CYBERARK®
The Identity Security Company™

WHITEPAPER

Zero Standing Privileges: Securing the Cloud to Drive Developer Success

Table of Contents

Introduction: The Perils of Developers in the Cloud

Cloud is now the engine of transformation.

From saving costs to streamlining operations and everything in between, a well-thought-out cloud strategy can do it all for your business. It's no wonder why in the next twelve months, 84% of organizations will reportedly be working with three or more cloud service providers (CSP)[1].

While this accelerating cloud adoption is enabling faster and more scalable software delivery, it's also giving rise to new vulnerabilities and operational challenges:

In an enterprise, developers are often the ones responsible for driving innovation, which requires them to have access to code repositories, databases and high-risk applications. This extensive access makes developers highly privileged identities, necessitating stronger access management controls for them to securely access cloud-based resources needed to do their job.

However, the tried-and-true privileged access management (PAM) controls that sufficed to secure standing access to on-premises infrastructure cannot emulate the same level of security for developers across hybrid and multi-cloud environments.

Furthermore, developers prefer always-on entitlements for ease of work that the ephemeral nature of cloud workloads and varying access permissions across CSPs make it increasingly difficult for security teams to configure without risking enterprise security.

While manually verifying developer access would impact their working velocity, enabling standing access to cloud workloads would create unprecedented risks. This whitepaper explores the middle ground that cloud engineers desperately seek, through a strategic deep dive into building security that's invisible to developers and loved by CISOs.

Read on to learn about:

1. Why standing access renders developers vulnerable in the cloud.
2. How Zero Standing Privileges (ZSP) can aid in balancing developer velocity and cloud security.
3. The importance of time, entitlements and approvals in securing enterprise cloud infrastructure.

[1] CyberArk, "Identity Security Threat Landscape Report 2024," May 2024.
[2,3,4] Tenable, "2024 Cloud Security Outlook – Navigating Barriers and Setting Priorities," 2024.

Deciphering Developer Needs to Enable Cloud Success

Developers are highly privileged employees with access to code repositories and databases that fuel day-to-day operations. As much as security practitioners would want to secure them with the established, trusted PAM controls of vaulting, rotation and session isolation, it's time to look beyond. After all, developer environments have evolved and so should security.

Developers On-Premises	Developers in the Cloud
Target resources: Long-lived systems such as Linux and Windows servers with fixed bandwidth. **Requirement:** Standing access to shared privileged accounts protected by credentials. **Security strategy:** Password vaulting, rotation and session isolation to prevent credential compromise.	**Target resources:** Elastic cloud workloads that spin up and down in real-time based on operational needs. **Requirement:** Dynamic native access to resources without waiting for approvals, which can potentially delay projects and create access fatigue, thus hampering their creativity. **Security strategy:** Using attribute-based access control (ABAC) or role-based access control (RBAC) for a fixed period of time to prevent unauthorized access to cloud resources.

To understand why dynamic access provisioning is critical to securing developer access in the cloud, let's visualize the basic framework of a typical cloud-first enterprise:

Step 1: Laying the Foundation

In today's digital landscape, identities and credentials are the building blocks of an organization's cloud presence. They are central to setting up the foundational Amazon Web Services (AWS) accounts, Microsoft Azure Tenants and Google Cloud Platform (GCP) projects.

Step 2: Mapping Entitlements

Every relationship between components deployed within the cloud, between administrators and engineers and the services they build or maintain, is controlled by entitlements mapped to roles assumed by different individual users. While entitlements continue to grow exponentially across CSPs to enable user access, it can be quantified at 1400 native services with 40,000 potential entitlements.

Step 3: Managing Access

In a microservices architecture built using a large number of native services, defining access for all can be challenging. Even if access is defined, the approval process can be burdensome. To navigate this, organizations can either choose to grant standing access (which creates overprivileged developer identities) or authenticate each request in real time (which affects development velocity).

Level Up Developer Security

When developers are expected to capitalize on the agility of cloud services to deliver minimum viable products quickly, they cannot afford to be slowed down by inefficient access management solutions. It's up to the security teams now to adapt to engineering demands lest developers resort to shadow IT to do their jobs at the cost of organizational security. In other words, security for developers has to be invisible: it must exist to protect them without any impact.

66%

of stakeholders say that shipping fast takes precedence over shipping secure[5].

Given that unsecured access poses tremendous vulnerability in today's hybrid and multi-cloud IT environment and traditional PAM controls slow down developers, just-in-time (JIT) access emerged to give developers a secure and efficient way to access cloud resources. It caters to the developers' needs by providing time-bound access to cloud-based resources when needed and revoked when not. While this doesn't impact the working state of developers and also aids in risk reduction, it still cannot fully control the entitlements of an identity post-authentication.

For instance, if a developer has been granted five-minute access to the AWS console to fix a malfunctioning service hosted in it, JIT cannot control what that developer does within that time frame. This creates an Achilles Heel in cloud security, leaving an attacker to think 'I'll wait' and forcing security teams to rethink the way they secure privileged access in a dynamic, cloud-first environment.

[5] ArmorCode, "State of Application Security 2023," 2023.

Prioritizing Privilege Controls for Developers

As privileged identities, developers need PAM—it just cannot work the same way across all environments for their working velocity to remain unimpacted. The challenge for security leaders, therefore, lie in reimagining PAM for developers in cloud environments without introducing new security solutions since organizations are already striving to control the vendor sprawl.

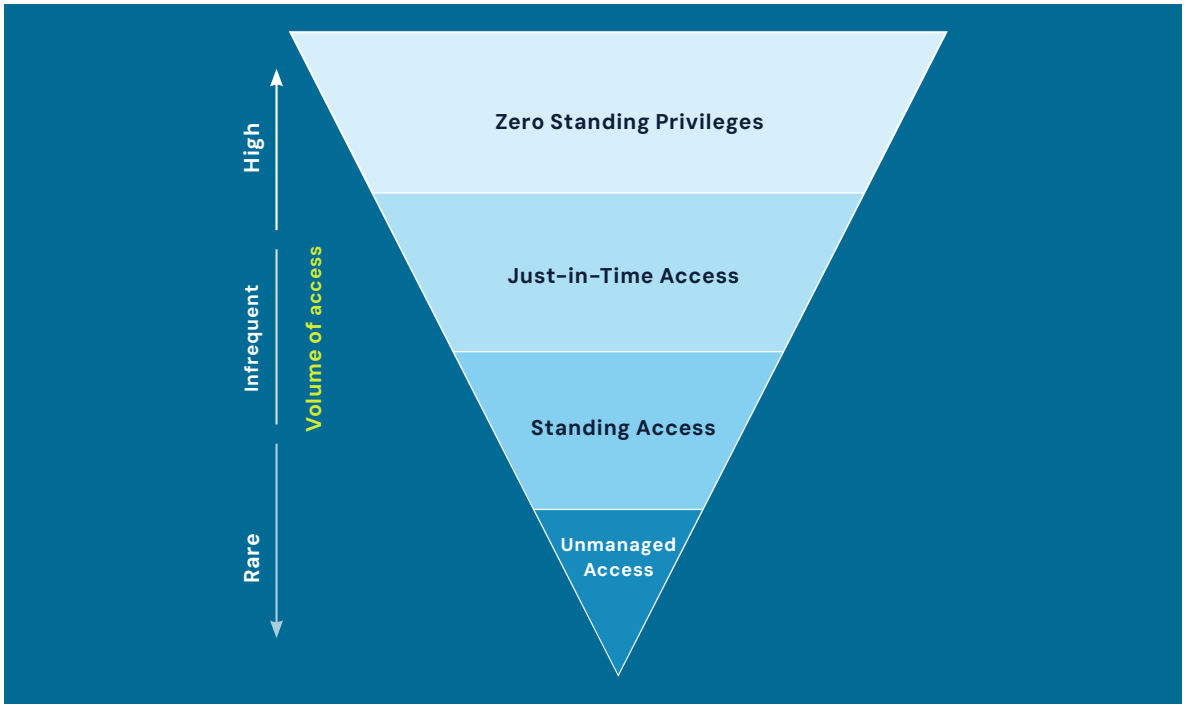
To make this work, it's important to understand the relationship between access and security: a higher scope of access demands strict privilege controls and vice versa. With standing and JIT access failing to adequately secure developers in complex cloud environments, Zero Standing Privileges emerged as an innovative, developer-friendly privilege control to secure their access in the cloud without compromising working velocity.

WHAT IS ZERO STANDING PRIVILEGES

Emerging from the concept of JIT, Zero Standing Privileges is a security principle that advocates for the removal of all persistent privileges for users within an enterprise's estate. ZSP maximizes risk reduction by removing all entitlements of an identity until it's invoked and temporary access permissions are granted.

The inverted pyramid below illustrates how privilege controls for developers must be applied with respect to the volume of access to maximize risk reduction.

1. **Highest Access:** Accounts that are accessed the most should be secured with stringent privilege control, such as Zero Standing Privileges. It offers maximum security without affecting user experience and takes the least amount of effort to implement.
2. **Infrequent Access:** Being relatively less accessed accounts, they are best secured by JIT access and traditional PAM controls.
3. **Rare Access:** This segment represents unmanaged access and should be kept to a minimum. If it's not possible to eliminate it, aim to bring it under managed access for effective risk mitigation.



Decoding the Difference: Just-in-Time Access vs. Zero Standing Privileges

Zero Standing Privileges is a breakthrough in access management. It works by providing secure, real-time access to what developers need without impacting productivity. While it sounds relatively simple, implementing it in a transient cloud environment, where the relationship between the federated identities and their entitlements is continuously evolving, can be challenging without the right privilege controls.

Like most security paradigms, JIT and ZSP are also centered on the idea of limiting availability to reduce the impact of access. However, ZSP is more effective in preventing unauthorized access in the cloud. The reason? Unlike JIT, ZSP doesn't stop at limiting access but removes the entire access pathway at the end of every time-bound session to prevent residual entitlements in the cloud from being exploited. It also offers security teams the granularity to control each user session by modulating time, entitlements and approvals, thereby keeping the cloud environments secure.

ZSP SIMPLIFIED

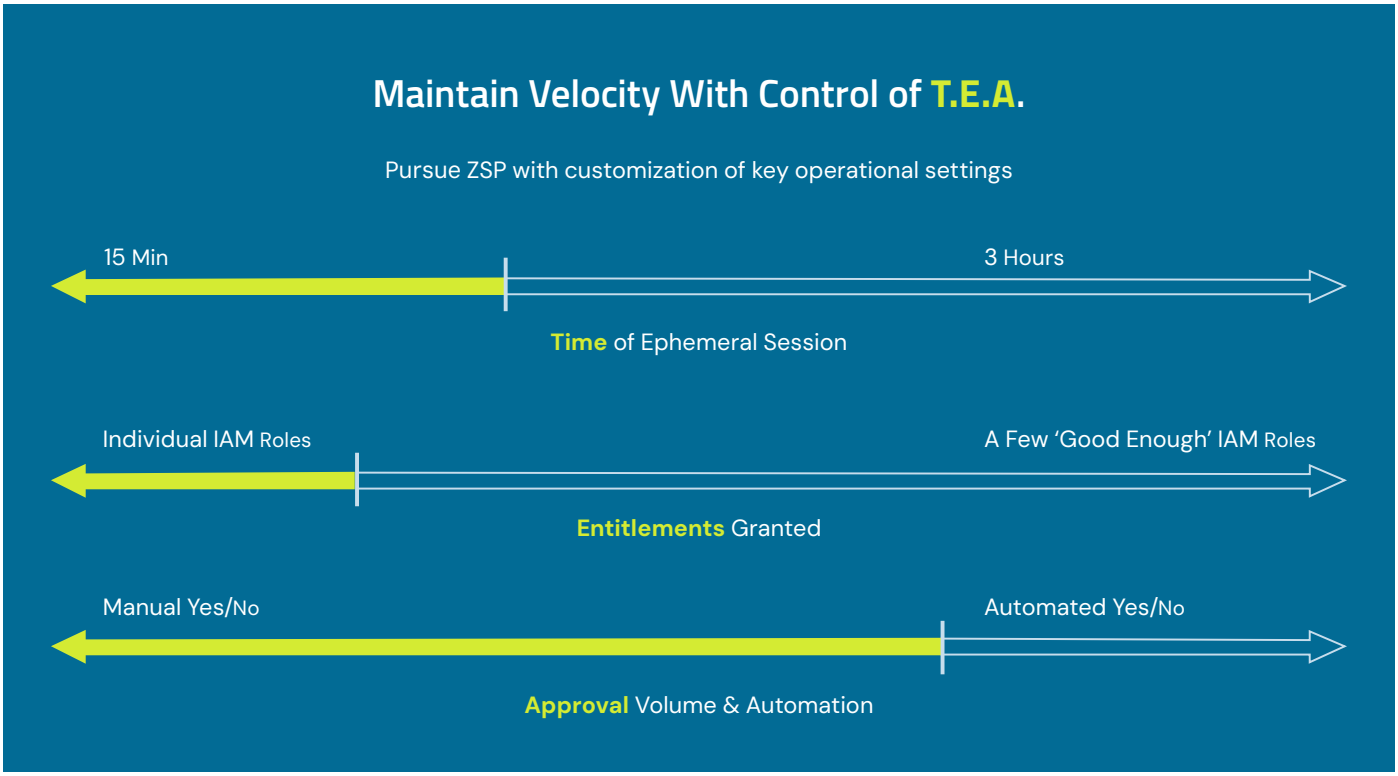
Imagine trying to access a sensitive document in a warehouse. With JIT, you'd have access to the entire warehouse for an assigned period of time to access those documents while checking on other things. This unconstrained access can be exploited to exfiltrate confidential data and resources. Whereas with ZSP, you'd be granted access only to the documents you need for a fixed duration while everything else on the floor remains inaccessible. Post that time period, all your entitlements are automatically revoked and you get checked out of the warehouse with nothing except what you came in for.

Just-in-Time Access	Zero Standing Privileges
• A security practice to seamlessly grant access to resources when needed for a fixed period of time. • Lacks granular security controls required to manage user sessions after they gain access.	• Similar to JIT with the exception of identities having no entitlements to a resource till that identity is invoked and entitlements are requested. • Has granular controls in the form of time, entitlements and approvals to ensure a user accesses only the resources they have permissions for after they log in.

Maximize Risk Reduction With T.E.A.

Time, entitlements and approvals (abbreviated as T.E.A.) are by far the most important parameters for enabling secure and seamless access to developers in the cloud. Realizing the true power of ZSP begins with the effective management of T.E.A.

- **Time:** The duration for which access is granted. This helps ease the administrator burden, boost developer confidence and reduce time-to-approval.
- **Entitlements:** The level of access granted. This helps in dynamic access provisioning of least privilege entitlements and also supports ABAC for cloud workloads, allowing organizations to provision entitlements only to workloads assigned to a specific attribute.
- **Approvals:** The level of checks undertaken before granting access. This helps in accelerating the approval process so developers do not have to wait for permissions. It can also be automated subject to risk-based rules within the system or ABAC tagging in the CSP.



Developers' top priorities are delivering the next stellar product, pushing out timely updates and fixing bugs. Anything that takes their attention away from these priorities will likely cause developers to embrace practices that fuel efficiency at the cost of organizational security.

For a long time, security has been that point of contention: time-consuming approval processes and cumbersome access management have made developers averse to security. A recent report found that 56% of developers say it's impossible to do their best work with their current software supply chain security tools[6]. Developers have been finding creative ways to bypass security to do their jobs, subjecting the organization to unforeseen threats and vulnerabilities.

Developers Perceive Security as a Blocker

With ZSP, developers can focus on their speed and priorities without bypassing security. Its granular controls, driven by time, entitlements and approvals, let developers securely access cloud resources without disrupting their natural flow of work.

[6,7,8,9] Chainguard, "CISO and Developer Trends in Software Supply Chain Security," November 2024.

Conclusion: Secure Developer Access to Speed Up Software Delivery

With the cloud attracting businesses with its promise of scale and agility, developers are facing the heat to deliver more in less time. They need solutions that secure native access without affecting their velocity and user experience. They need just-in-time access but with the ability to control user sessions and their finer entitlements.

At CyberArk, we address the problem by securing developer identities with Zero Standing Privileges, enabling them to gain native access to cloud resources via the console or command line interface (CLI). Our CyberArk Identity Security Platform is the only solution that's infused with ZSP capabilities to help enterprises:

- **Secure cloud access:** Developers can access cloud workloads natively without using siloed access management tools that add to the app sprawl and compromise visibility.
- **Maximize risk reduction:** Provide access to resources when needed and necessary conditions are met, without exposing your complete cloud environment.
- **Boost operational efficiency:** Automate access approvals to alleviate administrative burden and avoid compromising engineering velocity.

Experience the power of Zero Standing Privileges

Free Trial

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™