

What makes your growing business stronger

kaspersky



Cybersecurity
for small and mid-
sized businesses

What's happening — and why it matters to your business

For SMBs today, running a business means running on digital systems. Cloud platforms, remote work, mobile devices, online tools and services and AI-driven automation make many aspects of day-to-day operations easier, but they also create more entry points for attackers.



More AI-powered attacks

AI enables low-cost, automated phishing and password attacks at scale



More tools, more entry points

Every new service adds another potential door into your business



Limited time and staff

Small IT teams can't monitor everything all the time



Work outside company control

Using personal accounts and devices for work places data outside corporate protection and increases compliance and financial risk

What puts your business at risk — inside and out

Most cyber incidents in SMBs don't start with dramatic attacks. They start with everyday decisions, routine tasks and common business challenges.

External and internal risks



Download dubious files somewhere on the internet →



Operations grind to a halt



Open a suspicious email with extra discounts for employees →



Stolen credentials, business disruption



Install unknown software with hidden malware running →



Data theft, unstable systems



Using compromised or untrusted third-party services →



Disruption to customers and a resulting loss of trust

Challenges



Skill shortage in incident handling →



Wrong decisions make situations worse



Postponing security investments →



Higher recovery costs later



Overloaded IT team responsible also for cybersecurity →



Missed threats and delayed response



Fast IT growth of endpoints and using services →



Security can't keep up

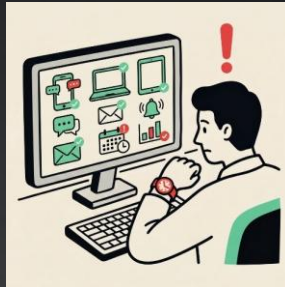
All these factors threaten business continuity and growth, leading to:

- potential financial losses
- data breaches
- and reputational damage.

Understand what can hold you back



You're 'too small to be a target'



You'll deal with it later when you have more time



You don't have resources and expertise to manage it



Security regulations don't really apply to you

But the right cybersecurity helps **overcome barriers and boost business growth**

Current security landscape for SMBs

43%

of attacks target SMBs*

≈ \$70 000

The average cost of an incident *

(data loss, phishing, ransomware, fraud, reputational damage)

1 week to 6 months



Potential downtime

What reliable security means for you

Early threat detection

Stop evasive threats before they become incidents

Automatic threat protection

Built-in protection against mass threats, reducing the need for manual response

Fast recovery if something goes wrong

Less downtime = more stability and less lost revenue

Lower workload for IT

Fewer manual tasks and mistakes, more time for what matters — with streamlined cloud-based deployment

Clear visibility

Know which devices, users and apps have access to your systems

Expert security – no need to build your own team

Strong protection without the cost and hassle of hiring specialists

Protection against social engineering

Awareness training that helps recognize scams, phishing and manipulation

Turn cybersecurity into a growth enabler



Business growth

Scale with confidence, seize new opportunities and build lasting customer and partner relationships.

Uninterrupted continuity

Prevent disruption and keep your business running smoothly

Efficient business operations

Reduce manual effort and become a less attractive target for attackers.



Strong security foundation

Multi-layered protection that defends your people, data and systems

Kaspersky Next Optimum

Core offering



Empowering your business with unmatched cybersecurity technologies and AI and human expertise — so you secure smarter and save bigger



MXDR Optimum

XDR Optimum

EDR Optimum

EDR Foundations



Security Awareness



Email Security



Workload Security



Vulnerability Management



Threat Lookup & Analysis

Expand Kaspersky Next Optimum with **security modules** as your needs evolve



Additional solutions to enhance protection with special pricing terms are available for new and existing Next Optimum customers

How Kaspersky addresses threats and challenges



How Kaspersky addresses threats and challenges

	 Kaspersky Next EDR Foundations	 Kaspersky Next EDR Optimum	 Kaspersky Next XDR Optimum	 Kaspersky Next MXDR Optimum
 Malware + <i>Common threats</i>	•	•	•	•
 Ransomware	•	•	•	•
 Fileless attacks	•	•	•	•
 Phishing	•	•	•	•
 Unknown malware <i>New & targeted</i>		•	•	•
 Human error		•	•	•
 Uncontrolled third parties		•	•	•
 Social engineering			•	•
 Lateral movement			•	•
 Lack of resources				•
 Business continuity				•

*Managed
service from
Kaspersky
experts*



How security modules cover specific security challenges

	 Security Awareness	 Email Security	 Workload Security	 Vulnerability Management	 Threat Lookup & Analysis
 Phishing and social engineering	●	●			
 Sensitive data exposure	●				
 Unknown or suspicious files		●			●
 Cloud workload exposure			●		
 Vulnerabilities and misconfigurations			●	●	
 External threat visibility				●	●

How Kaspersky addresses ransomware

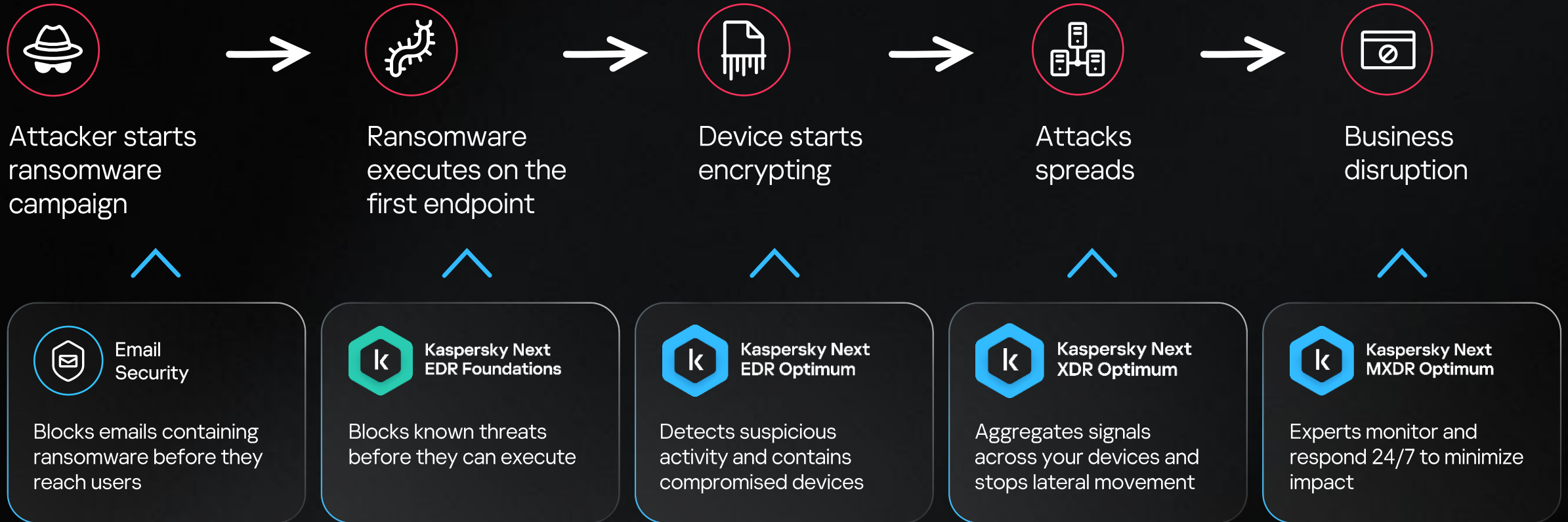


*Download dubious files
somewhere on the internet*



Operations grind to a halt

Stronger defense at every step of the ransomware path



Each layer adds another opportunity to stop a ransomware attack

Stronger defense at every step of the ransomware path



Don't let ransomware interrupt your business



Email
Security

Blocks emails containing ransomware before they reach users



Kaspersky Next
EDR Foundations

Blocks known threats before they can execute



Kaspersky Next
EDR Optimum

Detects suspicious activity and contains compromised devices



Kaspersky Next
XDR Optimum

Aggregates signals across your devices and stops lateral movement



Kaspersky Next
MXDR Optimum

Experts monitor and respond 24/7 to minimize impact

Each layer adds another opportunity to stop a ransomware attack

Step-by-step protection against ransomware

How protection works

What happens

Initial access

A malicious attachment is opened, or a download triggers ransomware

Encryption attempt

Encryption starts on one device

Lateral movement attempt

Ransomware spreads across other endpoints

Prevention



Kaspersky Next
EDR Foundations

Blocks known threats thanks to multi-layered anti-malware and exploit prevention

Captures how it started with root cause analysis

Stops or rollbacks malicious activity where possible with behavior detection and remediation engine

Limits propagation techniques through host intrusion prevention (HIPS) and exploit prevention

Step-by-step protection against ransomware

How protection works

What happens

Initial access

A malicious attachment is opened, or a download triggers ransomware

Encryption attempt

Encryption starts on one device

Lateral movement attempt

Ransomware spreads across other endpoints

Advanced investigation and response



Kaspersky Next
EDR Optimum

Blocks known threats thanks to multi-layered anti-malware and exploit prevention

Captures how it started with root cause analysis

Catches and prevents unusual user activity with Adaptive anomaly control

Checks if compromise already exists elsewhere after IoC-scanning

Stops or rollbacks malicious activity where possible with behavior detection and remediation engine

Accelerates containment and cleanup the consequences with guided and automate response

Limits propagation techniques through host intrusion prevention (HIPS) and exploit prevention

Get the fast isolation and remediation from console thanks to remote troubleshooting

Step-by-step protection against ransomware

How protection works

What happens

Initial access

A malicious attachment is opened, or a download triggers ransomware

Encryption attempt

Encryption starts on one device

Lateral movement attempt

Ransomware spreads across other endpoints

Extended capabilities



Kaspersky Next
XDR Optimum

Blocks known threats thanks to multi-layered anti-malware and exploit prevention

Captures how it started with root cause analysis

Catches and prevents unusual user activity with Adaptive anomaly control

Checks if compromise already exists elsewhere after IoC-scanning

Validates suspicious objects thorough Cloud Sandbox request

Stops or rollbacks malicious activity where possible with behavior detection and remediation engine

Accelerates containment and cleanup the consequences with guided and automate response

Limits account-based spread thanks to response via Active Directory

Limits propagation techniques through host intrusion prevention (HIPS) and exploit prevention

Get the fast isolation and remediation from console thanks to remote troubleshooting

Turn distributed signals across infrastructure to the meaningful picture of spreading with alert aggregation

Step-by-step protection against ransomware

How protection works

What happens

Initial access

A malicious attachment is opened, or a download triggers ransomware

Encryption attempt

Encryption starts on one device

Lateral movement attempt

Ransomware spreads across other endpoints

Managed protection



Kaspersky Next
MXDR Optimum

Blocks known threats thanks to multi-layered anti-malware and exploit prevention

Captures how it started with root cause analysis

Catches and prevents unusual user activity with Adaptive anomaly control

Checks if compromise already exists elsewhere after IoC-scanning

Validates suspicious objects thorough Cloud Sandbox request

Kaspersky experts validate whether it's ransomware or false positive, and set incident priority

Stops or rollbacks malicious activity where possible with behavior detection and remediation engine

Accelerates containment and cleanup the consequences with guided and automate response

Limits account-based spread thanks to response via Active Directory

Experts supervise containment steps and confirm encryption activity is fully stopped

Limits propagation techniques through host intrusion prevention (HIPS) and exploit prevention

Get the fast isolation and remediation from console thanks to remote troubleshooting

Turn distributed signals across infrastructure to the meaningful picture of spreading with alert aggregation

Coordinated expert-led response ensures all affected hosts are covered and no missed endpoints remain



Email
Security

Secure your business communications and sensitive data

*Extended mail protection
before attacks start*



Detect email-borne threats,
malicious attachments and
unauthorized data sharing



Reduce the risk of business
disruption, financial losses due
to scams, and data leaks



Get visibility into cloud data
and control data exchange
across email and data
platforms

Multiple deployment scenarios

Protect on-premise, SaaS or hybrid email
infrastructures with a single solution

Multi-layered protection for corporate email

Get full visibility across your email
infrastructure with robust mail security
technologies

Data access and sharing control

Control how sensitive data is accessed,
shared and transferred across email

What business and IT teams gain



Protection against
ransomware



Business



Keep business operations running with minimal disruption



Stay focused on growth instead of recovering from attacks

IT or small cybersecurity teams



Detect and isolate threats before they spread



Respond quickly with clear remediation guidance

How Kaspersky addresses **malware** and **fileless attacks**

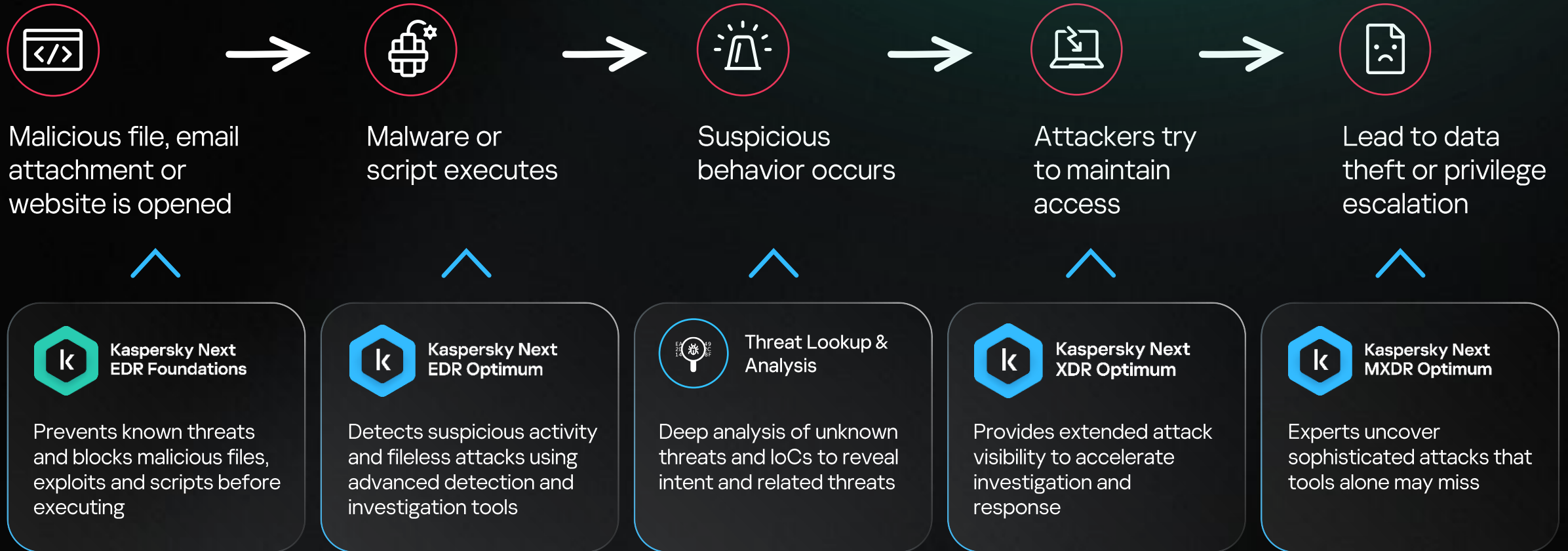


Install unknown software with hidden malware running



Data theft, unstable systems

Continuous protection against malware and fileless attacks



Every solution strengthens your protection

Continuous protection against malware and fileless attacks



**Attack contained.
Data and systems protected.**



**Kaspersky Next
EDR Foundations**

Prevents known threats and blocks malicious files, exploits and scripts before executing



**Kaspersky Next
EDR Optimum**

Detects suspicious activity and fileless attacks using advanced detection and investigation tools



**Threat Lookup &
Analysis**

Deep analysis of unknown threats and IoCs to reveal intent and related threats



**Kaspersky Next
XDR Optimum**

Provides extended attack visibility to accelerate investigation and response



**Kaspersky Next
MXDR Optimum**

Experts uncover sophisticated attacks that tools alone may miss

Every solution strengthens your protection

Step up your defense against malware and fileless attacks

What happens

Initial infection

User opens infected content or script

Fileless execution

Malicious scripts runs in memory without file on disk

Internal propagation

Threat attempts spread across endpoints or contact external servers

Escalation

Attackers try to maintain access or escalate privileges

How protection works

Core protection



Kaspersky Next
EDR Foundations

Automatically blocks malicious activity or suspicious process due to file, mail and web protection
Blocks malicious script execution before it runs with Anti-malware scan interface (AMSI)

Identifies suspicious runtime activity with behavior detection
Script monitoring tracks execution chains

Stops suspicious connections through network protection
Stops harmful actions to the OS with Host Intrusion Prevention (HIPS)
Limits propagation techniques via Exploit prevention

Root cause analysis shows how an attack chains develops
Remediation engine rolls back malicious actions

Step up your defense against malware and fileless attacks

What happens

Initial infection

User opens infected content or script

Fileless execution

Malicious scripts runs in memory without file on disk

Internal propagation

Threat attempts spread across endpoints or contact external servers

Escalation

Attackers try to maintain access or escalate privileges

How protection works

Active response



Kaspersky Next
EDR Optimum

Automatically blocks malicious activity or suspicious process due to file, mail and web protection
Blocks malicious script execution before it runs with Anti-malware scan interface (AMSI)

Automatically detect dubious process behavior if malware bypass signature thanks to Adaptive anomaly control

Identifies suspicious runtime activity with behavior detection
Script monitoring tracks execution chains

Guided response enable rapid containment
Prevents success unauthorized access due to remote troubleshooting

Stops suspicious connections through network protection
Stops harmful actions to the OS with Host Intrusion Prevention (HIPS)
Limits propagation techniques via Exploit prevention

Supports fast isolation and remediation from console with remote troubleshooting

Root cause analysis shows how an attack chains develops
Remediation engine rolls back malicious actions

Verifies environment for related artefacts through IoC scanning

Step up your defense against malware and fileless attacks

What happens

Initial infection

User opens infected content or script

Fileless execution

Malicious scripts runs in memory without file on disk

Internal propagation

Threat attempts spread across endpoints or contact external servers

Escalation

Attackers try to maintain access or escalate privileges

How protection works

Extended visibility



Kaspersky Next
XDR Optimum

Automatically blocks malicious activity or suspicious process due to file, mail and web protection
Blocks malicious script execution before it runs with Anti-malware scan interface (AMSI)

Automatically detect dubious process behavior if malware bypass signature thanks to Adaptive anomaly control

Detonates suspicious object and confirms malicious verdict through Cloud Sandbox

Identifies suspicious runtime activity with behavior detection
Script monitoring tracks execution chains

Guided response enable rapid containment
Prevents success unauthorized access due to remote troubleshooting

Provides wide visibility across the infrastructure based on alert aggregation

Stops suspicious connections through network protection
Stops harmful actions to the OS with Host Intrusion Prevention (HIPS)
Limits propagation techniques via Exploit prevention

Supports fast isolation and remediation from console with remote troubleshooting

Disable compromised attacks in one click thanks to integration with Active Directory

Root cause analysis shows how an attack chains develops
Remediation engine rolls back malicious actions

Verifies environment for related artefacts through IoC scanning

Alert aggregation ensures no recurring harmful activity

Step up your defense against malware and fileless attacks

What happens

How protection works

Managed protection



Kaspersky Next
MXDR Optimum

Initial infection

User opens infected content or script

Automatically blocks malicious activity or suspicious process due to file, mail and web protection
Blocks malicious script execution before it runs with Anti-malware scan interface (AMSI)

Automatically detect dubious process behavior if malware bypass signature thanks to Adaptive anomaly control

Detonates suspicious object and confirms malicious verdict through Cloud Sandbox

Kaspersky experts verify the scale of more evasive incident and prioritize real threats

Fileless execution

Malicious scripts runs in memory without file on disk

Identifies suspicious runtime activity with behavior detection
Script monitoring tracks execution chains

Guided response enable rapid containment
Prevents success unauthorized access due to remote troubleshooting

Provides wide visibility across the infrastructure based on alert aggregation

Ongoing expert-led monitoring of stealth behavior
Guided remediation support ensures full containment

Internal propagation

Threat attempts spread across endpoints or contact external servers

Stops suspicious connections through network protection
Stops harmful actions to the OS with Host Intrusion Prevention (HIPS)
Limits propagation techniques via Exploit prevention

Supports fast isolation and remediation from console with remote troubleshooting

Disable compromised attacks in one click thanks to integration with Active Directory

Coordinated expert-led and rapid response stops hidden spread

Escalation

Attackers try to maintain access or escalate privileges

Root cause analysis shows how an attack chains develops
Remediation engine rolls back malicious actions

Verifies environment for related artefacts through IoC scanning

Alert aggregation ensures no recurring harmful activity

Kaspersky team confirms full attack elimination and prevents similar attacks



Threat
Lookup &
Analysis*

Enhance threat investigation and analysis



Detect previously unknown threats
through deep analysis



Improve visibility into threats and
indicators of compromise (IoCs)



Strengthen investigation
with enriched context

Analyze threats

Detonate suspicious objects in an isolated cloud environment, identify similar malware and find out specific APTs behind them

Get the full picture

Enrich investigations with insights from all sources, including surface, deep, and dark web, as well as open-source data using GenAI

Boost your investigation flow

Improve understanding of threats with extended context and unique data

* An additional solution based on the particular functionalities of Kaspersky Threat Lookup and Kaspersky Threat Analysis Requests to enhance protection with special pricing terms are available for new and existing Next Optimum customers.

What business and IT teams gain



Protection against malware, mass and fileless attacks



Business



Fewer disruptions caused by malware



Lower risk of data loss and system downtime

IT or small cybersecurity teams



Spend less time investigating routine threats, with automatic detection of known threats



Faster response without the need for deep investigation expertise in-house

How Kaspersky addresses phishing and social engineering



Open a suspicious email with extra discounts for employees



Stolen credentials, business disruption

Unbeatable protection against human-related threats



Each solution is built to expand your protection

Unbeatable protection against human-related threats



No successful phishing attacks.
Business keeps running smoothly.



Email
Security

Blocks phishing emails and harmful links before they reach users



Security
Awareness

Equips employees to recognize and avoid phishing attacks



Kaspersky Next
EDR Foundations

Detects suspicious activity and fileless attacks using advanced detection and investigation tools



Kaspersky Next
EDR Optimum

Deep analysis of suspicious activity to understand its scope and contain threats faster



Kaspersky Next
XDR Optimum

Disable or restrict compromised accounts to prevent further spread



Kaspersky Next
MXDR Optimum

Kaspersky experts investigate across endpoints to confirm the threat has been fully removed

Each solution is built to expand your protection

When employees make mistakes, security takes over

What happens

Phishing delivery

User receives a malicious email or clicks a suspicious link

Payload execution

User opens an attachment or runs a downloaded file

Credential compromise

User enters personal credentials — compromised account used by attackers

Post-compromise activity

Attackers attempt internal misuse or privilege escalation

How protection works

Prevention



Kaspersky Next
EDR Foundations

Blocks known phishing links and attachments with file, mail and web protection

Multi-layered anti-malware protection scans downloaded content for hidden risks

Collects illegitimate activity on the endpoint level using behavior detection

Exploit prevention stops privilege escalation attempts

Stops malicious process and rolls back illegitimate changes via the remediation engine

Blocks unauthorized activities with Host Intrusion Prevention (HIPS)

Network threat protection stops suspicious outbound connections

Root cause analysis reconstructs the full execution chain

When employees make mistakes, security takes over

What happens

Phishing delivery

User receives a malicious email or clicks a suspicious link

Payload execution

Users opens an attachment or runs a downloaded file

Credential compromise

User enters personal credentials – compromised account used by attackers

Post-compromise activity

Attackers attempt internal misuse or privilege escalation

How protection works

Investigate and respond



Kaspersky Next
EDR Optimum

Blocks known phishing links and attachments with file, mail and web protection

Multi-layered anti-malware protection scans downloaded content for hidden risks

Security for Microsoft O365 filters phishing emails at cloud level before they reach users

Collects illegitimate activity on the endpoint level using behavior detection

Exploit prevention stops privilege escalation attempts

Accelerates containment with guided response

Stops malicious process and rolls back illegitimate changes via the remediation engine

Verify the scope of compromise running IoC scanning

Enable fast isolation and remediation from console with remote troubleshooting

Blocks unauthorized activities with Host Intrusion Prevention (HIPS)

Network threat protection stops suspicious outbound connections

Root cause analysis reconstructs the full execution chain

Encryption management protects sensitive information from exposure

Discard corporate data from compromised device through remote wipe

When employees make mistakes, security takes over

What happens

Phishing delivery

User receives a malicious email or clicks a suspicious link

Payload execution

Users opens an attachment or runs a downloaded file

Credential compromise

User enters personal credentials – compromised account used by attackers

Post-compromise activity

Attackers attempt internal misuse or privilege escalation

How protection works

Expand visibility



Kaspersky Next
XDR Optimum

Blocks known phishing links and attachments with file, mail and web protection

Multi-layered anti-malware protection scans downloaded content for hidden risks

Security for Microsoft O365 filters phishing emails at cloud level before they reach users

Detonates suspicious objects and confirms malicious verdicts in a safe environment (Cloud Sandbox)

Collects illegitimate activity on the endpoint level using behavior detection

Exploit prevention stops privilege escalation attempts

Accelerates containment with guided response

Centralizes visibility across all affected endpoints with alert aggregation

Stops malicious process and rolls back illegitimate changes via the remediation engine

Verify the scope of compromise running IoC scanning

Enable fast isolation and remediation from console with remote troubleshooting

Disable or restrict compromised accounts with response via Active Directory

Blocks unauthorized activities with Host Intrusion Prevention (HIPS)

Network threat protection stops suspicious outbound connections

Root cause analysis reconstructs the full execution chain

Encryption management protects sensitive information from exposure

Discard corporate data from compromised device through remote wipe

Assigned course via Security Awareness Platform to reduce click-rate and credential disclosure risk

When employees make mistakes, security takes over

How protection works

What happens

Phishing delivery

User receives a malicious email or clicks a suspicious link

Payload execution

Users opens an attachment or runs a downloaded file

Credential compromise

User enters personal credentials – compromised account used by attackers

Post-compromise activity

Attackers attempt internal misuse or privilege escalation

Expert support



Kaspersky Next
MXDR Optimum

Blocks known phishing links and attachments with file, mail and web protection

Multi-layered anti-malware protection scans downloaded content for hidden risks

Security for Microsoft O365 filters phishing emails at cloud level before they reach users

Detonates suspicious objects and confirms malicious verdicts in a safe environment (Cloud Sandbox)

Kaspersky experts validate phishing scope targeting multiple users

Analysts validate malicious intent and initiate incident workflow

Collects illegitimate activity on the endpoint level using behavior detection

Exploit prevention stops privilege escalation attempts

Accelerates containment with guided response

Centralizes visibility across all affected endpoints with alert aggregation

Security analysts investigate suspicious process chains

Confirm exploit attempt and validate containment actions

Stops malicious process and rolls back illegitimate changes via the remediation engine

Verify the scope of compromise running IoC scanning

Enable fast isolation and remediation from console with remote troubleshooting

Disable or restrict compromised accounts with response via Active Directory

Experts analyze abnormal behavior patterns and initiate coordinated response

Blocks unauthorized activities with Host Intrusion Prevention (HIPS)

Network threat protection stops suspicious outbound connections

Root cause analysis reconstructs the full execution chain

Encryption management protects sensitive information from exposure

Discard corporate data from compromised device through remote wipe

Assigned course via Security Awareness Platform to reduce click-rate and credential disclosure risk

Kaspersky team conducts cross-endpoint investigation to confirm no persistence remains



Security
Awareness

Turn employees into your strongest defense against cyberattacks

*Your strongest defense
against social
engineering*



Reduce awareness management effort and lighten the load on IT



Engage employees in protecting business data



Help employees recognize and respond to cyberthreats

Accessible, interactive learning

Help employees recognize and respond to cyberthreats

Lasting behavioral change

Reinforce secure behaviors until they become routine

Engagement across the board

Role-based training for everyone, from executives to frontline employees



Email
Security

Secure your business communications and sensitive data

*Extended mail protection
before attacks start*



Detect email-borne threats,
malicious attachments and
unauthorized data sharing



Reduce the risk of business
disruption, financial losses due
to scams, and data leaks



Get visibility into cloud data
and control data exchange
across email and data
platforms

Multiple deployment scenarios

Protect on-premise, SaaS or hybrid email
infrastructures with a single solution

Multi-layered protection of corporate email

Get full visibility across your email
infrastructure using robust mail security
technologies

Data access and sharing control

Control how sensitive data is accessed,
shared and transferred across email

What business and IT teams gain



Protection against
human-driven attacks



Business



Reduced risk of credential theft
and fraud



Long-term resilience against social
engineering

IT or small cybersecurity teams

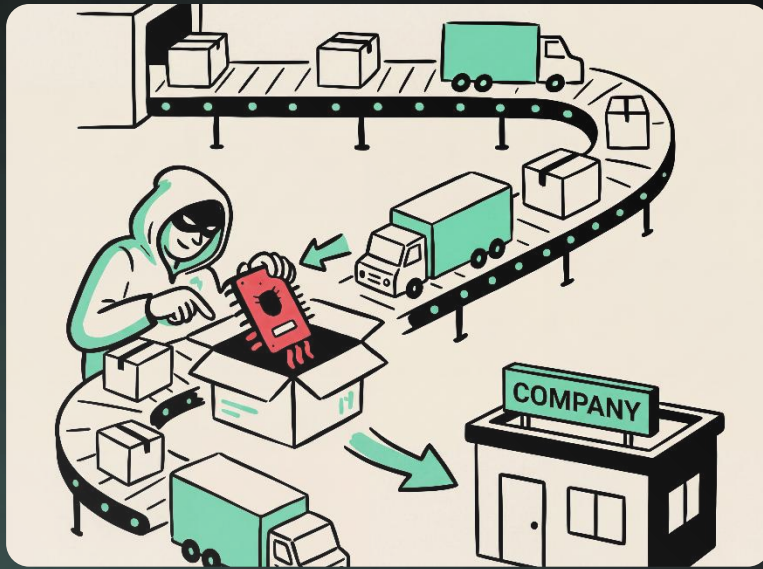


Less time spent recovering from phishing
attacks

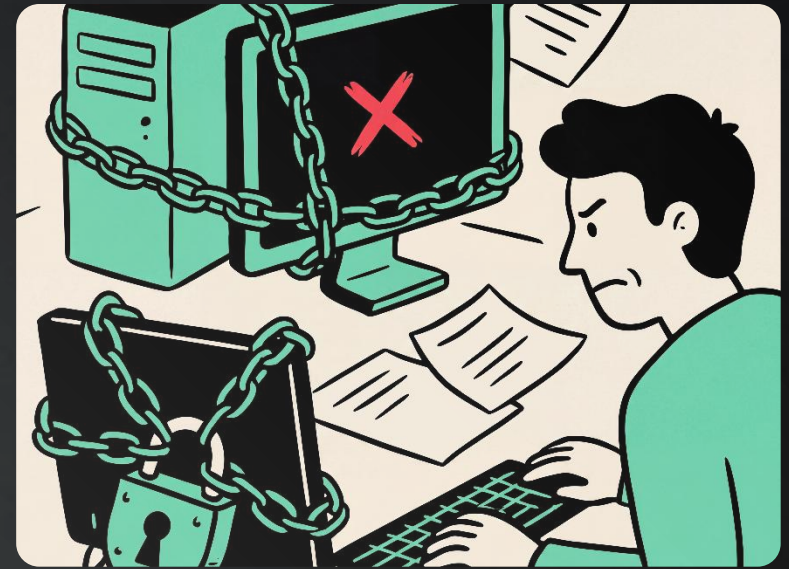


Fewer alerts = more time for strategic
work

How Kaspersky addresses unauthorised third-party risks



*Using compromised or untrusted
third-party services*



*Disruption to customers
and a resulting loss of trust*

Control the risk of third-party access

Each solution expands your protection



Third party is onboarded



**Kaspersky Next
EDR Foundations**

Know which third parties have access to your environment.



Legitimate access is used to perform tasks and processes



**Kaspersky Next
EDR Optimum**

Detect abnormal behavior, policy violations and risky accounts



Unusual behavior appears



**Kaspersky Next
XDR Optimum**

Correlate activity across your environment to understand attack scope and respond faster



Access is abused or moves laterally



**Kaspersky Next
MXDR Optimum**

Our experts investigate and respond 24/7 to contain threats before they spread



Protection for hybrid environments



**Workload
Security**

Discovers hybrid cloud assets and monitors their security posture

Protects cloud environments from exploits and other attacks

Detects unauthorized file changes and suspicious activity

Helps identify risks before they affect hybrid cloud operations



**Protects at
every stage**



Full visibility

Know who has access – and what they're doing



Early detection

Catch suspicious activity before it becomes a threat



Rapid response

Respond quickly to contain threats where they matter most

Reliable protection against unauthorized third-party access



* Root cause analysis and other capabilities are available in Next EDR Foundations. Next EDR Optimum builds on these with broader capabilities and more comprehensive risk coverage.



Workload
Security*

Protect your hybrid cloud environment with ease

Best-fit for cloud environments



Protect your hybrid cloud infrastructure from the broadest range of cyberattacks



Comply with regulatory requirements, even in highly regulated industries



Multi-layered protection with minimal false positives

360° overview in multi-cloud

A unified cloud console eliminates blind spots and saves time and resources on incident investigations

File Integrity Monitoring

Monitor file attributes and scan in real-time or to schedule to compliance with industry regulations and standards

Cost-efficient protection

Choose only the options you need and save resources through automation and ML/AI

* An additional solution based on Kaspersky Hybrid Cloud Security to enhance protection with special pricing terms are available for new and existing Next Optimum customers.

What business and IT teams gain



Visibility into
third-party risks



Business



Less risk of disruptions caused by third-parties



Trust from customers and business partners

IT or small cybersecurity teams

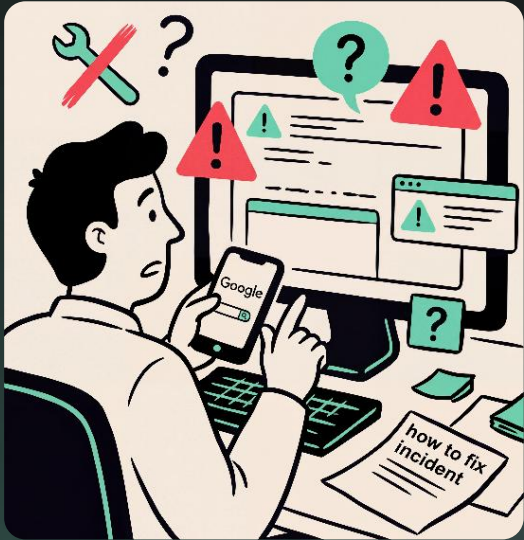


Early warning of exposed assets and hidden risks



Fewer blind spots beyond the corporate perimeter

How Kaspersky addresses internal limitations



Skill shortage in incident handling



Overloaded IT team responsible also for cybersecurity



Postponing security investments



Fast IT growth of endpoints and using services

Security that fits your resources

Built to help your business overcome security challenges as they evolve



**Kaspersky Next
EDR Foundations**

Automates protection against common threats, centralizes security management and reduces operational workload with vulnerability assessment



**Kaspersky Next
EDR Optimum**

Accelerates investigation and response with guided workflows while helping IT teams build incident response skills



**Kaspersky Next
XDR Optimum**

Reduces investigation complexity by correlating alerts and providing the context needed for faster decisions



**Kaspersky Next
MXDR Optimum**

Extend your team with 24/7 security experts who monitor, investigate and respond when internal resources are limited



**Vulnerability
Management**

Reduces the number of incidents your team needs to handle by continuously identifying, prioritizing and helping remediate vulnerabilities before attackers can exploit them



**Scale protection
without scaling
complexity**



Easy to manage
Centralized, easy-to-
use protection



Less manual work
Automate routine
security tasks



Higher efficiency
Focus your resources
where they matter most

Overcome internal security challenges with the right level of protection ⁴⁹

Common challenges	 Kaspersky Next EDR Foundations	 Kaspersky Next EDR Optimum	 Kaspersky Next XDR Optimum	 Kaspersky Next MXDR Optimum
Overloaded IT teams also responsible for cybersecurity	Multi-layered, automated protection reduces manual effort	Accelerate threat containment with guided and automated response	Stop attacks from spreading with response options via Active Directory integration	24/7 monitoring and response against evasive attacks
Rapid growth in endpoints and services	Centralized visibility of applications and missing patches on corporate devices with vulnerability assessment	Patch management and cloud security support growing environments	Centralized visibility beyond endpoints, supporting distributed infrastructure	Scale managed services at any time as your business grows
Shortage of skills in incident handling		Build incident response skills with dedicated cybersecurity training for IT administrators	Empower your team with user-friendly tools that simplify investigations – alert aggregation, richer context and faster containment	On-demand incident response assistance from Kaspersky experts
Postponed security investments			Build a stronger security culture with integrated awareness training	Gain expert protection while keeping EDR and XDR capabilities in-house — in a single, cost-effective solution



Vulnerability
Management*

Identify and remediate vulnerabilities across your infrastructure



Comprehensive visibility and control
of assets and vulnerabilities



Faster response cycles and reduced
mean time to remediate
vulnerabilities



Reduced risk of
compliance gaps

Context-aware vulnerability prioritization

Prioritize vulnerabilities using expert,
real-world threat intelligence

Agent-based vulnerability scanning

Perform in-depth vulnerability analysis
without exposing service account
credentials

Unified vulnerability and patch management

Manage the entire vulnerability lifecycle –
from detection to remediation – in a single
platform

* An additional solution based on Kaspersky Vulnerability Management to enhance protection with special pricing terms are available for new and existing Next Optimum customers

What business and IT teams gain



Security that works
with minimal effort



Business



Maintain stable operations even with limited internal resources



Lower the cost of incidents and recovery

IT or small cybersecurity teams

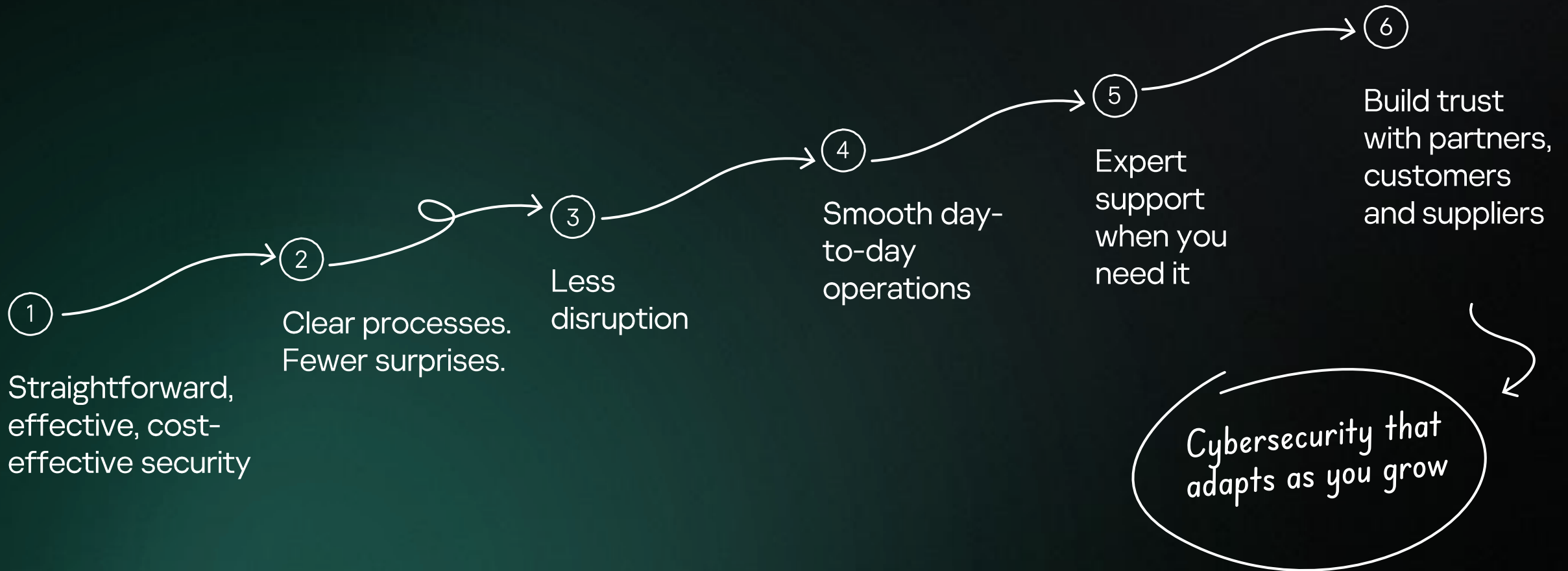


Fewer alerts and less manual work



Free up time for core IT work while experts handle security

Stay in the groove – grow with confidence



Why growing businesses choose Kaspersky Next Optimum

Prevent more

Stop more attacks before they need to be investigated

Manage less

Spend less time managing security and more time growing your business

Scale smarter

Expand your security without scaling complexity

And trust

Proven industry-leading protection recognized by independent testing



Transparent & independently acknowledged



**Proven.
Transparent.
Independent.**

The Kaspersky Global Transparency Initiative is built on concrete, actionable measures that allow stakeholders to validate and verify the trustworthiness of our products, internal processes and business operations.

13

Transparency
Centers across
the world



Regular independent
assessments

- SOC 2 audit
- ISO 27001 certification



Bug bounty
program

[Learn more](#)

Recognition that matters

Kaspersky products undergo regular independent assessments by leading research firm, with our cybersecurity expertise consistently recognized by top industry analysts worldwide

Most tested. Most awarded.

For over a decade, Kaspersky products have participated in 1122 independent tests and reviews, earning 861 first place results and 965 top-three finishes - testament to our industry-leading protection.

In 2025

100

tests & reviews

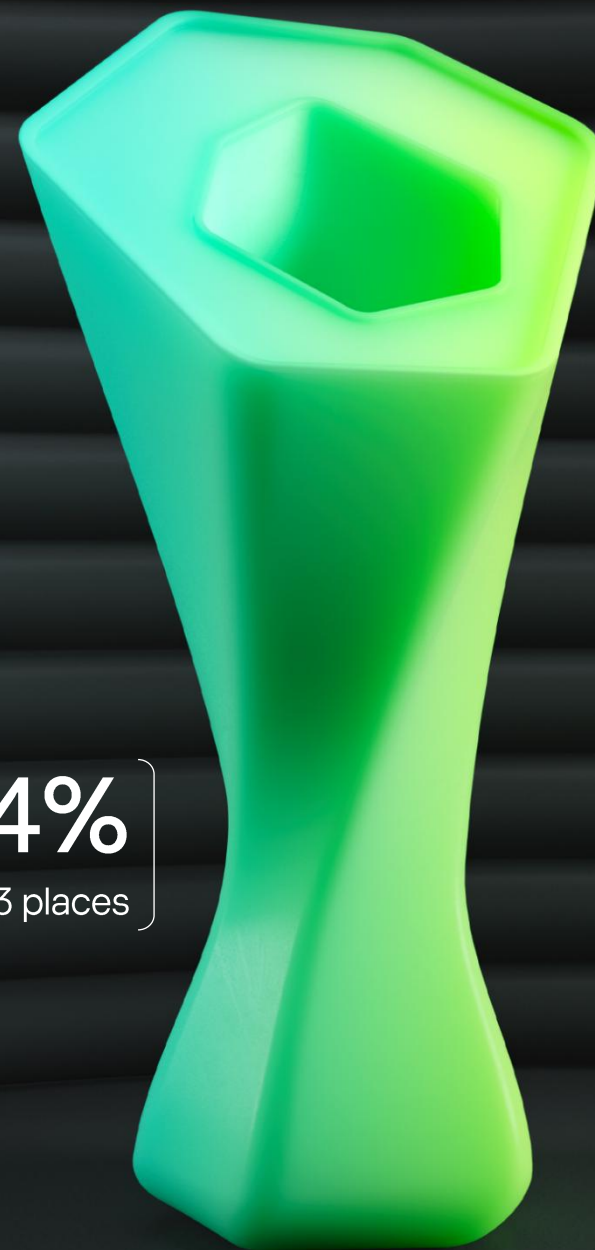
90

first places

94%

TOP3 places

[Learn more](#)



AI at the core of our portfolio

Dedicated AI Technology Research Center

Key focus areas:



Integrating AI into
cybersecurity solutions



Developing techniques to enhance
the security and responsible use of AI



Tracking AI-enabled threats to
anticipate emerging attack
vectors



Conducting GenAI research using
Kaspersky's large language model
(LLM) infrastructure



Establishing guidelines for the safe deployment of AI
systems

[Learn more](#)

AI
Technology
Research



An active industry contributor

56

As a key and active player in global threat intelligence, we work closely with the wider cybersecurity community to combat cybercrime worldwide.



MITRE | ATT&CK®

We contribute critical cyberthreat intelligence to global initiatives, including MITRE, to enhance the accuracy of the ATT&CK framework.



We work alongside international organizations such as INTERPOL, law enforcement agencies, CERTs and the global IT security community on joint cybercrime investigations and operations.



Kaspersky strengthens security across the industry by identifying and helping to fix zero-day vulnerabilities for leading brands including Adobe, Microsoft, Google, Apple and others.

NEW 2025

Google
CVE-2025-2783

kaspersky



Tailored security for
growing business

Explore

Learn more about
our solutions for SMBs