# How to Improve Endpoint Security to Protect Organizations Against Advanced Cyberattacks

Published 5 April 2023 - ID G00780242 - 22 min read

By Analyst(s): Satarupa Patnaik, Peter Firstbrook

Initiatives: Infrastructure Security; Build and Optimize Cybersecurity Programs

Immature security practices make endpoints an easy target in advanced cyberattacks. Security and risk management leaders should follow this guidance to evaluate their current endpoint protection and develop a prioritized roadmap to improve the resilience of their endpoints.

**Additional Perspectives**

- Summary Translation: How to Improve Endpoint Security to Protect Organizations Against Advanced Cyberattacks
  (26 May 2023)

## Overview

### Key Findings

- Security and risk management (SRM) leaders relying on traditional signature-based endpoint security struggle with defense against fileless attacks, ransomware and identity theft. These attacks leave organizations increasingly vulnerable. Risk evaluation and assessment of the attacker's landscape are prerequisites for improving endpoint security and avoiding further threats to the organization.
- Most organizations employ a mix of tools from different maturity levels. However, they need comprehensive security operations (SecOps) and incident response (IR) technologies to help coordinate alert triage, investigation and response across all security tools.

### Recommendations

SRM leaders responsible for infrastructure and endpoint security must:

- Start by implementing the prerequisites for maturity assessment, which include employing endpoint detection and response (EDR) tools to improve behavioral detection, and conducting risk evaluation and assessment of the attacker's landscape.
- Analyze the current level of endpoint security and the steps needed to improve protection and operational efficiency by developing a roadmap to increased endpoint maturity. The roadmap helps assess the security posture and ensure key pieces of each maturity level are not missing from the organization's environment — especially prioritized project requirements to further maturity levels.

## Introduction

Cyberattacks have become more sophisticated, with threat actors using fileless attacks and identity theft to gain a foothold in the environment. However, not all organizations face the same level of business risk or start from the same baseline of endpoint protection. According to the 2021 Gartner Global Security and Risk Management Governance Survey, roughly half (48%) of the surveyed organizations struggle to find and hire cybersecurity professionals. [1]

Obsolete practices, like relying primarily on preventive controls, such as signature-based antivirus tools, have left many organizations vulnerable to attacks. Prevention alone is not enough. A step up to continual vulnerability assessment (VA), endpoint security tuning, and detection and response are needed to strengthen the endpoint security posture. These capabilities will require increased focus on the expertise, procedures and availability of internal staff to operate these tools.

Every successful attack causes one or several issues to the business, such as disruption and damage to the organization's reputation, financial loss, critical data loss and subsequent attacks. Regulatory issues may also occur if the data stolen contains information from customers, vendors or third parties.

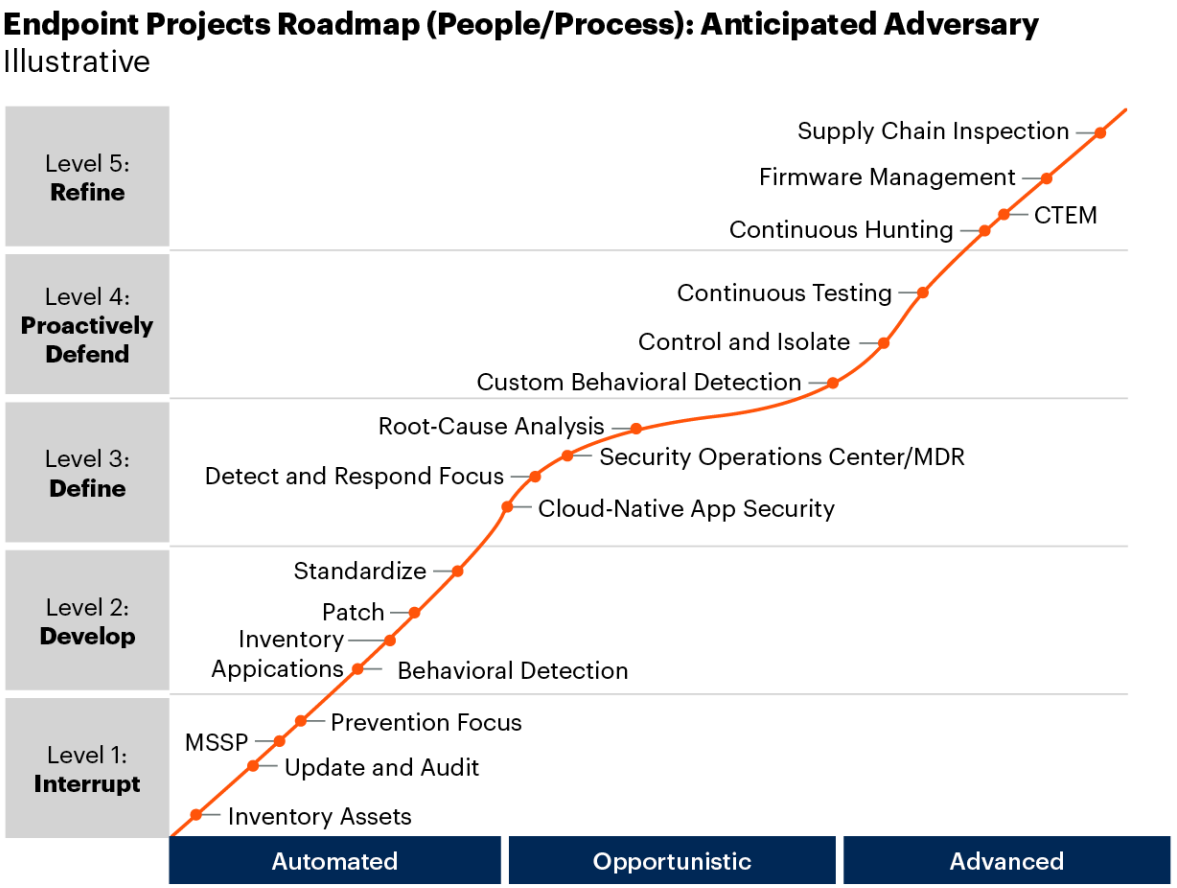
How can we improve endpoint protection to mitigate these attacks? This research describes the roadmap to enhance endpoint security using five security levels, each containing the respective projects designed to secure an organization against advanced cyberattacks. Accordingly, SRM leaders responsible for endpoint security must:

- Evaluate the risks to their organization.
- Assess the attacker's landscape.

- Develop a prioritized roadmap to achieve better protection and reduce the endpoint attack surface.

Figure 1 illustrates how to assess when a suggested project has the highest impact on security resilience.

Figure 1. Endpoint Project (People/Process) Roadmap: Anticipated Adversary




Source: Gartner
CTEM = continuous threat exposure management; MDR = managed detection and response; MSSP = managed security service provider
780242_C

Gartner

## Analysis

### Prerequisites for Maturity Assessment

Before determining the current endpoint protection maturity level and prioritizing the next steps, a few prerequisites need to be fulfilled. Examples include having an EDR solution in place, knowledge about the MITRE ATT&CK framework, and risk evaluation and assessment of the attacker landscape (see Note 1).

EDR capabilities are a prerequisite to enable behavioral-based attack detection. The MITRE ATT&CK framework provides an excellent overview of common attacker techniques and could be used to better understand the complexities of behavioral-based detection. [2] Although behavioral-based detection is more durable than lower-layer attempts to spot specific malicious code, it has a higher false-positive rate and will need an experienced operator to determine the intent. Overall, SRM leaders should evaluate risks and assess the attacker landscape. Doing so would help determine the current risk level, the acceptable risk appetite, the next steps required to mitigate the non acceptable risks and identify the next priority projects.

### Evaluate the Risks

SRM leaders must define the risk to the business while deciding the appropriate target level of endpoint security for their organization and the prioritized next-step projects. They should use the Ignition Guide to Conducting an Enterprise Risk Assessment to establish a business-oriented decision framework that defines the risk acceptance criteria, critical risks, and residual risks and identifies a starting point to measure the progress.

Additionally, to further evaluate the risks to their organizations, SRM leaders must create and maintain a risk register to provide a high-level overview of IT-related risks from a business perspective (see Toolkit: Document Your Cyber and IT Risks in a Risk Register).

### Assess the Attacker's Landscape

Each anticipated attack type and attacker profile must be scored based on the impact and likelihood of the attack. Then, SRM leaders should negotiate with business leaders on an appropriate level of security and residual risk. Attackers generally come in three varieties:

- The automated attacker has a reliable automated attack methodology to infect as many victims as possible. Typically, a vulnerability exploit or effective social engineering attack. These attackers may change tradecraft as mitigations become mainstream. However, their business model does not include zero-day or manual attack tradecraft. WannaCry ransomware is a good example of an automated attack. Other recent examples include EvilProxy and ransomware as a service (RaaS). [3]

- The opportunistic, persistent attacker uses new and off-the-shelf attack techniques to find victims. This type of attacker typically scans their victim's infrastructure for known vulnerabilities but uses a wide variety of tradecraft to move laterally and exploit the victim. This level of an attacker will grow with increased use of automated tools for exploitation and will likely expand targets to popular business process software. SamSam ransomware is a good example.
- The advanced persistent attacker has a specific goal and will use any method to achieve their aim. Advanced attackers will use simple tradecraft where possible but often combine this with exhaustively researched zero-day tactics, provided the goal is profitable enough. These types of attackers often prioritize remaining undetected threats for an extended period of time. Nation-state attacks, such as the attack on the Texas-based company SolarWinds, are a good example. [4]

When prioritizing endpoint protection projects, SRM leaders must consider the primary attack tradecraft. While there is a vast amount of malicious code and techniques, most can be boiled down to:

- Phishing
- Identity attacks — that is, stealing credentials.
- Software- and hardware-based supply-chain attacks. [5]
- Ransomware attacks.

Some trending attacks from 2022 include BEC, social engineering and MFA fatigue. [6,7] Ransomware attacks have also shifted from data encryption to double or triple extortion, data exfiltration and data corruption. [8,9,10,11,12]

Despite continued investments in cybersecurity, the threat landscape remains challenging — with digital business transformations, hybrid workforces and workplaces and interconnected digital supply chains expanding the attack surface. For more information, see How to Respond to the 2022 Cyberthreat Landscape.

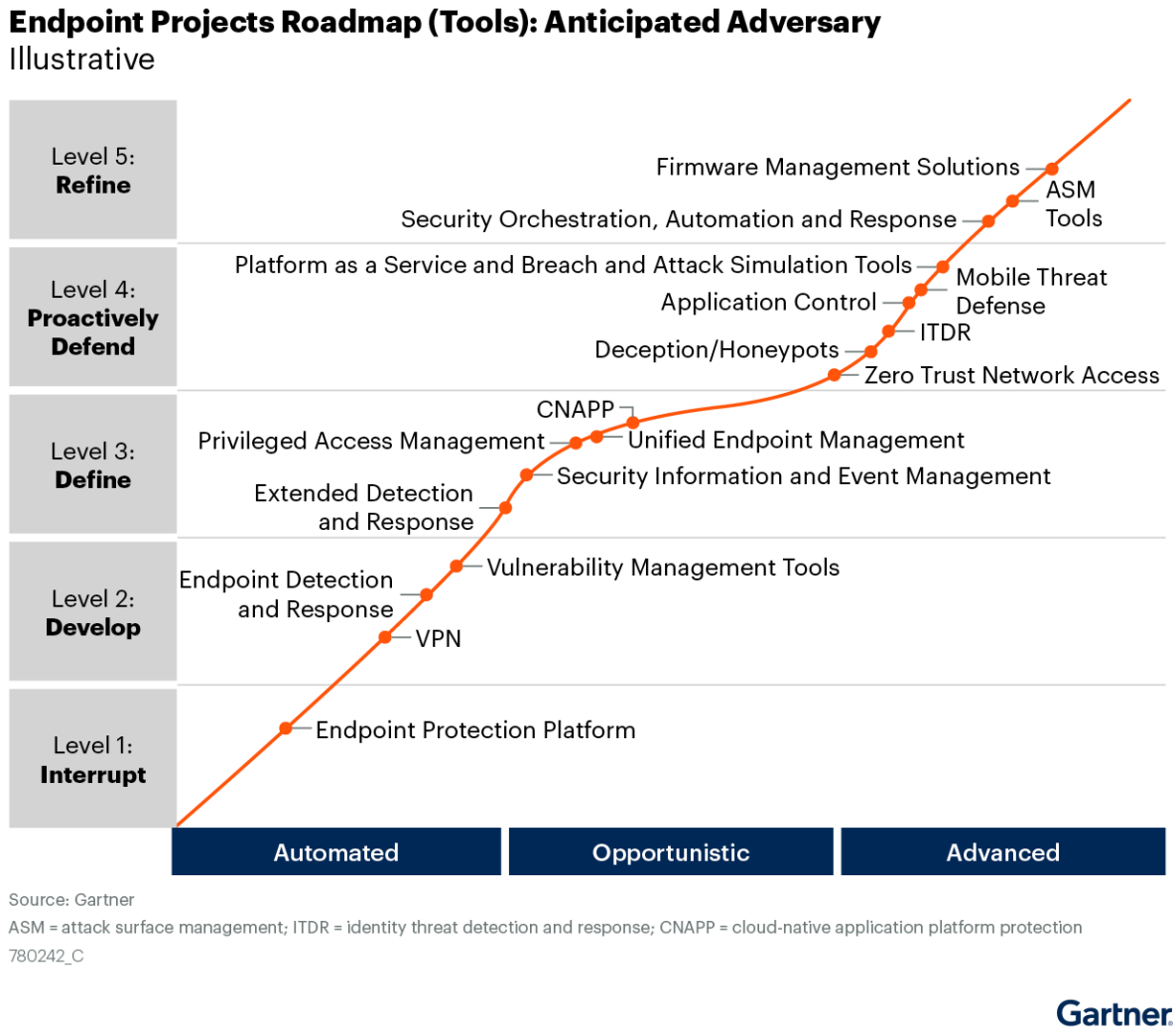
## Develop a Roadmap to Increased Endpoint Maturity

To address the modern threat landscape, SRM leaders should identify their current maturity level of endpoint security and prioritize projects for advancements. Some of these projects rely on tools implemented outside the endpoint context. Still, they can help reduce the overall endpoint attack surface and improve threat detection and response (TDR) capabilities (see Figure 2). However, not every process or program requires a specific tool or technology mapped to it. The people with the correct skill set, process or plan in place can achieve it.

SRM leaders responsible for endpoint and infrastructure security should prioritize the projects across the five maturity levels described in this research. Not all organizations will, or should, implement all the protection projects listed to achieve the highest level of endpoint security for their organization. Organizations must weigh the risks against the cost and inform the management of the achievable security level and the potential risks that may not be addressed, given the resources allocated. Then, the C-suite leaders can decide and communicate the acceptable risk appetite.

A second key consideration is that organizations at lower levels of sophistication may have to accept that they need to become more secure despite broken processes and a lack of fundamentals and staff. Managed security services can provide a fast track to improve operational security, allowing more focus on strategic priorities. However, organizations that expect to defend against advanced attackers should certainly strive for endpoint protection Level 5.

Figure 2. Endpoint Project (Tools) Roadmap: Anticipated Adversary




Source: Gartner
ASM = attack surface management; ITDR = identity threat detection and response; CNAPP = cloud-native application platform protection
780242_C

Gartner

### Endpoint Protection Level 1: Interrupt

The primary focus at this level should be on investing in people and processes. SRM leaders should start a conversation with business stakeholders about the type of threats that are reasonable to expect. Also, they should determine which corporate resources are the most critical to achieving business goals. SRM leaders should establish an end goal, a timetable and a budget to reach the desired endpoint protection level. Then, they should prioritize getting an inventory of assets and resources.

#### Projects at Level 1

- **Inventory endpoints:** Ensure that there is an accurate and updated inventory of all devices that connect to the network. This includes security controls in place and patch and configuration levels.

- **Inventory- and audit-existing security tools:** Many organizations at maturity Level 1 have outdated versions of security products. SRM leaders should start upgrading these tools up to the latest, stable version. Also, they should ask vendors for assistance in auditing the configuration. Examples of some commonly existing security tools include endpoint protection platform (EPP), secure email gateway (SEG) and secure web gateway (SWG).
- **Common configuration policy for endpoints:** Use the Microsoft Security Compliance Toolkit to assess the configuration policy to reduce configuration drift
- **Endpoint protection platform (EPP):** Considering that the state of patch configuration and vulnerability management (VM) is likely low at this level, it is important to invest in an EPP solution at this stage (see Solution Criteria for Endpoint Protection Platforms and Magic Quadrant for Endpoint Protection Platforms).
- **Outsource:** If increasing staff levels and staff skills is unlikely in the near term, opt for outsourcing SecOps and system management to managed security service providers (MSSPs). For more information, see Market Guide for Managed Security Services.
- **Migrate to platform vendors:** Companies with constrained security budgets and limited human resources should consider providers that have multiple solutions with integrated management.
- **Cloud-first deployment strategy:** Favor cloud-deployed solutions to reduce management burden and provide faster deployments (see Top Trends in Cybersecurity 2022).
- **Security awareness training:** Conduct security awareness training programs to educate employees and improve security behaviors. These programs should include phishing awareness and computer-based training. Also, programs that capitalize on vendor platforms can enable and augment the execution of a multichannel, context-specific and employee-centric approach (see Innovation Insight on Security Behavior and Culture Program Capabilities).

### Endpoint Protection Level 2: Develop

At Level 2, the organization should define its requirements, take inventory and develop an analysis and a plan to close gaps. SRM leaders should focus on getting application- and authentication-level inventory. The focus at Level 2 should expand in order to improve application-level network security, and backup and recovery.

Projects at Level 2

- **Application inventory and consolidation:** Begin by listing all executable programs. Then, determine providence and business value. Finally, consolidate applications and their versions.
- **Endpoint detection and response (EDR):** Implement an EDR solution as the primary tool for IR (see Gartner Fast Answer: What should I know about Endpoint Detection and Response?).
- **Vulnerability and patch management:** Reduce remediation exhaustion by integrating automated patch management solutions and the built-in patch management of vulnerability scanning tools. To improve the organization's security posture and resolve underlying processes, use VM metrics, such as automated patching (see The Top 5 Elements of Effective Vulnerability Management). Refer to the Market Guide for Vulnerability Assessment for details on the crucial technology elements for a successful VM program.
- **Phishing protection:** Invest in advanced phishing protection. Focus on solutions that mitigate identity-takeover attacks and business email compromise (BEC). For more information, see Market Guide for Email Security.
- **Cloud-secure web gateway (SWG):** On-premises SWGs should be replaced or augmented with cloud-delivered SWG. Doing so can expand protection to roaming workers and small offices (see Using Secure Web Gateway Technologies to Protect Users and Endpoints). Alternatively, replace the existing SWG with a security service edge (SSE). SSE is the convergence of cloud access security brokers (CASB) and SWG technologies. Doing so secures access to the web, cloud services and private applications (see Magic Quadrant for Security Service Edge).
- **Remote access solutions:** To secure the remote environment and protect the data in transit, properly-configured VPNs can be deployed according to zero-trust principles. Also, always-on VPNs that require device and user authentication provide similar protection to the zero trust network access (ZTNA) model. Currently, the leading VPN providers are enhancing their offerings to include similar options to ZTNA (see Remote Access Options for Enterprise Endpoints).

- **Retire end-of-life (EOL) operating systems:** Quantify EOL options by combining financial and other business-outcome variables using decision tools for monthly recurring revenue (MRR) decisions, such as Gartner's Toolkit (see Toolkit: Maintain, Refresh or Retire? How to Deal With Products at the End of Life). Also, update Windows OS to Windows 10 or 11 to reduce complexity and risk and improve digital-workplace maturity (see Toolkit: Maintain, Refresh or Retire? How to Deal With Products at the End of Life and How to Maximize the Benefits of Windows Modern Management).

- **Backup and recovery:** A solid endpoint-backup strategy is critical to prevent threats, such as ransomware (see Magic Quadrant for Enterprise Backup and Recovery Software Solutions). Ransomware is the biggest threat to most organizations. Its attack tactics have evolved to double or triple extortion, data exfiltration and data corruption — as the traditional encryption process is comparatively slower than these modern attack tactics.

### Endpoint Protection Level 3: Define

At Level 3, organizations should have most of the requisite tools, such as EPP, EDR, SEG and SWG. However, they should continue to improve processes and establish a formal security operations center (SOC) for IR. At this level, the reporting and tracking of performance begins to be addressed. To prevent more opportunistic attacks, SRM leaders should expand their focus from malware prevention to detection and response. Also, root cause analysis and the proactive hardening of endpoints become more important at this level.

### Projects at Level 3

- **Security operations (SecOps):** This planning measure helps to deal with alerts and incidents. Establish roles and responsibilities and start to work on IR handling guidelines (see Security Operations Primer for 2023). Clients wishing to learn more about this planning consideration should investigate solutions such as extended detection and response (XDR), threat detection, investigation and response (TDIR), managed detection and response (MDR) or co-managed security information and event management (SIEM). For more information, see 2023 Planning Guide for Security.

- **Extended detection and response (XDR):** Before implementing an XDR solution, SRM leaders should assess if the organization would benefit from the XDR (see Is Security Operations Ready for XDR?). Enhance the EDR capabilities by adding it to an XDR platform. Doing so provides a faster and more common detection, alert management and accurate IR capability across multiple security products (see Market Guide for Extended Detection and Response).

- **Integration with sandbox:** Consider integrating an automatic and on-demand sandboxing service to your EPP and EDR to test to perform in-depth dynamic analysis of unclassified files.

- **Strengthen your security team:** Ensure that the security team has enough staff and the necessary skills to run the operations. Less mature organizations lacking 24/7 SOC coverage, resources and expertise should seek fully managed offerings. Alternatively, if organizations are looking to improve the skills of internal staff, IR solutions can help staff interpret results and respond to alerts. If the staff is not experienced or trained in advanced threat hunting and analytics, consider outsourcing the required skill set from an MDR vendor (see Market Guide for Managed Detection and Response Services). Still, organizations should prioritize training the internal staff.

- **Expand the scope of vulnerability and patch management:** Use advanced prioritization methods that consider the probability of exploitation and the importance of affected systems to expand vulnerability and patch management programs (see A Guidance Framework for Developing and Implementing Vulnerability Management).

- **Incorporate a system for privileged credential life cycle management:** Develop an inventory and establish a process for privileged credential life cycle management and monitor privileged credential usage. Whenever appropriate and possible, remove administrator rights from users (see Guidance for Privileged Access Management and 5 Interlocking Strategies for a Successful PAM Implementation).

- **Multifactor authentication (MFA):** A MFA can be used for privileged accounts and critical business systems (see Market Guide for User Authentication).

- **Bring-your-own-device (BYOD) program:** Start to review the usage of employee-owned laptops and critical business systems. Capitalize on MFA to protect corporate applications. Provide employees with corporate-issued endpoint protection solutions and use network access control (NAC) to enforce usage. Determine when and where the BYOD program makes sense, analyze how to manage it and evaluate what to expect from its application (see How to 'COPE' With BYOD in 2022).

- **Cloud workload protection:** Enterprises should disaggregate the workspace and workload to successfully implement cloud-native application security. The former includes PCs and mobile OS, and the latter includes servers and security programs in cloud infrastructure as a service (IaaS). Cloud-workload security programs should use an integrated platform approach of cloud-native application platform protection (CNAPP). Doing so ensures that the development and deployment of cloud-native applications correspond to the DevSecOps approach (see Market Guide for Cloud-Native Application Protection Platforms).

- **Unified endpoint management (UEM):** An UEM solution should be implemented for agent and agentless management of computers and mobile devices through a single console (see Magic Quadrant for Unified Endpoint Management Tools).

- **Asset discovery of Internet of Things (IoT) and operational technology (OT) devices:** Implement asset discovery of IoT devices beyond Windows, Linux and macOS.

### Endpoint Protection Level 4: Proactively Defend

At Level 4, SRM leaders should expand their scope and focus on all network-connected devices by adopting techniques designed to reduce the attack surface for the IoT and out-of-support OS. During this level, detection activity moves up to the device and user behavioral level.

SRM leaders should implement identity threat detection and response (ITDR) and SIEM solutions for more extensive, custom behavioral detection capabilities and threat analytics. To reduce the attack surface, ramp up the use of default-deny controls, such as applications safelisting, network segmentation and web isolation. Adopt a continuous penetration testing mentality. Also, consider advanced tools such as deception and moving target defense.

### Projects at Level 4

- **IoT and OT multifunctional security platforms:** List what OT security solutions are currently being used in the organization and evaluate the growing list of solutions on the market for the best fit. Include all cyber-physical systems (CPS) — for example, OT, IoT, industrial IoT (IIoT) and Internet of Medical Things (IoMT) — and IT in a joint governance model (see Market Guide for Operational Technology Security).

- **Moving target defense:** Implement moving target defense technology to deflect highly invasive attacks. These tools can be integrated into the network, host and software security solutions and are important for organizations shifting to hybrid and remote workforces. For more information, see Emerging Technology: Critical Insights on Moving Target Defense for Application Security.

- **Identity threat detection and response (ITDR):** Implement ITDR on identity systems for custom behavior detection. Also, ITDR should be used to detect identity-based threats that escape conventional identity and access management (IAM) and preventive controls (see Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response). Automated and opportunistic attackers have now moved up the stack to the authentication layer, attempting more account takeover attacks through social engineering. ITDR will increasingly be used to detect account takeover attacks by spotting abnormal behavior of devices and user accounts.

- **Security information and event management (SIEM):** Most organizations at Level 4 have a SIEM but have not maximized its use. XDR solutions can replace common functions of SIEM with better out-of-the-box integration and workspace IR. However, large enterprises will still consider SIEM solutions to integrate global systems and applications (see Magic Quadrant for Security Information and Event Management).

- **Red team and blue team exercises:** Move from one-time penetration testing to active TDR exercises and continuous testing. The primary goal should be to test detection and response and assess if a specific scenario could happen to the organization, how far a threat would go and how the organization can handle it when it happens. Use breach and attack simulation (BAS) tools to assess what would happen if an exploit occurs and how the security controls would perform (see Using Security Testing to Grow and Evolve Your Security Operations).

- **Threat-hunting exercises:** Conduct threat-hunting exercises to detect potential unknown threats.

- **Application control:** Application control can be deployed for all unpatchable systems and internet-facing servers. Consider application control for critical business users or devices — that is, point of service (POS).

- **Script usage control:** Restrict and monitor script usage. PowerShell has a number of features to make it easier to monitor and control script usage. Modern EDR solutions can monitor malicious scripts, and some application control solutions can automatically restrict PowerShell to commonly used functions.

- **Isolation:** Deploy a ZTNA solution on your web applications to create an individualized "virtual perimeter" that encompasses the user, the device and the application. ZTNA offers a more isolated and resilient environment with better monitoring and removes the need to expose applications directly to the internet (see Market Guide for Zero Trust Network Access).

- **Microsegmentation:** Use microsegmentation to limit the assets an endpoint can interact with on the LAN. The goal is to isolate endpoints to specific network profiles, thus improving breach containment and strengthening regulatory compliance (see Emerging Tech: Adoption Growth Insights for Microsegmentation). Microsegmentation is particularly useful for isolating unpatchable servers, critical business process servers and IoT or OT devices.

- **Deception tools:** Consider implementing deception tools to detect active attackers (see Use Adversary-Generated Threat Intelligence to Improve Threat Detection and Response). Deception deploys highly-credible deceptive artifacts, such as credentials, files or applications. The first step is to deploy breadcrumbs — that is, clues that create a false trail to deceive attackers — onto the endpoint and trap attackers during the early stages of the cyber kill chain.

- **Mobile threat defense (MTD):** Implement MTD on mobile endpoints used by privileged users and high-value-target employees (see Guide to Endpoint Security Concepts).

### Endpoint Protection Level 5: Refine

This is the refinement stage. At Level 5, expanding activity will be focused on inspecting the supply chain for downstream attacks and cyber offenses happening lower into the computing stack, such as firmware attacks.

#### Projects at Level 5

- **Supply chain inspection:** Focus on equipment manufacturers and application supply chain. Consider geopolitical component risks, as they may impact the cyberthreat landscape. Accordingly, cyber warfare often crosses geographical borders. For example, conflicts between countries can lead to coordinated cyberattacks, thus impacting organizations located in the affected countries and worldwide businesses. [13] For more information, see Top Trends in Cybersecurity 2022.

- **Firmware management:** Start by listing, monitoring and patching firmware and microcontrollers.

- **Continuous threat hunting:** Skilled and experienced SOC analysts use event data from SIEM, endpoints, network devices and application logs to identify suspicious or malicious activity that has bypassed automated controls. Once discovered, the new indicators of attack (IoA) and indicators of compromise (IoC) are added to the prevention layer, forming a closed-loop prevention, detection and response practice.
- **Continuous threat exposure management (CTEM):** Establish regular, repeatable cycles for your CTEM program. Each cycle should adhere to a five steps process — scoping, discovery, prioritization, validation and mobilization — to guarantee consistent threat exposure management (see Implement a Continuous Threat Exposure Management (CTEM) Program).
- **Orchestration and automation:** Implement a security orchestration, automation and response (SOAR) solution that combines IR, orchestration and automation, and threat intelligence platform management capabilities in a single solution. Start by automating repetitive security tasks (see Market Guide for Security Orchestration, Automation and Response Solutions).

## Evidence

[1] **The 2021 Gartner Global Security and Risk Management Governance Survey** was conducted from April through May 2019 to better understand how risk management planning, operations, budgeting and buying are performed, especially in the following areas:

- IT risk management
- Cybersecurity program management
- Business continuity management
- Privacy Cyberphysical system security

The research was conducted online among 615 respondents across North America, EMEA, Asia/Pacific and Latin America regions. Qualifying organizations have at least 100 employees and $50 million in total annual revenue for fiscal 2020. All industry segments qualified except agriculture, IT services, and software and IT hardware manufacturing. Further, each of the five technology-focused sections of the questionnaire required the respondents to have certain job roles and categories and have at least some involvement or responsibility with at least one of the technology domains we explored. Interviews were conducted online.

The survey was developed collaboratively by a team of Gartner analysts and Gartner's Research Data, Analytics and Tools team.

*Disclaimer: Results of this survey do not represent global findings or the market as a whole but reflect the sentiments of the respondents and companies surveyed.*

[2] ATT&CK, MITRE | ATT&CK.

[3] EvilProxy Commodifies Reverse-Proxy Tactic for Phishing, Bypassing 2FA, Dark Reading.

[4] Nearly 3 Years Later, SolarWinds CISO Shares 3 Lessons From the Infamous Attack, Dark Reading.

[5] Worldwide Software Supply Chain Attacks Tracker (Updated Daily), Comparitech.

[6] Lessons Learned from the Marriott Hack of 2022, ThreatBlockr.

[7] Uber Data Breach 2022: What You Need to Know, Appknox.

[8] What Is Double Extortion Ransomware?, Zscaler.

[9] Triple Extortion Ransomware: A New Trend Among Cybercriminals, Heimdal.

[10] LockBit Ransomware Gang Gets Aggressive With Triple-Extortion Tactic, BleepingComputer.

[11] Ransoms Without Ransomware, Data Corruption and Other New Tactics in Cyber Extortion, SentinelOne.

[12] Ransomware Data Theft Tool May Show a Shift in Extortion Tactics, BleepingComputer.

[13] How Geopolitics Impacts the Cyber-Threat Landscape, Gartner.

## Note 1: Definition of MITRE ATT&CK Framework

MITRE ATT&CK defines its framework as follows:

*"MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."*

For more information, see the MITRE ATT&CK webpage.

## Document Revision History

Roadmap for Improving Endpoint Security - 19 June 2018

## Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

IT Score for Security and Risk Management

Top Trends in Cybersecurity 2022

Magic Quadrant for Endpoint Protection Platforms