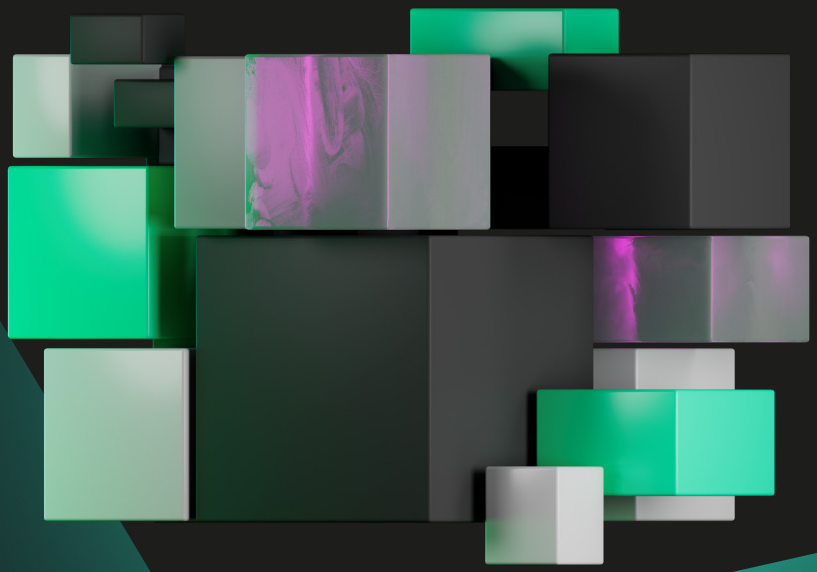
kaspersky



The future of AI in cybersecurity: what's next?

A new era of cybersecurity has arrived

Few industries match security's speed of growth. Attacker innovation and persistence ensures that it never, ever stands still. In 2024, for example, the mean time to investigate and report cyber incidents surged by 48% compared to the previous year, reflecting a significant increase in attack complexity.[1]

AI has facilitated an increase in the volume of attacks too, with bad actors automating tasks such as coding, copywriting and reconnaissance. The barrier to entry has also been lowered, with lesser-skilled adversaries able to do more with the same limited skill set.

Vladislav Tushkanov, Group Manager at the Kaspersky AI Technology Research Center, says:

> Those already skilled are able to work faster – and those not skilled at all gain more capability. This is called an 'uplift' – when a complete script kiddie can do something that they couldn't do before. Instead of spending a month studying programming, they can just ask ChatGPT.

1. Kaspersky, MDR Analyst Report 2024, (Kaspersky, 2025)

It's unsurprising then that in 2024, most InfoSec pros saw a notable increase in cyberattacks compared to the previous year.[2] This is because AI has moved from a peripheral offensive role to a central one. The same is true of defense, with AI helping to detect anomalies fast and lessen the burden on IT-security staff.

And thus, the AI arms race is underway. A frontrunner in that race is Kaspersky, which has been leveraging AI under the hood of its solutions since 2004. Unlike many vendors still getting to grips with its defensive potential, Kaspersky has already built proven expertise, as demonstrated by its AI Technology Research Center.

This means it is perfectly placed to not only anticipate threats but also to shape what comes next, ensuring its customers can thrive under increasingly tumultuous conditions.

Cyberthreats are becoming AI-native

Bad actors are adopting AI tools to maximize the speed and stealth of their attacks. A particularly dangerous proponent are deepfakes, which encompass AI-generated image, video and audio content. British engineering firm Arup fell victim to such content when an employee was duped by an AI-generated video call into sending $25 million to criminals.[3] Elsewhere, fraudsters made $35 million after forging emails and audio to convince an employee of a UAE company that a director needed money for an acquisition.[4]

Tushkanov adds:

> Synthetic media allows attackers to depict events that didn't happen, and they use it against both end users and businesses. The crypto community often suffers. For example, scammers collect money they purport is for charity, or pose as your boss and request a wire transfer.

This has made attacks more personal and targeted than ever before. They play on the victim's emotions – be it fear, greed or trust – to drive action. But it's not just deepfakes causing problems. AI can enhance or automate various stages of a cyberattack. It can significantly increase the speed, efficiency and adaptability of the attack; for example, by providing an attacker with contextual advice on how to avoid detection by security solutions.

It can enable lower-skilled attackers to do more and at greater speed. This cut-and-paste method, however, has resulted in attacks that are extremely similar in terms of their execution. So, while there's a constant barrage of them, they're not particularly hard to spot.

Tushkanov explains:

> To detect AI, and to prevent your analysts from getting bogged down in routine, in the daily analysis of an ever-increasing number of alerts, you need machine learning (ML). It copes with this perfectly – and your professionals will save time for complex or business-critical tasks.

Increasing attack volumes have left 72% of businesses seriously concerned about the leveraging of AI by attackers.[5] They want equally fast and intelligent defenses, perhaps knowing that traditional defenses struggle against scalable, self-evolving threats. It's therefore crucial that businesses can rely on vendors with experience implementing AI to stay ahead of attackers.

Vladislav Tushkanov says:

> We shouldn't think 'all is lost, cybercriminals will hack everyone now.' We should say, 'AI has given us the same efficiency boost,' because everyone engaged in cyberdefense and threat monitoring enjoys using AI just as much as the bad guys.

2. Kaspersky, Cyber Defense & AI: Are You Ready to Protect Your Organization? (Kaspersky, 2024)
3. Milmo Dan, UK Engineering Firm Arup Falls Victim to £20m Deepfake Scam, (The Guardian, 2024)
4. Lemos Robert, Deepfake Audio Nabs $35M in Corporate Heist, (Dark Reading, 2021)
5. Kaspersky, Rising Concerns, Lingering Gaps: Most Organizations Fear AI-Driven Cyberattacks but Lack Key Defenses, (Kaspersky, 2024)

AI is the new cybersecurity cornerstone

It's clear that AI is becoming a cornerstone of modern security, evolving from a supporting tool to the central intelligence driving advanced defense systems. Its growing role brings a shift toward predictive analytics and contextual awareness as foundational capabilities in threat detection and response.

Harnessing AI's potential demands deep expertise, proven experience and a foundation of trust. It also requires the ability to adapt and learn from global telemetry. This is something Kaspersky has been doing for years, ensuring its defenses stay one step ahead in an ever-changing threat landscape. Its deep expertise in applying these technologies to cybersecurity, coupled with its unique datasets, efficient methods and advanced model-training infrastructure, have become the bedrock of its approach to solving complex business challenges.

But what's the real difference between a vendor like Kaspersky and a skilled newcomer? Vladislav Tushkanov says:

> It's a difference in approach of course. If you've been doing this for a long time, you understand what challenges you can face, because it's far likelier you have faced them before. And this reduces the likelihood of critical mistakes. You can't really get that experience any other way – only by learning on the job.

So, while AI is becoming increasingly important to cybersecurity vendors, it's not as simple as "pick up and play." It's something that must be built into solutions and iterated over time, drawing on vast global telemetry to be effective. This is why Kaspersky is able to analyze and classify over 460,000 malicious samples every day using AI technologies.

How tomorrow's AI will transform security operations

A key objective in cybersecurity is not just reducing mean time to respond but also preventing attacks before they happen. AI is central to achieving this goal by enabling faster detection, automated response and predictive capabilities that allow businesses to move from reactive to proactive defense. By anticipating threats and acting in real time, AI can significantly shrink response windows and minimize damage.

But achieving this goal doesn't mean replacing cybersecurity professionals; it means empowering them. Human-AI collaboration will define the next era of cyberdefense as AI increasingly handles repetitive tasks and delivers insights that guide decision-making. Analysts will be freed to focus on complex investigations and strategic planning, supported by intelligent systems that learn and adapt alongside them. Tushkanov adds:

> Right now everyone is talking about 'agents.' This refers to intelligent systems or components that perform tasks autonomously or semi-autonomously to protect environments. You tell them, 'I have this script executed on the host, what do you think?', and they say, 'Under normal conditions, this shouldn't be executed. I would report it.'
>
> So, there is a hypothesis: if you can create an agent system where you can load enough context so a first-line human analyst can make an informed decision, then, theoretically, large language models (LLMs) will be able to decide with equal reliability. That would mean more first-line automation. There are things that are easy to script: a clear sequence of necessary actions. And theoretically, you can write a script that will perform these actions, receive the variables needed for the decision and make that decision.
>
> But many scenarios do not work this way. During the investigation, there are multiple options of where to go and what to look at. Only a human eye can understand in which direction the investigation should proceed. In the future, LLM agents may be able to make such decisions. But right now, the human touch is crucial.

Building resilient, trustworthy AI for a smarter defense

Kaspersky isn't only interested in keeping security human in the wake of AI. It's also focused on developing trustworthy and secure AI that stays ahead of emerging threats. Secure AI development and application is therefore critical to its business strategy because it ensures that its algorithms are trustworthy and resilient. For example, it trains its AI under strict security standards so that its detections are never manipulated and it works hard to protect its models from exploitation. This aligns with growing expectations around ethics, transparency and compliance and is especially beneficial for Kaspersky's customers in heavily regulated sectors. To build further trust, the vendor periodically opens its doors to reveal its inner workings.

Conclusion: the future of security is AI-powered

The future of cybersecurity will be AI-native, shaped not just by the power of algorithms but by the trust, resilience and human judgment behind them. As threats grow more complex and fast-moving, the leaders in this new era will be those who can seamlessly combine cutting-edge AI with decades of real-world security expertise.

Kaspersky's legacy in cybersecurity, paired with its deep, ongoing investment in AI, is delivering solutions that are not only intelligent but resilient, adaptive and ready for what's next. From predictive threat detection to autonomous response, it is building systems that learn, evolve and defend – empowering organizations to stay ahead, not just keep up.

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