Securing IT and Cloud Operations

CYBERARK

Modernizing IT Security in Multi-Cloud Environments

SOLUTION BRIEF

CyberArk is a Leader in the 2024 Gartner® Magic Quadrant™ for Privileged Access Management

REDUCE RISK AND INCREASE ROI WITH CYBERARK

For the past decade, 93% of organizations suffering two or more identity-related breaches in the past 12 months.[1]

89% of organizations adopt a multi-cloud approach.[2]

CyberArk customers achieve 309% average three-year ROI.[3]

[1] CyberArk, "2024 Identity Security Threat Landscape Report," May 2024.

[2] Flexera, "Flexera 2024 State of the Cloud Report," March 2024.

[3] IDC White Paper, sponsored by CyberArk, "The Business Value of CyberArk," IDC #US52652224, November 2024.

Challenge

Navigating Risks in Evolving IT and Cloud Environments

IT and cloud environments are evolving, and new attack methods are emerging. However, the primary cybersecurity risk remains constant — compromised identities and credentials.

Cloud-focused organizations face a multifaceted challenge in managing security and compliance risks. Cloud transformations create risks such as infrastructure misconfigurations, compromised access to elastic virtual machines (VM) and database workloads, and lateral movement caused by insufficient entitlements management. Security programs must protect access for every identity, from on-premises to elastic workloads and cloud-native architecture and holistically protect both system and operational access.

Failing to implement a proper identity security posture can lead to failed audits or non-compliance, resulting in financial penalties, business delays and erosion of stakeholder trust. But that's nothing compared to the disruption a data breach can cause to a business's reputation and performance. Another source of risk is poor adoption of privileged access management (PAM) controls within cloud operations teams.

Managing Privileged Access in Complex Environments

System access describes using dedicated accounts and credentials, such as built-in system accounts or shared admin accounts. For cloud operations teams, this also includes IaaS root and registration accounts or admin accounts for SaaS apps. Examples include accounts used to access Windows and Linux servers, domain controllers and databases, or root and admin accounts for SaaS and IaaS environments.

Operational access describes the use of accounts and roles provisioned for ongoing IT or cloud operations, such as federated access to identity and access management (IAM) roles used in the administration of SaaS apps, elastic workloads and VMs and cloud-native services.

Another challenge is high-risk access for third-party vendors. Without consistent visibility and control, external privileged access exposes organizations to additional risks of breaches, failed audits, or the inability to receive cyber insurance. Maintaining separate solutions, processes and technologies for different environments creates extra overhead, inefficiency, and lack of visibility. Board-level pressures regarding Zero Trust frameworks and persistent ransomware threats further complicate this challenge. Organizations must address these interconnected issues to ensure operational resilience and meet compliance.

Applying privilege controls in native workflows improves adoption, increasing IT team productivity by 49%.[4]

PROTECT HIGH-RISK ACCESS IN EVERY ENVIRONMENT

Secure administrative native access to infrastructure across all environments:

- Windows and Linux servers
- SaaS apps
- Elastic VMs, database and Kubernetes workloads
- Cloud-native services
- System access using shared accounts and credentials
- Operational access using federation to cloud IAM roles

Extend to secrets management:

- Secure, rotate and deliver credentials used by service accounts
- Eliminate hardcoded passwords in scripts and automation tools

Extend controls to third-party vendors:

- Provision external JIT access without VPNs, passwords, agents, or corporate devices
- Securely provide offline access to credentials in air-gapped environments
- Maintain central control of session isolation, monitoring, and recording

Satisfy audit and compliance frameworks:

- AICPA SOC 2
- NIST
- PCI DSS
- DORA

Solution

Enhancing Privileged Access Management

The CyberArk Identity Security Platform helps protect the high-risk access of IT, cloud operations, SRE, platform engineering and DevOps teams — with native workflows in every environment. The platform supports shared and federated access to long-lived systems, elastic workloads and cloud-native services.

End users can securely and natively access cloud services via the web console and CLI, while security teams can fully automate processes, accelerating time to compliance. Key PAM controls, including credential management, rotation and session isolation, minimize the risk of shared system accounts' privileged access and reduce risk by isolating sessions and using credentials without exposing them to users or machines. This lowers the number of unmanaged credentials and users with local admin rights and standing access while increasing the number of secured IT target systems. Additionally, session isolation and protection prevent lateral movement and limit malware spread.

Comprehensive Identity Security

Organizations can implement privilege controls for operational access required to maintain, migrate, and scale systems on-premises and in the cloud. Attribute-based access control and adaptive multi-factor authentication (MFA) are utilized to authorize and authenticate users, while session isolation prevents the spread of malware.

Organizations can pursue a Zero Standing Privileges (ZSP) approach to secure access to cloud-native services. CyberArk replaces always-on entitlements with just-in-time (JIT) 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. Native user experience and technology integrations improve adoption, reduce risk and increase operational efficiencies. CyberArk protects the most targeted users with strong authentication and endpoint privilege controls.

CyberArk helps organizations satisfy a wide range of audit and compliance requirements. The platform provides comprehensive reporting on using and granting admin access, access certification, and automation of privileged lifecycle management. Meanwhile, centralized session audit trails and recordings with built-in risk scoring save valuable time and resources. With a holistic identity security program, organizations can secure digital transformations and achieve risk reduction and audit and compliance outcomes.

Learn more about how to secure IT admins.

[4] IDC White Paper, sponsored by CyberArk, "The Business Value of CyberArk," IDC #US52652224, November 2024.

Gartner® Magic Quadrant™ for Privileged Access Management, by Abhyuday Data, Michael Kelley, Nayara Sangiorgio, Felix Gaehtgens, Paul Mezzera, 9 September 2024