CHECKLIST

Top Nine Criteria When Selecting An Endpoint Detection and Response (EDR) Solution

Endpoint security solutions range from the original antivirus solutions of yesteryear to extended detection and response (XDR) platforms that tie multiple security solutions together for a better ecosystem. As the needs arise for endpoint security solutions, vendors will attempt to make their solutions match buyer expectations and analyst terms through their messaging but not their engineering. This checklist provides nine criteria informed EDR purchasers consider when evaluating a change or supplement to their endpoint security strategy.

☑ Protection Efficacy

This is where evaluation begins as an EDR solution has to, at its basic core, protect against the current and future threat landscape. Organizations that haven't made a change in their security strategy in the past few years are often still using older EPP or AV solutions that don't protect against the latest threat vectors, such as fileless attacks. Look into how an EDR solution reduces the attack surface and go from there. With the proliferation of people working from home and away from the office, you need to trust that the EDR solution you select will be able to protect the endpoint no matter where it is operating.

☑ 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 state/provincial and local government agencies. MITRE's Engenuity ATT&CK evaluations are a good source to see how well a vendor's EDR client responds to ransomware, but one must also look at how the vendor responds to all forms of ransomware. Additionally, the artificial-intelligence (AI) and machine-learning (ML) capabilities are seen as most important when it comes to ransomware defense. This is made evident when buyers ask, "Can it defend against ransomware if the endpoint is offline, such as at home?" Other considerations are around real-time rollback and the types of systems the EDR client can perform the rollback task on.

☑ MITRE ATT&CK Evaluation Results

Even vendors that fail to block attacks and/or discover the majority of sub techniques in the MITRE ATT&CK Evaluations will find a way to make themselves look like a top-tier EDR solution using the results. The best way to judge if an EDR solution will stop attacks and appropriately discover sub techniques, for the sake of blocking and threat hunting, is to look at four possible things from the evaluation. First, did they elect to participate in the protection tests? They may discover sub techniques well, but may not have the ability to stop them. Secondly, did it block all the attacks they participated in? Note that some clients either don't operate on Linux or were developing threat hunting for Linux at the time of the latest round (e.g., Fortinet). Thirdly, did they discover over 90% of all sub techniques in the detection test? This is important for threat hunting and protection. Fourthly, was the vendor able to detect a strong majority of these sub techniques with analytics (also known as "Technique") as this demonstrates that the solution doesn't require threat intelligence to operate?

☑ Anti-tampering Capabilities

Attackers want to compromise the device's firmware, especially within ransomware attacks. Buyers need to understand how a solution protects the device from such an attack. The use of a malicious bootloader, also called a bootlocker, is a common step in the malware development process. If the malware succeeds, it makes it impossible

to recover files, roll back the system's damage, or even use the system, which is especially painful for healthcare and retail organizations that need to assist patients or transact sales. The EDR set you purchase should act as a firewall for the kernel level of the system to protect it against attacks that attempt to breach this layer or change the operating system.

☑ Operating System Support

Are you considering connecting OT systems to the network? If so, they will need protection, and many of them run on older operating systems like Windows 7 or XP. Do you have Windows Servers or Linux in your environment like many manufacturing, finance, and education organizations? Do you have executives and creative services people using macOS at home? If the vendor does support these operating systems (old and new), ask if the licensing costs are the same for both servers and workstations.

☑ Agent Weight

One of the largest pushes to move to endpoint security software leveraging AI and ML is to reduce the reliance on signatures, which are very limited and slow down the endpoint trying to do its job. EDR solutions range in their impact on system resources, and one should only consider solutions that use less than 1% of CPU utilization on average.

☑ EDR Automation

This is where EDR excels and separates from the old AV and EPP platforms. This is what will turn an overburdened SOC or IT staff from ignoring alerts to one that focuses on fine-tuning an EDR solution to do the work for them so more time can be spent on EDR management and threat hunting (as needed). Ask how granular the policy engine is. Look into how it may integrate with other security appliances and services before heading into an XDR license.

☑ XDR Capabilities

XDR is something people are considering and is going to be one of the largest-growing segments in IT security. Because this is a newer term and yet to be fully defined in many people's minds, vendors are rushing to make the EPP and EDR solutions look like an XDR, but Gartner expresses caution. A mature XDR company should have an experienced SIEM and SOAR product line to expand and grow from. Look for a solution that interfaces with that company's solution set and not third-party APIs, which Gartner calls an "Open XDR," and therefore not the real solution people need and expect from the category.

☑ Managed Service Options

SOC staff is overburdened, and having an outsourced team manage the alerts and incidents that result from the course of encountering elements of the threat landscape 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 to the environment. Buyers frequently ask if deployment services are available along with an MDR team. They also ask if that team is internal to the vendor or outsourced to an additional third party. For global companies that work around the clock, they will also inquire if the vendor has support centers in their region. Because EDR has a relationship with the rest of the security ecosystem, working with a vendor that provides incident response services is much more efficient than one who has to rely on APIs and permissions.

Conclusion

Not all EDR vendors are the same. To discover what is best for one's organization, buyers must ask critical questions about the capabilities of the market's EDR platforms and if they are up to the task to protect their endpoints no matter where they work or how they connect to the internet. Consider your timeline for moving to an XDR solution and see if the EDR solution on offer today can help bridge that gap as your security plans drive toward orchestration.

FORTINET®

www.fortinet.com

May 18, 2022 3:08 PM
1518451-A-0-EN