CYBERARK®
The Identity Security Company™

SOLUTION BRIEF

Secure Cloud Workload Identities

Transparently Secure Secrets and Developer Access to Cloud Workloads and Resources

- **Accelerate dev and ops with powerful, secure access:** Give developers and cloud ops secure access to native services, while providing security with control of the cloud provider's native services.
- **Avoid changes to developer workflows:** Flexible solutions "meet devs where they are", includes transparent integrations with native vaults, cloud-agnostic APIs, automated secrets rotation and dynamic secrets.
- **Centrally manage and discover secrets:** Integrated platform centrally manages secrets across cloud environments. Discovers and gains insights on vaulted secrets and secures access to workload identities.
- **Meet enterprise scale and resilience needs:** Unique architecture provides high performance and high availability while leveraging the cloud provider's regions and availability zones.

Challenge

Securing cloud workloads, machine identities and access is essential to any digital business, and no organization wants to address the implications of a breach, but as cloud operations scale, securing cloud environments can become increasingly challenging. Key challenges include:

- **Not securing all identities.** Digital businesses use a mix of human and machine identities. While the mix shifts from mostly human identities during development, as applications are deployed machine identities will likely dominate. Attackers will exploit any weak points to get a foothold. The result is that enterprises are not secured unless access and secrets are secured and managed.
- **Over provisioning access.** Developers, platform engineers and workloads all need secure access, but with a mix of identities, access types, cloud services, roles, multiple clouds, accounts and subscriptions, it rapidly gets too complicated to effectively manage and apply the right controls. The result is over provisioned access and creative workarounds to avoid controls — ultimately increasing security risks and expanding the attack surface.
- **Secrets and vault sprawl.** Sprawl makes managing secrets difficult and increases the enterprises risk profile as there is no single "source of truth." With sprawl, secrets cannot be shared securely across vaults and rotation is at best infrequent.
- **Unmanaged secrets.** When organizations are unaware of unmanaged secrets such as in native vaults, they expose the enterprise to unknown levels of risk.
- **Over stretched security teams.** Too often, security teams face an expanding cyber debt while challenged with more responsibilities to protect the organization and limited resources.

"Digital transformation at TIAA is all about improving customer services and business operations, so we always want to increase the speed of deployment."

LEAD SECURITY ENGINEERING MANAGER, TIAA

Read Customer Story

Solution

CyberArk's solution is designed to centrally secure machine identities and transparently provide developers, site reliability engineers (SRE) and platform engineering secure access to native cloud services. All without changes to developer workflows.

The solution improves security across cloud environments, and specifically:

- **Secures dev and ops access to native services.** Provides DevOps admins, devs and platform teams secure native access to cloud consoles and services. The centralized approach reduces risk of over provisioning by implementing least privilege with on-demand elevation, and applying the principles of Zero Standing Privileges and Zero Trust.
- **Centrally secures all identities and eliminates vault sprawl.** Integrated platform gives security teams centralized management and rotation of secrets across cloud and multi-cloud environments, which eliminates vault sprawl and simplifies audit processes.
- **Transparently discovers and secures secrets in built in-vaults.** Enables the security team to centrally manage, rotate and enforce unified policies on secrets in the cloud service provider's native (built-in) vaults. Discovers and provides insights on vaulted secrets, including unmanaged secrets.
- **Secures Kubernetes environments and secrets used by DevOps tools.** Helps ensure DevOps tools and workloads in Kubernetes environments can securely access resources. Enables cloud portability by providing the same experience regardless of the cloud environment.
- **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 and resources contact **sales@cyberark.com** or learn more about how to secure your **cloud workload identities**.

CYBERARK®