CYBERARK®

Why It's Critical to Secure Application Secrets Across Your Enterprise

By Kurt Sand

General Manager, DevSecOps

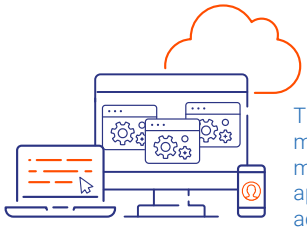
Like most organizations, you've likely fast-tracked a major IT or digital initiative in the last few years. From moving infrastructure into the cloud (public, private or most likely a mix of both), to adopting agile development methodologies like continuous integration and delivery (CI/CD), these transformative projects are key to unlocking operational efficiencies and building a more resilient enterprise. They have also led to a massive increase in applications and robotic process automation (RPA) bots — as well as the secrets (SSH keys, API keys and other credentials) used to authenticate these machine identities.

The number of non-human, or machine, identities is growing exponentially, with both types requiring secrets to perform their jobs. To safeguard valuable corporate assets, privilege-centric protections must extend across human and non-human identities, with secrets management as an integral piece of a comprehensive Identity Security program.

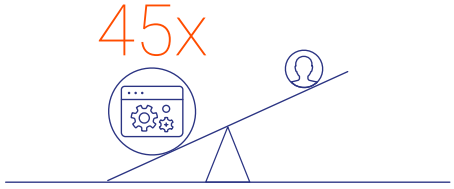
Secrets Are Everywhere

Secrets are highly attractive targets for attackers. Spread across application types and tech generations in your IT environment — from mainframe to DevOps tools to cloud-native — keeping tabs on all your secrets is difficult; securing all your secrets is even harder.

While security teams have gotten better at securing secrets in production, SolarWinds, Codecov and other high-profile breaches have demonstrated attackers' collective "shift left" to target vulnerable development and testing environments, as well as production. Many of the tools used to orchestrate the development and delivery of custom-built cloud applications require powerful secrets and privileges to access sensitive resources with little to no human involvement. For example, CI/CD tools



The average staff member accesses more than 30 applications and accounts.[1]



Machine identities outnumber human identities by a factor of 45x.[2]

[1,2] CyberArk, "2022 Identity Security Threat Landscape," April 2022.

for configuration management, such as **Ansible**, and those used to run automated tests and builds, like **Jenkins**, are "tier 0" tools that can enable full control of the environment. Yet too often, security controls are limited or inconsistent in these environments. You cannot protect your applications, let alone your greater software supply chains, without applying the same security rigor to the tools used to build them. This starts by securing secrets at every point along the development lifecycle and across your application portfolio.

71% of organizations suffered a successful software supply chain-related attack that resulted in data loss or asset compromise.[3]

Secrets Management Requires Visibility, Automation and Collaboration

A massive number of application secrets likely already exists across your enterprise. But chances are these secrets are siloed with individual project teams or are scattered across multiple tools, creating secrets sprawl (see sidebar). Security or development teams may rely on manual processes to manage and rotate secrets, costing valuable time and slowing down development. And it may be hard to coordinate secrets management activities across the various teams involved with application development and deployment, including developers, operations, cloud architects and more.

A more effective and comprehensive secrets management strategy depends on three main pillars: visibility, automation and collaboration.

ACCORDING TO AN IDC SURVEY,

Secrets management is often dispersed across different teams and tools, creating a need for centralized management.

- **32%** indicated the lack of centralized secrets management makes it hard to establish and share best practices across teams.
- **72%** report they are using secret management processes supplied by the native capabilities of the platform used to develop and deploy apps.
- **42%** acknowledged that multiple secrets management platforms are used across different project teams or groups.

IDC Infobrief, sponsored by CyberArk, "Managing Application Secrets Across the Enterprise," Doc. #US48924522, March 2022.

THREE PILLARS OF EFFECTIVE SECRETS MANAGEMENT

Visibility

Before you can manage anything, you need a full inventory of the many application types that require privileged access to resources, along with all their associated secrets. But when secrets are managed differently across various teams and projects — which **87% of organizations say is the case**[4] — secrets sprawl can make tracking difficult and can introduce operational complexity. A centralized view can help you get a handle on these secrets and get a complete picture of your digital identity landscape.

Automation

Development teams need to move fast, and they can't have secrets management-related tasks slowing them down when they're looking to deploy new applications or features. By automating secrets management, such as automatically onboarding applications and rotating secrets, you can make it easier for developers to do the right thing without sacrificing speed or taking security shortcuts to meet their deadlines.

Collaboration

As mentioned above, there are many different teams working on application development and deployment. Silos can create gaps and critical secrets management tasks can fall through the cracks. Building more efficient collaboration processes can help bring teams into alignment and reinforce strong, consistent security practices across the organization.

[3,4] CyberArk, "2022 Identity Security Threat Landscape," April 2022.

Continued on next page.

How We've Seen Centralized Secrets Management Work for Customers

Many CyberArk customers say that centralizing secrets management played a pivotal role in addressing secrets sprawl and software supply chain vulnerabilities.

For example, a large bank was struggling to manage the large number of secrets across its application portfolio. By deploying a centralized secrets management solution with native integrations to DevOps tools, the bank was able to improve operational efficiency without impacting end user productivity. Instead of juggling disparate secrets management policies, one centralized platform meant one streamlined program to support, with 360-degree visibility.

Other customers have centralized secrets management to fortify their software supply chains, simplifying how developers and security teams secure applications and CI/CD pipelines. Out-of-the-box integrations with existing tools and platforms make it easy to automate tasks such as credential rotation and auditing, running data collection in the background without disrupting development workflows.

CENTRALIZED SECRETS MANAGEMENT BENEFITS

Defend Against Attacks

Remove hard-coded secrets and islands of security to extend your privileged access management (PAM) program and achieve greater visibility and control.

Drive Operational Efficiencies

Automatically manage, rotate and audit secrets to help security teams save time and keep developers focused on innovating.

Enable the Digital Business

Utilize out-of-the-box integrations with existing development tools and cloud platforms to streamline secrets management and keep moving fast.

Satisfy Audit and Compliance

Centralize audit logs for quick accessibility, simplifying and easing compliance requirements.

Final Thoughts: Why It's Critical to Secure Application Secrets Across the Enterprise

As you build out your comprehensive Identity Security program, securing machine identities and application secrets – everywhere they exist – is critical to reducing security vulnerabilities, minimizing the attack surface and streamlining operations. But it can't slow down development teams or delay automation initiatives — after all, speed is the currency of business.

The right centralized secrets management approach enables the best of both worlds, bringing development, operations and security teams together and propelling your enterprise to the forefront of digital innovation.

Learn more about CyberArk

CYBERARK®