REDUCE ACTIVE DIRECTORY EXPOSURES AND DETECT LIVE AD ATTACKS

Threat actors have proven that they can evade security controls to establish a beachhead inside an organization's network. Once inside, Active Directory (AD) is one of the most common targets they go after since it provides authentication and authorization to all enterprise resources. Attackers exploit AD exposures and misconfigurations to steal the required information they need to gain privileged access and find targets to attack.

Organizations must reduce those exposures and misconfigurations and detect when adversaries target AD as part of their attack. They need solutions that offer live attack detection for activities that target AD and work together to provide constant visibility and remediation for critical domain, computer, and user-level exposures.

THE ACTIVE DIRECTORY ATTACK SURFACE

Active Directory is a prime target during cyberattacks because it is the source of truth for all resources across the enterprise. Attackers compromise endpoints and target data on the AD controllers to progress the attack, then use it to identify high-value targets, gain privileged access, and obtain domain dominance.

Traditional approaches, such as periodic Active Directory assessments or constant log analysis combined with SIEM correlation, are complicated and expensive, often resulting in attacker activities going undetected.

90% of enterprises globally use Active Directory.

Attackers target 95 Million AD accounts daily.

80% of attacks include compromising AD.

Organizations who want efficient and continuous protection of their AD infrastructure should look to the Attivo Networks Active Directory Protection solutions as innovative approaches to address their needs.

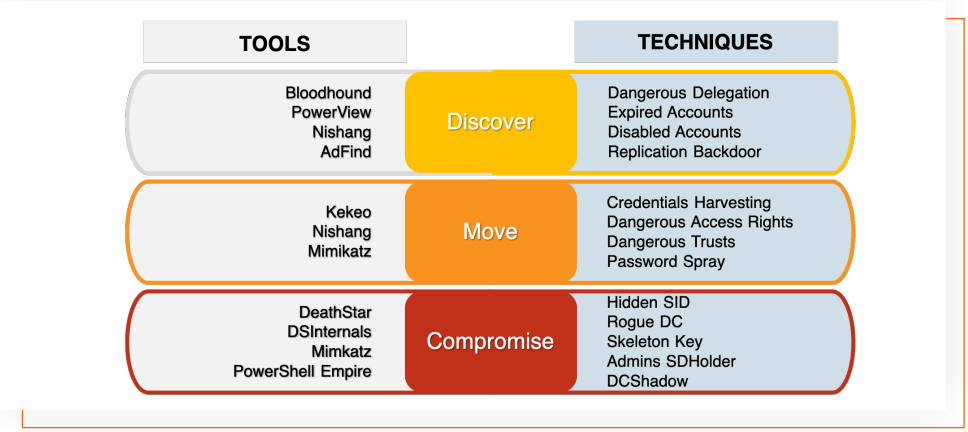

Figure 1. Examples of tools and techniques to compromise Active Directory addressed by Attivo Networks solutions

CYBER HYGIENE AND CONTINUOUS ATTACK SURFACE REDUCTION

Once attackers compromise an endpoint, they search for any useful data and credentials to facilitate their plan. The solution identifies and remediates endpoint credential exposures and misconfigurations, then continually monitors them to prevent an attacker's lateral movement. The solution's AD-related protection functions identify exposed API keys, credentials, and secrets to applications, databases, file servers, and domain controllers. It can also detect if AD privileged accounts, shadow admins, and service accounts are stored on the endpoint, creating a new exposure that attackers can leverage. By remediating these exposures before attackers can take advantage of them, defenders can reduce the attack surface they must protect and limit the lateral movement paths available to threat actors.

ATTIVO ACTIVE DIRECTORY PROTECTION BENEFITS

- Improve Active Directory Cyber Hygiene
- Continuous visibility to exposures and misconfigurations in Active Directory
- Keep unauthorized users from exploiting Active Directory
- Detect threats and stop attacks in real-time
- Reduce Active Directory attack surface
- Add detection efficiency without needing privileged access or touching production Active Directory
- Attack path visibility based upon exposed credentials and access to Active Directory
- Non-disruptive to employee access or operations
- Scales to support on-premises and cloud operations

LIVE ATTACK INTERCEPTION

Attackers query AD as part of their discovery and data gathering activities to identify high-value privileged accounts and objects to target during their attack. The solution detects when attackers make unauthorized AD queries from the endpoints. When the AD controller responds, the solution hides the sensitive or critical accounts and objects, such as domain administrators, service accounts, or domain controller information, and inserts fake results in their place. These facsimiles point to non-production locations such as black-hole ports or network decoys. The solution effectively disrupts adversarial intelligence gathering, derailing downstream attack activities that rely on accurate AD data to progress the attack.

CONTINUOUS VISIBILITY TO EXPOSURES AND PRIVILEGE ESCALATION

Attackers will search the AD controllers for exposures that enable them to conduct lateral movement, gain privileged access, or obtain domain dominance. The solution provides visibility to AD security hygiene issues, such as Kerberoasting vulnerabilities and other misconfigurations, and actionable alerting for key exposures at the domain, computer, and user levels. It offers real-time detection of AD privilege escalation and granular restrictions for access to AD information

without impacting business operations. The solution continuously monitors identities and privileged account risks related to credentials, service accounts, stale accounts, shared credentials, and identity attack paths. For example, the solution can alert on DCSync and DCShadow attacks, two tactics that are extremely challenging to detect. It also provides insight into identity entitlements and least privilege access across on-premise and multi-cloud environments.

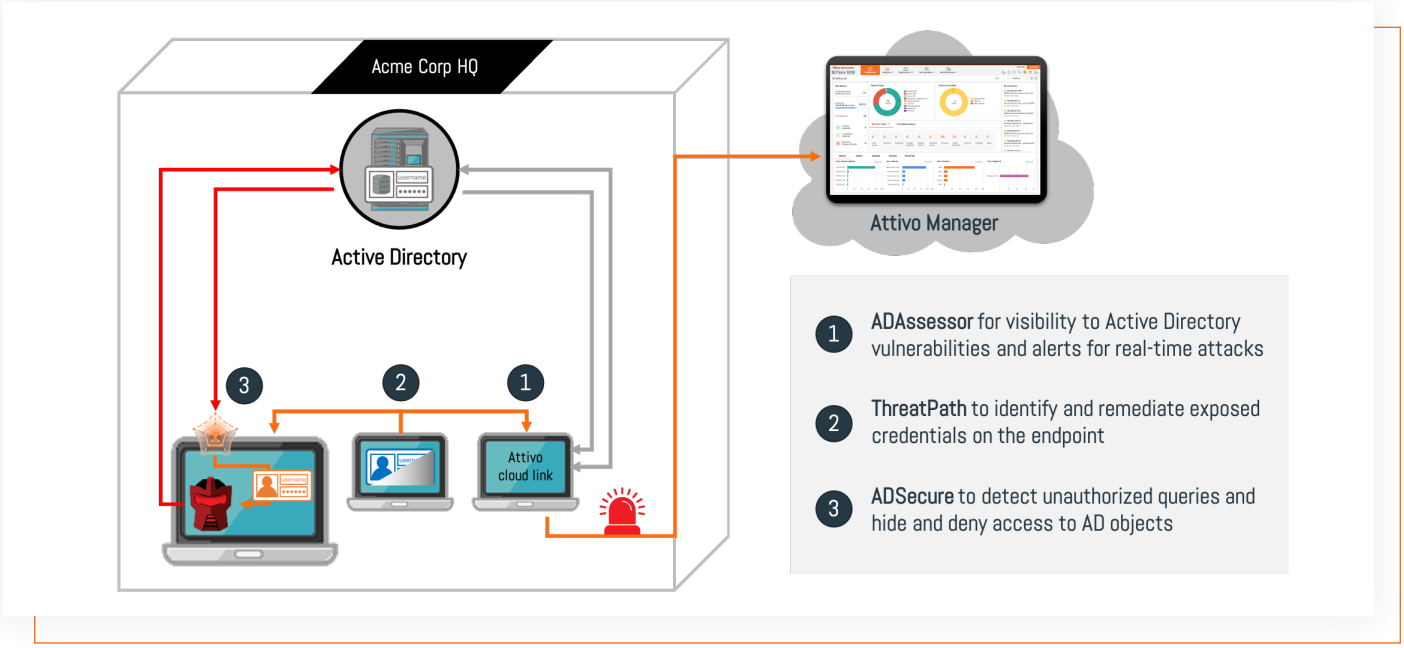

Figure 2. Graphic showing Attivo Networks Active Directory protection solutions

AD ATTACK SURFACE MANAGEMENT AND REAL-TIME ATTACK DETECTION

Attivo Networks Active Directory Protection solutions, as shown in figure 2 above, provide continuous visibility, concealment, and misdirection for AD exposures and attacks in near-real-time. The solutions function together to detect and derail domain, device, and user-level vulnerabilities and attacks without requiring excess permissions or installation on the AD controllers. Organizations deploying these solutions gain easy, efficient, and effective protection for their AD environment.

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 130 awards for its technology innovation and leadership. www.attivonetworks.com