Case Study

SKYHAWK SECURITY

SundaySky realizes 5-figure ROI with Skyhawk Security

SundaySky transforms how businesses connect with their customers through video, making it easy to create, personalize, and optimize video at scale. Supporting the largest brands in highly regulated industries, like healthcare, finance, and financial services, means securing their video content is critical. Threat actors could create nefarious content and significantly damage the brand.

SundaySky uses AWS Cloud to support their international customer base. They were looking for a solution that would detect threats in the cloud before they became serious issues and preemptively detect threats, and they found that solution in Skyhawk Synthesis Security Platform.

Challenges

Like all security teams, SundaySky is highly utilized, and with a high-profile customer base, they need to lean on powerful solutions to ensure their cloud security. The SOC can spend up to 32% of their time on issues that are not a threat. The more time they waste on non-threats, the more time threat actors can be in their cloud, accessing data. They need a platform that accurately identifies threats and enables them to respond fast. A breach will not just compromise their infrastructure; it will compromise their customers' brands. This cannot happen.

SUNDAYSKY

> **"Skyhawk's Purple Team is the risk-superset view of the environment, allowing us to see in advance all the bad things that can happen. It is like the worried mom reminding you to take your coat or wear a helmet. The purple team prepares our cloud security team, so we are not surprised."**
>
> **Amit Levran**
> **Head of Security**

Solution

Skyhawk Synthesis Security Platform delivers preemptive, interactive, and real-time CDR in a single platform. The Continuous Autonomous Purple Team identifies weaknesses in the security posture and the prioritizes those fixes taking into account the severity, the level of exposure and the business value of the asset, which is defined by the business priority rules, so the team at SundaySky knows what needs to be addressed first and fast. The output of the Purple Team is used to update the cloud threat detections as well, so the team can realize the full flexibility of the cloud without concerns their security is not up to date.

SundaySky does their due diligence, and at the time of the renewal, they evaluated other solutions up against Skyhawk Security. They could not find another solution which comes close to the capabilities of the Skyhawk Platform. The cloud threat detection and response surfaces threats in real-time, with a focus on what matters most to their business through the business priority rules. The business priority rules ensure that the most valuable cloud assets for SundaySky are protected. These can be customized to align with their business priorities and their cloud infrastructure. This comprehensive view of their cloud security is critical.

Results

The key result of using Skyhawk is measured in real dollars, they realize a mid, five –figure savings annually while ensuring the security of their cloud as they eliminated the need for a 24X7 SOC service for AWS. Skyhawk Security is able to deliver a comfortable level of cloud security without the need for an around-the-clock, outsourced team. They have complete trust in the platform and in the prioritization of alerts. They get a pessimistic view of their cloud security, so they can clearly identify the weaponized threats.

The Purple Team's preemptive approach shows them in advance, what will happen, and the response. The cloud security team then knows, when they see this alert, it is a real alert that requires attention. The cloud security team also knows what to do as they have seen the attack rehearsed with the Purple Team.

SundaySky's security team is confident and much more relaxed now that they have Skyhawk Security. It is a great feeling and one that is new to them.

Skyhawk Synthesis Security Platform

AI-based Autonomous Purple Team instantly 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. The security team is confident in using automated response as the attack has been rehearsed, and the team knows it is not what should happen, the alert is verified as true. Furthermore, the automated response has also been rehearsed, ensuring no production impact.

> **"The Cloud Threat Detection and response is the "alarm" system to find threats fast. Having comprehensive threat detection as an alarm system along with the "worried mom" gives us a lot of confidence in our cloud security."**
>
> **Amit Levran**
> **Head of Security**

How does it work:

- **Discover:** Identifies all cloud assets and maps out the paths threat actors could use to gain access.
- **Analyze:** the configuration, vulnerabilities, and security controls that are in place are fully analyzed and attack recipes are created.
- **Simulate Attacks:** Leveraging the attack recipes, the Simulation Digital Twin is used to fully execute the attacks.
- **Evaluate Defenses:** Where the attack is successful, it is prioritized based on the business value of the asset that is vulnerable.
- **Adapt:** CDR machine learning models are updated for more accurate detections; pre-verified automated response is put in place for verified alerts.

Skyhawk's CDR with Purple Team: What does this mean for you?

- Preemptive security enables automated response thus reducing MTTD and MTTR to seconds
- Addresses the Progressive Technology-based Adversarial-Driven Risk
- Preemptive defense with Skyhawk runs continuously, adapting to changes in real time, ensuring newly introduced assets or configurations are always under protective assessment
- Significant reduction in threat exposure
- Reduce the impact of unresolved posture findings as once threat actors take advantage of them, Skyhawk Security will find the threat
- Manage the risk from posture findings that cannot be addressed as they will impact CloudDevOps productivity
- Improve team productivity as the CDR analyzes tens of thousands of events to prioritize a dozen alerts for your security team to address

About Skyhawk Security
Skyhawk Security is the originator of Cloud Threat Detection and Response (CDR), leveraging a multi-layer AI-based approach to identify and stop cloud threats before they become breaches. Skyhawk revolutionizes CDR with its Continuous Proactive Protection, an AI-powered Autonomous Purple Team, enabling security teams to take a proactive approach to cloud security for the very first time. Recently added Interactive CDR provides an out-of-band verification on cloud activities, incorporating principles of Zero Trust, so security teams can verify cloud events, and take action if needed. Led by a team of cyber security and cloud professionals who built the original CSPM category, Skyhawk's platform evolves cloud security posture management far beyond scanning and static configuration analysis, continuously adapting and improving threat detection so that it is always aligned with the cloud architecture.

Contact us today to learn more! skyhawk.security

SKYHAWK
SECURITY