IDENTITY SECURITY CHECKLIST

Attivo NETWORKS

INTRODUCTION

Organizations have traditionally looked at identity protection to authenticate and authorize a user's access to the network and its resources. While useful, it does not provide the necessary visibility into identity security, including credential theft and misuse, entitlement overprovisioning, privilege escalation, and lateral movement. Visibility into identity system hygiene issues and vulnerabilities is also often missing.

Adding identity security should be a priority for every CISO and their teams since advanced attackers have proven they can evade security controls and infiltrate an organization's network. Once inside, they target identities within the enterprise to advance their attacks. Using the information they gather from endpoints, Active Directory, and the cloud, they compromise identities such as user, service, application, and administrator accounts to gain privileged access to the on-premises and cloud networks.

This checklist should help organizations understand identity and entitlement risks across their networks from endpoints to Active Directory to the cloud. Completing these questions will identify gaps and determine what types of solution capabilities are needed to provide visibility to exposures, vulnerabilities that create risks, and live attack activity.

VISIBILITY TO EXPOSURES AND RISKS

- ☐ How do you gain visibility to identity-related (credentials, entitlements, privileges) risk at the endpoint? In Active Directory? In the Cloud?
- ☐ How much effort is involved in identifying these identity-related risks?
- ☐ What level of visibility do you have to attack paths for attack surface risk reduction?
- ☐ What level of visibility do your tools provide? (user, device, domain)
- ☐ What issues can it identify? (Account, policy, group, infrastructure, Kerberos security, dangerous delegations, etc.)
- ☐ How often do you re-evaluate these risks?
- ☐ How do you track these risks?
- ☐ How do you visualize your results and the risk associated with those results?
- ☐ How often does this information get updated?

DETECTING ATTACKS

- ☐ How do you detect identity-based attacks at the endpoint? In Active Directory? In the Cloud?
- ☐ How much effort is involved in detecting identity-based attacks?
- ☐ How quickly can you detect identity-based attacks?
- ☐ How much data-sharing occurs between different security solutions regarding identity-based attacks?
- ☐ How do you address identity-based attacks related to lateral movement? Credential theft? Privilege escalation?

IDENTITY SECURITY CHECKLIST

Attivo NETWORKS

REMEDIATION AND MITIGATION

- ☐ What remediation options do your solutions offer?
- ☐ How much automation do your tools provide for remediation?
- ☐ What mitigation information does the solution provide if remediation is not an option?

ANALYSIS

- ☐ How actionable are your solution's alerts?
- ☐ Does the vendor provide MITRE or other framework mapping?
- ☐ How does it present findings?
- ☐ What analysis tools does it provide?
- ☐ How much data sharing does it offer?

Once one understands current security controls and their gaps, it is useful to use this information to qualify new vendor security offerings and capabilities. Most identity security solutions are coming from emerging vendors, which may mean that their coverage will be limited. We encourage security teams to look at the depth of visibility and detection provided and the ability to provide comprehensive coverage from endpoints to Active Directory to multi-cloud environments.

This paper is sponsored by Attivo Networks:

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®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Data concealment technology hides critical AD objects, data, and credentials, eliminating attacker theft and misuse, particularly useful in a Zero Trust architecture. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys obfuscate the attack surface to derail attacks. Forensic data, automated attack analysis, and automation with third-party integrations serve to speed threat detection and streamline incident response. ThreatDefend capabilities tightly align to the MITRE ATT&CK Framework and deception and denial are now integral parts of NIST Special Publications and MITRE Shield active defense strategies. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com

ANC083021
www.attivonetworks.com