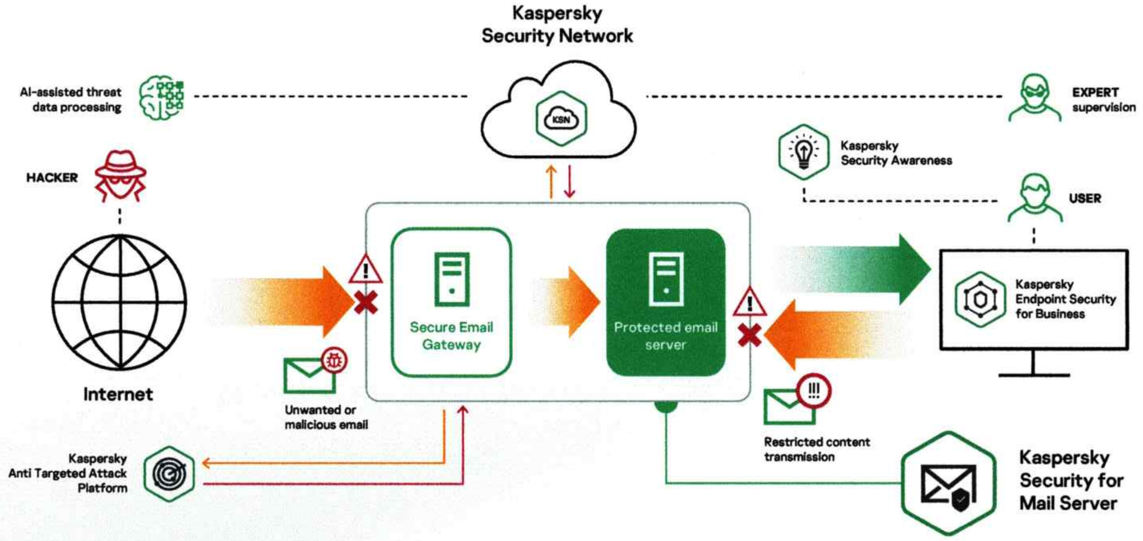
Kaspersky Security for Mail Server detects malicious or undesirable content not only at the gateway, but also at the level of individual Microsoft Exchange Server mailboxes – or/and Microsoft Exchange Online. Delayed phishing attacks designed to evade gateway level countermeasures, BEC messages generated 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
USER
Unwanted or malicious email
Phishing Website
Stolen credentials
HACKER
C&C Server
Email Gateway / MTA
Mailbox Server
Mail server
Internet
Restricted content transmission
Email-borne infection results in a data theft

The email-based threat model

SOCIETATEA CU RĂSPUNDERE LIMITATĂ REPUBLICA MOLDOVA, mun.CHIŞINĂU
"BTS PRO" S.R.L.
Nr. 3
IDNO 1008600061565

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

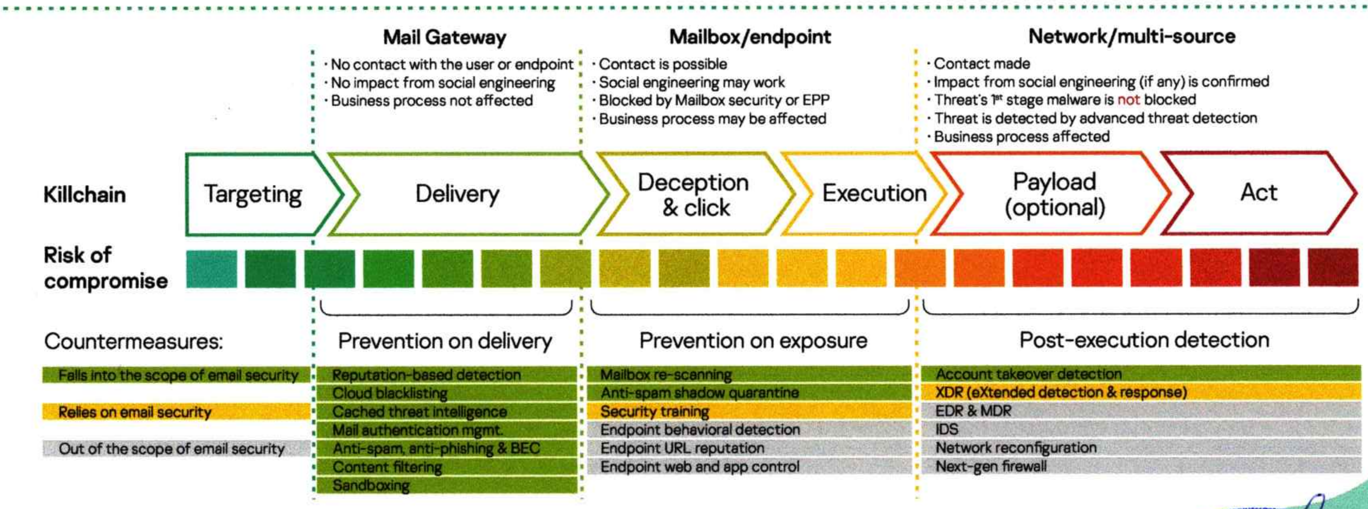
The solution supports clustered architectures in order to tackle growing traffic loads and ensure the resilience of the entire email security system in case of a disaster. To ensure that no critical data is lost due to disinfection, deletion or a technical mishap, original messages can be backed up according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

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

Risk of compromise

Countermeasures:

Countermeasures:	Prevention on delivery	Prevention on exposure	Post-execution detection
Falls into the scope of email security	Reputation-based detection	Mailbox re-scanning	Account takeover detection
	Cloud blacklisting	Anti-spam shadow quarantine	XDR (eXtended detection & response)
Relies on email security	Cached threat intelligence	Security training	EDR & MDR
	Mail authentication mgmt.	Endpoint behavioral detection	IDS
Out of the scope of email security	Anti-spam, anti-phishing & BEC	Endpoint URL reputation	Network reconfiguration
	Content filtering	Endpoint web and app control	Next-gen firewall
	Sandboxing		

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.

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.

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

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.

SOCIETATEA CU RĂSPUNDERE LIMITATĂ, REPUBLICA MOLDOVA, mun. CHIŞINĂU
S.R.L.
"BTS PRO"
Nr. 3
IDNO 1008600061565