CYBERARK®
The Identity Security Company™

EBOOK

Cloud Security Your Developers Will Love

Table of Contents

Cloud Security: Navigating a Labyrinth of Identities and Entitlements

It was August 8, 2022. A threat actor had just breached a software engineer's corporate laptop to gain unauthorized access to their cloud-based development environment. Reportedly, the source code and some of the company's internal system secrets were stolen. However, by August 25, the company confirmed it had neutralized all threats and that the breach was successfully contained.

More than six months later, on February 27, 2023, the company reported that one of their DevOps engineers' home computers had been compromised using data stolen during the initial breach in August. It turned out that the company had suffered a monthslong sustained attack that exposed sensitive customer data, vault secrets and AWS production backups.

The company was Last Pass and the incident subjected them to widespread ignominy for failing to detect a threat actor in their environment that stealthily wreaked havoc for months. If anything, this devastating breach underscores the importance of securing developer access in the cloud amidst accelerating digital transformation - the leading cause of identity-related attacks[1]. It also draws attention to the fact that standing access for developers in hybrid and multi-cloud environments can lead to potentially catastrophic consequences.

As the architects of the modern enterprise, developers need speed, simplicity and user-friendly security controls to do their jobs in this increasingly complex digital world. They are highly privileged identities with access to code repositories and databases — and 20% of security professionals are already battling elevated enterprise risks owing to overprivileged developer identities in their organizations. This makes developer security imperative for organizations to protect everything they're building in today's cloud-first era.

[1,3,4,5] CyberArk, "2024 Identity Security Threat Landscape Report," May 2024.
[2] Crowdstrike, "Crowdstrike 2024 Global Threat Report," 2024.

Cloud Security: A Pressing Concern for Enterprises

75%

increase in cloud intrusion in 2023[2].

84%

of organizations will use three or more cloud service providers (CSP) in the next twelve months[3].

31%

of security leaders say that cloud workloads are home to the riskiest, most unmanaged identities that exist within an organization[4].

In this eBook, you'll learn about:

- Securing developer access to the cloud using an identity-centric approach.
- Building security controls that developers love.
- Enabling better control of time, entitlements and approval (T.E.A) for developers without losing velocity.

Complexities in Securing Cloud Access for Developers

As developer environments change with organizations migrating to the cloud, so do their roles and the circumstances under which they operate. This necessitates security teams to think of new ways to secure their access to critical enterprise resources living in the cloud.

When workloads were on-premises and identity proliferation was unheard of, developers typically used a shared account to access target resources running in the foundational Linux and Windows servers. In other words, the attack surface was smaller, allowing organizations to get by with standing access for developers guarded by basic identity and access management (IAM) tools.

In on-premise environments, a compromised developer account would, at best, provide access to a subset of services – for instance, a Windows domain account. Only in the rarest of cases can an attacker gain access to the data center to provision expensive graphics processing unit (GPU) instances that can be used to mine cryptocurrencies. However, the same is possible in the cloud, provided an account has the necessary permissions.

Given the complex nature of cloud applications and workloads that work together to support a host of different services, enabling standing access to developers would mean leaving the gates open to attackers. At the same time, selectively granting admin rights to developers in the cloud is bound to limit their productivity and delay scheduled deliveries.

For instance, if a microservice powering an application running Kubernetes cluster goes down, the developer would require instantaneous admin rights to multiple cloud environments (the cloud service provider and the Kubernetes cluster) to troubleshoot and get the service up and running quickly.

This dynamic access calls for a security-first approach to protecting developer identities in the cloud as they code their way through crunched timelines to deliver minimum viable cloud solutions aimed at scaling business efficiency and productivity.

What Makes Cloud Security So Tricky

- Every user in the cloud could be an admin given the interconnected environment they live in.
- Users with read-only rights can potentially configure new services.
- Troubleshooting one application requires access to several other resources.
- Everything moves faster in the cloud and developers cannot wait for access to do their job.

Consistent Security Controls for Different Cloud Environments

When it comes to securing privileged access in the cloud, the approach has remained largely the same over the years: vaulting and credential rotation, followed by session recording and isolation between endpoints and target systems.

However, securing developer access in the cloud calls for a more strategic approach. Each layer of the enterprise cloud infrastructure has different workloads with unique access complexities and security challenges. The following page offers a snapshot of the various cloud environments, the workloads living in them and the security solutions required to secure developer access to them.

As much as developers want unfettered access to move seamlessly across the enterprise, they are guarded by several siloed third-party security tools to secure their access in the cloud.

The solution? Consistent security controls obtained by layering existing IAM and privileged access management (PAM) solutions, whose complexity can be dynamically adjusted to enable secure access for developers to all parts of the cloud. And it all starts by placing empathy at the heart of your security strategy.

Vendor Sprawl Drives Cyber Debt

94%

of security leaders use more than 10 vendors for identity-related cybersecurity initiatives[6].

[6] CyberArk, "2024 Identity Security Threat Landscape Report," May 2024.

Secure Developer Access to Every Layer of the Cloud

1. Long-lived Systems

Use case: Secure system access to datacenter, OT and lift-and- shift workloads with shared accounts.

Method: Credential management & rotation, session isolation.

2. Elastic Workloads

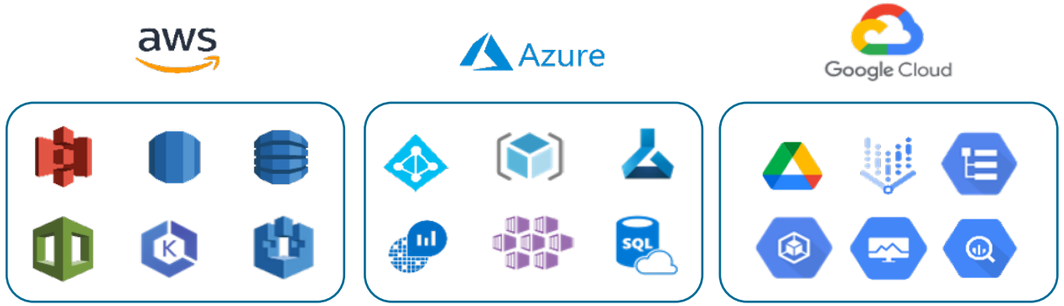
Use case: Secure operational access to VMs and elastic workloads.

Method: Dynamic, just-in-time access.

3. Cloud-Native Services

Use case: Secure operational access to cloud native services.

Method: Native, zero standing privileges access.



4. Third-Party SaaS Apps

Use case: Secure operational admin access to third party SaaS apps.

Method: Session protection & monitoring.

Ensuring Cloud Success With Developer-Friendly Security Controls

Being empathetic towards developers can be as simple as not keeping them waiting for approvals while they're looking to debug an existing issue or make changes to the code block.

While no one security solution can make it happen, a layered approach focused on securing identities backed by the following core principles can go a long way toward implementing a developer-friendly cloud security strategy.

1. **Standing Access:**

   Provides developers with long-standing access to critical resources through shared accounts whose credentials are automatically vaulted and rotated to prevent credential-based attacks. This approach leverages foundational privilege access management (PAM) and IAM solutions to secure built-in, administrative accounts that must exist, need security controls but are seldom used.

2. **Just-in-time (JIT) Access:**

   Elevates developer access when they need it (just-in-time) to ensure their velocity remains unimpacted. This approach uses attribute-based access control (ABAC) to verify whether a developer seeking access to a target resource is who they claim to be.

3. **Zero Standing Privileges (ZSP):**

   Equips developers with the least privilege access rights to cloud resources that are dynamically created and deleted on the fly for each session. ZSP is, in many cases, the desired state for building the most effective and least disruptive privilege controls.

Adopt an Integrated Identity Security Strategy

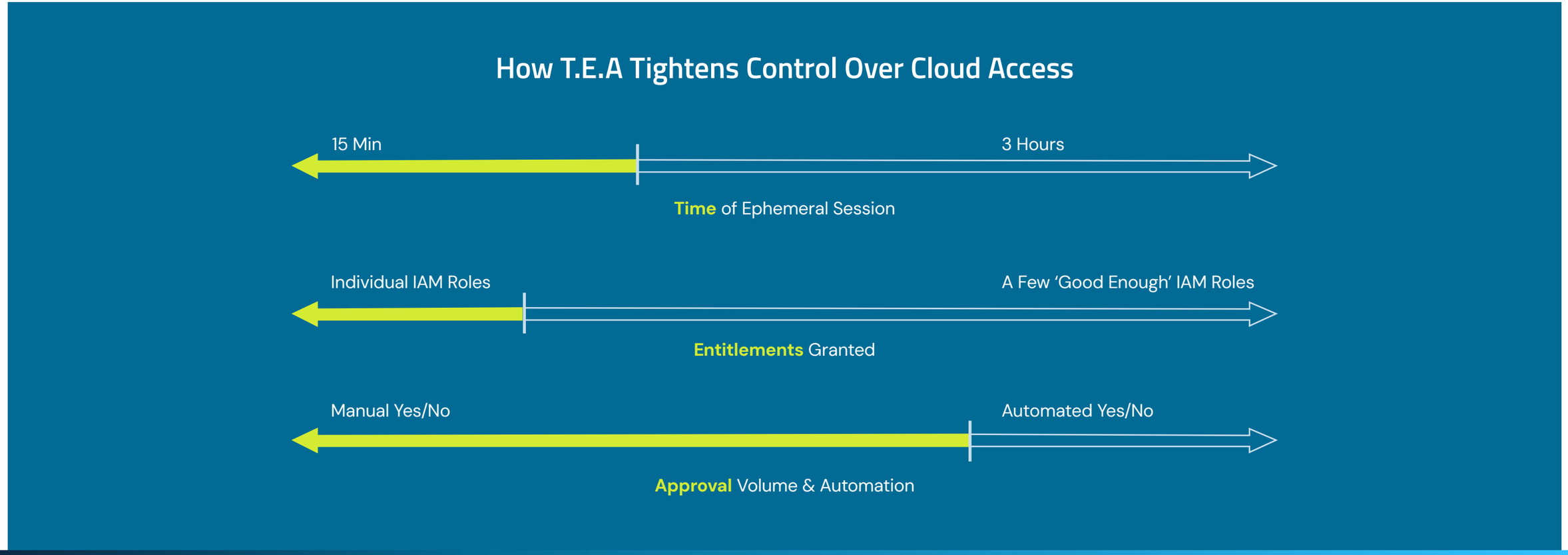
Modern security teams are spread thin managing competing priorities and you cannot expect them to manually grant standing access, JIT or ZSP to developers based on the resources they are trying to access in the cloud. It will not only increase administrative burden but make security a blocker, instead of an enabler.

That's where an integrated identity security strategy comes into play. Start with broad spectrum implementation of zero trust architecture and ensure continuous authentication of all identities based on real-time threat intelligence powered by CyberArk CORA AI, which sits at the heart of the CyberArk Identity Security Platform. This will enable security teams to automate access provisioning and de-provisioning for developers working in the cloud, eliminate manual errors and increase operational efficiency.

Modulating T.E.A to Maximize Security Without Affecting Developer Velocity

Nothing frustrates a developer more than being stopped in the middle of a coding sprint due to lack of access. No wonder they are so averse to adopting security solutions. But what if there was a way to smartly provision access for developers just when they need it to prevent slowing them down? That's what the concept of time, entitlements and approval (TEA) is all about.

Let's understand how it works with an example: imagine an application hosted in Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP) has gone down. Our DevOps engineer, Dave, first needs to access the cloud security provider (CSP) console or command line interface (CLI) to diagnose the issue.



To do so, Dave first needs to access the PAM solution that securely manages the CSP credentials before connecting to the cloud console via session management. From Dave's point of view, this is a tedious, time-intensive process to diagnose and resolve the issue at hand. He would have, instead, loved to have native access to the CSP CLI to get the job done sooner.

However, with ZSP, Dave can natively access the CSP console or CLI using his own federated identity without having to use another solution protected by standing credentials. This greatly improves his user experience while providing native access to the CSP console which further strengthens Dave's security.

Zero standing privileges ensures no entitlements are available by default and privileges are only granted for a specific time period to the developer after necessary approvals are met. An audit trail of Dave's activities performed using his federated identity within the cloud environment will be maintained for the approved time period. Once the session expires, Dave's entitlements are automatically revoked back to ZSP and the environment is secured.

T.E.A makes this concept of Zero Standing Privileges easier to manage. If the security team has dynamic control of the T.E.A they can ensure that Dave has the right access, designed exactly for his requirements.

Conclusion: Enabling Developers With an Integrated Identity Security Strategy

Security is a two-way street: it should protect you from attackers while powering you towards your goals. For developers, succeeding in today's cloud-first environment means gaining native access to cloud consoles without losing velocity while staying clear of attackers.

At CyberArk, we make this possible through the CyberArk Identity Security Platform to secure developers and all other identities with the right levels of privilege controls to help:

Drive measurable cyber risk reduction by layering JIT access with ZSP to remove any standing access while consistently analyzing and monitoring access across hybrid and multi-cloud environments.

Enable operational efficiencies by centrally delegating access to the entire cloud estate from a single platform and enabling native user experience for monitored sessions.

Secure digital transformation by providing seamless, native access to SaaS and cloud CLI console from one platform and addressing critical sessions at required developer velocity.

Satisfy audit and compliance by gaining unified visibility with comprehensive audit trails of cloud administrative access and integrating into information technology service management (ITSM) tooling to achieve segregation of duties with minimal disruption.

For more prescriptive guidance on securing developers in the cloud, read the CyberArk Blueprint.

READ THE BLUEPRINT

Get hands on experience using CyberArk Secure Cloud Access with a Free Trial

FREE TRIAL

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. 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., 02.25 Doc Item ID: 1827639200 (TSK-6858)

CYBERARK®
The Identity Security Company™