
 info@archerround.au

 1800 841 224

 <https://www.archerround.com>



30 years of Cybersecurity Excellence



Archer & Round Cybersecurity Report

Securing Cloud Environments: Best Practices for 2025

June 2025 Edition



info@archerround.au



1800 841 224



<https://www.archerround.com>



ARCHER & ROUND

30 years of Cybersecurity Excellence

Executive Summary

Cloud adoption continues to accelerate globally, with businesses relying heavily on platforms like AWS, Microsoft Azure, and Google Cloud for their operations. However, this shift has also expanded the attack surface for cybercriminals. Cloud misconfigurations, identity management gaps, and increasingly sophisticated attacks are among the leading threats in 2025. This report highlights the key risks to cloud security and outlines best practices for building robust, cloud-native defenses that scale with your organization.

Key Findings

Misconfiguration is the #1 Cloud Threat.

Gartner reports that by 2025, 99% of cloud security failures will be the customer's fault, primarily due to misconfiguration and inadequate identity controls.

Data Breaches in the Cloud Are Increasing.

According to Microsoft's 2025 Cybersecurity Report, cloud data breaches rose by 25% in the past year, often due to insufficient access controls.

Identity is the New Perimeter.

Cloud security now hinges on robust identity and access management (IAM) as traditional network boundaries dissolve.

Multi-Cloud Complexity Increases Risk.

Many organisations use multiple cloud providers, complicating visibility, security policy enforcement, and incident response.

Zero Trust Architectures Are Becoming the Global Standard.

Cloud-native Zero Trust strategies are now essential to reducing exposure in highly distributed environments.



info@archerround.au



1800 841 224



<https://www.archerround.com>



ARCHER & ROUND

30 years of Cybersecurity Excellence

2025 Major Cloud Threats in 2025

THREAT TYPE	DESCRIPTION	EXAMPLE
Misconfiguration	Open storage buckets, weak permissions	Unsecured AWS S3 bucket leak
Credential Compromise	Stolen cloud account credentials	Phishing leading to account takeover
Supply Chain Attacks	Exploitation of third-party cloud integrations	Malicious code in SaaS plugin
API Security Gaps	Poorly secured APIs allowing data exposure	API abuse for sensitive data retrieval
Inadequate Logging	Lack of monitoring allowing undetected breaches	Delayed detection of lateral movement

Best Practices for Cloud Security in 2025

1. Adopt a Zero Trust Approach

Assume breach by default. Enforce least privilege access, verify continuously, and segment workloads.

2. Automate Cloud Configuration Management

Use tools like AWS Config, Azure Security Center, and third-party platforms to detect and remediate misconfigurations automatically.



info@archerround.au



1800 841 224



<https://www.archerround.com>



ARCHER & ROUND

30 years of Cybersecurity Excellence

3. Strengthen Identity and Access Management (IAM)

Enforce strong password policies, multi-factor authentication (MFA), and role-based access control across all cloud environments.

4. Secure APIs and Integrations

Apply strict API security controls, validate inputs, and monitor third-party integrations for vulnerabilities.

5. Ensure Continuous Monitoring and Logging

Utilise cloud-native security tools and SIEM platforms to maintain visibility and enable real-time threat detection.

6. Regularly Review Cloud Security Posture

Conduct periodic security assessments and penetration tests focused on cloud environments.

7. Encrypt Data at Rest and in Transit

Adopt default encryption settings for storage and network traffic to protect sensitive information.

8. Develop a Cloud-Specific Incident Response Plan

Include cloud environments in your organisation's broader incident response strategy and rehearse response scenarios.

Looking Ahead: Cloud Security is Shared Responsibility

All major cloud providers emphasize the Shared Responsibility Model, where the provider secures the cloud infrastructure, but the customer must secure data, identities, and configurations. Organisations that invest in proactive cloud security now will better protect themselves against the rapidly evolving global threat landscape.



info@archerround.au



1800 841 224



<https://www.archerround.com>



ARCHER & ROUND

30 years of Cybersecurity Excellence

Global Standards and Frameworks to Follow

- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27017:2015 – Cloud Security Controls
- CIS Benchmarks for Cloud Providers
- Cloud Security Alliance (CSA) Guidelines

Recommended Resources:

- AWS Security Best Practices
- Microsoft Cybersecurity Reports
- Cloud Security Alliance

Archer & Round Cyber Intelligence Team

Safe | Secure | Reliable

Contact us: info@archerround.com