CLOUD IDENTITY & ENTITLEMENT PROTECTION CHECKLIST

Attivo NETWORKS®

In the cloud, non-human identities routinely have entitlements to other resources, resulting in a significant expansion of identities and entitlements an organization must manage. The growing number of identities and entitlements within the cloud substantially increases risk, making them high-value targets for attackers. Use this checklist to evaluate current cloud identity security procedures to identify risks and gaps. Compare them against solution capabilities to address specific requirements.

QUESTIONS TO ASK IN LOOKING TO SECURE IDENTITIES & ENTITLEMENTS IN THE CLOUD

CONDUCTING ASSESSMENTS

- □ How do you perform identity and entitlement assessments today?
- □ How do you discover exposed identities and lateral movement?
- □ Are your current mechanisms automated or manual?
- □ How much effort is involved in performing assessments?
- □ What is the frequency of those assessments?
- □ How do you visualize your results and the risk associated with those results?

TRACKING IDENTITIES AND ENTITLEMENTS

- □ How many identities and entitlements are in the entire enterprise? In each cloud?
- □ How do you monitor newly created entitlements?
- □ How do you track changes to entitlements between assessments?
- □ Are you notified when entitlement changes get made to critical assets?

MANAGING IDENTITIES AND ENTITLEMENTS

- □ Which identities have Azure directory or subscription role assignments?
- □ Which identities have access to each of your critical Azure services, such as Microsoft Graph API, Key Vault, or storage accounts?
- □ Which Azure applications have multiple credentials defined? Are using delegated permissions?
- □ Which identities have access to each of your critical AWS services, such as IAM, KMS, and Lambda?
- □ Which identities have full access to those AWS services?
- □ Which identities have cross-account access within your organization?
- □ Which user accounts have MFA disabled? Are inactive?
- □ How do you view identity entitlements and exposures across platforms?
- □ How do you know what attack paths exist to your critical cloud resources?
- □ How can you track entitlement changes for a critical object?