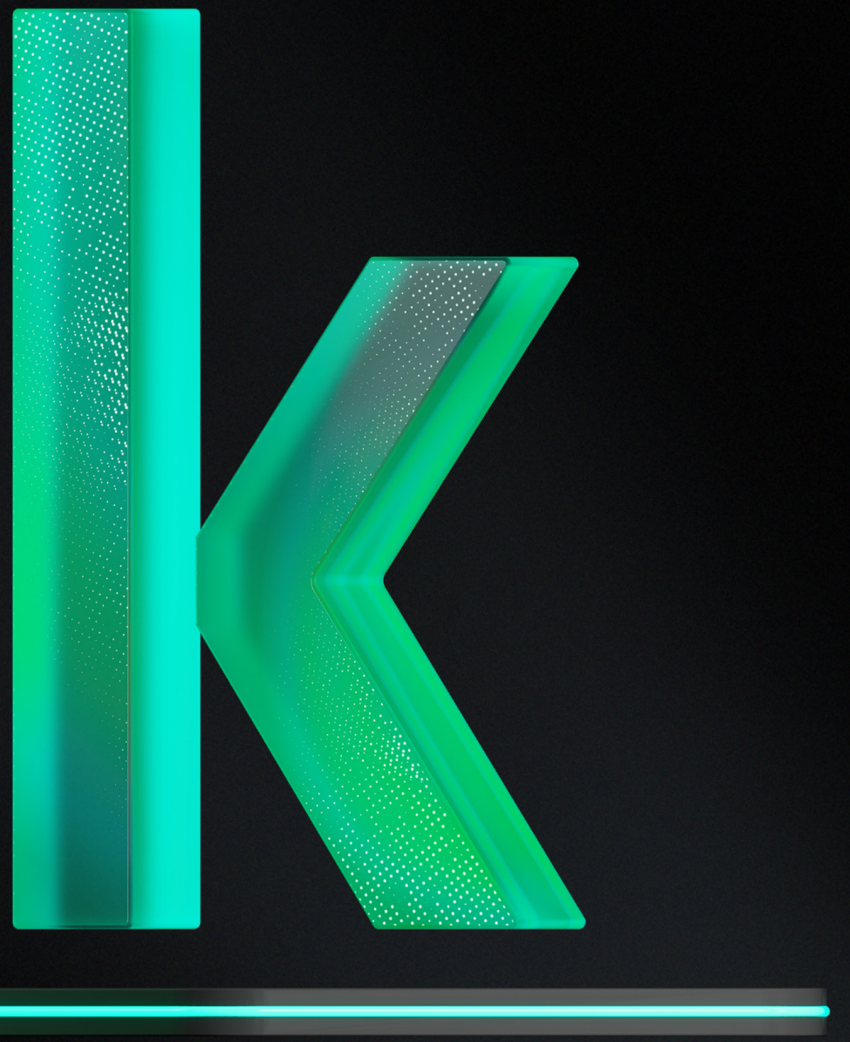
Kaspersky Enterprise Cybersecurity

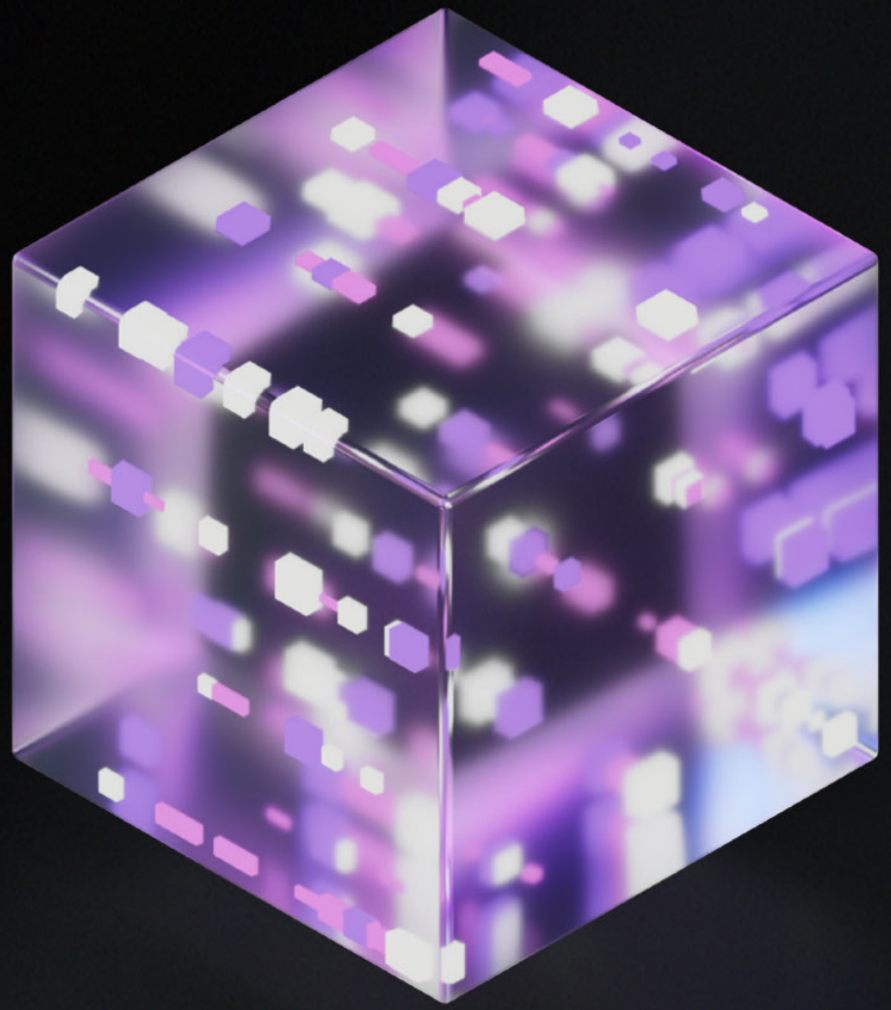


kaspersky bring on the future

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.



Why Kaspersky?

Enterprise portfolio:

01 Turning IT and OT risks into resilience

02 Guiding your SOC to virtuoso-level precision and efficiency

03 Managing risk with threat intelligence

04 Creating safe DevOps environments and protecting your cloud workloads

05 Training your entire team to be more secure and protected

06 Managing your security incidents with external expert guidance and support

Case studies

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.

~5,500
highly qualified specialists

50%
employees in R&D

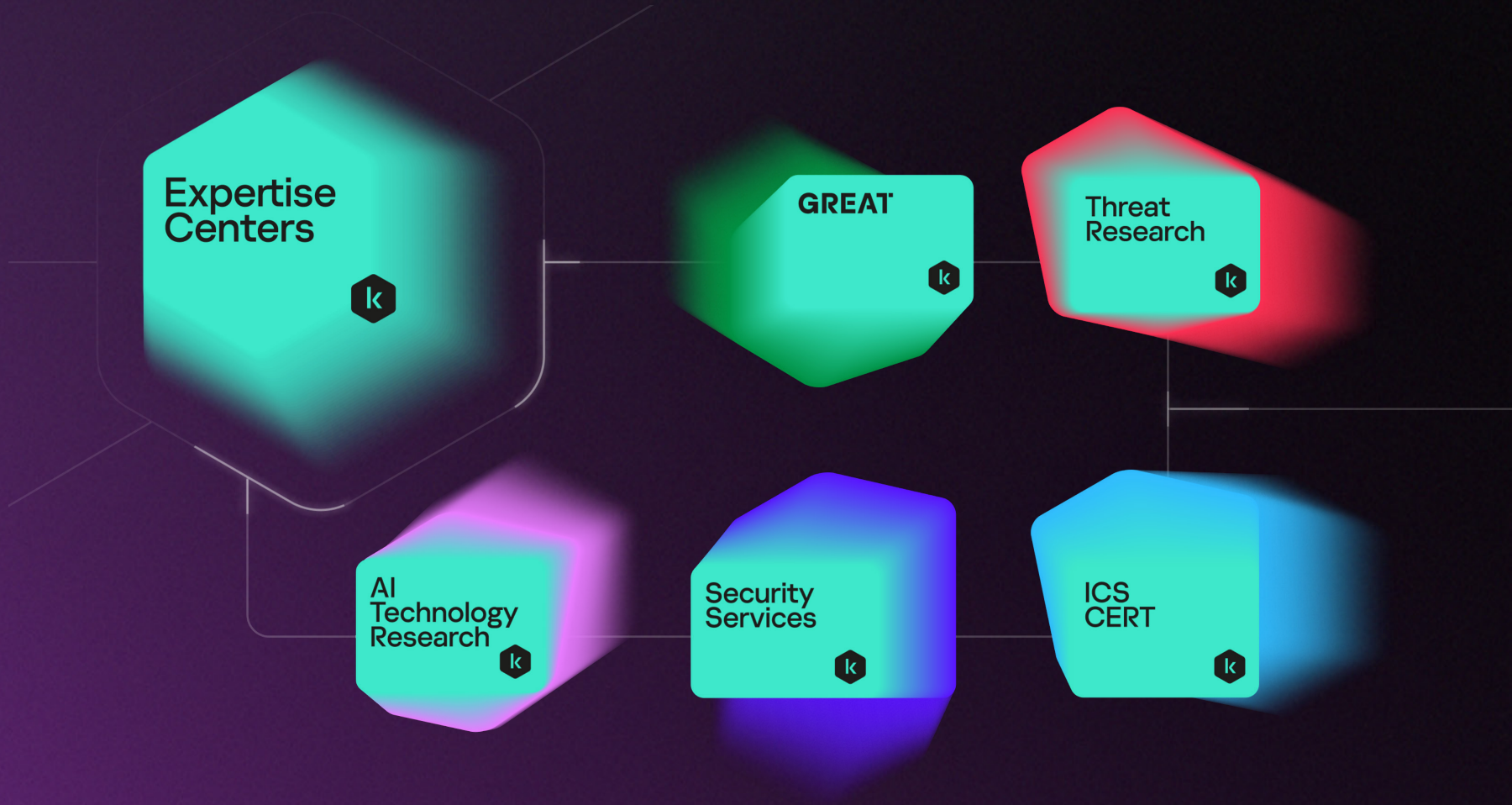
50+
globally recognized cybersecurity experts

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.

Learn more



AI at the core of the Kaspersky portfolio

20+ years

Kaspersky has used ML and AI to stay ahead of evolving cyberthreats, driving innovations in ML and AI, and embedding AI tools into internal processes and cybersecurity solutions architecture

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

Learn more

AI Leader in evolving from reactive defence to proactive intelligence

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

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

50,000 files | 100,000 users / day

Trained flexible hash with an integrated ML model

~1000 phishing web page 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

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

Learn more

Bug bounty program

Recognition that matters

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

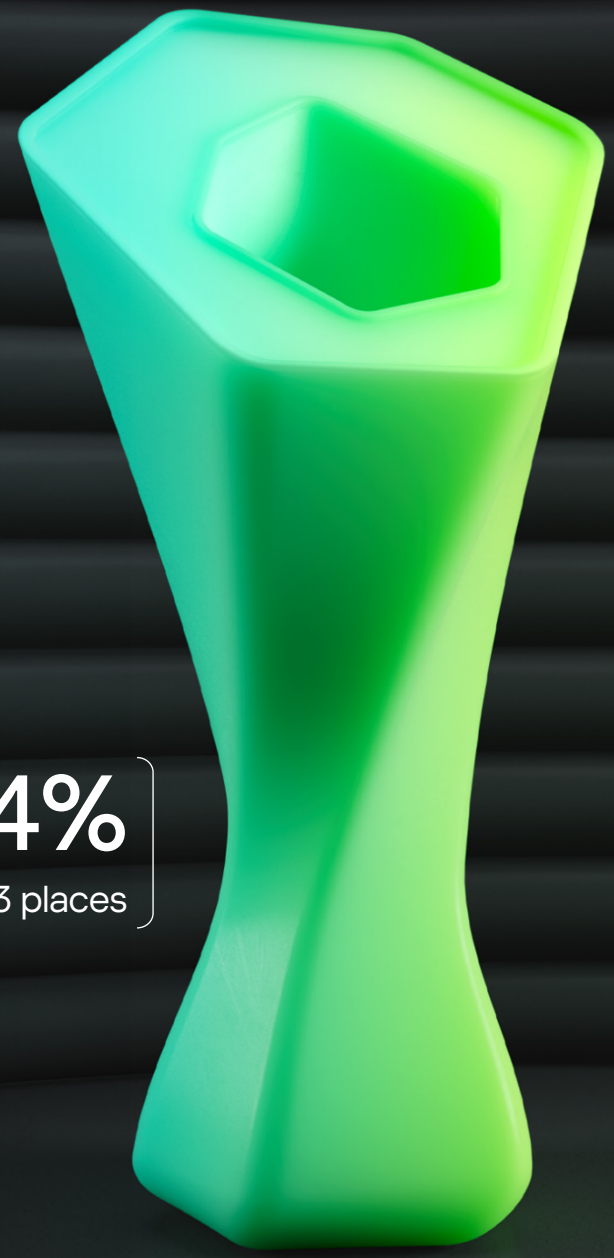
Most tested. Most awarded.

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

In 2025

100	90	94%
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+
registered patents

500+
inventions between 2005 and 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 reduces the attack surface and the risk of vulnerabilities, and the security monitor prevents unauthorized actions
- Developed from scratch by Kaspersky — no third-party code in the kernel
- The 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.

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

Why Kaspersky?

Enterprise portfolio:

01 Turning IT and OT risks into resilience

02 Guiding your SOC to virtuoso-level precision and efficiency

03 Managing risk with threat intelligence

04 Creating safe DevOps environments and protecting your cloud workloads

05 Training your entire team to be more secure and protected

06 Managing your security incidents with external expert guidance and support

Case studies

Turning IT and OT risks into resilience

Cybercrime evolves. So do we. Across IT, OT and converged environments, our solutions mitigate the most serious business impacts of cybercrime.

Corporate environments

Cybercrime can trigger financial losses, operational downtime, data breaches and fraud, resulting in customer loss and lasting reputational damage.

+

Industrial environments

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

Challenges

- An expanding attack surface
- Compliance
- Legacy systems
- New and evolving threats and vulnerabilities
- Shortage of skilled experts
- 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, continually 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 asset protection	Advanced asset-based security
Endpoints	Kaspersky Next EDR Foundations	Kaspersky Next XDR Expert
Network	Kaspersky Security for Mail Server	Kaspersky Anti Targeted Attack
Workloads	Kaspersky Hybrid Cloud Security	Kaspersky Cloud Workload Security

Comprehensive cross-asset defense and optimized security operations

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 Technologies

2 Knowledge

3 Expertise

Learn more

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
- Kaspersky Thin client
- Kaspersky Automotive Secure Gateway

2

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

3

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

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 organization's security posture and 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


Tailored security for corporate environments
Kaspersky Next offers a tiered approach to strengthening protection as your business grows — from essential endpoint protection and EDR to advanced AI-driven XDR for proactive cyberthreat defense.
Learn more

Kaspersky Next delivers versatile, multi-layered security for businesses of all sizes

Kaspersky Next Optimum

Learn more

For small and mid-sized businesses looking to scale protection without adding complexity.

Whether handled by an IT team or a small security group, this offering delivers easy-to-use tools with strong EPP, enhanced by EDR features. It also enables a smooth upgrade to essential XDR or MXDR as security needs grow.

Kaspersky Next Expert

Learn more

For enterprises that stay ahead of sophisticated threats by adopting the latest technologies and advanced security solutions.

This offering delivers advanced EDR and XDR capabilities, powerful automation and flexible expansion through on-demand technologies, enabling larger security teams to maximize their impact.

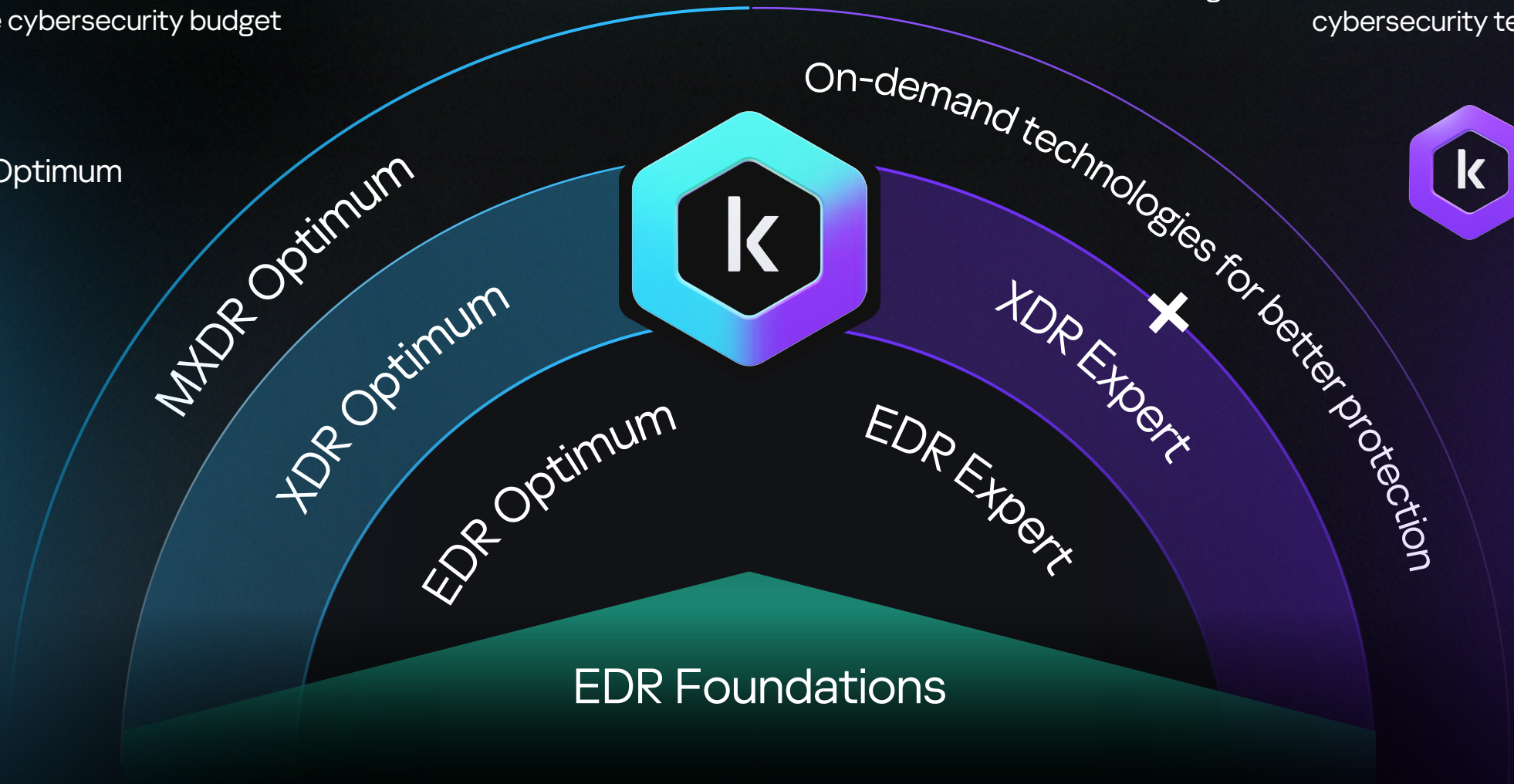
Kaspersky Next

For growing businesses with an established IT infrastructure and a reasonable cybersecurity budget

Optimum

For highly advanced enterprises with significant resources and a dedicated cybersecurity team or SOC

Expert



An 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 enables proactive cyberthreat defense — delivering total cybersecurity.

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).

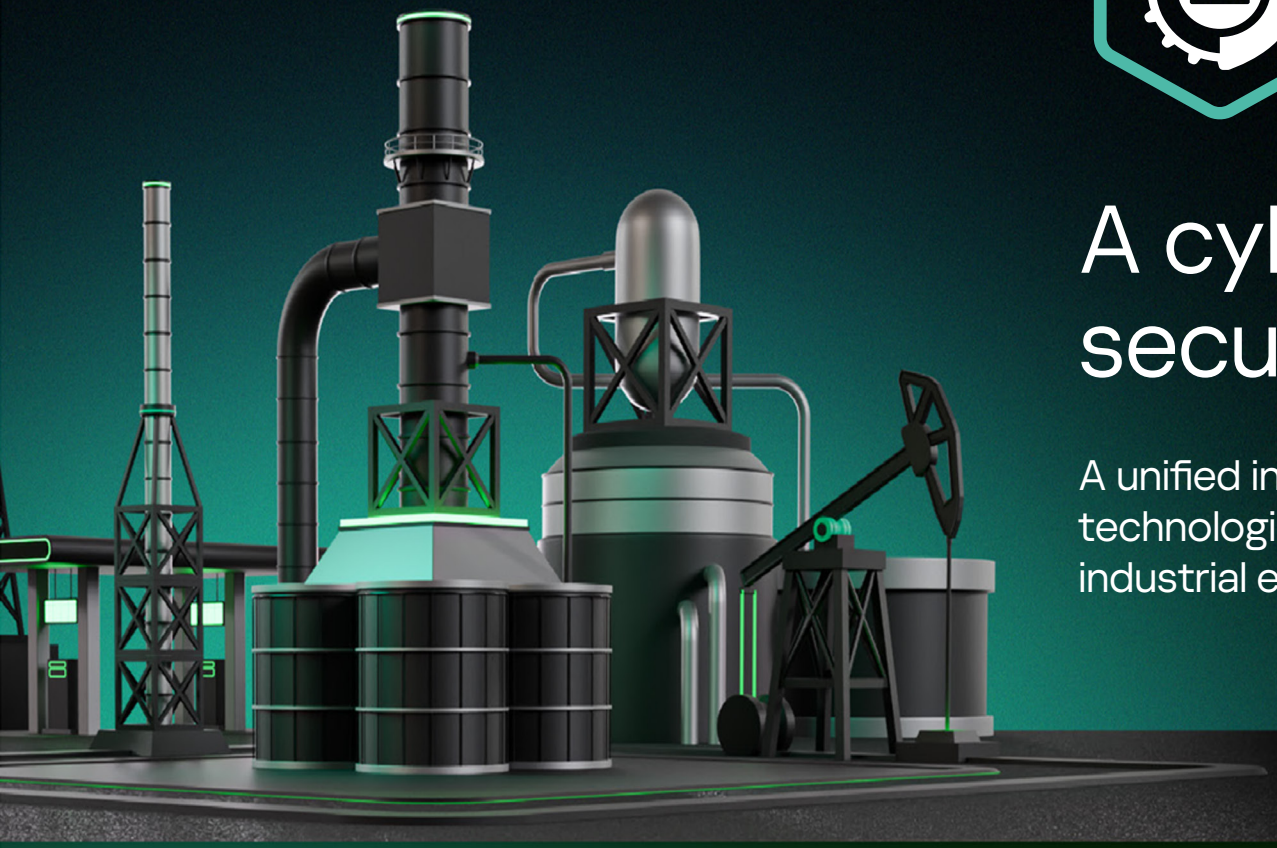
Monitoring, detection, threat hunting and investigation with AI assistance.

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 third year in a row

Learn more



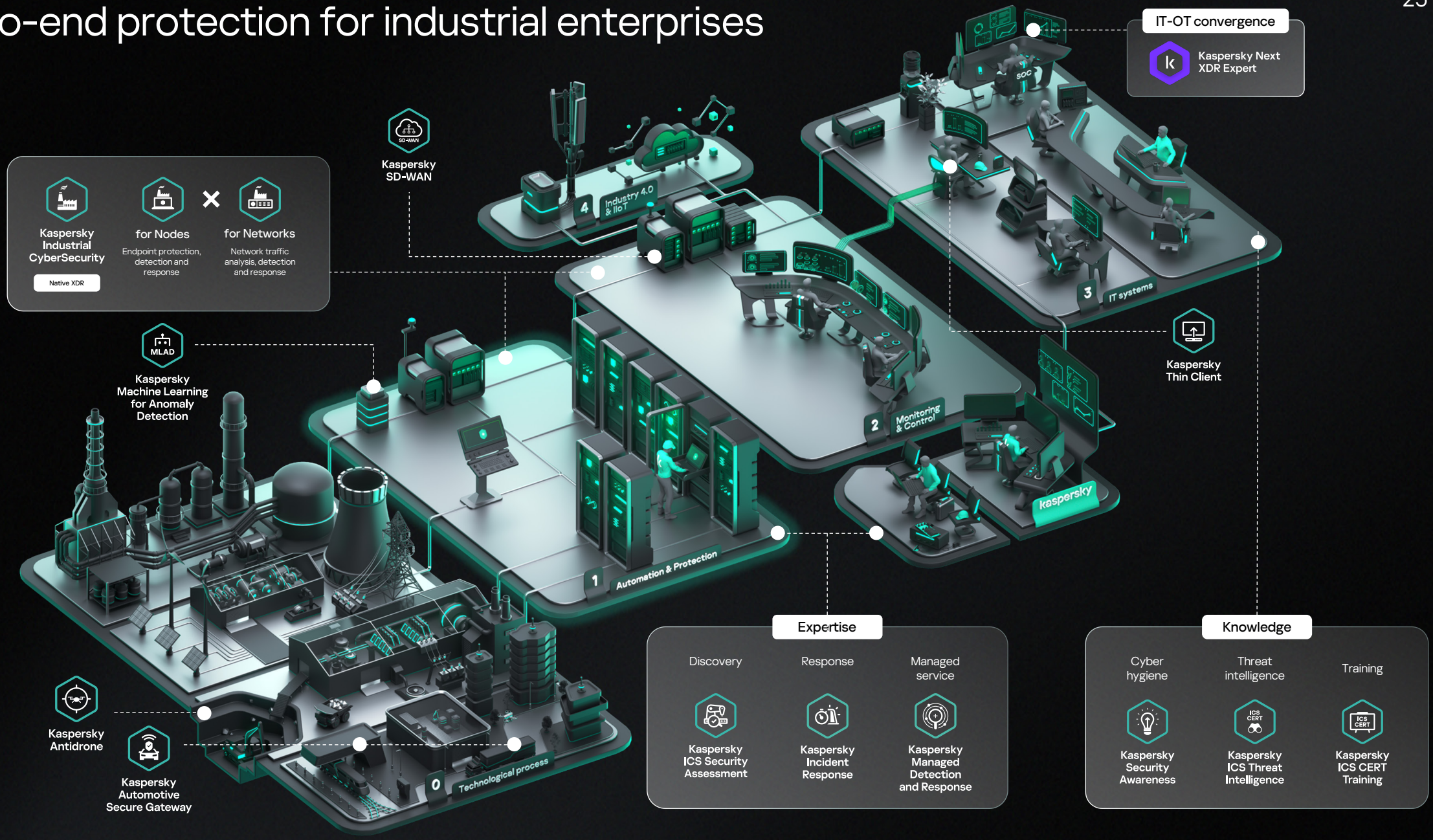
Kaspersky
OT CyberSecurity

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



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

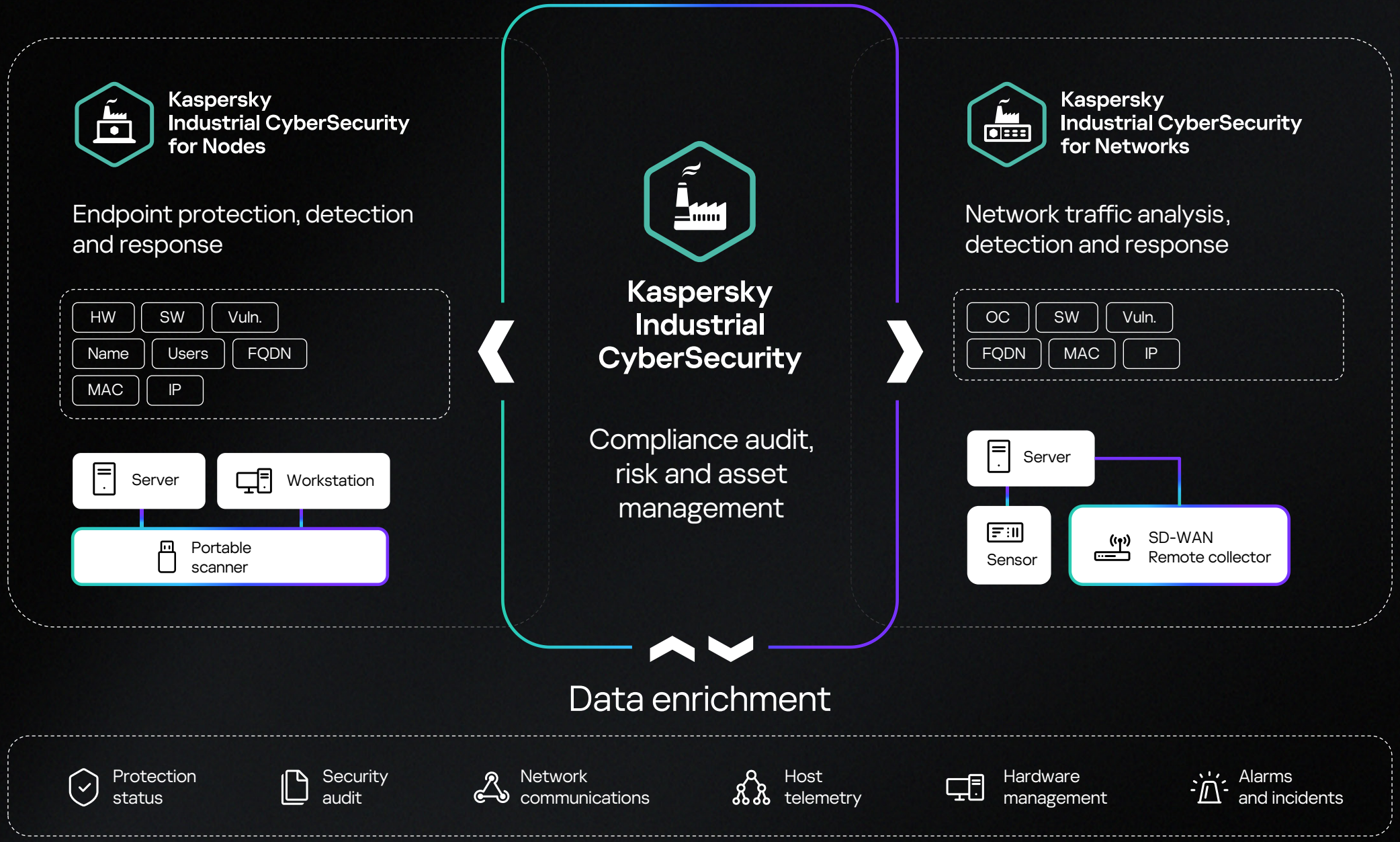
Reveal hidden threats. Detect anomalies, vulnerabilities and intrusion attempts long before they become dangerous.

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

Operate without affecting technological workflows, ensuring no 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

02

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 and improve their effectiveness and efficiency

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 technology stack

SIEM

Kaspersky Unified Monitoring and Analysis Platform

XDR

Kaspersky Next XDR Expert

NDR

Kaspersky Anti Targeted Attack

EDR

Kaspersky Next XDR 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

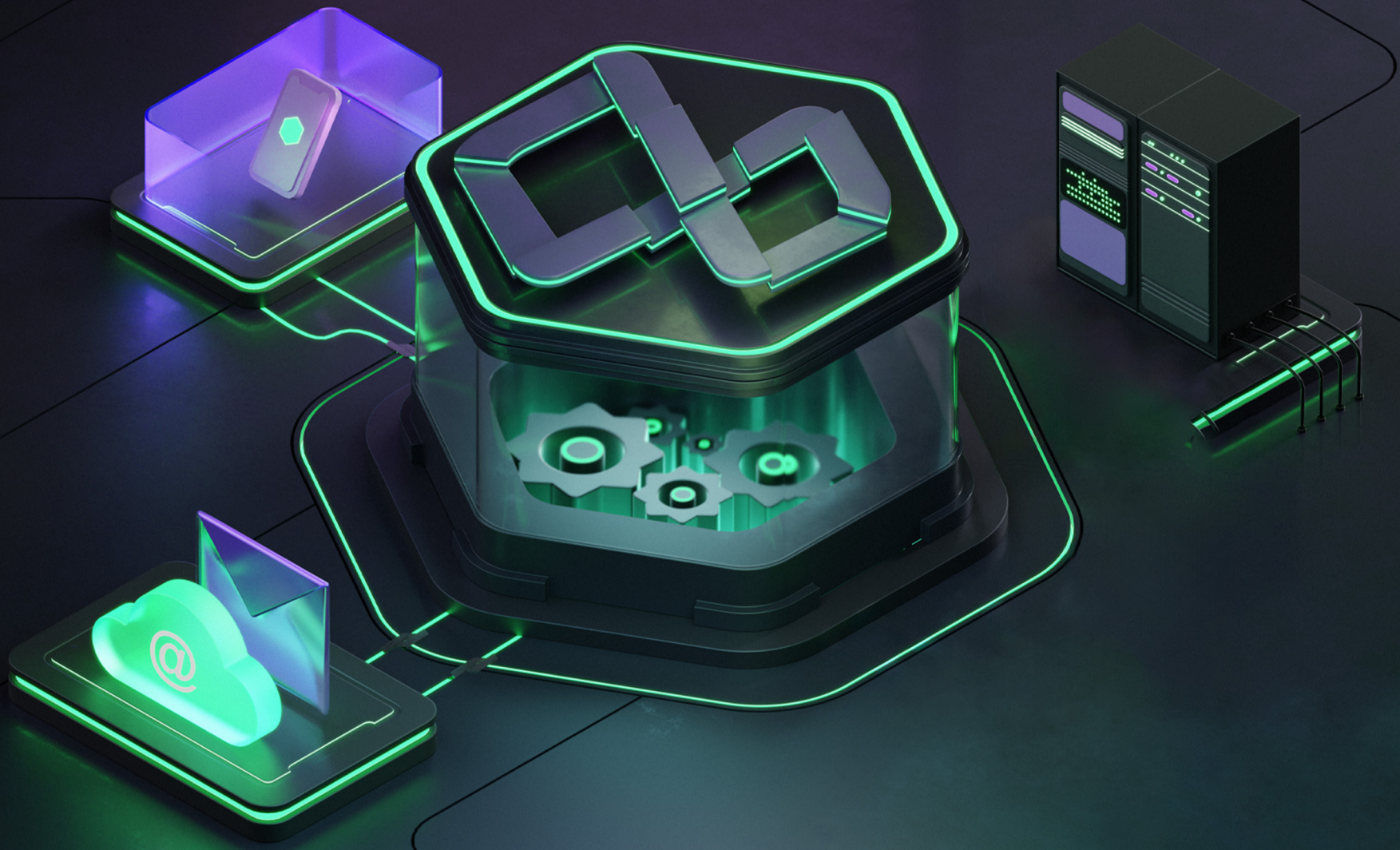
Kaspersky SOC Consulting

- SOC maturity assessment
- Tabletop exercise
- Adversary attack emulation

How Kaspersky SOC Consulting benefits your business

Kaspersky SOC Consulting services help organizations 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 businesses to detect, respond to and mitigate cyberthreats more efficiently and with greater 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 you, maintaining robust protection as you grow.

6. **Enjoy tailored SOC design:** Address cybersecurity threats specific to your business while respecting 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. By collecting and aggregating logs from all security controls and correlating the data in real time, Kaspersky SIEM provides SOC teams with all the information they need 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 empower your SOC

Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack is an advanced anti-APT solution that defends against sophisticated cyberthreats. It combines advanced Sandbox, Network Detection and Response (NDR), Endpoint Detection and Response (EDR), providing native XDR capabilities and 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

03

Managing risk with threat intelligence

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

Cyberattacks evolve rapidly

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 are vital to manage risks more effectively.

And businesses face new challenges:

Lack of context

Raw threat intelligence often lacks the necessary context, making it difficult to assess how specific threats impact business 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, up-to-date threat intelligence to gain deep visibility into cyberthreats targeting their business to ensure they're always 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 — keeping you 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

AI-powered

- Tactical
- Operational
- Strategic

Human-readable Threat Intelligence

Kaspersky Threat Intelligence Portal

All services available via the Threat Intelligence portal are powered by the **Kaspersky Threat Landscape** — a complete view of the global and company-specific threat environment

- Kaspersky Threat Lookup
- Kaspersky Threat Analysis
  - Sandbox
  - Attribution
  - Similarity
- Kaspersky Threat Intelligence Reporting
  - APT
  - Crimeware
  - ICS
- Kaspersky Digital Footprint Intelligence

Human-readable threat intelligence

Kaspersky Threat Intelligence Portal

A single access point for all human-readable threat intelligence data — designed for both IT and OT — where services work together to reinforce each other.

How we help

Provides a unified web interface for reliable, up-to-date threat intelligence to support early attack prevention and incident investigation.

Offers detailed reports on threats related to APT groups, financially motivated cybercriminals, and industrial organizations.

Strengthens file analysis processes through sandboxing, attack attribution, and file similarity detection.

Protects brand reputation by tracking digital assets and threats across darknet resources.

Powered by Kaspersky Threat Landscape, region- and industry-specific threat intelligence that gives organizations clear visibility into the threats that matter most to their business.

Experience our industry-leading threat intelligence

Machine-readable threat intelligence

Kaspersky Threat Data Feeds

Over 30 threat data feeds, tailored to diverse security needs across both IT and OT, provide information on known malware, phishing websites, the latest vulnerabilities, and exploits.

How we help

Reinforces security solutions — including SIEM, NGFW, IDS/IPS, and secure web proxies — with continuously updated IoCs and actionable context.

Integrates with security controls and TI platforms, such as Kaspersky CyberTrace, for streamlined threat management and proactive defense.

Improves detection quality and reduces false positives while securing the software development lifecycle (SDLC) through actionable intelligence.

Empowers security teams to quickly identify and prioritize critical alerts from SIEM, NGFW, and TI platforms by automating the initial triage process.

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.

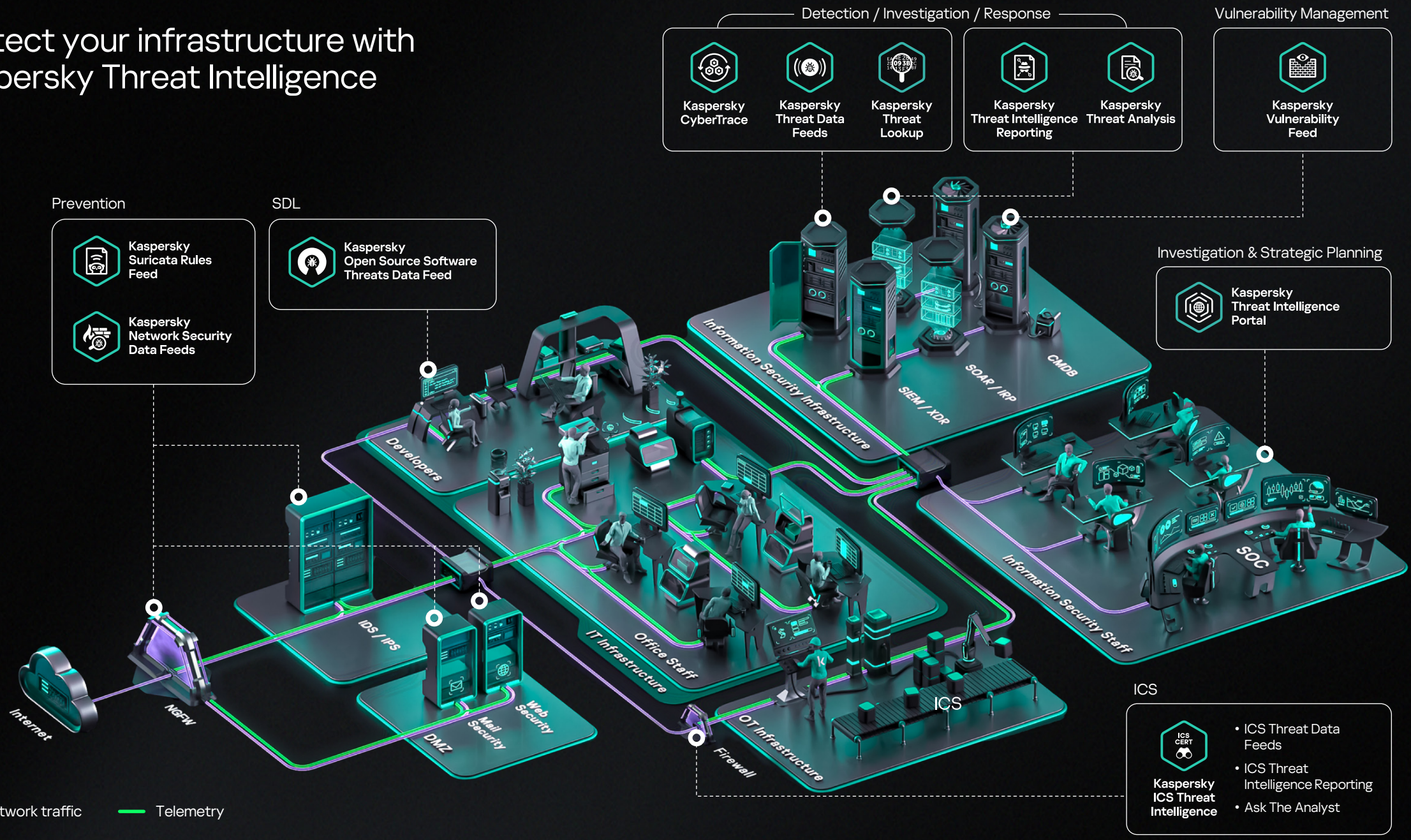
Kaspersky CyberTrace

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

Targeted 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



04

Creating safe DevOps environments and protecting your cloud workloads

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

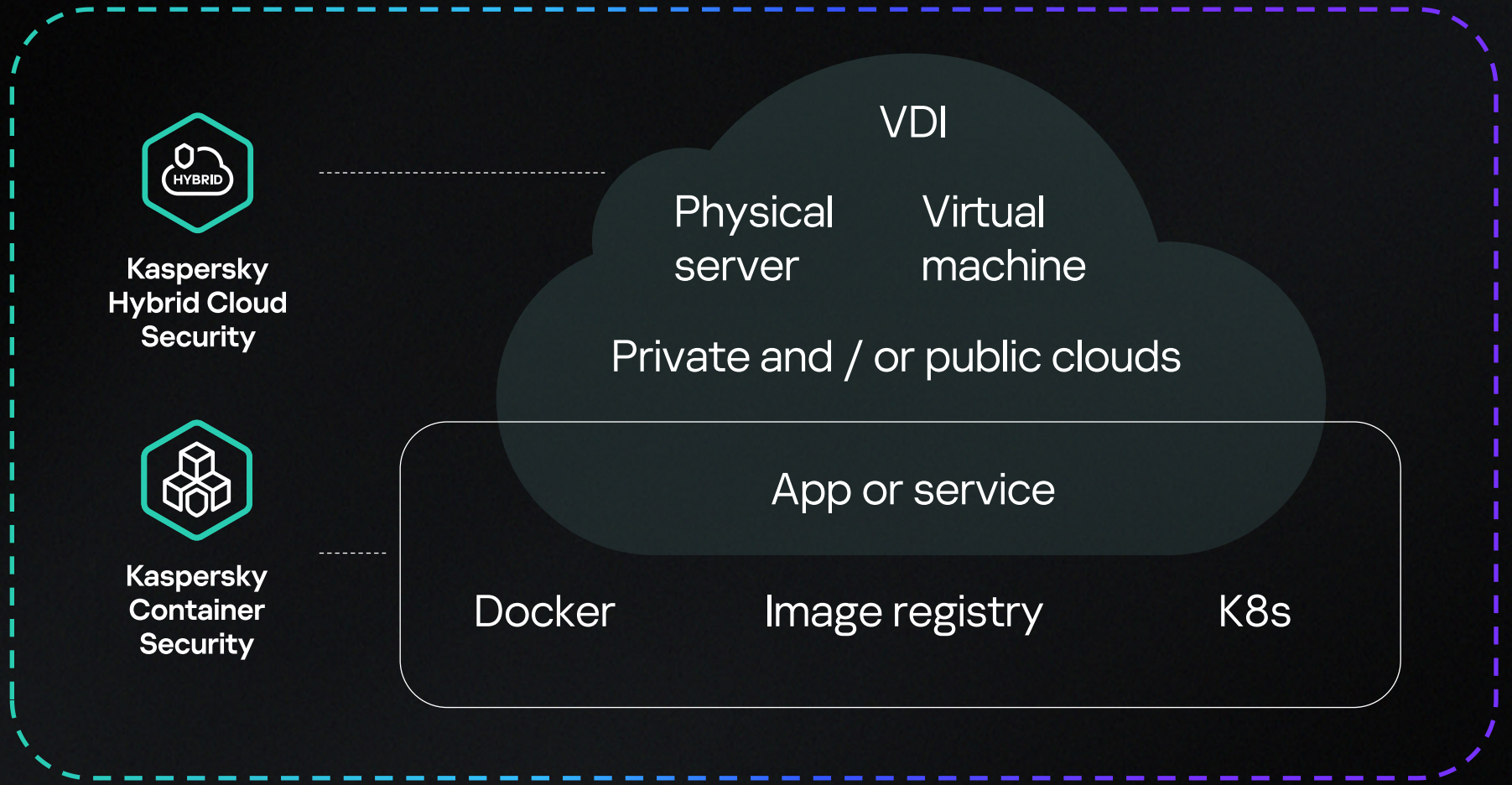
Challenges

Insecure third-party resources

Limited visibility and control in hybrid cloud environments

Insecure software development (including container images and runtime)

Kaspersky Cloud Workload Security



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

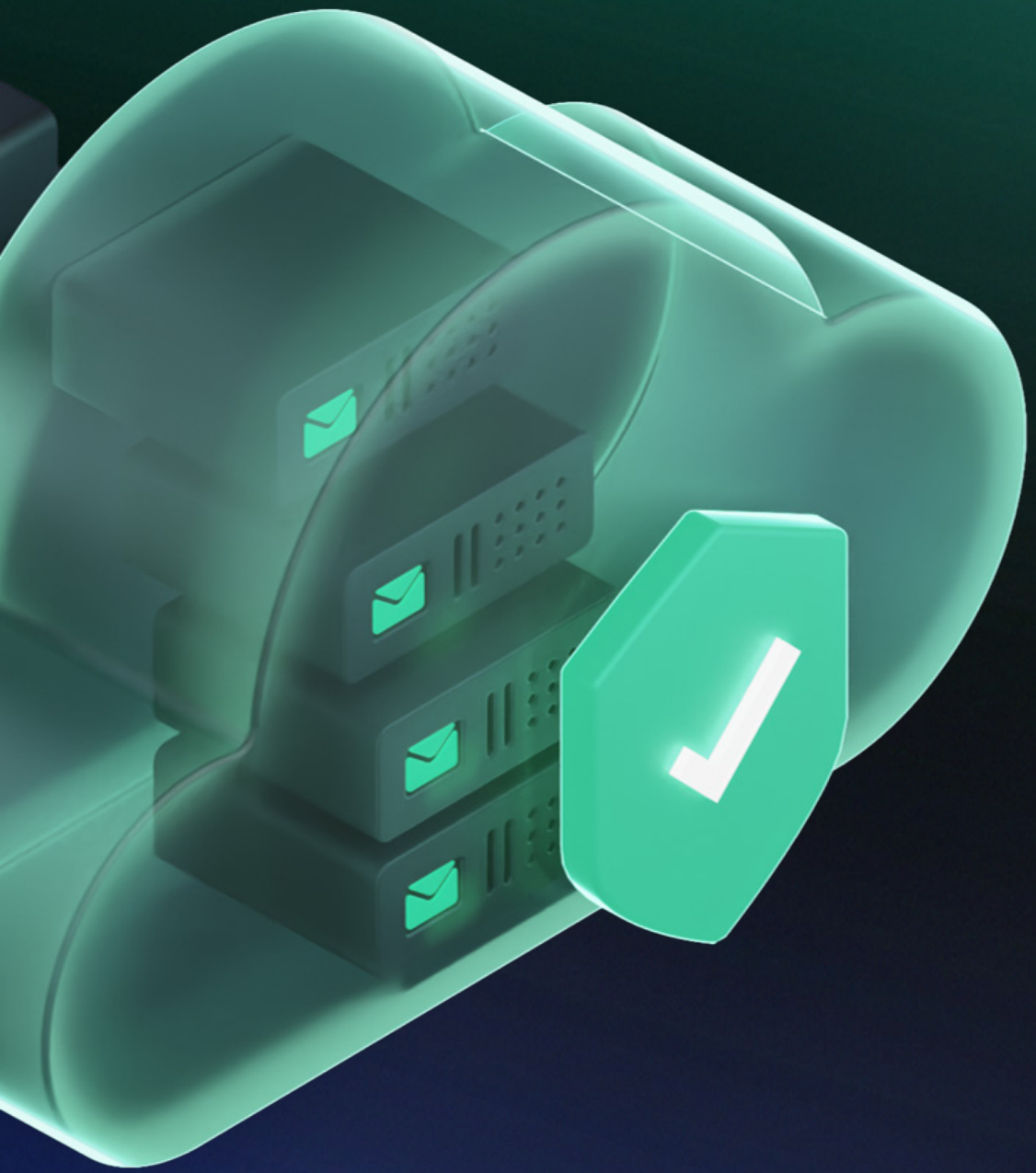
Kaspersky Hybrid Cloud Security

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 regulatory compliance
- Increase visibility of hybrid infrastructures and reduce 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

Protect applications at every step of development and operation

Increase the transparency of development environments and processes

Audit infrastructure and applications for regulatory compliance

Accelerate the release of client-oriented applications and services

05

Training 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.

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

Lack of security awareness

Lack of qualified technical staff

Gaps in employee knowledge and skills

We help organizations build a resilient cybersecurity framework that addresses staff-related challenges and reduces human-driven incidents. We strengthen the capabilities of IT and security teams, help mitigate skills shortages, and foster a culture of cyber vigilance, enabling employees to recognize and avoid threats while empowering technical teams to get the most from their security investments.

Kaspersky Security Awareness

Kaspersky Security Awareness builds a strong cybersecurity culture across the organization, from senior leadership to employees. Game-based training supports executives and managers in implementing effective cyberdefense strategies, while the automated platform empowers staff to recognize and respond to threats proactively — reducing human-related incidents and improving organizational resilience.

Experience the Kaspersky Automated Security Awareness Platform with a free trial

Kaspersky training portfolio

Our training portfolio includes cybersecurity and product training that equips information security specialists with the skills to use complex security solutions effectively and customize them to specific requirements. Cybersecurity training covers areas such as malware analysis, threat hunting and incident response, helping organizations get more value from their security investments and maintain a strong security posture.

Kaspersky Cybersecurity Training

Kaspersky Product Training

Cybersecurity Training

Topics

- Malware analysis
- Threat hunting
- Incident response
- Solutions security
- Industrial cybersecurity

Training formats

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

Managing your security incidents with external expert guidance and support

06

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

Kaspersky Security Services

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 previous attacks

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 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.

How we help

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

Deliver the benefits of an in-house SOC without the cost and complexity of having to build on 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.

How we help

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

Conduct expert-led investigations with Kaspersky cybersecurity professionals for deep incident analysis.

Our cost-effective incident management reduces the financial impact 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

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. Organizations worldwide rely on our proven expertise and innovation to defend their digital frontiers. Explore our latest reports and stay ahead of emerging threats.

Get the reports

Kaspersky Support Services

Maximizing value from your Kaspersky products

Kaspersky Professional Services

Kaspersky Premium Support

Support Services portfolio: benefits

Direct access to Kaspersky expertise, enabling rapid response to issues and enhanced solution performance

Vendor expertise

Vendor knowledge sharing, onboarding, product testing, expert consultations and answers to key questions.

Prioritized response

Your requests are prioritized with guaranteed response times via SLA, ensuring prompt resolution of critical issues.

Reduced internal overhead

By leveraging KPS for complex deployments, your internal teams can focus on core business priorities, reducing operational strain.

Custom capabilities

Unlock unique capabilities customized to your products, offering enhanced flexibility and deeper security insights for your needs.

Professional Services

Kaspersky Professional Services

Kaspersky Professional Services provides expert support to optimize and secure your IT environments, strengthening infrastructure protection and resilience against sophisticated cyberthreats.

Learn more

Assessment services

- Cybersecurity health check
- Compliance assessment
- Health Check
- Security fundamentals assessment

Implementation services

- Security architecture design
- Installation / upgrade
- Complex implementation
- Configuration

Maintenance services

- Handling critical situations (on-site engineer)

Optimization services

- Security hardening
- Product resilience (fault tolerance, disaster recovery, high availability)

Premium Support

Kaspersky Premium Support

Kaspersky Premium Support ensures fast, reliable access to vendor expertise through strict SLAs. Our certified professionals provide timely guidance and resolution to maintain business continuity and maximize the effectiveness of your Kaspersky solutions.

- Phone support
- Fast response
- Expert guidance

Learn more

* For severity level 1 requests
** Response time for highest support level

	Standard Support	Premium Support
Requests via web portal	yes	yes
Phone support	no	yes
Support team working hours	8/5	24/7 *
Response time for Severity Level 1 requests	no SLA	up to 30 min ** (24/7)
Response time for Severity Level 2 requests	no SLA	up to 4 hours ** (8/5)
Response time for Severity Level 3 requests	no SLA	up to 6 hours ** (8/5)
Response time for Severity Level 4 requests	no SLA	up to 8 hours ** (8/5)

Proven solutions trusted globally

We protect nearly 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	~3,200	126
Government	~6,100	122
Energy	~1,450	90
Manufacturing	~28,300	155
Retail	~12,400	119
Healthcare	~4,600	95

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 confidence of our global business partners.

LijunZhong

IT Manager, Kin Yat Holdings Limited

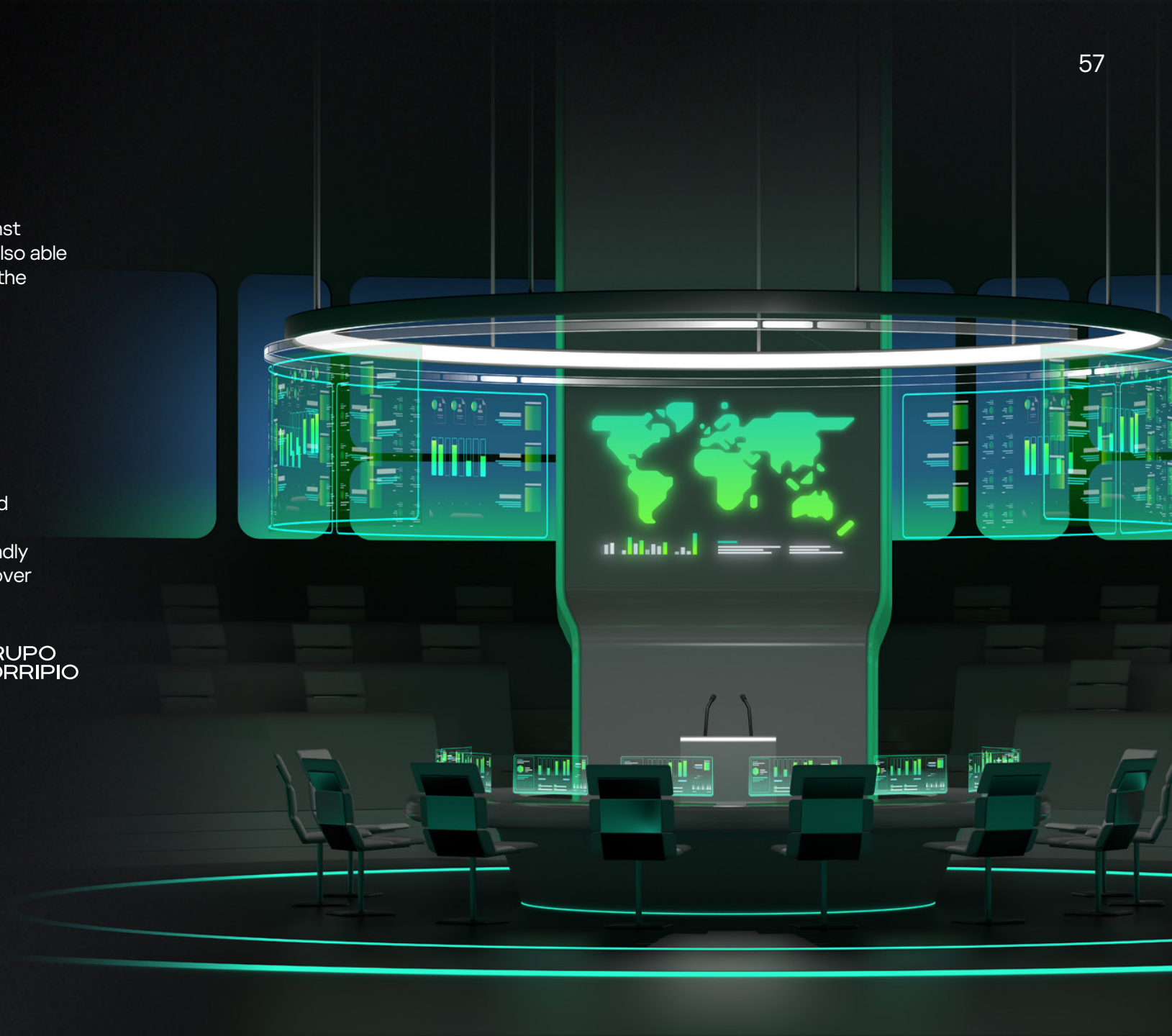
> Over the years, Kaspersky has been our strategic ally and an important part of our history. Kaspersky's centralized monitoring and management through intuitive, user-friendly interfaces have allowed us greater visibility and control over our cyber security infrastructure.

Radhames Mendez

Senior Business Continuity Manager, Grupo Corripio

GRUPO CORRIPIO

Explore our case studies



Advanced protection for the Qatar Olympic Committee

Doha, Qatar

National Olympic Committee representing Qatar

Read the full 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 XDR 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 full 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 revolutionized 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

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

#kaspersky
#bringonthefuture