DATASHEET

Fidelis Active Directory Intercept™

Multi-layered Defense for Active Directory

Active Directory (AD) is the cornerstone of identity and entitlements management in over 90% of organizations. It authenticates and authorizes user access to resources, provides for the storage and management of information, and deploys services such as certificates, federation, LDAP, rights management, and more. As such, AD provides the perfect launch point from which adversaries dive in deep, move laterally, escalate privileges, and conduct malicious activity, such as code execution, data exfiltration, account spoofing, and more.

Protecting AD is a primary concern for nearly every organization. But many tools fall short, missing the signs that point to an imminent attack. And once an attacker gains AD access, it's game over. They can easily vanish into the flow of expected network traffic and data access, becoming invisible to most AD protection tools.

That's where Fidelis Active Directory Intercept™ comes in.

See More. Stop More. Only with Active Directory Intercept.

Fidelis Active Directory Intercept combines AD-aware network detection and response (NOR) and integrated AD deception technology with foundational AD log and event monitoring to not just identify AD threats - but to respond swiftly. Active Directory Intercept gives you contextual intelligence so you can know exactly how, where, and how deep your adversary has burrowed into your network, along with powerful response tools and the ability to defend against future attacks.

Give your organization the power to:

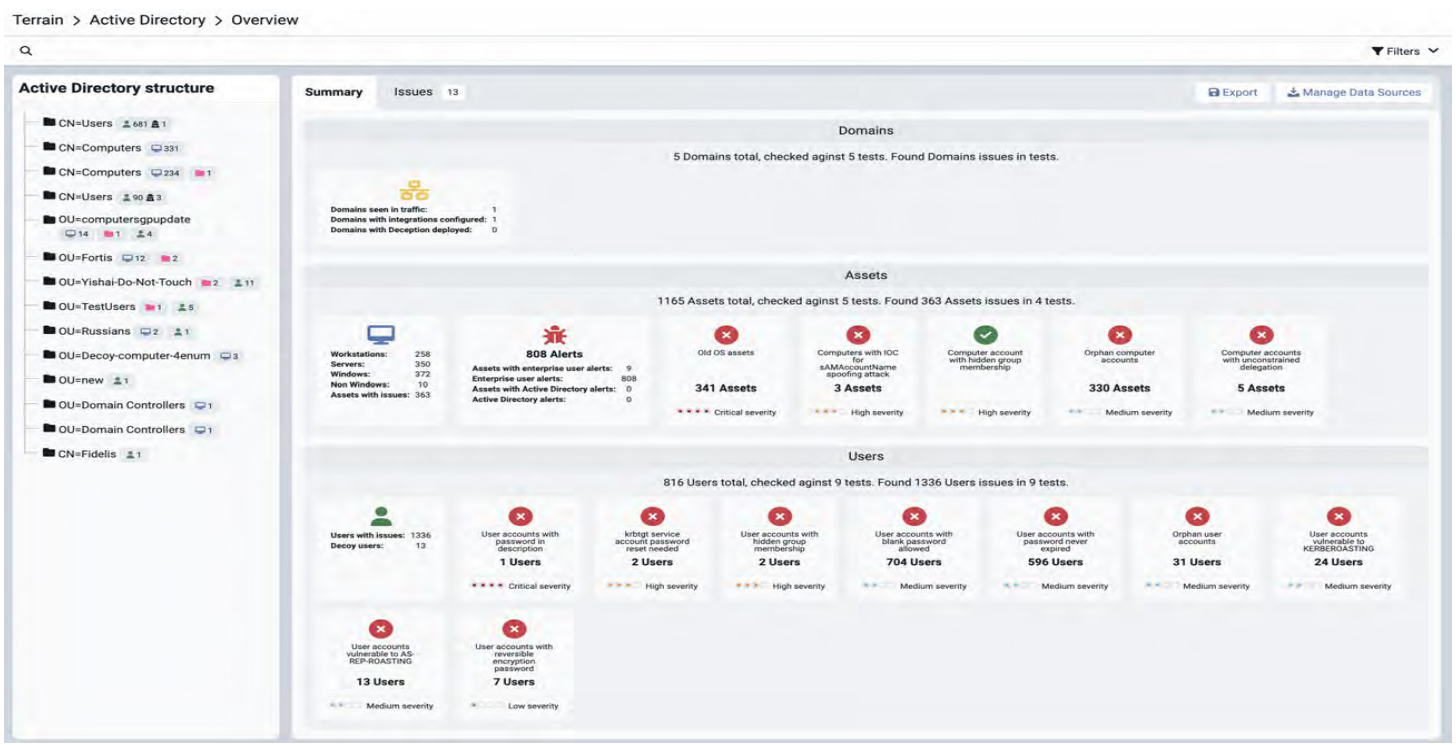
See - gain full visibility into AD objects for deep insight across your organization's resources, access paths, and more.

Detect - alert on AD misconfigurations, indicators of compromise, and active threats before they become critical security issues.

Defend - combine powerful network sensors with AD configuration monitoring and automated AD-aware deception for multi-layered defense that gives you the time and intelligence needed to study, understand, and block attacker movements.

Respond - automatically thwart adversaries with scripts and playbooks and gain powerful forensic analysis tools for real-time response to active AD threats.

Improve - rely on intelligence that learns and grows, along with powerful alert mapping to MITRE ATT&CK TTPs, to make threat-informed decisions and continually improve your AD security posture.



How Active Directory Intercept Works

With a unique combination of network traffic analysis, integrated deception, and AD monitoring, Fidelis Active Directory Intercept provides defense in depth for even the most complex environments.

Network Traffic Analysis

Fidelis Network® provides game-changing threat detection and response capabilities, both within and beyond AD, including:

- Active Threat Detection TM that correlates alerts and provides high confidence detections that map attempted AD attacks to MITRE ATT&CK TTPs
- Deep Session Inspection TM that finds threats to AD deep within nested and obfuscated files as they move across the wire.
- In-line or out-of-band encrypted traffic analysis.
- Contextual intelligence that tells you the who, what, where, and when of an attacker's movements, before, during, and after an attack.

Integrated Intelligent Deception

With full terrain mapping and risk profiling, Fidelis Deception® automatically deploys intelligent deception to stop AD attacks by:

- Knowing where attackers are likely to strike.
- Creating convincing decoys, including AD objects in on-premises and Azure AD environments.
- Placing breadcrumbs strategically throughout the network to lead attackers away from real AD users and domains
- Giving cyber defense teams time to study the threat.
- Providing high-confidence and actionable alerts that point definitively to active network threats.

Active Directory Log and Event Monitoring

Trust a foundation of AD defense that reduces the likelihood of a successful attack. Powered by Active Directory Intercept, you'll gain:

- A hierarchal view of your AD environment.
- Information on all active directory entities (user, computer, group, and domain).
- AD misconfiguration detection.
- Real-time malicious/suspicious activity detection and response.
- Detection of potential AD compromise
- Drill-down capabilities to investigate AD issues.
- Comprehensive log analysis for attack detection.

Intercept and Defeat AD Attacks and Attempts

With sensors placed strategically across your network and clouds, you'll detect, thwart, and protect against AD threats that other tools miss. Here are just a few of the AD-based threats that Active Directory Intercept detects:

- Active Directory Reconnaissance
- Active Directory anomaly detection
- Brute-force Authentication Attempts
- Extraction of DPAPI domain backup keys
- Kerberoasting
- Password Sniffing
- LLMNR Poisoning
- DCSync Attack
- DCShadow Attack

And more!

Explore More

Want to learn more about Active Directory Intercept? Give us a call or send us an email. We would love to discuss the cybersecurity needs of your unique AD environment.

About Fidelis Security®

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.