CHOOSING AN ACTIVE DIRECTORY VISIBILITY SOLUTION

Advanced attackers find many ways to evade security controls and infiltrate an organization's network. Once inside, they aggressively target the Active Directory (AD) infrastructure within the enterprise to advance their attacks. They compromise identities such as user, service, application, and administrator accounts to gain privileged access to the domain.

Active Directory (AD) is a high-value target for attackers, who frequently compromise it to escalate their privileges and expand their access. Unfortunately, its operational necessity means that users must have ready access to AD throughout the enterprise, making it difficult to secure. Mergers and acquisitions add to the complexity of the situation as poorly understood group settings and policies get added to the equation.

Organizations across industries currently lack detection capabilities for attacks targeting AD. They need solutions that provide visibility to AD exposures and live attack activity detection, allowing them to remediate or mitigate these security vulnerabilities before attackers exploit them.

THE IMPORTANCE OF ACTIVE DIRECTORY ATTACK DETECTION

By design, AD readily exchanges information with any member system it manages. Attackers can also leverage this access to gather information on the entire domain quietly and quickly. Security teams may not realize that attacks on AD are occurring because the activities appear as if AD is providing the data to a member system as part of normal operations.

Attackers can extract user accounts, system accounts, and trusted domain information from any compromised member system on the AD domain. They can find privileged accounts, overlapping security rights that provide elevated privileges, or essential systems to target as part of their attacks. These can include trusted domain controllers, mission-critical production servers, or databases with sensitive data. Detecting AD attacks can be difficult because, typically, organizations must manually defend against such activities.

Organizations lacking AD attack detection can't effectively protect their AD domain controllers from attackers as they seek to advance their charge or do mass encryption for conducting a ransomware attack. Existing EDR and other threat detection solutions do not detect AD attacks, leaving significant gaps for threat actors to leverage.

However, recent innovative solutions provide AD attack visibility and detection capabilities, noting that they come with varying capabilities and operating requirements. Organizations should carefully evaluate available offerings to choose the right fit for their needs.

FINDING THE RIGHT ACTIVE DIRECTORY ATTACK DETECTION SOLUTION

Requirements vary between organizations, but the following questions are a starting point to evaluating a solution.

DEPLOYMENT

- ☐ What are the deployment requirements?
- ☐ What privileges or rights does it require?
- ☐ How easily does it deploy?
- ☐ How easy is it to scale?
- ☐ Where is the management console located: on-premises or in the cloud?

ANALYSIS

- ☐ How actionable are the alerts?
- ☐ How does it present findings?
- ☐ What analysis tools does it provide?
- ☐ Can it show mappings to CVEs or MITRE?
- ☐ How much data sharing does it offer?

ATTACK DETECTION

- ☐ What AD attack detection capabilities does it offer?
- ☐ From where does it detect attacks: endpoint, domain controller, or other?
- ☐ How quickly does it alert on detection?
- ☐ What types of attacks can it detect?
- ☐ What information does it provide as part of the detection?
- ☐ How is detection information provided?
- ☐ What visibility can it provide to exposures, misconfigurations, or attack paths?

RESPONSE

- ☐ What response options does it offer?
- ☐ How much automation does it provide to initiate a response?

ATTACK SURFACE REDUCTION AND REAL-TIME ATTACK DETECTION

Attivo Networks® Active Directory protection solutions provide continuous visibility, concealment, and misdirection for AD exposures and attacks in near-real-time. The ADAssessor, ADSecure, and ThreatPath® solutions work together to detect domain, device, and user-level exposures and derail attacks without requiring excess permissions or installation on AD controllers. Organizations deploying these solutions gain easy, efficient, and effective protection for their AD environment. To learn more, visit: https://attivonetworks.com/solutions/threat-detection/active-directory-protection/

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