Securing All Secrets

Centrally Manage and Secure Secrets for all Machine and Non-human Identities

CYBERARK

SOLUTION BRIEF

HIGHLIGHTS

Eliminate vault sprawl: Improve security with centralized management of secrets across the enterprise's hybrid and multi-cloud environments for all types of applications including COTS, RPA, .Net, Java, mainframe, DevOps tools, containers and cloud services.

Accelerate developer productivity: Flexible solutions "meet devs where they are" with cloud-agnostic APIs and transparent use of native vaults. Code accelerators and the industry-leading range of integrations for third-party software and tools increases developer productivity.

Run at enterprise scale and performance: Architected to meet the needs of large enterprises running apps in hybrid, cloud, containerized and mainframe environments. Addresses the elastic, huge volumes of secrets, latency and resiliency needs of global operations.

Simplify and automate secrets management: SaaS options, code accelerators, automation tools, out-of-the-box integrations and UI wizards simplify securing and managing secrets.

Challenge

Securing secrets everywhere, including in cloud and hybrid IT environments, is essential to any business, and no organization wants to address the implications of a breach. However, with a broad range of applications and identities in on-premises and cloud environments, securing secrets across the entire organization can become increasingly complicated. Key challenges include:

- **Security risks from secret and vault sprawl.** The rapid growth of secrets across multi-cloud and hybrid environments increases complexity and risk. Hardcoded, unmanaged secrets in source code and repositories expose organizations to breaches and unauthorized access, making robust secrets management essential to secure critical systems and reduce the attack surface.
- **Manual secrets management is error-prone, costly and inefficient.** Reliance on manual processes often leads to human mistakes, inconsistent practices and delays in critical tasks like secrets rotation — if it happens at all — leaving organizations vulnerable and driving up operational costs.
- **Audit findings.** Failure to meet basic security requirements or provide proof of compliance can result in costly downtime and productivity losses. Without audit trails and centralized visibility into security policies, organizations struggle to enforce controls and demonstrate compliance with regulatory and internal standards.
- **Overstretched security and IT teams.** With limited resources and expanding responsibilities, teams struggle to protect the organization effectively. Scalability and flexibility are critical as organizations manage hundreds of on-premises and cloud applications, each handling secrets with its own security policies and rotation schedules. This fragmentation complicates management, widens security gaps and limits adaptability to evolving environments and requirements.

> The attack surface is vast. And it is not only people; there are non-human identities that every organization needs to secure, control and manage... We vault and rotate tens of thousands of credentials used by applications and manage more than 40 million API secrets calls a month."
>
> –Senior Leader, Enterprise Security Team, Cisco

Read Customer Story

Solution

CyberArk's solution significantly improves security by centrally managing and securing secrets for a broad range of applications and machine identities in cloud and hybrid IT environments. Now, organizations can replace hardcoded and unmanaged secrets with rotated and dynamic secrets, support developer's preferred workflows and simplify on-boarding third-party software with hundreds of certified integrations.

The solution improves security by securing secrets across all environments, and specifically:

- **Centrally secures all application identities and eliminates vault sprawl.** An integrated platform gives security teams centralized management and rotation of secrets used by a broad range of applications and cloud workloads running within hybrid, cloud and multi-cloud environments. It eliminates vault sprawl and simplifies audit processes.
- **Secures Kubernetes environments and secrets used by DevOps tools.** Helps ensure DevOps tools and workloads in Kubernetes environments can securely access resources. It enables cloud portability by providing the same experience, regardless of the cloud or hybrid environment.
- **Improves operational efficiency** by automating security processes, reducing manual effort and eliminating human error. Seamlessly integrates security into existing workflows, avoiding disruptions to development teams. With hundreds of out-of-the-box integrations, it accelerates the secure deployment of third-party software, cloud and development environments, ensuring faster time-to-value. The intuitive user interface simplifies adoption, reducing the learning curve and enabling teams to quickly implement and maintain security best practices.
- **Secures IVS, COTS, RPA, DevOps tools and home-grown software.** Hundreds of partner certified out-of-the-box (OOB) integrations simplify securing a vast range of tools and third-party software. Applies strong authentication to applications requesting credentials.
- **Automates, simplifies and guides security processes.** SaaS options and automation tools increase security team productivity and enable adoption of security processes at scale to help reduce cyber debt. Accelerators and code examples increase developer productivity.

For additional information or to schedule a demo contact sales@cyberark.com or learn more about securing all secrets.