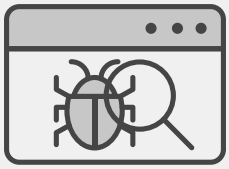
POINT OF VIEW

Power Greater Visibility, More Productivity, and Faster Responses with EDR, NDR, and NGFW Integration

Executive Summary

A recent survey found that 75% of security practitioners feel that today's threat landscape is the most challenging it's been in the past five years.[1] It's not hard to understand, then, why even the most skilled, fully staffed security teams are struggling to improve incident and response times, secure unmanaged devices, and keep up with increasingly complex attacker tactics, techniques, and procedures (TTPs). Meanwhile, cybercriminals successfully circumvent security controls to exfiltrate data and avoid detection. Security teams often attempt to address these challenges through disparate solutions, leading to inefficient response processes that result in a security operations center (SOC) of overwhelmed analysts. However, by integrating endpoint detection and response (EDR), network detection and response (NDR), and next-generation firewall (NGFW) technology, security teams gain comprehensive visibility, greater productivity, and streamlined response processes.



On average, it took organizations 277 days to identify and contain a breach in 2023.[2]

Networks Continue Expanding While Organizations Struggle to Find Security Talent

As organizations evolve their business models, device proliferation is inevitable. And while this leads to positive outcomes for the organization's bottom line, it often overwhelms security and IT teams. More than 60% of security practitioners say the size of their organization's attack surface has expanded in the past three years.[3] At the same time, businesses struggle to recruit, hire, and retain the skilled cybersecurity talent necessary to adequately protect the organization. Nearly 70% of leaders say their organization faces additional risks because of the cybersecurity skills shortage.[4]

Between constantly expanding attack surfaces and a lack of skilled professionals to fill open roles, it's no surprise that many security teams are overwhelmed.

The Three Key Challenges that SOC Teams Routinely Experience

Here are the top three challenges SOC analysts typically experience and why combining endpoint protection with enhanced network intelligence and response is essential to successful security operations.

Attackers are becoming increasingly adept at evading detection. To obfuscate attacks, attackers combine malicious activity with routing network traffic, using encrypted channels to exfiltrate data, and encrypting command-and-control (C2) communications, making it challenging for security teams to discover and distinguish between legitimate and potentially malicious actions.

Investigation and response activities take longer because of siloed solutions. As cybercrime proliferates, security teams face too many alerts to investigate all of them thoroughly. Many teams use manual processes, and each investigation requires significant resources as analysts look for the necessary context to prioritize and determine the next steps.

A lack of comprehensive visibility results in unsecured devices. Security teams often do not have complete visibility regarding what devices are connected to the network, leaving questions about what is and is not being monitored. Without this comprehensive picture, they can't take the appropriate actions to secure various devices.

Combine NDR, EDR, and NGFW Technology to Enhance Security Operations

Organizations can address these challenges by integrating network and endpoint detection solutions—ideally within a single security platform—to streamline analysis and response efforts.

Combining EDR, NDR, and NGFW technologies brings network and endpoint data together, providing security teams and threat hunters with unparalleled visibility and high-fidelity detection of unknown threats and indicators of malicious activity.

This is achieved by automatically correlating and analyzing security events from several data sources: NDR behavioral network traffic analysis supplemented by EDR host context and attack isolation using either EDR for agent-supported endpoints or NGFW for unmanaged assets. When combined, this telemetry can help security analysts spot and stop any malicious behavior early in the attack life cycle across both on-premises and cloud environments. The integration of these technologies results in:

- **Reduced alert triage times:** When integrated with EDR, the NDR solution can correlate endpoint detections with its network-based detections. Using this enriched threat intelligence, analysts can view prioritized alerts, run additional investigations, and facilitate response actions, reducing the need to manually collect information from disparate tools.
- **Accelerated threat hunting and reduced false positives:** Analysts gain insights into attack activity, such as data exfiltration, C2, lateral movement, and malware deployment, while EDR and NDR solutions leverage automatic detection tuning, powered by AI and ML and human analysis to reduce false positives and provide high-fidelity detections.
- **Real-time endpoint visibility:** Certain operational technology (OT) and Internet-of-Things (IoT) devices have limitations with computing and memory resources and cannot support an EDR agent. This combined solution discovers any device connected to the network, including unmonitored and shadow IT endpoints that are not covered by other security controls. As a result, security teams can track and contain attacks involving OT and IoT infrastructure without installing and maintaining endpoint agents.

Conclusion

A platform approach to security makes it possible to integrate EDR and NDR telemetry with an organization's NGFW, harnessing the power of data to provide analysts with enriched detection and response capabilities and a holistic view of activity occurring on their network. Integrated data sources and robust threat intelligence also offer analysts higher-fidelity detections, which streamlines their investigation and response processes.

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

[2] Cost of a Data Breach 2023, IBM, July 24, 2023.

[3] 67% of Daily Security Alerts Overwhelm SOC Analysts, Help Net Security, July 20, 2023.

[4] 2023 Cybersecurity Skills Gap Report, Fortinet, March 21, 2023.

FORTINET

www.fortinet.com

March 2, 2024 5:49 PM

2574347-0-0-EN