Skyhigh Security



# Securing Cloud Native Applications with Skyhigh Security CNAPP

Every enterprise is undergoing a digital transformation. Most enterprises are leveraging the agility and innovation velocity of the public cloud, either solely or in conjunction with their private data centers. These enterprises need a simplified architecture, one that enables them to leapfrog the cost and complexity of the patchwork of point products, and benefit from the fabric of the cloud-native ecosystem—without major investments in tools or developer talent.

Skyhigh Security Cloud Native Application Protection Platform (CNAPP) extends Skyhigh Security's Cloud Access Security Broker (CASB) data protection. It provides both data loss prevention (DLP) and malware detection for threat prevention and governance and compliance. Our CNAPP comprehensively addresses the needs of this new cloud-native application world, improving security capabilities and reducing the total cost of ownership (TCO) of cloud security.

## The Skyhigh Security Cloud Native Application Protection Platform

Skyhigh Security CNAPP is the industry's first platform to bring application and data context to uniquely converge cloud security posture management (CSPM) for public cloud infrastructure and cloud workload protection platforms (CWPPs) to protect workloads, including VMs, containers, and serverless functions.

According to Gartner, "There is synergy in combining CWPP and CSPM capabilities, and multiple vendors are pursuing this strategy. The combination will create a new category of CNAPPs that scan workloads and configurations in development and protect workloads and configurations at runtime."[1]

CSPM is a class of security tools that enable compliance monitoring, DevOps integration, incident response, risk assessment, and risk visualization. Per Gartner, "Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement, and mistakes. Security and risk management leaders should invest in cloud security posture management processes and tools to proactively and reactively identify and remediate these risks."[2]

CWPPs are workload-centric security protection solutions that are typically agent-based. They address the unique requirements of server workload protection in modern hybrid data center architectures that span on-premises, physical and virtual machines (VMs), and multiple public cloud Infrastructure-as-a-Service (IaaS) environments. This includes support for container-based application architectures.

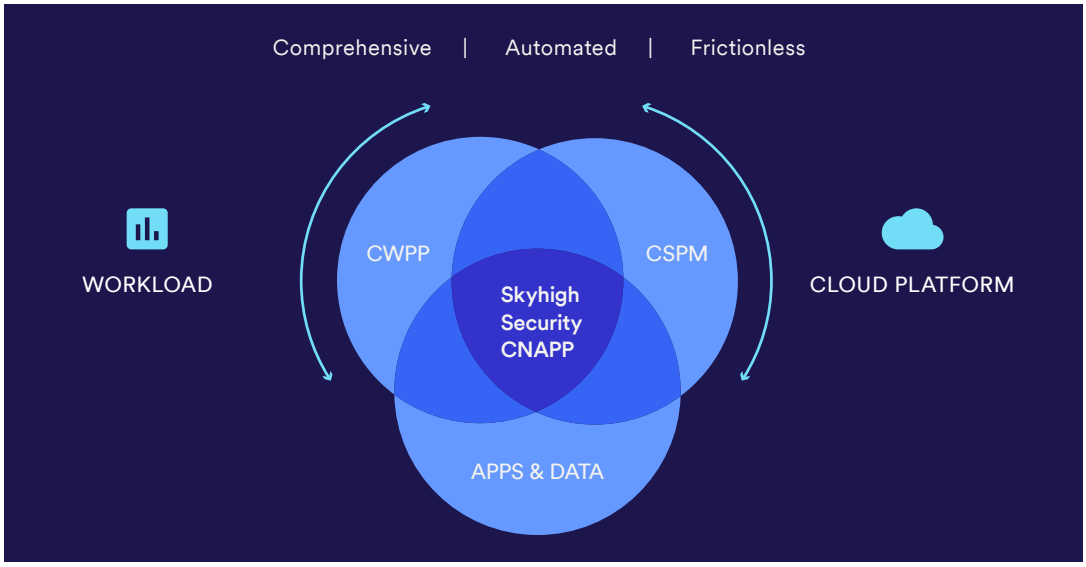
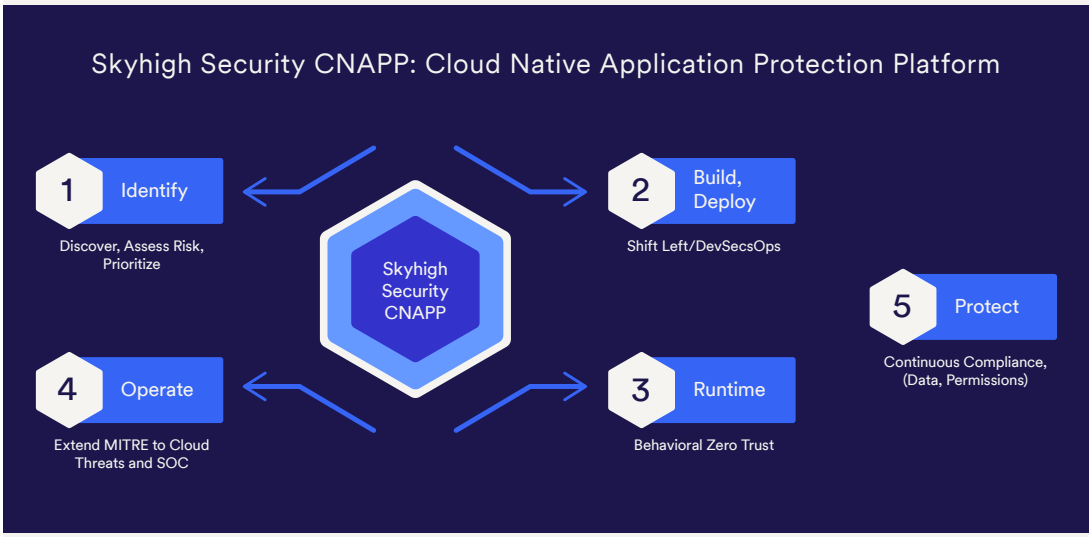



Figure 1. Skyhigh Security CNAPP—Under the Hood.

1 Source: Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald, Tom Croll, 14 April 2020. ID: G00716192. Analyst(s): Neil MacDonald, Tom Croll.

2 Source: Innovation Insight for Cloud Security Posture Management. Published: 25 January 2019. ID: G00377795 Analyst(s): Neil MacDonald.

Figure 2. The five elements of Skyhigh Security CNAPP.




# Skyhigh Security CNAPP Components

## 1 Identify: Discover and prioritize based on risk

The ability to comprehensively discover, classify, and prioritize risk across public cloud providers, applications, and data.

- Gain visibility of regulated or sensitive data stored in cloud storage services like Amazon S3, Azure Blob Storage, and GCP Cloud Storage. Perform on-demand scans to identify malicious files or automatically quarantine files that have protected data.
- Detect security misconfigurations and mitigate drift in IaaS platforms, as well as popular container services like Amazon EKS, ECS, AWS Fargate, Azure Kubernetes Services, and Google Kubernetes Engine.
- Scale security and empower development, operations, and architect teams. Identify risky applications and provide near-real time feedback on incident resolution and unintentional risk exposure.

## 2 Build and deploy: Shift left and DevSecOps

The ability to protect against configuration drift and provide vulnerability assessment at the time infrastructure is being “built as code.”

- IIntegrate security into the CI/CD pipeline to proactively detect and correct insecure configurations, software vulnerabilities, or changes in once-secure configurations.
- Automate security checks and balances at different stages by shifting left within the code pipeline, making security resolution faster and less time-consuming.
- Enable enterprise scale by applying industry-leading practices, like immutable infrastructure and golden image pipeline, to embed security into workload images with controls, like Center for Internet Security (CIS) Benchmarks for Linux and Windows.

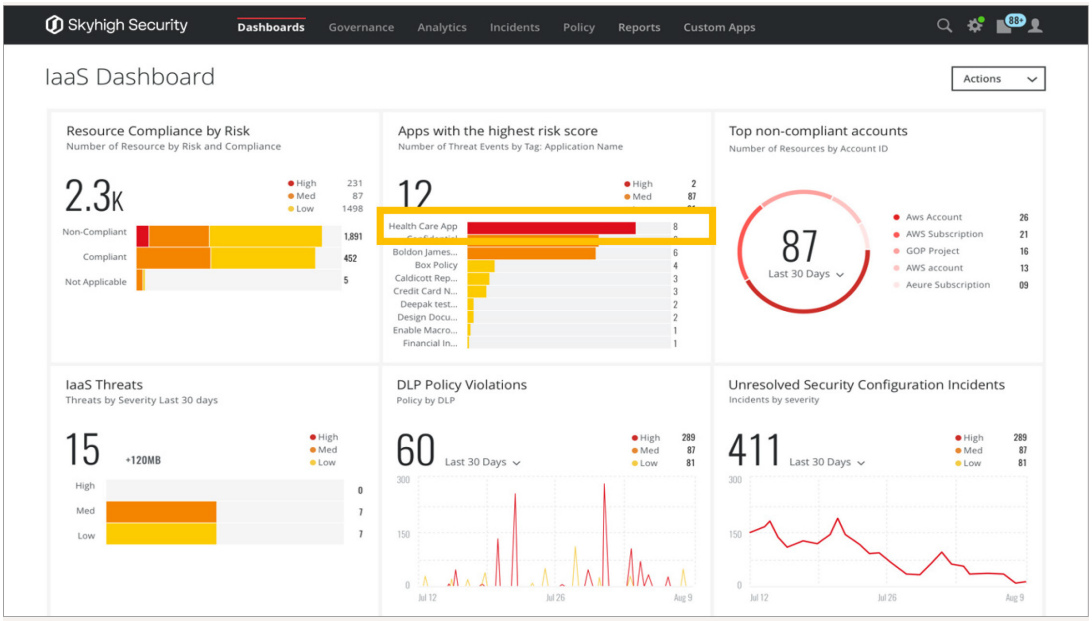



Figure 3. Skyhigh Security CNAPP: risk-driven prioritization summary view.

## 3 Runtime: Behavioral Zero Trust

The ability to build Zero Trust policy based on behavioral observation with application and service segmentation.

- Discover inter-application communications based on known good configurations to secure behavior of complex and dynamic workloads and containers. This includes baselining the behavior of an application in a controlled environment and then using that as a measure of what's acceptable in production.
- Protect cloud native applications with features like active allow listing, file monitoring, and operating system (OS) hardening with dynamic enforcement capabilities to prevent unauthorized execution of vulnerable code in applications.

## 4 Operate: Extend MITRE ATT&CK to cloud threats and the SOC

The ability to detect and mitigate cloud native threats by mapping it to the MITRE ATT&CK framework.

- Empower the SOC by mapping the cloud-native threats to the MITRE ATT&CK framework for proactive remediation.
- Visualization of network flow traffic to provide granular visibility, detect suspicious and malicious network traffic, and use threat intelligence to eliminate false positives.
- Enable active and proactive threat protection by identifying compromised accounts, insider threats, privileged user threats, and malware based on automated models, predefined policy or custom rules and thresholds.

5

## Protect: Continuous compliance, data, and permissions

The ability to ensure continuous compliance and business continuity.

- Skyhigh Security CNAPP provides the umbrella of continuous compliance, allowing companies to track their cloud native applications and platforms against regulatory frameworks, such as PCI-DSS, HIPAA, NIST 800-53, and GDPR standards.
- Run granular management of permissions across cloud infrastructure. Help identify user permissions, inactive accounts and inappropriate access. Block risky users, revoke access, and enforce additional authentication.
- Meet audit requirements and automate security controls for workloads, data, and storage.

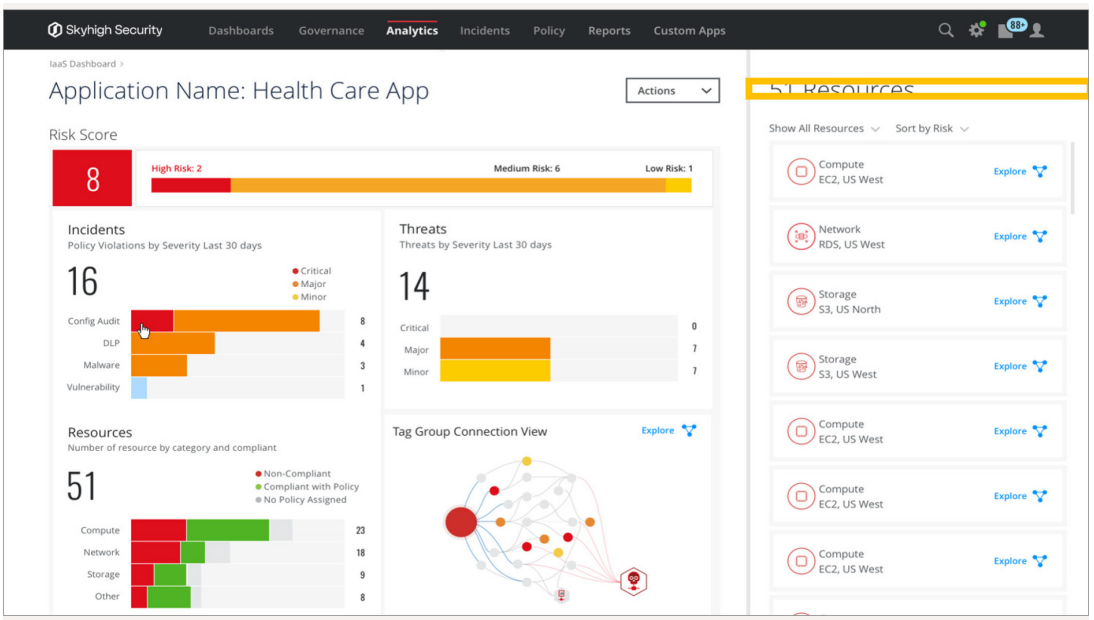



Figure 4. Skyhigh Security CNAPP: individual service view.

## In summary

For existing applications to gain the agility, scalability, resilience, and cost benefits of cloud-native computing, enterprises need to pivot from “lift-and-shift” projects to a modernized cloud migration strategy. Skyhigh Security CNAPP combines security capabilities using the same data and threat protection policies in Skyhigh Security CASB to improve compliance while simplifying and accelerating the adoption of cloud native applications.

## Learn more

For more information please visit skyhighsecurity.com or invite us for a demo at https://skyhighsecurity.com/demo

## About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

**For more information visit us at skyhighsecurity.com**

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

Skyhigh Security is a registered trademark of Musarubra US LLC. Other names and brands are the property of these companies or may be claimed as the property of others. Copyright © 2023.
October 2023. SB-EN-000004-01