Multi-layered Defense: Enhancing Security with Fidelis Active Directory Intercept™

Active Directory (AD) serves as the cornerstone of identity and entitlements management in over 90% of organizations.

As the main system for user login and access permissions, it is very important for protecting Active Directory environments, networks, assets and information. However, its centrality also makes Active Directory a prime target for attackers looking to exploit vulnerabilities, leading to unauthorized access, privilege escalation, and malicious activities that pose significant AD risks.

Active Directory is the ideal starting point for adversaries to delve deep, move laterally, escalate privileges, and engage in malicious activities such as code execution, data exfiltration, account spoofing, and more. Protecting AD is a top priority for almost any organization, yet many traditional technologies fail to detect the warning signals of an impending attack.

Why Attackers Target Active Directory

Active Directory is an attractive target for cybercriminals because it plays a crucial role in managing network access and control. If attackers breach AD, they can take over an entire organization’s network. This allows them to access sensitive data, escalate privileges, and often remain undetected for long periods. This situation poses a high risk of data exfiltration, ransomware attacks, or worse.

The complexity of AD environments, often spanning on-premises, cloud, and hybrid infrastructures creates visibility challenges. Misconfigurations, inadequate privilege management or the failure to regularly patch vulnerabilities create entry points for adversaries. In many cases, cybercriminals capitalize on these misconfigurations, combining them with brute-force attempts

or phishing to compromise accounts. Once inside, attackers escalate their privileges, taking full control of the AD environment.

88%

Alarming Stat

88% of organizations affected by ransomware lacked proper AD security best practices, like multi-factor authentication (MFA) or privileged access controls.

Before Securing AD After Securing AD How It Transformed AD Security Weak Passwords Everywhere Strong Password Policies in Place No more guessing games—complex passwords lock down entry points. No Multi-Factor, No Protection MFA Secured for All Users Hackers can't get past this two-step defense, keeping accounts safe. Open Access, No Boundaries Access Only Where Needed (Least Privilege) Locked doors everywhere—minimized permissions block unnecessary access. Admin Privileges for Many Admin Access Only for the Few Restricted admin powers stop privilege abuse dead in its tracks. Misconfigured Group Policies Up-to-Date Group Policies that Work Policies are now your frontline defense—keeping systems secure. User Activity in the Dark Real-Time User Monitoring Suspicious behavior? Spotted and stopped before it became a threat. No Logs, No Clue Audit Logs That Tell the Story Detailed logs shed light on attacks, providing clear paths to solutions. Old Systems, New Vulnerabilities Regular Patching & Updates Always a step ahead—no weak points for attackers to exploit. Unrestricted External Access Controlled, Conditional Access Keep the doors locked—external services access only when necessary. Slow to Respond Automated Detection & Response Breach? Act in seconds, not hours—automated responses save the day. Backups? What Backups? Regular Backups & Recovery Plans Data loss is history—tested recovery plans ensure business continuity.

Fidelis Active Directory Intercept™: A Multi-layered Defense

To counter these threats, Fidelis Active Directory Intercept™ offers a comprehensive solution to mitigate these risks. It leverages a multi-layered approach that combines AD-aware network detection and response (NDR), integrated deception technology, and advanced log and event monitoring. This approach enables organizations to enhance their **threat defense for Active Directory**, detecting, responding to, and preventing a wide range of AD-related attacks, including Active Directory reconnaissance, brute-force authentication attempts, Kerberoasting, password sniffing, and more.

With Fidelis Active Directory Intercept™, you gain complete visibility into AD objects, enabling in-depth analysis of resources and access paths. This technology provides a defense-in-depth approach to Active Directory that allows defenders to effectively identify, analyze, and block adversary movement with features like:

AD Threat Detection

- Powerful network sensors provide real-time traffic analysis to identify even subtle indicators of threats against Active Directory.
- AD log analysis monitors configurations to effectively identify and analyze adversary movements.

AD Attack Response

- Automated AD-aware deception capabilities lure adversaries away from high-value

assets and provide defenders with high-confidence, context-rich alerts.
- MITRE ATT&CK framework mapping accelerates threat response and facilitates threat-informed decision making.
- Advanced forensic tools and automated playbooks and scripts give defenders the power to thwart AD attacks prior to impact.

AD Threat Prevention

- Continuous AD configuration monitoring improves security hygiene and closes security gaps before they become entry points for attackers.

Master Active Directory Security – Protect Your Critical Assets

Safeguard your AD before, during, and after an attack. In this whitepaper, you'll find:

- Attack Prevention Strategies
- Incident Response Tools
- Advanced Threat Detection

Download Now

How Fidelis Active Directory Intercept™ Works?

One of the most powerful aspects of Fidelis Active Directory Intercept™ is its ability to perform advanced network traffic analysis. This is accomplished through Fidelis Network®, which offers advanced Active Directory defense and threat detection capabilities that go beyond traditional signature-based methods.

Using machine learning and behavioral analysis, Fidelis identifies unusual activities, even those that are hidden in encrypted data, nested files, or obfuscated sessions. This helps security teams find attacks that traditional detection methods might miss, giving them a significant advantage over attackers.

Fidelis Active Threat Detection correlates activities with MITRE ATT&CK TTPs, providing valuable context for incident response and threat hunting. Fidelis Deep Session Inspection™ enhances threat identification by analyzing nested and obfuscated files, uncovering hidden threats. The solution can also analyze encrypted traffic, both in-line and out-of-band, allowing detection of malicious activities within encrypted communications.

Active Directory Intercept provides contextual intelligence, enabling organizations to swiftly respond and prevent future attacks by understanding the extent of adversary presence.

Fidelis Active Directory Intercept™ offers comprehensive defense for complex environments by combining network traffic analysis, integrated deception, and AD monitoring. It can detect and prevent a variety of AD-related attacks, such as Active Directory reconnaissance, brute-force authentication attempts, Kerberoasting, password sniffing, and others.

Advanced AD Security Strategies

While tools like Fidelis Active Directory Intercept™ offer a robust layer of Active Directory attack and defense, organizations must also adopt best practices to fortify their AD environments.

Here's the list of some of the best practices:

- Implement Multi-Factor Authentication (MFA)
- Adopt Least-Privilege Access
- Conduct Regular Security Audits
- Enforce Strong Password Policies
- Implement Network Segmentation
- Use Privileged Access Workstations (PAWs)
- Enable Just-in-Time (JIT) Privileged Access Controls

By using these methods, companies can make it harder for attackers to get in, prevent lateral movement, and reduce the chance of large-scale security breaches.

Secure Your AD with Proven Strategies

In this Active Directory Hardening Checklist, you'll discover:

- Access Control
- Privileged Workstations
- Multi-layered Defense
- JIT Access

Download Now

The Power of Threat Intelligence and Continuous Improvement

Leveraging a range of threat intelligence feeds, Fidelis Active Directory Intercept™ effectively detects and responds to AD threats. Its intelligence continuously learns and adapts to Active Directory security requirements, building a baseline of normal behavior for identifying anomalies.

Mapping alerts to MITRE ATT&CK TTPs provides valuable context for threat-informed decisions. Organizations can enhance their AD security posture over time by leveraging insights gained from monitoring, detection, and response to improve access controls, authentication mechanisms, and overall defense layers.

With Active Directory Intercept, organizations gain the power and tools needed to effectively protect critical assets.

In Conclusion

Fidelis Active Directory Intercept™ is a powerful solution for enhancing AD security and mitigating potential threats. Its multi-layered defense approach, incorporating AD-aware network detection and response, integrated deception technology, and advanced log monitoring,

empowers organizations to detect and respond to AD threats effectively.

By leveraging contextual intelligence, threat mapping to MITRE ATT&CK TTPs, and continuous improvement mechanisms, organizations can continually enhance their AD security posture. With Fidelis Active Directory Intercept™, organizations can confidently safeguard their critical AD infrastructure and protect against evolving cyber threats.