REDUCE ACTIVE DIRECTORY EXPOSURES & 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, they often target Active Directory (AD) since it is the source of truth for all resources across the enterprise. 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 AD live attack detection and work together to provide continuous visibility and remediation for critical domain, computer, and user-level exposures.

ACTIVE DIRECTORY STATS

1. 90% of enterprises globally use AD.
2. Attackers target 95 Million AD accounts daily.
3. 80% of attacks include compromising AD.

ACTIVE DIRECTORY AS A HIGH-VALUE TARGET

Active Directory is a prime target during cyberattacks because it provides authentication and authorization to all enterprise resources. 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 AD assessments or constant log analysis combined with SIEM correlation, are complicated and expensive, often resulting in attacker activities going undetected. Organizations who want efficient and continuous protection of their AD infrastructure should look to the Attivo Networks AD Protection portfolio as an innovative approach to address their needs. The portfolio is comprised of the ThreatPath, ADSecure-EP, ADSecure-DC, and ADAssessor solutions.

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

CYBER HYGIENE AND CONTINUOUS ATTACK SURFACE REDUCTION

Once attackers compromise an endpoint, they search for valuable data and credentials to facilitate their plan. The ThreatPath solution identifies and remediates 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 and limit the lateral movement paths available to threat actors from both endpoints and the domain controllers.

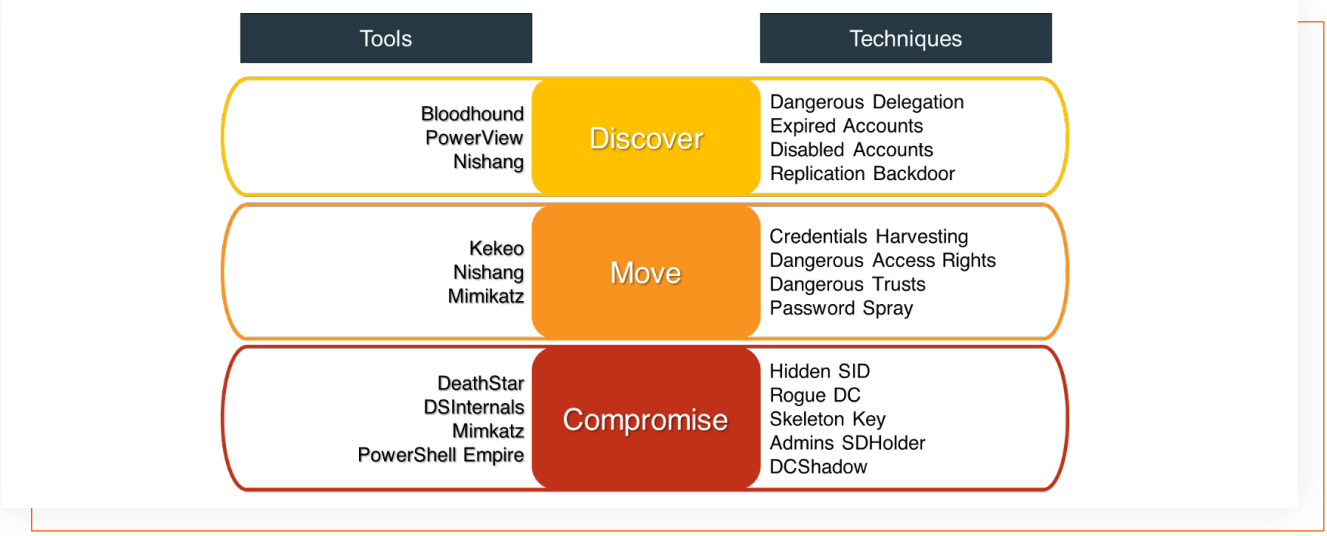

Figure 1. Examples of tools and techniques to compromise Active Directory addressed by Attivo Networks solutions

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 ADSecure-EP solution detects when attackers make unauthorized AD queries from Windows 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. This offering is for organizations that do not want to install anything on the domain controllers and work in a predominantly Windows OS environment.

Organizations can use the ADSecure-DC solution to protect against attacks from managed and unmanaged systems, IoT and OT devices, and Windows and non-Windows systems. The solution installs on the domain controllers but does not interfere with their operations. The solution identifies enumeration and attacks targeting AD and detects suspicious user behaviors using deep packet inspection and behavior analytics without false positives. The solution supports Microsoft Windows Server 2008 and later. This offering is for organizations that do not want to install sensors on all endpoints but still want AD attack detection or have non-Windows or unmanaged systems on the network.

Both solutions effectively disrupt 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 ADAssessor 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 accessing AD information without impacting business operations, providing exposure information with appropriate remediation steps. The solution continuously monitors identities and privileged account risks related to credentials, service accounts, stale accounts, shared credentials, and identity attack paths. The solution alerts on attack activities that reflect changes across multiple objects at the AD domain controllers, such as mass account lockouts or password changes. It also covers adjacent attack vectors related to AD Certificate Services (ADCS) and ADFS (AD Federation Services).

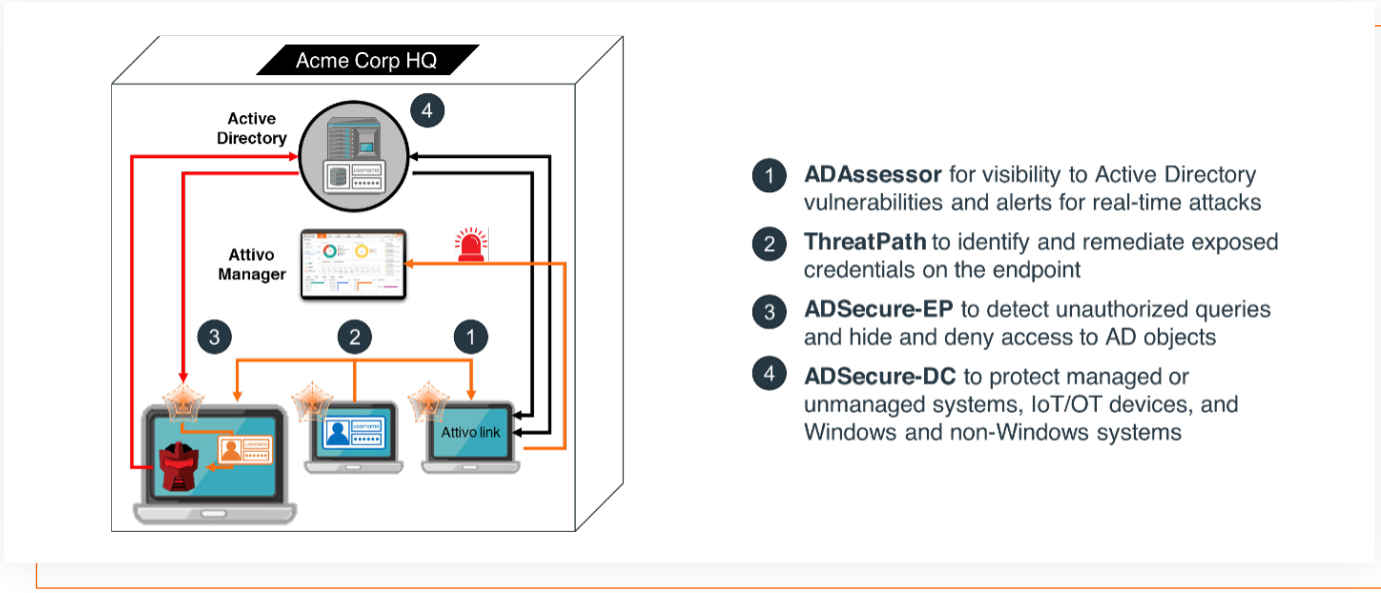

Figure 2. Graphic showing Attivo Networks Active Directory protection solutions

AD ATTACK SURFACE MANAGEMENT AND REAL-TIME ATTACK DETECTION

Attivo Networks Active Directory Protection solutions, as shown in figure 2 above, provide continuous visibility, detection, concealment, and misdirection for AD exposures and attacks in near-real-time. The solutions function together to detect domain, device, and user-level vulnerabilities and derail 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 identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. The ThreatDefend® Platform provides unprecedented visibility to risks, attack surface reduction, and attack detection across critical points of attack, including endpoints, in Active Directory, and cloud environments. www.attivonetworks.com