Bridging AD Security Gaps with Identity Threat Detection and Response

Enhance your hybrid Active Directory security hygiene.

Quest

Introduction

With 80% of security breaches now involving compromised identities, Active Directory (AD) and Entra ID security is a top priority for many organizations. Losing control of Active Directory or Entra ID equates to losing control of your enterprise.

As cyber threats become more sophisticated, attackers are constantly finding new ways to exploit vulnerabilities.

While Endpoint Detection and Response (EDR) Network Detection and Response (NDR) solutions are essential for defending against a wide range of threats, they focus primarily on endpoint and network security. However, there are distinctions to be made here: EDR protects devices and endpoints like computers, phones, and servers, while NDR focuses on monitoring traffic within the network to detect unusual patterns.

Both EDR and NDR address different layers of security, but together, they help provide a more comprehensive defense. Extended Detection and Response (XDR) is designed to aggregate and correlate signals from both EDR and NDR to give a more unified view of potential threats.

Despite the strengths of EDR and NDR, identity security could still be lacking, leaving your organization vulnerable to attacks that specifically target Active Directory and Entra ID. This is where Identity Threat Detection and Response (ITDR) solutions, such as Quest Security Guardian, become crucial. ITDR solutions complement EDR, NDR, and XDR by filling the gaps in identity security, ensuring comprehensive cyber resilience, security hygiene, and robust threat mitigation.

The Importance of EDR, NDR, and XDR in Cyber Resilience

EDR solutions are engineered to monitor, detect, and respond to threats on endpoints like laptops, desktops, and servers. They offer key benefits such as:

- Real-time monitoring and response: Continuous monitoring and real-time threat detection and response.
- Detailed forensic analysis: Comprehensive data to understand and mitigate attacks.
- Automated response: Mechanisms to isolate affected endpoints and prevent threat spread.

NDR solutions, on the other hand, are focused on monitoring network traffic to detect and respond to any anomalies or unusual activity. NDR provides insight into network traffic, helping detect lateral movement and network-based threats, which may not be visible through endpoint solutions alone. Key benefits of NDR include:

- Enhanced network visibility: Real-time monitoring of network traffic to detect both known and unknown threats.
- Behavioral analysis and anomaly detection: Identifies patterns and deviations from normal behavior in network traffic, often using machine learning.
- Lateral movement detection: NDR is particularly effective at detecting how threats spread laterally across networks, making it an essential part of a defense strategy.

XDR integrates and aggregates data from both EDR and NDR (and other sources like ITDR), combining endpoint data, network data, and identity data to create a broader, more comprehensive view of an organization's security posture. By correlating signals from multiple layers, XDR can:

- Improve threat detection: Correlate data from EDR, NDR, ITDR, and other sources to identify complex threats.
- Streamline response efforts: Centralized platform for incident response across the entire IT environment, leveraging integrated insights.
- Enhance visibility: Provide a unified, holistic view of the organization's security posture, covering endpoint, network, and identity threats.

The Role of ITDR

While EDR and NDR focus on protecting endpoints and network traffic respectively, Identity Threat Detection and Response (ITDR) focuses on protecting identity infrastructure — an essential component often overlooked in traditional security frameworks. Gartner has recognized identity as a primary attack vector, emphasizing the vulnerabilities and misconfigurations common in platforms like Active Directory and Entra ID.

ITDR addresses these challenges by specifically focusing on monitoring, detecting, and responding to identity-related threats. It's important to understand that ITDR complements EDR, NDR, and XDR by providing targeted protection for identity layers that aren't addressed by endpoint or network solutions. Organizations relying solely on EDR and NDR for comprehensive security may find themselves vulnerable to identity-based attacks that target privileged accounts and critical AD infrastructure.

ITDR with Microsoft Defender for Identity

Microsoft Defender for Identity (MDI) is a notable ITDR solution with some great benefits, including:

- Strong LDAP Query and Authentication Vulnerability Focus: It is effective at detecting vulnerabilities related to Lightweight Directory Access Protocol (LDAP) and authentication.
- Integration with the Microsoft Ecosystem: Seamless integration with other Microsoft security products for a unified security approach.

However, despite these advantages, it is important to consider the limitations that MDI has:

- No real Tier 0 concept: Lacks focused protection for critical assets such as domain controllers and highly privileged accounts.
- Limited security posture assessments: Provides only basic assessments of Active Directory security posture, potentially leaving organizations unaware of critical vulnerabilities and misconfigurations.
- No object protection: Does not offer specific protection mechanisms for critical Active Directory objects, leaving them vulnerable to unauthorized access and changes.
- Little GPO awareness: Limited awareness of Group Policy Objects (GPOs), crucial for maintaining secure AD configurations.

When it comes to true cyber resilience, it is important to consider these limitations and explore additional ITDR solutions beyond MDI.

Better ITDR with Security Guardian

Quest Security Guardian offers a comprehensive ITDR solution that enhances cyber resilience by addressing gaps left by EDR and XDR. It provides organizations with:

- Focused visibility into critical Tier 0 assets.
- Benchmarking against industry best practices.
- Protection for critical objects, including GPOs.
- Continuous monitoring for indicators of exposure (IOEs) and indicators of compromise (IOCs).
- Seamless integration with SIEM tools like Microsoft Sentinel and Splunk.

Furthermore, Security Guardian integrates with and enhances Microsoft Defender for Identity, empowering MDI-reliant organizations with:

- Advanced alerts on Attacker Tools, Techniques, and Procedures (TTPs): Delivers actionable alerts on attacker activities and tactics within Active Directory, providing deeper insights into potential threats.
- Enforcement of Privilege Account Management policies: Ensures compliance with Privilege Account Management policies on Tier 0 objects by addressing implicit relationships.
- Automatic categorization and drift detection: Continuously categorizes Tier 0 objects and swiftly identifies deviations from the known state, maintaining consistent protection.
- Proactive identification and protection: Detects, alerts on, and safeguards against misconfigurations, including Group Policy Object (GPO) setting changes, and attacks targeting Active Directory databases (.DIT files).
- Compliance and retention management: Preserves findings and audit data in line with compliance and retention requirements, ensuring comprehensive record-keeping.
- Efficient forwarding to Sentinel: Transmits findings to Microsoft Sentinel, which then forwards signal data to Microsoft Defender for Identity (MDI). Note: This integration requires special Microsoft licensing for MDI to Sentinel forwarding.

By integrating these capabilities, Security Guardian not only enhances the functionality of Microsoft Defender for Identity but also provides additional layers of protection and compliance that are crucial for robust identity security. And with Security Guardian now integrating with Microsoft Security Copilot, simplifying and optimizing hybrid AD security tasks is easier than ever, no matter the user's skill level.

Conclusion

EDR and XDR solutions are indispensable components of modern cybersecurity strategies, but they do not cover identity security comprehensively. Integrating a powerful ITDR solution, like Quest Security Guardian, is essential for filling these critical gaps and achieving true cyber resilience.

Learn more about Security Guardian and how it can help you reduce your attack surface with simplicity and speed.

Quest

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Refer to our website (www.quest.com) for regional and international office information.