kaspersky

How Kaspersky AI helps to protect endpoints

How Kaspersky AI helps to protect endpoints

The threat landscape is more dangerous than ever before. Cybercrime has been a specialized industry for a long time and its perpetrators are constantly crafting new malware and ideating new attack techniques. The Kaspersky collection now contains more than 2.1 billion malicious samples, a number that has doubled in just the last five years. Its automatic systems are discovering more than 467,000 new threats every day, and that number too has doubled in recent years.

The point where malware threats can be countered with traditional technologies alone has long been surpassed. That's why Kaspersky started using AI 20 years ago and has been continuously improving its technologies since. It believes in a multi-layered approach to cybersecurity – and that each layer can be strengthened using AI.

Regarding endpoint protection, the first layer is static analysis, which is the first line of defense. Kaspersky's endpoint solutions monitor possible sources of infection – such as internet surfing, email, local network, removable USB drives and new applications – depending on the platform and operating system. All incoming objects are scanned by its engines, in which multiple AI technologies exist.

Kaspersky's engines extract metadata and dissect the object to collect features – unique parameters that can describe the object. These features (thousands of them in fact) are processed by machine learning (ML) models based on decision tree ensembles. These predictive models are trained on datasets consisting of millions of carefully picked training examples using algorithms such as random forest or gradient boosting and comprise a set of decisions. One of these models, PE Forest, detects tens of thousands of malicious files every day. These models are used both in the cloud and at the edge.

Another important technology used for static analysis is similarity hashing. Also called locality-sensitive hashing, it is an AI method used to detect similar malicious files. To create similarity hashes, the system extracts file features and uses orthogonal projection learning to determine the most important. ML-based compression is then applied so that value vectors of similar features are transformed into similar or identical patterns. This method provides solid generalization and noticeably reduces the size of the detection record base, since one record can detect the whole family of polymorphic malware (i.e., malware that alters its body each time it replicates, while retaining its core functionality).

The complex distributed infrastructure found in Kaspersky Security Network (KSN), combined with automatic processing systems, acts as a global cyber-brain, collecting and analyzing threat data from millions of voluntary participating users to spot threats instantly. It analyzes millions of samples every day and processes billions of notifications from KSN, aggregating threat intelligence about suspicious objects using multiple AI technologies. Astraea Reputation System aggregates all of the statistics with meta-information about suspicious objects worldwide in real time. The object's reputation is then calculated following analysis, and information about new malware threats is immediately available to all users through KSN. If Astraea has insufficient information about the object to make a decision, it will repeat the analysis when extra information is gathered.

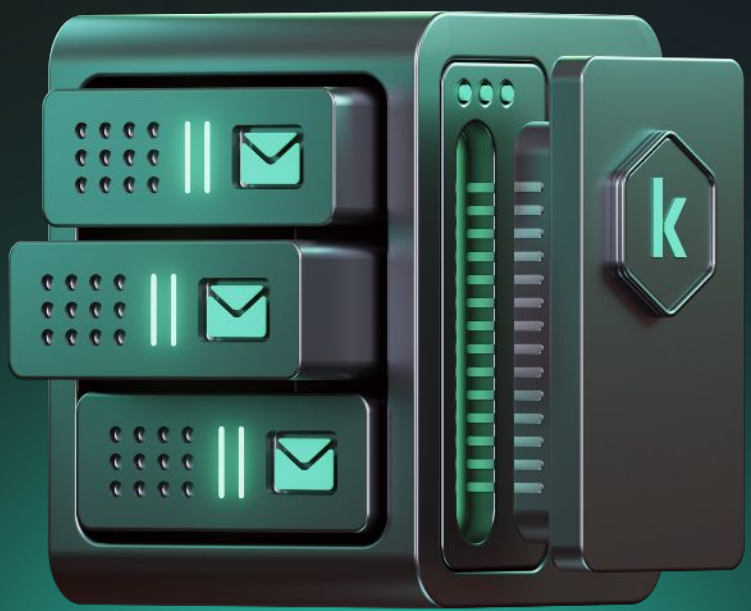
Similarity Hash Detection System is another ML-based technology aimed at detecting malware variations. The cloud component of the system aggregates multiple file features from different sources including in-lab automatic systems of malware processing. An ML algorithm is then used to find features common to a whole group of similar malicious files. Based on these features, Similarity Hashes (SH) are calculated and made available to KSN users. According to Kaspersky's telemetry, this technology protects hundreds of thousands of its customers from new malware every day.

Elsewhere, Cloud ML for Android is a cloud-based technology that protects Android smartphone users. The model is trained on millions of mobile malware samples and can detect malicious apps with high accuracy, covering over 90% of new and unknown threats and preventing millions of attacks on Kaspersky customers every year.

Kaspersky's internal automatic processing systems also use AI extensively. Besides the aforementioned technologies, it uses heavy ML models that cannot be run on endpoints or in the cloud (due to high resource requirements) but are extremely capable and accurate. For example, it uses ML models based on neural networks trained on hundreds of millions of legitimate and malicious samples both to find new malware and to prevent false positives. The model detects over 80% of new malicious files through its automatic processing systems. Other ML models analyze behavioral logs and traffic from its sandboxes. Detection for malicious objects is rapidly delivered to endpoints protected by its solutions using cloud-based KSN services.

Kaspersky's patented web phishing detection model is trained on a comprehensive dataset of millions of samples to detect malicious web pages based on both its content and metadata. It works by extracting advanced insights into patterns that define phishing pages, ensuring robust threat identification and enabling detection of hundreds of thousands of phishing web-resources per year. Extensive testing and specialized filtering mechanisms are designed to minimize false positives while maintaining industry-leading accuracy.

Kaspersky also uses AI to detect malicious and phishing domains based on their infrastructure relationships with known malicious and phishing domains. It constructs a graph of domains based on their metadata and DNS resolves and uses ad-hoc ML models to reveal whether the classification can be spread from known malicious or phishing domain vertices to their graph neighborhoods. Trained on millions of domains, the model prevents several million phishing-link clicks each year.



If the threat wasn't stopped before the execution, the second layer of protection kicks in. A behavioral detection engine monitors all process behaviors using a behavioral AI model, the power of KSN, and information from static analyses to detect malicious patterns and stop malicious behavior.

And it does not stop there. Even if a threat happens to penetrate the static analysis layer, the next layer steps in – expert security solutions for its SOC-expert customers. Kaspersky Next XDR leverages AI to improve the effectiveness of SOC teams by reducing the noise of unnecessary alerts, automatically analyzing and explaining events and detecting anomalous behavior such as DLL hijacking attacks. The Kaspersky Threat Intelligence Portal uses AI to summarize threat intelligence data and reduce the load on analysts.

As described above, Kaspersky leverages ML across multiple layers, from file structure analysis to behavior monitoring, using various types of AI. This covers both on-device and cloud-based scenarios; for example, gradient boosting, deep neural networks and large language models. These technologies provide protection to millions of users in real time, adapting to the dynamic evolution of cybercrime.

By harnessing the power of AI, Kaspersky not only detects known malware but also predicts and neutralizes emerging threats with unprecedented precision.[1] This proactive approach ensures that users are shielded from sophisticated attacks, such as zero-day exploits and polymorphic malware, which constantly evolve to evade detection.

Furthermore, Kaspersky's AI-driven solutions are designed to minimize false positives, balancing robust security with operational efficiency. Through continuous learning and updates, its systems adapt to new attack vectors and threat landscapes, maintaining a high level of accuracy and reliability. Whether protecting individual devices, corporate networks or critical infrastructure, its ML technologies empower users to stay one step ahead of cybercriminals.

1 Kaspersky. Most tested. Most awarded. Kaspersky Protection. (Kaspersky, 2024).

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