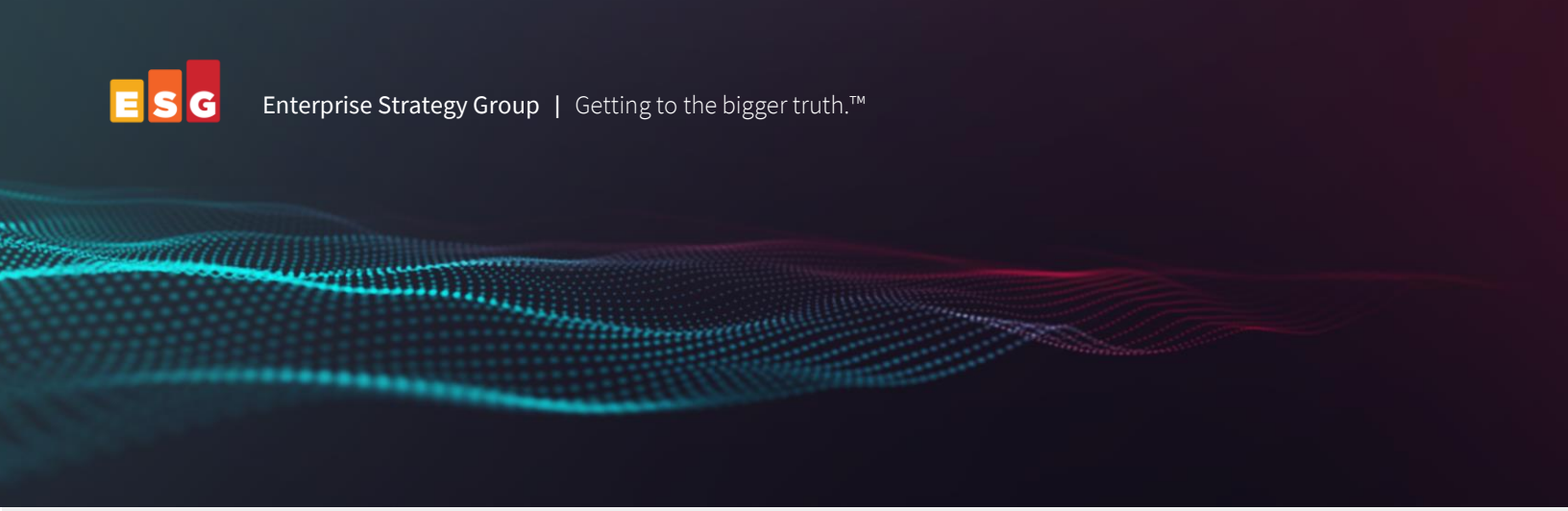


ESG WHITE PAPER

The Need for Speed: Second Generation EDR

Accelerating Detection and Response

By Dave Gruber, ESG Senior Analyst

May 2020

This ESG White Paper was commissioned by Fortinet and is distributed under license from ESG.

Contents

Overview

Endpoint security plays an integral role in modern security architecture. While initially focused on protecting individual endpoints from malware and other known threats, modern endpoint security solutions have grown to utilize multiple detection techniques capable of preventing or detecting both known and unknown threats while helping security and IT teams respond to broader threats involving multiple endpoints.

But even with the use of advanced machine learning and behavioral analytics, endpoint security solutions still are not able to prevent 100% of threats. This leaves a gap for security teams, who need a mechanism to detect and respond to threats that make it through preventative controls. Security teams have rallied around endpoint detection and response tools (EDR) as the primary mechanism to address this gap. According to recent ESG research, EDR was the most often cited priority when organizations were asked what their biggest endpoint security investment priorities are for the next 12-18 months.[1]

EDR solutions have evolved dramatically since first entering the security scene almost 8 years ago. While first created as a digital forensics investigation tool for only the most expert of security professionals, modern EDR solutions are highly automated and can be utilized by most security analysts to effectively close the gap where prevention solutions fall short.

Second generation EDR offers multiple advantages for security teams, including reduced alerts, accelerated threat understanding, and playbook-driven automated response actions. These second generation EDR solutions strengthen prevention, reduce the noise, speed response, and enable more security analysts to redirect their efforts to stopping the most sophisticated threats.

These important advancements in EDR are enabling security teams to more rapidly close the gap left by endpoint protection solutions, keep up with the adversary, and stop threats before damage occurs—all while reducing stress on the security analyst.

The Evolution of EDR

First Generation EDR

Endpoint detection and response solutions were initially developed to enable skilled security analysts to more easily investigate incidents. By capturing historical endpoint telemetry, analysts could "roll back the tape" to see what was happening as attacks unfolded.

First Generation EDR Tools

First generation EDR solutions were crude tools used for incident investigation by highly skilled analysts who needed to execute manual queries to look for specific indicators of compromise.

While effective, first generation EDR solutions were crude tools used for incident investigation, typically by highly skilled analysts who needed to execute manual queries to search for specific indicators of compromise.

While providing centralized access to endpoint telemetry, first generation EDR solutions were crude tools requiring significant manual attention to investigate and ultimately remediate threats. Organizations struggled to find enough skilled analysts to operate these tools effectively.

[1] Source: ESG Master Survey Results, *Trends in Endpoint Security*, March 2020. All ESG research references in this white paper have been taken from this master survey results set.

EDR V1.1 – Adding Threat Intelligence

To ease the manual query process, EDR solutions added an automated comparison of endpoint telemetry to indicators of compromise (IOCs) from threat intelligence sources to speed the identification of suspicious or malicious activities. This important addition spawned new use cases for EDR, including the ability to proactively look for attacks in progress, but still typically required highly skilled resources to complete investigations.

EDR V1.2 – The Addition of Remediation Tools

The desire to remediate from within the same tool spawned the addition of native response capabilities, allowing analysts to request additional data from endpoints, ban processes, isolate endpoints, block specific IPs, and more. This important advancement enabled security analysts to access and remediate endpoints without involving IT resources, eliminating a key friction point for timely remediation.

EDR V1.3 – New Use Cases

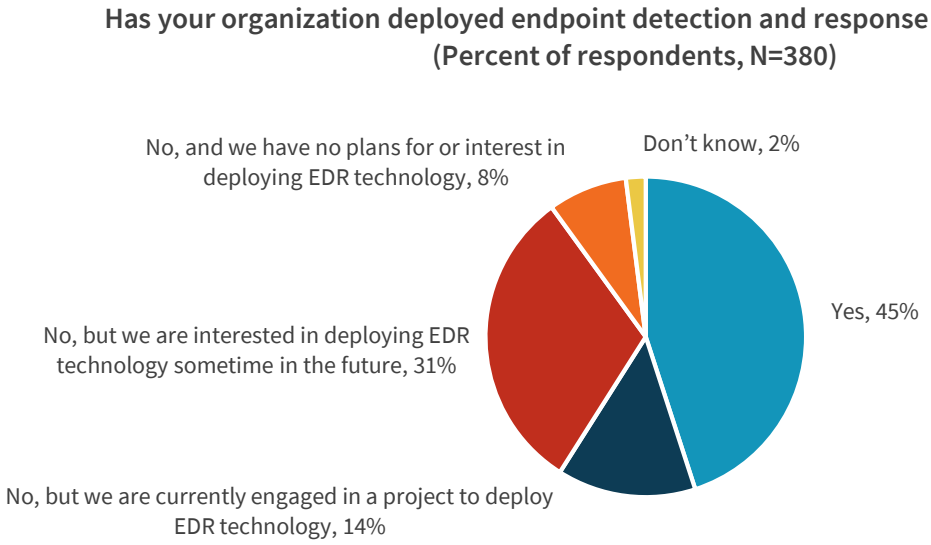
Security analysts saw an opportunity to apply EDR tools to the investigation of attacks currently underway, enabling them to both stop attacks in progress and proactively hunt for hidden adversaries dwelling within the infrastructure. This "active" use of EDR uncovered new threats previously undetected.

Closing the Efficacy Gap

Even with the application of machine learning, big data, and behavioral analytics, endpoint protection solutions are unable to stop 100% of threats. Accepting this outcome, the security community has adopted a "prevent what you can, detect and respond to what you can't stop" approach to endpoint security.

While a majority of organizations continue to use a "prevention-first" approach to endpoint security, EDR solutions have become a widely accepted approach to close this gap. When asked about EDR usage in a recent ESG survey, more than half report already having the technology deployed (45%) or are currently in the process of doing so (14%) (see Figure 1). And more than one-third of respondents who have recently switched—or plan to switch—endpoint vendors attribute this change to the need for improved threat detection and response capabilities.

Figure 1. EDR Is Becoming Mainstream

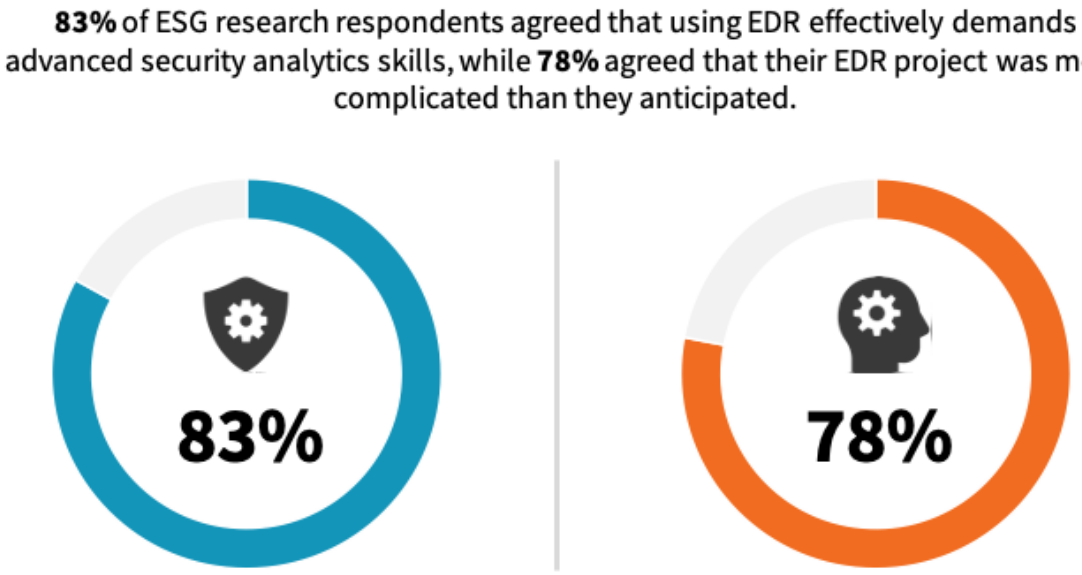


Source: Enterprise Strategy Group

Limitations: Where First Generation EDR Solutions Break Down

While the use of first generation EDR tools has become commonplace within mature, well-staffed SOC teams, the acute shortage of skilled security resources has limited many organizations from realizing the value of these tools. 83% of ESG research respondents agreed that using EDR effectively demands advanced security analytics skills, while 78% agreed that their EDR project was more complicated than they anticipated.[2]

Figure 2. EDR Is Not Without Its Challenges



Source: Enterprise Strategy Group

First generation EDR is well suited for responding to data breach investigations but is often too slow for fast moving threats where real-time response is required. Ransomware can inflict damages in seconds. Few can afford the 24-hour window between detection and containment for today's rapid attacks. Because first generation EDR solutions have limited integration with prevention controls, security analysts are left with the burden of manually configuring other security controls to shut down current and stop future attacks.

Further, first generation EDR solutions often overwhelm security teams with alerts, making alert triage and investigations difficult and time consuming, while driving up program costs. Security analysts are in a race against time, sifting through alerts to find attacks in progress—hoping to act before damage occurs. This adds tremendous stress for many analysts, often leading to burnout.

Managed Detection and Response

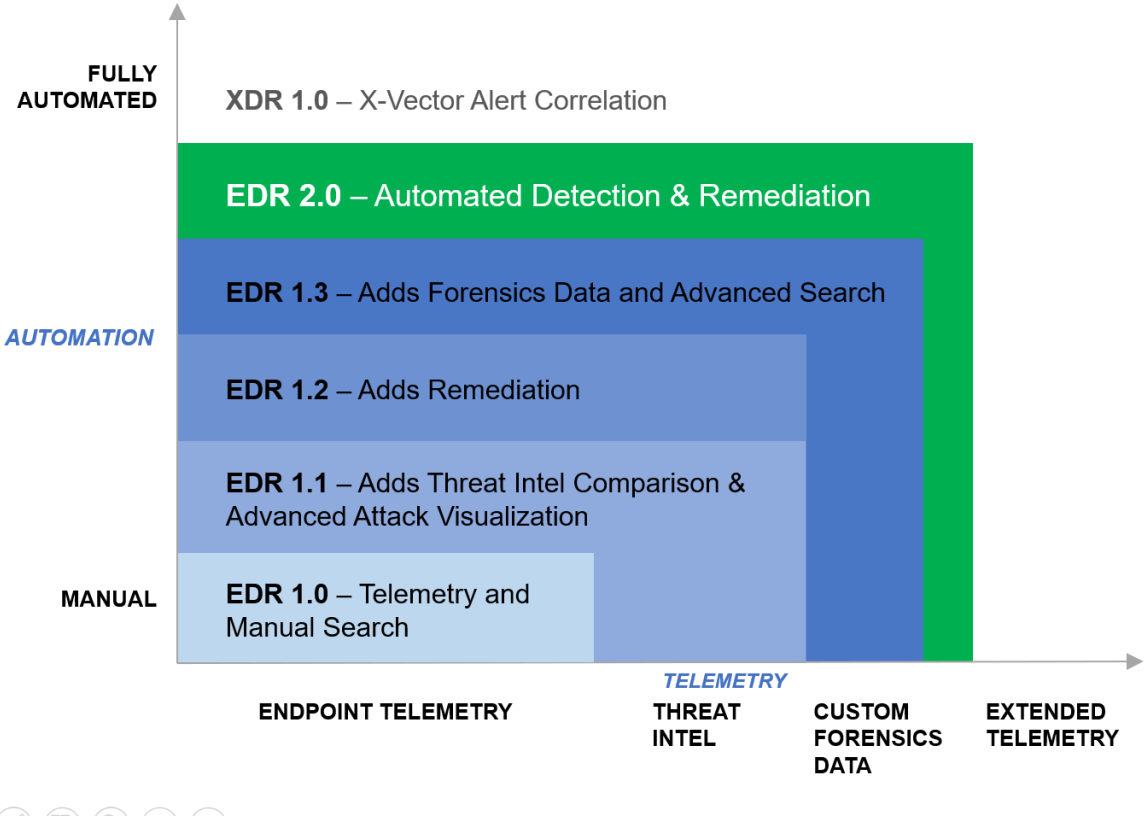
MDR services can supplement teams with skill deficits or provide additional 7x24 coverage. Services extend from simple alert triage to full investigation and response.

Even as automated response actions are added, such as process termination or full endpoint isolation, this "blunt" response containment approach can often disrupt business operations. False positives can intensify this issue.

[2] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

To assist with overcoming these challenges, many companies are subscribing to managed detection and response (MDR) services, most of which only perform basic alert triage through email-based communications. This approach is often too slow and typically returns the burden of response back to local security analysts.

Figure 3. The Evolution of EDR



Source: Enterprise Strategy Group

Second Generation EDR (EDR 2.0) : Fast, Effective EDR for All

Improving the speed and efficacy of detection and response programs requires a careful balance of visibility, investigative analysis, and automated actions based on a comprehensive understanding of an attack.

Second generation EDR solutions are more tightly integrated with prevention controls, working together to block malicious or suspicious activities in real time. When EDR solutions can automatically and selectively mitigate threats quickly, security teams can stop damage while having the tools and time they need to fully investigate, minimizing business disruption.

Minimal Business Disruption

When EDR solutions can automatically and selectively mitigate threats quickly, organizations can continue operations with minimal business disruption.

Second generation EDR solutions add policy-driven, automated risk mitigation control, employing behavior-based detection to identify suspicious or malicious activity, which can trigger automatic, real-time blocking to prevent attackers from achieving their goals of data exfiltration, encryption, or lateral movement to other valuable assets. These solutions are often able to disarm an attack without interrupting normal business operations by selectively blocking outbound communications or file system access, without the need for full system isolation or full process termination.

Utilizing automated, customizable playbooks, remediation can happen both immediately and automatically, stopping attacks before they can advance within the infrastructure.

Threat Classification

Continuous threat classification helps second generation EDR solutions prioritize actions, while helping security analysts focus on high risk incidents. Leveraging cloud-driven big data analytics and artificial intelligence (AI), these solutions can enhance a weak endpoint signal by utilizing extended analysis and adding threat intelligence from a broad collection of attack signals. Threats can be reclassified at any time, triggering automated response actions. This continuous threat classification process stops escalating threats as adversaries advance their attack strategies.

Classifying an incident as malicious, suspicious, inconclusive, or likely safe creates a triage model for both automated and manual intervention. Based on initial classification, organizations can leverage predefined, customizable playbooks to automate high fidelity response to common threats, alleviating analysts from spending time on more mundane tasks. Playbooks can be customized based on an organization's risk tolerance, specific attack targets (endpoint groups), and threat category.

Through continuous enrichment, analysis, and classification of attack characteristics, these automated response actions improve progressively over time, increasing the volume of incidents handled automatically. Over time, as the analyst resources free up, time can be redirected to higher value tasks, including furthering the development of additional incident response processes and automation and other proactive tasks/strategies. This relieves strain on security analysts, limits business disruption, and ultimately strengthens security posture.

New Sources of Telemetry Bring Additional Clarity

As EDR solutions mature, new detection and response solutions known as XDR are emerging, bringing together telemetry from endpoint, network, cloud, and email. XDR solutions continue to support investigations and automated response but bring additional clarity as adversaries utilize more complex attack techniques involving multiple threat vectors. XDR solutions can simplify the security stack while improving the mean time to detection and response.

Security Orchestration, Automation, and Response

Many organizations have implemented specific security orchestration, automation, and response (SOAR) solutions to automate and orchestrate response. However, moving response closer to core controls enables real-time response, limiting damage and business disruption. For example, in a manufacturing OT environment, most would prioritize uptime, preferring to disarm and remediate threats without taking a system offline. In this critical systems environment, second generation EDR solutions can provide automated response with minimal to no service disruption while allowing security analysts to investigate. Similarly, in a retail environment, a POS device can be isolated with a confirmed infection, supporting PCI compliance regulations. Second generation EDR solutions aren't intended to replace SOAR solutions, but instead augment them with more responsive defenses.

The Bigger Truth

Today's diverse threat landscape will continue to challenge industry-leading endpoint security solutions to prevent every attack, leaving organizations with the task of closing this gap with a combination of humans and automated threat detection and response tools.

Endpoint detection and response tools have come a long way since their initial introduction. Advancements in EDR solutions are enabling security teams to implement proactive risk mitigation strategies, leveraging second generation EDR

solitions to reduce excessive noise levels, automate and speed response, and enable security professionals to quickly investigate and stop attacks.

Second generation EDR sets the stage for new levels of automated detection and response, resulting in a more resiliant, self-healing environment where security analysts can refocus their time on mitigating the most important, sophisticated threats. 34% of surveyed IT professionals who recently switched endpoint security vendors or plan to switch cited *the need for better threat detection and response* as one of the drivers of the switch.

With the addition of these advanced automation capabilities, second generation EDR solutions should enable organizations to detect and respond faster, stop more threats, and do so more efficiently, requiring less effort from highly skilled security analysts. And when events require a security analyst's attention, threats can be disarmed while investigations take place, limiting business disruption.

Organizations that are investing in EDR should strongly consider second generation solutions that include more automated detection, response, and remediation capabilities that can accelerate response, ensure endpoint resiliance, and enable existing security teams to keep up with the modern endpoint threat landscape.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188