PRAETORIAN

WHITE PAPER

Praetorian's Top Five Cloud Risks and Their Mitigations

We observed five major themes over 18 months of client engagements that spanned the three major cloud platforms.

INSIDE THIS REPORT

INTRODUCTION

The State of Cloud Security

On nearly every engagement, Praetorian found improperly managed secrets. Whether stored unencrypted in buckets, embedded in the source of cloud functions, or embedded in instance metadata, improperly managed secrets can significantly weaken the overall security posture of a cloud environment.

Praetorian analyzed the last 18 months of engagement data from Cloud & Infrastructure Security, Product & Application Security, and Hardware & IoT security services with cloud-based components. The breadth of the analysis spans 117 engagements, 654 findings, and 317 unique findings.

117

CLOUD ENGAGEMENTS ANALYZED
ACROSS AWS, AZURE, AND GCP

This whitepaper distills the major themes we have observed on client engagements that span the three major cloud platforms. Focusing efforts to avoid, mitigate, and eliminate the risks outlined in this paper will position organizations to have a strong cloud security foundation.

> **Key Finding:** The top five cloud risks represent the most common vulnerabilities we encounter across all three major cloud platforms. Addressing these foundational issues provides the greatest security improvement for the least investment.

RISK #1

Identity and Access Management

42%

of findings relate to IAM issues

The most prevalent category of cloud security weaknesses

Anyone who has spent time in cloud environments would predict—correctly—that the most prevalent flaws relate to Identity and Access Management (IAM). 42 percent of the findings we identified fell into this category.

On nearly every engagement, Praetorian found improperly managed secrets, including cloud access keys, database connection strings, and third-party service credentials. Whether stored unencrypted in buckets, embedded in the source of cloud functions, or embedded in instance metadata, improperly managed secrets can significantly weaken the overall security posture of a cloud environment.

One common issue was the age of IAM access keys, which often are quite old when we encounter them. Clients within our dataset had generated the keys once and then never rotated them. Since IAM keys typically are valid until revoked, the long-lived access keys increase the risk of account compromise.

IAM is complicated and developing an IAM policy that follows the Principle of Least Privilege is difficult. This combination often results in privilege escalation paths within cloud environments. Common scenarios include the promotion of overprivileged development configurations to production, the ability for a user to create or modify resources with privileges higher than they currently possess, or relationship-based attacks like role chaining.

Mitigation

- **Eschew static credentials** - Implement federated single-sign-on (SSO) for human accounts to enforce organization-wide security policies
- **Use short-lived credentials** - Temporary credentials from SSO solutions are preferred over long-lived access keys
- **Use cloud-native secrets storage** - Platform-specific secrets management for third-party and internal resources
- **Scope permissions tightly** - Limit secret retrieval permissions to only services that require them

RISK #2

Configuration Management

27%

of findings relate to configuration issues

The second most prevalent category of cloud security weaknesses

Configuration management is a broad category that covers configuration-based weaknesses outside the access, encryption, IAM, and logging categories. The risks in this category accounted for 27 percent of the overall weaknesses identified.

Issues in this category include:

- Absence of critical controls
- Misconfiguration of services that could lead to data exposure or privilege escalation
- Flaws in architectural design

Mitigation

All platform providers (AWS, Azure, GCP) have published security best practices, including architectural guidance. Users should base their design and implementation of cloud environments on this guidance.

> **Best Practice:** Further configuration of the selected components should follow the security guidance for the individual services. Each cloud provider maintains comprehensive documentation on secure configurations for their services.

- Review AWS Well-Architected Framework security pillar
- Follow Azure Security Benchmark recommendations
- Implement Google Cloud security best practices
- Use infrastructure-as-code with security scanning

RISK #3

Resource-Based Access Control

14%

of findings relate to resource access

Despite lower frequency, these present the most critical vulnerabilities

Resource-based access control-related vulnerabilities were the third most prevalent category of findings at 14 percent. Despite their relative infrequency, they presented the most critical vulnerabilities we identified.

Praetorian found misconfigured policies that included ECR, Lambda, SQS, and the best-known offender, S3. The impact of these vulnerable policies ranged from excessive internal access to anonymous access with all actions permitted on the service (wildcard Principal and Action).

Additionally, lax network access controls granted asset access to attackers outside the intended resource scope. These manifested as unconstrained Security Groups, overly broad provider permissions, and accidental public exposure of services due to insecure defaults.

In simpler terms, sensitive resources such as database instances, cloud functions, and compute instances were exposed directly on the internet due to misconfigured access controls. These exposed resources were susceptible to brute-force authentication attacks and resource exhaustion/denial of service.

Mitigation

Mitigating this risk means minimizing the attack surface of your cloud infrastructure. Users must scope resource-based access controls to only the principals requiring access.

- Avoid resource-based policies where possible; use fine-grained IAM policies instead
- Create allowed list of known source IP addresses
- Rearchitect network access over private connections (VPC peering or Direct Connect)
- Enable tighter network access controls for all resources

RISK #4

Logging and Monitoring

Logs are essential to know what's happening within cloud infrastructure, yet mismanagement or lack of them constituted the fourth most-prevalent theme in our work over the past year. Without accurate logs, engineering teams may be blind to the actions and events occurring within their accounts and subscriptions and unable to perform incident response should an event occur.

Some quirks exist even when logging is enabled, depending on the cloud provider. For example, certain high-value activities may not be logged by default, or logs may be stored in locations that are difficult to query or analyze.

Mitigation

Organizations should enable logging of all meaningful actions throughout a resource's lifetime, including creation, modification, and deletion. Best practice also ensures a log for all global and account-level operations.

Critical Actions to Log:

- All IAM changes (user creation, policy modifications, role assignments)
- Resource creation, modification, and deletion events
- Access to sensitive data stores and resources
- Failed authentication attempts and access denials

Users must also monitor the logging once they have enabled it properly. Configuring alerts for well-known IAM abuse cases and access/modification/deletion of business-sensitive resources should be the baseline for establishing effective monitoring.

RISK #5

Data Protection

Data protection generally falls into two major categories: data in transit and data at rest. Protecting data in both states helps protect the confidentiality of the data and prevent its unintended exposure. We found enough instances of clients mishandling one or the other (or both) that this was our fifth most-common theme over the course of the year.

Data in Transit

Data is in transit when it is moving from one location to another, such as user-to-service, application-to-service, or service-to-service. Misconfigurations at this stage typically happen in one of the following two ways: by explicitly enabling and using clear-text protocols or by failing to disable them when they're enabled by default.

> **Example Issue:** Praetorian observed application-to-service data exposure when data providers such as databases or caching services did not enforce encrypted transfer protocols. The applications relied on providers encrypting the data transiting their services on the backend. Most providers may do this effectively; however, cross-provider access or traffic routing issues could unintentionally expose sensitive data.

Mitigation for Data in Transit

Enabling and enforcing secure connections will ensure that data is encrypted in transit. This means:

- Require TLS 1.2 or higher for all connections
- Disable clear-text protocols (HTTP, FTP, Telnet)
- Enforce encryption at the application level, not just relying on provider defaults

Data at Rest

The combination of unencrypted data at rest with misconfigured resource-based access led to some of the highest impact vulnerabilities Praetorian identified. Many of the well-known public breaches also involved this type of mismanagement.

Mitigation for Data at Rest

CONCLUSION

Building a Strong Cloud Security Foundation

Cloud resources have allowed organizations to implement their businesses at an Internet-scale quickly. The very real benefits associated with incorporating the cloud also come with a responsibility to secure the platforms, services, and resources.

654

TOTAL FINDINGS ANALYZED
FROM 117 ENGAGEMENTS

Focusing efforts to avoid, mitigate, and eliminate the risks outlined in this whitepaper will position organizations to have a strong cloud security foundation. The five major themes we've identified represent the most common and impactful vulnerabilities across AWS, Azure, and GCP.

Key Takeaway: Addressing these foundational issues provides the greatest security improvement for the least investment. Start with Identity and Access Management, then work through Configuration Management, Resource-Based Access Control, Logging and Monitoring, and Data Protection.

Ready to Secure Your Cloud Environment?

Partner with Praetorian to assess your cloud security posture and implement effective mitigations.

Contact Us