Securing Secrets and Certificates Within CSPs

CYBERARK®

Centrally Discover and Manage Machine Identities While Enabling Native Access to the Cloud Service Provider's (CSP) Built-in Capabilities

SOLUTION BRIEF

HIGHLIGHTS

- Enables security teams to better manage and reduce risk by discovering certificates and secrets across their cloud environments and centrally managing security for machine identities across the entire enterprise.
- Accelerates risk reduction by working with the cloud provider's native (built-in tools) while avoiding changes to the developer or operation team's workflows.
- Helps drive increased efficiency and faster, more secure deployments by automating key machine identity security functions, including secrets rotation and certificate renewal.
- Reduces errors by eliminating manual processes. Simplifies achieving audit and compliance goals.
- Meets the dynamic needs of enterprises by supporting cloud, multi-cloud and hybrid environments. Helps future-proof against emerging challenges.

Challenges

Security teams face challenges in effectively managing the often vast and rapidly growing numbers of certificates, secrets and machine identities used across the organization's cloud environments, even when the CSP's built-in services are widely used.

- **High cost of failure from outages and breaches.** The cost cannot be overstated. Outages caused by expired certificates and stolen credentials cause significant operational disruptions and can severely damage the organization's reputation and brand. Additionally, these failures increase the compliance and audit burden.
- **Lack of visibility increases risk.** Too often, the security teams have little visibility to the various secrets stores, secrets and certificates created by development and operations teams using the cloud provider's native tools. Vault sprawl presents a significant challenge, and without comprehensive visibility, risk exposure remains unknown and difficult for security teams to assess and manage.
- **Native tools are widely used but have limitations.** While loved by developers, they typically only support the cloud provider's environment. Additionally, their limited functionality often does not meet the security team's needs, such as secrets rotation, providing a centralized view of machine identities and the ability to support external CAs. Some CSPs also promote vault sprawl as a best practice for project teams.
- **Machine identities are increasingly complex to secure.** As the industry moves towards reduced certificate validity periods, renewals become more frequent. Also, issues with some certificate authorities (CAs) have required many certificates to be rapidly replaced. Multi-cloud, hybrid environments and shadow IT practices further increase complexity. Additionally, emerging technologies, such as quantum computing and AI, add another layer of complexity and unpredictability.
- **Need to automate more and avoid errors.** It's not getting any easier. Security teams are increasingly required to do more to secure their machine identities but with limited resources. Without automation, security teams cannot keep pace with the dynamic nature of cloud environments, leading to potential security gaps and operational setbacks. Also, manual processes like discovery, renewal and rotation are inefficient and highly error-prone.

SOLUTION BRIEF

CYBERARK®

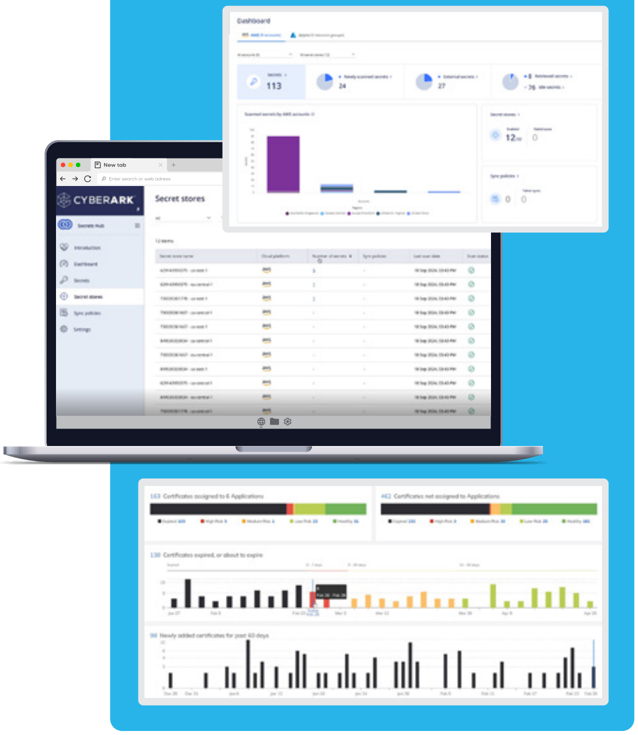
Solution

Now, security teams can more effectively and efficiently discover and manage secrets and certificates in organizations that are using the cloud provider's built-in capabilities. It's all transparent to developers and operations, without requiring changes to their workflows. Additionally, security teams now have the flexibility to centrally manage machine identities across multi-cloud and hybrid environments.

Specifically, the solution improves security across cloud environments by:

- **Centrally securing machine identities across cloud environments.** Strengthens security and operations by discovering, managing, rotating and renewing secrets and certificates across the entire enterprise, including those already managed using the cloud provider's native (built-in) capabilities. All without requiring changes to existing developer and operations workflows.
- **Discovering and establishing an inventory of certificates and secrets.** Enables security teams to prioritize risk reduction by discovering and building an inventory of certificates and secrets across the enterprise's entire cloud estate. This enables security teams to prevent expired certificates, unmanaged and insecure credentials from causing security incidents and operational outages.
- **Simplifying and automating machine identity security processes.** Helps increase efficiency and consistency by automating the entire certificate lifecycle management process. Simplifies securing and managing machine identities with automation tools, code accelerators, user interface wizards and out-of-the-box integrations, including those with third party CAs.
- **Helping to achieve the organization's audit and compliance goals.** Replaces manual processes with automated processes that provide repeatability, reduce risk and meet audit requirements. Enables security to manage, rotate and renew secrets and certificates based on policy. Centrally logs machine identity security activities to help meet audit requirements.
- **Proactively preparing for future and emerging challenges.** Automated certificate renewal processes simplify addressing mandates to renew certificates more frequency, such as due to shrinking validity periods or to address CA issues. Additionally, the solution is continuously evolving to take advantage of AI technology and prepare for quantum computing.

Solution Provides Powerful Discovery Tools



For additional information or to schedule a demo contact sales@cyberark.com or learn more about securing machine identities in your cloud environment.

CYBERARK®