Securing Developers

With CyberArk Secure Cloud Access

CYBERARK®

SOLUTION BRIEF

Secure developer access at cloud velocity — on the only identity security platform with zero standing privileges capabilities.

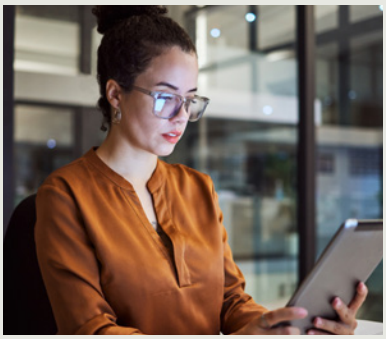
71%

Incident response data indicates a 71% increase year over year in volume of attacks using valid credentials of all incidents X-Force responded to in 2023.

30%

The X-Force team discovered that for the first time ever, abusing valid accounts became cybercriminals' most common entry point into victim environments, representing 30% of all attacks.

Source: IBM, "2024 IBM X-Force Cloud Threat Landscape Report", October 2024.



Challenge

Cloud Convenience Creates Complexity

The cloud has enabled faster, more reliable and more scalable delivery of software — and the first experience an organization will have in the cloud is identity. Identities and credentials are required to create a cloud IT organization's foundational AWS root accounts, Azure tenants, and GCP projects. And yet, basic security is still not in place — over 75% of cloud identities are not protected with foundational controls like multi-factor authentication.

Attackers Know This — and They Exploit It

The core identity security challenge for securing developers is that when you make the safe option inconvenient, you incentivize risky behavior. Security teams need to grant developers the access they need when they need it. For cloud-native businesses using a range of cloud service provider (CSP) services, it's tough to know who needs access to what. And, even if access is defined, approval processes can be a burden. This means that organizations must effectively choose to grant more access than may be purely necessary, introduce security risks, or accept the costs of increased downtime.

Attackers know this and realize the security debt compromised by these development challenges. They look for ways to exploit this gap, breaching cloud workloads every month.

Breaching one account with the right entitlement allows an attacker to build data centers of expensive infrastructure or access sensitive data stored in the cloud. Access must be strictly controlled. Enforcing different security controls for users or administrators is not an option.

So, how do we design a better experience for our developers and cloud engineers while keeping security foundational?

THE RIGHT TEA FOR THE JOB

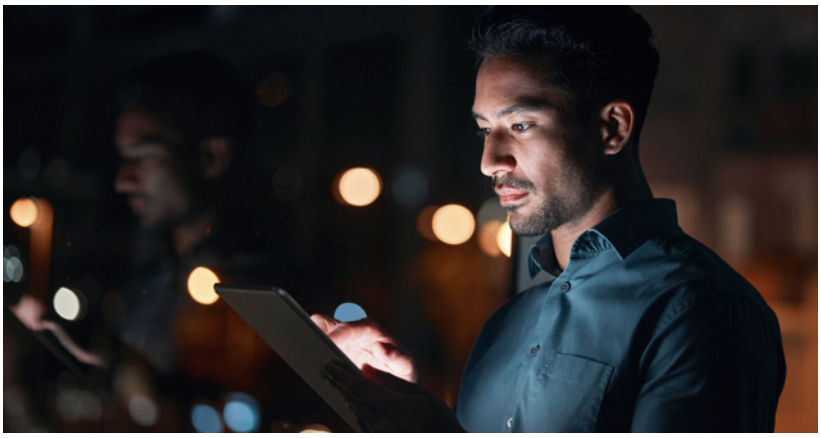
By combining the concept of time, entitlements and approvals (TEA), security teams no longer need to manage standing credentials for "what if" scenarios and force developers and cloud engineers to use them.

- **Time.** Secure cloud access provides granular control of time session durations. Access is only approved for the window of time required.
- **Entitlements.** No entitlements are available by default, providing an essential layer of security.
- **Approvals.** Only after the necessary approvals are met (automatic, contextual, manual) will privileged access be granted.

Solution

Secure, Native Access for Developers

The CyberArk Identity Security Platform offers native, secure cloud access for developers, enabling 35% improved productivity[1] for developers, while delivering upon cyber risk reduction. The solution helps organizations better control and secure multi-cloud environments, using elevating just-in-time (JIT) access with zero standing privileges (ZSP). By taking this approach, developers receive the permissions they need to do their jobs while reducing risks of credential theft by removing excessive access and unnecessary entitlements. Developers retain their native user experience without impacting their productivity.



Defend Your Cloud With CyberArk

CyberArk's cloud security capabilities are built to empower the developer to drive operational efficiencies. Developers can delegate and automate access requests, reducing the time and effort required to request access. Developers can also customize workflows using the CyberArk Identity Flows capability, allowing for low code building of workflows that model business processes and meet the needs of a dynamic work environment.

With CyberArk cloud security, organizations can achieve risk reduction, audit and compliance outcomes, while enabling developers to remain secure as they deliver software faster and better in the cloud.

Learn more about how to secure developers.

[1] Source: IDC White Paper, sponsored by CyberArk, "The Business Value of CyberArk," IDC #US52652224, November 2024.