kaspersky

Democratizing cybersecurity: how Kaspersky AI is making defense accessible to all

The great new cybersecurity divide

Cyberthreats are like a freight train travelling downhill without brakes. They continue to gather momentum and stopping them is difficult for even the most resilient organizations. Expert-level cyberdefense, once a privilege, has become a necessity. But this need is not easily satisfied. The people with the skills, expertise and experience to intervene are in short supply, and even the wealthiest businesses are struggling to recruit them.

Yet, traditionally, the world has relied on such experts to keep it safe. Before cybersecurity became a core business function, when cyberthreats existed but not abundantly, a couple of experts who could manage basic antivirus and firewalls sufficed. In the last decade, however, headline-hitting attacks such as NotPetya, WannaCry and SUNBURST have annihilated the idea that basic defenses are enough.

A new security pendulum now swings in the form of AI, and it is coveted by bad actors and defenders alike. It can facilitate faster, more expansive attacks, but it can also bridge the security skills gap by equipping everyday users and businesses with advanced capabilities, lowering the barrier to entry. If democratized, AI in cybersecurity will reduce – not eliminate – the need for experts so that every business has a fair chance of defending itself.

Fittingly, Kaspersky is using its own AI expertise to realize this vision.

A dearth of cybersecurity expertise

Today, there is a global shortage of skilled and experienced security professionals. More than 40% of InfoSec pros say their organization's security teams are "somewhat" or "significantly" understaffed, while half of them say the theoretical knowledge gained in their formal education was useless when it came to performing their current job. Less than half of them were provided hands-on experience at college or university at all.[1]

Not only is there a dearth of prepared security pros, but many organizations cannot afford them, making it impossible to run a 24/7 security operations center (SOC). Even those with immense resources are struggling to recruit, with 48% of InfoSec professionals claiming it takes more than six months to fill a position.[1]

Unfortunately, even the most advanced products cannot protect an organization on their own. They require skilled operators to be effective, which means a lack of qualified analysts and operators leaves organizations vulnerable.

Compounding the skills shortage is burnout among security operations professionals. Head of Unified Platform at Kaspersky Ilya Markelov says,

> When a cybersecurity professional is doing their job well, their day-to-day work should be largely routine – checking logs, reviewing accounts, checking rules, ensuring policy compliance, etc. Although these may not be complex tasks, they are critical. Doing them manually quickly leads to burnout, and as a result, analysts often consider changing jobs or professions. One of our AI goals is thus to reduce operational burden and minimize routine tasks.

The skills shortage, combined with the complexity of modern threats, has made manual monitoring and response unviable for most businesses. Incidents that could have been detected early are therefore going unnoticed, resulting in financial losses for businesses everywhere.

Kaspersky AI as the equalizer

Kaspersky has been developing AI-powered cybersecurity for more than 20 years and its machine learning (ML) models are trained on global threat intelligence and leverage a huge amount of telemetry. They can identify the most critical alerts from its monitoring systems, ensuring Kaspersky customers have time to focus on serious threats.

The company also trains its models on all available industry knowledge – not just its own. Take the MITRE ATT&CK matrix, for example, a vast knowledge bank concerning attackers' tactics, techniques and procedures. Kaspersky's AI recommends incident response actions based on the framework's descriptions, meaning it doesn't rely exclusively on its own expertise.

Markelov says,

> Another good example of our AI in action is the Kaspersky security information event management (SIEM) system. If there's a log containing a cybersecurity event, the user sees the event as an encrypted string, which is completely unintelligible. This is because malware operators try to hide their presence in logs by encrypting their commands. But our AI module decodes these commands from the garbled strings and explains what the script will do – in readable language that's easy to understand.
>
> Previously, to process such an event and determine if it was dangerous, the operator had to find a script to decode the cipher, such as Base64. This required knowledge and effort to identify what the code was; to decrypt it to see the command, such as a PowerShell script with numerous parameters; and to open the PowerShell documentation to understand what would happen if the script executed.
>
> Our AI ensures none of this is necessary. The operator simply clicks a button on the interface and our module explains what the script will do, including a traffic light alert indicating the risk level of each threat.

Everything Kaspersky strives to do with AI is with the customer in mind. That's why it focuses heavily on ease of deployment, intuitive dashboards and proactive protection that simplifies the lives of security teams.

[1] Kaspersky. The Portrait of Modern Information Security Professional. (Kaspersky Daily, 2024).

Why and how Kaspersky is making enterprise-grade security accessible to all

Kaspersky has spent years gathering data about, experimenting with and deploying AI in its solutions. But it considers this expertise useless unless it can get it into the hands of the many. The company's philosophy is that every business has a right to world-class security – be it a tech startup, major hospital or digital bank – and that the more secure organizations are collectively, the closer a safe tomorrow gets.

SMBs

Kaspersky is particularly interested in helping small-to-medium sized businesses (SMBs) who may lack the budget or expertise to maintain a dedicated security team. Its AI-driven solutions can help such businesses detect threats including malware, ransomware and phishing automatically without constant human intervention, meaning they can greatly increase their security without hiring in.

Its systems also integrate seamlessly with existing IT infrastructure and can provide real-time alerts for suspicious activity, even taking automated steps to neutralize threats. This means its SMB customers can protect themselves with minimal effort and cost – almost like having their own virtual analyst.

Markelov says,

> We leverage AI to enable less skilled, less experienced people to perform complex security product management tasks. Generative AI reduces the skill requirements because the system explains and guides extensively – advising where to look, what to do and what a particular command does – all in plain language. It provides the necessary context and additional information to the user, thereby reducing the skill and experience requirements.

But despite heavy automation, the final decision always rests with the human operator, as the company believes in every business's right to autonomy.

Enterprises

Unlike smaller businesses, large enterprises often have mature security teams. Kaspersky's AI is here to augment those teams – not replace them.

Markelov continues,

> The value lies in reducing the workload on the team, lowering skill requirements and maximizing efficiency through automation. AI doesn't replace analysts, but allows them to focus on critical tasks instead of getting bogged down in routine.

Enterprises are also facing increasing complexity – not only as they adopt new systems but also as they are targeted in more advanced attacks. Kaspersky's AI and automation can equip their security teams to manage this increasing complexity, eliminating the need for proportionate growth and, ultimately, save them money.

What you get: trust, transparency and elite performance

Kaspersky wants AI cybersecurity to benefit all. And that means those using it must be able to trust it. Secure AI development and application is therefore critical to its business strategy because it ensures that its algorithms are trustworthy and resilient. It trains its AI under strict security standards, for example, so that you know its detections are never manipulated, and it works hard to protect its models from exploitation.

Markelov comments,

> As our AI models continues to learn, our experts review results and adjust as needed. We also provide users with full reasoning behind AI decisions. For example, instead of merely indicating that a green light equals safe, we explain why AI views it as safe. We also indicate whether we think the AI may be hallucinating and leave all final decisions with the end user.

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 company periodically opens its doors to reveal its inner workings.

Elsewhere, its dedicated research unit, the Kaspersky AI Technology Research Center, unites data scientists, ML engineers, threat experts and infrastructure specialists to tackle the most challenging tasks at the intersection of AI/ML and cybersecurity. This includes not only the development of applied technologies but also research into the security of AI algorithms.

Accompanying this trust and transparency is elite performance, as AI drives its award-winning solutions day in, day out. As an example, its AI technology closed over 70,000 alerts within its MDR service in 2024.[2]

Markelov says,

> All our technologies are independently tested. Kaspersky participates in many market comparisons that evaluate the detection and response capabilities of all our products – which we consistently lead in accuracy and speed of response. Not just for our AI, but our entire product suite.

[2] Kaspersky. MDR Analyst Report 2024. (Kaspersky, 2025).

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.

Conclusion

AI in cybersecurity is no longer optional. It is essential in keeping pace with bad actors and helping to plug the cybersecurity skills gap. Fortunately, the AI found in Kaspersky's solutions is opening up elite cybersecurity to every business.

www.kaspersky.com