CYBERARK®
The Identity Security Company™

SOLUTION BRIEF

Secure Cloud Operations Teams

Protect Access Used to Migrate, Scale and Operate Applications

Security is one of the top two challenges for global organizations.[1]

99%

of security professionals agree they'll face an identity-related compromise in the year ahead, with credential theft remaining the No. 1 concern.[2]

82%

share of breaches that involved data stored in cloud environments — public, or across multiple environments.[3]

Challenge

Cloud-focused organizations face a multifaceted challenge in managing security and compliance risk. Security programs must must protect access to every workload in production, from on-premises workloads that are being slowly decommissioned to newly migrated, elastic workloads and cloud-native architectures.

Reducing risk and meeting compliance across these environments requires consistent identity security practices. Cloud transformations create specific risks, such as infrastructure misconfigurations for lift-and-shift apps, compromised access to elastic virtual machine (VM) and database workloads, and lateral movement caused by insufficient entitlements management for the explosion of identities in cloud environments.

Another source of risk is poor adoption of privileged access management (PAM) controls within cloud operations teams primarily attributed to subpar user experiences with shared access models. Cloud and DevOps teams migrating, scaling and adjusting workloads need both system and operational access.

System access describes the use of dedicated accounts and credentials, such as IaaS root and registration accounts or admin accounts for SaaS apps. Operational access describes access provisioned for ongoing cloud operations, such as federation to identity and access management (IAM) roles used to migrate workloads, adjust scaling policies for elastic VMs and database services, and configure cloud service provider storage and networking services.

To secure ongoing cloud operations, organizations must protect both system and operational access. Yet maintaining separate processes and technologies for different environments creates extra overhead,

[1] Flexera 2023 State of the Cloud Report

[2] CyberArk 2023 Identity Security Threat Landscape Report

[3] IBM Security Cost of a Data Breach Report, 2023

inefficient processes, and a lack of visibility. And siloed reporting and monitoring practices across environments can slow down audit processes or even cause compliance gaps.

To ensure operational resilience and meet compliance, organizations must address these interconnected issues.

Solution

The CyberArk Identity Security Platform helps protect the high-risk access operations teams use to migrate, scale and operate infrastructure and services for internal and customer-facing applications. The platform provides defense-in-depth control on access for cloud operations, SRE, platform engineering and DevOps teams – with native workflows to facilitate end-user adoption.

CyberArk unifies support for both shared and federated access to long-lived systems, elastic workloads and cloud-native services supporting customer-facing or internal applications. End users can securely and natively access cloud services via both web console and CLI, while security teams can fully automate onboarding and offboarding processes, facilitating a faster time to compliance.

To secure access to cloud-native services, organizations can pursue a Zero Standing Privileges (ZSP) approach. CyberArk replaces always-on entitlements with just-in-time elevation to roles scoped with least privilege permissions. Roles and entitlements are assigned on the fly, reducing the risk of credential theft and lateral movement as stolen passwords will have no permissions. Meanwhile, users retain their preferred workflows and access rights once authenticated in line with Zero Trust principles.

- Secure and native user experience for:
  - System access using shared accounts and credentials.
  - Operational access using federation to cloud IAM roles.
- Protect administrative access to infrastructure across all environments including:
  - Datacenter servers, domain controllers, databases, etc.
  - SaaS apps.
  - Elastic VM, database, and K8s workloads.
  - Cloud-native services.
- Satisfy audit and compliance requirements for frameworks including:
  - AICPA SOC 2.
  - NIST.
  - PCI DSS.
  - AWS, Azure and GCP Well-Architected Frameworks.

For operational access to elastic workloads, the platform provides seamless, just-in-time access. Attribute-based access control and adaptive multi-factor authentication (MFA) authorize and authenticate users, while session isolation prevents the spread of malware.

CyberArk helps organizations consistently satisfy audit and compliance with comprehensive reporting on the use and granting of admin access, access certification, and automation of privileged lifecycle management. Meanwhile, session audit trails and recordings streamline audit reviews.

With thorough identity security controls in place, organizations can consistently satisfy audit and compliance requirements – while securing their digital transformation.

Learn more about how to secure your **cloud operations teams**.

CYBERARK®

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.