WHITE PAPER

Enhance Security Operations with Product Consolidation and XDR

Executive Summary

The constantly evolving cyberthreat landscape combined with a steady stream of security technologies designed to address these threats pose numerous challenges for security teams. The complexity of using multiple products from numerous vendors and the volume of alerts generated can easily overload organizations, especially given the ongoing shortage of skilled cybersecurity professionals available to fill critical roles.

An average organization uses multiple security tools from various vendors, which together can generate thousands of alerts daily. The complexity and disjointed nature of the environment can be a constant headache for many leaders. Teams have multiple management portals to inspect, and they must manually connect the data from each of them. As a result, teams respond more slowly to alerts, have less time for investigations, and run a greater risk of missing an attack in progress or letting attackers linger in the environment.

Making security management and threat mitigation even more difficult is the fact that cybersecurity skills are scarce. It's estimated that closing the cybersecurity skills gap would take an additional 4 million cybersecurity professionals.[1]

Reduce Complexity with Consolidation

According to a recent article, 95% of organizations are pursuing a security vendor consolidation strategy.[2] Goals of consolidation are to improve operational efficiency and cyber risk posture while reducing costs and staffing needs. To do so, organizations must consider the pros and cons of a point product approach to a consolidated platform approach. For most organizations, consolidation will likely happen around a small number of strategic platforms supplemented by select point products rather than taking an all-or-nothing approach.

As a starting point, rather than aiming for immediate consolidation with a single vendor, businesses can focus on consolidating around a few key security vendor platforms, potentially enhancing these with a limited selection of point product vendors as needed. This approach leverages natural categorizations and platforms, such as endpoints, networks, email, cloud, and identity management platforms.

Every security strategy must cover all attack vectors, especially as the digital attack surface expands and networks evolve. While most attacks ultimately seek out the endpoints—end-user computing, servers, and containers—there are multiple paths cybercriminals take to reach their targets. The majority of malware is delivered by email, and the remainder is downloaded from the internet. Still, web applications and their vulnerabilities are a primary source of data breaches. These applications can be hosted by the customer on-premises or in the public cloud or use Software-as-a-Service providers. If security controls do not span the entirety of the network, attacks will slip through the cracks.

Organizations need to recognize the various stages of an attack. Many of today's cyber threats are multistage, making them more challenging to detect but offering multiple opportunities to detect and prevent. Deploying technologies at multiple cyber kill chain stages establishes defense in depth, strengthening benefits gained by security vendor consolidation.

Detect and Respond to Threats Faster

Despite years of development within cybersecurity, the approach to solving many problems is still relatively immature, as evidenced by deploying multiple point products that don't have a native relationship with one another. Only now are multiple security platforms for networks, email, endpoint, cloud, and more coming together under the extended detection and response (XDR) conceptual architecture.

An effective XDR solution collects, normalizes, and correlates data across security controls. The solution can help security teams detect threats faster, aid investigations, and speed up responses.

What to Look for When Evaluating XDR Solutions

When evaluating XDR solutions, ask the right questions and understand if the providers you're evaluating can help solve your organization's unique security challenges. Below are common use cases teams seek to solve when evaluating XDR solutions.

Enhance threat detection across diverse environments: A good XDR solution integrates seamlessly with a wide range of security products across endpoints, networks, cloud services, email, and other applications. XDR uses advanced analytics, artificial intelligence, and machine learning to detect sophisticated cyberthreats that might evade traditional security measures, offering a unified view of threats across the entire digital estate.

Offer automated incident response: The solution should significantly reduce the time it takes to respond to threats by automating response actions. XDR automatically isolates infected endpoints, blocks malicious IP addresses, and can apply patches to vulnerabilities, helping security teams to mitigate threats quickly and efficiently.

Protect against advanced persistent threats (APTs): With the ability to correlate and analyze data from multiple sources, an XDR solution excels at uncovering subtle indicators of APTs. It helps identify and disrupt these sophisticated, multi-vector attacks to protect sensitive data and critical infrastructure from compromise.

Include compliance management and reporting: Organizations that operate under strict regulatory requirements can leverage the solution for continuous monitoring and reporting. It ensures that all security policies are enforced across the board and that any deviations are quickly identified and rectified, helping maintain compliance with industry standards and regulations.

Offer cloud and hybrid environment security: As businesses increasingly adopt cloud services, securing these environments becomes more complex. Effective XDR solutions offer extensive visibility and security for multi-cloud and hybrid environments, enabling organizations to effectively detect and respond to cloud-specific threats.

Streamline security operations: By integrating with existing security infrastructure and providing automated orchestration capabilities, XDR solutions help streamline security operations. This improves the efficiency of incident response processes and lowers the mean time to detect and remediate while allowing security personnel to focus on strategic security initiatives.

Provide forensic analysis and incident investigation: In the aftermath of a security incident, XDR solutions provide comprehensive data aggregation and analysis tools to support forensic investigations. This helps security teams understand the breach's scope, identify the attack vectors used, and implement measures to prevent future incidents.

Support zero-trust architectures: XDR solutions support zero-trust by continuously verifying the security status of devices and users, enforcing strict access controls, and minimizing the attack surface, regardless of the user's location or the device used.

Enhance ransomware detection and mitigation: XDR solutions based on EDR platforms are adept at identifying and mitigating ransomware attacks early in the attack chain. A strong XDR solution helps prevent the encryption of critical systems and assists in recovery efforts by outlining the scope and impact of the attack.

The right XDR solution can enhance an organization's security posture significantly by offering a comprehensive suite of security capabilities designed to address the complex and evolving landscape of cyberthreats.

Conclusion

With consolidation and an effective XDR solution, organizations can greatly improve their security posture and operational efficiency. Read this solution brief for more details on XDR and how you can integrate it with your security ecosystem.

[1] How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, ISC², November 3, 2023.

[2] Chris Selland, What IT Executives are Saying About Vendor Consolidation, CIO, October 26, 2023.

FORTINET

www.fortinet.com

April 16, 2024 2:54 PM

859744-B-0-EN