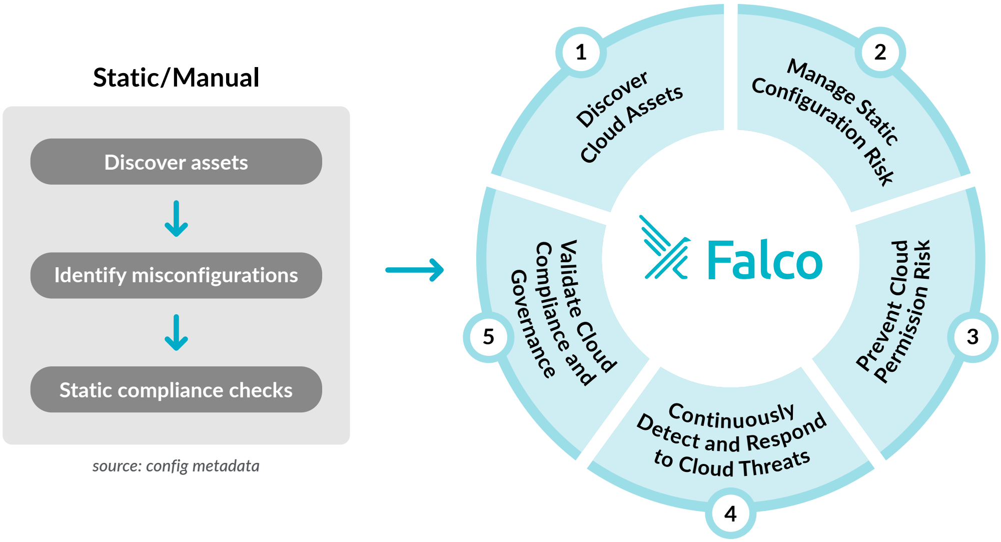
5 Steps to Securing Multi-Cloud Infrastructure

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.


Static/Manual
Discover assets
Identify misconfigurations
Static compliance checks
Falco
1
Discover Cloud Assets
2
Manage Static Configuration Risk
3
Prevent Cloud Permission Risk
4
Continuously Detect and Respond to Cloud Threats
5
Validate Cloud Compliance and Governance

source: config metadata

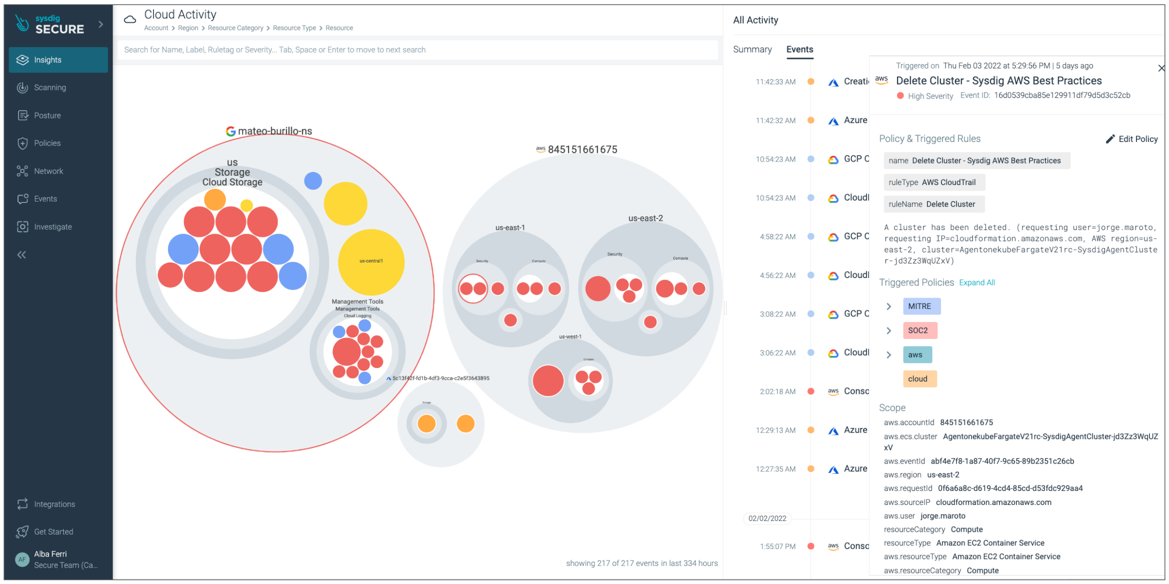
[1] Gartner: Innovation Insight for Cloud Security Posture Management

1

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.



```
11:42:33 AM  Creati
11:42:32 AM  Azure
10:54:23 AM  GCP C
10:54:23 AM  Cloudl
4:58:22 AM   GCP C
4:56:22 AM   Cloudl
3:08:22 AM   GCP C
3:06:22 AM   Cloudl
2:02:18 AM   Conso
12:29:13 AM  Azure
12:27:35 AM  Azure
02/02/2022
1:55:07 PM   Conso
```

Triggered on Thu Feb 03 2022 at 5:29:56 PM | 5 days ago

Delete Cluster - Sysdig AWS Best Practices

High Severity Event ID: 16d0539cba85e129911df79d5d3c52cb

Policy & Triggered Rules

name Delete Cluster - Sysdig AWS Best Practices

ruleType AWS CloudTrail

ruleName Delete Cluster

```
A cluster has been deleted. (requesting user=jorge.maroto,
requesting IP=cloudformation.amazonaws.com, AWS region=us-
east-2, cluster=AgentonekubeFargateV21rc-SysdigAgentCluste
r-jd3Zz3WqUZxV)
```

Triggered Policies

MITRE
SOC2
aws
cloud

Scope

aws.accountId	845151661675
aws.ecs.cluster	AgentonekubeFargateV21rc-SysdigAgentCluster-jd3Zz3WqUZxV
aws.eventId	abf4e7f8-1a87-40f7-9c65-89b2351c26cb
aws.region	us-east-2
aws.requestId	0f6a6a8c-d619-4cd4-85cd-d53fdc929aa4
aws.sourceIP	cloudformation.amazonaws.com
aws.user	jorge.maroto
resourceCategory	Compute
resourceType	Amazon EC2 Container Service
aws.resourceType	Amazon EC2 Container Service
aws.resourceCategory	Compute

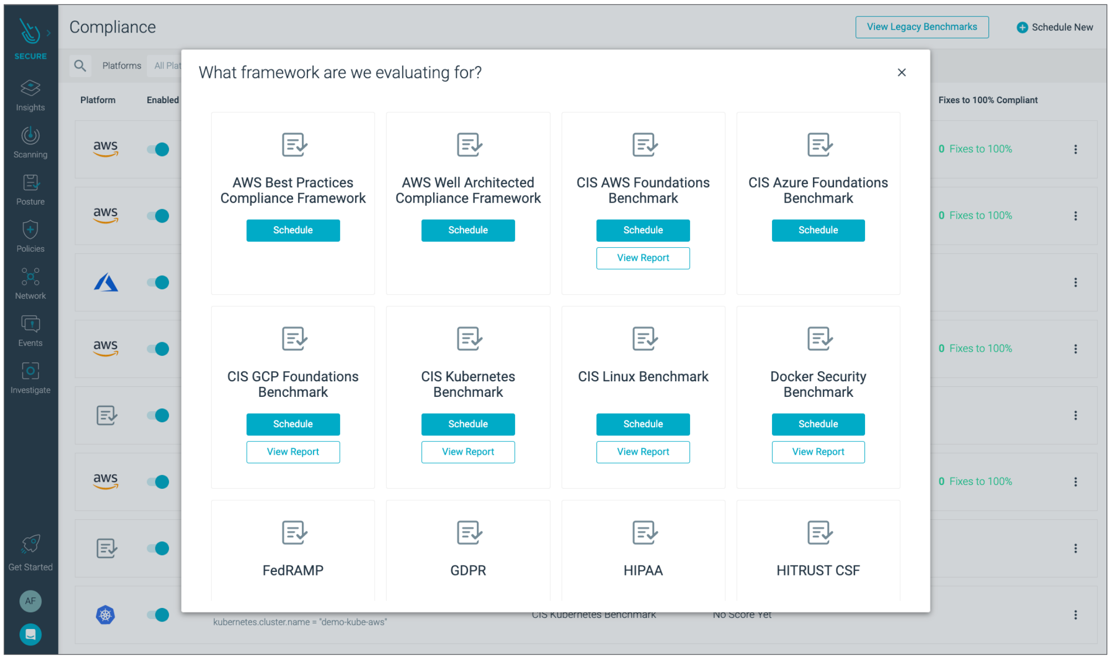
2

Manage Static Configuration Risk (CSPM)

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.



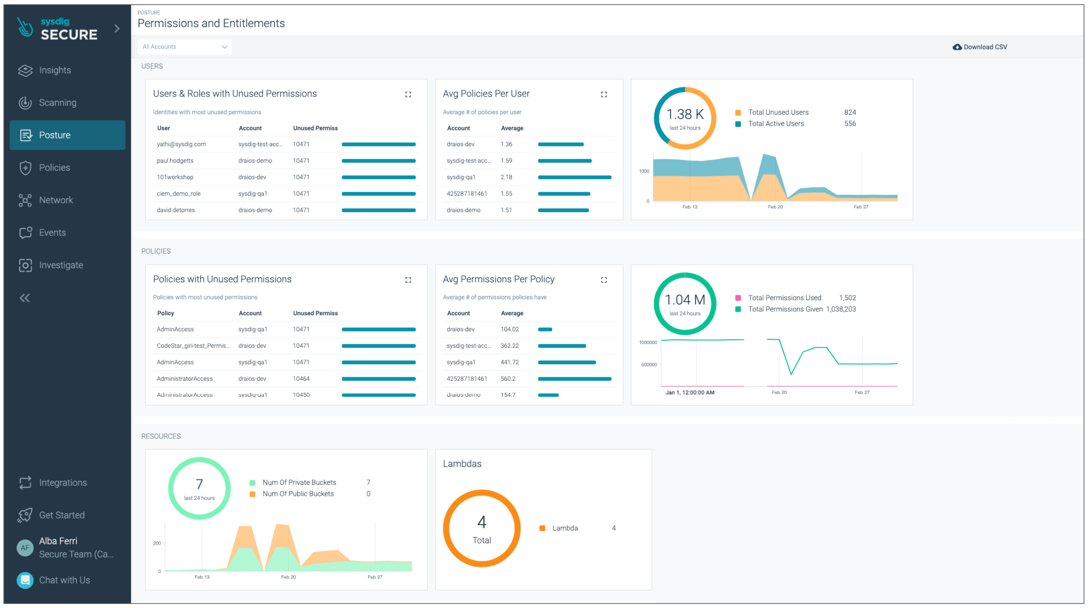
3

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.



POSTURE
Permissions and Entitlements

USERS

Users & Roles with Unused Permissions

Identities with most unused permissions

User	Account	Unused Permiss
yathi@sysdig.com	sysdig-test-acc...	10471
paul.hodgetts	draios-demo	10471
101workshop	draios-dev	10471
ciem_demo_role	sysdig-qa1	10471
david.detorres	draios-demo	10471

Avg Policies Per User

Average # of policies per user

Account	Average
draios-dev	1.36
sysdig-test-acc...	1.59
sysdig-qa1	2.18
425287181461	1.55
draios-demo	1.51

🟧	Total Unused Users	824
🟦	Total Active Users	556

POLICIES

Policies with Unused Permissions

Policies with most unused permissions

Policy	Account	Unused Permiss
AdminAccess	sysdig-qa1	10471
CodeStar_giri-test_Permis...	draios-dev	10471
AdminAccess	sysdig-qa1	10471
AdministratorAccess	draios-dev	10464
AdministratorAccess	sysdig-qa1	10450

Avg Permissions Per Policy

Average # of permissions policies have

Account	Average
draios-dev	104.02
sysdig-test-acc...	362.22
sysdig-qa1	441.72
425287181461	560.2
draios-demo	154.7

🟥	Total Permissions Used	1,502
🟩	Total Permissions Given	1,038,203

RESOURCES

🟩	Num Of Private Buckets	7
🟧	Num Of Public Buckets	0

Lambdas

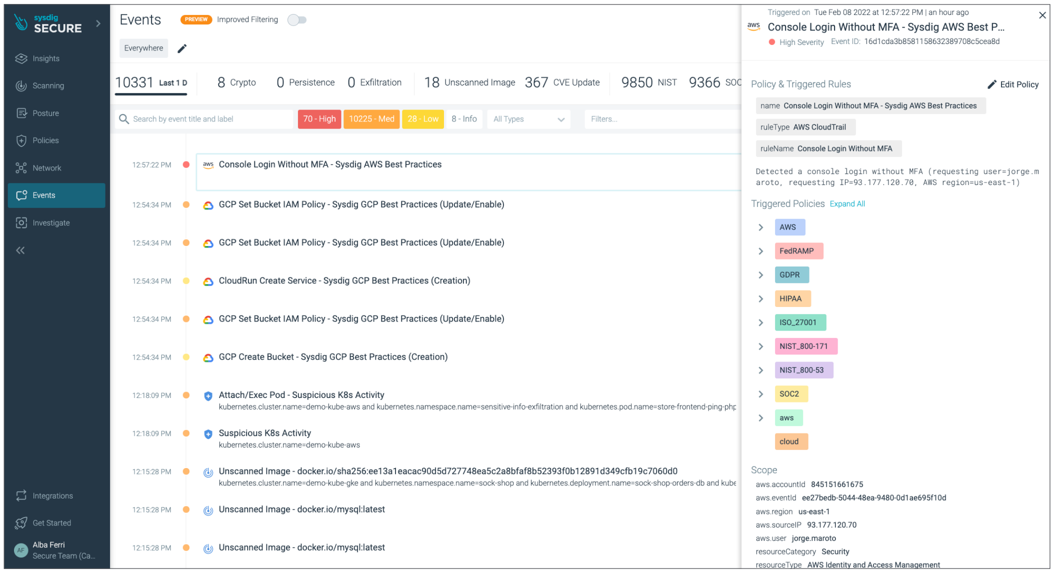
🟧	Lambda	4

4

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.



10331 Last 1 D | 8 Crypto | 0 Persistence | 0 Exfiltration | 18 Unscanned Image | 367 CVE Update | 9850 NIST | 9366 SOC

70 - High | 10225 - Med | 28 - Low | 8 - Info

```
12:57:22 PM  Console Login Without MFA - Sysdig AWS Best Practices
12:54:34 PM  GCP Set Bucket IAM Policy - Sysdig GCP Best Practices (Update/Enable)
12:54:34 PM  GCP Set Bucket IAM Policy - Sysdig GCP Best Practices (Update/Enable)
12:54:34 PM  CloudRun Create Service - Sysdig GCP Best Practices (Creation)
12:54:34 PM  GCP Set Bucket IAM Policy - Sysdig GCP Best Practices (Update/Enable)
12:54:34 PM  GCP Create Bucket - Sysdig GCP Best Practices (Creation)
12:18:09 PM  Attach/Exec Pod - Suspicious K8s Activity
             kubernetes.cluster.name=demo-kube-aws and kubernetes.namespace.name=sensitive-info-exfiltration and kubernetes.pod.name=store-frontend-ping-php
12:18:09 PM  Suspicious K8s Activity
             kubernetes.cluster.name=demo-kube-aws
12:15:28 PM  Unscanned Image - docker.io/sha256:ee13a1eacac90d5d727748ea5c2a8bfaf8b52393f0b12891d349cfb19c7060d0
             kubernetes.cluster.name=demo-kube-gke and kubernetes.namespace.name=sock-shop and kubernetes.deployment.name=sock-shop-orders-db and kube
12:15:28 PM  Unscanned Image - docker.io/mysql:latest
12:15:28 PM  Unscanned Image - docker.io/mysql:latest
```

Triggered on Tue Feb 08 2022 at 12:57:22 PM | an hour ago

aws Console Login Without MFA - Sysdig AWS Best P...

High Severity Event ID: 16d1cda3b8581158632389708c5cea8d

Policy & Triggered Rules

name Console Login Without MFA - Sysdig AWS Best Practices

ruleType AWS CloudTrail

ruleName Console Login Without MFA

```
Detected a console login without MFA (requesting user=jorge.m
aroto, requesting IP=93.177.120.70, AWS region=us-east-1)
```

Triggered Policies

AWS
FedRAMP
GDPR
HIPAA
ISO_27001
NIST_800-171
NIST_800-53
SOC2
aws
cloud

Scope

aws.accountId	845151661675
aws.eventId	ee27bedb-5044-48ea-9480-0d1ae695f10d
aws.region	us-east-1
aws.sourceIP	93.177.120.70
aws.user	jorge.maroto
resourceCategory	Security
resourceType	AWS Identity and Access Management

Detect misconfigurations 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.

5

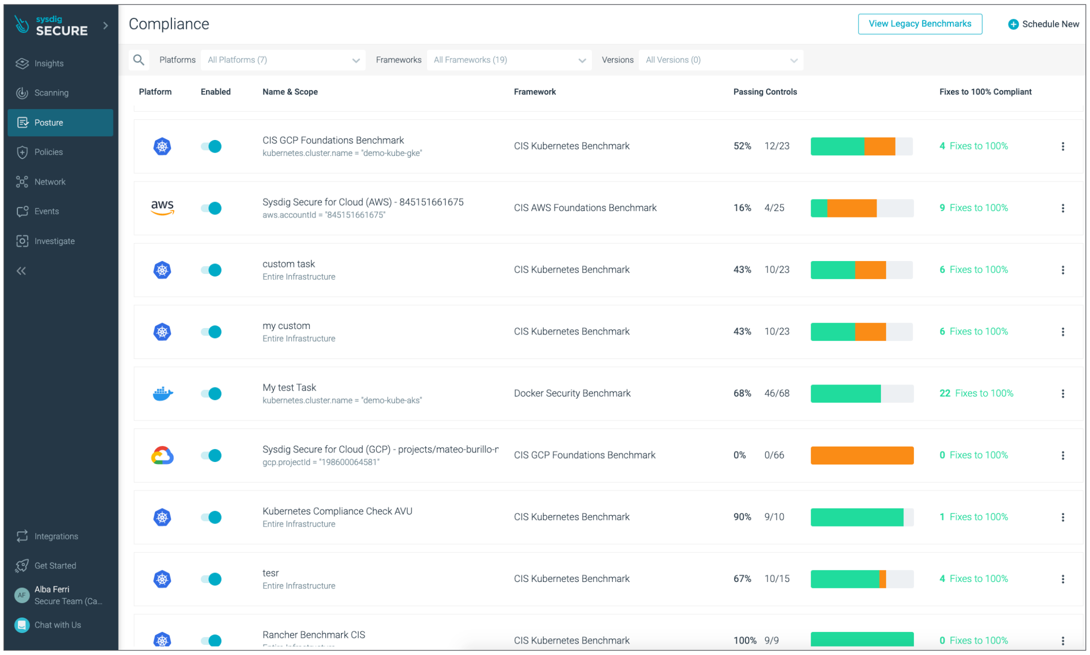
5 STEPS TO SECURING MULTI-CLOUD INFRASTRUCTURE

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.



Compliance

Platform	Enabled	Name & Scope	Framework	Passing Controls		Fixes to 100% Compliant
	●	CIS GCP Foundations Benchmark kubernetes.cluster.name = "demo-kube-gke"	CIS Kubernetes Benchmark	52%	12/23	4 Fixes to 100%
aws	●	Sysdig Secure for Cloud (AWS) - 845151661675 aws.accountId = "845151661675"	CIS AWS Foundations Benchmark	16%	4/25	9 Fixes to 100%
	●	custom task Entire Infrastructure	CIS Kubernetes Benchmark	43%	10/23	6 Fixes to 100%
	●	my custom Entire Infrastructure	CIS Kubernetes Benchmark	43%	10/23	6 Fixes to 100%
	●	My test Task kubernetes.cluster.name = "demo-kube-aks"	Docker Security Benchmark	68%	46/68	22 Fixes to 100%
	●	Sysdig Secure for Cloud (GCP) - projects/mateo-burillo-r gcp.projectId = "198600064581"	CIS GCP Foundations Benchmark	0%	0/66	0 Fixes to 100%
	●	Kubernetes Compliance Check AVU Entire Infrastructure	CIS Kubernetes Benchmark	90%	9/10	1 Fixes to 100%
	●	tesr Entire Infrastructure	CIS Kubernetes Benchmark	67%	10/15	4 Fixes to 100%
	●	Rancher Benchmark CIS	CIS Kubernetes Benchmark	100%	9/9	0 Fixes to 100%

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

Security Controls	AWS	Azure	GCP	Sysdig	How Sysdig Complements
Visibility	Partial visibility through AWS Console	Partial visibility through Azure Portal	Partial visibility through Cloud Console	✓	Deep visibility into multi-cloud infrastructure, services, and applications. Visualize and correlate findings and events across clouds. Identify and resolve issues faster. Easily extend cloud security to multi-cloud with a unified view and out-of-the-box policies.
Excessive Permissions	AWS Identity & Access Management	Azure AD/ IAM	Cloud Identity & Access Management (IAM)	AWS Only	Implement service-based access control to streamline security and monitoring information to individual users and teams.
Cloud Threat Detection	AWS GuardDuty	Azure Defender	Google Security Command Center	✓	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.
CSPM & Compliance	AWS Config CIS AWS Foundation Benchmarks AWS GuardDuty	Azure Policy	Compliance Reports Manager	✓	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.

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

Start Your Free Trial

Get Personalized Demo