Whitepaper

Automation Where It Matters Most:

How Small Teams Can Scale Up a Cyber-Prevention Strategy

Publication date:

07. 30. 2024

When it comes to cybersecurity, smaller organizations face many of the same threats and risks as larger ones, but have fewer resources they can bring to bear. Automating some of the tasks not only allows smaller teams to get more done, but also improves security by allowing essential tasks such as threat detection and vulnerability scanning to run at far greater scale. Here we take a look at the many ways to support a prevention-first cybersecurity strategy with automation.

According to a 2023 report,[1] 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

[1] Ponemon Institute, Cost of a Data Breach Report 2023

HARDEN SYSTEMS AND PREVENT RISKY BEHAVIORS

Endpoint security solutions have gone far beyond their original function of protecting systems with a software firewall and scanning for malware. Modern systems that include a central management console for administering endpoint security are capable of automating a number of security-related functions, with group assignments for managing endpoints by department or security need. This allows security teams to comprehensively manage the security posture of multiple hundreds or thousands of systems from a single pane of glass.

Security consoles can automate a number of tasks that improve the cybersecurity posture.

Vulnerability & patch management
Vulnerability scanning can be set to run automatically and patches applied immediately to address the highest-risk vulnerabilities or can be delayed to off-hours to avoid inconveniencing users.

Virtual desktop infrastructure
Virtual desktop infrastructure solutions often include tools and features that allow for automated re-imaging and cloning of virtual desktops, ensuring quick deployment, consistency and efficient management of desktop environments.

Action triggers
Some consoles are capable of automating activities such as launching scans, enforcing policy changes, and installing or uninstalling software.

Software remediation
Installation of unapproved software can be automatically detected and remediated automatically or semi-automatically with actions such as alerting IT, alerting the user or immediately blocking the installation.

Automated inventory
Detailed records of the hardware and software installed at each endpoint, automatically gathered and maintained by the endpoint security solution, assist with budgeting and planning upgrades.

DETECT THREATS QUICKLY AND ACCURATELY

Automation, and in particular automation that leverages artificial intelligence, is capable of doing something that's beyond human capacity: sifting through and correlating massive amounts of data about network traffic and endpoint activity and separating abnormal threats from normal behavior.

In the case of malware in particular, threat actors have proven adept at evading signature-based methods that detect known malware at the file level. They make superficial modifications and test them against endpoint security solutions until they evade the defenses, and pack the payloads so the malicious code isn't apparent in the file and only executes in memory.

Modern endpoint security software applies a number of measures that work in concert in an automated fashion.

Genetic matching
Rather than examining the whole file, the detection engine looks at telltale signs within the file that are indicative of malware, and are difficult to modify.

In-memory scanning
The detection engine examines computer memory looking for suspicious processes that evaded file-based detection, and shuts them down before they are able to execute.

Behavioral analysis
Suspicious files are allowed to safely execute in a sandbox, and activities are examined for malicious behaviors.

Cloud sandboxing
Examining malicious files in a cloud-borne sandbox takes advantage of massive processing power and scalability of the cloud to run more in-depth analysis than is practical on the endpoints.

GATHER INTELLIGENCE AND STOP EMERGING THREATS

Modern endpoint protection software doesn't only detect and block threats, but also serves as a vast network of sensors gathering massive amounts of intelligence about global threats. All of this information is gathered in real-time and processed with automated methods including artificial intelligence, providing a constantly updated picture of threat-actor activity around the world.

When endpoints are connected to the cloud and behavioral analysis detects new malware, the means to detect and block it are sent to all other endpoints in the targeted organization. Shortly thereafter they are shared with the connected endpoints at other organizations across the globe.

Automatically generated and shared intelligence is a major benefit of a modern connected endpoint protection platform, with the data disseminated via telemetry feeds for ingest by the endpoint software and other security tools.

Malicious files feeds provide information on newly discovered malware samples and the indicators of compromise associated with them, and the information needed to detect, identify and block them.

APT feeds typically focus on the indicators of compromise associated with the various active APTs, and are delivered directly to the security consoles to enable fast defensive action.

Botnet feeds focus on delivering intelligence about active botnets and the command and control servers associated with them, but may also include information about the organizations that are the likeliest targets.

Domain, IP or URL feeds identify locations associated with botnets, phishing campaigns or currently active attacks; vendors may deliver one, two or all three so that the malicious site can be blocked at the most appropriate level.

CORRELATE EVENTS AND DETECT ATTACKS

Despite the sophisticated protective technology of an automated endpoint protection platform, cyber adversaries are determined, motivated and inventive when it comes to finding ways to get past or around organizations' cyber defenses. Use of an endpoint detection and response (EDR) or extended detection and response (XDR) system to help detect, contain and mitigate intrusions is rapidly becoming the norm.

> Smaller organizations are likely to turn to specialists to operate a system, an offering termed managed detection and response (MDR). It is projected that by 2025, 60% of organizations will be using the services of MDR providers.[2]

Regardless of whether management is internal or external, these systems ingest massive amounts of data to detect potential threats and anomalous behavior. Therefore, for security analysts, it can be difficult and time-consuming to ascertain whether a suspicious event occurs in isolation or is part of a coordinated attack.

Current XDR systems are capable of applying artificial intelligence to correlate seemingly disparate events and determine which are part of a linked chain that indicates that an intruder is present or an attack is underway. They then put the information required to investigate the incident at the security analyst's fingertips. This level of automation reduces the time required for humans to detect and investigate an incident, so they can proceed as quickly as possible to executing an effective response.

[2] Gartner, Market Guide for Managed Detection and Response Services, Pete Shoard, Al Price, Mitchell Schneider, Craig Lawson, Andrew Davies, et al, February 2023

SPEED UP MITIGATION, CONTAINMENT AND RESPONSE

In addition to detecting threats, some endpoint protection platforms are capable of eradicating them as well without human intervention based on the configuration settings.

If there is a high probability that detected activity is malicious, some EDR/XDR systems can execute containment fully and automatically based on predefined response scenarios, or interactively with an assist from automation that invokes complex sequences with a click. Options typically include blocking executables, killing processes, isolating endpoints from the network and shutting down the endpoint or rebooting it. An EDR/XDR system that is integrated with endpoint protection also provides access to the endpoint platform's malware-removal capabilities.

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.

LEARN MORE

Digital Security
Progress. Protected.