POINT OF VIEW

Strengthen Your Security Posture with Network Detection and Response Technology

Executive Summary

The increasing complexity of today's threat landscape keeps even the most well-staffed, highly skilled security teams on their toes. And the proliferation of these cyberthreats means that security professionals are tasked with more, yet often don't have the necessary resources to adequately protect their organization's expanding attack surface. To effectively safeguard your organization and reduce analyst burnout, it's crucial to embrace consolidated security technologies enhanced by machine learning (ML) and artificial intelligence (AI), including a robust network detection and response (NDR) solution. Network detection and response solutions offer AI-driven breach prevention to help your security operations center (SOC) team detect and remediate incidents faster and more efficiently.

Nearly 70% of organizations report that they don't have enough security professionals on staff.[1]

Today's Threat Landscape Is Taking a Toll on Your Analysts

It's no secret that the threat landscape continues to grow more complex by the day. For example, in the first half of 2022, Fortinet FortiGuard Labs identified 10,666 new ransomware variants—an increase of nearly 100% compared to the previous six months.[2] Bad actors continually find more sophisticated ways to infiltrate networks, making every organization a target, regardless of size or industry.

At the same time, SOC teams face several distinct challenges. Recruiting and retaining qualified security professionals remains an uphill battle for most organizations. According to a recent study, while the cybersecurity industry added 464,000 more professionals this year, an estimated 3.4M additional security workers are still needed to fill open roles and secure organizations effectively.[3] This talent shortage has tangible implications for businesses, as 80% of security leaders surveyed say their enterprise has suffered at least one breach they can attribute to a lack of cybersecurity skills or awareness.[4]

As the volume and complexity of cyberthreats increase, understaffed SOC teams often add point products to their list of go-to technologies to mitigate new risks. However, adding more siloed technologies in response to new threats increases an organization's attack surface and often slows and complicates daily operations, which is the opposite of the intended result.

Given these challenges, enterprises must implement consolidated security technologies—ideally augmented by ML and AI—that help speed detection and response across the entire network, strengthening the organization's security posture and creating efficiencies for analysts.

The average total cost of a data breach is $4.35M, and 83% of organizations have suffered more than one breach.[5]

Network Detection and Response Technology Enhances SOC Efficiency

Network detection and response solutions offer AI-driven breach prevention and help overworked SOC teams shift from being reactive to proactive. The technology learns what's typical for your organization, scans for and detects network anomalies across your entire environment, alerts your SOC to suspicious network activity, and leverages automation to quarantine and quickly control a potential incident. As a result, SOC teams can remediate incidents faster while reducing the amount of manual work needed to mitigate a threat.

Adopting NDR technology is a basic requirement for all organizations but is particularly helpful for short-staffed or smaller SOC teams. A strong NDR solution enhances SOC efficiency by:

Detecting potential cyber incidents earlier: The solutions learn what normal network behavior looks like for your organization and then apply ML and advanced analytics to detect signs of sophisticated attacks. Because NDR technology constantly evolves based on your enterprise's network activity, threats are detected faster and more accurately.

Rapidly identifying all compromised users and devices across the network: When an incident occurs, one of the most challenging and time-consuming tasks is detecting compromise in the numerous devices on your network that can't support an endpoint detection and response (EDR) agent. With NDR technology, you can deploy dedicated sensors throughout your entire network to analyze traffic coming from all devices¬—including Internet-of-Things (IoT) and operational technology (OT) devices—which reduces the amount of manual work required of your team.

Containing the incident faster with AI: A good NDR solution uses AI to analyze code generated by malicious traffic and determine its spread throughout the network, identifying the outbreak source and tracing how widespread the attack is across your environment. By allowing your NDR technology to complete an initial quarantining process, your SOC team can focus on deciding the right next step to remediate an incident.

Network Detection and Response Solutions Are an Integral Part of a Holistic Security Strategy

Consider an NDR solution as a foundational component of your security technology stack. By learning what's normal for your environment and using AI-driven advanced analytics to detect anomalous behavior, your SOC can utilize NDR technology to stop attacks faster and spend less time remediating them.

However, the best NDR solutions are just one part of a consolidated, holistic approach to risk management. As the proliferation of ransomware and other cyber risks continues, organizations of all shapes and sizes must extend their dynamic detection and response capabilities across their networks, including their most common points of infection, endpoints. To achieve this, many organizations are also replacing their traditional endpoint security with advanced EDR technology, which provides deeper analysis to identify signs of compromise on endpoints and even disrupt malware mid-attack. And EDR solutions designed to work hand-in-glove with NDR technologies provide even broader visibility and control across your attack surface. Smaller SOC teams can enhance their operations even further by embracing managed detection and response (MDR) services to offload initial alert monitoring and triage, freeing up internal staff time to focus on higher-level work.

Implementing the right security technology is crucial to protecting your organization against an evolving array of cyberthreats. But instead of relying on a myriad of point products, consider consolidating security technologies to reduce vendor and solution

sprawl. This approach offers numerous benefits for your team—it enables advanced threat correlation, centralizes management and orchestration, and provides a more coordinated response to threats across your entire network.

Conclusion

Threat actors show no signs of slowing anytime soon, so security teams everywhere must implement the right technology, people, and processes to mitigate their organization's risk now and as their networks and services continue to evolve. By embracing NDR's AI-driven technology, security leaders can reduce the burden placed on their SOC team, increase operational efficiencies, and reduce the likelihood of analyst burnout by quickly identifying and stopping cyber incidents.

[1] "(ISC)² Cybersecurity Workforce Study 2022," (ISC)², October 20, 2022.

[2] "Global Threat Landscape Report, 1H 2022" Fortinet, August 26, 2022.

[3] "(ISC)² Cybersecurity Workforce Study 2022," (ISC)², October 20, 2022.

[4] "2022 Cybersecurity Skills Gap Global Research Report," Fortinet, April 27, 2022.

[5] "Cost of a Data Breach Report 2022," IBM, July 27, 2022.

FORTINET

www.fortinet.com

March 21, 2023 11:14 PM

2052068-0-0-EN