CHECKLIST

CHOOSING A CLOUD INFRASTRUCTURE ENTITLEMENT MANAGEMENT SOLUTION

Organizations are adopting the cloud in growing numbers, but with this growth comes unanticipated security challenges with user identity management and the explosion of "non-human" identities such as applications, serverless functions, and virtual machines. Unfortunately, traditional security tools are ill-equipped to handle this explosion of resource management and, as a result, over-provision access and exasperate security risks.

THE IMPORTANCE OF VISIBILITY TO MANAGE CLOUD ENTITLEMENT EXPOSURES

Traditional IGA and PAM solutions struggle to address the unique security challenges with the cloud's granular and dynamic nature. Existing cloud security tools (CSPM, CWPP, and CASB) address specific aspects of cloud infrastructure security, but they generally lack identity and access controls. Manual methods to ensure a least-privilege approach to security do not scale in an environment with so many identities and entitlements. Existing security paradigms cannot inherently combat the new wave of identity security. This need has resulted in a new class of tools for Cloud Infrastructure Entitlement Management (CIEM), sometimes called Cloud Permissions Management (CPM).

According to Gartner, CIEM is a specialized identity-centric SaaS solution that manages cloud access risk using time-limited access controls. Leveraging analytics and machine learning to detect anomalies, CIEM manages entitlements and data governance in hybrid and multi-cloud IaaS architectures. CIEM streamlines the implementation of least privilege access controls in highly dynamic organizational IT environments.

Vendor solutions vary widely in capabilities and requirements. Organizations should carefully evaluate the available offering to choose the right fit for their needs.

FINDING THE RIGHT CIEM SOLUTION

Requirements vary between organizations, but the following questions will help security teams comprehensively evaluate a solution.

REMEDIATION AND MITIGATION

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

VISIBILITY

- ☐ What level of visibility does it provide? (Identity risks, entitlement exposures, etc.)
- ☐ What issues can it identify? (Excess entitlements, unused entitlements, dormant accounts, over-provisioning, too much privilege, etc.)
- ☐ How customizable is the risk assessment?
- ☐ How many checks does it conduct?
- ☐ What identity exposures does it include? What vulnerabilities?
- ☐ How extensive is the coverage?
- ☐ What attack path visualization does the solution provide?
- ☐ What entitlement changes does it track?
- ☐ What events does it create when impacting critical objects?
- ☐ What visibility does the vendor or solution provide from endpoints to Active Directory to the cloud?
- ☐ How often does it update?

DEPLOYMENT

- ☐ What are the deployment requirements?
- ☐ What privileges or rights does it require?
- ☐ How easy/intuitive is it to deploy?
- ☐ How well does it scale across multi-cloud environments?
- ☐ Where is the management console located: on-premises or in the cloud?
- ☐ Can the console consolidate data across endpoints, Active Directory, & clouds?

ANALYSIS

- ☐ How actionable are the alerts?
- ☐ How does it present findings?
- ☐ What analysis tools does it provide?
- ☐ How much data sharing does it offer?

ATTACK DETECTION

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

THE ATTIVO NETWORKS SOLUTION

The company's IDEntitleX solution provides actionable visibility to cloud identity and entitlement exposures so organizations can take corrective action for risky entitlements and drift from security policies. The solution makes identifying and reducing risk simple by offering intuitive and interactive graphical visualizations for cloud identities, roles, permissions, and resources.

Security teams now see misconfigurations and excess permissions that attackers can leverage to create attack paths, move laterally, and maintain persistence within the cloud 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