CHECKLIST

Attivo NETWORKS® A SentinelOne Company

# CHOOSING AN ACTIVE DIRECTORY VISIBILITY SOLUTION

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

Organizations across industries currently lack awareness of identity exposures and entitlement within their Active Directory infrastructure. They need solutions that provide visibility to these exposures, allowing them to remediate or mitigate these security vulnerabilities before attackers exploit them.

## THE IMPORTANCE OF VISIBILITY TO MANAGE THE AD ATTACK SURFACE

Attackers view identities as the primary mechanism to laterally move once they've established a beachhead inside the network. Organizations generally consider enterprise identities as a means to authenticate and authorize a user to access the network and its resources and do not always have the necessary visibility into identity and entitlement security hygiene issues or have reliable visibility into Active Directory.

This lack of visibility makes it difficult to know when identity risks and entitlement exposures resulting from misconfigurations, policies, settings, or overly permissive provisioning become vulnerabilities for attackers to target. Security teams require adequate visibility to effectively manage these security issues within AD, especially as identity attacks increase across the security landscape.

There is a new class of solutions that provide visibility to these AD security issues. They vary in capabilities and requirements. Organizations should carefully evaluate the available offering to choose the right fit for their needs.

## FINDING THE RIGHT AD VISIBILITY 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?

### ATTACK DETECTION

- □ What attack detection capabilities does it offer?
- □ How quickly does it alert on detection?

### REMEDIATION AND MITIGATION

- □ What remediation options does it offer?
- □ How much automation does it provide for remediation
- □ What mitigation information does it offer if remediation is not an option?

© 2022 Attivo Networks. All rights reserved.

### VISIBILITY

□ What level of visibility does it provide? (user device, domain)

□ What issues can it identify? (Account, policy, group, infrastructure, Kerberos security, dangerous delegations, etc.)

□ How many checks does it conduct?

□ What exposures does it include? What vulnerabilities?

□ How extensive is the coverage?

□ Does vendor or solution provide visibility from endpoint to AD to cloud?

□ How often does it update?

### ANALYSIS

□ How actionable are the alerts?

□ What framework mappings (e.g., MITRE) does the vendor provide?

□ How does it present findings?

□ What analysis tools does it provide?

□ How much data sharing does it offer?

Attivo Networks offers a variety of solution bundles to address AD and other identity visibility, detection, and protection needs.  Please visit www.attivonetworks.com for more information and 3rd party reviews from (CDM) and (eWeek).

## ABOUT ATTIVO NETWORKS®

Attivo Networks®, a SentinelOne company, provides Identity Threat Detection and Response (ITDR) and cyber deception solutions for protecting against identity compromise, privilege escalation, and lateral movement attacks. Through data cloaking, misdirection, and cyber deception, the platform efficiently prevents attacks across Active Directory, cloud environments, and devices.

© 2022 Attivo Networks. All rights reserved.