CYBERARK®
The Identity Security Company™

SOLUTION BRIEF

# Secure IT Admin Access Across All Infrastructure

## Redefine Your Privileged Access Management Program

## Challenge

IT environments are evolving. New attack methods are emerging. But the primary cybersecurity risk — compromised identities and credentials remains constant. And the powerful accounts and credentials administrators use are the top targets. Once attackers gain initial access, they move laterally and escalate privileges until they can exfiltrate data, disrupt business or deploy ransomware.

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 business reputation, performance and continuity.

Securing administrative access across hybrid and multi-cloud IT is increasingly complex. As IT evolves, organizations must holistically protect both system and operational access.

System access describes the use of dedicated accounts and credentials, such as built-in system accounts or privileged accounts shared by admins. 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 operations, such as federated access to identity and access management (IAM) roles used in administration of SaaS apps, elastic workloads and cloud-native services.

**99%**

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

**82%**

share of breaches that involved data stored in cloud environments — public, or across multiple environments.[2]

High-risk access for third-party vendors is another challenge. Without consistent visibility and control, external privileged access exposes organizations to additional risks of breaches, failed audits or inability to receive cyber insurance.

Maintaining separate solutions for different environments creates overhead, inefficiency and limited visibility across systems. And board-level pressures regarding Zero Trust frameworks and persistent ransomware threats further complicate this challenge.

[1] CyberArk 2023 Identity Security Threat Landscape Report
[2] IBM Security Cost of a Data Breach Report, 2023

- Secure administrative access to infrastructure across all environments:
  - Windows and Linux servers, databases
  - SaaS apps
  - Elastic VM, database and Kuberenetes workloads
  - Cloud-native service
- 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 access just-in-time 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.
- Deliver PAM controls to machine accounts used by the IT organization and eliminate hardcoded passwords to maintenance scripts and automation tools.

CyberArk has been named a Leader in the 2023 Gartner® Magic Quadrant™ for Privileged Access Management.

## Solution

Privileged access management (PAM) capabilities delivered from the CyberArk Identity Security Platform secure high-risk access for IT teams across all environments.

Essential PAM controls like credential management, rotation and session isolation greatly reduce the risk of standing privileged access with shared system accounts. Sessions are isolated and credentials are used directly with the target system, without ever exposing them to the user or machine.

Security teams can also apply defense-in-depth controls to operational access used to maintain, migrate, and scale systems on-premises or in the cloud. Across shared and federated access models, the platform offers role-specific least privilege just-in-time (JIT) and Zero Standing Privilege (ZSP) workflows.

Native user experience and technology integrations improve IT adoption, scaling risk reduction benefits and enabling greater operational efficiency. CyberArk helps protect the working environment of the most targeted users in the organization with strong authentication and endpoint privilege controls.

PAM controls deliver measurable risk reduction, such as significantly reducing the number of unmanaged credentials, users with local admin rights and users with standing privileges — all while increasing the number of IT target systems secured. Session isolation and protection also prevent lateral movement and limit the spread of malware.

CyberArk helps organizations satisfy a wide range of audit and compliance requirements. The platform provides comprehensive reporting on the use and granting of 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 PAM program in place, organizations can achieve their intended risk reduction, audit and compliance outcomes — while securing their digital transformations.

Learn more about how to **secure IT admin access**.

Gartner® Magic Quadrant™ for Privileged Access Management, by Felix Gaehtgens, James Hoover, Michael Kelley, Brian Guthrie, Abhyuday Data, 5 September 2023.

*GARTNER is a registered trademark and service mark, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

CYBERARK®