CHECKLIST

Top 5 Considerations When Selecting an Extended Detection and Response Solution

Many organizations are looking at security vendor consolidation to improve risk posture and security operations while reducing costs or staffing requirements. Extended detection and response (XDR) solutions are a great option to help achieve these goals. According to Gartner, "the primary benefits of XDR should be threefold:

- Improve protection, detection, and response capabilities
- Improve overall operational security staff productivity
- Lower total cost of ownership (TCO) to create effective detection and response capability[1]"

However, organizations must not choose an XDR solution blindly as Gartner finds, "XDR products have significant promise, but also carry risks such as vendor lock-in. The XDR market is immature and capabilities vary widely across products from different vendors."[2] The following questions should be considered when evaluating solutions:

☑ How many (and which) attack vectors are covered by the XDR solution?

Any avenue of attack not covered by the XDR solution is a gap waiting to be exploited by cyber criminals. If not part of the XDR solution, it may require a point product to be integrated or operated independently. Assess endpoint (managed and unmanaged end-user devices, as well as headless Internet of Things [IoT] and Industrial Internet of Things [IIoT] devices); access (wired and wireless); identity; network (home, branch, and corporate); cloud (public, private, or Software-as-a-Service [SaaS]); email; and web application coverage.

☑ How many (and which) Cyber Kill Chain stages are covered by the XDR solution?

Lockheed Martin's Cyber Kill Chain Model (similar to the MITRE ATT&CK Framework) outlines seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives. A cyberattack typically needs to progress through these in order to complete its mission. Breaking the chain at any one of the stages results in successful cyber defense, so the more stages covered by cybersecurity, the more chances to stop the attack.

☑ How effective are the components of the XDR solution?

Simply checking a feature box does not ensure security. Security effectiveness can vary greatly across technologies, products, and vendors. That's why there are many reputable independent test houses that routinely assess security effectiveness. Make sure that the products that send alerts, provide telemetry, and enact response for the XDR solution have been tested by leading independent organizations such as AV Comparatives, SE Labs, Virus Bulletin, and ICSA Labs and demonstrate high security effectiveness—not just once, but regularly.

☑ How usable is the XDR solution for your staff?

Every organization has a unique size, structure, and skill set to its security function. At the same time, each XDR solution has varying degrees of integration and automation. Consider the degree to which the XDR solution simply correlates security information (like the traditional security information and event management [SIEM]) vs. fully automating the functions of correlation, detection, investigation, and response.

☑ Is the XDR solution proprietary to one vendor, open to all, or a mix?

Vendor-specific XDR solutions are typically better integrated, but of course, require choosing products from that vendor's portfolio. Open XDR systems sound great, but often require a lot more ongoing engineering simply to normalize and correlate data, falling short in terms of detection and investigation over time. Consider how comfortable you are being limited to a vendor's portfolio in return for more automation.

To achieve better protection and efficiencies through security vendor consolidation, it's important to select the right XDR solution for your organization.

[1] Peter Firstbrook and Craig Lawson, "Innovation Insight for Extended Detection and Response," Gartner, March 19, 2020.

[2] Ibid.

FORTINET

www.fortinet.com

December 3, 2020 7:38 AM

830153-0-0-EN

D:\Fortinet\Checklist\813925 - MOF Checklist\cl-FA-top-5-considerations-when-selecting-an-extended-detection-1232020\cl-FA-top-5-considerations-when-selecting-an-extended-detection-1232020