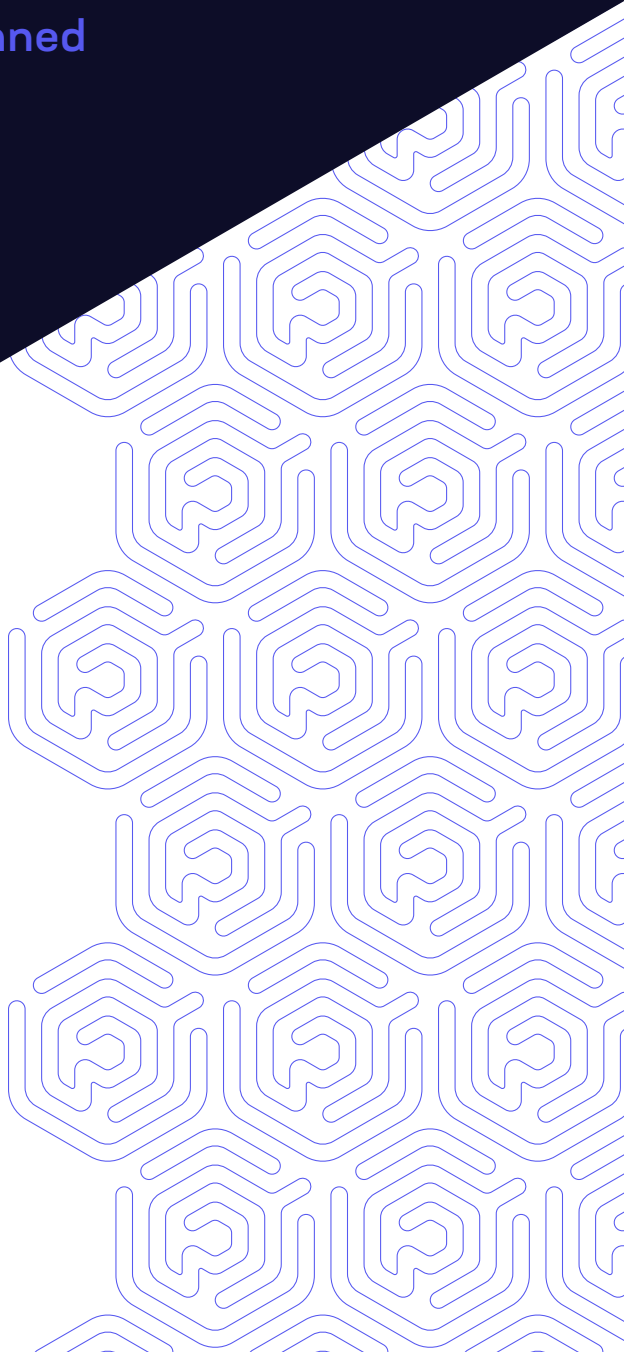
WHITE PAPER

# 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.



praetorian

On nearly every engagement, Praetorian found improperly managed secrets.

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. This whitepaper distills the major themes we have observed on client engagements that span the three major cloud platforms, AWS, Azure, and GCP.

INSIDE THIS REPORT



# Identity and Access Management

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 that lead to this vulnerability 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

Praetorian recommends eschewing static user credentials where possible. A better practice is to implement federated single-sign-on (SSO) for human accounts to enforce organization-wide security policies in the cloud accounts. Additionally, short-lived temporary credentials from these solutions are the preferred method for granting CLI access rather than long-lived access keys to minimize the impact of their exposure.

Praetorian also recommends using platform-specific or cloud-native or secrets storage management for storing secrets required to authenticate to third-party services and internal resources that can't use IAM/role-based access controls. The permissions to retrieve these secrets should be scoped to include only the services that require them for usage.

## Configuration Management

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, and included absence of critical controls, misconfiguration of services that could lead to data exposure or privilege escalation, and 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. Further configuration of the selected components should follow the security guidance for the individual services.

# Resource-Based Access Control

→

Exposed resources were susceptible to brute-force authentication attacks and resource exhaustion/denial of service.

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).

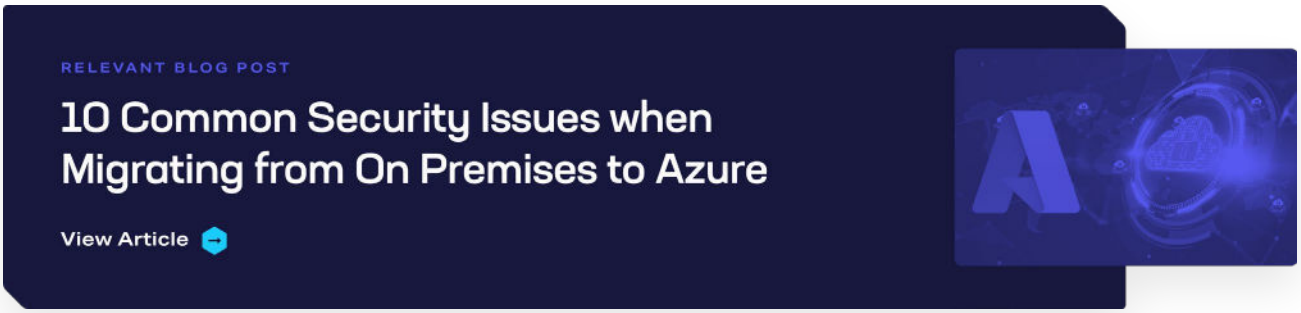
Additionally, lax network access controls granted asset access to attackers outside the intended resource scope. These manifested as unconstrained Security Groups, overly broad provider permissions, and accidental public exposure of services due to insecure defaults. In simpler terms, sensitive resources 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. Praetorian recommends avoiding resource-based policies where possible and instead creating fine-grained IAM policies to access resources. Often this requires creating an allowed

list of known source IP addresses or rearchitecting the network access to be performed over private network connections (VPC peering or Direct Connect).

In most cases, enabling tighter network access controls was sufficient to mitigate the identified risks. The Azure instances, however, required modification of some insecure default configurations. We documented these in issues one and two in the Praetorian blog post "10 Common Security Issues when Migrating from On Premises to Azure".




# 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.

## 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.

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.

# Data Protection

→

For example, 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.

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.

### Mitigation

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

## 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

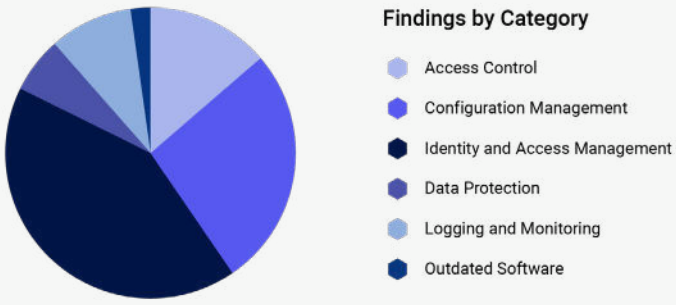
Once data arrives at its destination, it also needs to be encrypted. The mechanics of this encryption will vary depending on the medium, but users should scope both access to the resource and the keys to decrypt

its contents as tightly as possible. This rule applies to all storage types, including buckets and volumes, databases, queues, etc., in order to limit impact if accidental exposure occurs.

# Conclusion

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. Focusing efforts to avoid, mitigate, and eliminate the risks outlined in this white paper will position organizations to have a strong cloud security foundation.

## Stats




| Row Labels | Count of title | Average of risk_score | Max of risk_score |
|---|---|---|---|
| Access Control | 32 | 13.4375 | 15 |
| Configuration Management | 63 | 13.3015873 | 15 |
| Identity and Access Management | 99 | 13.21212121 | 15 |
| Data Protection | 14 | 13.14285714 | 14 |
| Logging and Monitoring | 22 | 13.04545455 | 14 |
| Outdated Software | 5 | 13 | 13 |
| Grand Total | 235 | 13.24255319 | 15 |