ADASSESSOR FOR CONTINUOUS VISIBILITY TO ACTIVE DIRECTORY EXPOSURES & LIVE ATTACKS

Active Directory (AD) is a Microsoft product consisting of several services to administer permissions and access to networked resources on a Windows Network. Because it is the primary source of information for all enterprise resources and seamlessly integrates business applications, it is a high-value target for attackers.

Attackers can target exposures within the Active Directory to quickly extract sensitive data on the entire domain, such as user accounts, system accounts, or trusted domain information. This data provides objects to target such as privileged accounts, groups with overlapping security rights that provide elevated privileges, or critical systems such as trusted domain controllers, production servers or databases storing sensitive data. AD contains the required information attackers need to expand their access, establish persistence, elevate privileges, move laterally, and identify targets to attack.

Active Directory security can be extremely difficult because many of these exposures aren't readily apparent unless the organization does an exhaustive audit. By identifying critical AD exposures and alerting on attacks that target them, organizations can improve their security before attackers can compromise their AD data.

DETECTED EXPOSURES:

- Dangerous Delegation
- Dangerous Trusts
- AdminSDHolder Inconsistency
- DCShadow
- Password Spray
- and many more

The Attivo Networks ADAssessor solution provides ongoing visibility into critical domain, computer, and user-level exposures for quick remediation. The solution then continues monitoring AD for activities that signify a possible attack.

CHALLENGES

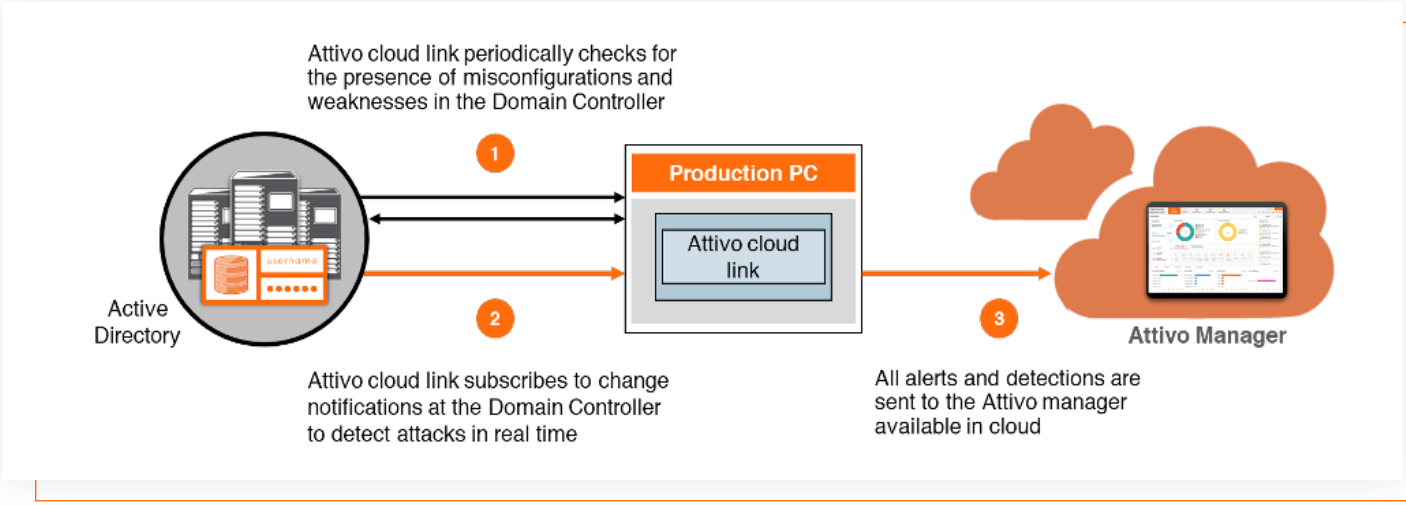
- Most organizations monitor logs for unusual behavior, which doesn't provide real-time assessment of Active Directory to detect exposures or changes in settings and policies that may introduce weaknesses for attackers to leverage
- Multi-level IT teams manage Active Directory and can introduce changes without understanding the risk or exposures that these additions can cause
- Existing security controls are not AD-aware and lack the ability to detect mass changes from brute force attacks, DCsync, DCshadow, and similar attack tactics

ADASSESSOR

The ADAssessor solution is a standalone offering that provides continuous visibility to AD exposures vulnerable to attack and detects advanced Active Directory attacks in real-time. The solution includes functions to

automatically remediate these exposures and works with the Attivo Networks ADSecure solution to provide advanced Active Directory protection.

Once an organization deploys ADAssessor, it detects vulnerabilities within their AD environment, including misconfigurations, excessive privileges, or data exposures. It then remediates those weaknesses before attackers can take advantage of them, ultimately reducing the AD attack surface and risk. Running continuously or on-demand, ADAssessor will automatically monitor AD, analyze changes, and identify new exposures that indicate possible malicious activity.



BENEFITS

- Visibility to AD security hygiene issues and actionable alerting for key exposures at the domain, computer, and identity levels
- Real-time detection of AD privilege escalation and granular restrictions for access to AD information without impacting business operations
- Continuous insights into identities and service account risk related to credentials, privileged accounts, stale accounts, shared credentials, and identity attack paths
- Easy to deploy: the solution runs from a single endpoint and doesn't require privileged access to Active Directory

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE® Shield, and its capabilities tightly align to the MITRE ATT&CK® Framework. Attivo has won over 150 awards for its technology innovation and leadership. www.attivonetworks.com