CYBERARK®
THE IDENTITY SECURITY COMPANY®

WHITEPAPER

2025 AWS Playbook: Identity Security and Cloud Compliance

Table of Contents

Introduction

As the digital landscape continues to evolve, the rapid proliferation of cloud infrastructure and services often leads to the explosion of identities with high-risk access. The dual risks of credential-based identity compromise attacks, misconfigured cloud permissions and compromised access and entitlements can be extremely difficult to secure. Identity paradigms, entitlements and roles vary greatly across cloud providers and pose a significant challenge for cloud security teams and organizations using multiple cloud providers. This entitlement sprawl sits at the center of the challenge to keep up with the constant changes that make up the dynamic nature of the cloud. Implementing least privilege is a mission-critical identity security control recommended by leading cloud service providers (CSPs) like AWS.

Cloud migration and digital transformation have become commonplace for many modern enterprises. While migrating to the cloud, understanding the security requirements and protecting data, applications and workloads has become critical. Amazon Web Services (AWS) remains a dominant force in the competitive cloud service provider market, steadily widening its lead over both established players and new entrants. According to the Flexera 2024 State of the Cloud Report, AWS was the most adopted cloud service provider, with 49% of respondents reporting using AWS for significant workloads.

KEY DRIVERS FOR AWS CLOUD STRATEGY:

1. Best-in-class capabilities
2. Redundancy and high availability
3. IT modernization
4. Mergers and acquisitions
5. Flexibility and scalability
6. Operational efficiency

The highly complex world of cloud security calls for organizations to demonstrate the ‘never trust, always verify’ process of Zero Trust. Zero standing privileges (ZSP) and least privilege both play crucial roles in solving privileged access challenges. The ZSP philosophy both removes standing privileges to limit implicit trust and provides several levels of control to verify access. Just-in-time access can help reduce the risk of credential theft posed by standing access as a user cannot log in until this temporary access is granted. Least privilege restricts users and applications to the minimum permissions required for their tasks. The risk of compromising an identity with standing access enables an attacker to access critical infrastructure, steal sensitive data or disrupt cloud-hosted services by changing configurations.

According to the CyberArk 2024 Identity Security Threat Landscape Report, 21% of respondents say regulatory compliance is one of their top two cloud security concerns. Implementing the concept of ZSP has benefits beyond risk reduction, especially for audit and compliance programs. However, identity has evolved in line with cloud services. Every relationship between components deployed within the cloud, even between administrators, engineers, and the services they are build or maintain is controlled by entitlements mapped to roles. These stakeholders can quickly become burdened with managing thousands of permissions and identities across separate cloud platforms, each with distinct permission and entitlement paradigms.

Achieving compliance with industry standards and sustaining regulatory compliance for IT systems is a more challenging task in the complex cloud environment. Cybersecurity compliance enables us to meet industry standards and regulatory requirements to mitigate cybersecurity risk.

This whitepaper covers identity security compliance challenges, benefits and best practices for securing privileged access in AWS.

Modern Identity Security Challenges in the Cloud

Rapidly expanding cloud permissions pose a significant challenge for cloud security teams. In large enterprises, managing cloud permissions becomes a major security risk and hinders operational efficiency. Develop identity security programs that align with people, processes and technology to limit your exposure and better control risk.

Data Breaches

Data breaches can occur due to a lack of scalable identity access management systems, failure to use multi-factor authentication (MFA), weak passwords and poorly managed keys and certificates. Numerous breaches have been the result of excessive permissions being assigned to users, roles and machines in cloud environments. Managing the data in the cloud and digital sovereignty is another big concern in cloud environments. Data's inherent value and its impact on business operations made it a prime target for attackers. Identity and access management (IAM) is the key to mitigating data breaches and accelerating the importance of strong security practices.

Weak Identity, Credential, Access and Key Management

Many organizations poorly implement basic identity security controls in their cloud environments. This increases complexity and the need for governance and widens the attack surface, as organizations now have a greater variety of identities and credentials that can be compromised. Instead, most of the cloud identities are not protected with MFA. In AWS, 60% of IAM users have active access keys older than one year, with over half unused for more than 90 days.[4]

ENTERPRISE TOP CLOUD CHALLENGES

80%

of organizations experienced an identity-related breach due to a software supply chain attack.[1]

In the next 12 months

84%

of organizations will use three or more CSPs.

40%

of data breaches involved data stored across multiple environments.[2]

$5.17M

Average cost of a breach in public clouds.[3]

These unsecured or long-lived credentials can be exploited by attackers to enable unauthorized access through cryptojacking, data breaches, destruction of intellectual property and other sensitive data, ransomware and supply chain disruption. In the rush to innovate, organizations often let developers and engineers operate with too many permissions to launch and modify cloud infrastructure.

The rapid growth in SaaS applications further complicates entitlement management and increases privilege creep. To mitigate the sprawl, security teams need centralized IAM solutions, adherence to the principle of least privilege and regular audits to identify and eliminate unnecessary permissions.

---

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

[2,3] IBM, "Cost of a Data Breach Report 2024," July 2024.

[4] DataDog, "State of Cloud Security," Nov. 2024.

Misconfiguration and Inadequate Change Control

Misconfiguration and inadequate change control in the cloud environment can lead to unauthorized access, data leakage, or malicious manipulation. Attackers and malicious insiders can exploit these excessive, always-on permissions to access critical cloud infrastructure, steal or alter sensitive data, or interrupt cloud-hosted services. Automation tools, testing and validating changes, and documenting and reviewing the changes can help avoid this challenge.

Account Hijacking

Malicious attackers use phishing methods, vulnerability exploitation or stolen credentials to access highly privileged accounts in the cloud. Account hijacking enforces full compromise including control of the account, its services and the data within. Hijacking allows malicious actors to use cloud workloads for crypto mining, steal data and attack further targets. The impact can be severe — from significant operational and business disruptions to eliminating organization assets, data and capabilities. Hijacking enables threat actors the ability to use cloud workloads for crypto mining, steal data and attack further targets and create significant operational and business disruptions to complete elimination of organization assets, data and capabilities.

Insider Threats

Insider threats are current or former employees, contractors or other trusted third parties who use their privileged access to act in a way that could negatively affect the organization. These trusted insiders have direct access to the company network, sensitive data and intellectual property (IP), as well as company policies or other information. Strong privileged access controls help ensure that humans, applications and machines have only the necessary levels of access to sensitive applications and infrastructure to do their jobs and that activities occurring within the cloud environment aren't at risk.

Cloud misconfigurations are the third most common initial attack vector and account for 15% of initial attack vectors in security breaches.

Source: IBM, Cost of a Data Breach Report 2024, July 2024.

ZERO TRUST ALIGNMENT

In the next 12 months,

64%

of organizations have or will prioritize Identity Threat Detection and Response (ITDR) capabilities.

100%

of organizations indicated that they will prioritize new tools or technologies in the next 12 months. Topping that list: ITDR.[5]

This emerging security discipline will help organizations like yours manage and secure the massive number of human and machine identities across the enterprise.

ITDR enables Zero Trust initiatives, keeps identity as the central focus and protects what's most precious to your organization: data.

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

Benefits of Cloud Identity Security

Security is the top priority while moving to the cloud. Cloud identity security helps ensure compliance with regulations and industry-specific compliance standards to secure the cloud estate and rapidly reduce risk across hybrid and AWS environments. Organizations can leverage cloud identity security to measure and visualize exposure levels, implement and continuously and validate least privilege, helping to meet compliance with regulations and frameworks. Leveraging cloud security and compliance supports resiliency, performance, privacy and compliance needs while reducing operational costs.

1. Compliance and Governance

Cloud identity security compliance helps reinforce security while mitigating risks and industry-specific compliance standards as well as cloud compliance requirements. Organizations that suffer data breaches could be out of compliance with regulations governing sensitive customer data. The regulations that apply to an enterprise may not differentiate between a data center and a cloud; they typically target the data regardless of where it is stored. When it comes to audit and compliance, enterprises must have people, processes, and technology strategies to comprehensively secure their modern environments to the same degree as on-premises workloads. Cloud identity security ensures compliance and built-in compliance features to meet regulatory requirements such as HIPAA and GDPR. Additionally, compliance features enforce data encryption, secure data transmission protocols, and robust data privacy measures for data protection and privacy and improve audit and compliance review processes with informative data on user patterns and activities.

REGULATIONS AND CLOUD SERVICE PROVIDER FRAMEWORKS WITH IDENTITY SECURITY REQUIREMENTS	
REGULATIONS	**FRAMEWORKS**
• Service Organization Controls 2 (SOC 2)	• NIST Cybersecurity Framework
• General Data Protection Regulation (GDPR)	• NIST 800-53 and NIST 800-171 standards
• The California Consumer Privacy Act (CCPA)	• MITRE ATT&CK Framework
• ISO 27001	• Cloud Security Alliance Cloud Controls Matrix
• Payment Card Industry Data Security Standard (PCI DSS)	• Amazon Web Services – IAM Security Best Practices
• The Health Insurance Portability and Accountability Act (HIPAA)	• Amazon Web Services – Well-Architected Framework (Security Pillar)
• Sarbanes-Oxley Act (SOX)	
• The Digital Operational Resilience Act (DORA)	

2. Centralized Identity Security for AWS Environments

Organizations need centralized control of cloud identities throughout their cycle. Excessive and unused cloud permissions expose organizations to the risk of a data breach, potentially resulting in significant regulatory and financial penalties. Centralized cloud security allows quickly identify and mitigate the risks in the cloud infrastructure. Enterprises need a centralized and defined route to control identity within their chosen cloud providers. Simplifying user lifecycles, enforcing access control policies and gaining visibility into administrator actions are essential for compliance and operational efficiency, as is maintaining consistency of security controls. This helps address the skill shortage and knowledge gap organizations need for cloud development teams, as they can reduce the number of cloud experts required on the team by simplifying uniform controls across cloud.

Identity is the very first experience of the cloud an organization will have. For example, identities and credentials are required to create the foundational AWS root accounts of a cloud IT organization. Every relationship between components deployed within the cloud, even that between admins, engineers and the services they are building or maintaining is controlled by entitlements mapped to roles. These entitlements and roles vary greatly across cloud providers. This entitlement sprawl is a major bump in the road to secure cloud.

3. Native User Experience

Imagine that an application running in AWS and is not functioning as expected. A developer would need to gain access to the CSP console or command line interface (CLI) to diagnose and fix the issue. Too many organizations fail to secure this privileged access properly — applying MFA as the only security measure. Others make developers jump through hoops to use shared credentials. Developers need seamless access to cloud resources, while security teams need to secure privileged access without slowing them down.

By provisioning zero standing privileges across the AWS environments, security teams have peace of mind knowing that developers can easily request on-demand access elevation and rapidly receive the elevated entitlements needed to save the day. Developers can natively access the console or CLI using their own federated identity, which greatly improves user experience and aids their productivity.

4. Integration with Cloud Services

Cloud identity security provides integration support with cloud services and applications and supports industry-standard protocols such as OpenID Connect and Security Assertion Markup Language (SAML), enabling interoperability across diverse ecosystems. It provides the broadest integration support in AWS with the same features. Ensure that integrations are set up with the common tools used by the cloud security teams, cloud admins and infrastructure engineers. Integrations to ITSM and ChatOps tooling help seamlessly integrate access approval workflows and notifications and consistently and centrally analyze, secure and monitor access across AWS environments.

Three Phases to Cloud Identity Security Success

The cloud represents a major change for the business where many established identity and access management best practices no longer apply or require controls to be enforced in differing ways. This shift means there is often confusion as to where to start and how to rapidly address risk in the cloud. Nearly 99% of organizations who were victims of an identity-related breach faced a direct impact to their business in the last 12 months.[6]

Phase #1: Meet Baseline Requirements

The first step starts with the relevant industry standards you must meet in to remain compliant (e.g., SOC 2, PCI and NIST). Then 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 to apply industry and internal standards and fix high-risk misconfigurations that could result in vulnerabilities.

Phase #2: Standardize Audit and Reporting

The second step focuses on bringing entitlements and roles into compliance. Organizations must standardize identity security hygiene to satisfy audit and compliance and this process starts with a push to define and maintain standards. These standards need to be sustainable and realistic, based on the access the user base requires. Use a data-driven approach to remove access to never/seldom-accessed systems and implement preventative controls to halt new unapproved roles and access. Start by creating standardized reports that continuously benchmark the current state against industry and internal standards.

Phase #3: Continuous Improvement

The third phase focuses on automation with proactive security in mind. Start by implementing automation to enforce industry and internal standards for both human and service-to-service access. Reduce manual work and improve operational efficiency by automating compliance and audit approval processes. This means all your new cloud environments will have access policies in place and the roles and identity settings will be configured correctly ensuring security and compliance for the enterprise.

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

Best Practices to Secure Cloud Identities

Today, most of the customers turn to AWS partners to help them achieve their digital transformation objectives and solve complex technical challenges. More than half of employees have access to sensitive data, often via the rapidly increasing number of applications enterprises deploy. The security teams now challenged themselves to balance organizational risk mitigation while managing an increasing number of non-human identities and secrets across sprawling public cloud, private cloud and on-premises environments. The following are five best practices to better control risk and secure cloud identities.

1. Zero Standing Privileges (ZSP)

ZSP is the best way to solve security challenges in the cloud. Access is provided just in time with ZSP, enabling holistic control of identity security within AWS. ZSP is a strategic step to move closer to a Zero Trust model and enables you to grant just-in-time (JIT) privileges across your cloud environment. The ZSP model reduces cloud risk surface and helps you comply with cloud access control requirements stipulated by leading industry standards like NIST and SOC 2. Just-in-time elevation and least privilege reduce risk for the most sensitive sessions in the public cloud - those that involve configurations of cloud environments.

2. Native and Unified Control of Secrets

The cloud is essential for accelerating growth, improving efficiency and remaining competitive and most companies are now developing applications in the cloud. Automation, DevOps and the growth of cloud environments have led to an explosion of machine identities — also called non-human identities — for applications, cloud workloads, containers, services and other automated tasks. These non-human identities all have accounts, credentials and secrets that must be secured. Bringing secrets management into one solution also allows security teams to scale their efficiency — applying policies consistently and simplifying audit tasks. Identity security strategies in cloud environments are able to manage native vaults within the cloud and unify control of secrets leveraged across the many accounts/tenants/organizations that make up an AWS estate.

Securing privileged access for all cloud identities

People and Processes

- Include developers, site reliability engineering (SRE) and data science teams in cloud identity security programs to drive adoption of controls.
- Conduct holistic reviews to implement and continuously assess least privilege for all human and machine identities.
- Leverage just-in-time elevation for all operational access in cloud environments, to move towards the ideal state of ZSP.
- Centrally store and routinely rotate any necessary standing credentials used by human and machine identities.
- Make progress towards the ideal state of ZSP with reporting to achieve compliance with requirements including NIST, PCI DSS and SOC 2.

Technology

- Integrate access request workflows with ticketing and ChatOps tools used by developers to maximize adoption.
- Improve security posture and minimize risk in AWS environments by moving identities to ZSP.
- Elevate operational access on a just-in-time basis.
- Centralize secrets management to a single credential repository for consistent policy enforcement, while allowing developers to use their preferred cloud service provider (CSP) tooling.

3. Insight to Action

An Insight to Action framework enables you to gain the right set of insights and take meaningful riskreduction actions. This Insight to Action framework links risk insights to remediation recommendations that can be applied programmatically, through click-and-remediate solutions or automation. Ensure that integrations are set up with the common tools used by the cloud security teams, cloud admins and infrastructure engineers. Integrations to ITSM and ChatOps tooling help seamlessly integrate access approval workflows and notifications. Finally, it helps to quickly implement a proposed remediation, yet still allows for a clear and easy path to return the removed entitlements when required during an outage.

4. Audit and Accountability

Understanding and attesting actions in the cloud is meant to be easy. When you're working in AWS or hybrid environments, the number of separate vaults for credentials and secrets can quickly get overwhelming. A centralized secrets management solution can give you a single pane of glass rather than waiting for each vault to rotate and manage passwords and bringing information from various of vaults to create an audit trail. With audit and accountability, identify malicious and erroneous user activity within cloud consoles with step-by-step web session audit and monitor both standing and just-in-time access. Every cloud provider offers a centralized logging service, but organizations need deeper visibility. Federated identities and role assumptions often inadvertently mask the identity undertaking work in an actual cloud environment. Identity security programs need to be able to make every action attestable to meet even the most basic audit requirements.

How CyberArk Solutions Can Help Support Compliance

Reasons to Consider Compliance

Identity Management, Authentication and Access Control

Access to physical and logical assets and associated facilities is limited to authorized users, processes and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

- The CyberArk identity security platform manages access permissions and authorizations, incorporating the principles of least privilege and separation of duties.
- CyberArk Secure Cloud Access (SCA) enforces just-intime access for operations in AWS environments following the principle of least privilege access. Sessions are also time-bound; hence, permissions are revoked at the end of a session.
- Additional identity security platform capabilities reduce standing access to compute workloads by implementing just-in-time access using attribute-based access control policies.

Protective Technology

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

- CyberArk Secure Cloud Access enables just-in-time access for operations in AWS environments following the principle of least privilege access. Sessions are also time-bound; hence, permissions are revoked at the end of a session.
- Additional identity security platform capabilities reduce standing access to compute workloads by implementing time-based access using attribute-based access control policies.
- CyberArk Secrets Hub does not define any access policies for the managed secrets.

SOC 2 Mapping

- The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
- The entity authorizes, modifies, or removes access to data, software, functions and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.
- The entity uses detection and monitoring procedures to identify changes to configurations that introduce new vulnerabilities and susceptibilities to newly discovered vulnerabilities.
- The entity authorizes, designs, develops or acquires, configures, documents, tests, approves and implements changes to infrastructure, data, software, and proce dures to meet its objectives.

- The Identity Security Platform centrally manages access for infrastructure and software and access credentials are implemented on the network or access point. While credentials are removed and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.
- MFA is built-in for strong authentication or integration with any SAML-based IDP. The platform provides a single centralized interface for provisioning human users and service accounts and controls the authentication process based on credentials or tokens.
- Integration with CyberArk Secrets Hub and CyberArk Privilege Cloud helps to securely and centrally manage cloud secrets.

Conclusion: Next Steps for Adopting Cloud Identity Security

The cloud is the future for the modern enterprise, with most organizations choosing AWS, either for a lift and shift migration or to build new cloud-native applications. The cloud brings levels of efficiency to enterprises that could never be realized in legacy environments.

Public cloud provider adoption is influenced by the organization's cloud usage level. As organizations mature, they tend to gravitate toward market leaders. As was the case last year, AWS is used more frequently by organizations that have been using the cloud over a longer period and are heavy cloud users. Implementing cloud security compliance measures and adopting best practices like ZSP, least privilege and just-in-time privilege access across AWS cloud will help ensure organizations minimize their security risks.

Why Organizations Should Adopt Cloud Identity Security

1. Delivers measurable cyber risk reduction.
2. Enables operational efficiency.
3. Secures key initiatives including cloud migration and digital transformation.

Next Steps

Want to learn more about how cloud identity security can help secure cloud identities and environments to improve operational efficiency? Get a free trial today.

About CyberArk

CyberArk (NASDAQ: CYBR) 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 environments 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 https://www.cyberark.com, read the CyberArk blogs or follow on LinkedIn, X, Facebook or YouTube.

CYBERARK®