



Digital Security  
Progress. Protected.

# ESET TECHNOLOGY:

AI and Proactive  
Cyber Defense

## THE CHALLENGE — AND THE CALL FOR AI

Today's cyber-adversaries are motivated, ingenious, and persistent, and security teams that are tasked with preventing them from getting a foothold in the network need all the resources they can get.

Artificial intelligence (AI) technologies that extend human capabilities are one way to support and augment the efforts of human cyber-defenders. While there has been a sudden burst of interest in these technologies both inside and outside of security circles, the fact is that AI technologies have been defending networks for more than 25 years, as we'll explain later.

But first, let's get some definitions out of the way. When we say proactive defense in

the context of defending an endpoint: we mean never allowing attack vectors to reach the endpoint or never allowing it to execute.

When we say proactive defense it is in the context of defending the network in general: we mean either denying entry, or if an intruder does manage to gain entry — say, through a user name and password purchased on the dark web — detecting and shutting down the threat before any real damage is done such as encrypting or exfiltrating data.

## PREVENTION OVER REMEDIATION

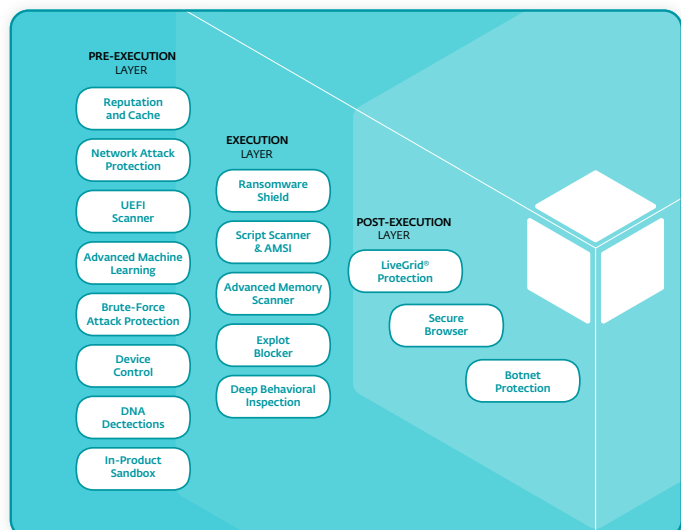
Clearly, preventing threat vectors in the first place is better than cleaning up the mess and damage an incident leaves behind. That's why ESET offers multiple layers of protection technology that block malicious code from entering, or executing within, a user's system. Indeed, during the crucial pre-execution phase alone, ESET utilizes eight layers of protection, including two different forms of advanced machine learning.

### THE BUSINESS IMPACT OF SECURITY AI AND AUTOMATION

According to a 2023 report,<sup>1</sup> extensive use of security AI and automation delivered these benefits for organizations compared to organizations that did not use them.

- >100-day reduction in the time taken to identify and contain data breaches
- \$1.76 million in lower data breach costs

<sup>1</sup> Ponemon Institute, Cost of a Data Breach Report 2023



- Pre-Execution Layer: These technologies halt attacks before they can become dangerous and include Advanced Machine Learning, Network Attack Protection, UEFI Scanner and more.
- Execution Layer: These technologies include Ransomware Shield, Advanced Memory Scanner and Exploit Blocker.
- Post-Execution Layer: Botnet Protection and LiveGrid® are just two of ESET's "post-execution" protection technologies.

Thanks to ESET's top-tier research and exclusive telemetry, we utilize our endpoint software to collect distinctive data on attacks and techniques worldwide. This includes insights from countries targeted by the most advanced hacker groups, often ahead of other security solutions. ESET research provides insight into the Tactics, Techniques and Procedures (TTPs) used in hands-on attacks, fileless attacks or complex attack chains, which then enables our customers to reduce their attack surface and the TTPs related to that attack surface. By touching the core of threat attack techniques, ESET blocks or complicates attacks across the entire attack chain.

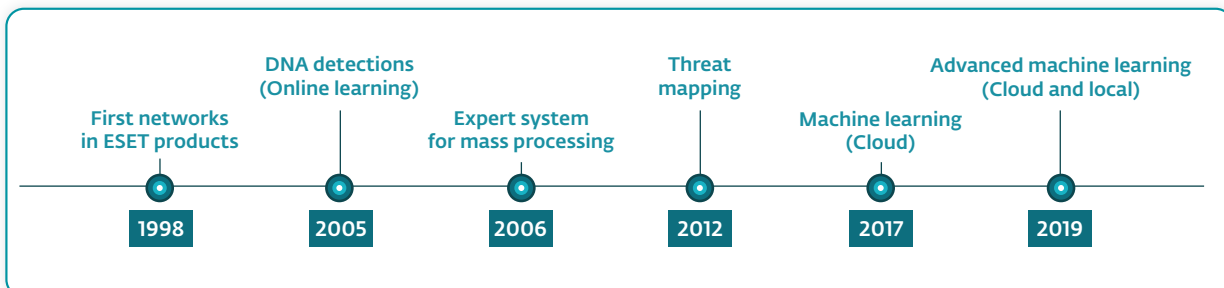
Processing hundreds of millions of Indicators of Compromise/Attack (IOCs/IOAs) every day, ESET leverages AI and machine learning to shift the attack chain left—offering truly prevention first technology.

## AI AT THE ENDPOINTS

In the mid-1990s, the internet was booming and so was the proliferation of adversaries. ESET engineers realized that one particular type of machine-learning AI algorithm — neural networks — had the potential to detect rapidly evolving threats with greater speed. The results were not merely promising, but led to a completely new approach to reducing the attack surface that also included heuristics and behavioral detection that were also powered by neural networks.

By the mid-2000s, adversaries had learned how to alter their threat vectors sufficient to evade detection. ESET responded by introducing "DNA detection," which extracts features of the sample and converts it into a form more suitable for matching and detection by the neural network machine-learning engine.

By the mid-2010s, after three decades of fighting adversaries, ESET had amassed a library of extracted features and "DNA genes" that provided a massive data set for training its neural network model. Meanwhile, big data and cheaper hardware were providing the information and the infrastructure necessary to build affordable, applicable machine learning algorithms in fields both inside and outside of security, leading to a surge of investment into academic and practical research.





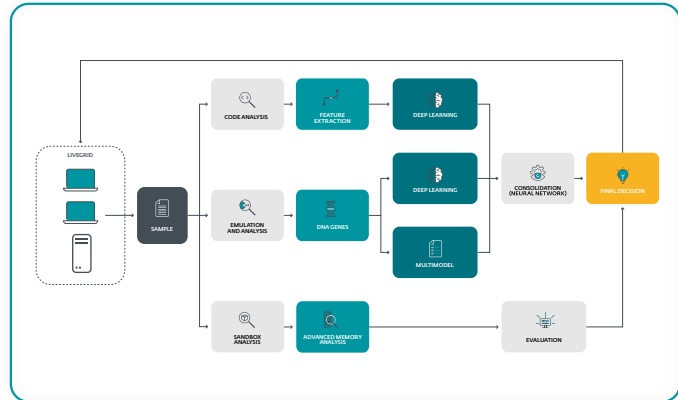
## AI IN THE CLOUD

In early 2016 ESET started to shape its new and exceptionally robust AI-powered detection engine in the cloud, trained by its highly organized adversary collection. The cloud-based engine has far greater processing power than an endpoint for processing more data and running more demanding computations, and is able to run a small army of machine learning models in parallel.

While the neural network engine on the endpoint is still able to run independently and classify most samples on its own, previously unrecognized, emerging threats that cannot be classified are automatically sent to the cloud engine.

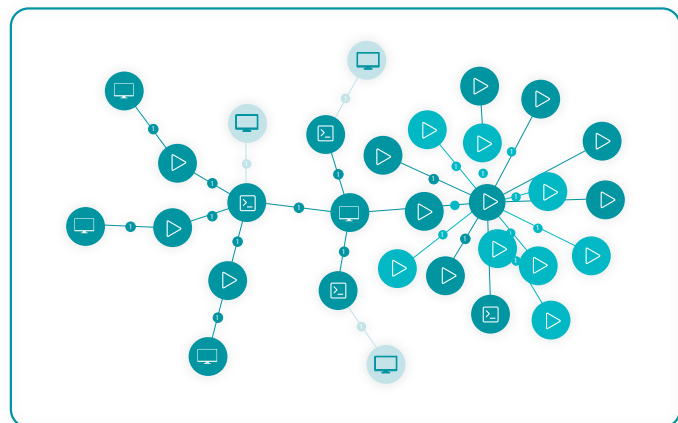
So, how does ESET Advanced Machine Learning in the cloud work?

1. Every sample entering ESET Advanced Machine Learning in the cloud is subjected to static analysis. The engine extracts the features of the sample, collecting information that is then fed to deep-learning algorithms.
2. The sample is also emulated as a part of dynamic analysis, producing DNA genes. These are fed to a series of precisely chosen classification models and another deep-learning algorithm.
3. The sample is then executed in a sandbox — a separate, high controlled environment where untrusted programs can be run and observed without harm — and compared with a set of previously known, periodically reviewed, and automatically updated clean and malicious samples.
4. The results from the previous steps are consolidated either via a neural network or other forms of evaluation and used to produce a final decision, labeling the sample as clean, a potentially unwanted or unsafe application, or malicious.
5. The information is then distributed to all ESET clients either via regular update or via ESET LiveGrid®, resulting in faster reactions to attack vectors and a greater awareness of emerging threats.



## AI ACROSS THE NETWORK

ESET Inspect is the XDR-enabling component of the ESET PROTECT Platform. It collects real-time data about ongoing activity on endpoints, which is then matched against behavior detection to detect suspicious activities automatically. The gathered information is processed, aggregated, and stored in a searchable form, creating a drill-down summary of unusual and suspicious activities.



ESET Inspect also provides the enterprise security team with information for forensic investigation of past incidents and offers response capabilities to mitigate the presence of threat actors and advanced persistent threats in the network. Machine learning is integrated into the ESET Inspect scanning process, and it is essential to the process of flagging suspicious activities and samples.

However, not everything that is suspicious is a genuine threat and alert fatigue is the bane of security teams everywhere. Therefore, ESET Inspect uses AI to look across the patterns of activity to detect when one or more suspicious events are related and reflect not merely isolated incidents but related or coordinated activity. It automatically generates a security incident complete with AI-created descriptions of what was found.

## AI IN HUMAN HANDS

AI today cannot replace skilled and knowledgeable security analysts and it's unlikely it ever will. AI technologies can certainly do things that security analysts would find much more difficult and time-consuming to do without help: Sift through and spot patterns in massive amounts of log data faster than humans can, and draw insights from that data at a scale that's beyond human capability.

Given the current state of AI, however, human analysts still need to be in the loop. Even if AI's findings indicate with seemingly absolute certainty that an attack is underway, humans need to corroborate the findings and ensure that the proposed remediation measures are appropriate to the threat and the organizational impact is justifiable.

Moreover, security analysts are needed to help train the models to the highest degree of accuracy, validate the output, stay abreast of the most current threat intelligence, and guide model evolution to keep up with the ever-changing tactics and techniques of adversaries.

## About ESET

### AI-NATIVE PREVENTION FOR TOMORROW'S THREATS

Stay one step ahead of known and emerging cyber threats with our **AI-native, prevention-first approach**. ESET combines the power of AI and human expertise to make protection easy and effective.

Developed over 30 years, ESET's best-in-class protection is powered by our **in-house global cyber threat intelligence**, including our **extensive R&D network** led by industry-acclaimed researchers.

**ESET PROTECT**, our scalable, cloud-first XDR cybersecurity platform combines next-gen prevention, detection and proactive threat-hunting capabilities with a wide range of security services, including **managed detection and response** (MDR). Our highly customizable, integration-ready solutions support all deployment methods, include local support and have minimal impact on performance. They identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

**Our mission isn't just to stop attacks in their tracks; it's to prevent them from ever happening.** ESET protects your business so you can unlock the full potential of technology.