kaspersky

How 20 years of AI expertise is shaping the future of cybersecurity

Two decades of AI, one mission: build a safer world

Cybersecurity is undergoing a dramatic transformation driven by the rise of artificial intelligence. Threats are growing in complexity and speed and many businesses are demanding AI-powered solutions to counter them. In fact, 94% deem them crucial,[1] and with good reason: in 2024, organizations using AI and automation extensively in prevention averaged savings of $2.2 million versus those that didn't.[2]

Vendors are racing to capitalize on this demand with campaigns built on "next-gen" AI features, but amid the surge of solutions, one truth stands out: not all are created equal. AI models, by nature, are only as good as the data they're trained on and the context in which they're applied. Inexperienced vendors may rely on limited datasets, overlook subtle attack vectors or fail to prevent adversarial manipulation, which can lead to false positives, misplaced confidence – and missed threats.

Kaspersky, however, began implementing AI and machine learning (ML) in its solutions over two decades ago. While movies like I, Robot were envisaging humanity's demise at AI's hands, Kaspersky was exploring the potential of this infant technology to make the world a safer place. This foresight, coupled with long-term investment, has resulted in smarter, faster and more reliable protection today – not built on hype but on years of innovation and proven performance.

All of this leaves Kaspersky well placed to shape the future of AI-driven security.

[1] Kaspersky, Cyber defense & AI: Are You Ready to Protect Your Organization?, (Kaspersky, 2024)
[2] IBM, Cost of a Data Breach Report 2024, (IBM, 2025)

20 years of innovation, training and real-world testing

For over two decades Kaspersky has built and refined advanced ML models trained on huge volumes of anonymized global telemetry, collected ethically and responsibly from millions of endpoints worldwide. This reservoir of high-quality data has enabled Kaspersky to develop AI systems that are not only safe and accurate but also resilient to evolving threats.

What sets Kaspersky apart is that AI isn't a bolt-on feature; it's embedded in every layer of its technology stack. Head of Unified Platform at Kaspersky Ilya Markelov says:

> All of our products include AI technology. SIEM, EPP, EDR, NDR, XDR, MDR, Threat Intelligence – all of them. Where there's no AI assistant, there's KSN – a global network delivering insights from our cloud-based models to our customers. AI drives almost everything we do.

This deep integration ensures faster detection, smarter automation and a consistent standard of protection across all of its products.

With AI as a foundational capability, not an add-on, Kaspersky delivers cybersecurity that's informed by its real-world usage. The vendor doesn't propose what AI might be able to do; it has proof of what it's already done with the technology, being one of the first to start leveraging it. Kaspersky CEO and Founder Eugene Kaspersky says:

> What I'm especially pleased and proud of in this process is that our company was one of the first in the industry to successfully implement this bright AI future. How else could we cope, for example, with almost half a million new malware every day? No educational system in the world could graduate so many experts.

While today the company has a well-established AI Technology Research Center, which tackles challenges at the AI–cybersecurity intersection, it began the journey in 2004 when its first AI/ML technology for automatic analysis of malicious code was born.[3] Kaspersky named it Auto-woodpecker because, at the time, it lovingly called its human analysts who were "pecking away" at viruses "woodpeckers." Auto-woodpecker could do this usually time-consuming job independently, freeing specialists from routine work and helping to highlight identical (or likely) incidents. The result was productivity that increased many times over.

Another milestone in the company's journey was its patenting of an automated false-positive testing technology based on ML algorithms in 2015.[4] Between 2019 and 2022, the number of ML inventions patented by Kaspersky increased by 19 times.[5] And in 2024 it achieved a 25% increase in APT detection using ML.[6]

More recently, in 2025, Kaspersky updated its SIEM platform with a powerful new AI module for faster and more effective alert triage.[7]

[3] Kaspersky Eugene, What is "Autowoodpecker" and What Does Artificial Intelligence Have to do with It? The Mystery of A 20-Year AI Journey, (E-Kaspersky LiveJournal, 2025)

[4] Kaspersky, Kaspersky Lab Patents Automated False-Positive Testing Technology Based on Machine Learning Algorithms, (Kaspersky, 2015)

[5] Kaspersky, The Number of Machine Learning Inventions Patented by Kaspersky Has Increased 19 Times Over the Past Three Years (Kaspersky, 2022)

[6] Kaspersky, Kaspersky Achieves 25% Increase in APT Detection with Machine Learning, (Kaspersky, 2024)

The result: smart, fast, accessible protection

Kaspersky's long-term AI investment has resulted in a cybersecurity portfolio that delivers smart, fast and accessible protection for businesses of all sizes. Its AI technologies power real-time threat detection, behavioral analysis and automated response, ensuring a rapid and intelligent defense against both known and emerging threats. Trained on global threat intelligence, its models are capable of detecting novel and targeted attacks that may evade traditional security tools.

These capabilities are embedded across the entire product suite. In 2024, more than 6 million attacks on users of Kaspersky's mobile products were prevented by Cloud ML, a cloud-based AI technology that detects even previously unknown malicious Android apps in real time by analyzing a set of unique attributes. Kaspersky Anti Targeted Attack (KATA) solution uses machine learning to uncover complex, multi-stage threats for enterprises. And around 1,000 phishing webpages are detected daily by its ML-based web phishing detection engine.

A fully AI-powered portfolio – not just at the top end – means the technology works for, and is accessible to, Kaspersky's broad range of customers. Small to medium-sized businesses can access enterprise-grade protection without the need for large in-house teams, while enterprises get security that augments their capability and scales alongside them.

Conclusion: proven experience matters

Kaspersky has continuously refined its AI technology to stay ahead of evolving cybersecurity threats. Its long-term commitment to in-house development allows it to build AI that is not only smarter but also more trustworthy and better equipped for the challenges of tomorrow. This deep expertise enables it to deliver proactive, reliable protection that adapts and learns as cyberthreats evolve. And as cybercrime becomes faster and more sophisticated, Kaspersky's AI will become an even more vital asset in securing businesses from harm.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With over a billion devices protected to date from emerging cyberthreats and targeted attacks, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection, specialized security products and services, as well as Cyber Immune solutions to fight sophisticated and evolving digital threats. We help over 200,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

www.kaspersky.com