CYBERARK®
The Identity Security Company™

DATA SHEET

Secure Infrastructure Access

The Challenge

As IT environments evolve and new attack methods emerge, the primary cybersecurity risk remains constant – compromised identities and credentials. Once attackers gain initial access, they move laterally and escalate privileges until they can exfiltrate data, disrupt business, or deploy ransomware. Failing to implement proper session management capabilities can lead to failed audits or non-compliance, resulting in financial penalties, business delays and erosion of stakeholders' trust. As environments evolve, organizations must protect privileged sessions across both system access and operational access.

'System access' refers to privileged sessions to specific systems with dedicated accounts and credentials, such as built-in system accounts or privileged accounts shared by admins. For example, accounts used to access Windows and *nix servers, domain controllers and databases, or root and admin accounts for SaaS and IaaS environments. 'Operational access' refers to the use of both accounts and roles provisioned for ongoing IT operations, such as federated access to identity and access management (IAM) roles used in the administration of SaaS apps, elastic workloads and cloud-native services.

Maintaining a strong security posture without disrupting employees' work is challenging, as organizations need solutions that are easily deployed and managed.

The Solution

The CyberArk Identity Security Platform offers a nonintrusive, lightweight, agentless SaaS solution for isolating and monitoring privileged sessions to organizational assets across hybrid and multi-cloud environments. Access may be provisioned with vaulted credentials without exposing them to the user or machine, or without credentials in Zero Standing Privileges (ZSP) workflows.

SECURE NATIVE ACCESS TO INFRASTRUCTURE ACROSS ALL HYBRID OR MULTI CLOUD ENVIRONMENTS:

1. Windows & *nix servers.
2. Elastic VM, databases & Kubernetes.
3. Cloud-native services.

UNIFIED SUPPORT FOR:

- Access with vaulted credentials.
- Access with Zero Standing Privileges.

SESSION MANAGEMENT CAPABILITIES ENABLE:

- Secure access with either vaulted credentials or Zero Standing Privileges (ZSP).
- Session isolation, monitoring and recording.
- Unified audit view.
- Lightweight deployment.
- Reduced Total Cost of Ownership (TCO).

The solution offers native session management and centralized audit of isolated privileged sessions to workloads to prevent the spread of malware—without sacrificing user experience in RDP, SSH, databases and Kubernetes sessions.

For access to long-lived systems, the solution employs vaulting technology to securely manage privileged accounts, generating detailed session audits and video recordings for all IT administrator or developer sessions on remote machines. CyberArk ensures users access the target machines through fully isolated sessions without exposing privileged account credentials or their client applications. Instead, credentials are securely stored in the CyberArk Vault. When an access request is made, the solution verifies the user's permissions against access control policies stored in Safes and retrieves the necessary credentials. The end user maintains an active session on the target machine for the duration specified in the settings.

For access with Zero Standing Privileges (ZSP), the authorization is done with attribute-based access (ABAC) policies which define both the available platform resources and the level of privileges assigned to the user. Upon session termination, the user's access is revoked, preventing standing access. ZSP provisioning varies by target type and ensures secure, temporary access without persistent credentials. The access is managed according to specified policies and access rules, with all sessions fully isolated to prevent the spread of malware.

How it Works

When users access a target machine using their preferred client (e.g., SSH, RDP, database, or Kubernetes), the VPN-less connection request is secured with multi-factor authentication (MFA). Then, the request is directed through the lightweight connector which authenticates the user via the organization's directory service or identity provider. Access with vaulted credentials and Zero Standing Privileges (ZSP) workflows require different authorization mechanisms to allow access to targets. The lightweight connector creates an encrypted and secure reverse tunnel between the CyberArk service and the target machine. Once authorization is complete, native access is granted.

SESSION MANAGEMENT WITH CYBERARK HELPS ORGANIZATIONS:

- Deliver measurable cyber-risk reduction.
- Satisfy audit and compliance.
- Enable operational efficiencies.

About CyberArk

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

CYBERARK®