CYBERARK®
The Identity Security Company

EBOOK

Securing Non-human Identities and Managing Secrets in Multi-cloud Environments

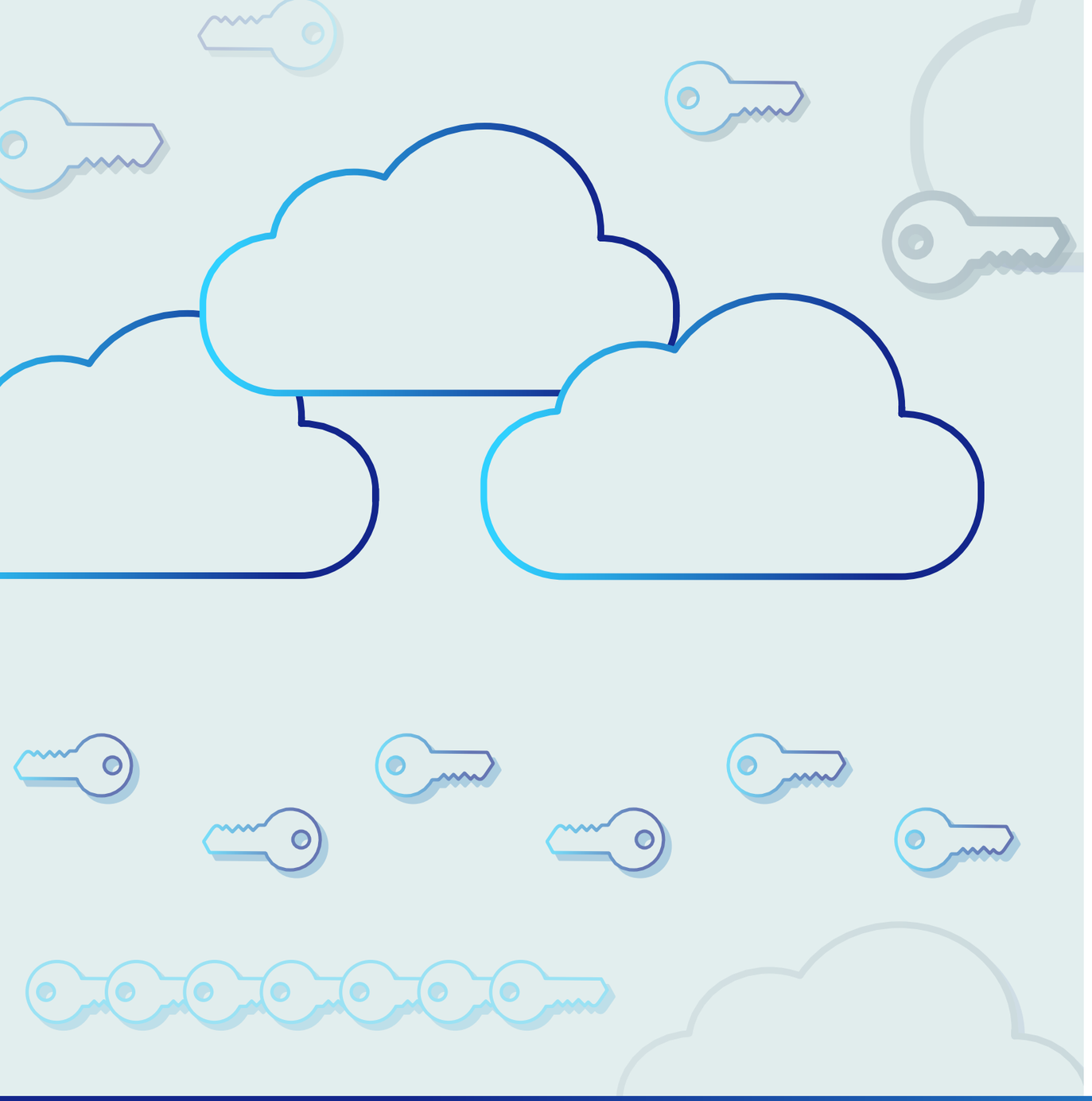


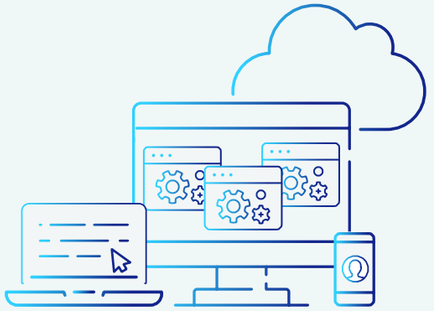
Table of Contents

More Clouds and More Non-human and Machine Identities...

Cloud migration and digital transformation have become commonplace for many modern enterprises today. The cloud is essential for accelerating growth, improving efficiency and remaining competitive, and most companies are now developing applications in the cloud. According to the Enterprise Strategy Group (ESG) 2023 Technology Spending Intentions Survey, 71% of organizations are now developing cloud-native applications.[1]

Because change is the only constant in today's business environment, most organizations deploy multiple clouds and leverage multiple cloud service providers (CSPs) to maintain pricing control, enable flexibility and avoid cloud vendor lock-in. And this trend is only growing, as a recent CyberArk survey found that 85% of respondents said they would be using three or more cloud service providers by 2023.[2]

Automation, DevOps and the growth of cloud environments have led to an explosion of machine identities — also called non-human identities — for applications, cloud workloads, containers, services and other automated tasks. These non-human identities all have accounts, credentials and secrets that need to be secured. As digital transformation initiatives are implemented and expanded, so too have the number of non-human identities. The CyberArk 2022 Identity Security Threat Landscape Report found that machine identities outnumber human ones by a factor of 45 to 1, which could mean 98% of an organization's accounts and identities are non-human or machine.[3]



85% are using three or more cloud service providers in 2023.

98% of of identities are non-human.

[1] Enterprise Strategy Group (ESG), "Complete Survey Results: 2023 Technology Spending Intentions Survey." 21 November 2022.
[2] Enterprise Strategy Group (ESG), "The Holistic Identity Security Model." February 2023.
[3] CyberArk, "2022 Identity Security Threat Landscape Report," April 2022.

...More Secrets

Applications, cloud workloads, automation tasks and other non-humans or machines use secrets in order to access critical systems and resources and do their jobs. Secrets are digital credentials (passwords, API keys, SSH keys or any secret information used to log in) that are used to grant access to privileged accounts, applications, databases, services and other protected resources.

A machine identity typically uses and has access to many secrets to perform its daily automated tasks, and these identities are scattered across different tools and platforms. Often these secrets are hard coded directly into the application code or left unprotected in a script or configuration file. Sometimes, however, they are managed within multiple third-party vaults across different tools or platforms, each with their own different method for storing, accessing and managing secrets.

What does this mean for security teams? They're now challenged with balancing organizational risk mitigation while managing an increasing number of non-human identities and secrets across sprawling public cloud, private cloud and on-premises environments. Each secret is a potential vulnerability, as attackers can use compromised secrets to access critical systems and resources.

The 2022 Uber breach is just one recent example of the risk of unsecured secrets and non-human identities.[4] The breach was caused by hard-coded secrets for a privileged access management (PAM) solution being directly embedded and exposed in a PowerShell script the attacker used to gain admin access to all secrets stored within their system. These credentials then allowed the attacker to escalate privileges and gain high-level access across the Uber IT infrastructure.

When you consider the number of secrets that must be secured and rotated and the number of tools and platforms security teams have to interact with to do these tasks, you can see how it quickly gets overwhelming. Not to mention if applications need to be moved from one environment to another, it can become a time-consuming hassle for development and security teams. Many security teams also don't have the bandwidth to either separately manage secrets in each of the environments and tools where they're stored or implement and maintain a self-hosted secrets management solution.

> "Much of the Uber cyberattack analysis has focused on social engineering and multiple MFA attack vectors, but the real turning point for the attack happened post initial access. The presence of embedded credentials, in a misconfigured network share, is critical to deconstructing this attack. It was the harvesting credentials for a PAM solution embedded in PowerShell script that allowed the attacker to gain high-level access, escalate privileges and set off on a veritable field day inside Uber's IT environment."
>
> **SHAY NAHARI** | Vice President, Red Team Services, CyberArk

[4] CyberArk, "Unpacking the Uber Breach," 20 September 2022.

Holistic Identity Security and Secrets Management

Security teams have more to protect than ever before, all while facing resource challenges. To solve this, teams are turning to centralized, SaaS-based secrets management to provide visibility and efficiency, identify threats, audit access and holistically manage secrets to mitigate organizational risk.

Centralizing secrets management can help security teams stay on top of all of these secrets used by non-human identities without having to chase them down in each of the different tools and environments they're used in. Centralization means security has a single pane of glass through which they can view all the secrets, in every environment. Secrets can be rotated automatically, instead of having to learn the nuances of the secrets management function of each tool they're stored in. Bringing secrets management into one solution also allows security teams to scale their efficiency – applying policies consistently and simplifying any audit tasks. And using a centralized solution that's owned by security means that the development organization can untether itself from any secrets management tasks in the tools they use to build applications, allowing them to focus on development instead.

When this type of centralized secrets management solution is also SaaS-based, those efficiency gains increase. The security team doesn't have to worry about implementing or maintaining a solution and can focus on higher value-added tasks. The power of SaaS also means teams can start small and scale up as their environments become more complex and as the number of secrets to manage grows.

Five Benefits of SaaS-based Secrets Management for Multi-cloud Environments

So what are some specific benefits that a SaaS-based secrets management solution can offer security teams working in these complex environments? Let's take a look at the top five.

Reduce vault sprawl. When you're working in multiple clouds or hybrid environments, the number of separate vaults for credentials and secrets can quickly get overwhelming. Rather than security teams hunting for each vault to rotate and manage passwords and having to bring information from a variety of vaults to create an audit trail, a centralized secrets management solution can give you a single pane of glass in which to work.

Enable cloud portability. The beauty of the cloud is that developers can build and deploy applications faster than ever before. But by relying on the native secrets management capabilities of the platform the application is built on, you're locked into using that platform. That becomes an issue if there comes a time when you need to move an application from one environment to another. With a centralized secrets management solution, you can build applications in whichever cloud platform your developers prefer for that specific use case, and move applications from cloud to cloud or from on-prem to cloud without creating a ton of extra work to manage the secrets used in those applications – no need to rewrite apps for a new cloud.

Provide a uniform experience for security and developers. Rather than security teams learning multiple different secrets management platforms (which can take time and extra team members), a centralized solution allows security to enforce policies in a unified manner and only operate in one system. This saves time and money on training (from not having to worry about adding additional staff to support every cloud provider), so security can really focus on delivering business value. Developers can also benefit from a uniform experience of fetching and managing secrets so they can spend more time on coding and less time worrying about the security side of things.

Automate rotation and other security policies. A SaaS-based, centralized solution means that you can automate formerly manual tasks such as secrets rotation and the application of certain security policies. This saves security teams time, especially given the vast number of secrets and identities that need to be rotated on a regular basis across multiple different cloud service providers.

Speed up time-to-value and frees up resources. Having a SaaS-based solution means that you can reap the benefits of the cloud with your secrets management software too. Security teams don't have to worry about operating and maintaining their own secrets management solution (or multiple solutions), but instead can focus their time and attention on the crucial security tasks they need to complete. A SaaS-based solution is quick to deploy and ready to use, taking care of the heavy lifting for security teams who need to act fast and cover a lot of ground. Frequent, automatic updates also mean one less thing for security teams to worry about.

How Conjur Cloud Can Help

If your security team is looking for a solution that is quick to deploy and can streamline secrets management across multi-cloud and hybrid environments, CyberArk Conjur Cloud may be a good fit.

Conjur Cloud is a modern secrets management solution, designed to simplify and streamline the management of non-human secrets and credentials wherever they are, any cloud, any environment. With Conjur Cloud, security teams and developers can use the same secrets management solution for any cloud platform or even on-premises, reducing the impact of cloud vendor lock-in and enabling organizational resources to be more dynamic and flexible.

A centralized secrets management solution like Conjur Cloud can help security teams:

1. **Extend privileged access management** for human credentials to include non-human.
2. **Enable Zero Trust security by authenticating**, authorizing and auditing machine-to-machine access via secrets and credentials.
3. **Protect against software supply chain attacks** and provide CI/CD pipeline security by removing hard-coded secrets from tool scripts and configuration files that put the software supply chain at risk.
4. **Eliminate the "secret zero" problem** and establish machine identity by leveraging the native attributes of applications, containers and other non-human identities.

Seamlessly Integrate With CyberArk Privilege Cloud

Conjur Cloud seamlessly integrates with CyberArk Privilege Cloud, so that security teams can holistically manage both human and non-human identities through one single pane of glass. Learn more about the benefits of CyberArk Privilege Cloud by visiting our website.

LEARN MORE

Increase Your Efficiency With the CyberArk Identity Security Platform Shared Services

One of the benefits of Conjur Cloud is that it is part of the CyberArk Identity Security Platform. With the Identity Security Platform, security teams can access shared services to further increase their operational efficiency. Centralized audit and user management gives security teams even more visibility and control across their Identity Security tools, including secrets management.

LEARN MORE

Multiple clouds and hybrid environments don't need to mean extra work for security teams or developers. Centralizing secrets management with a SaaS-based solution like Conjur Cloud can help ease the way and allow the teams to harness the full power of cloud environments. Since it's SaaS-based, Conjur Cloud enables organizations to:

- **Simplify and centralize secrets management across hybrid and multi-cloud environments.** Conjur Cloud manages secrets within any cloud or on-premises environment, meaning no more security islands and no need for developers or security teams to learn multiple secrets management tools. With Conjur Cloud, you can manage, enforce and audit non-human access in one place.
- **Reduce staff training and maintenance cost.** With Conjur Cloud, there is one uniform experience for developers, DevOps and security teams, and software updates are handled automatically.
- **Build cloud-portable applications.** With Conjur Cloud, there is no need for developers to write and maintain specialized secrets management code that depends on the current cloud provider being used or if the application is hosted on-premises.
- **Faster time-to-value.** Conjur Cloud allows security teams to quickly deploy their new secrets management solution because there is no secrets management hardware or software to host.

Want to learn more about how Conjur Cloud can help your security team streamline secrets management quickly and effectively? Schedule a meeting with our team of trusted experts today.

GET A PERSONALIZED DEMO

CyberArk is the global leader in Identity Security. Centered on privileged access management, 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. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

U.S., 02.23 Doc. TSK-3006

CYBERARK®
The Identity Security Company