CYBERARK®
The Identity Security Company™

WHITEPAPER

Buyer's Guide to Securing Developers in the Cloud

Table of Contents

Introduction

Developers are one of the most valuable assets for the modern digital enterprise—and often the most excessively privileged. In today's hybrid, cloud and multi-cloud world, the surge of new identities and attacks and the emergence of 'permission sprawl' has reached a point of chaos.

Despite more and more software development occurring in the cloud, basic cloud security is often still not in place. Attackers know this, and look for ways to exploit this gap, breaching cloud workloads every month. Breaching one identity with the right entitlements allows an attacker to build data centers of expensive infrastructure or access sensitive data stored in the cloud. Last year, 93% of organizations[1] suffered two or more identity-related breaches. Meanwhile, the US Bureau of Labor Statistics projected that job growth for software developers would outpace all other occupations by 17%.[2]

These trends underscore a paradigm shift: an increasing reliance on developer innovation and an equally strong push for an identity security strategy.

The Time to Secure Developers is Now

Access must be strictly controlled, but you can't secure all of IT with standing accounts and vaults alone. The fact is, no organization wants to put a strain on its software developers. If security processes become too onerous, efficiency will suffer. If managers insist on tight restrictions and cumbersome reviews, the relationship between the security team and developers will break down. When you make the safe option inconvenient, you incentivize risky behavior.

Effective and secure cloud access for developers rests on one central principle: it must be loved by CISOs and invisible to developers. Without modernizing our identity security strategies, we can't protect one of our most critical identities.

89%

organizations embracing a multi-cloud approach.[3]

95%

organizations reporting a cloud-related breach in the last 18 months.[4]

40%

of data breaches involved data stored across multiple environments.[5]

$4.88M

Average cost of a data breach.[6]

$5.17M

Average cost of a breach in public clouds.[7]

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

[2] U.S. Department of Labor, Bureau of Labor Statistics, Occupational Outlook Handbook, Software Developers, May 2023.

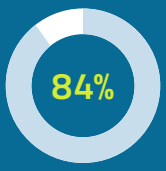
[3] Flexera, Organizations Embracing Multi-cloud, 2024 State of the Cloud Report, March 2024.

[4] Tenable Blog, Tenable Cloud Security Study Reveals a Whopping 95% of Surveyed Organizations Suffered a Cloud, May 2024.

[5,6,7] IBM, Cost of a Data Breach Report 2024, July 2024.

Cloud Security: A Pressing Concern for Enterprises

increase in cloud intrusion in 2024.[8]



of organizations will use three or more cloud service providers in the next 12 months.[9]

of security leaders say that cloud workloads are home to the riskiest, most unmanaged identities that exist within an organization.[10]

Organizations need a convenient, cloud-native identity security solution that embraces all the advantages of cloud, like elasticity and automation, without interrupting developers for the sake of security.

Security teams must adapt at the pace of their engineering velocity and double down on identity security to secure their cloud investments.

TODAY'S SECURITY CHALLENGES

Multiple clouds, disparate controls: Cloud service providers may agree on the importance of identity security, but not on the controls and integrations that enforce it. This places a massive burden on the identity security teams responsible for building and enforcing access control policies. Having to manage this sprawl can leave gaps open for an innovative attacker.

Undefined roles: Before the cloud, most applications existed in a relatively static architecture with simplistic access control policies. In modern applications, there are 40,000 possible entitlements mapped to the roles of individual users across 1400 services in the largest three cloud providers. These entitlements vary greatly and make approval processes extremely burdensome. Organizations that don't want to accept the costs of increased downtime end up granting engineers more access than may be necessary in order to accelerate troubleshooting.

Lift-shift first, security second: When migrating existing applications to a cloud infrastructure, existing access controls are rarely fully compatible with cloud service provider (CSP) IAM paradigms. Organizations must create additional roles and permissions, increasing the number of vulnerable. identities. Unfortunately, challenging cloud adoption goals and strict budgets push teams to skip over best practices, increasing complexity, attack surface size and the need for governance.

"Just make things work" mindset: Engineering speed provides value to businesses: the faster you release software, the faster you meet customers' needs. Any security decisions that slow this pace can impact the bottom line. To protect developers' flow state, many teams allow broad access rather than investing the time to set the least privileged permissions.

Tooling preferences: When business success is measured by speed and innovation, invisible solutions that work natively with preferred tools is critical. Software engineers don't want to change their preferences in the name of security.

[8] CrowdStrike, Global Threat Report 2024, February 2024.

[9,10] CyberArk, "2024 Identity Security Threat Landscape Report," May 2024.

Evaluation Criteria

For bad actors, the number one goal is to gain access so they can do reconnaissance, move laterally and escalate privileges to exfiltrate data, disrupt operations or deploy ransomware. For developers, the most crucial aspect is access when they need it, without requiring manual approvals. Security teams are worried about all of the above: the risk of an attack and the risk of driving the development teams mad.

So what does this process look like in the cloud? Businesses must choose a solution that makes the safe option convenient for developers. We recommend the following features:

- Native access to clouds
- ZSP enforcement
- Controls on T.E.A. (time, entitlements and approvals)
- Clean and clear audit reporting, and
- Unified identity environment

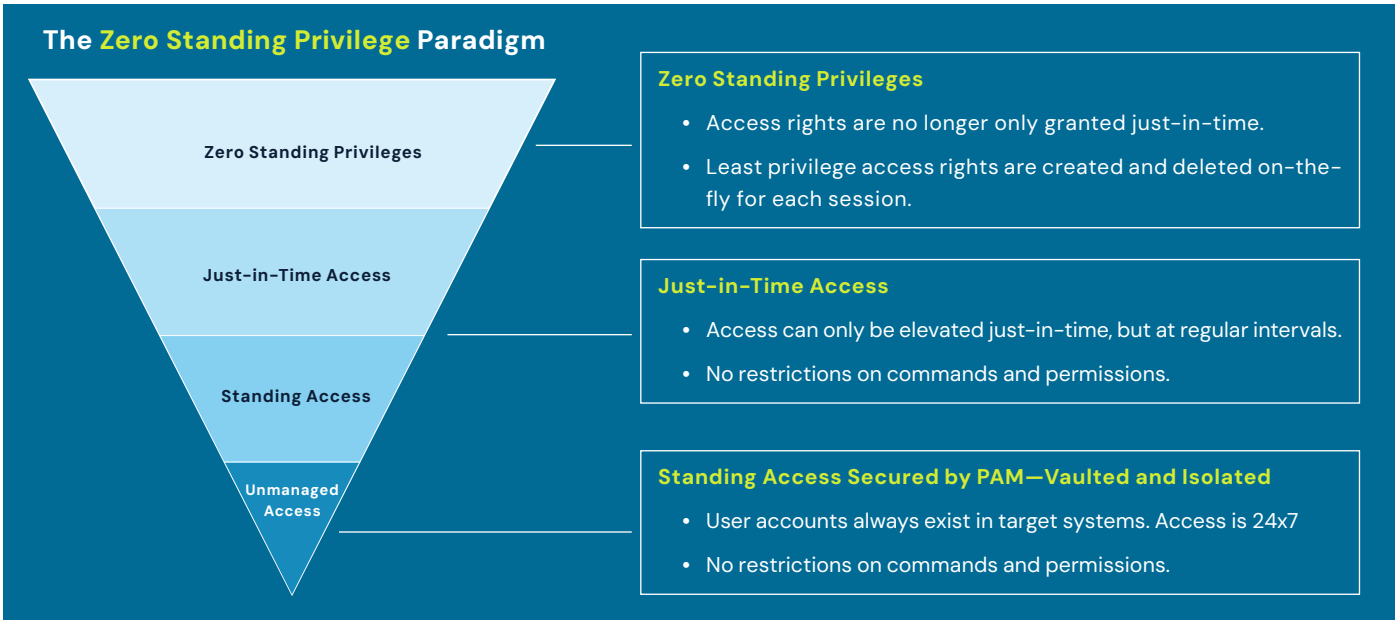
1. Native Access to Clouds

For developers, succeeding in today's cloud-first environment means gaining native access to multi-cloud consoles and staying clear of attackers with zero drama. Cloud-native means it's not just made in the cloud, but ***for*** the cloud. Developers are empowered to launch protected and monitored sessions natively (without the need for a jump server) in order to achieve seamless disruption-free access.

Imagine that an application running in AWS, Azure or GCP is not functioning as expected. A DevOps engineer would need to gain access to the CSP console or command line interface (CLI) to diagnose and fix the issue. But first, they need to access a privileged access management (PAM) solution that securely manages the CSP credentials before connecting to the cloud console via session management. For an engineer, this is as tedious and time-intensive as it sounds. They would love to have native access to the CSP CLI to get the job done sooner.

In a critical situation, the right solution allows the engineer to request on-demand access elevation to securely request and rapidly receive the elevated entitlements needed to save the day.

With zero standing privileges (ZSP), developers can natively access the CSP console or CLI using their own federated identity without having to use another solution protected by standing credentials. This greatly improves the user experience while providing native access to the CSP console, which further strengthens security. Let's look more closely at ZSP.



2. Zero Standing Privileges

Nearly all identity security paradigms agree on the 'never trust, always verify' process of Zero Trust. However, in the highly complex world of cloud security, reducing the availability and impact of access isn't always realistic. How do you give developers access to the one thing they need to do—and nothing else?

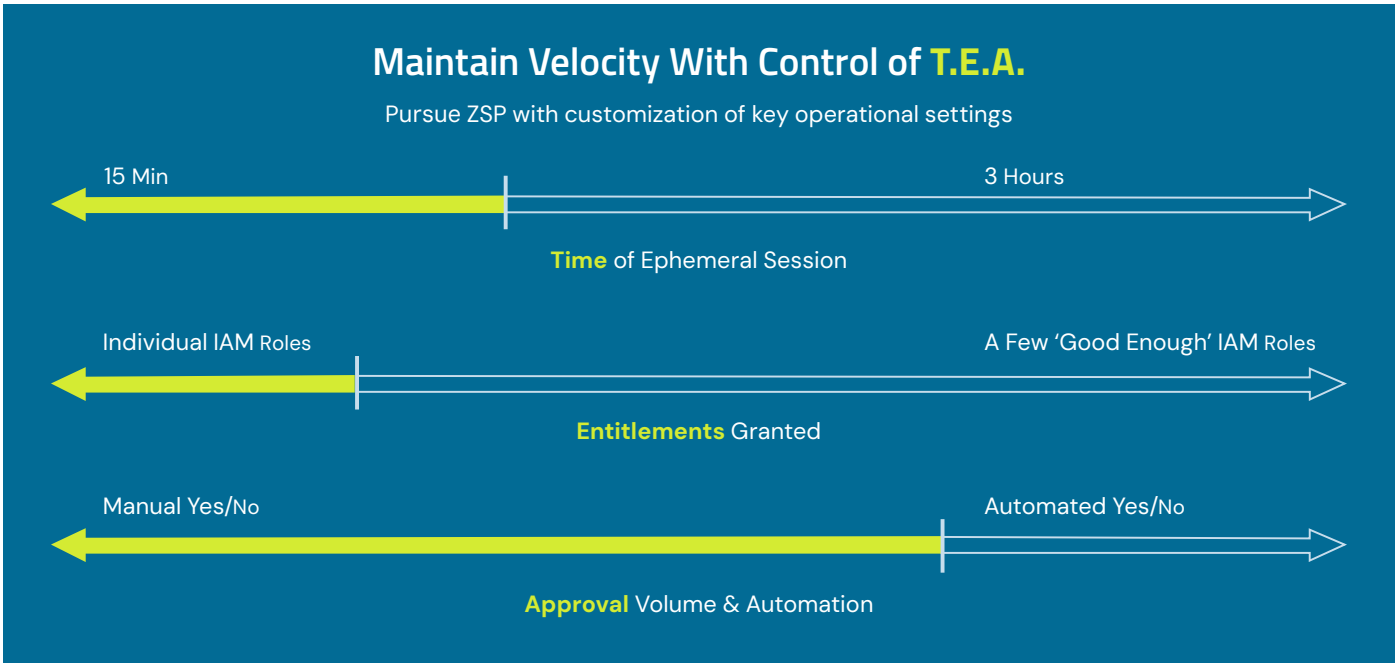
Zero standing privilges enforces real-time least privilege in the cloud by granting only the relevant permissions a user needs — and only when needed — to accomplish a given task. It removes standing privileges, limits implicit trust and provides several levels of control to verify access. If a threat actor takes over an account, their options are extremely limited without any access.

3. The Right T.E.A for the Job

T.E.A makes the concept of ZSP easier to manage. By combining the concept of time, entitlements and approvals (TEA), you no longer need to manage standing credentials and force developers and cloud engineers to use them.

Nothing frustrates a developer more than being stopped in the middle of a coding sprint due to lack of access. But you don't want standing credentials with privileged entitlements available at any given time for end users (and potentially attackers) to utilize. Here's how it should work:

- **Time: the duration of access.** With granular control of session durations, you can ease administrator pain, increase developer confidence and minimize the time-to-approval.
- **Entitlements: the level of access granted.** With dynamic provisioning of least privilege entitlements, the right solution provides organizations with comprehensive visibility to provision entitlements only to workloads that are assigned a specific attribute (e.g., 'K8s' or 'Test').
- **Approvals: the level of checks undertaken upon access.** True ZSP is only attained when the request is subject to an approval – but approvals can be a time-intensive burden. By integrating approvals with IT service management (ITSM) and ChatOps tooling, admins can accelerate provisioning. These approvals can be subject to risk-based or attribute-based controls (ABAC) tagging in the CSP. This greatly reduces the number of total approval tasks compared to competitive solutions, which often requires approval for every individual role requested.



4. Audit and Reporting

The right PAM solution should not only isolate privileged sessions to prevent session hijacking and lateral movement; it should also provide a clear reporting trail for compliance audits and inquiries. As privacy and security requirements for customers and systems increase around the globe, regulators and auditors will expect to see a solution that fulfills (or exceeds) data protection requirements. The right PAM solution should:

- Maintain strict governance over access to privileged accounts to defend against cyberattacks and protect against data theft and abuse.
- Provide detailed reporting on privileged account information and usage, simplifying compliance audits and risk assessment exercises.
- Automatically detect anomalous behavior to identify in-progress attacks in real-time, accelerate incident response and simplify incident reporting.

5. Unified Identity Environment

Developers want unrestricted access to navigate smoothly across the enterprise, but their access to the cloud is typically secured by multiple isolated third-party security tools. In fact, 94% of security leaders use more than 10 vendors for identity-related cybersecurity initiatives.

Uniform security controls that integrate existing IAM and privileged access management (PAM) solutions should allow dynamic tailoring to secure developer access across all cloud environments. A layered approach focused on securing identities and centrally delegating access to the entire cloud estate from a single platform

Single sign-on (SSO), adaptive multi-factor authentication (MFA) and PAM solutions work together seamlessly, allowing users to log in to multiple applications with a single set of credentials, and adjusting authentication factors based on each user's risk profile.

Choose a vendor with a mature product that demonstrates strong partnerships and alliances across the security landscape. Given the increasing interdependence of systems and the demands of a Zero Trust approach, this integration is mission-critical. Look for features like scalable and resilient architecture, comprehensive identity protection for both human and non-human users and support for hybrid and multi-cloud environments.

Be wary of vendors that might offer lower-cost solutions that lack integration or support for key alliances. While they may seem budget-friendly initially, a vendor that skimps on proven integration techniques or fails to provide experienced service experts can leave your organization with stranded technologies, system risks and increased development costs down the line.

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

How Well Can Your Security Vendor Secure Privileged Access in Cloud Environments?

Baseline Requirements	Elevated Requirements
Implement Zero Standing Privileges Replace always-on access with configured policies based on roles, workload attributes and privileged access needs provisioned JIT.	**Build a proactive strategy to get ahead of audits** Deliver required evidence, artifacts and reports centered on continuous visibility for access to all identities.
Maintain frictionless native access Support existing developer workflows and integrate with existing tooling.	**Define models permitting a "critical situation" level of access** Ensure on-call cloud engineering teams can quickly solve problems without waiting for approvals.
Centralize secrets management and governance to a single hub Allow developers to use their preferred tooling so the business can apply necessary industry and internal standards.	**Isolate and monitor high-risk access to cloud workloads and services** Streamline processes by storing audit trails in the same place as web apps or on-premises session logs.

Secure Developers in the Cloud with a Unified Platform

CyberArk delivers measurable cyber risk reduction, operational efficiency, secure digital transformation and audit compliance. By leveraging CyberArk's unified platform, organizations can ensure secure, seamless access while minimizing risk and maximizing productivity.

Key capabilities include:

- Validating users with context-aware, Zero Trust access controls.
- Centrally securing secrets for applications and machine identities.
- Limiting lateral movement with privileged session isolation and just-in-time (JIT) elevation.
- Simplifying access to cloud environments with a unified platform for both human and non-human identities.
- Providing comprehensive audit trails for cloud administrative access to meet compliance requirements.

With these capabilities, CyberArk enables organizations to secure their cloud environments and developers efficiently, ensuring operational excellence and regulatory compliance.

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™