5 Steps to Securing Multi-Cloud Infrastructure

As cloud adoption accelerates, there is a growing need to manage security risks within these dynamic environments. With multi-cloud architectures, organizations can be overwhelmed by the sheer number of services they need to secure. A single misconfiguration in one service can lead to a serious data breach, but the reality is that human errors are impossible to avoid. Automation is required to stay on top of security gaps.

According to Gartner, “Nearly all successful attacks on cloud services are the result of customer misconfiguration and mistakes.” They also predict that through 2023, at least 99% of cloud security failures will be the customer’s fault.

Imagine a scenario where one of your critical services suddenly stops working. A DevOps engineer investigates, and after a few hours of work, discovers a manual change to a firewall rule that should protect the failing service. Even worse, she discovers many other unplanned firewall rule changes. She feels lucky that one of those modifications triggered the investigation.

How can you keep track of constant additions and changes to cloud services? How can you flag misconfigurations and suspicious activity across multiple clouds? How do you focus on the alerts that signal a real threat? Tackling these unique cloud security risks requires a continuous and automated approach. Our checklist outlines how organizations can set up the security strategy to follow as they move to the cloud.

1 Gartner: Innovation Insight for Cloud Security Posture Management
Discover Cloud Assets

- Identify the systems, applications, services, and scripts running in your cloud environment. Determine if they are secure and compliant.
- Map cloud assets including accounts, VPCs, regions, S3 buckets, RDS, etc. Understand where your sensitive data (e.g., customer data, data governed by compliance regulations) is stored and processed.
- Visualize cloud activity across multiple cloud services.

This will help baseline your current operating state, as well as help you prioritize the services with most critical threats and accelerate remediation.
Identify risky configuration settings and gain visibility into the current security posture of your cloud and container environment. Detect misconfigurations such as public storage buckets, exposed security groups, leaked secrets/credentials, etc. Also determine if you have configuration drift.

Check your cloud configuration against CIS benchmark for securing cloud services, community-sourced policies, or your own security baseline. With CIS Cloud Benchmarks, you can execute a curated collection of checks periodically on your cloud account that will inform you which services and configurations present a security challenge.

Get remediation procedures with implementation guidance using the cloud providers Console, or CLI commands to harden your security posture.
5 STEPS TO SECURING MULTI-CLOUD INFRASTRUCTURE

Prevent Cloud Permission Risk (CIEM)

Over-permission accounts and roles are one of the most common cloud misconfiguration security problems. Managing excessive permissions can be confusing, since IAM policies can often combine resources, actions and identities. Implementing least privilege access is crucial to avoid risks of data breaches and prevent privilege escalation and lateral movement. Make sure your access reviews include identifying active and inactive users and their associated permissions. Apply the just-enough permissions needed to perform core tasks. Review these permissions on an ongoing basis. Track your progress towards a stronger IAM security posture with out-of-the-box dashboards summarizing the key risks.
Continuously Detect and Respond to Cloud Threats

Continuously detect suspicious cloud activity across all cloud accounts, users, and services by analyzing cloud activity logs.

- Look for suspicious patterns or abnormal behavior and use your data for incident response.
- Detect process execution patterns for unexpected behavior or remote code executions.
- Look for credential theft, especially for longer-lived credentials or high-privilege credentials.
- Identify changes in configuration of cloud resources (e.g., S3), infrastructure ports for virtual servers, containers, and container orchestration platforms.
- Identify sensitive data leaks through unintentional exposure of information.
- Examine data from past incidents to detect patterns.

Detect misconfiguration and unexpected activity when cloud resources are created, deleted, or modified across all of your cloud accounts. This will reduce your exposure to risk from compromised cloud accounts or unintended human error. Manage your risk by using cloud activity logs and Falco rules as the source of truth for operational audits. Detect threats as soon as they happen, and enable governance, compliance, and risk auditing for your cloud accounts.
Validate Cloud Compliance and Governance

Achieve and maintain compliance with security frameworks through a rich set of Falco rules for security standards and benchmarks, like NIST 800-53, PCI DSS, SOC 2, MITRE ATT&CK®, and the CIS benchmarks.

Enable governance and enforcement of your organization-specific security controls. This will allow your Cloud teams to easily validate compliance for auditors as well as customers.

Continuously track cloud compliance progress against benchmarks and standards, with detailed reports and alerts. Accelerate mean time to response (MTTR) with guided remediation tips.
Sysdig is driving the standard for cloud and container security. The company pioneered cloud-native runtime threat detection and response by creating Falco and Sysdig as open source standards and key building blocks of the Sysdig platform. With the platform, teams can find and prioritize software vulnerabilities, detect and respond to threats, and manage cloud configurations, permissions and compliance. From containers and Kubernetes to cloud services, teams get a single view of risk from source to run, with no blind spots, no guesswork, no black boxes. The largest and most innovative companies around the world rely on Sysdig.

### How Sysdig Extends CSP’s Security Tools

<table>
<thead>
<tr>
<th>Security Controls</th>
<th>AWS</th>
<th>Azure</th>
<th>GCP</th>
<th>Sysdig</th>
<th>How Sysdig Complements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excessive Permissions</td>
<td>AWS Identity &amp; Access Management</td>
<td>Azure AD/IAM</td>
<td>Cloud Identity &amp; Access Management (IAM)</td>
<td>✔️</td>
<td>Implement service-based access control to streamline security and monitoring information to individual users and teams.</td>
</tr>
<tr>
<td>Cloud Threat Detection</td>
<td>AWS CloudTrail</td>
<td>Azure Activity Logs</td>
<td>Google Cloud Audit logs</td>
<td>✔️</td>
<td>Detect and block attacks, combining deep visibility through cloud logs, and audit events with cloud metadata. Powered by open-source CNCF runtime security project Falco.</td>
</tr>
<tr>
<td>CSPM &amp; Compliance</td>
<td>AWS Config CIS AWS Foundation Benchmarks AWS GuardDuty</td>
<td>Azure Policy</td>
<td>Compliance Reports Manager</td>
<td>✔️</td>
<td>Enforce continuous compliance with out-of-the-box configuration checks for PCI, GDPR, NIST, HIPAA, etc. and report with custom assessments and dashboards. Continuously validate compliance using out-of-the-box image scanning policies, automated CIS benchmark checks and runtime policies.</td>
</tr>
</tbody>
</table>

Dig deeper into how Sysdig provides continuous cloud security across AWS, GCP and Azure

**Start Your Free Trial**

**Get Personalized Demo**