FORTINET

Advanced Cybersecurity Strategies

Leveraging ZTNA, EDR, and XDR for Comprehensive Protection

Table of Contents

Executive Overview

Organizations face growing cybersecurity challenges due to a turbulent threat landscape and expanded attack surfaces, making traditional defenses inadequate. The shift to a more hybrid workforce further complicates access control, increasing the risk of lateral movement by attackers.

Today's sophisticated threats, like polymorphic and fileless malware, demand advanced detection and response. Fragmented IT access policies, insufficient security solutions, and alert fatigue exacerbate inefficiencies. This ebook explores strategies for managing secure access, endpoint detection and response (EDR), and extended detection and response (XDR) within a unified security approach, offering comprehensive protection and easing the operational burden on security teams.

In the second half of 2023, 73% of firms faced severe cyberattacks, a 4% increase and botnet activity rose by 15%.[1]

The Imperative of Secure Access

Most people understand secure access from the lens of virtual private network (VPN) solutions. While VPN is still used for remote access, zero-trust solutions better address hybrid workforce requirements and the lateral movement of threats. Zero-trust network access (ZTNA) embodies the principle of “never trust, always verify,” setting it apart from traditional VPN solutions by continuously verifying users and devices before granting access to applications and data.

The increasing complexity of cyberthreats and the limitations of perimeter-based security models highlight the need for ZTNA. Unlike VPNs, which inherently trust internal traffic once it has passed the perimeter, ZTNA ensures that every access request is scrutinized, significantly reducing the risk of unauthorized access and the expansion of an attack if it happens to evade the network defenses.

ZTNA provides enhanced security by minimizing the attack surface through stringent verification processes. By continuously validating users and devices, ZTNA prevents attackers from moving laterally within networks. This approach is crucial for securing remote and hybrid work environments where traditional perimeter defenses fall short. Improved access control ensures that only authenticated users can access critical applications, providing a secure and seamless remote work experience while mitigating the risk of lateral movement within networks.

Best Practices and Real-World Insights for ZTNA Implementation

Implementing ZTNA involves transitioning from implicit trust to a zero-trust model. This process requires careful planning and consideration, including establishing strong authentication mechanisms and integrating ZTNA with existing security infrastructure. Best practices for successful ZTNA deployment include continuously monitoring and updating security policies and ensuring that the system adapts to evolving threats and organizational needs.

Real-world examples of ZTNA implementation demonstrate its effectiveness, with organizations reporting enhanced security, improved access control, and a seamless user experience. These case studies offer valuable insights and lessons learned, highlighting common challenges and solutions in deploying ZTNA. As ZTNA continues to evolve with emerging technologies, organizations must prepare for future access control and security challenges by strategically integrating these advancements.

In summary, ZTNA provides a comprehensive solution for modern cybersecurity challenges by ensuring authenticated access, continuous endpoint monitoring, and coordinated threat response, ultimately enhancing an organization’s cybersecurity posture and lightening the workload on security teams.

67% of organizations have deployed ZTNA, reflecting its growing importance in modern cybersecurity strategies.[2]

Leveraging Endpoint Detection and Response

When it first comes to anti-malware technology within endpoint security, most people first think of traditional antivirus solutions. However, EDR solutions have emerged to address the limitations of traditional antivirus. EDR goes beyond simple signature-based detection to provide continuous monitoring and advanced threat response capabilities. EDR solutions play a crucial role in modern cybersecurity strategies by detecting and responding to sophisticated threats that traditional antivirus might miss.

EDR offers security teams real-time threat detection through continuous endpoint monitoring, leveraging behavior-based detection methods to identify malicious activities while using fewer system resources than traditional endpoint protection platforms (EPPs). This approach enables rapid response and mitigation, significantly reducing the mean time to detect (MTTD) and mean time to repair (MTTR) incidents. By automating threat responses via integrated playbooks, EDR minimizes the impact of attacks and enhances the overall security posture of an organization.

Implementing EDR solutions involves several key steps, including establishing strong policies and procedures, integrating EDR with existing security infrastructure, and continuously updating the system to address new threats. Best practices for effective EDR deployment emphasize the importance of comprehensive visibility into endpoint activities and correlating endpoint data for improved threat analysis.

In short, EDR provides a robust solution for modern cybersecurity challenges by ensuring real-time threat detection, rapid response, and comprehensive visibility into endpoint activities while reducing the operational burden on security teams.

The average organization takes over 198 hours to identify, triage, and contain threats, exposing them to increased risks during this extended timeframe.[3]

Considering Extended Detection and Response

XDR builds upon the capabilities of EDR by integrating multiple security layers to provide a comprehensive view of the threat landscape. XDR correlates data from various sources such as networks, email, endpoints, servers, and cloud, enabling holistic threat detection and coordinated responses.

While security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions are commonly used for centralized monitoring and automated response, XDR can be an effective first step for organizations without existing automation. XDR complements SIEM and SOAR by providing deeper integration and automation across security layers, reducing MTTD and MTTR. For organizations looking to streamline their security operations, XDR offers a first step to a more integrated and efficient approach to response to alerts.

Best practices for XDR deployment emphasize the importance of comprehensive visibility into the entire IT environment, enabling security teams to quickly identify and respond to sophisticated attacks. Look for an XDR solution built upon an EDR solution that comes from a provider with a SIEM and SOAR offering as well as a complementary suite of products designed to work together instead of relying on a bank of fickle APIs.

Real-world examples of XDR implementation demonstrate its effectiveness, with organizations reporting enhanced security and visibility, improved threat detection, dramatic alert reduction, and faster response times. XDR also reduces the operational lift on security teams past what EDR can provide and can pave the way for more advanced automation with SIEM and SOAR solutions.

In the second half of 2023, organizations saw a 10% increase in unique exploit detections, with an average of 63 exploit detections per organization. This surge contributes to overwhelmed security teams, underscoring the need for integrated security solutions that XDR could solve.[4]

How Integrating Secure Connectivity, EDR, and XDR Could Work

In a hypothetical situation, imagine a company called Acme Consumer Technology, a midsize tech company with a largely remote and hybrid workforce, faced significant cybersecurity challenges, including targeted attacks. They have already implemented a comprehensive security framework that integrates ZTNA. This integration ensures continuous verification of users and devices, holistic threat detection, and coordinated automated responses, providing a robust defense against sophisticated cyberthreats, especially for those that want to spread laterally like ransomware.

In this scenario, Acme Consumer faced an extremely evasive and well-crafted attack. An attacker sent a highly targeted phishing email containing a seemingly legitimate file. When the file was opened, it turned out to be a Trojan that bypassed initial defenses. The Trojan downloaded additional malicious payloads through the firewall, installed them on the device, and attempted to move laterally and deploy Cobalt Strike beacons across connected networks, including cloud workloads like on Google Cloud. Initially, alerts were raised in a few locations, but the staff ignored them since they were too low of a priority.

Because Acme Consumer operates on zero-trust principles, the attack was limited only to that device and could not spread. The XDR platform played a crucial role in piecing together this complex attack from email security, the EDR/XDR console, and the firewall manager. It could have also detected it within the Google Cloud Security Command Center if it had gotten that far.

It identified connections between low-fidelity alerts, linking the initial file opening to subsequent malicious activities.

Attackers frequently misuse valid accounts to move laterally across networks, using legitimate tools to evade detection and escalate privileges. This makes it crucial for organizations to have integrated security solutions that can detect and respond to these sophisticated tactics.[5]

The XDR system emailed the SOC manager and a Slack notification to a tier-one analyst detailing the suspicious activities. The analyst reviewed the alert in the XDR console. Because their system wasn't configured to take automatic remediation steps, the analyst agreed with the recommended response actions provided by XDR to block the sender and affiliated IP address and delete all files and code from the attacker. Furthermore, the user's password was reset, and infected ZTNA device tags were applied to compromised devices, isolating them on a remediation VLAN through NAC integration. This made it seem like the intrusion didn't happen, blocking the possibility of follow-on attacks.

Things to Consider Before Deploying ZTNA and EDR with or without XDR

Deploying ZTNA, EDR, and XDR can significantly enhance an organization's security posture with proper planning and integration. ZTNA streamlines access control for on-premises and remote users, while EDR and XDR provide advanced threat detection and response capabilities.

Using a phased approach is essential, starting with pilot testing and considering professional deployment support. To prevent staff burnout, organizations should consider a managed detection and response service that offers comprehensive 24×7 monitoring and response, easing the operational load on internal teams while maintaining robust security.

[1] Global Threat Landscape Report, Fortinet, May 2024.

[2] Key Takeaways from the State of Zero Trust Report, Fortinet, June 2023.

[3] The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Security Group, July 2023.

[4] Global Threat Landscape Report, Fortinet, May 2024.

[5] Ibid.

FORTINET

www.fortinet.com

September 19, 2024 8:38 PM / 2836692-0-0-EN