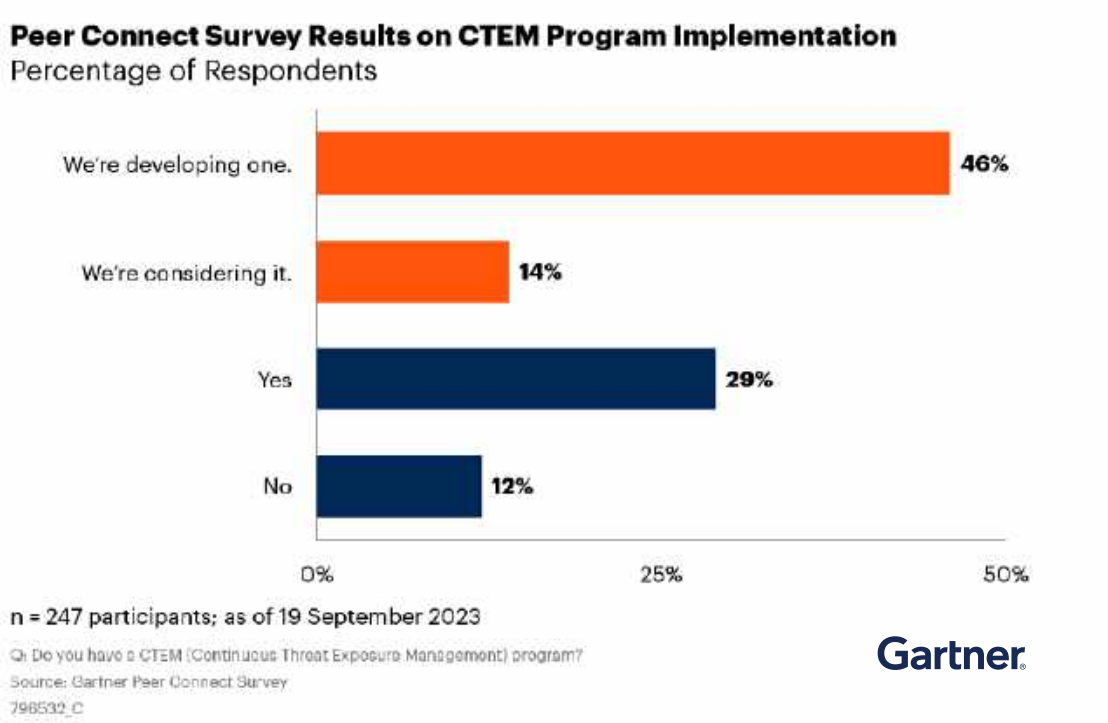
SKYHAWK SECURITY

OPERATIONALIZE YOUR CLOUD-NATIVE CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM) PROGRAM

Continuous evolving clouds with continuously evolving threats need continuous threat exposure management (CTEM). This programmatic approach to managing threat exposures can help organizations dramatically reduce breaches. Many organizations are well on their way.



According to Gartner®, these are several Strategic Planning Assumptions that, according to us, make CTEM incredibly attractive to security teams:

"By 2026, organizations prioritizing their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach."[2]

"Through 2026, nonpatchable attack surfaces will grow from less than 10% to more than half of an enterprise's total exposure, reducing the impact of automated remediation practices."[3]

"Through 2025, security leaders who implement cross-team mobilization as part of their exposure management program will gain 50% more security optimization than those only prioritizing automated remediation."[4]

"Through 2026, more than 60% of threat detection, investigation and response (TDIR) capabilities will leverage exposure management data to validate and prioritize detected threats, up from less than 5% today."[6]

"By 2027, the likelihood of breaches will reach threefold for organizations who fail to continuously manage remote access architecture and processes."[5]

1. Gartner, Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management by Jeremy D'Hoinne, Pete Shoard Published October 16, 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
2. Gartner, Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management by Jeremy D'Hoinne, Pete Shoard Published October 16, 2023
3. Gartner, Predicts 2023: Enterprises Must Expand from Threat to Exposure Management by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, John Watts Published December 1, 2022
4. Gartner, Predicts 2023: Enterprises Must Expand from Threat to Exposure Management by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, John Watts Published December 1, 2022
5. Gartner, Predicts 2023: Enterprises Must Expand from Threat to Exposure Management by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, John Watts Published December 1, 2022
6. Gartner, Predicts 2023: Enterprises Must Expand from Threat to Exposure Management by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, John Watts Published December 1, 2022

Organizations should be rushing to implement such a security program, especially in the cloud. Cloud attack surfaces are not completely under the control of their customers, this makes it difficult to patch for security and best practice configurations may not align with the organizations business requirements. Clouds are also completely remotely accessed, aligning to another strategic assumption. The net of the situation is: organizations that do business in the cloud need a CTEM Program.

Organizations no longer move to the cloud to try to lower costs – most organizations do not realize significant savings running their applications in the cloud. What companies do realize is the ability to spin up and spin down resources almost on demand, to meet changing business requirements. This flexibility and agility of cloud resources and services makes it very difficult to secure. A dynamic environment cannot be secured with static tools, a programmatic approach that leverages dynamic solutions that are also agile and flexible are needed. Visibility into a cloud environment also presents challenges to security. With just a credit card a company's cloud environment can expand, making it challenging to secure.

We believe, The Five Steps of a CTEM Cycle Align to Skyhawk Security's Continuous Proactive Protection

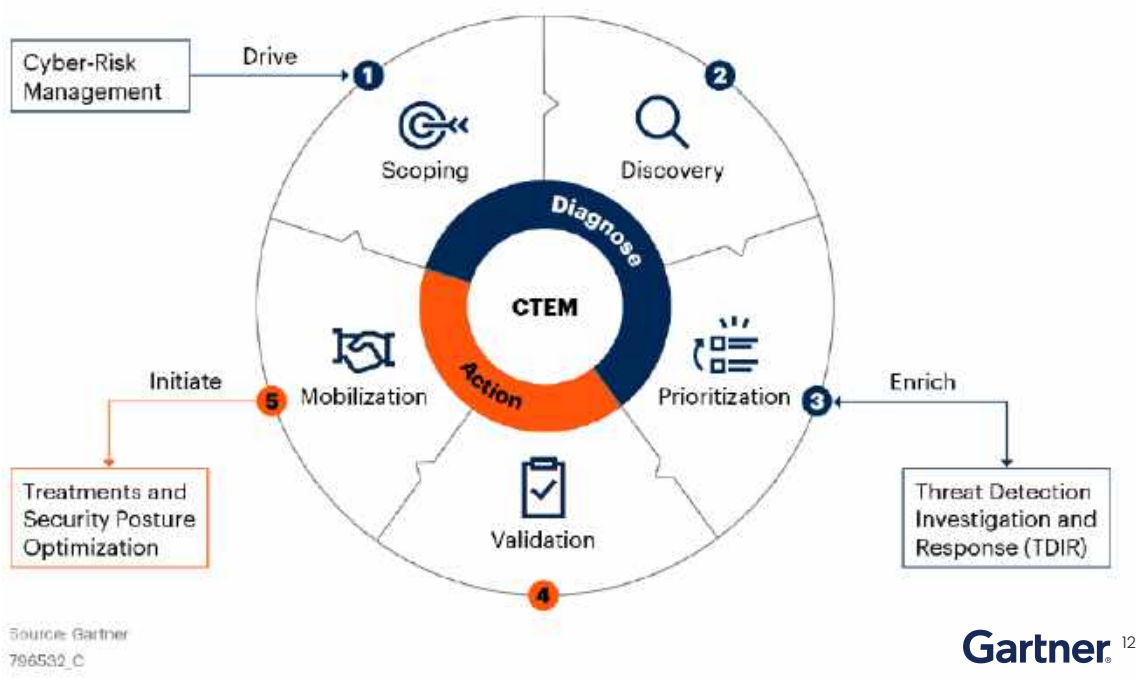
Gartner	Gartner Description	Skyhawk Description
Scoping	"To define and later refine the scope of the CTEM initiative, security teams need first to understand what is important to their business counterparts, and what impacts are likely to be severe enough to warrant collaborative remedial effort."[7]	Understand the environment, with Skyhawk, it looks for the easiest ways to get to the most valuable assets
Discovery	"Once scoping is completed, it is important to begin a process of discovering assets and their risk profiles. Priority should be given to discovery in areas of the business that have been identified by the scoping process, although this isn't always the driver."[8]	Discovery of assets, crown jewels, based on scoping, as well as the entire inventory, misconfigurations, and vulnerabilities.
Prioritization	"The goal of exposure management is not to try to remediate every issue identified nor the most zero-day threats, for example, but rather to identify and address the threats most likely to be exploited against the organization."[9]	Understand the weaponized and exploitable combinations which enable threat actors to compromise your most vulnerable crown jewels.
Validation	"In a security program context, "validation" is the part of the process by which an organization can validate how potential attackers can actually exploit an identified exposure, and how monitoring and control systems might react."[10]	Validate how potential attackers can actually exploit an identified exposure, and how monitoring and control systems (threat detection, posture, identities) will react.
Mobilization	"The objective of the 'mobilization' effort is to ensure the teams operationalize the CTEM findings by reducing friction in approval, implementation processes and mitigation deployments. It requires organizations to define communication standards (information requirements) and documented cross-team approval workflows."[11]	Identify and correct issues including misconfigurations, posture issues and create response and remediation for other threats if possible; apply deep learning updates to threat detectors.

7. Gartner, Top Strategi Technology Trends for 2024: Continuous Threat Exposure Management by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider Published October 16, 2023
8. Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider Published July 21, 2022
9. Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider Published July 21, 2022
10. Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider Published July 21, 2022
11. Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider Published July 21, 2022

Skyhawk's Continuous Proactive Protection continuously analyzes customer cloud infrastructure, proactively runs attack simulation against it and uses the results to prepare verified detections, validated automated response and remediation recommendations to ensure the cloud has the most up to date security defenses in place. This continuous protection process includes learning and automated adaptation of threat detection methods. This enables security teams to take a proactive and adaptive approach to their security strategy for the very first time.

For us, the key to a CTEM program is that it continuously evaluates the environment and seeks feedback in terms of its security and leverages this feedback to harden the environment and improve detection. We believe, the continuous feedback is key and what allows security to continuously improve to effectively manage threat exposure with adaptive threat detection. To us, the alignment of the continuous feedback of CTEM to Continuous Proactive Protection, which also seeks feedback, makes Skyhawk Synthesis a key technology for CTEM. Organizations can look at several technologies and integrate their inputs and outputs for CTEM, or they can leverage Skyhawk Synthesis.

Continuous Threat Exposure Management Image



The Maturity Model of CTEM

Skyhawk Synthesis Security Platform can help organizations accelerate the maturity of their CTEM Program and can be used to automate the deployment of the entire CTEM framework. Skyhawk is continuously evaluating the cloud to find new and vulnerable cloud assets as the cloud architecture evolves. Skyhawk Security evaluates the cloud configuration to determine where the crown jewels are, and then identifies the attack paths to those assets. The attack paths that lead to the most valuable assets are prioritized for further analysis as a breach of those crown jewels presents the greatest risk to the business. This is done automatically and continuously to find the most critical threat exposures so they can be addressed fast.

Skyhawk's Continuous Proactive Protection, an AI-based autonomous purple team, attacks and defends the cloud architecture simultaneously to find new methods that threat actors can use to penetrate the cloud. Using GenAI also helps organizations ensure they have the right defenses in place to stop AI-based attacks, which are on the rise. The output from this purple team identifies threat detection models that need to be updated, posture gaps, and can generate automated response and remediation recommendations.

Skyhawk Security is Critical for an Effective CTEM Program

Skyhawk Security's Continuous Proactive Protection provides consistent feedback to improve an organization's cloud posture, ML-based detection, and can generate an automated response or remediation as needed. The key that makes this successful is the platform continuously seeks out feedback from the environment leveraging Generative AI-based red team and blue team, or an AI-based autonomous purple team. As the cloud architecture changes, and posture and detection methods are updated, the platform seeks feedback to identify other weaknesses with posture or detection. The platform continues to seek out and identify threats and exposures, automatically and continuously. This continuous proactive protection helps organizations be three times less likely to suffer a breach.

13. Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider Pbulished July 21, 2022

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 cybersecurity 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 generative AI and ML sequencing of context-based behaviors, Skyhawk provides CDR within a 'Runtime Hub' to quickly detect and remediate malicious activities across multiple cloud platforms **as they happen**. Skyhawk Security is a spin-off of Radware® (NASDAQ:RDWR).

Contact us today to learn more at skyhawk.security

SKYHAWK SECURITY

SKYHAWK SECURITY

Realize CTEM for Cloud with an AI-based Autonomous Purple Team

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.

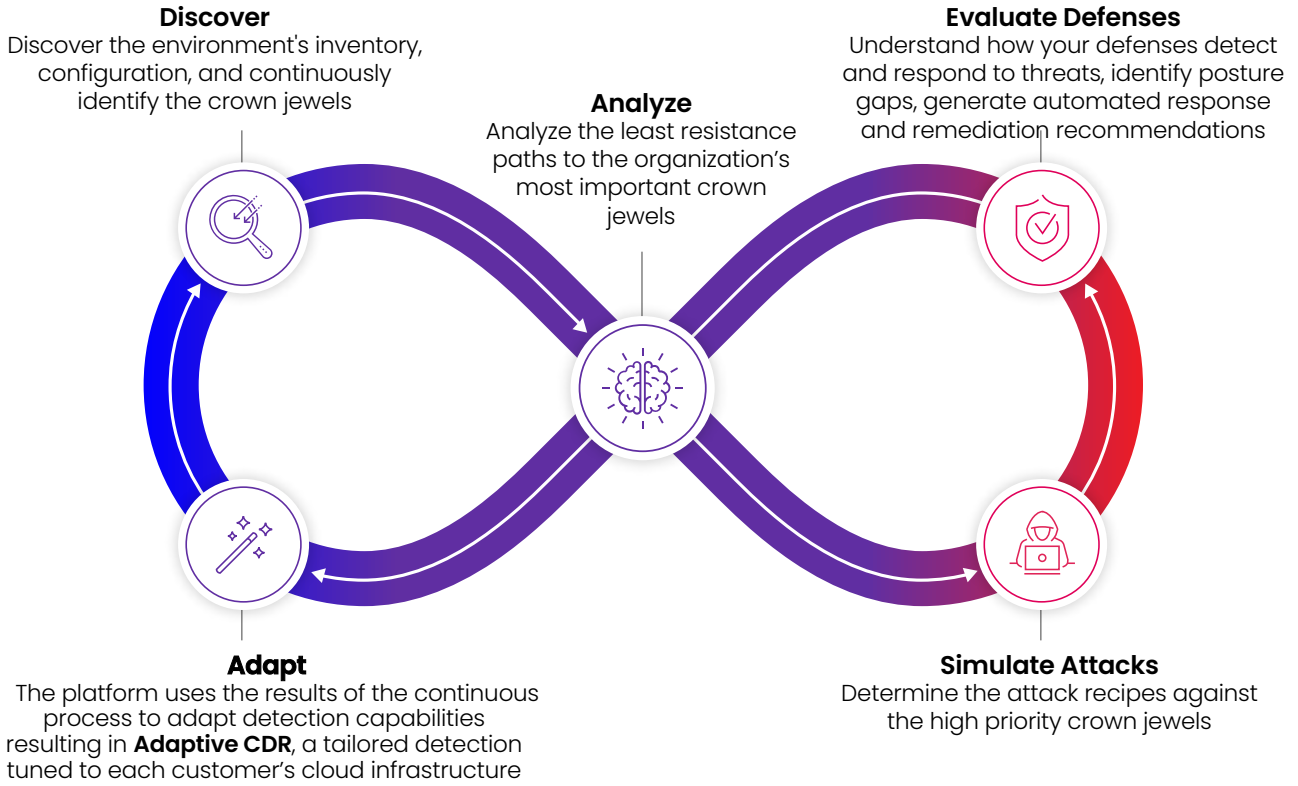
- **Detection you can trust for response automation:** The biggest inhibitor for customers to use response automation, is to trust the detection and response do no harm. Providing a continuous autonomous purple team results in pre-validated, trusted detections, with pre-validated, tested responses ensuring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



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