SKYHAWK SECURITY

Skyhawk Synthesis: Continuous Proactive Protection

AI-Based Autonomous Purple Team

Cloud adoption is driven by the agility and accessibility it provides. Ironically, these are also two factors contributing the most to the challenges organizations face in securing clouds, given the constant nature of tension between agility and security, amplified by the lack of perimeter. The rapid advancement in AI adds another new vector and complexity. Threat actors now leverage AI to continuously evolve, change tactics, techniques, and approaches which lowers the skills set required to deploy an attack.

Current cloud security solutions fall short because they are reactive, not proactive. Some, like CNAPP, only detect misconfigurations or vulnerabilities after they are deployed. CDR and CIRA solutions only react to suspicious behaviors after they happen and then respond, which again, is too late.

Skyhawk Security's **Continuous Proactive Protection** turns that around with the industry's first proactive — not reactive —security solution. Using Skyhawk's proprietary AI technology, the system proactively examines your cloud, evaluates your defenses and develops offensive attacks from the perspective of an attacker. It then tests your responses to the attacks, before they actually happen, to help you determine the best way improve your cloud's security.

Benefits

- **Eliminate alert fatigue** by raising realerts on actual incidents, and not how threat actors "may gain access" to your cloud –allowing you to focus on what's really important
- **Reduce the total cost of ownership** with fast containment leveraging deep insight into each activity to allow the SOC team respond efficiently in time
- **Improve your prevention security strategy and risk management** with robust threat detection

Operating in a continuous cycle, Skyhawk is effectively delivering proactive protection through an Autonomous Purple Team that is constantly improving your cloud security. The result is nothing less than a paradigm shift in cloud security.

Continuous Proactive Protection

Continuous Proactive Protection ensures that your cloud is ready for a potential attack, with an adaptive security strategy built exactly for your cloud, delivering digital twins acting as an autonomous purple team. The platform continuously discovers your cloud's assets, monitors your configuration, vulnerabilities, topology and IAM to understand the least resistant paths to your most precious assets. In addition, the platform uses various feeds of data from real tools, including methods and techniques of threat actors attacking cloud infrastructure. The system then uses this information to simulate attacks, defines specific and verified detections and generates automated responses. In addition, the system makes hardening recommendations which are prioritized against actual threats. This new capability delivers these key benefits:

- **Proactive security:** Many CDR solutions are passive, waiting for suspicious indicators of compromise to happen. By utilizing Skyhawk's continuous autonomous purple team, you stay steps ahead of threat actors with the ability to predict the tactics that will be exploited, enabling security teams to be prepared with both validated and verified automated responses (CIRA). It also prioritizes the remediation of weaponized threats, so those more threatening issues are corrected first.
- **Continuous and Adaptive protection:** Clouds are always changing, the infrastructure, configuration, and permissions, are being updated to support changing business requirements. This is one of the key benefits, but it also makes security extremely challenging. Skyhawk Synthesis is always monitoring your cloud and always

identifying adjustments that should be made to your security methods to prevent cloud breaches with a security solution that is specific to your usage of the cloud. It delivers a completely customized security approach designed exactly for your cloud.

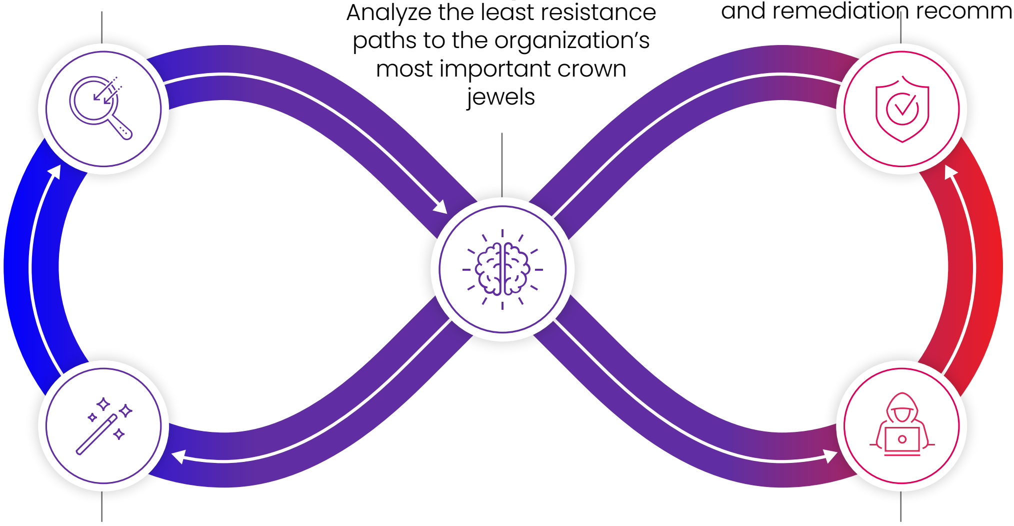
- **Detection you can trust for response automation:** The biggest inhibitor for customers to use response automation, is to trust the detection and response do no harm. Providing a continuous autonomous purple team results in pre-validated, trusted detections, with pre-validated, tested responses ensuring they can be trusted.

This new capability is built with the following key building blocks:

- **"Always Working" Purple Team:** Defend against attack plans that are perpetually executed against your cloud to understand issues and weaknesses in your security posture so you can continuously improve your security.
- **Pre-validated automated response:** Not all misconfigurations, IAM privileges, or access can be completely addressed to minimize risk or closed off from exposure. Some configurations must be left due to architectural or legacy reasons. Skyhawk's pre-validated automated response can be used to stop the progress of threat actors to prevent cloud breaches
- **Continuous learning:** Since the Skyhawk system acts as an automated purple team, AI learning techniques are being used, resulting in a continuously updating detection models, thus ensuring that new indicators are identified, minimizing the risk of threat actors learning how to evade detection.

How does this work?

The Skyhawk Synthesis Security Platform is a constantly working purple team for your cloud. The platform is constantly simulating attacks on your cloud, while constantly defending your cloud, to get a complete assessment of how threat actors will exploit your least resistance paths to get access to your precious data assets. Security gaps are easily identified so security teams know what to secure first and fast.



Discover
Discover the environment's inventory, configuration, and continuously identify the crown jewels

Analyze
Analyze the least resistance paths to the organization's most important crown jewels

Evaluate Defenses
Understand how your defenses detect and respond to threats, identify posture gaps, generate automated response and remediation recommendations

Simulate Attacks
Determine the attack recipes against the high priority crown jewels

Adapt
The platform uses the results of the continuous process to adapt detection capabilities resulting in **Adaptive CDR**, a tailored detection tuned to each customer's cloud infrastructure

And then the entire process repeats itself, so new learnings are always used to update the security of your cloud to prevent cloud breaches.

The Outcome

As mentioned, the output in the model is used in two ways. First, recommendations are provided to harden the configuration to increase security. The platform makes recommendations on how to adjust the configuration, permissions, or change in the cloud to ensure threat actors cannot move further in the cloud. These resolvable issues are prioritized based on weaponized threats, so the security team knows which to address first.

Second, there is the response to active threats. There are some cases where hardening updates cannot be made as it impacts productivity of teams or for other reasons. In those cases, a pre-validated response is required to ensure that the threat actor is unable to move forward to the precious data assets in your cloud. Skyhawk Synthesis will create an appropriate, automated response to stop any threatening activities to ensure a threat does not evolve to a breach.

Skyhawk Synthesis Security Platform Overview

Skyhawk Synthesis is a Cloud Breach Prevention Platform (CBP) and is the hub for logs and telemetry information from across your cloud environment to accurately identify threats before they become breaches. Skyhawk Synthesis monitors the cloud runtime for actual malicious behaviors that are happening right now so you can see how threat actors have penetrated your environment, and how they are making the lateral movement, to finally get access to your most precious crown jewels. Skyhawk Synthesis delivers real insights into what is threatening your environment in runtime so you can achieve your main security goal – to prevent cloud breaches by providing Runtime observability to detect real threats as they are happening so security teams can stop these activities before, they evolve to breaches.

Detection you can trust

Every business manager is looking to add more automation into their workstreams, and this is especially true for the CISO. Ensuring the fast and predictable remediation of a security issue is the ultimate goal. The only thing that is holding CISO's back from going full automation is trust. Is the triggered remediation action going to stop productivity? Shut down a website? Prevent a transaction from going through? CISOs need to trust that the remediation will not negatively impact the business. With the Purple Team, CISOs can trust the triggers. The Purple Team is learning from your environment and takes the full context of the cloud, along with permissions, and normal work patterns before executing the remediation plan. Security teams can leverage automation to quickly respond to threats before the company's name ends up in the news or on social media.

- Eliminate alert fatigue by raising **realerts** on actual happenings, and not how threat actors "may gain access" to your cloud – allowing you to focus on what's really important
- Reduce the total cost of ownership with fast containment leveraging deep insight into each activity to allow the SOC team respond efficiently in time
- Improve your prevention security strategy and risk management with robust threat detection

The Skyhawk platform's mode of operation assumes an incident is inevitable, therefore, you must have the right protection so that you can respond to an incident before it becomes a breach. It is important to note that CNAPP tools presenting paths, focus on visibility and posture improvements and do not observe behaviors in near-real-time, making it exceedingly difficult to stop a threat. Other tools are promoting assume a breach, those are focused on the incident response automation, and are post breach investigative tools after the damage was done. Skyhawk Synthesis delivers real insights into what is threatening your environment in near real time so you can achieve your main security goal – to prevent cloud breaches.

About Skyhawk Security

Skyhawk Security is the originator of Cloud threat Detection and Response (CDR), helping hundreds of users map and remediate sophisticated threats to cloud infrastructure in minutes. Led by a team of cyber security and cloud professionals who built the original CSPM category, Skyhawk Security evolves cloud security posture management far beyond scanning and static configuration analysis. Instead, using advanced AI sequencing of context-based behaviors, Skyhawk provides CDR in the 'Runtime Hub'. The sequence of these events elevates the awareness of actual alerts, or realters, which pose a threat to the business, reducing the noise and alert fatigue that other tools create. Threat detection gives organizations the observability they need to fully understand the business impact to mitigate risk, so security analysts can quickly detect and remediate malicious activities across multiple cloud platforms **as they happen.**

Contact us today to learn more at skyhawk.security

SKYHAWK
SECURITY