CYBERARK®
The Identity Security Company™

# Why Cloud Identity Security and Why It Seems So Hard

**By Charles Chu**
*General Manager, Cloud Security*

The cloud has had a profound impact on businesses – from a digital-native business that's built entirely in the cloud with no physical goods and services to a traditional enterprise that's lifting and shifting traditional workloads for agility and all points in between. But that fast pace has created security challenges that rise in importance as companies consider mitigating reputational risk, entering new industries with regulatory compliance standards or increasing their equity valuation.

To achieve a secure posture, organizations need to solve the fundamental issue of "who should have access to what and when" in a pragmatic and holistic fashion.

## Why Focus On Identity Security? The Attacker Mindset Is Still the Same

Attackers know that the richest bounty is co-opting someone's identity. That's the reason why identity is the common element behind some of the highest-profile breaches in the last few years. One misconfigured, overpermissioned identity can wreak havoc on an organization. The breaches at SolarWinds, Okta and Uber, just to name a few, have all been based on identity. These breaches were so damaging because the attackers were able to compromise identities that had highly privileged access that could be exploited for maximum impact.

## Why Cloud Identity Security Is So Hard

You first need to build a door before you design a lock. This simple truism can explain why Identity Security is so hard for organizations. In an incredibly short amount of time, the "door" to cloud-native applications has morphed and changed multiple times.

Circa 2010, most organizations building cloud-native applications had to develop every feature and function in their applications – most likely running in virtual machines (VMs). The industry then evolved to services running in containers. Then all the cloud service providers (CSPs) began offering the basic

application building blocks as a service like message queues, notification engines and workflow engines, which eliminated the need to build these functions at all. Today, we can use these CSP building blocks, focus only on building high-value business functions and do it serverless without the need to understand any old-school notions of VMs, containers, memory allocation and the rest.

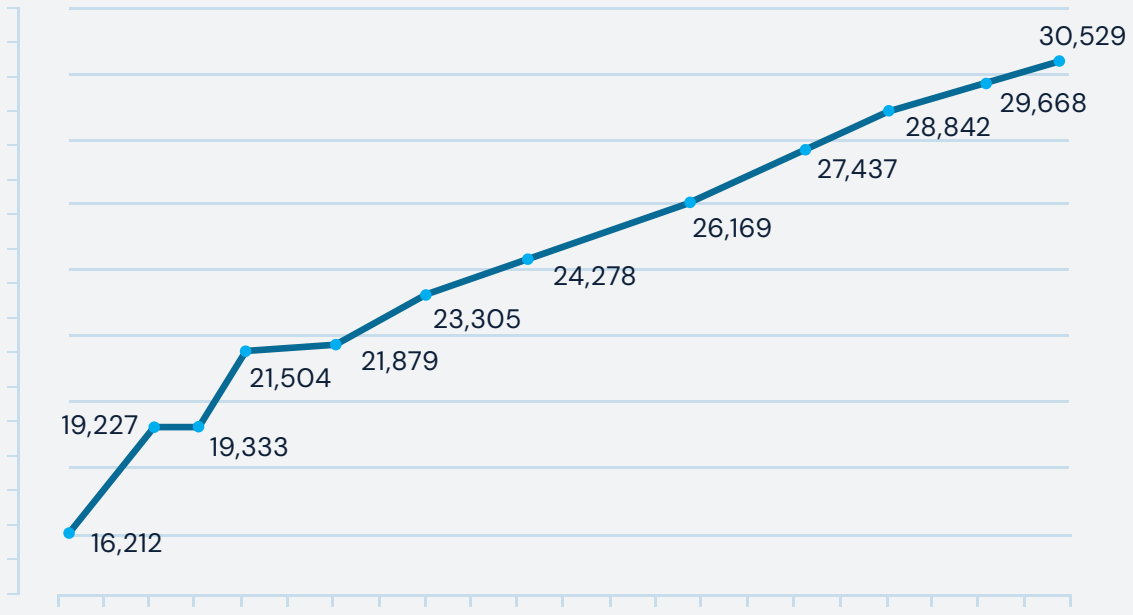
Enterprises that are lifting and shifting their traditional workloads over to the cloud don't have it much easier as they now have additional layers of architecture to consider. These companies must now consider access to the CSP that the app is hosted in, access to the VM that is running the application and then access to the application itself. Security teams that formerly worked in only on-premises environments must now add security controls to these additional layers.

How many different types of locks to how many different types of doors do we have to build? Determining "who has access to what and when" can be vastly different for a lift and shift workload, an old-school homegrown service running in a Linux VM, versus a managed service like a workflow engine that's provided by the CSP or a serverless app. Better (or worse?) yet, if the company is more than a decade old, then it may have to account for all these scenarios as it considers Identity Security.

It's no wonder that roles and entitlements are not well defined as organizations sort through the multiple types of doors and locks that they have to secure. This, in turn, has driven a huge increase in the number of entitlements companies have created, as this CyberArk internal research shows.

**TOTAL CLOUD PERMISSIONS**

**(CyberArk Cloud Entitlements Catalog)**



## Cloud-native Architectures Drive New Issues

Cloud-native architectures have a special challenge because of the proliferation of tools – cloud monitoring, solutions that automate provisioning, repositories, scanning and on and on. Some are within the companies' environment, while others are hosted by the vendor. Compromising a single identity for an innocuous code-scanning tool may open the door that leads to a serious breach.

In addition to the human access challenge, cloud-native architectures have driven the creation of an explosion of new service identities and the resultant headache of managing the sheer volume of identities and secrets. To compound the problem, many implementations allow all homegrown (micro) services to freely communicate with each other. The result is a complex n2-1 problem to manage both the volume of secrets and determine the service-to-service entitlements.

Lastly, there are some very legitimate reasons to sometimes put aside all the wonderfully curated roles, entitlements and access controls. When an outage occurs, the engineers (site reliability or software) need to move fast. No one would advocate for the poor on-call engineers who are confronted with a weekend outage to be forced to go through layers of manual access requests to troubleshoot and fix an outage. Clearly, any solution would have to account for these real-life scenarios.

## Now What? A Pragmatic and Holistic Approach

In one recent informal survey, we found that over 80% of digital-native businesses failed a security self-assessment. Anecdotally, we've not heard a single company declare that they are 100% confident in their current and future cloud Identity Security posture.

### THREE PRACTICAL STAGES TO IMPROVE CLOUD ACCESS SECURITY

**Meet Baseline Requirements**

- Start with the relevant industry standards you must meet in order to remain compliant (e.g., SOC2, PCI and NIST).
- Apply immediate risk reduction by securing cloud console access while maintaining frictionless native access by engineers.
- Centralize governance of secrets to a single hub for visibility and to apply industry and internal standards.
- Fix high-risk misconfigurations that could result in a vulnerabilities.

**Standardize Audit and Reporting**

- Use a data-driven approach to remove access to never/seldom-accessed systems.
- Enable access session recordings for outage situations for proper audit documentaion.
- Implement preventative controls to halt new unapproved roles and access
- Create standardized reports which continuously benchmark current state against industry and internal standards.
- Centralize access governance of services and APIs to secrets.

**Encourage Continuous Improvement**

- Implement automation to enforce industry and internal standards for both human and service-to-service access.
- Automate compliance and audit approval processes to reduce manual work and improve efficiency.
- Automate detection of hard-coded credentials and secrets.

To make progress in securing access to the cloud, we recommend a phased approach to first ensure compliance with relevant industry regulations (this is non-negotiable) and, very importantly, to continue to make improvements while always keeping development and business velocity at top of mind.

Cloud architectures will continue to evolve, and managing access will continue to be a complex challenge. Securing access for both your human and non-human identities is a must, but it has to be balanced with maintaining your developers' velocity and ability to respond quickly to new market needs or critical system issues. The challenge cuts across numerous cloud environments and teams, a myriad of cloud-native tools and both human and service credentials.

Consider a holistic solution that provides access to a diverse set of systems, identities personas and use cases. A holistic, centralized solution will help apply appropriate controls through policy-based access to help meet baseline compliance requirements, standardize audit and reporting and enable continuous improvement into the future.

**Secure Your Cloud Identities**

---

**About CyberArk**

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, 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.

CYBERARK®
The Identity Security Company™