FORTINET

Top 9 Considerations for Evaluating Endpoint Detection and Response Solutions

Table of Contents

Executive Overview

Endpoint protection platforms (EPP) range from the original antivirus solutions of yesteryear to extended detection and response (XDR) platforms that tie multiple security solutions together. As the need arises for endpoint security solutions, vendors will attempt to match buyer expectations and analyst terms through their messaging but not their engineering.

This ebook discusses nine criteria for informed endpoint security purchasers to consider when evaluating a change or supplement to their endpoint security strategy.

On average, it takes over 21 days to detect a breach—a timeline that gives attackers ample opportunity to move laterally within networks and inflict greater damage.[1]

Introduction

Selecting the right endpoint security solution has become increasingly challenging as threats evolve and organizations adapt to hybrid and remote work environments. Legacy tools, such as traditional antivirus platforms, no longer provide adequate protection against sophisticated attacks like fileless malware, advanced persistent threats, and ransomware. Businesses need security solutions that detect and block known threats and adapt to address emerging risks in real time.

Endpoint security platforms must now encompass more than just detection and response. A modern approach combines secure connectivity, proactive vulnerability management, and automation to rapidly protect against threats while minimizing the need for manual intervention. Organizations require solutions that can safeguard devices no matter where they are and ensure consistent protection across various operating systems and environments.

Below are the top nine considerations to help you navigate the complexities of selecting an endpoint security solution. Focusing on key areas such as protection efficacy, secure connectivity, and system compatibility provides the necessary framework to make informed decisions that align with your organization’s needs.

Secure Connectivity

Securing connectivity is crucial in today's distributed work environment. When evaluating solutions, prioritize those that go beyond virtual private network (VPN) support with support for zero-trust network access (ZTNA) for securely connecting users via remote access to your corporate network.

While VPNs are reliable for securing data in transit, ZTNA offers a more advanced approach by continuously verifying users, devices, and applications before granting access, regardless of location. Unlike traditional perimeter-based security, ZTNA ensures that no entity is trusted by default, even after initial authentication. This ongoing verification process minimizes the risk of unauthorized access and lateral movement within the network, significantly enhancing security and minimizing the scope of an attack. Moreover, ZTNA provides granular control over access to specific resources, offering a more tailored and secure model. For organizations aiming to future-proof their security, ZTNA strengthens protection and simplifies compliance, user experience, and management across diverse environments.

Lateral movement remains a critical issue, with 54% of observed threat activities involving remote services enabling attackers to move laterally through networks once they gain initial access.[2]

Protection Efficacy

Now that organizations are embracing the hybrid workforce, you need to trust that the endpoint security solution you select will protect the endpoint no matter where it operates. It needs to protect against today's threats and those that will surface in the future. Organizations that haven't changed their security strategy in the past few years often still use older EPP or AV solutions that don't protect against the latest threat vectors, such as fileless attacks. Given that real-time protection is enabled through behavior-based anti-malware defense, you must start your search with a tool with EDR capabilities based on two initial criteria. First, see how an EDR solution reduces the attack surface, such as the ability to discover rogue devices, set virtual patching policies for vulnerable applications, and set application control policies. Second, see how the behavior-based anti-malware engine operates, ask if it works within the system's memory instead of just hooking in from the user space (see Agent Weight section below), and inquire whether it can safely monitor files for malicious changes and roll back damage. Knowing how each solution works will help you shortlist candidates for your EDR project.

Ransomware Defense and Recovery

Ransomware is the most destructive form of malware to date and one of the most attractive to attackers today, especially when targeting industries such as healthcare, financial services, energy, manufacturing, and government. The fourth round of the MITRE ATT&CK Evaluations is a good source to see how well a vendor's EDR client responds to ransomware and how the vendor responds to all forms of ransomware. Additionally, artificial intelligence (AI) and machine learning (ML) capabilities are vital to ransomware defense. Be sure to ask if it can defend against ransomware if the endpoint is offline, such as at home. Other considerations are around real-time ransomware rollback and the types of systems the client can perform the rollback task on, such as Windows, macOS, and Linux.

Anti-Tampering Capabilities

Selecting an endpoint security solution impervious to hacker manipulations—specifically, one that cannot be bypassed or turned off—is paramount to ensuring the continuous integrity and security of your organization's security infrastructure. In today's sophisticated threat landscape, attackers often employ documented evasion tactics to bypass or deactivate EPPs and other security solutions. Endpoint security tools, which serve as frontline defense mechanisms against these advanced threats, monitor and analyze endpoint activities in real time to detect suspicious behavior. If attackers, armed with evasion tactics, successfully circumvent these tools, they can move laterally within the network undetected and then manipulate, exfiltrate, or even destroy critical data.

Operating System Support

Are you considering connecting operational technology systems to the network? If so, they will need protection. Many run on older operating systems like Windows 7. Do you have legacy Windows servers or Linux in your environment like many manufacturing, energy, financial services, and educational organizations? Do you have executives or employees in departments like creative services using macOS? If the vendor or your managed security service provider does support these operating systems, ask if the licensing costs are the same for both servers and workstations and whether they can be managed from the same console. Also, see how much attack insight the solution provides for Windows and Linux using round five of the MITRE Engenuity ATT&CK Evaluations.[3] While some vendors will boast about their OS coverage model, ask if they have full EDR and XDR-like feature parity from their oldest to newest operating systems.

Lightweight Agents

One of the most compelling reasons to adopt endpoint security software that employs AI and ML is to reduce the reliance on signatures, which are very limited and typically compromise user experience. EDR solutions range in their impact on system resources. Consider only solutions that use less than 1% of CPU on average or less than 2% for critical servers. Clients that operate on the kernel level will perform better than those in the user space that hook into the kernel. This will also improve interoperability between solutions as well as visibility into code.

Automated Responses

This is where EDR excels, placing it light years beyond old AV and EPP platforms. Automation will take an overburdened security operations center team or IT staff from ignoring alerts to a team that focuses on fine-tuning an EDR solution to do the work for them so more time can be spent on activities like threat hunting. When evaluating solutions, ask about the granularity of the policy engine. Before adopting an XDR license, understand how it may integrate with other security and IT infrastructure.

XDR Capabilities

XDR is an approach that many security practitioners consider, and it is sure to be one of the largest-growing segments in cyber security. A mature XDR vendor should have an experienced security information and event management (SIEM) and security orchestration, automation, and response (SOAR) product line from which they can expand and grow. Look for a solution that interfaces with the provider's platform with native sensors versus one that is mainly composed of third-party sensors through APIs that some analysts would call either an "open" or "hybrid" XDR. An XDR solution built upon EDR may be the right tool to add the extended detection and remediation of threats beyond the endpoint with automated incident response.

Deployment and Managed Service Options

Security professionals often report feeling overburdened, so supplementing your team with a service to deploy the endpoint agents, manage alerts, and handle incident response is a huge help. Managed detection and response (MDR) services are recommended for all customers, especially in the first year, to help fine-tune the EDR technology in the environment.

Buyers frequently ask if the managed services team is internal to the vendor or outsourced to a third party. Global companies that work around the clock will also inquire if the vendor has support centers in their region. Because endpoint security has a relationship with the rest of your security ecosystem, working with a vendor that provides incident response services can be advantageous in case of a potential breach, given their experience working with all types of security technology.

Conclusion

Not all EPP vendors are the same. To discover what's best for your organization, ask critical questions about the capabilities of the various platforms available and how they protect endpoints no matter where they operate. Consider your timeline for moving to an XDR solution and see if your shortlisted vendors can help bridge that gap as you work toward full orchestration.

[1] Aviv Kaufmann, ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, August 1, 2023.

[2] 2H 2023 Threat Landscape Report: A Semiannual Report by FortiGuard Labs, Fortinet, May 2, 2024.

[3] ATT&CK Evaluations for Fortinet, MITRE Engenuity, accessed August 29, 2024.

FORTINET

www.fortinet.com

September 26, 2024 5:21 PM / 2839406-0-0-EN