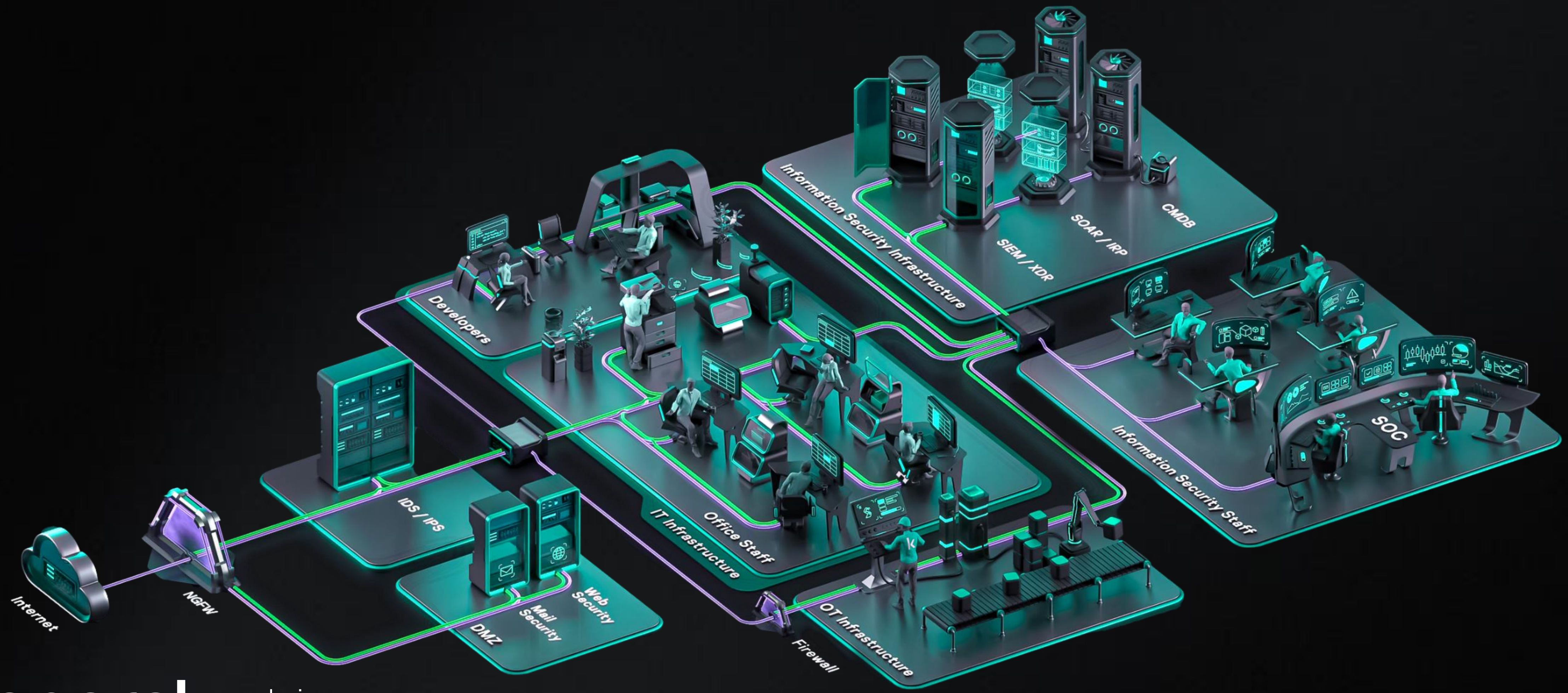


kaspersky bring on the future

Brandon Muller – Senior Technical Consultant **- META**

Technology leadership built on global expertise and AI-driven innovation

Research and investigation

World-leading threat research and incident investigation are at the heart of our portfolio.

Our unparalleled global expertise keeps customers ahead of evolving threats and fully supported throughout the incident response cycle.

Secure AI-powered approach

A security-first approach to artificial intelligence is built into our solutions.

From AI-enhanced threat discovery and alert triage to GenAI-driven threat intelligence. We've been pioneering AI in cybersecurity for years — and we're leading the way.

Secure software development

From a secure software development lifecycle to secure-by-design principles.

Security is embedded in every stage of our product development. Our rigorous approach ensures resilient, secure systems that keep customers protected.

~5,000

highly qualified specialists

50%

employees in R&D

50+

globally recognized cybersecurity experts

5

Unique Expertise Centers

Unmatched expertise

Our unique team of experts work together across **five Expertise Centers**, combining specialized knowledge and skills to tackle the most sophisticated, dangerous cyberthreats. This collaborative approach strengthens our state-of-the-art protection technologies and ensures our products and solutions set the industry standard for security and reliability.

GREAT

AI Technology Research

Threat Research

Security Services

Expertise Centers

ICS CERT

Active industry contributor

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

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

MITRE | ATT&CK®

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

Our work is guided by the ethical principles of responsible vulnerability disclosure.

Kaspersky strengthens security across the industry by identifying and helping to fix zero-day vulnerabilities for leading companies such as Adobe, Microsoft, Google, Apple, etc.

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

Learn more

Bug bounty

Recognition that matters

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

Most tested. Most awarded.

For over a decade, Kaspersky products have participated in 1022 independent tests and reviews, earning 771 first place results and 871 top-three finishes - testament to our industry-leading protection.

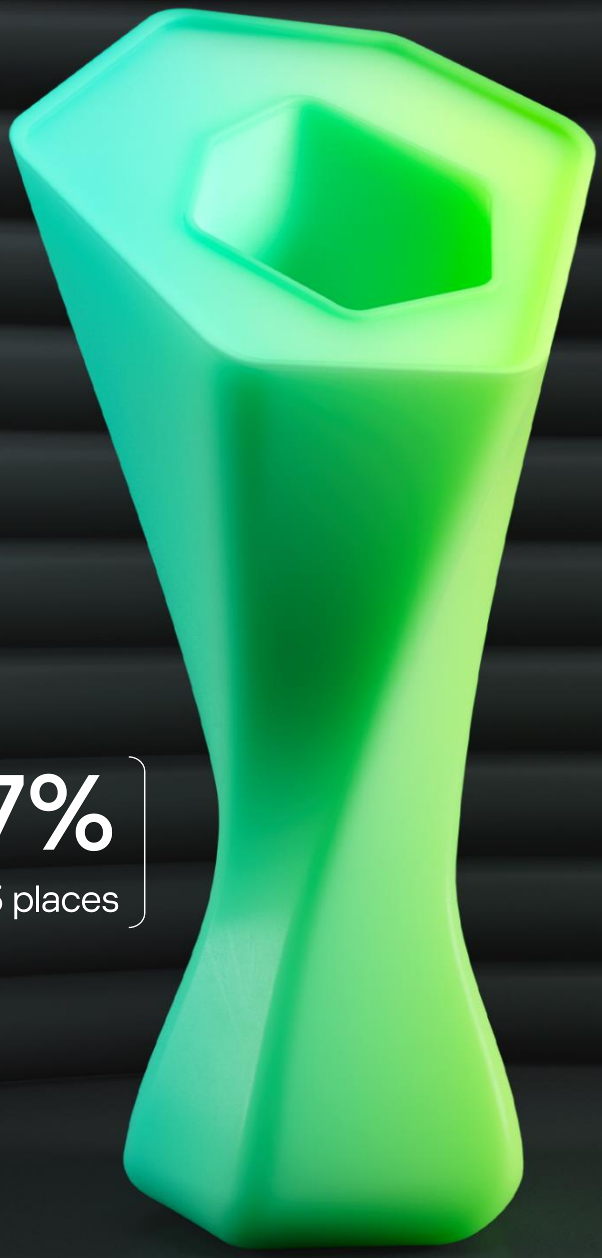
In 2024

95
Tests & reviews

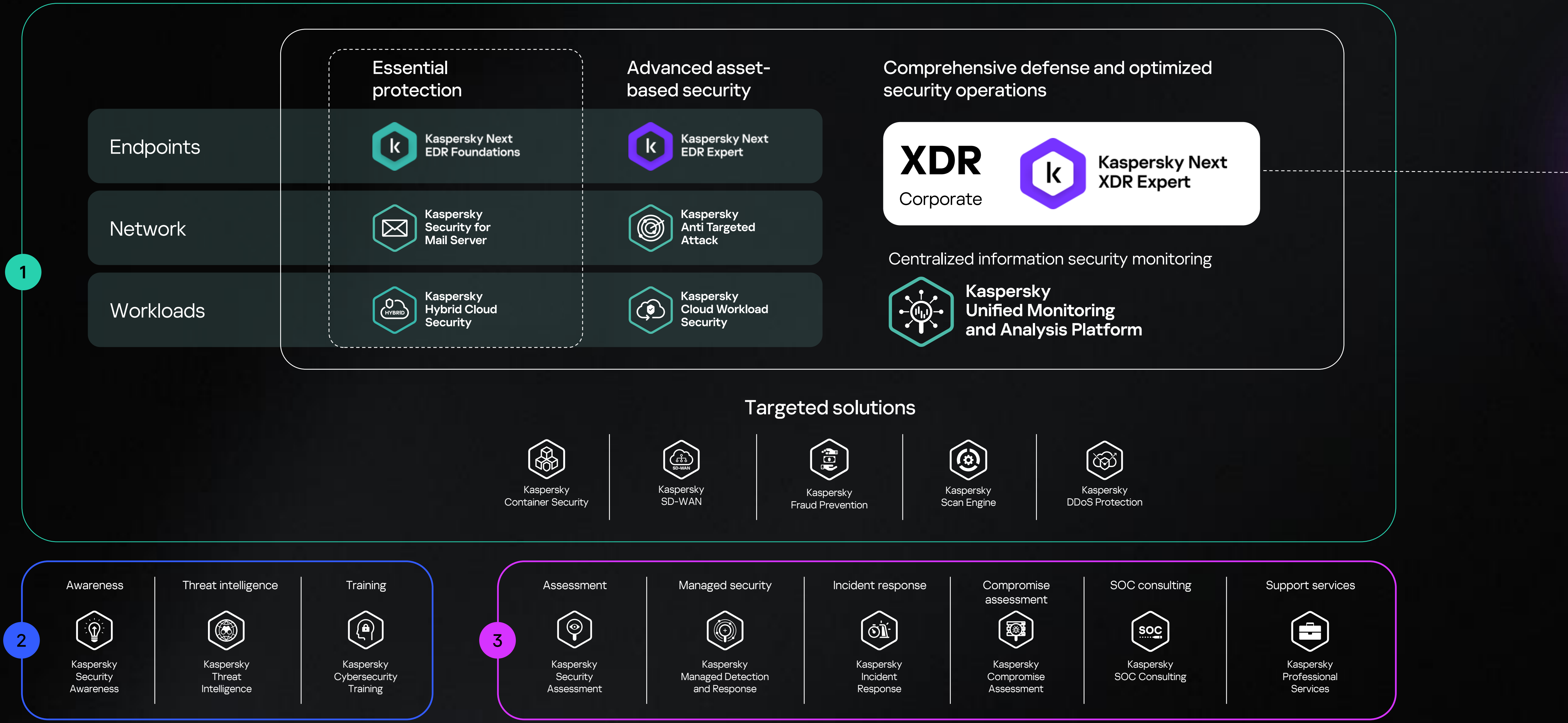
91
First places

97%
TOP3 places

Learn more



Kaspersky for IT environments



1

Essential protection

Advanced asset-based security

Comprehensive defense and optimized security operations

	Essential protection	Advanced asset-based security
Endpoints	Kaspersky Next EDR Foundations	Kaspersky Next EDR Expert
Network	Kaspersky Security for Mail Server	Kaspersky Anti Targeted Attack
Workloads	Kaspersky Hybrid Cloud Security	Kaspersky Cloud Workload Security

XDR Corporate

Kaspersky Next XDR Expert

Centralized information security monitoring

Kaspersky Unified Monitoring and Analysis Platform

Targeted solutions

- Kaspersky Container Security
- Kaspersky SD-WAN
- Kaspersky Fraud Prevention
- Kaspersky Scan Engine
- Kaspersky DDoS Protection

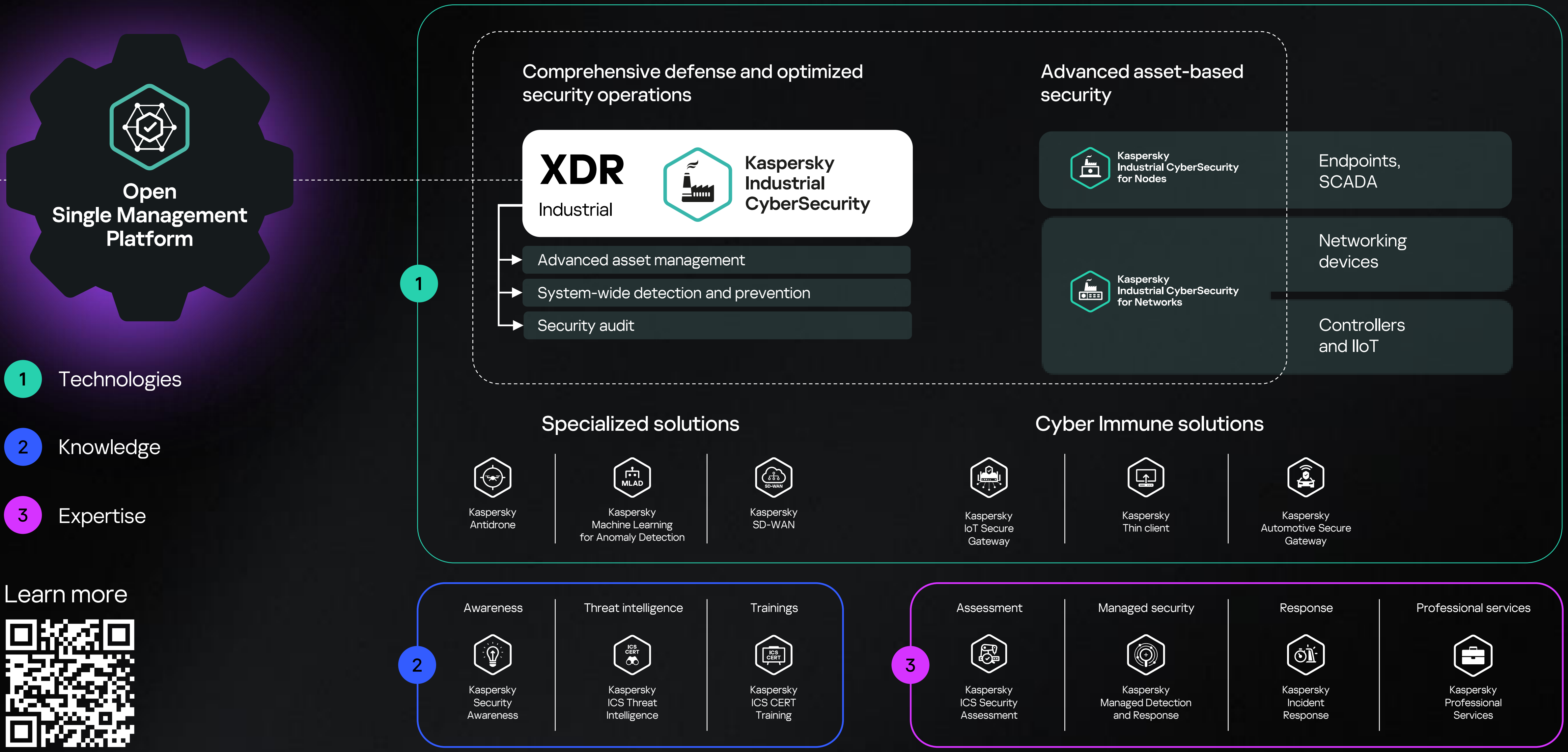
2

Awareness	Threat intelligence	Training
Kaspersky Security Awareness	Kaspersky Threat Intelligence	Kaspersky Cybersecurity Training

3

Assessment	Managed security	Incident response	Compromise assessment	SOC consulting	Support services
Kaspersky Security Assessment	Kaspersky Managed Detection and Response	Kaspersky Incident Response	Kaspersky Compromise Assessment	Kaspersky SOC Consulting	Kaspersky Professional Services

Kaspersky for OT environments



Open Single Management Platform

1 Technologies

2 Knowledge

3 Expertise

1

Comprehensive defense and optimized security operations

XDR Industrial

Kaspersky Industrial CyberSecurity

- Advanced asset management
- System-wide detection and prevention
- Security audit

Advanced asset-based security

Kaspersky Industrial CyberSecurity for Nodes — Endpoints, SCADA

Kaspersky Industrial CyberSecurity for Networks — Networking devices; Controllers and IIoT

Specialized solutions

- Kaspersky Antidrone
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN

Cyber Immune solutions

- Kaspersky IoT Secure Gateway
- Kaspersky Thin client
- Kaspersky Automotive Secure Gateway

2

Awareness	Threat intelligence	Trainings
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

3

Assessment	Managed security	Response	Professional services
Kaspersky ICS Security Assessment	Kaspersky Managed Detection and Response	Kaspersky Incident Response	Kaspersky Professional Services

Learn more

Kaspersky Next MXDR Optimum

Secure smarter, save bigger — empower your growing business with powerful cybersecurity backed by AI and world-leading expertise

kaspersky

bring on
the future

Contents

01

01 Kaspersky Next product line

02 MXDR Optimum overview

03 Breakdown of functionality

04 Additional information

Kaspersky Next

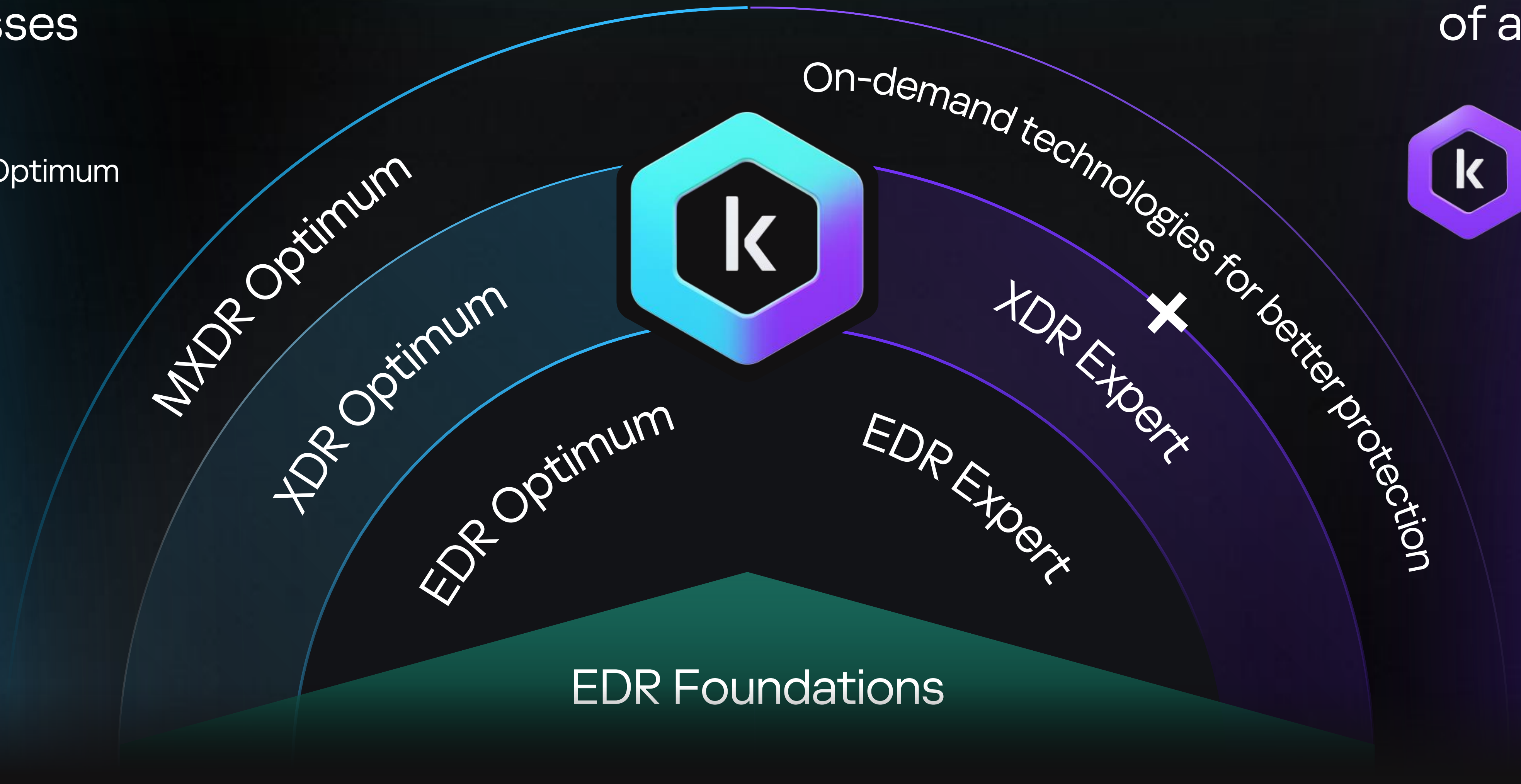
Tailored security for every business

Small & mid-sized businesses

Optimum

Enterprises of all sizes

Expert



MXDR Optimum

XDR Optimum

EDR Optimum

On-demand technologies for better protection

XDR Expert

EDR Expert

EDR Foundations

Layers customized to different business challenges

Challenges

Optimum

Small & mid-sized business

- The complexity and intensity of cyberthreats
- Limited cybersecurity expertise and budget
- Regulatory compliance requirements relating to endpoint protection
- Need for an effective, scalable and easy-to-manage solution

Challenges

Expert

Enterprises of all sizes

- Advanced persistent threats
- Potential disruption to business continuity, financial losses and reputational damage
- A shortage of specialists able to handle sophisticated threats
- Countless alerts to be examined - many of which prove to be false positives

Why choose Kaspersky Next?

Built on our best-in-class endpoint solution

For over a decade, Kaspersky products have consistently ranked at the top in independent tests and reviews, earning first-place awards and top-three finishes.

Our proven automated endpoint protection reduces the number of alerts security teams need to analyze, improving their efficiency.

Backed by deep knowledge, skills and expertise

Kaspersky Next is built on decades of the accumulated experience and deep expertise of our global security teams. Our specialists work collaboratively to address complex cyberthreats, continuously refining the technologies that power our products. This expert-driven approach ensures our solutions are reliable, innovative and aligned with real-world security needs.

Multi-layered prevention based on AI technology

Kaspersky uses predictive algorithms, clustering, neural networks, statistical models and expert algorithms to boost detection speed and improve accuracy.

Cybersecurity that grows with you

Kaspersky Next protects businesses of all sizes. As your needs grow, you can easily scale from essential endpoint protection to advanced, expert-level solutions available in higher tiers.

Contents

02

01 Kaspersky Next product line

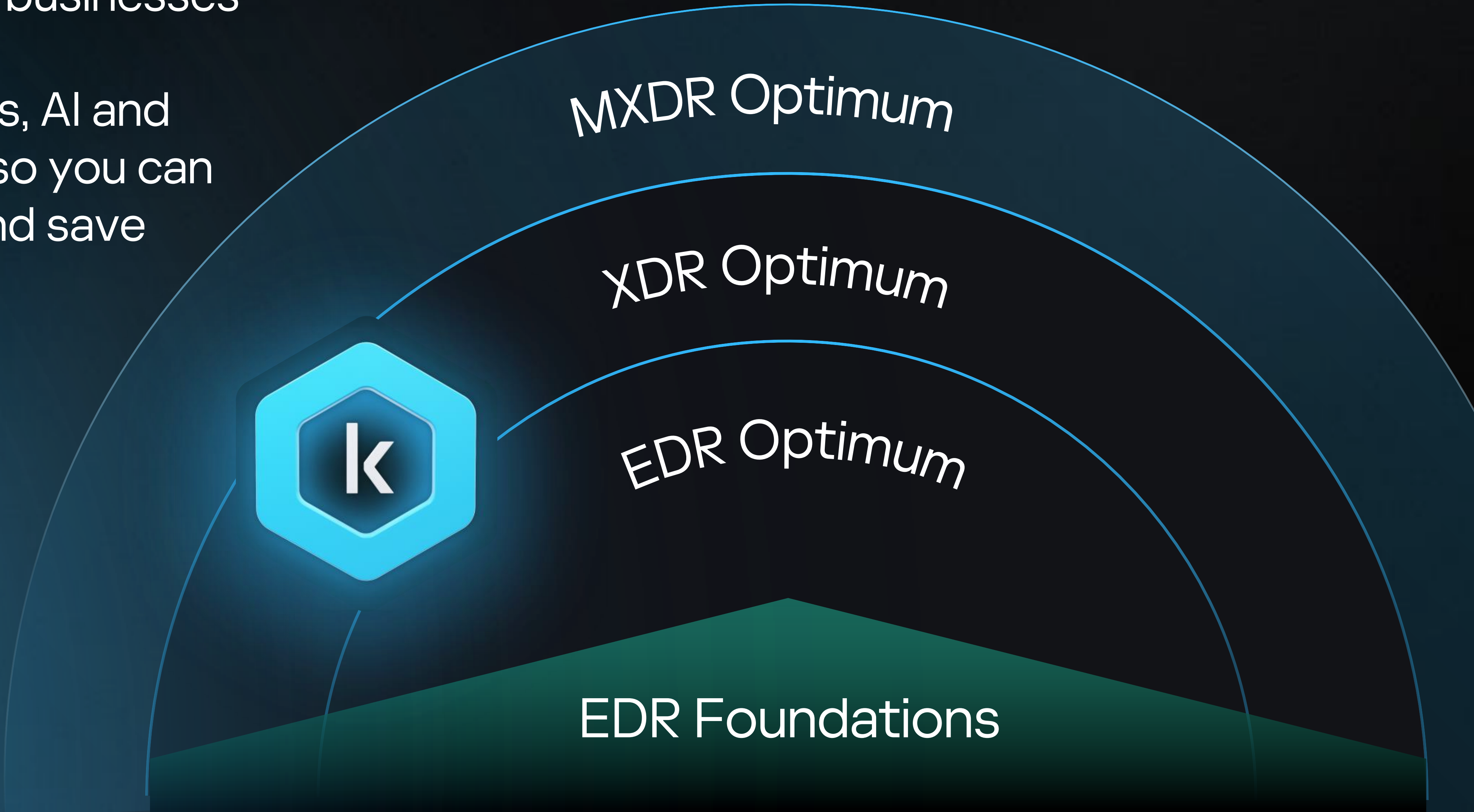
02 MXDR Optimum overview

03 Breakdown of functionality

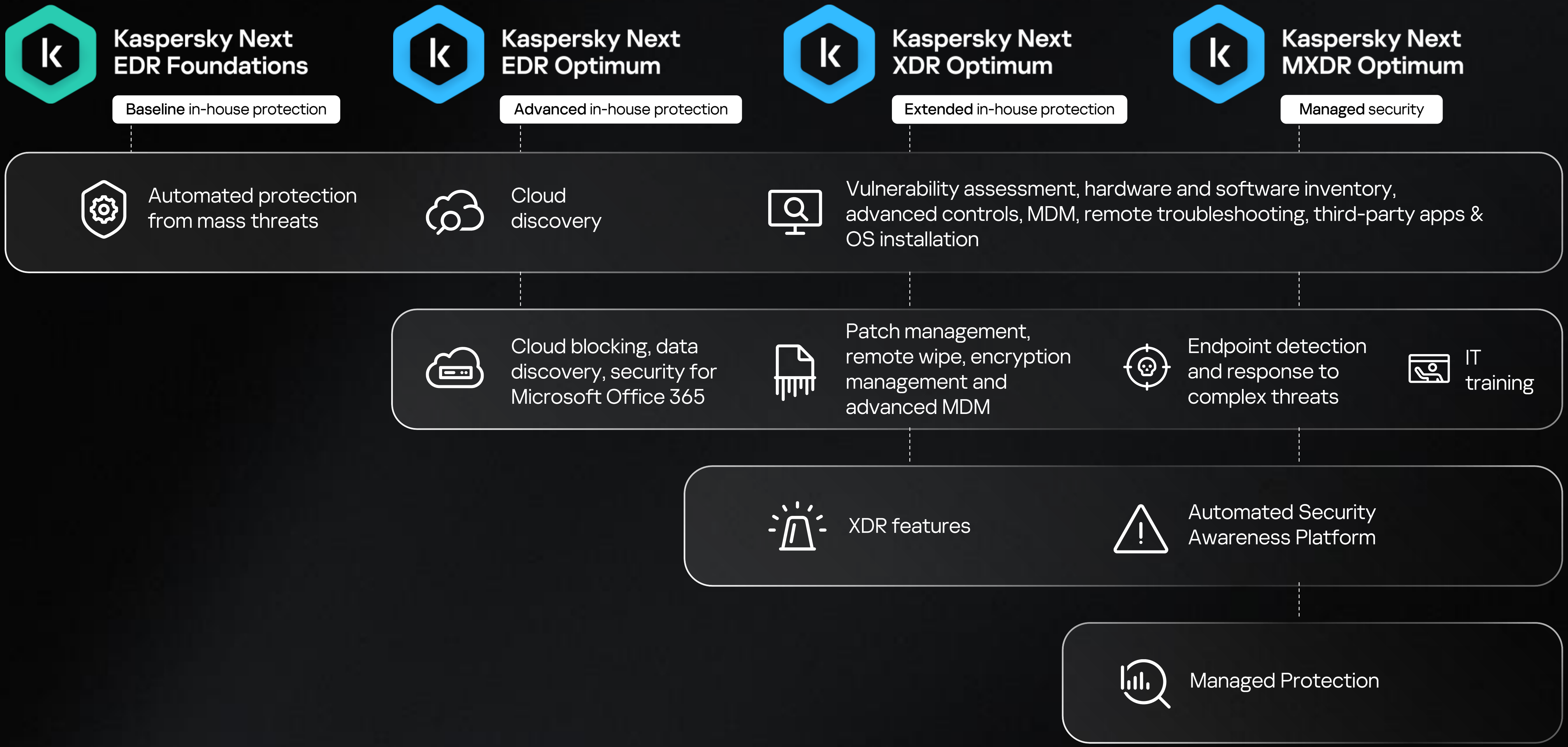
04 Additional information

Kaspersky Next Optimum

Empowering your businesses with unmatched cybertechnologies, AI and human expertise so you can secure smarter and save bigger.



Features comparison



Kaspersky Next EDR Foundations

Baseline in-house protection

Kaspersky Next EDR Optimum

Advanced in-house protection

Kaspersky Next XDR Optimum

Extended in-house protection

Kaspersky Next MXDR Optimum

Managed security

Automated protection from mass threats

Cloud discovery

Vulnerability assessment, hardware and software inventory, advanced controls, MDM, remote troubleshooting, third-party apps & OS installation

Cloud blocking, data discovery, security for Microsoft Office 365

Patch management, remote wipe, encryption management and advanced MDM

Endpoint detection and response to complex threats

IT training

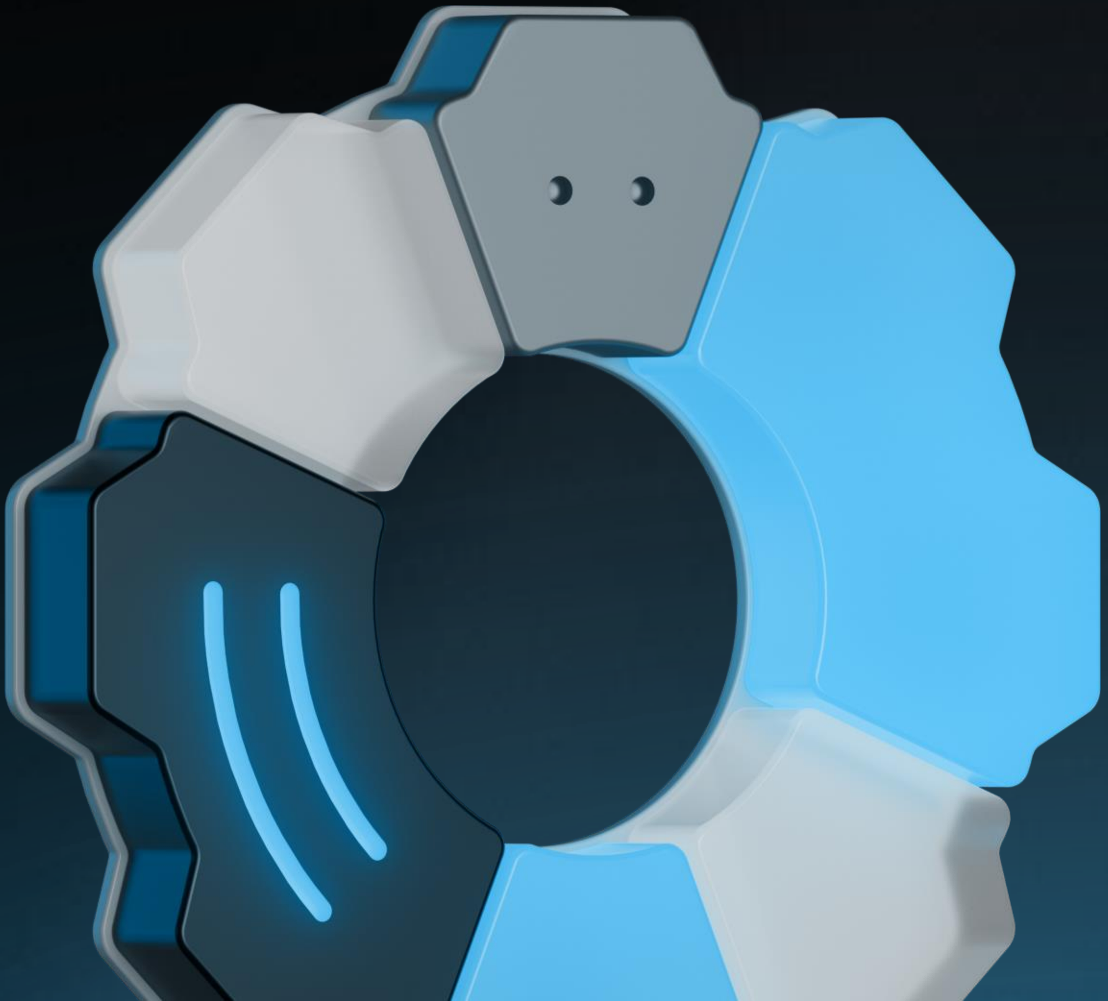
XDR features

Automated Security Awareness Platform

Managed Protection

Contents

03



01 Kaspersky Next product line

02 MXDR Optimum overview

03 Breakdown of functionality

04 Additional information

Strong EPP

Endpoint protection

Endpoint protection

Tracking incoming and outgoing data over the device, scan it for threats and stop them before causing farm.

Multi-layered protection

Signature-based protection, heuristic and behavioral analysis with pattern-based detection technology.

Advanced protection

With ML analysis of malicious patterns and anonymized data from Kaspersky Security Network (KSN) about actual threats.

Additional protection

Preventing intrusions, controlling access to system files and blocking suspicious connections to devices, including Android and iOS.

Attack surface reduction

System hardening

Multiple control components, including Adaptive Anomaly Control and ML algorithms help automatically adapt system hardening and security policy configuration to user behavior.

Vulnerability and patch management

Vulnerability and patch management simplify updates and streamline IT and security operations by supporting OS and third-party software installation across hosts.

Optimal XDR

Endpoint detection and response features

Indicators of compromise

Indicators of compromise (IoC) search with automatic cross-endpoint response

Root cause analysis

Data and visualization tools to ascertain the root cause of the threat and whether any additional response actions are needed

Automated response

Built-in response guidance and automation

Enrichment

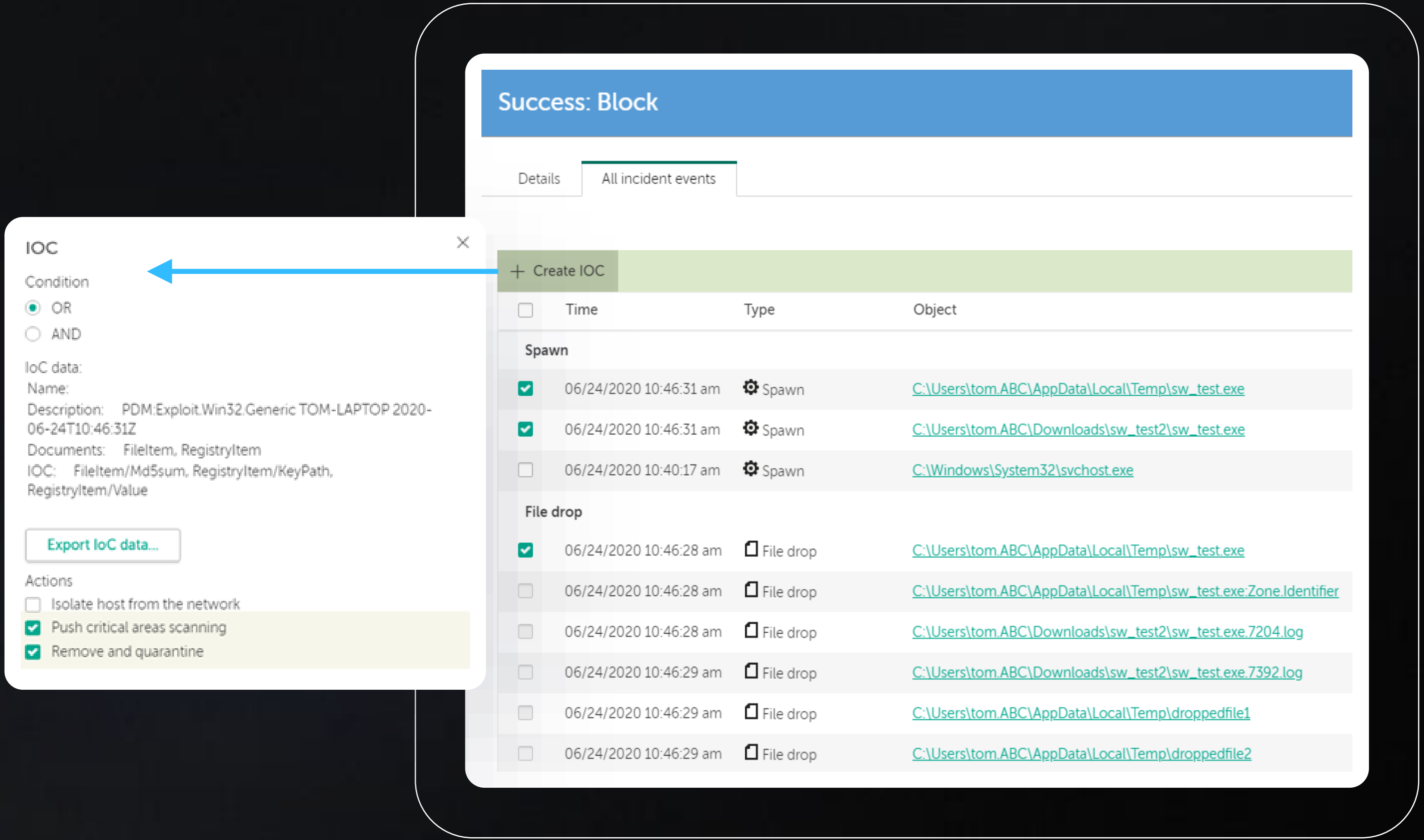
Access to our Threat Intelligence Portal

Indicators of compromise

Import IoCs from a trusted source and run cross-host scans to reveal threats that might be hiding on your endpoints.

Generate an IoC for an analyzed alert with a few clicks, and scan for similar threats on other hosts to find out the true scope of the discovered threat.

Run a scan on-demand to find existing threats or set up a scheduled scan.



IOC

Condition

● OR

○ AND

IoC data:

Name:

Description: PDM:Exploit.Win32.Generic TOM-LAPTOP 2020-06-24T10:46:31Z

Documents: FileItem, RegistryItem

IOC: FileItem/Md5sum, RegistryItem/KeyPath, RegistryItem/Value

Export IoC data...

Actions

□ Isolate host from the network

☑ Push critical areas scanning

☑ Remove and quarantine

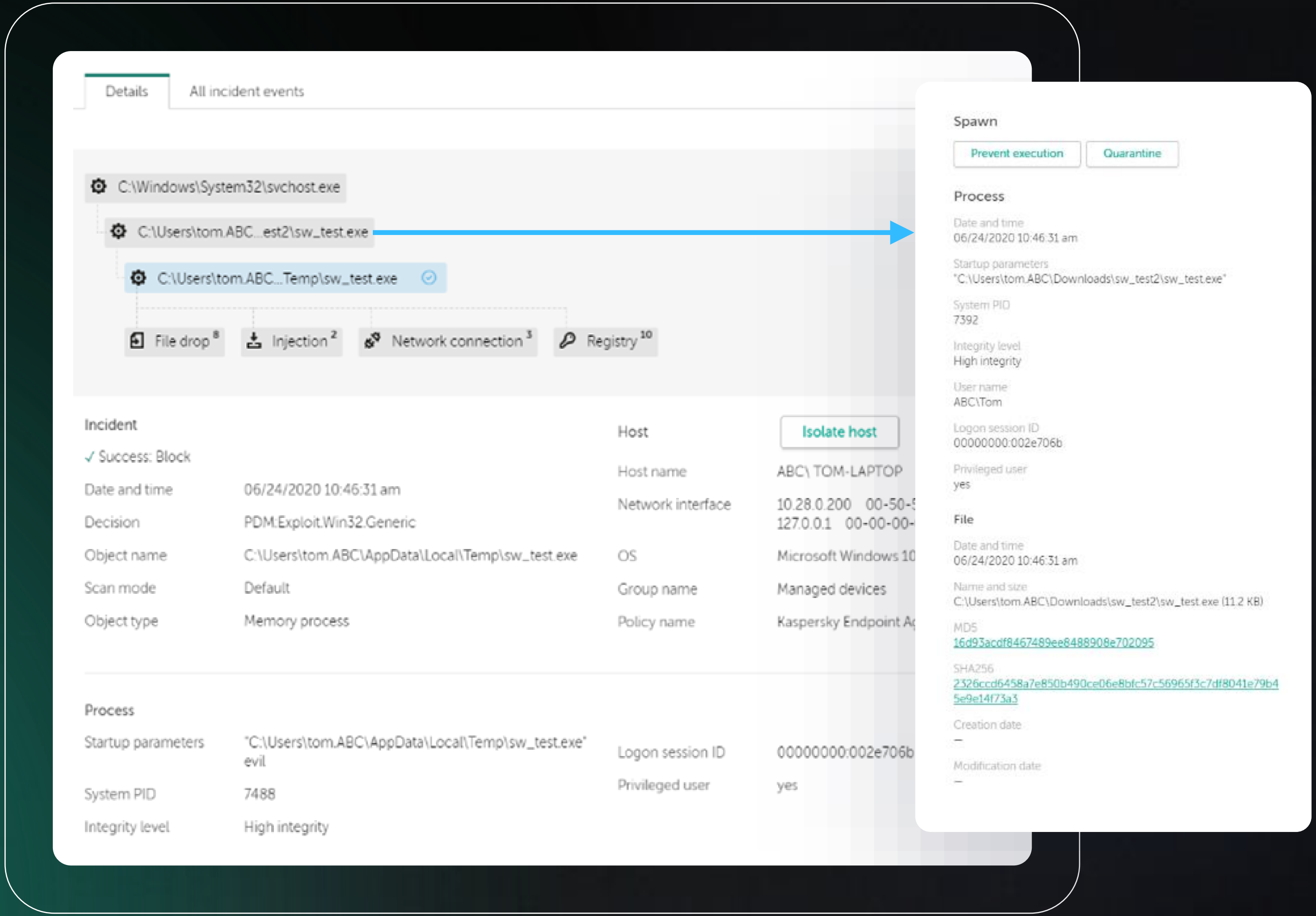
Success: Block

Details | All incident events

+ Create IOC

□	Time	Type	Object
Spawn			
☑	06/24/2020 10:46:31 am	Spawn	C:\Users\tom.ABC\AppData\Local\Temp\sw_test.exe
☑	06/24/2020 10:46:31 am	Spawn	C:\Users\tom.ABC\Downloads\sw_test2\sw_test.exe
□	06/24/2020 10:40:17 am	Spawn	C:\Windows\System32\svchost.exe
File drop			
☑	06/24/2020 10:46:28 am	File drop	C:\Users\tom.ABC\AppData\Local\Temp\sw_test.exe
□	06/24/2020 10:46:28 am	File drop	C:\Users\tom.ABC\AppData\Local\Temp\sw_test.exe:Zone.Identifier
□	06/24/2020 10:46:28 am	File drop	C:\Users\tom.ABC\Downloads\sw_test2\sw_test.exe.7204.log
□	06/24/2020 10:46:29 am	File drop	C:\Users\tom.ABC\Downloads\sw_test2\sw_test.exe.7392.log
□	06/24/2020 10:46:29 am	File drop	C:\Users\tom.ABC\AppData\Local\Temp\droppedfile1
□	06/24/2020 10:46:29 am	File drop	C:\Users\tom.ABC\AppData\Local\Temp\droppedfile2

Root cause analysis



Incident

✓ Success: Block

Date and time	06/24/2020 10:46:31 am
Decision	PDM.Exploit.Win32.Generic
Object name	C:\Users\tom.ABC\AppData\Local\Temp\sw_test.exe
Scan mode	Default
Object type	Memory process

Host

Host name	ABC\ TOM-LAPTOP
Network interface	10.28.0.200 00-50-5 127.0.0.1 00-00-00-
OS	Microsoft Windows 10
Group name	Managed devices
Policy name	Kaspersky Endpoint Ag

Process

Startup parameters	"C:\Users\tom.ABC\AppData\Local\Temp\sw_test.exe" evil
System PID	7488
Integrity level	High integrity
Logon session ID	00000000:002e706b
Privileged user	yes

Spawn

Process

Date and time	06/24/2020 10:46:31 am
Startup parameters	"C:\Users\tom.ABC\Downloads\sw_test2\sw_test.exe"
System PID	7392
Integrity level	High integrity
User name	ABC\Tom
Logon session ID	00000000:002e706b
Privileged user	yes

File

Date and time	06/24/2020 10:46:31 am
Name and size	C:\Users\tom.ABC\Downloads\sw_test2\sw_test.exe (11.2 KB)
MD5	16d93acdf8467489ee8488908e702095
SHA256	2326ccd6458a7e850b490ce06e8bfc57c56965f3c7df8041e79b45e9e14f73a3
Creation date	–
Modification date	–

Enriched data from the threat detection gives a complete understanding of what has occurred, which host was involved and under which user the incident took place.

An automatically generated process tree enables you to quickly see and analyze how the threat developed on the host in order to determine its root cause.

Using all the available data and visualization tools, you can ascertain the root cause of the threat and whether any additional response actions need to be performed.

Threat Intelligence Portal

Users can use Kaspersky Threat Intelligence Portal to check any suspicious files, file hashes, IP addresses and web addresses so they can validate and prioritize associated security alerts, and ensure a timely response to threats

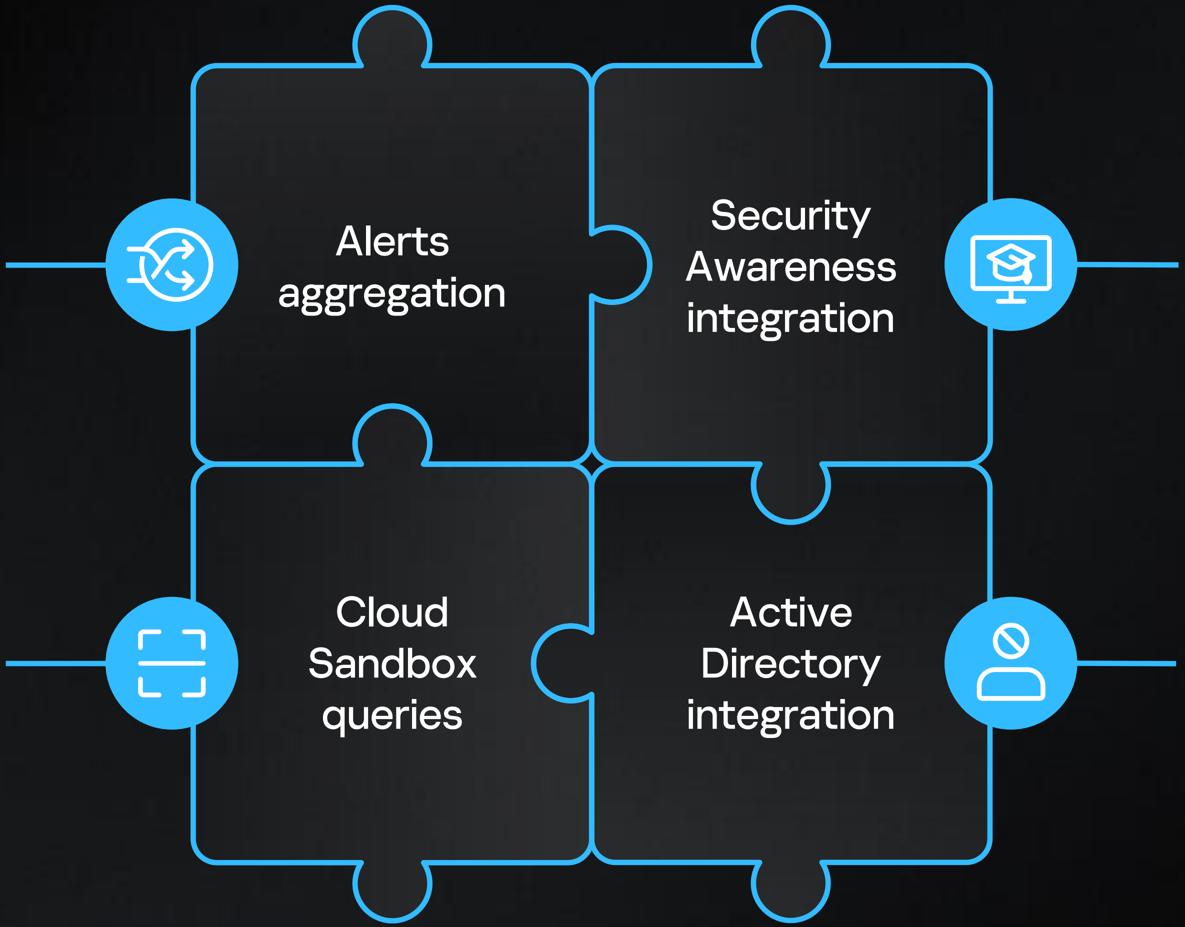
A file’s reputation from Kaspersky Threat Intelligence Portal is integrated into the alert card for even faster and more accurate root cause analysis

Detecting advanced threats present in files – running them through the full stack of our technologies

Enriching and prioritizing alerts by analyzing suspicious IPs, file hashes, domains and web addresses

Executing suspicious web addresses in our URL sandbox and receiving a comprehensive threat report

Extended detection and response features



Alerts aggregation

Security Awareness integration

Cloud Sandbox queries

Active Directory integration

Combining smaller, weaker signals into something larger and possibly more insightful by aggregating Kaspersky Security Center alerts and providing customers with a vital XDR benefit.

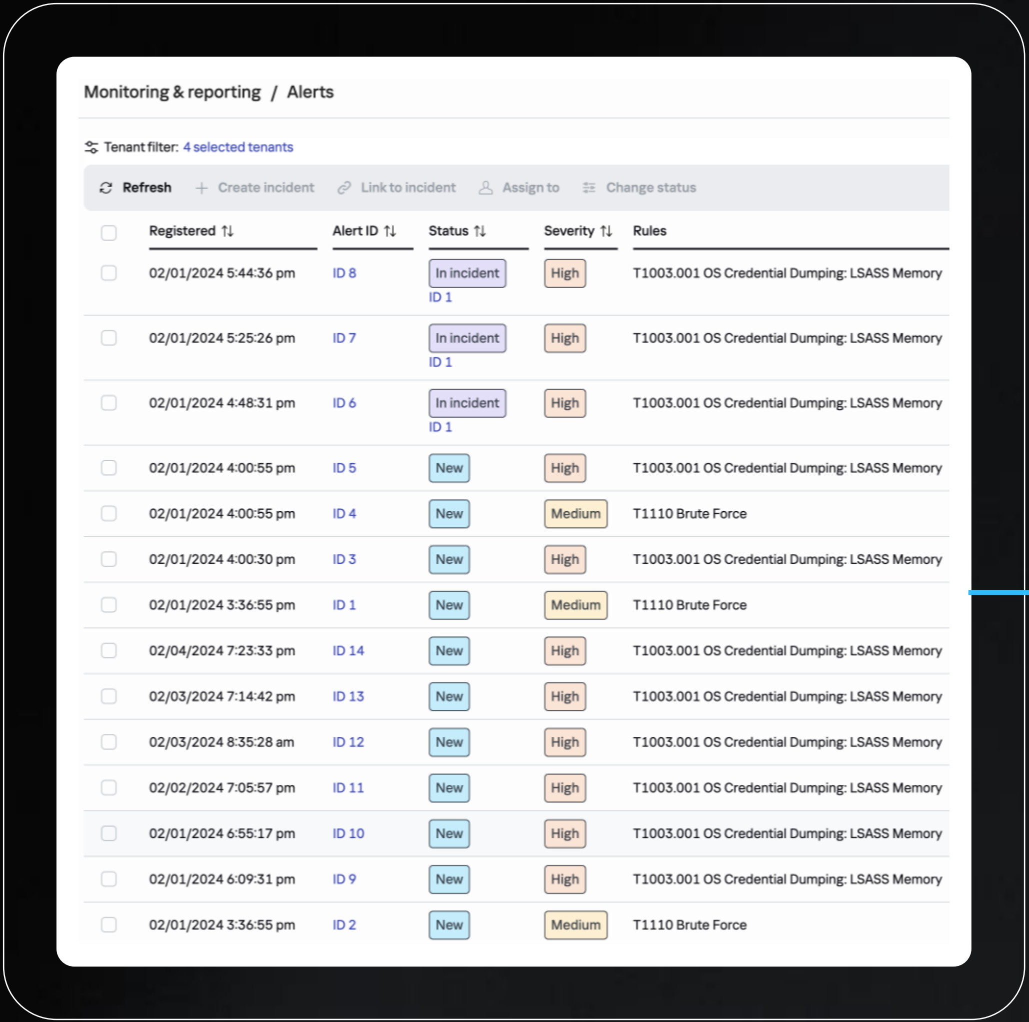
Increasing the effectiveness of incident response and threat investigation by allowing users to submit potentially harmful files for detonation to our Cloud Sandbox from the alert card.

Enabling the ability to respond through integration with the Kaspersky Security Awareness Platform.

To cut down on repetitive work and free up time for more prescient assignments, users can configure automatic training assignments directly from the alert card.

Leveraging third-party party response and allowing to block users.

Alerts aggregation



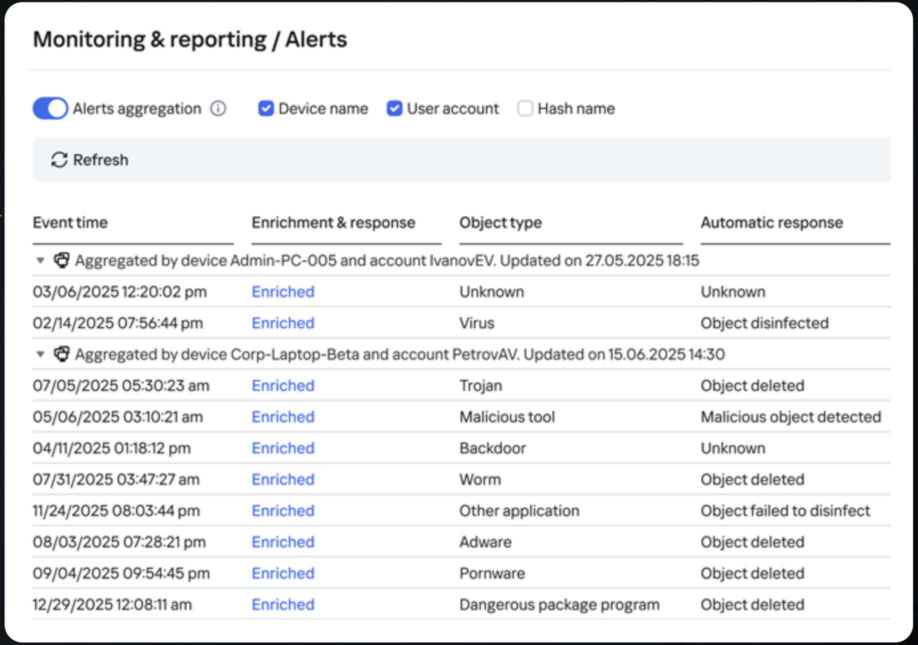
Monitoring & reporting / Alerts

Tenant filter: 4 selected tenants

□	Registered ⇅	Alert ID ⇅	Status ⇅	Severity ⇅	Rules
□	02/01/2024 5:44:36 pm	ID 8	In incident ID 1	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/01/2024 5:25:26 pm	ID 7	In incident ID 1	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/01/2024 4:48:31 pm	ID 6	In incident ID 1	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/01/2024 4:00:55 pm	ID 5	New	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/01/2024 4:00:55 pm	ID 4	New	Medium	T1110 Brute Force
□	02/01/2024 4:00:30 pm	ID 3	New	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/01/2024 3:36:55 pm	ID 1	New	Medium	T1110 Brute Force
□	02/04/2024 7:23:33 pm	ID 14	New	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/03/2024 7:14:42 pm	ID 13	New	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/03/2024 8:35:28 am	ID 12	New	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/02/2024 7:05:57 pm	ID 11	New	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/01/2024 6:55:17 pm	ID 10	New	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/01/2024 6:09:31 pm	ID 9	New	High	T1003.001 OS Credential Dumping: LSASS Memory
□	02/01/2024 3:36:55 pm	ID 2	New	Medium	T1110 Brute Force

One sample could affect 100 hosts and this would generate 100 alerts.

Grouping related alerts helps simplify threat investigation and enhance incident response efficiency, while reducing the cognitive load of the analyst.



Monitoring & reporting / Alerts

● Alerts aggregation ☑ Device name ☑ User account □ Hash name

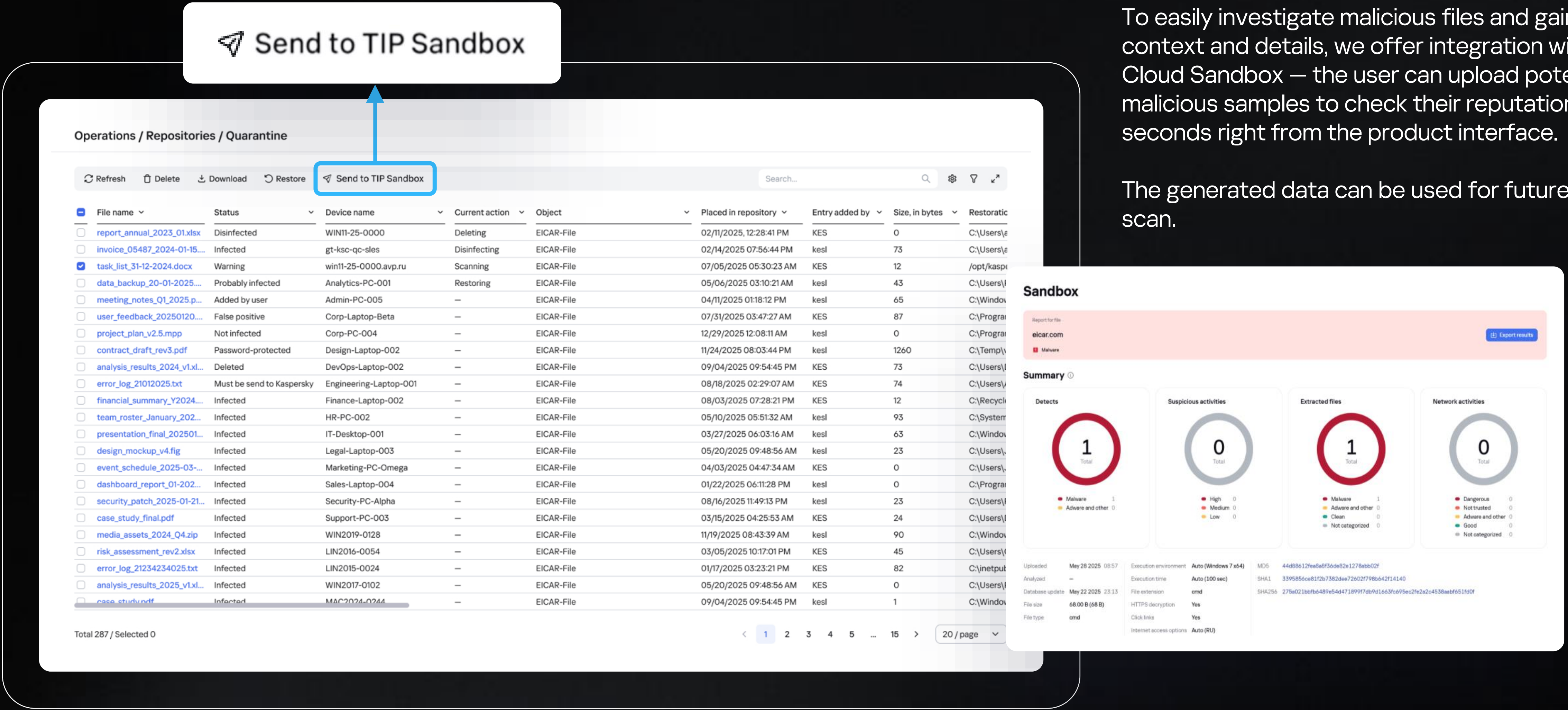
Event time	Enrichment & response	Object type	Automatic response
▾ Aggregated by device Admin-PC-005 and account IvanovEV. Updated on 27.05.2025 18:15			
03/06/2025 12:20:02 pm	Enriched	Unknown	Unknown
02/14/2025 07:56:44 pm	Enriched	Virus	Object disinfected
▾ Aggregated by device Corp-Laptop-Beta and account PetrovAV. Updated on 15.06.2025 14:30			
07/05/2025 05:30:23 am	Enriched	Trojan	Object deleted
05/06/2025 03:10:21 am	Enriched	Malicious tool	Malicious object detected
04/11/2025 01:18:12 pm	Enriched	Backdoor	Unknown
07/31/2025 03:47:27 am	Enriched	Worm	Object deleted
11/24/2025 08:03:44 pm	Enriched	Other application	Object failed to disinfect
08/03/2025 07:28:21 pm	Enriched	Adware	Object deleted
09/04/2025 09:54:45 pm	Enriched	Pornware	Object deleted
12/29/2025 12:08:11 am	Enriched	Dangerous package program	Object deleted

Cloud sandbox queries

Integration with Kaspersky Cloud Sandbox allows to perform various actions using Kaspersky Threat Intelligence Portal

- Automatic detection of file types
- Managing obsolete tasks for execution
- Uploading and executing a file in in Cloud Sandbox
- Uploading a file from a web address and then executing it in Cloud Sandbox
- Anti-evasion features to counter malware designed to avoid sandboxes
- Executing an extracted file from the Cloud Sandbox report
- Exporting the results of the analysis

Cloud sandbox queries



Operations / Repositories / Quarantine

	File name	Status	Device name	Current action	Object	Placed in repository	Entry added by	Size, in bytes	Restoratic
☐	report_annual_2023_01.xlsx	Disinfected	WIN11-25-0000	Deleting	EICAR-File	02/11/2025, 12:28:41 PM	KES	0	C:\Users\a
☐	invoice_05487_2024-01-15....	Infected	gt-ksc-qc-sles	Disinfecting	EICAR-File	02/14/2025 07:56:44 PM	kesl	73	C:\Users\a
☑	task_list_31-12-2024.docx	Warning	win11-25-0000.avp.ru	Scanning	EICAR-File	07/05/2025 05:30:23 AM	KES	12	/opt/kaspe
☐	data_backup_20-01-2025....	Probably infected	Analytics-PC-001	Restoring	EICAR-File	05/06/2025 03:10:21 AM	kesl	43	C:\Users\
☐	meeting_notes_Q1_2025.p...	Added by user	Admin-PC-005	—	EICAR-File	04/11/2025 01:18:12 PM	kesl	65	C:\Windov
☐	user_feedback_20250120....	False positive	Corp-Laptop-Beta	—	EICAR-File	07/31/2025 03:47:27 AM	KES	87	C:\Progra
☐	project_plan_v2.5.mpp	Not infected	Corp-PC-004	—	EICAR-File	12/29/2025 12:08:11 AM	kesl	0	C:\Progra
☐	contract_draft_rev3.pdf	Password-protected	Design-Laptop-002	—	EICAR-File	11/24/2025 08:03:44 PM	kesl	1260	C:\Temp\
☐	analysis_results_2024_v1.xl...	Deleted	DevOps-Laptop-002	—	EICAR-File	09/04/2025 09:54:45 PM	KES	73	C:\Users\
☐	error_log_21012025.txt	Must be send to Kaspersky	Engineering-Laptop-001	—	EICAR-File	08/18/2025 02:29:07 AM	KES	74	C:\Users\
☐	financial_summary_Y2024....	Infected	Finance-Laptop-002	—	EICAR-File	08/03/2025 07:28:21 PM	KES	12	C:\Recycl
☐	team_roster_January_202...	Infected	HR-PC-002	—	EICAR-File	05/10/2025 05:51:32 AM	kesl	93	C:\System
☐	presentation_final_202501...	Infected	IT-Desktop-001	—	EICAR-File	03/27/2025 06:03:16 AM	kesl	63	C:\Windov
☐	design_mockup_v4.fig	Infected	Legal-Laptop-003	—	EICAR-File	05/20/2025 09:48:56 AM	kesl	23	C:\Users\.
☐	event_schedule_2025-03-...	Infected	Marketing-PC-Omega	—	EICAR-File	04/03/2025 04:47:34 AM	KES	0	C:\Users\.
☐	dashboard_report_01-202...	Infected	Sales-Laptop-004	—	EICAR-File	01/22/2025 06:11:28 PM	kesl	0	C:\Progra
☐	security_patch_2025-01-21...	Infected	Security-PC-Alpha	—	EICAR-File	08/16/2025 11:49:13 PM	kesl	23	C:\Users\
☐	case_study_final.pdf	Infected	Support-PC-003	—	EICAR-File	03/15/2025 04:25:53 AM	KES	24	C:\Users\
☐	media_assets_2024_Q4.zip	Infected	WIN2019-0128	—	EICAR-File	11/19/2025 08:43:39 AM	kesl	90	C:\Windov
☐	risk_assessment_rev2.xlsx	Infected	LIN2016-0054	—	EICAR-File	03/05/2025 10:17:01 PM	KES	45	C:\Users\
☐	error_log_21234234025.txt	Infected	LIN2015-0024	—	EICAR-File	01/17/2025 03:23:21 PM	KES	82	C:\inetpu
☐	analysis_results_2025_v1.xl...	Infected	WIN2017-0102	—	EICAR-File	05/20/2025 09:48:56 AM	KES	0	C:\Users\
☐	case_study.pdf	Infected	MAC2024-0244	—	EICAR-File	09/04/2025 09:54:45 PM	kesl	1	C:\Windov

Total 287 / Selected 0

Sandbox

Report for file

eicar.com

Malware

Summary

Detects: 1 Total
- Malware 1
- Adware and other 0

Suspicious activities: 0 Total
- High 0
- Medium 0
- Low 0

Extracted files: 1 Total
- Malware 1
- Adware and other 0
- Clean 0
- Not categorized 0

Network activities: 0 Total
- Dangerous 0
- Not trusted 0
- Adware and other 0
- Good 0
- Not categorized 0

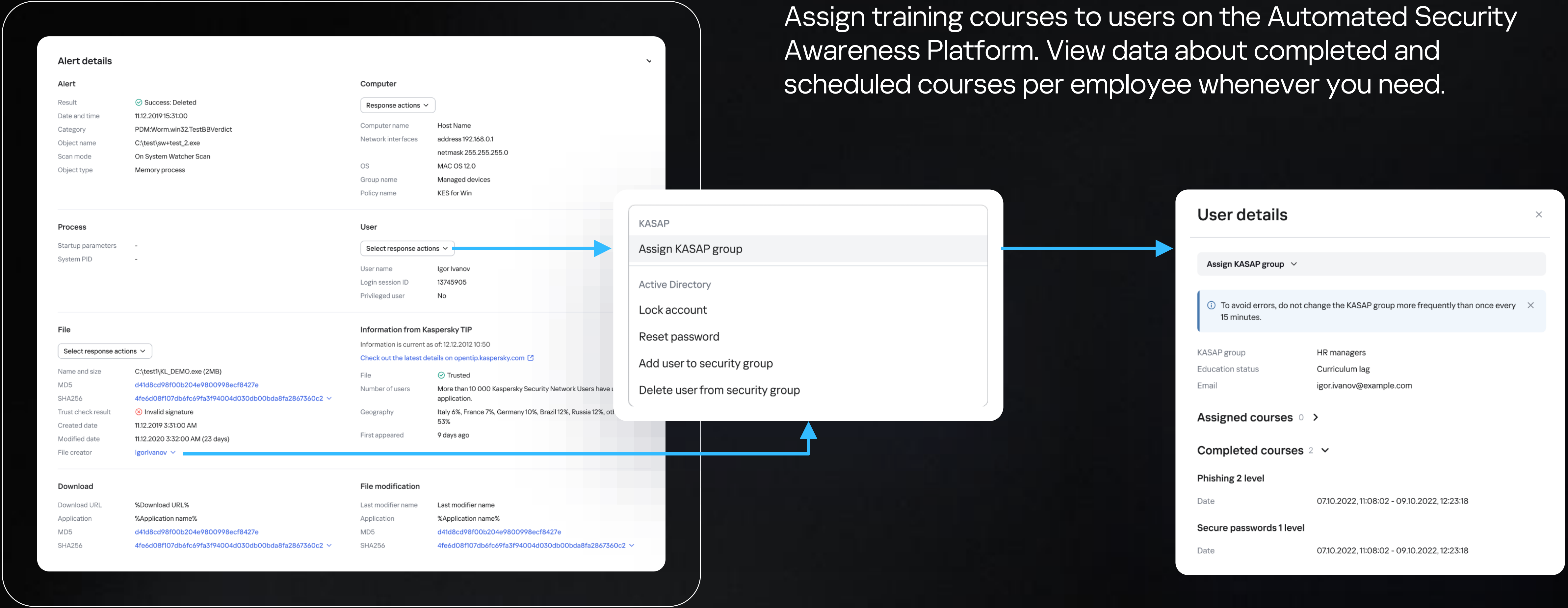
Uploaded	May 28 2025 08:57	Execution environment	Auto (Windows 7 x64)	MD5	44d88612fea8a8f36de82e1278abb02f
Analyzed	–	Execution time	Auto (100 sec)	SHA1	3395856ce81f2b7382dee72602f798b642f14140
Database update	May 22 2025 23:13	File extension	cmd	SHA256	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
File size	68.00 B (68 B)	HTTPS decryption	Yes		
File type	cmd	Click links	Yes		
		Internet access options	Auto (RU)		

To easily investigate malicious files and gain more context and details, we offer integration with our Cloud Sandbox — the user can upload potentially malicious samples to check their reputation within seconds right from the product interface.

The generated data can be used for future IoC scan.

Security Awareness integration

Assign training courses to users on the Automated Security Awareness Platform. View data about completed and scheduled courses per employee whenever you need.



Alert details

Alert

Result	✓ Success: Deleted
Date and time	11.12.2019 15:31:00
Category	PDM:Worm.win32.TestBBVerdict
Object name	C:\test\sw+test_2.exe
Scan mode	On System Watcher Scan
Object type	Memory process

Computer

Response actions

Computer name	Host Name
Network interfaces	address 192.168.0.1 netmask 255.255.255.0
OS	MAC OS 12.0
Group name	Managed devices
Policy name	KES for Win

Process

Startup parameters	-
System PID	-

User

Select response actions

User name	Igor Ivanov
Login session ID	13745905
Privileged user	No

File

Select response actions

Name and size	C:\test1\KL_DEMO.exe (2MB)
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA256	4fe6d08f107db6fc69fa3f94004d030db00bda8fa2867360c2
Trust check result	⊗ Invalid signature
Created date	11.12.2019 3:31:00 AM
Modified date	11.12.2020 3:32:00 AM (23 days)
File creator	IgorIvanov

Information from Kaspersky TIP

Information is current as of: 12.12.2012 10:50

Check out the latest details on opentip.kaspersky.com

File	✓ Trusted
Number of users	More than 10 000 Kaspersky Security Network Users have u application.
Geography	Italy 6%, France 7%, Germany 10%, Brazil 12%, Russia 12%, ot 53%
First appeared	9 days ago

Download

Download URL	%Download URL%
Application	%Application name%
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA256	4fe6d08f107db6fc69fa3f94004d030db00bda8fa2867360c2

File modification

Last modifier name	Last modifier name
Application	%Application name%
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA256	4fe6d08f107db6fc69fa3f94004d030db00bda8fa2867360c2

User details

Assign KASAP group

ⓘ To avoid errors, do not change the KASAP group more frequently than once every 15 minutes.

KASAP group	HR managers
Education status	Curriculum lag
Email	igor.ivanov@example.com

Assigned courses 0

Completed courses 2

Phishing 2 level

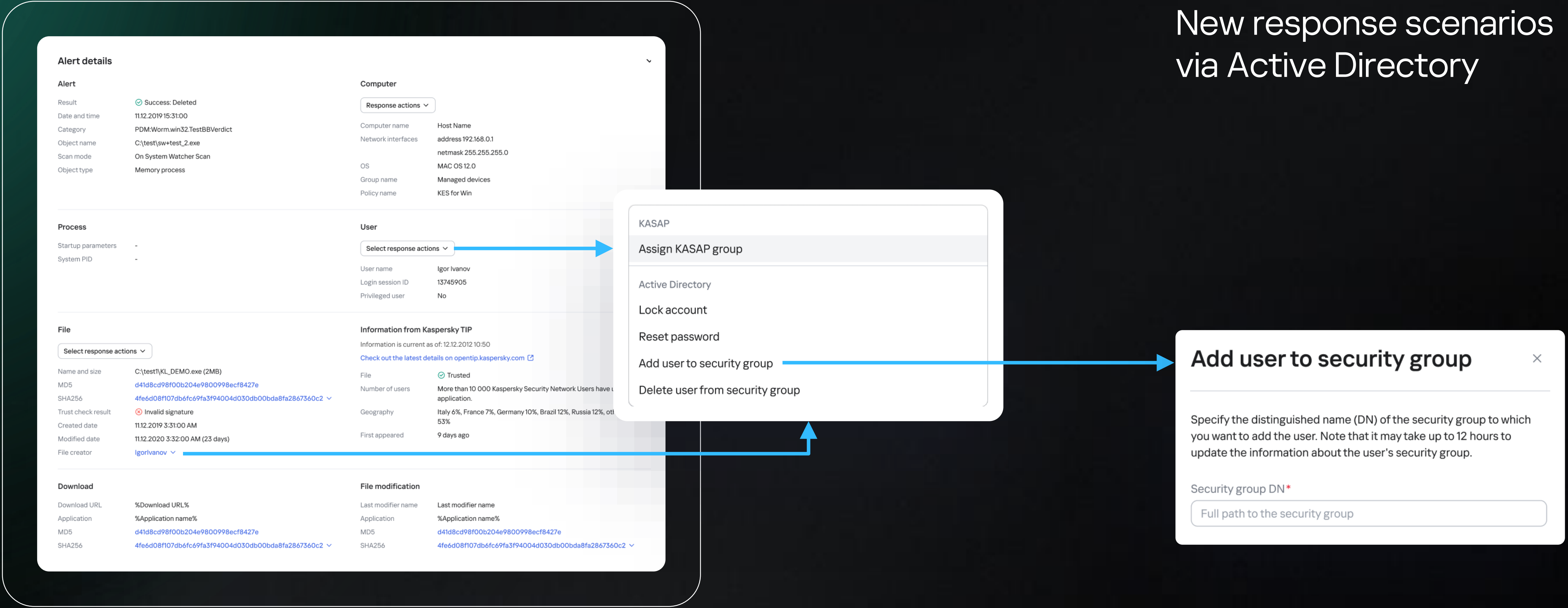
Date	07.10.2022, 11:08:02 - 09.10.2022, 12:23:18

Secure passwords 1 level

Date	07.10.2022, 11:08:02 - 09.10.2022, 12:23:18

Active Directory integration

New response scenarios via Active Directory



Alert details

Alert

Result	Success: Deleted
Date and time	11.12.2019 15:31:00
Category	PDM:Worm.win32.TestBBVerdict
Object name	C:\test\sw+test_2.exe
Scan mode	On System Watcher Scan
Object type	Memory process

Computer

Response actions

Computer name	Host Name
Network interfaces	address 192.168.0.1 netmask 255.255.255.0
OS	MAC OS 12.0
Group name	Managed devices
Policy name	KES for Win

Process

Startup parameters	-
System PID	-

User

Select response actions

User name	Igor Ivanov
Login session ID	13745905
Privileged user	No

File

Select response actions

Name and size	C:\test1\KL_DEMO.exe (2MB)
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA256	4fe6d08f107db6fc69fa3f94004d030db00bda8fa2867360c2
Trust check result	Invalid signature
Created date	11.12.2019 3:31:00 AM
Modified date	11.12.2020 3:32:00 AM (23 days)
File creator	IgorIvanov

Information from Kaspersky TIP

Information is current as of: 12.12.2012 10:50

Check out the latest details on opentip.kaspersky.com

File	Trusted
Number of users	More than 10 000 Kaspersky Security Network Users have u application.
Geography	Italy 6%, France 7%, Germany 10%, Brazil 12%, Russia 12%, ot 53%
First appeared	9 days ago

Download

Download URL	%Download URL%
Application	%Application name%
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA256	4fe6d08f107db6fc69fa3f94004d030db00bda8fa2867360c2

File modification

Last modifier name	Last modifier name
Application	%Application name%
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA256	4fe6d08f107db6fc69fa3f94004d030db00bda8fa2867360c2

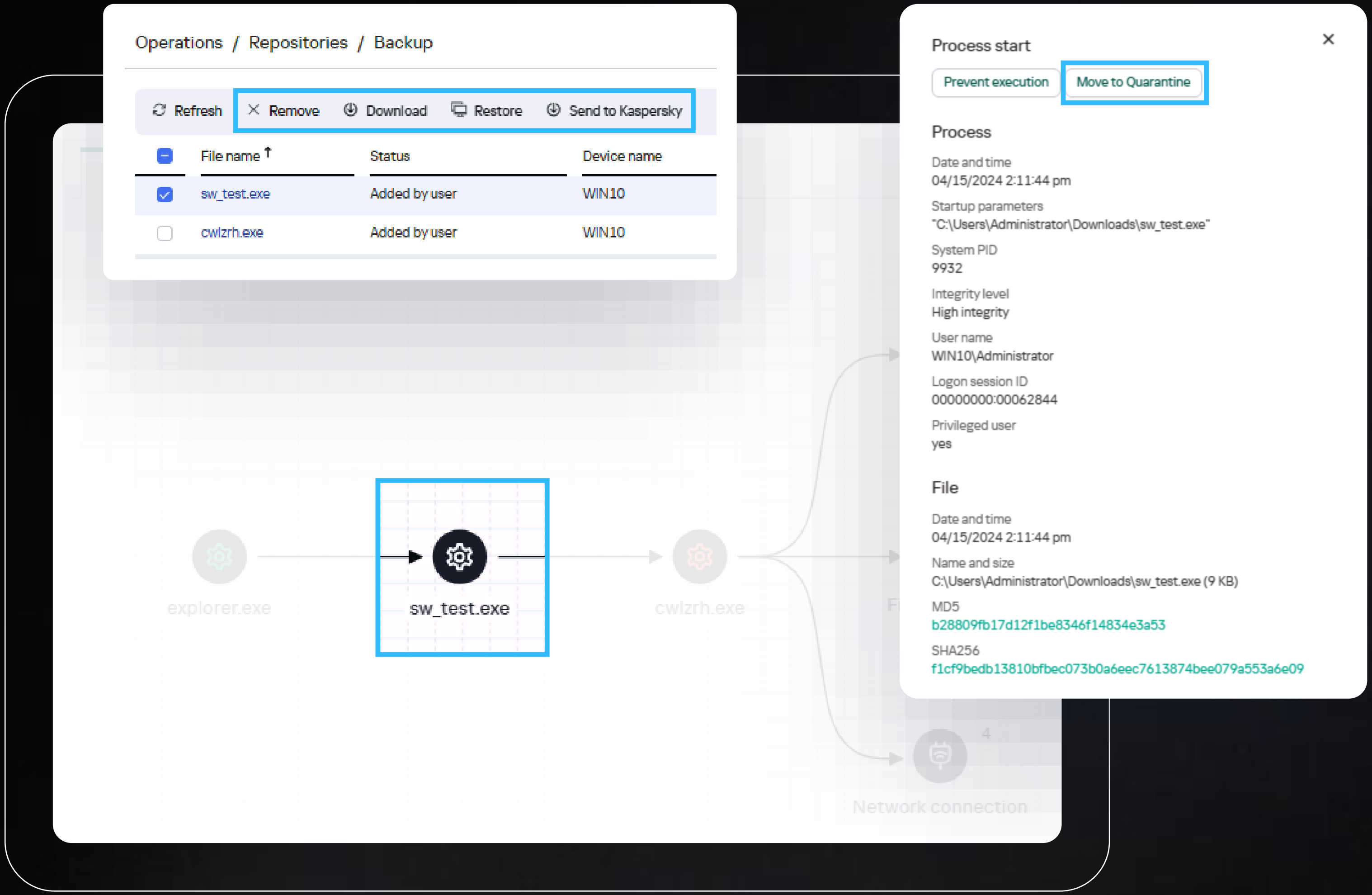
Add user to security group

Specify the distinguished name (DN) of the security group to which you want to add the user. Note that it may take up to 12 hours to update the information about the user's security group.

Security group DN*

Full path to the security group

Response options



☐	File name	Status	Device name
☑	sw_test.exe	Added by user	WIN10
☐	cwlzrh.exe	Added by user	WIN10

Process

Date and time
04/15/2024 2:11:44 pm

Startup parameters
"C:\Users\Administrator\Downloads\sw_test.exe"

System PID
9932

Integrity level
High integrity

User name
WIN10\Administrator

Logon session ID
00000000:00062844

Privileged user
yes

File

Date and time
04/15/2024 2:11:44 pm

Name and size
C:\Users\Administrator\Downloads\sw_test.exe (9 KB)

MD5
b28809fb17d12f1be8346f14834e3a53

SHA256
f1cf9bedb13810bfbec073b0a6eec7613874bee079a553a6e09

Quarantine an executable file from the chain and access it remotely for future research in the administration console.

Mark any executable file from the chain and block it on any of your hosts before it starts malicious behavior.

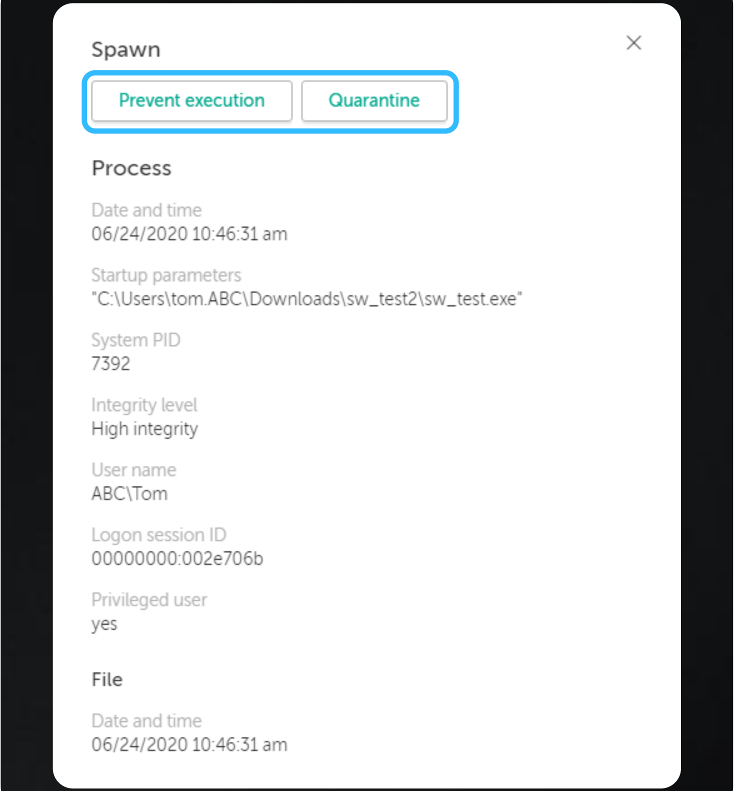
Other response options include: isolate host from the network, search the threat on other machines, scan critical areas and learn more with threat intelligence.

Automated response

Respond to a threat with a single click from the alert card, and act on analyzed threats instantly.

Set up an automated response with a simple checkbox, and it will be applied on discovery with an IoC scan.

In alert card



Spawn

Prevent execution | Quarantine

Process

Date and time
06/24/2020 10:46:31 am

Startup parameters
"C:\Users\tom.ABC\Downloads\sw_test2\sw_test.exe"

System PID
7392

Integrity level
High integrity

User name
ABC\Tom

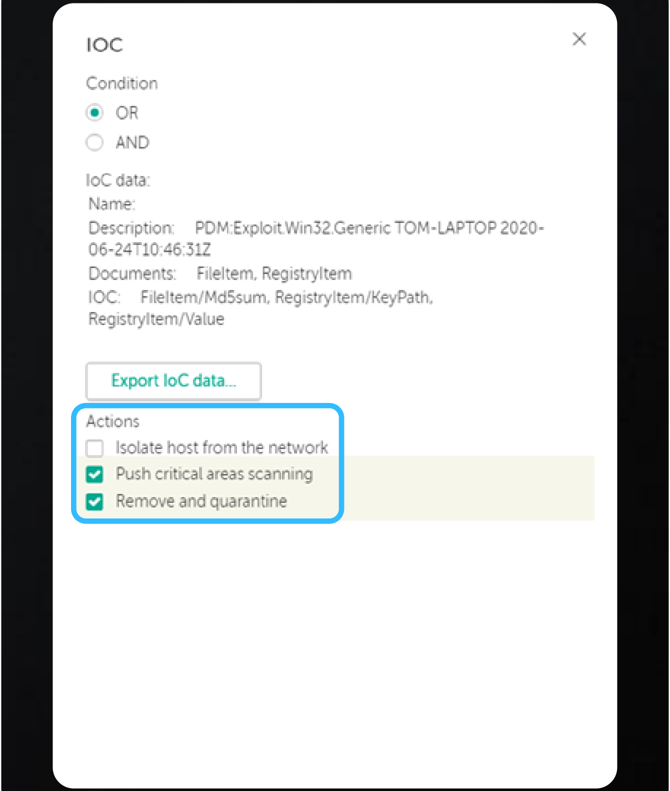
Logon session ID
00000000:002e706b

Privileged user
yes

File

Date and time
06/24/2020 10:46:31 am

In IoC scan



IOC

Condition
● OR
○ AND

IoC data:
Name:
Description: PDM:Exploit.Win32.Generic TOM-LAPTOP 2020-06-24T10:46:31Z
Documents: FileItem, RegistryItem
IOC: FileItem/Md5sum, RegistryItem/KeyPath, RegistryItem/Value

Export IoC data...

Actions
□ Isolate host from the network
☑ Push critical areas scanning
☑ Remove and quarantine

Managed security

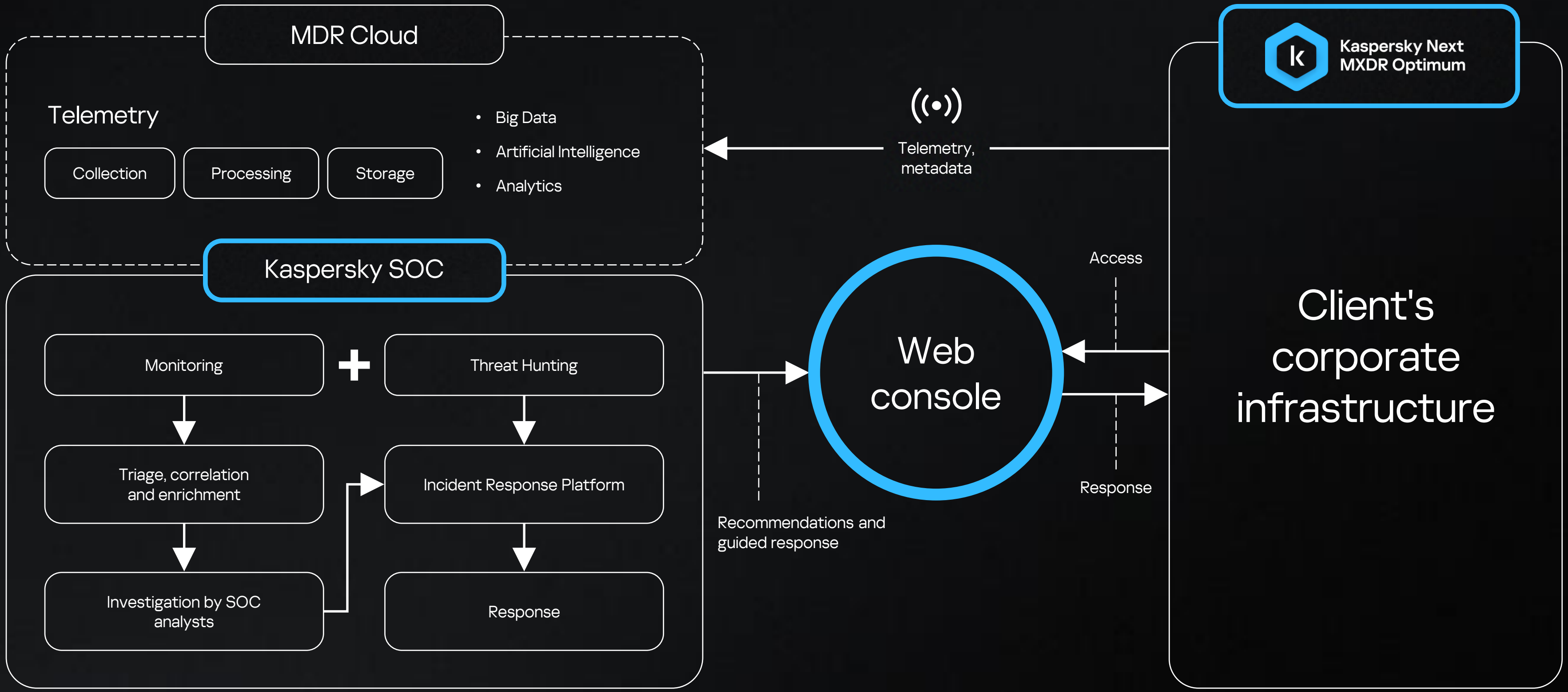
Managed security

1 Kaspersky Next MXDR Optimum captures and forwards data to the Kaspersky SOC.

2 Telemetry, metadata and alert prioritization are analyzed by ML/AI tools, with the active involvement of Kaspersky SOC experts.

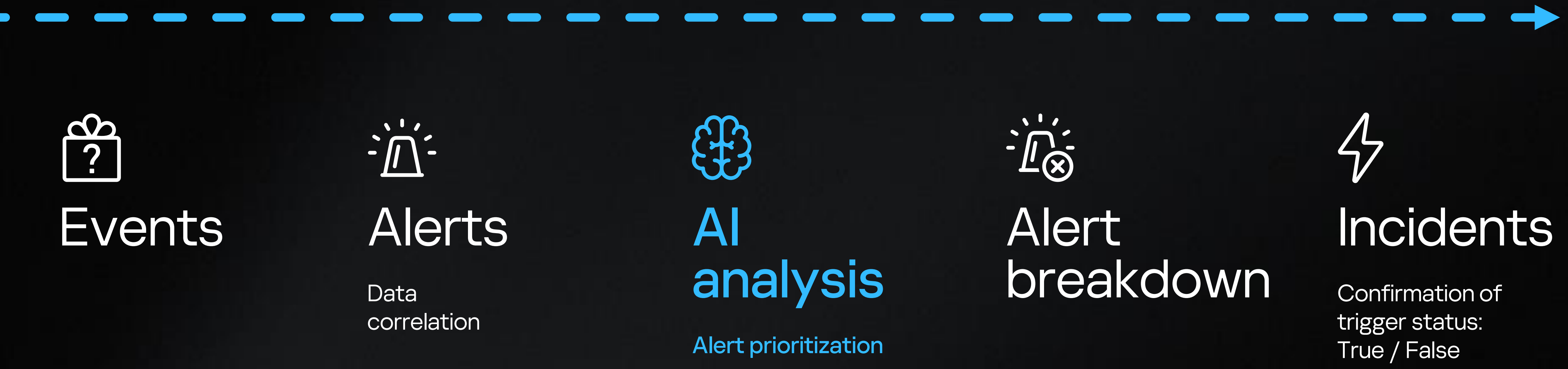
3

The Kaspersky SOC team investigates alerts and notifies you as our client about malicious activity, providing recommendations and step-by-step guided response.


MDR Cloud
Telemetry
Collection
Processing
Storage
• Big Data
• Artificial Intelligence
• Analytics
Kaspersky SOC
Monitoring
+
Threat Hunting
Triage, correlation and enrichment
Incident Response Platform
Investigation by SOC analysts
Response
Telemetry, metadata
Kaspersky Next MXDR Optimum
Access
Web console
Response
Recommendations and guided response
Client's corporate infrastructure

Artificial intelligence (AI) engines

AI mechanisms automatically filter false positives, significantly enhancing analyst productivity and resulting in reduced mean time to prioritization, detection, and response – MTTD / MTTR



Events

Alerts

Data correlation

AI analysis

Alert prioritization

Alert breakdown

Incidents

Confirmation of trigger status: True / False

Capabilities of AI technologies

1

Faster detection

AI analyzes suspicious objects right at the instant the data arrives

2

Resolves 35–40% of alerts

Significantly increases analyst throughput, enabling reduced reaction time SLAs

3

Alert prioritization

Allows our analysts to focus on the most important alerts

4

Automatic alert resolution

No need to involve human analysts

SLA

Priority level	Reaction time	Target value
High (example: targeted attack)	1 hour	90%
Medium (example: common malware)	4 hour	90%
Low (example: adware, riskware, etc.)	24 hours	90%

Reaction time

The time from detection of the incident (‘Created time’) to publishing it on the MDR console (‘Updated time’).

Target value

Percentage of incidents where the reaction time and the response time meet the target value objective.

More information including incident criteria can be found in Terms and Conditions

Advantages of Kaspersky Next MXDR Optimum

Expert response when you need it most — at no extra charge

Access to Kaspersky’s elite Global Emergency Response Team is included, for rapid breach containment whenever it’s needed.

Rapid damage control to prevent escalation

Our experts know exactly what to do and how to do it quickly in order to contain the incident and prevent further damage (financial losses, reputational damage etc).

Learn from global cybersecurity experts

Work with internationally renowned experts who have resolved major incidents across many different industries, and who apply their insights to strengthen your own security strategies.

Strengthen your defenses with actionable guidance

Use extended response tools to clarify any uncertainties at the right moment, helping neutralize similar incidents in the future.

Additional protection

Cloud security

Cloud discovery

Monitor the usage of 2700+ services to discover unauthorized cloud usage

Cloud blocking

Block user access to inappropriate or unauthorized cloud resources, social networks or messengers

Data discovery

Gain visibility and control of sensitive data in MS SharePoint Online, OneDrive and Teams

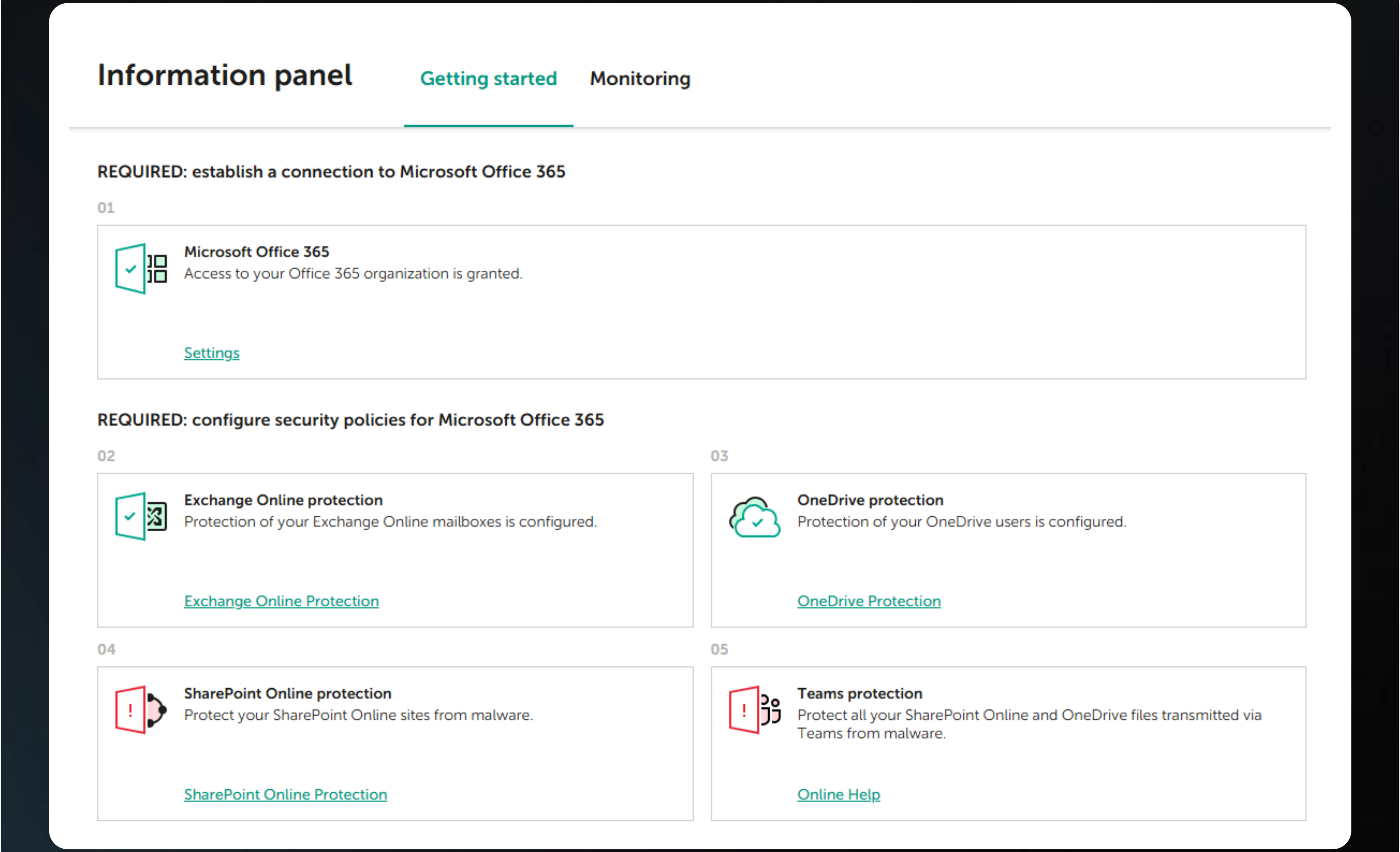
Office 365 security

Anti-phishing, anti-malware, antispam, removal of unwanted attachments

Find out what sensitive data is stored in Microsoft 365 apps.

Office 365 security

- Advanced threat protection
- Anti-phishing, anti-malware, anti-spam, removal of malicious attachments
- For all major MS Office 365 applications



REQUIRED: establish a connection to Microsoft Office 365

01 **Microsoft Office 365**
Access to your Office 365 organization is granted.
Settings

REQUIRED: configure security policies for Microsoft Office 365

02 **Exchange Online protection**
Protection of your Exchange Online mailboxes is configured.
Exchange Online Protection

03 **OneDrive protection**
Protection of your OneDrive users is configured.
OneDrive Protection

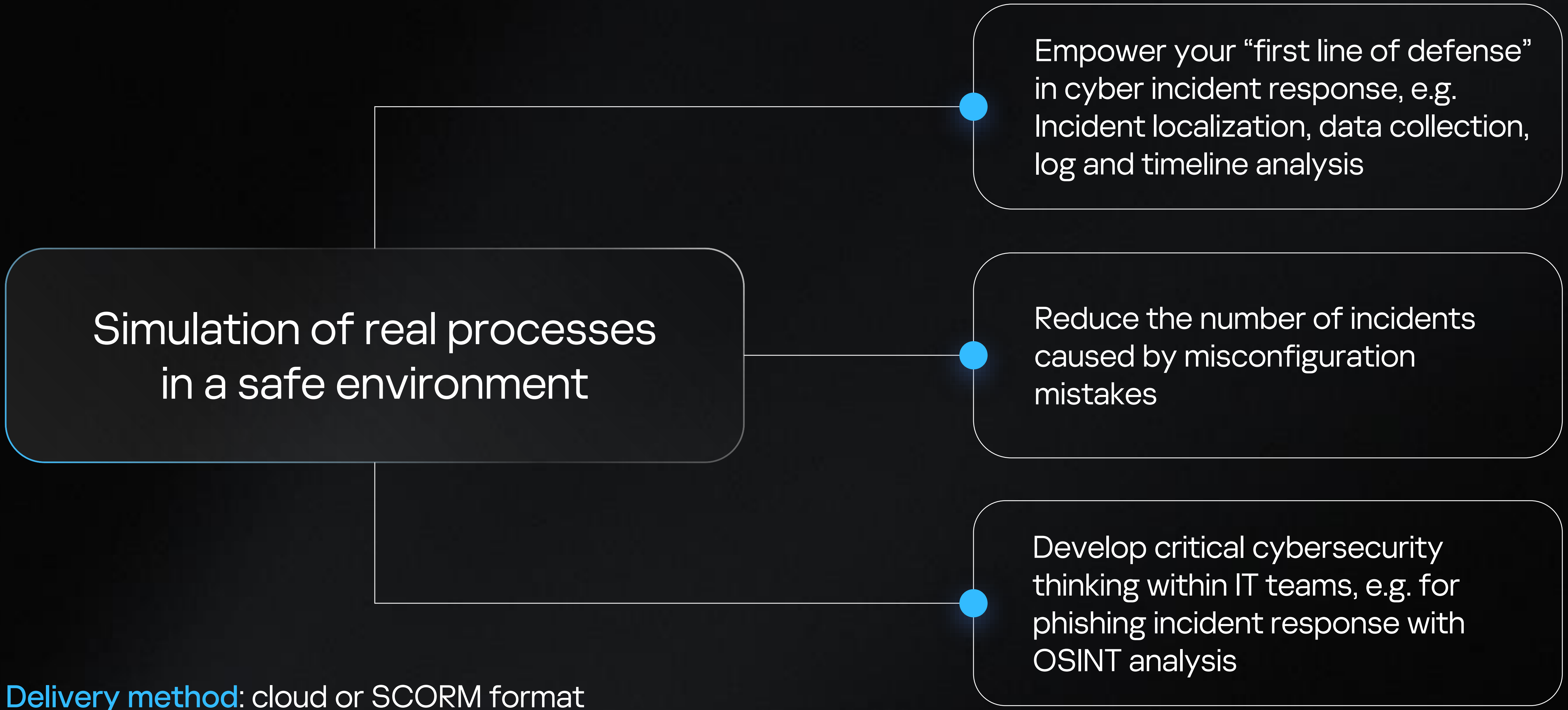
04 **SharePoint Online protection**
Protect your SharePoint Online sites from malware.
SharePoint Online Protection

05 **Teams protection**
Protect all your SharePoint Online and OneDrive files transmitted via Teams from malware.
Online Help

Train your entire team to be more secure and protected

By equipping IT staff and non-technical employees with essential knowledge and skills, organizations strengthen their IT security team while cultivating a strong security-conscious culture across the workforce. This helps protect critical assets, ensure compliance and maintain trust.

Cybersecurity trainings for IT



Simulation of real processes in a safe environment

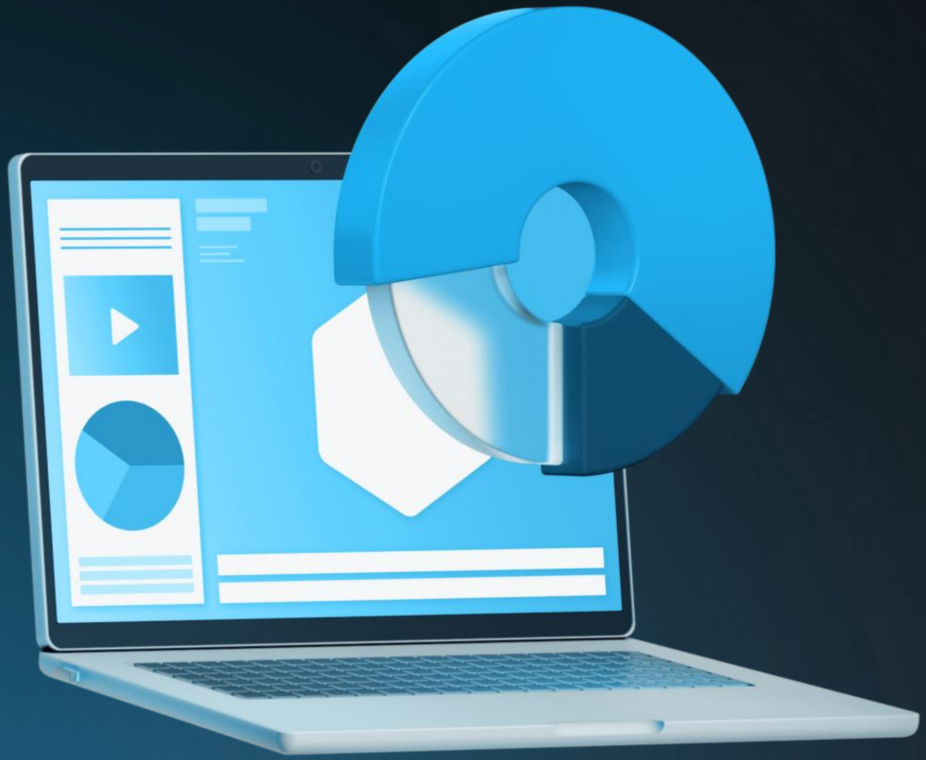
Empower your “first line of defense” in cyber incident response, e.g. Incident localization, data collection, log and timeline analysis

Reduce the number of incidents caused by misconfiguration mistakes

Develop critical cybersecurity thinking within IT teams, e.g. for phishing incident response with OSINT analysis

Delivery method: cloud or SCORM format

The solution includes trainings for the users with access to our online learning platform that builds cybersecurity awareness



- Ease of use and learning efficiency for employees
- Time-saving program administration for companies
- Launch your awareness program in just a few steps

Optimum offering for mid-sized businesses

Kaspersky Next EDR Foundations

Automated protection from mass threats

- Multi-layered anti-malware
- Behavior detection
- Exploit prevention
- Universal Linux Kernel Module (ULKM)
- Remediation engine
- File, email, web and network threat protection on endpoint level
- Firewall
- Host Intrusion Prevention
- AMSI protection
- BadUSB attack prevention
- Root cause analysis with an alert card
- Global threat intelligence via Kaspersky Security Network
- Mobile threat defense

System hardening

- Vulnerability assessment
- Hardware and software inventory
- Application, web and device controls
- Mobile device management (MDM)
- Remote troubleshooting
- Third-party apps & OS installation

Cloud security

- Cloud discovery

+

Kaspersky Next EDR Optimum

Endpoint detection and response to complex threats

- Indicators of compromise (IoC) search with automatic cross-endpoint response
- Adaptive anomaly control
- Single-click and guided response
- System critical object check
- Move file to quarantine/recover file from quarantine
- Network isolation/remove network isolation
- Get/delete file
- Start/terminate process
- Critical areas scan
- Execution prevention
- Execute command

System hardening

- Patch management
- Remote wipe
- Encryption management
- Advanced MDM

Cloud security

- Cloud blocking
- Data discovery
- Security for Microsoft Office 365: Exchange, OneDrive, SharePoint, Teams

IT training

- Cybersecurity training for IT administrators

+

NEW

Kaspersky Next XDR Optimum

Extended detection and response to complex threats

- Alerts aggregation
- Active Directory Response from the alert card

Automated Security Awareness Platform

- Flexible security awareness training for employees
- Customizable courses available in 25 languages
- Security awareness dashboards and reports
- Simulated phishing campaigns
- Video and audio training formats
- Automated Security Awareness Platform response from the alert card

Kaspersky Cloud Sandbox

- Uploading and executing a file in Cloud Sandbox
- Uploading a file from a web address and then execute it in Cloud Sandbox
- Anti-evasion features to counter malware designed to avoid sandboxes
- Executing the extracted file from the Cloud Sandbox report
- Exporting the analysis results
- Automatic detection of file types
- Managing obsolete tasks for execution

+

NEW

Kaspersky Next MXDR Optimum

Managed protection

- 24/7 continuous monitoring and threat hunting
- Incident submitting for further investigation by Kaspersky SOC
- Direct communication with the SOC team about incidents
- Notifications about incidents via email/Telegram
- Guided and automated response scenarios
- REST API for integration with IRP/SOAR
- Artificial Intelligence mechanisms accelerating incident investigation
- Assets visibility with their current statuses
- Compatibility with third-party EPP applications
- User-friendly MDR portal dashboards
- Regular reports
- Raw telemetry storage for 3 months

kaspersky

Trust your cybersecurity
to the experts and focus on your business

Explore

Learn more about
the product