# Cloud Security Posture Management
## by Skyhawk Synthesis Security Platform

There are two key components to any solid cloud security strategy: prevention and detection. Skyhawk Security addresses both components. Our innovative Cloud Threat Detection and Response platform known as Skyhawk Synthesis Security Platform provides comprehensive cloud security detection and remediation, cloud infrastructure and entitlement management and cloud security posture management (CSPM), a baseline capability that most organizations require as a part of their preventative security strategy. It is for this reason that Skyhawk Security now offers CSPM capabilities – free of charge. You can monitor misconfigurations and manage compliance and governance free for up to 1,000 assets in your cloud, with Skyhawk.

## Detection of Misconfigurations

Skyhawk Synthesis helps organizations detect cloud misconfigurations across a wide range of potential issues, with detailed explanations in terms of the impact and how to fix it. The risk-prioritized alerts based on risk-assessment and severity enable security teams to respond to the most pressing issues. The warnings by category provide a simple overview of which elements of your infrastructure are the weakest in your security strategy.

A deep dive into the alert provides detail on why it is important, recommendations, as well as information on when the issue was first and last detected. If resources are available, a link is provided to support the security team.

### Key Capabilities

- Identification of misconfigurations so they can be corrected to prevent data leaks and risky newsworthy events

- Simplify compliance initiatives with reports that support local and international security standards like PCI, GDPR and more

- Enforce behaviors and improve governance initiatives with the ability to customize rules to support your data handling policies for your business and your cloud
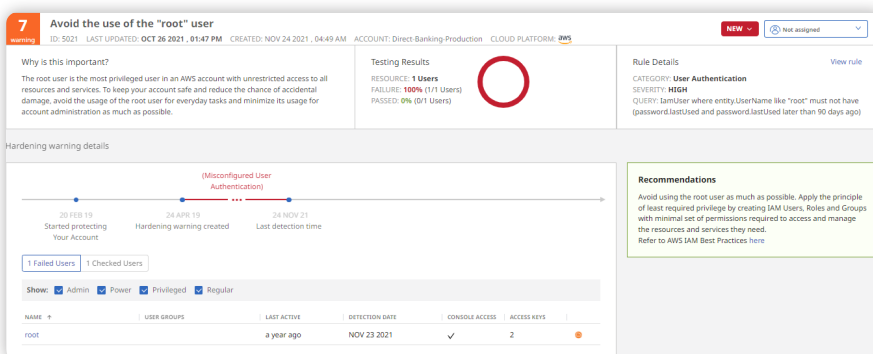


Image 1: Skyhawk Synthesis identifies misconfigurations, like use of the "root" user for everyday tasks to reduce the impact of compromised users.

## Compliance Reporting

Skyhawk Synthesis provides extensive reports to simplify compliance with internal and external regulations as well as security best practices. There are also Amazon Web Services (AWS) and Azure compliance reports which align to the Center for Internet Security (CIS) benchmarks. The level of non-compliance is scored so you can determine how grave the misalignment is and what action needs to be taken. The reports include PCI DSS, SOC2, NIST Cyber Security Framework, ISO 27001 and more, providing both high-level verification of your compliance status, as well as line-by-line assessment of each individual criterion in the standard.

## Create Custom Rules to Enforce Best Practices

Many organizations have data handling policies that do not align to a specific compliance initiative, but that does not make them unimportant. Skyhawk Synthesis allows you to create custom rules that will trigger a misconfiguration alert. These custom policies are not limited to data, they allow cloud security teams to ensure compliance with internal and external policies across the entire cloud, delivering greater control for security teams.

| Reports | Attack Simulation | Settings |
| --- | --- | --- |

Activity Summary Report

**Radware Compliance Reports**

AWS CIS Foundation Compliance Report

Azure CIS Foundation Compliance Report

COVID-19 Best Practices

GDPR Compliance Report

HIPAA Compliance Report

ISO 27001 Compliance Report

NIST Cyber Security Framework Compliance Report

PCI DSS Compliance Report

SOC2 Compliance Report

**Custom Governance Reports**

AWS Prod Bundle

Azure Prod Bundle

Image 2: Skyhawk Synthesis provides many comprehensive reports for internal and external compliance initiatives. Custom reports can also be created to ensure the cloud is used and managed exactly as the business requires.

## What's included in the offering?

| Cloud Security Posture Management | Free CSPM Tier | Enterprise Tier |
| --- | --- | --- |
| Visibility across clouds (AWS, Azure, GCP) | ☑ | ☑ |
| Complete posture management and hardening | ☑ | ☑ |
| Compliance reports | ☑ | ☑ |
| Governance reports | ☑ | ☑ |
| Remediation | | ☑ |
| Assets | Up to 1000 assets | Unlimited |
| Cloud locations | USA, UK, EU, Israel, Japan, Australia | All supported locations without limits |
| **Cloud Threat Detection and Response** | | |
| Threat detection | | ☑ |
| Attack Simulations | | ☑ |
| Threat response | | ☑ |
| Cloud Infrastructure and Entitlement Management | | ☑ |
| Least privileges recommendations | | ☑ |
| Unused permission alerts | | ☑ |
| Support | Slack channel | Ticketing system, dedicated customer support engineers |
| Guided install | ☑ | ☑ |
| Integrations | Not included | Jira, Slack |

## Contact us today to learn more!
### skyhawk.security/get-free-cspm/

SKYHAWK
SECURITY