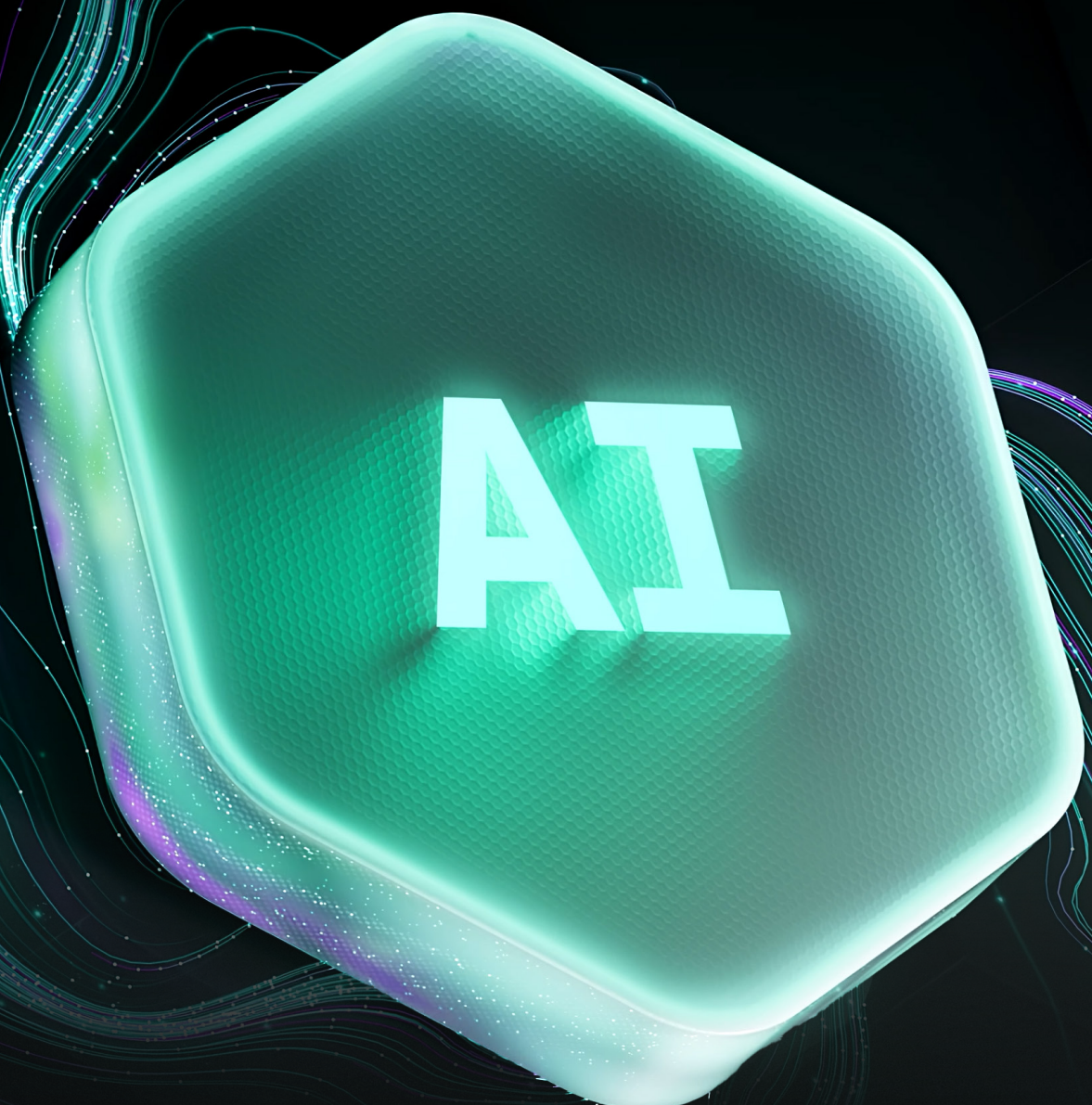




AI

Explore how AI powers Kaspersky's portfolio

Our AI journey began in 2005. Long before the current boom, we were using machine learning to solve core security problems. Today, this heritage gives us a clear advantage.

AI is the tool. Expertise is the advantage.

The AI hype is deafening. Every vendor promises magic. At Kaspersky, we take a different approach. We see AI not as a silver bullet, but as a powerful, practical tool that must be built on a foundation of trustworthy data and deep human expertise.



Our AI strategy: two key dimensions

AI is in our DNA

- Dedicated Kaspersky AI Technology Research Center
- 20+ years of AI innovation
- We've been studying AI threats for as long as we've been using AI for protection



AI threat landscape monitoring

~30 years of threat research expertise lets us cut through the hype and counter real threats:

- Track scammers exploiting AI hype
- Monitor how cybercriminals use AI to work faster and at scale
- Anticipate the evolution of AI threats to build stronger protection
- Secure our systems against AI-driven threats



Proven expertise

- More than 130 AI patents
- Signatory to the EU AI Pact
- Developed the AI Secure Development Guidelines
- AI-based threat detection mechanisms play a pivotal role in the sustained year-over-year performance of Kaspersky products in independent tests

We structure our world-leading AI research and development around two critical missions:

AI-powered cybersecurity

We use AI to defend your organization against the full spectrum of threats, from high-volume malware to sophisticated, AI-enhanced attacks.

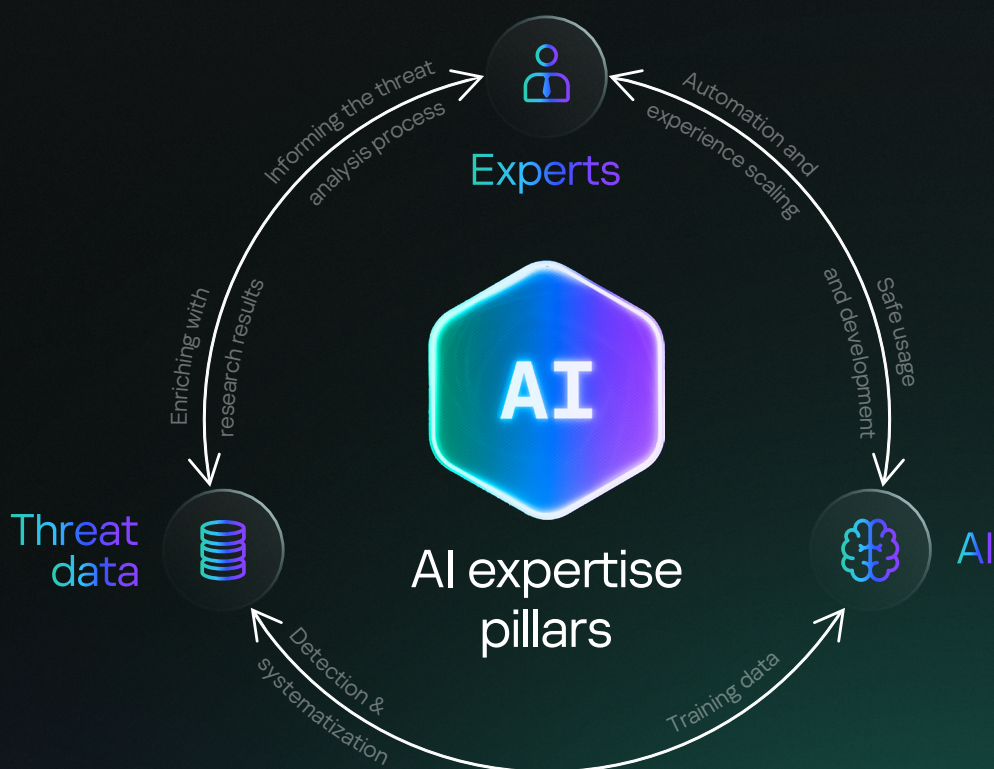


Security of AI

As your organization adopts AI, a new attack surface emerges. **Kaspersky AI CERT** helps you secure your AI systems, from LLMs to industrial models, against prompt injection, data poisoning, model theft and supply chain compromise.



The foundation: data + experts + AI



TOP 3

Most tested. Most secure. Proven over years of independent validation.

[Learn more](#)



Our AI is only as strong as its data and the experts behind it. Kaspersky Security Network accumulates the anonymized global threat telemetry, which is continuously enriched by expert security researchers and incident responders. This virtuous cycle keeps our AI models accurate and resilient.

AI in action: stronger security, smarter SecOps

1 AI for threat detection: the quiet genius

Our multi-layered AI stack is embedded across our IT and OT security portfolio, working quietly to stop malware, ransomware, phishing and other attacks before they impact your business.

It combines statistical, static and behavioral AI/ML models running across the cloud and customer systems, ensuring the most effective detection of new threat variants without over-reliance on cloud mechanisms or constant connectivity.



Growing number of threats:
500 000/day

Malicious objects detected by Kaspersky



2 AI for SecOps: augmenting your team, not replacing it

The security talent shortage is acute. Your SOC analysts are overwhelmed by alert volume. Our AI for SecOps is the ultimate force multiplier, helping your team work smarter, investigate more effectively and respond faster.

2.1 AI automation for security operations

DLL hijacking detection

Uses global, anonymized DLL loading telemetry to baseline normal activity, then assesses anomalies and alerts analysts.

Account theft detection

Learns normal account behavior for baseline to detect anomalies.

AI risk scoring

Models «normal» host activity, identifies unusual alert chains likely to indicate compromise and automatically prioritizes, helping analysts cut through the noise and focus on higher-priority threats.

Used in:



**Kaspersky Next
XDR Expert**



**Kaspersky
Unified Monitoring
and Analysis Platform**

AI-driven managed security

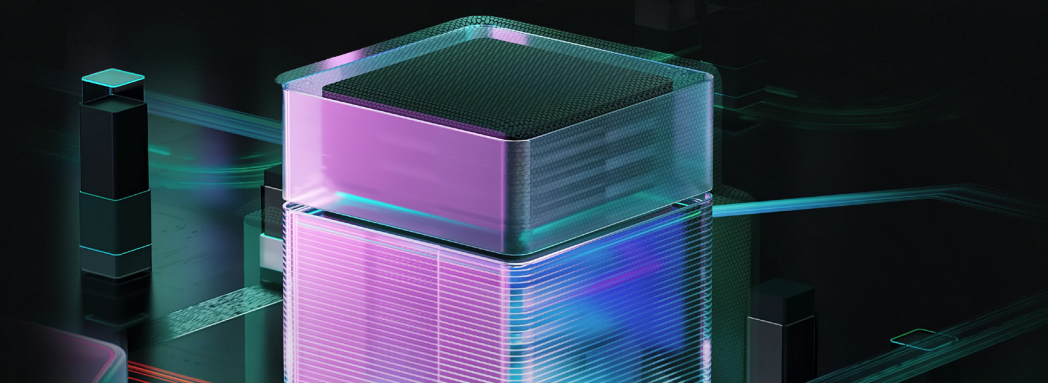
Our analysts' work is augmented by our AI Auto-Analyst, ensuring 24/7 coverage and faster mean time to respond (MTTR). According to Kaspersky MDR statistics, the AI Auto-Analyst technology reduces the load on Kaspersky SOC experts **by 25%**.



**Kaspersky Next
MXDR Optimum**



**Kaspersky
Managed Detection
and Response**



2.2 GenAI assistance for security operations

KIRA: your GenAI copilot for SecOps

Kaspersky Investigation and Response Assistant (KIRA) is a family of GenAI tools tuned to security. You can connect any OpenAI compatible LLM – your data, your choice.



Incident summarization

Generate a plain language narrative of the entire attack chain in a single click.

On demand script analysis

Deobfuscate malicious code to understand behavior in seconds.

Natural language threat hunting

Ask in plain English and get structured queries in return, lowering the learning curve.

Container image scanning result summaries

Get a clear, complete image description, with risk analysis and a final assessment.

GenAI-assisted threat intelligence

Our GenAI assistant is engineered to sift through massive volumes of OSINT data, transforming raw information into succinct, easy-to-digest reports that accelerate your situational awareness.



Kaspersky Next
XDR Expert



Kaspersky
Unified Monitoring
and Analysis Platform



Kaspersky
Container
Security



Kaspersky
Threat Intelligence
Portal



AI-driven cybersecurity.
Outthinking cyberthreats.

[Learn more](#)

www.kaspersky.com

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

#kaspersky
#truetobusiness