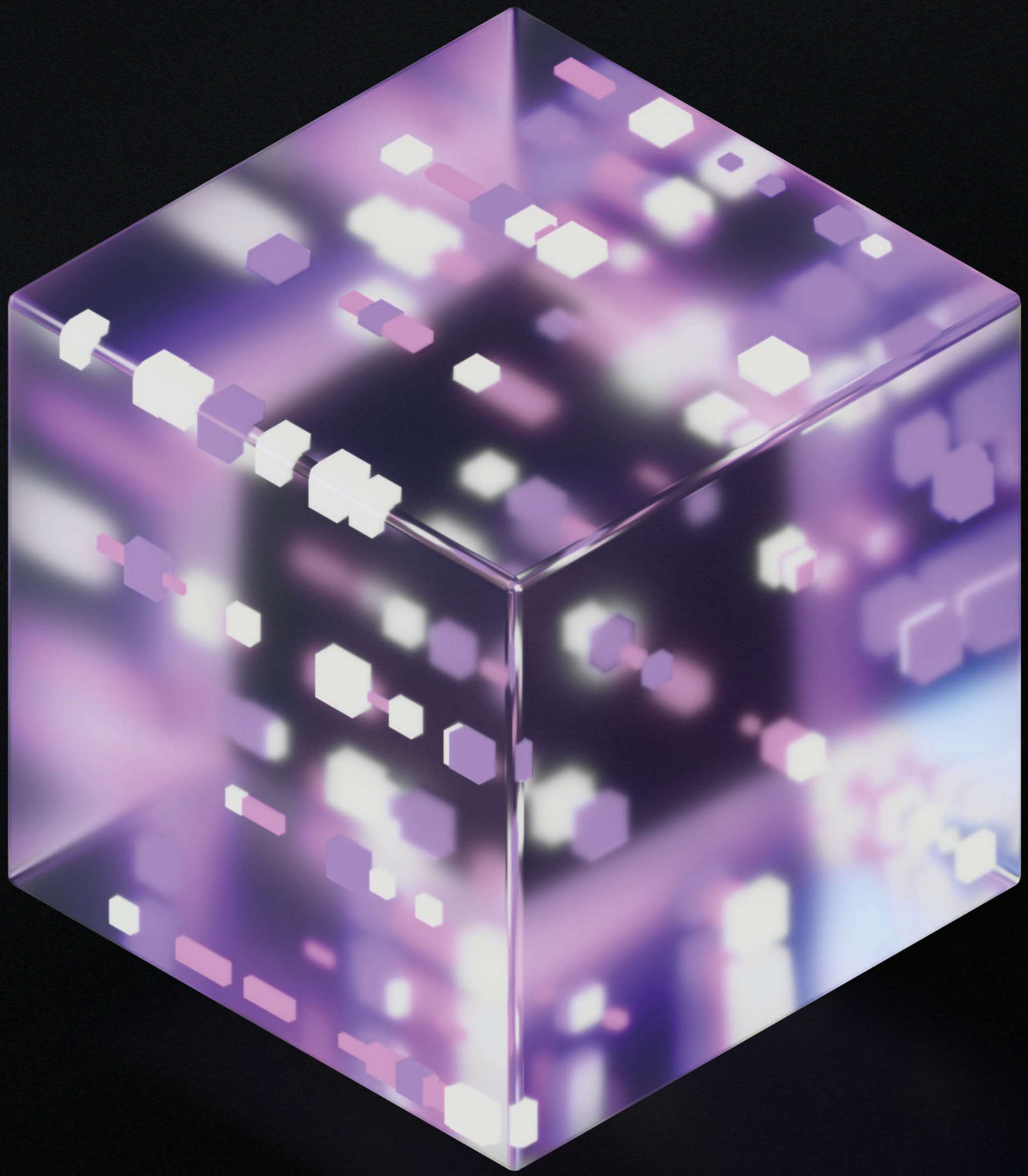
Kaspersky Enterprise Cybersecurity

kaspersky bring on the future

Why choose Kaspersky?

Discover how Kaspersky's world-class expertise and AI-powered portfolio are redefining enterprise cybersecurity.

Kaspersky is more than just a cybersecurity provider — we're a trusted global partner, combining decades of experience with relentless innovation and a dedication to transparency. Our advanced solutions, built on rigorous research, real-world testing and an AI-driven approach, deliver uncompromising protection for enterprises.



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

AI at the core of the Kaspersky portfolio

For **over 20 years,** Kaspersky has used ML and AI to stay ahead of evolving cyberthreats

Our **dedicated AI Technology Research Center** drives innovation while ensuring AI and ML are used securely and ethically.

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
- Establishing guidelines for the safe deployment of AI systems
- Conducting GenAI research using Kaspersky's large language model (LLM) infrastructure

Learn more

50,000
files

100,000
users / day

Trained flexible hash with an integrated ML model

~1000
phishing web pages detected / day

ML-based web phishing detection engine

15,000
files

7,000
users / day

ML-enabled detection record generation

100,000
files / day

Large neural network to detect malware in-lab

Five key ways in which AI enables us to protect our customers better than anyone else:

1. AI- and ML-powered threat discovery
2. Enhancing security operations efficiency through AI
3. GenAI for threat intelligence and security operations
4. Secure AI approaches and methodologies
5. AI-based behavior analysis and anomaly detection in IT and operational technology (OT) environments

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

INTERPOL

PARIS CALL
FOR TRUST AND SECURITY
IN CYBERSPACE
11 · 12 · 2018

industrial internet®
CONSORTIUM

AFRIPOL

Coalition
Against
Stalkerware

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

Bug bounty

Learn more

Recognition that matters

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

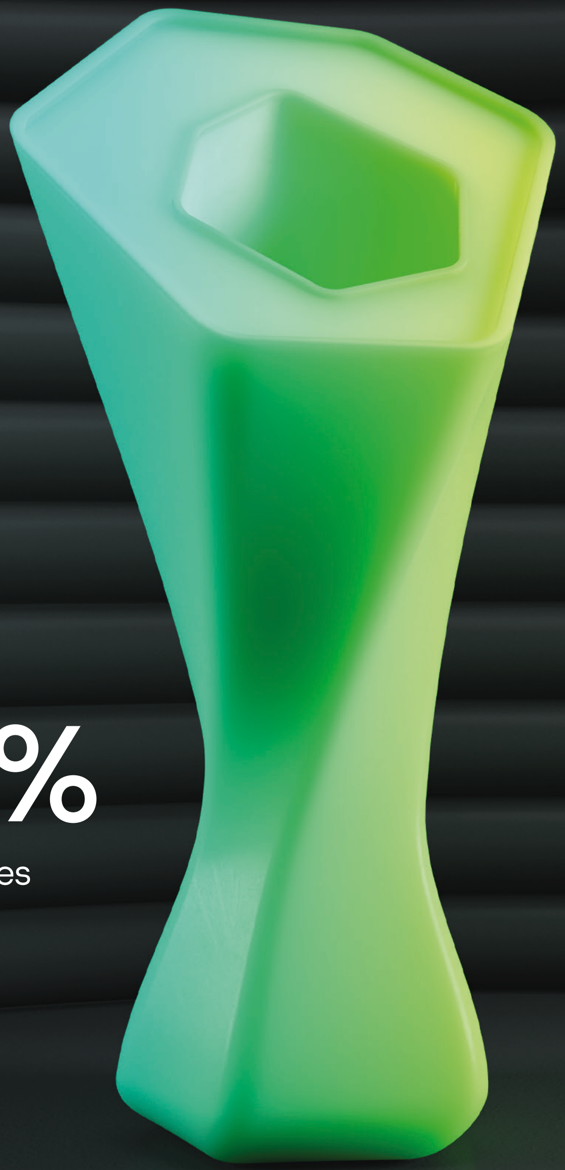
Most tested. Most awarded.

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	91	97%
Tests & reviews	First places	TOP3 places

Learn more



Driving innovation, ready for tomorrow's challenges

Patents, inventions, ML / AI, our own operating system (OS)

1,500+

successfully registered patents

500+

inventions between 2005–2024

20+ years

driving innovations in ML and AI, we embed AI tools into our processes and cybersecurity solutions architecture

KasperskyOS
Be Immune

Our groundbreaking **KasperskyOS** enables the shift from cybersecurity to Cyber Immunity.

About KasperskyOS

Microkernel operating system with enhanced cybersecurity requirements

- Microkernel architecture minimizes the attack surface and risk of vulnerabilities and the security monitor makes unauthorized actions impossible
- Developed from scratch by Kaspersky and doesn't contain any third-party code in the kernel
- Foundation for creating Cyber Immune products and solutions

kaspersky cyber immunity

Cyber Immunity is our approach and methodology for developing secure-by-design solutions

Cyber Immune systems are specifically designed to resist even unknown threats and maintain stable operation under attack.

Designing a Cyber Immune future

KasperskyOS-based Cyber Immune solutions are engineered with innate protection, providing built-in defenses against malicious code and hacker intrusions to protect your critical systems at the core.

Kaspersky Thin Client

Kaspersky IoT Secure Gateway

Kaspersky Automotive Secure Gateway

KasperskyOS Mobile

KasperskyOS-based solutions are backed by a comprehensive ecosystem partner program, driving innovation and growth through co-development. With Kaspersky Appicenter, a one-stop shop for application developers and global hardware vendors, partners gain the tools and support they need to succeed.

Kaspersky Appicenter

Learn more

Cybersecurity built for your business

We have the experience, expertise, insights and adaptability to meet you where you are — and take you where you need to go, safely.

Portfolio

Turning IT and OT risks into resilience

Cybercrime evolves. So do we. Whether working in IT, OT or convergence environments, our solutions mitigate the most critical impact of cybercrime.

Corporate environment

+

Industrial environment

Cybercrime can trigger financial downturns, downtime, data breaches and fraud, leading to customer loss and severe reputational damage.

Attacks can disrupt production, cause financial losses and steal intellectual property, jeopardizing technological stability and business continuity.

Challenges

- An expanding attack surface
- New and evolving threats and vulnerabilities
- Compliance
- Experts and Skills shortages
- Legacy systems
- Budget constraints

01

Unlock your cyberdefense

Flip the page to explore our portfolio, built around three key pillars to strengthen your defense at every stage.

Technologies

1

Equip your in-house experts with the tools and capabilities needed to detect and respond to cyberthreats

Knowledge

2

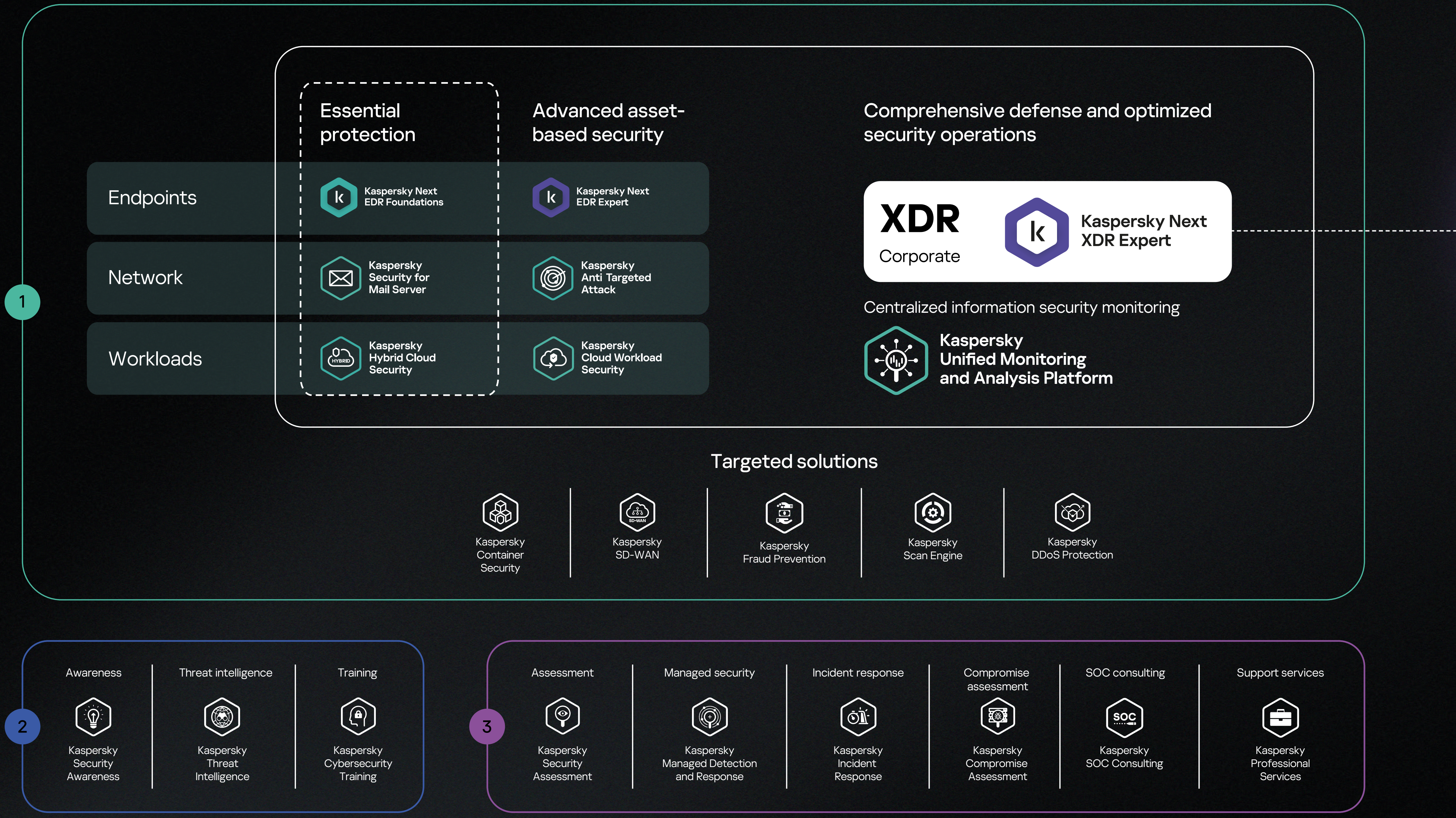
Stay informed about evolving threats, continuously upskill your team to handle incidents effectively and promote security awareness

Expertise

3

Access external experts for assessments, immediate incident response and strategic guidance

Kaspersky for IT environments



1

Essential protection

Advanced asset-based security

Comprehensive defense and optimized security operations

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

Kaspersky Security Awareness

Threat intelligence

Kaspersky Threat Intelligence

Training

Kaspersky Cybersecurity Training

3

Assessment

Kaspersky Security Assessment

Managed security

Kaspersky Managed Detection and Response

Incident response

Kaspersky Incident Response

Compromise assessment

Kaspersky Compromise Assessment

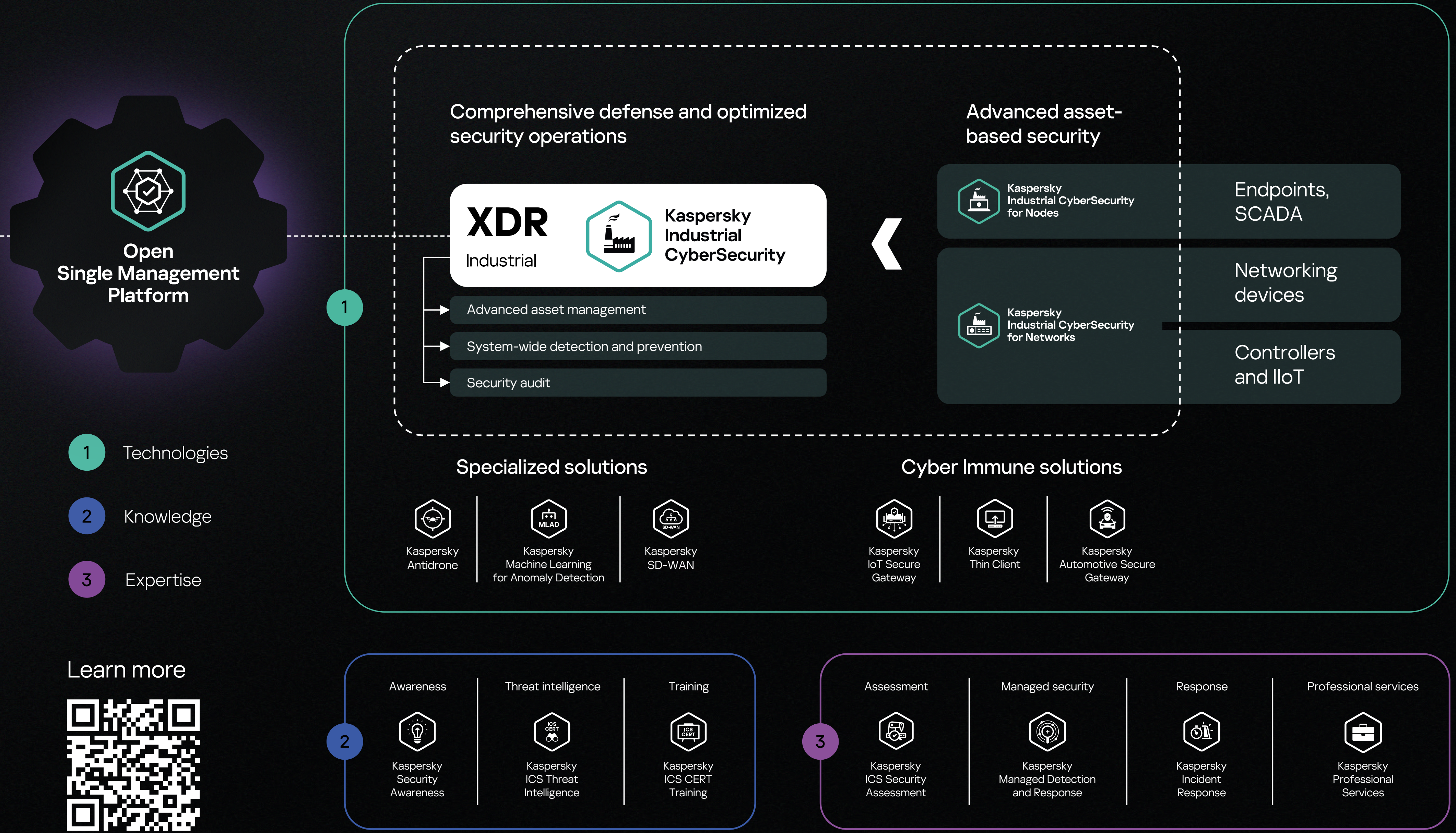
SOC consulting

Kaspersky SOC Consulting

Support services

Kaspersky Professional Services

Kaspersky for OT environments



Open Single Management Platform

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	Training
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

1 Technologies

2 Knowledge

3 Expertise

Learn more

Open Single Management Platform for IT, OT, and hybrid scenarios

Corporate cybersecurity

XDR

Kaspersky Next XDR Expert

Learn more

Open Single Management Platform

Cybersecurity
at the convergence of IT
and OT environments

Industrial cybersecurity

XDR

Kaspersky Industrial CyberSecurity

Learn more

The Open Single Management Platform provides a comprehensive view of the security posture of an organization's infrastructure. It streamlines incident management, administration and security maintenance.

The platform is a key embedded component of Kaspersky Next XDR Expert and our unified IT-OT XDR technology stack, helping to defend against complex cyberattacks that can move between IT and OT environments.

- Incident management from a single console
- Automation and orchestration
- Deployment toolkit

- Centralized asset and case management
- Playbooks
- Investigation graph

Kaspersky
Next

A core cybersecurity proposal for corporate environments

Kaspersky Next is a next-generation product line built to protect against the onslaught of today's sophisticated and emerging corporate cyberthreats, with leading-edge endpoint protection (EPP), endpoint detection and response (EDR) and extended detection and response (XDR) that stops attacks in their tracks.

Learn more

Kaspersky Next:
Take your corporate security to the next level

Kaspersky Next EDR Optimum

Optimum defense against advanced threats

EDR for small cybersecurity teams

- Strong endpoint protection
- Advanced security controls
- Enhanced EDR capabilities
- Expanded cloud security
- Cybersecurity training for IT administrators

Kaspersky Next XDR Expert

Expert defense against the most sophisticated threats

Ultimate XDR for large cybersecurity or SOC teams

- Strong endpoint protection
- Advanced security controls
- Powerful EDR capabilities
- Advanced threat detection and response across the infrastructure
- Investigation graph & case management & playbooks
- Seamless 3rd party integration

Kaspersky Next EDR Foundations

Fundamental protection from mass threats

Unequalled endpoint protection

- Strong endpoint protection
- Basic security controls
- Basic EDR capabilities
- Maximum automation

Open XDR platform that defends against sophisticated cyberthreats

Kaspersky Next XDR Expert

Designed to accelerate threat detection, provide real-time visibility and automate response, it delivers comprehensive cybersecurity for proactive cyberthreat defense.

How we help

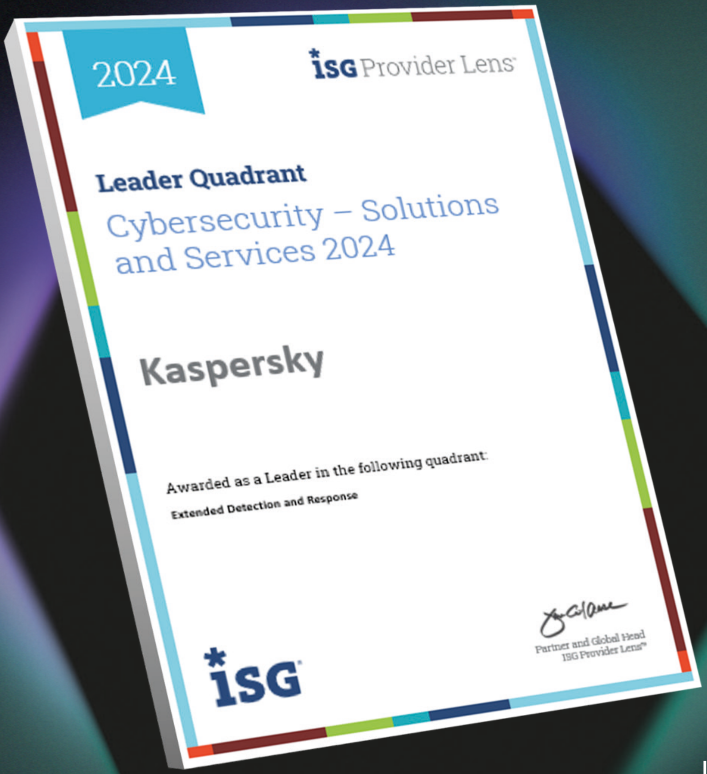
Identify complex and persistent threats with improved mean time to detect (MTTD) and automated operations that speed up mean time to response (MTTR).

Monitoring, detection, threat hunting and investigation with AI assistance.

Endpoint, hybrid cloud and mail protection.

Increase efficiency with advanced case management.

Kaspersky has been recognized as a leader in the XDR category for the second year in a row



2024

ISG Provider Lens

Leader Quadrant

Cybersecurity – Solutions and Services 2024

Kaspersky

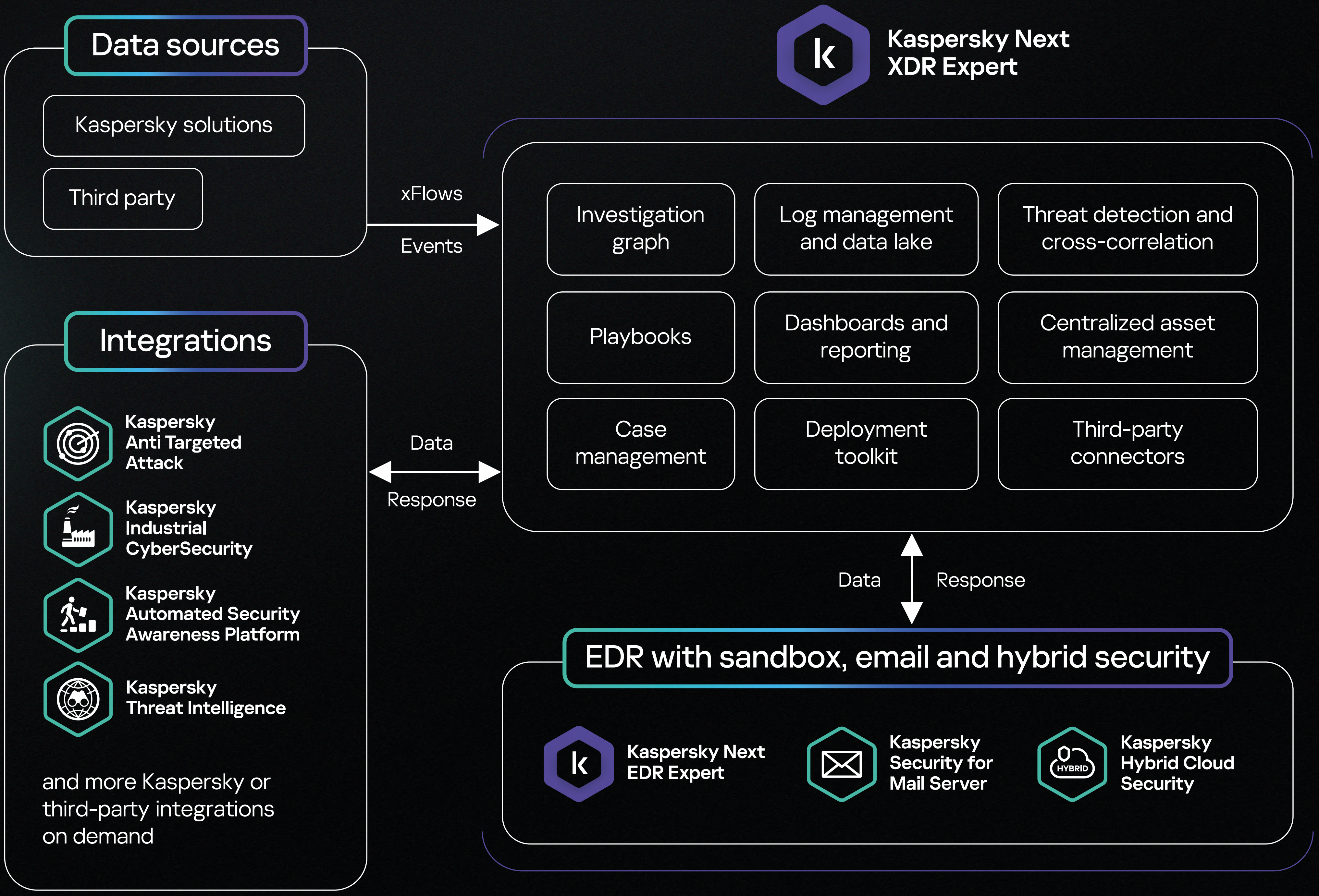
Awarded as a Leader in the following quadrant:

Extended Detection and Response

Partner and Global Head
ISG Provider Lens™

ISG

Learn more



Data sources

Kaspersky solutions

Third party

xFlows

Events

Integrations

Kaspersky Anti Targeted Attack

Kaspersky Industrial CyberSecurity

Kaspersky Automated Security Awareness Platform

Kaspersky Threat Intelligence

and more Kaspersky or third-party integrations on demand

Data

Response

Kaspersky Next XDR Expert

Investigation graph

Log management and data lake

Threat detection and cross-correlation

Playbooks

Dashboards and reporting

Centralized asset management

Case management

Deployment toolkit

Third-party connectors

Data

Response

EDR with sandbox, email and hybrid security

Kaspersky Next EDR Expert

Kaspersky Security for Mail Server

Kaspersky Hybrid Cloud Security

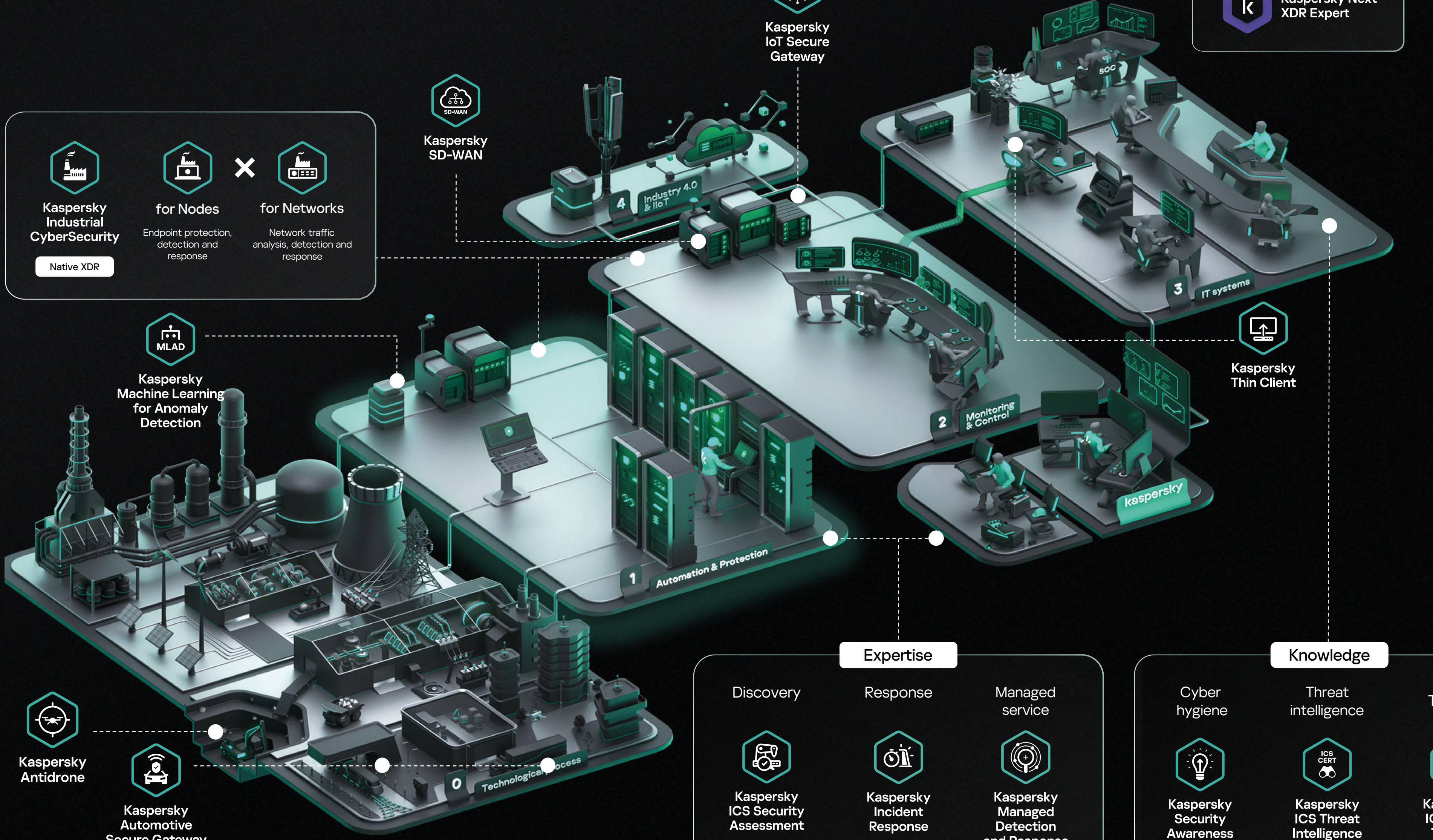
Kaspersky
OT CyberSecurity

A cyber-physical industrial security ecosystem

A unified industrial safety concept bringing together the technologies, knowledge and expertise needed to protect industrial enterprises at every level.

Learn more

End-to-end protection for industrial enterprises



IT-OT convergence

Kaspersky Next XDR Expert

Kaspersky IoT Secure Gateway

Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity

Native XDR

for Nodes ✕ for Networks

Endpoint protection, detection and response

Network traffic analysis, detection and response

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Thin Client

Kaspersky Antidrone

Kaspersky Automotive Secure Gateway

Expertise

Discovery	Response	Managed service
Kaspersky ICS Security Assessment	Kaspersky Incident Response	Kaspersky Managed Detection and Response

Knowledge

Cyber hygiene	Threat intelligence	Training
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

OT XDR platform for critical infrastructure protection

Kaspersky Industrial CyberSecurity

The core of the OT ecosystem, functioning as an XDR platform. It features natively integrated nodes and network security products for the protection of industrial automation and control systems (IACS).

How we help

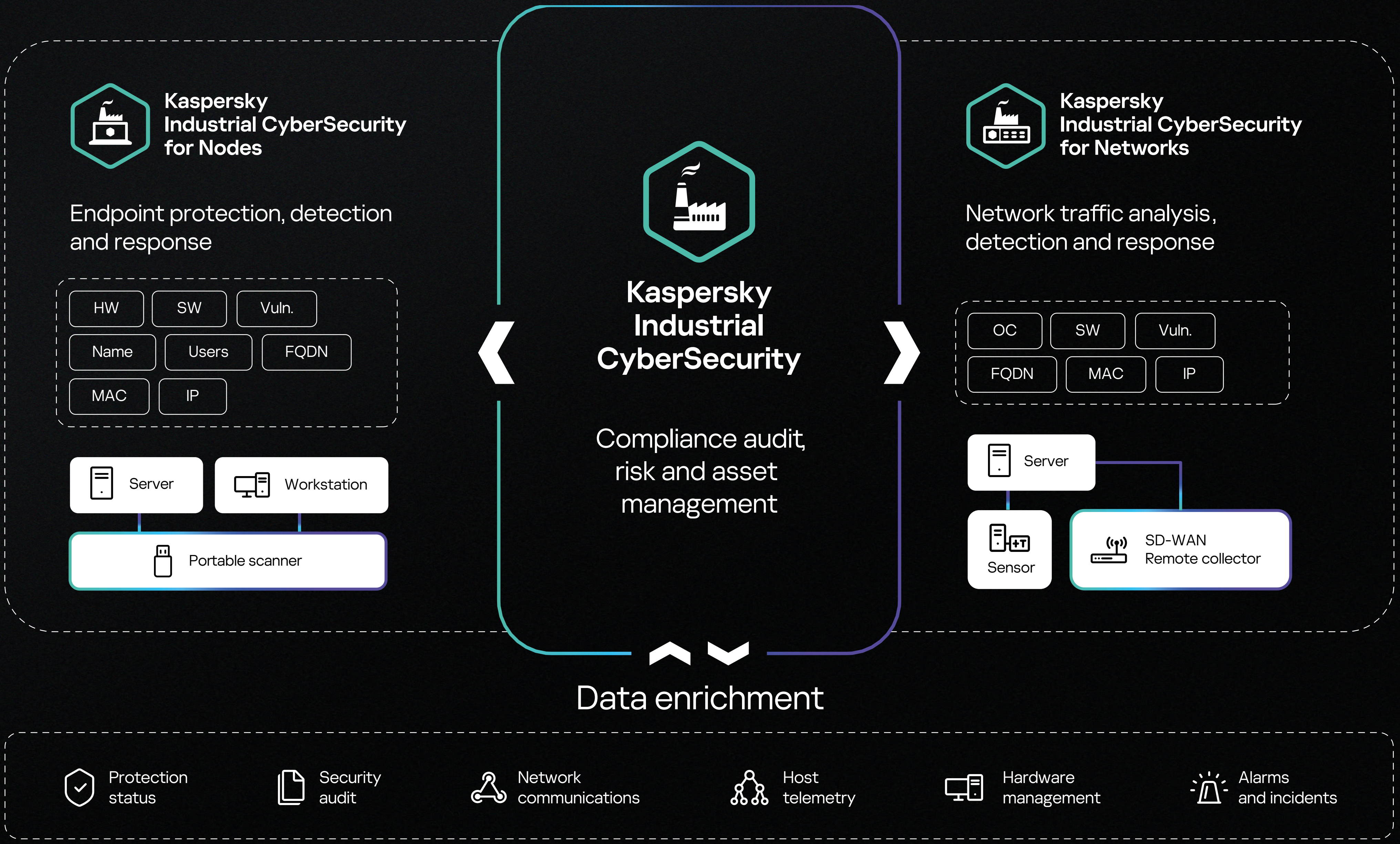
Reveal hidden threats. Detect anomalies, vulnerabilities and intrusion attempts long before they become dangerous.

Manage complex infrastructure. Automate response and management, ensuring quick reactions to incidents.

Operate without affecting technological workflows, ensuring no unacceptable damage occurs.

Meet the highest standards of industrial cybersecurity with our certified solutions.

Learn more



Kaspersky Industrial CyberSecurity for Nodes

Endpoint protection, detection and response

HW
SW
Vuln.
Name
Users
FQDN
MAC
IP

Server
Workstation
Portable scanner

Kaspersky Industrial CyberSecurity

Compliance audit, risk and asset management

Kaspersky Industrial CyberSecurity for Networks

Network traffic analysis, detection and response

OC
SW
Vuln.
FQDN
MAC
IP

Server
Sensor
SD-WAN Remote collector

Data enrichment

Protection status
Security audit
Network communications
Host telemetry
Hardware management
Alarms and incidents

Guiding your SOC to virtuoso-level precision and efficiency

The top challenges for today's SOCs

Cyberthreats are evolving faster than defenses

Skills acquisition and retention

Impact of compliance

Kaspersky helps organizations build robust SOCs, improve their effectiveness and efficiency

02

Run

Managed security

MDR

Kaspersky Managed Detection and Response

- All the major benefits of having your own SOC

Investigation

Incident Response

Kaspersky Incident Response

- Incident response retainer
- Incident response emergency

Build

Core technological stack

SIEM

Kaspersky Unified Monitoring and Analysis Platform

XDR

Kaspersky Next XDR Expert

NDR

Kaspersky Anti Targeted Attack

EDR

Kaspersky Next EDR Expert

Frameworks and processes

Consulting Services

Kaspersky SOC Consulting

- SOC framework development
- Cyberthreat intelligence framework
- Incident response readiness

Improve

Threat intelligence

Data Feeds

Kaspersky Threat Data Feeds

Threat Intelligence Platform

Kaspersky CyberTrace

Threat Intelligence Portal

Kaspersky Threat Intelligence Portal

Threat Intelligence Insights

Kaspersky Ask the Analyst

Skills and performance

Trainings

Kaspersky Cybersecurity Training

- Security operations and threat hunting
- Incident response
- Malware analysis
- Digital forensics

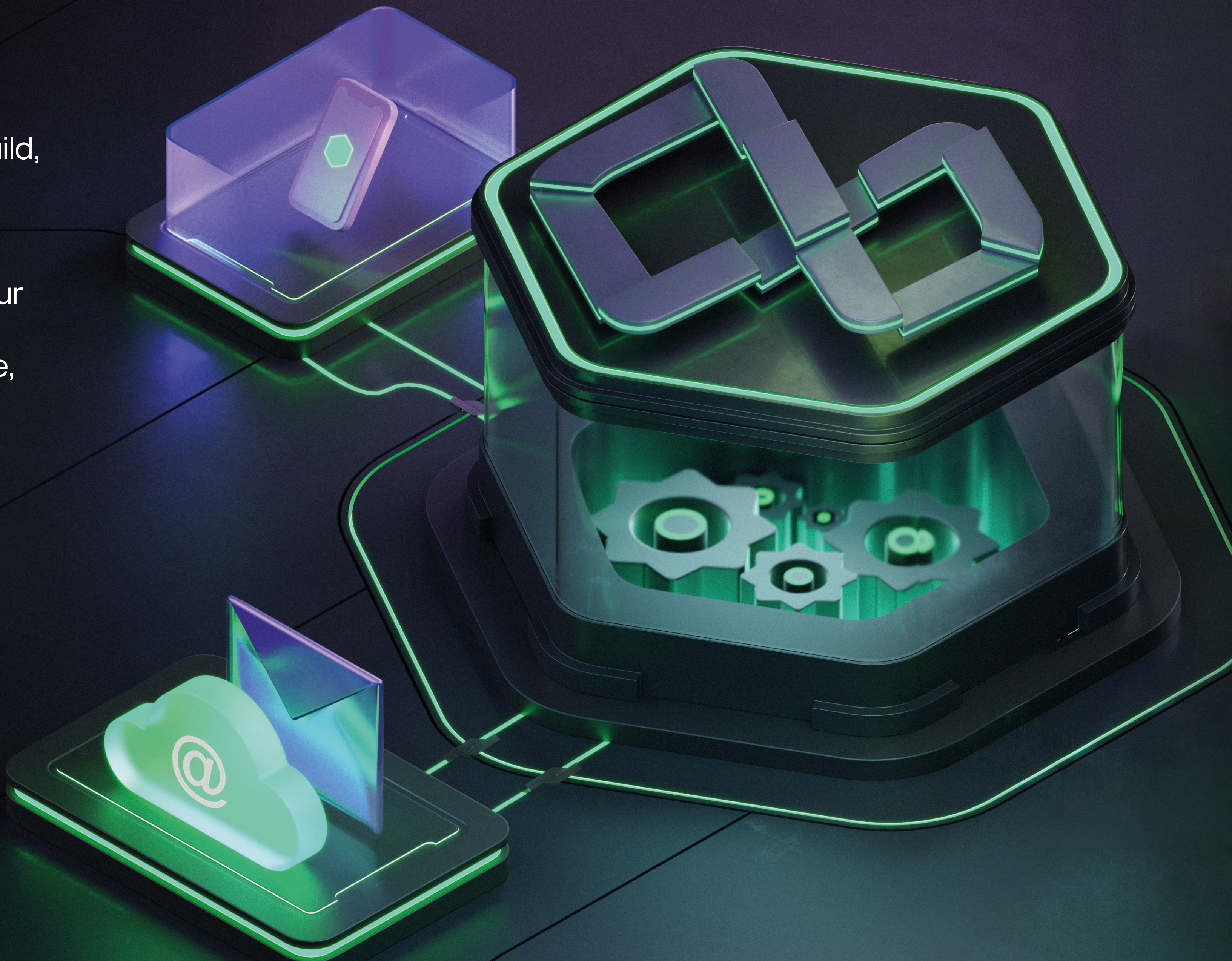
Consulting Services

Kaspersky SOC Consulting

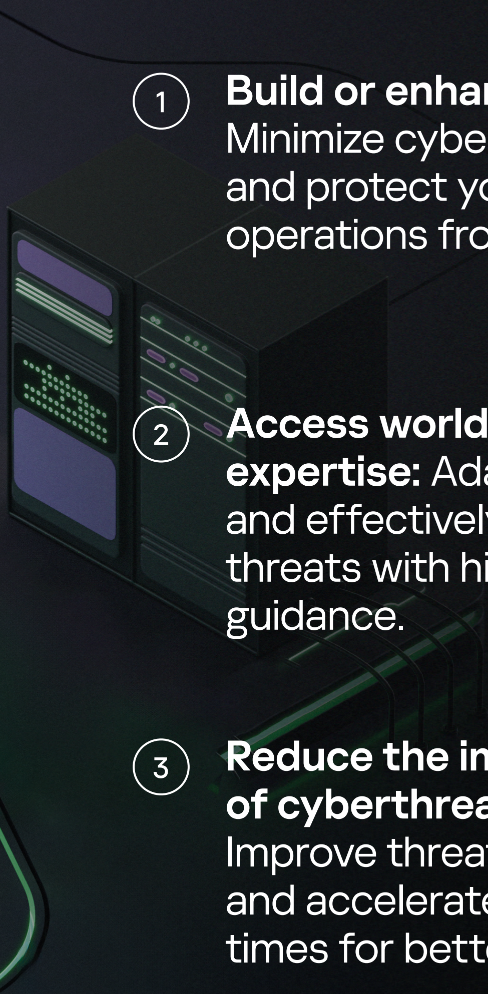
- SOC Maturity assessment
- Tabletop exercise
- Adversary attack emulation

How Kaspersky SOC Consulting benefits your business

Kaspersky SOC Consulting services help businesses build, support or enhance their SOCs. Backed by decades of cybersecurity expertise and experience operating our own SOC across hundreds of infrastructures worldwide, we enable organizations to detect, respond to, and mitigate cyberthreats with greater efficiency and confidence.



Learn more



1. **Build or enhance your SOC:** Minimize cybersecurity risks and protect your business operations from disruption.

2. **Access world-class expertise:** Adapt quickly and effectively to evolving threats with high-level guidance.

3. **Reduce the impact of cyberthreats:** Improve threat detection and accelerate response times for better outcomes.

4. **Optimize resources:** Streamline processes to achieve better IT security results without overspending.

5. **Scale with your business:** Ensure your SOC evolves with your growth, maintaining robust protection as you expand.

6. **Enjoy tailored SOC design:** Address cybersecurity threats specific to your business while considering regulatory requirements.

An advanced AI-enhanced SIEM platform for your SOC

Kaspersky Unified Monitoring and Analysis Platform

A next-generation security information and event management (SIEM) solution for managing security data and events for comprehensive defense.
By collecting logs from all security controls and correlating the data in real time, Kaspersky SIEM aggregates and provides all the information to the SOC for deep incident investigation and response.

How we help

Log management with data sovereignty.

Real-time streaming correlation.

Threat detection, incident response and threat hunting with AI assistance.

Immediate visibility into your security posture, supporting regulatory compliance.

Learn more

Anti-APT solution with NDR and EDR to enpower your SOC

Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack is an advanced anti-APT solution that defends against sophisticated cyberthreats. It provides everything from Network Detection and Response (NDR) to native XDR capabilities, securing key attack entry points at network and endpoint levels. By delivering full visibility across your entire IT infrastructure, it strengthens your SOC's defenses against targeted attacks.

How we help

Defend your corporate infrastructure and your business against sophisticated attacks.

Simplify network traffic and endpoint control via a single interface.

All-in-one security across web traffic, emails, endpoints to protect your business.

Automation of threat discovery and response tasks reduces incident detection and response times.

Learn more

Managing risk with threat intelligence

Integrating machine-readable intelligence, human expertise and strategic guidance to proactively counter evolving threats.

03

Rapidly evolving cyberattacks

The rapid emergence of new vulnerabilities and attack vectors makes it challenging for organizations to stay ahead of potential risks. Tools enhanced with threat intelligence to manage risks more precisely.

And businesses often face new challenges:

Lack of context

Raw threat intelligence often lacks the necessary context, making it difficult for organizations to assess how specific threats impact their operations and assets.

Information overload

Vast amounts of threat data from multiple sources makes it challenging to identify which threats are truly relevant to your environment.

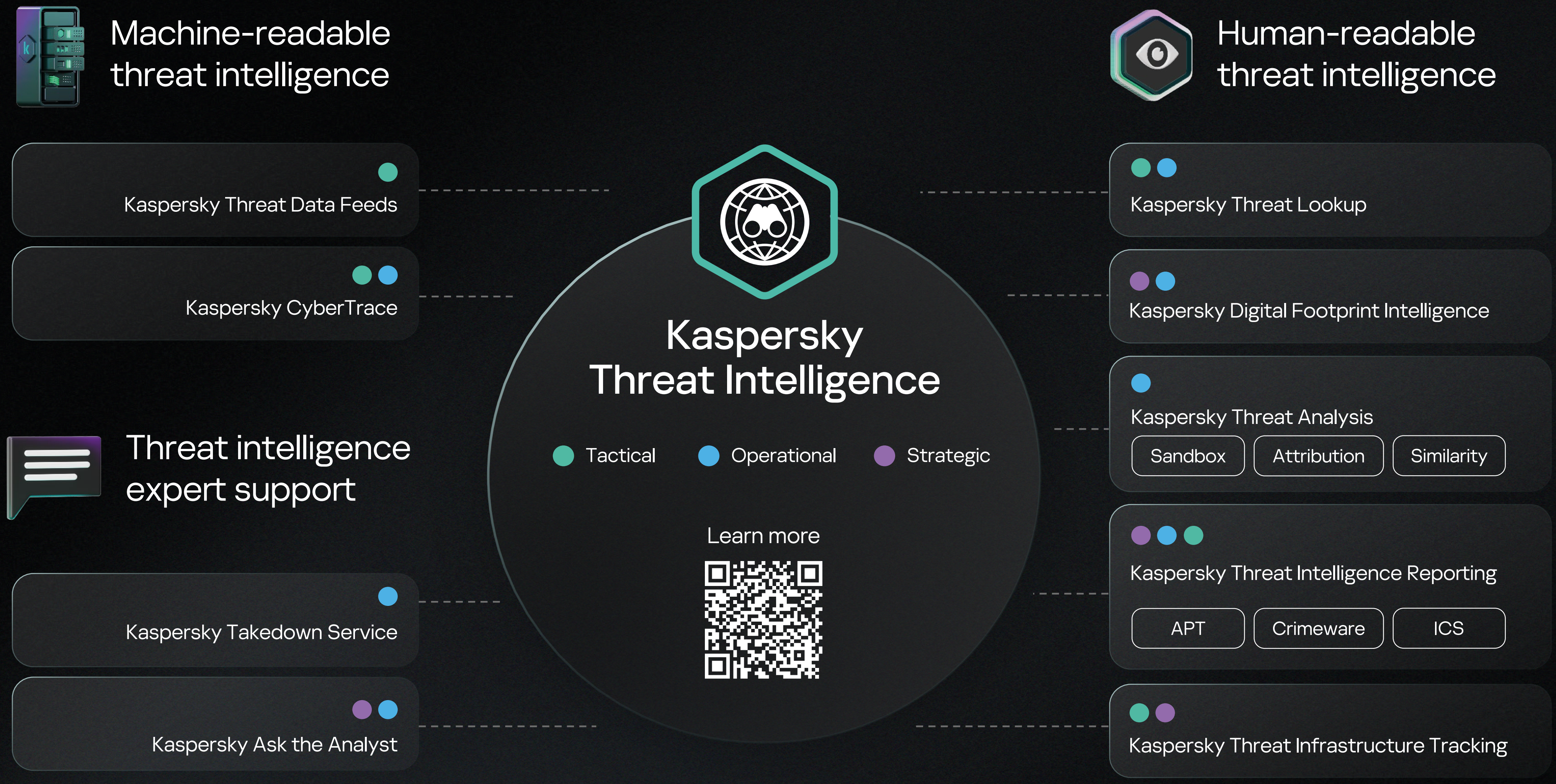
Organizations need aggregated, relevant and up-to-date threat intelligence to gain deep visibility into cyberthreats targeting their business — ensuring they stay prepared and protected.

→

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence delivers a comprehensive 360-degree view of the global threat landscape, including the tools and tactics used by threat actors. By combining intelligence sources and threat data feeds, it delivers instant access to tactical, operational and strategic threat intelligence — consolidating all acquired cyberthreat knowledge into a single access point.

Kaspersky Threat Intelligence — stay ahead of your adversaries



Machine-readable threat intelligence

- 🟢 Kaspersky Threat Data Feeds
- 🟢🔵 Kaspersky CyberTrace

Threat intelligence expert support

- 🔵 Kaspersky Takedown Service
- 🟣🔵 Kaspersky Ask the Analyst

Kaspersky Threat Intelligence

🟢 Tactical 🔵 Operational 🟣 Strategic

Learn more

Human-readable threat intelligence

- 🟢🔵 Kaspersky Threat Lookup
- 🟣🔵 Kaspersky Digital Footprint Intelligence
- 🔵 Kaspersky Threat Analysis: Sandbox | Attribution | Similarity
- 🟣🔵🟢 Kaspersky Threat Intelligence Reporting: APT | Crimeware | ICS
- 🟢🟣 Kaspersky Threat Infrastructure Tracking

Human-readable threat intelligence

Kaspersky Threat Intelligence Portal

Our human-readable threat intelligence is designed for both IT and OT. The Kaspersky Threat Intelligence Portal provides a single access point, where services are integrated to enrich and reinforce one other.

How we help

Provide complete cyberthreat intelligence and relationships through a powerful master search tool spanning all active threat intelligence products and external sources.

Automate the routine analysis of suspicious files using sandboxing, state-of-the-art attribution and similarity technologies.

Deliver a comprehensive view of your digital footprint, including any assets that may be vulnerable to attack or compromise.

Offer multiple commercial reporting tracks tailored to your specific needs.

Powered by Kaspersky Threat Landscape — region- and industry-specific threat intelligence that helps organizations understand the exact threats they face.

Try our industry-leading threat intelligence

Machine-readable threat intelligence

Kaspersky Threat Data Feeds

Over 30 threat data feeds tailored to diverse security needs, covering both IT and OT.

How we help

Reinforce your security solutions including SIEMs, NGFW, IPS/IDS, security proxy, etc., with continuously updated IoCs and actionable context.

Improve incident response by automating initial triage while equipping security analysts with the context they need.

Prevent threats and manage vulnerabilities related to all industries and to industrial organizations in particular.

Flexible delivery formats and mechanisms allow easy integration into security controls.

General threat data feeds

- Malicious URL
- Ransomware URL
- Phishing URL
- Botnet C&C URL
- Mobile Botnet C&C URL
- Malicious Hashes
- Mobile Malicious Hashes
- IP Reputation
- IoT URL
- ICS Hashes
- APT Hashes
- APT IP
- APT URL
- Crimeware Hashes
- Crimeware URL

Delivered to: SIEM, SOAR, IPR, TIP, EDR, XDR, etc.

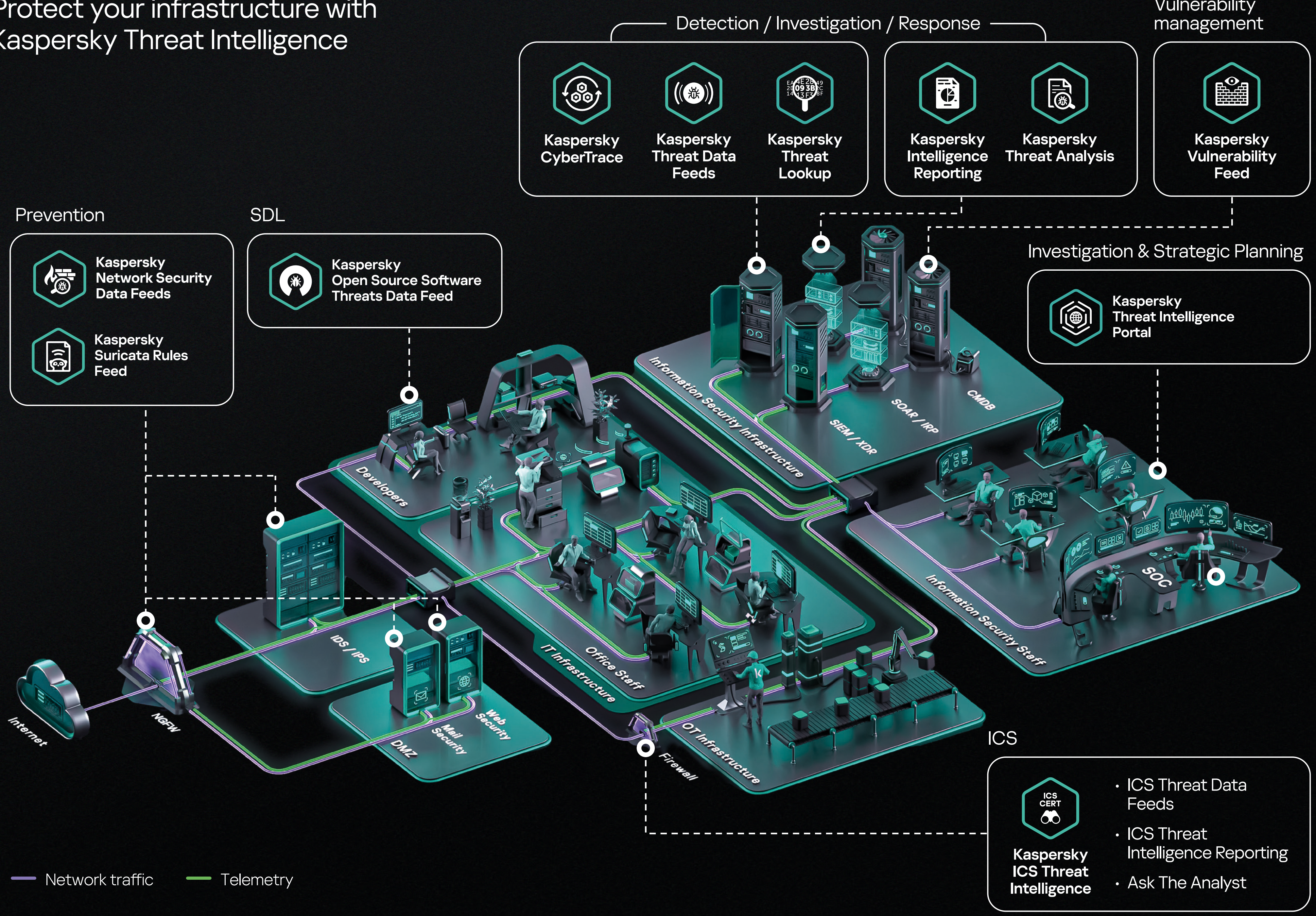
Kaspersky CyberTrace

Kaspersky Threat Data Feeds can be integrated with third-party Threat Intelligence platforms and with our own Kaspersky CyberTrace.

Specific threat data feeds

- Network Security Data Feeds (for NGFW)
- Suricata Rules Feed (for IDS / IPS)
- Sigma Rules Data Feed (for SIEM/EDR)
- Yara Rules Data Feeds (for YARA-scanner)
- Vulnerability / ICS Vulnerability Feed (SBOM /CMDB)
- Open Source Software Threats Data Feed (OSA /CSA / ASOC)
- Cloud Access Security Broker Data Feed (CASB)

Protect your infrastructure with Kaspersky Threat Intelligence



Detection / Investigation / Response

Kaspersky CyberTrace

Kaspersky Threat Data Feeds

Kaspersky Threat Lookup

Kaspersky Intelligence Reporting

Kaspersky Threat Analysis

Vulnerability management

Kaspersky Vulnerability Feed

Prevention

Kaspersky Network Security Data Feeds

Kaspersky Suricata Rules Feed

SDL

Kaspersky Open Source Software Threats Data Feed

Investigation & Strategic Planning

Kaspersky Threat Intelligence Portal

ICS

Kaspersky ICS Threat Intelligence

- ICS Threat Data Feeds
- ICS Threat Intelligence Reporting
- Ask The Analyst

▬ Network traffic ▬ Telemetry

Create safe DevOps environments and protect your cloud workloads

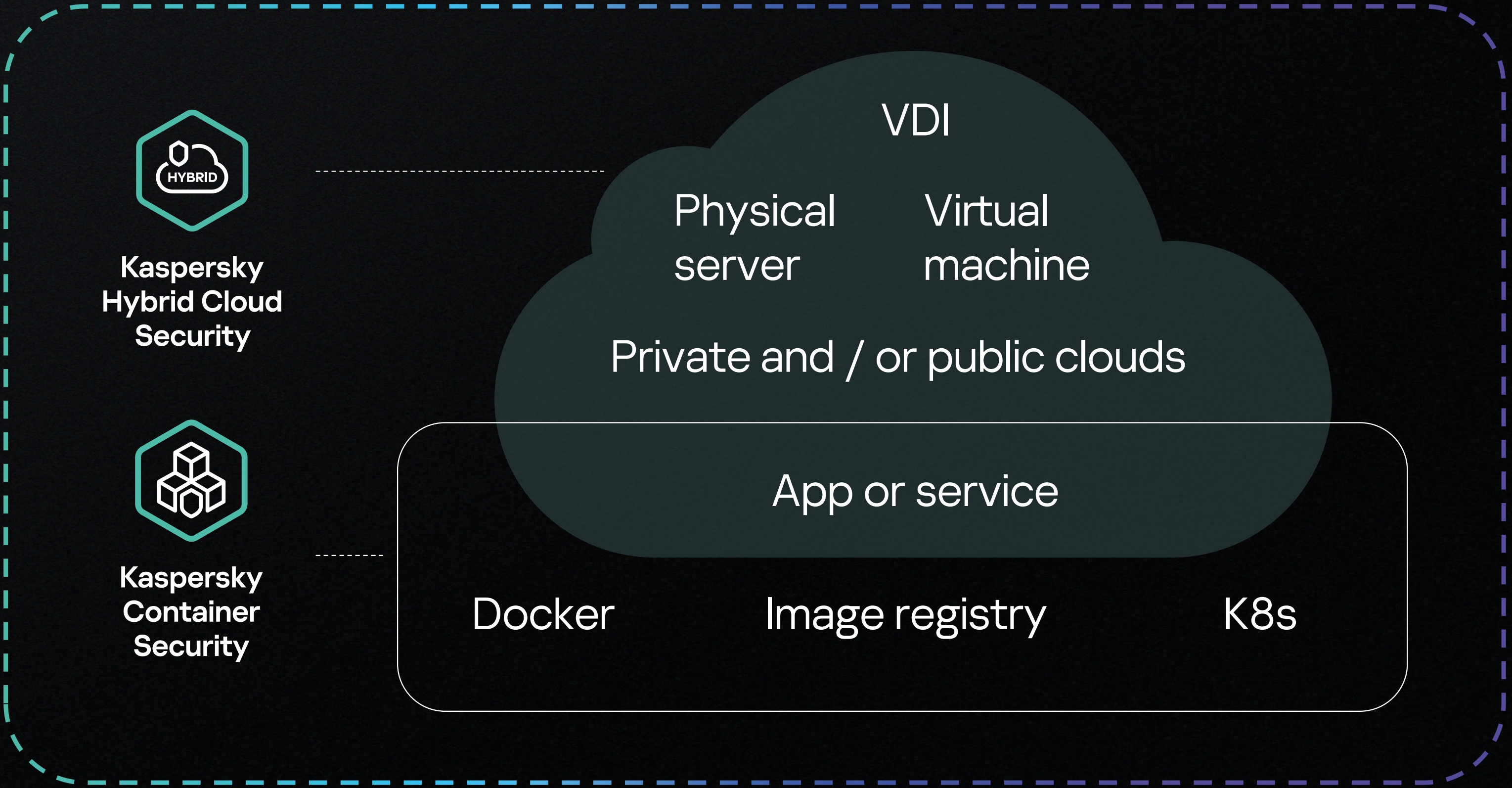
Cloud migration and containerization strengthen business agility, resilience and competitiveness — but also introduce new cybersecurity challenges

Challenges

- Insecure third-party resources
- Limited visibility and control in hybrid cloud environments
- Insecure software development (including container images and runtime)

04

Kaspersky Cloud Workload Security



Kaspersky Hybrid Cloud Security
HYBRID
Kaspersky Container Security
VDI
Physical server
Virtual machine
Private and / or public clouds
App or service
Docker
Image registry
K8s

Developers rely on containerization, and businesses are scaling their cloud environments. However, the specific security risks of these environments can cause significant damage and require specialized protection solutions.

Kaspersky Cloud Workload Security is specifically designed to protect DevOps and cloud environments. It mitigates cloud risks with multi-layered threat protection and ensures full visibility across private, public, and hybrid clouds. It secures CI/CD pipelines and containerized applications by protecting key components throughout the development lifecycle.

Learn more

Hybrid Cloud Security

Kaspersky Hybrid Cloud Security

Secures your entire hybrid infrastructure to defend against the broadest range of cloud-related cyberattacks while going easy on your resources.

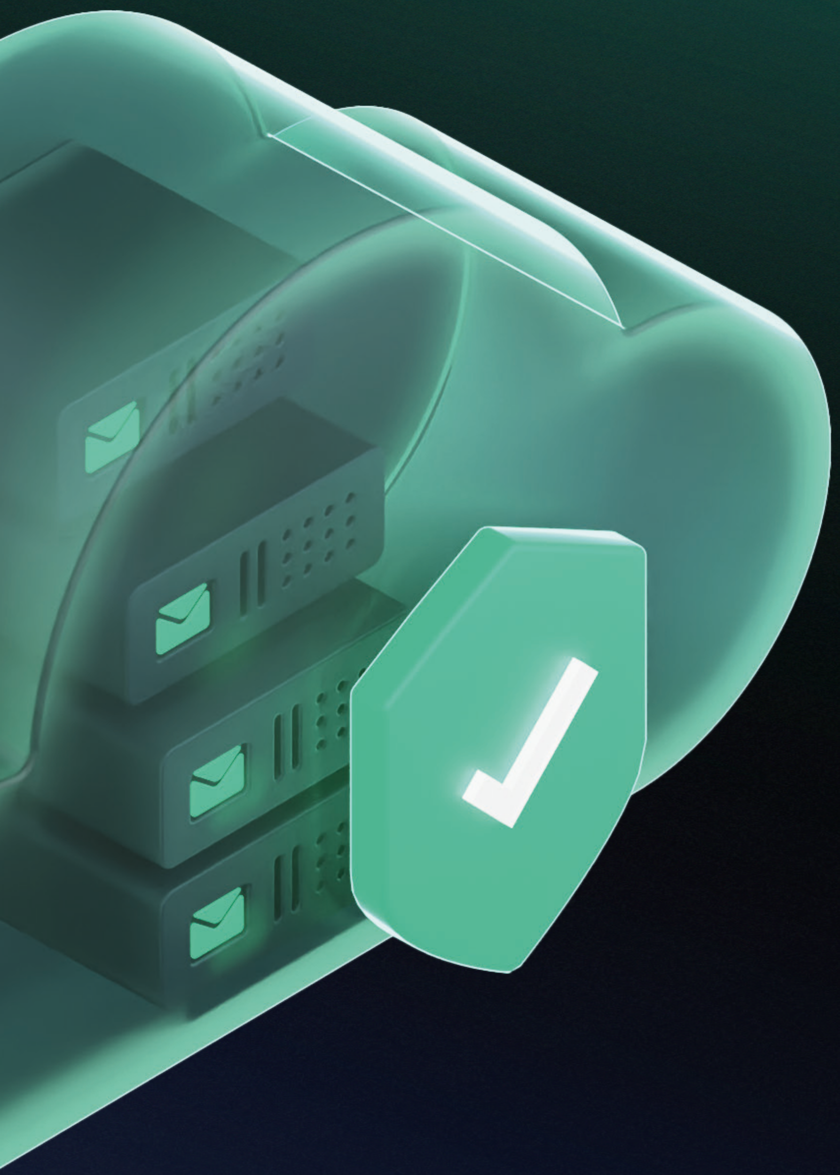
How we help

Protect hybrid environments across all workload types and cloud platforms

Maintain compliance with regulatory requirements

Increase visibility of hybrid infrastructures and reduces IT incidents

AI-driven protection to minimize false positives



Container Security

Kaspersky Container Security

Protects your entire lifecycle of containerized apps, from development to operation.

How we help

Protects applications at every step of development and operation

Increase the transparency of development environments and processes

Audit infrastructure and applications for regulatory compliance

Accelerates release of client-oriented applications and services

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.

05

These are the challenges businesses face when dealing with security issues:

Lack of security awareness

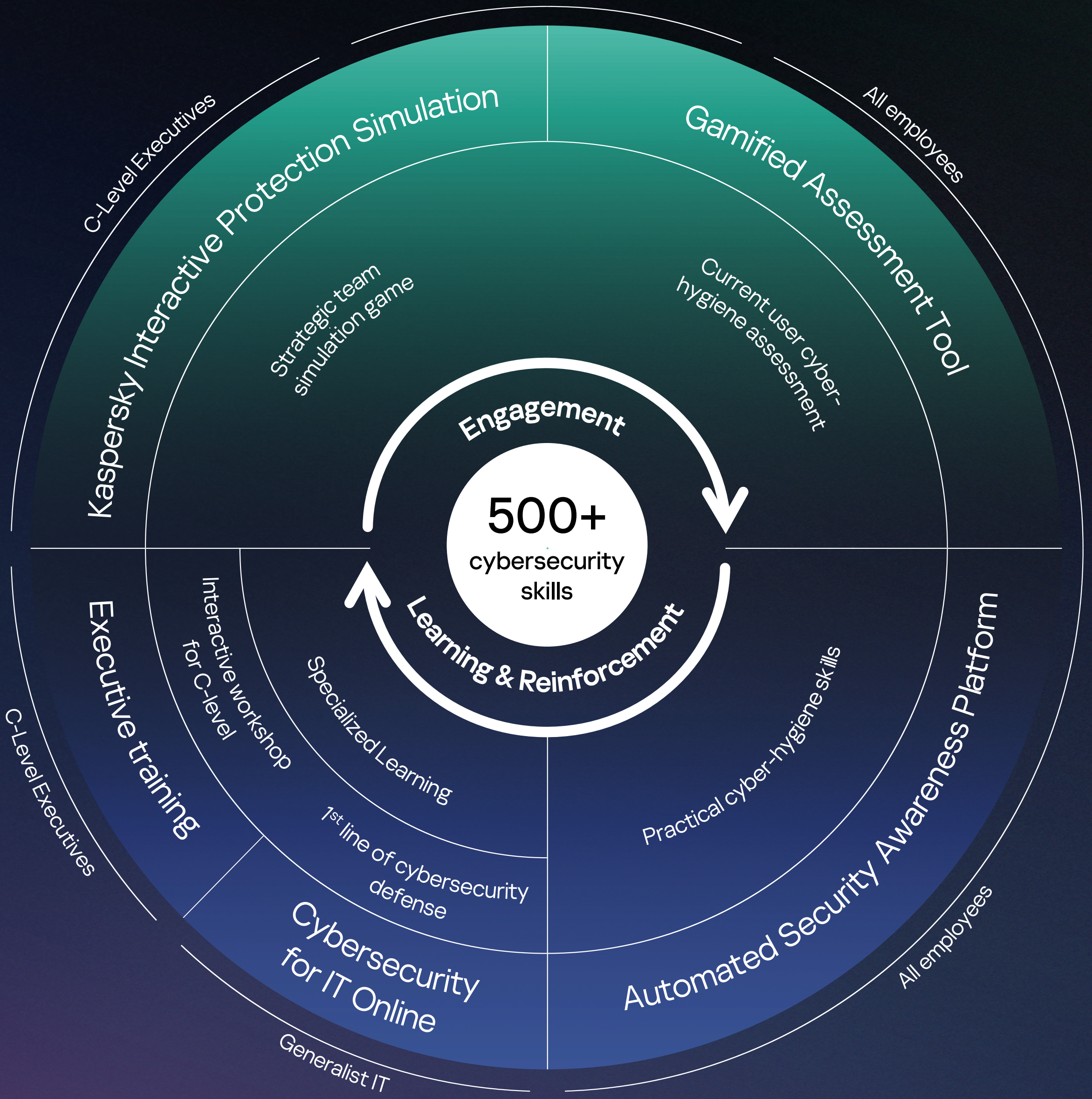
Lack of qualified technical staff

Employee knowledge & skills gaps

→

We help organizations build a resilient cybersecurity framework that also addresses staff-related challenges and reduces human-related incidents. We enhance the capabilities of IT and security teams, address the shortage of qualified staff, foster a culture of cyber vigilance, teaching employees to recognize and avoid threats, while empowering technical teams to maximize security solutions' effectiveness.

Kaspersky security awareness



Kaspersky Interactive Protection Simulation
C-Level Executives
Strategic team simulation game
Gamified Assessment Tool
All employees
Current user cyber-hygiene assessment
Engagement
500+
cybersecurity skills
Learning & Reinforcement
Executive training
C-Level Executives
Interactive workshop for C-level
Specialized Learning
1st line of cybersecurity defense
Cybersecurity for IT Online
Generalist IT
Practical cyber-hygiene skills
Automated Security Awareness Platform
All employees

Our security awareness boosts cybersecurity culture inside organizations, engaging everyone from senior management to employees. Kaspersky-specific, game-based training helps executives and managers implement effective cyberdefense strategies while the automated platform empowers staff to proactively defend against threats. This approach reduces human-related incidents and enhances overall organizational resilience.

Kaspersky Automated Security Awareness Platform free trial

Kaspersky training portfolio

Our training portfolio includes cybersecurity and product training that equips information security specialists with the skills to effectively use complex security solutions and customize them to your unique requirements. Cybersecurity training covers areas like malware analysis, threat hunting and incident response, helping organizations to get the most out of their security investments and maintain a strong security posture.

Kaspersky cybersecurity training

Kaspersky product training

Cybersecurity training

Topics

- Reverse engineering
- Incident response
- Active threat hunting
- Industrial cybersecurity training

Training formats

- Offline
- Online (instructor-led)
- Self-paced

Manage your security incidents with external expert guidance and support

Comprehensive cybersecurity services that empower your organization in the face of sophisticated threats. Supported by our expertise, your business stays protected and prepared against any security challenge.

Kaspersky security services

06

Kaspersky Managed Detection and Response

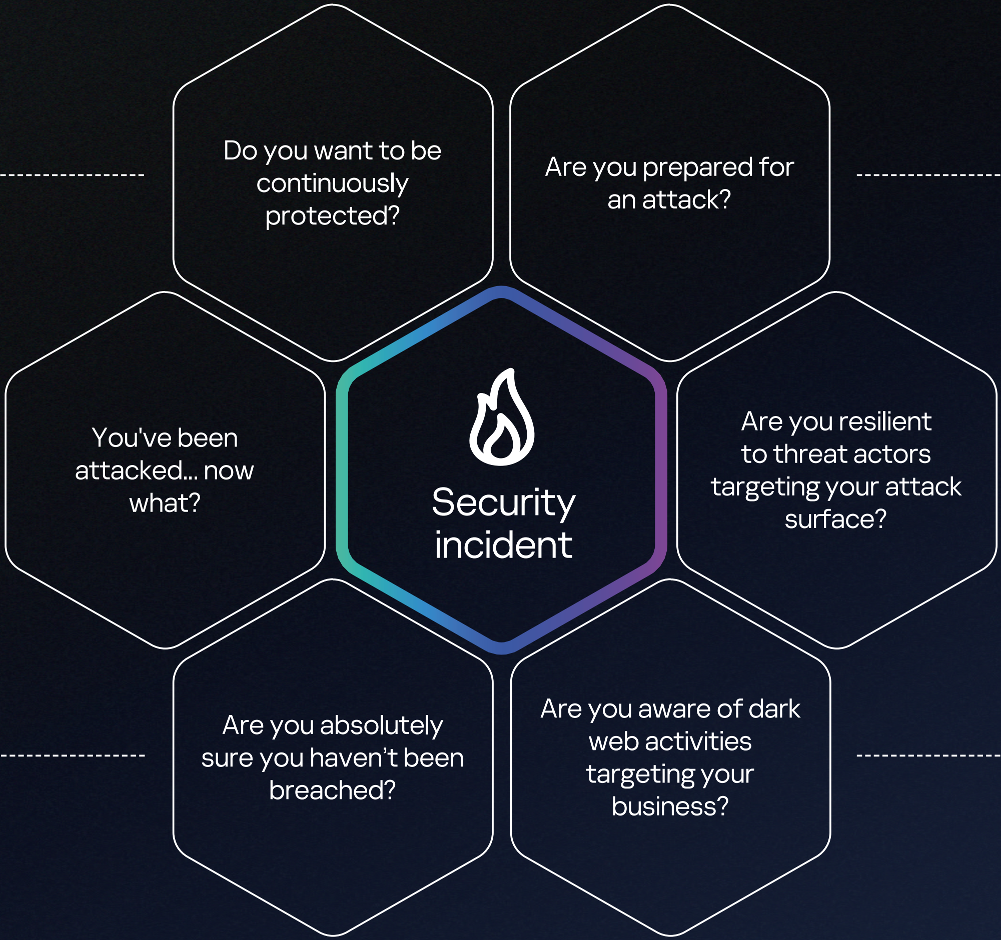
Continuous monitoring, detection and response

Kaspersky Incident Response

Digital forensics, incident response and malware analysis

Kaspersky Compromise Assessment

Detection of compromise, and traces of past attacks



Security incident

Do you want to be continuously protected?

Are you prepared for an attack?

You've been attacked... now what?

Are you resilient to threat actors targeting your attack surface?

Are you absolutely sure you haven't been breached?

Are you aware of dark web activities targeting your business?

Kaspersky SOC Consulting

Establish your own SOC or enhance your existing security operations

Kaspersky Security Assessment

Practical exercises demonstrating how an adversary would breach your security

Kaspersky Digital Footprint Intelligence

Monitoring of your digital assets to detect external threats

Learn more

MDR & incident response

Kaspersky Managed Detection and Response

Round-the-clock managed protection against cyberthreats and sophisticated attacks that traditional automated security measures miss.

Learn more

How we help

Ensure rapid threat detection and response, minimizing potential downtime and financial losses.

Give you all the major benefits of having your own SOC without the trouble and expense of establishing one yourself.

Reduce your security costs and the need to hire and train multiple, expensive IT security professionals to cover all the bases.

Enable you to refocus your in-house IT security resources to deal with other business-critical issues.

Kaspersky Incident Response

The service covers the full incident investigation and response cycle, from initial response and evidence collection to identifying the primary attack vector and preparing an attack mitigation plan.

Learn more

How we help

Minimize business disruptions and reduce operational downtime through rapid incident containment and resolution.

Conduct expert-led investigations. Leverage Kaspersky's cybersecurity professionals for deep incident analysis.

Our cost-effective incident management reduces the financial losses associated with security breaches.

Deliver enhanced cyber resilience that strengthens defenses against similar future attacks with tailored security enhancements.

Explore how MDR and incident response became the guardians of Digital Kingdoms in 2024

Silent shields & digital dragons: MDR's proactive protection

The dragon's hour: how incident response turns ruin into resilience

For decades, our MDR and incident response services have protected enterprises across industries. Today, organizations worldwide rely on our proven expertise and relentless innovation to defend their digital frontiers. Stay ahead of emerging threats explore our latest expert reports.

Get
the reports

Proven solutions trusted globally

We protect over 200,000 corporate clients worldwide across diverse industries, delivering effective security solutions for organizations of all sizes and complexities.

200

countries and territories

30+

representative regional offices

From global reach to local relevance, Kaspersky delivers trusted protection everywhere.

Tailored for every industry

	Business customers by sector	Countries
Financial services	~3,500	130
Government	~6,300	125
Energy	~1,600	93
Manufacturing	~38,000	171
Retail	~12,700	125
Healthcare	~4,900	89

And more

Transportation | Oil & gas | IT | Education | Telecoms

Case studies

“

With Kaspersky, we were able to protect ourselves against cyberthreats, data loss and targeted attacks. We were also able to achieve the highest security standards that boosted the condence of our global business partners.

Lijun Zhong
IT Manager, Kin Yat Holdings Limited

“

Over the years, Kaspersky has been our strategic ally and has been an important part of our history. Kaspersky’s centralized monitoring and management through intuitive, user-friendly interfaces have allowed us greater visibility and control over our cyber security infrastructure.

Radhames Mendez
Senior Business Continuity Manager,
Grupo Corripio

GRUPO
CORRIPIO

Read all case studies

Advanced protection for Qatar Olympic Committee

Doha,
Qatar

National Olympic
Committee
representing Qatar

Read
the story

Challenge

The Qatar Olympic Committee (QOC) faced growing cybersecurity threats, requiring a robust and scalable security framework. With multiple digital assets and critical IT infrastructure, it needed a proactive solution to protect sensitive data and ensure seamless operations.

Solution

The integration of implemented Kaspersky solutions provided comprehensive protection.

- Kaspersky Anti Targeted Attack
- Kaspersky CyberTrace
- Kaspersky Threat Data Feeds
- Kaspersky Threat Lookup
- Kaspersky Next EDR Expert

Outcome

The Qatar Olympic Committee significantly improved cyberthreat detection, rapid response and SOC efficiency with Kaspersky solutions. Enhanced security controls, seamless scalability and proactive updates ensured resilience. Kaspersky's support during implementation and incident response strengthened QOC's ability to mitigate evolving global cyberthreats effectively.

> Kaspersky exceeded my expectations with their features and by listening to what we needed. They gave us confidence in the product and the people behind it and enabled us to have a more secure network.
>
> **Rashid AlNahlawi**
> IT Security Consultant, Qatar Olympic Committee

Enhanced centralized IT and OT security for Condor Carpets

Hasselt, Netherlands

Europe's largest carpet manufacturer

Read the story

Challenge

Condor Carpets wanted to ensure robust and scalable protection for its expansive industrial network. Given the developing landscape of cyberthreats, Condor Carpets needed a solution to safeguard its IT systems and in particular its Operational Technology (OT) network.

Solution

Kaspersky solutions helped to build up centralized security for IT and OT segments.

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Threat Data Feeds
- Kaspersky Next EDR Optimum

Outcome

The partnership with Kaspersky has significantly fortified Condor Carpets against cyberthreats, enhancing its overall security posture while ensuring the seamless functioning of its manufacturing processes. This successful implementation has laid a strong foundation for the continued growth and resilience of Condor Carpets in an increasingly digitized industrial landscape.

> Kaspersky solutions have revolutionised our network and cybersecurity profile. We're confident in their ability to protect our complex operations.

Patrick de Haan
IT Manager, Condor Carpets

www.kaspersky.com

#kaspersky
#bringonthefuture