CASE STUDY

# How this Hyper-growth Technology Startup Used Data-driven Security to Gain 3-year Savings of $28 million

## THE CUSTOMER

As a forward-thinking technology startup entering a phase of hyper-growth, this customer is well on their way to revolutionizing their industry.

## THE CHALLENGE

The company's presence in major cities globally, along with manufacturing facilities and offices, means a distributed workforce handling sensitive, proprietary information. Coupled with a significant number of physical assets, its global security operations center (GSOC) is tasked with managing alerts, incident response, and coordination with guarding units.

While the company relies heavily on data-driven analytics and cutting-edge technology to make decisions about its own innovations, its physical security tech stack could benefit from additional features to make it truly proactive.

Security leadership needed data to help them understand the effectiveness of their GSOC operations and its overall return on investment (ROI) it provides to the business. Given its rapid scaling of operations, finding programmatic efficiencies was key to being able to do more with their current resources.

The company's GSOC also wanted to enhance how they brought together multiple disparate systems and applications that were generating usable data – information coming in from access control systems, video cameras, video management systems, and analytics. The result was a siloed approach to security that resulted in more time from operators and analysts to glean the information they needed to provide informed response to incidents and events.

## OPPORTUNITIES

- Security operations that were more siloed, creating barriers to response
- Challenges with communication between the GSOC and guards at various global facilities
- Analog SOPs and procedures that hindered response time
- False alarms from multiple sensors creating a 98%+ false alarm rate

"Security leaders often have a hard time getting the organization to shift their view of physical security as a cost center rather than a valuable business driver. In this instance, HiveWatch was able to find areas where the business could save resources and time, and backed it up with data to prove it. **Cost savings over a 3-year period of $28 million** is significant to any business, especially a startup and we're just getting started."

**Ryan Schonfeld**
Founder & CEO, HiveWatch

While the company was collecting the right information, it didn't have a way to track and store data related to security incidents, such as tailgating, false alarms, or time to resolve incidents. When guards were dispatched as they were needed, they didn't always have the full picture of what was happening at any given time and communications from the GSOC to the field were challenged.

"The company's security was reactive – to alarms, incidents, events – instead of being more proactive in their approach," said Ryan Schonfeld, Founder & CEO, HiveWatch. Shifting to a more proactive approach would help the company's security leaders to better address resource allotment and lead to cost savings over time.

Additionally, as the technology being used wasn't always on-site in their facilities – but used throughout multiple locales – operators needed the ability to track valuable assets in the field and respond accordingly in the event of an emergency. This included the ability to dispatch its own team to specific geographic locations quickly and efficiently.


## THE SOLUTION

The relationship between the company and HiveWatch grew as leadership worked together to determine how technology could augment the company's security posture using the HiveWatch® GSOC Operating System (OS).

The HiveWatch® GSOC OS is a cloud-based Security Fusion Platform® that works with existing security systems to power a GSOC. Since the platform is software-based, it required no additional hardware or rip and replace for the company to install, layering its capabilities seamlessly into the company's existing systems, which included video surveillance cameras, video management systems, access control, and guarding applications.

**"The company wanted visibility into its security operations and functionality that would allow operators to have the information they needed, when they needed it."**

Jordan Hill, Head of Product, HiveWatch

Prior to implementing the HiveWatch® GSOC OS, the company had to manually bring in data from its various systems to collect all of the information they needed about an incident. This meant going to the access control platform to look up the alarm and search for the correlating camera to capture video footage.

An important part of this was the ability for the OS to build out floor plans that guarding units could look at to see exactly where an incident was happening on their mobile device in the field.

After the HiveWatch platform was implemented and operators were trained on the platform, the team monitored performance and how long it took to resolve incidents. The teams met weekly to address challenges, discuss how to move forward, and to make updates to training modules in an effort to better streamline the process.

"Throughout this process, HiveWatch was using incoming data to share what's happening with security leadership, uncovering areas where more training was needed, and supporting their documentation efforts to streamline workflows," Hill said. "By doing this, we were able to shorten the detection cycle using the platform and detect potential opportunities to update their internal processes."

As the partnership grew, the company expressed the need for a central repository to automate standard operating procedures (SOPs) that would make it easier for operators to understand the next steps in an emerging incident based on the kind of event that was unfolding. As a result, HiveWatch implemented the feature and made it widely available to this and other customers.

The company also looked to the HiveWatch platform to solve the problem of tailgating – where someone passes through an entry to a secure area, either forced or accidental, when another person accesses the facility.

## THE RESULTS

- Time to resolve from 15 minutes to sub-1 minute
- Root cause found on 30% of false alarms in first 60 days
- Streamlining operations freed up 57% of GSOC operators' time

### *Data-driven security leads to long-term savings of $28 million*

The benefit of the HiveWatch® GSOC OS was related entirely to the data: Using the data from the platform to understand the company's third-party guard spend, operator efficiencies, device health, and more allowed security leadership to make meaningful operational decisions that saved money and resources.

"Being able to show the HiveWatch efficiencies and understanding where they could do more with their current resources, where to utilize people vs. technology, and build more efficiencies led the organization to better use the team they have and save money over time," said Schonfeld. "Data was the enabler."

The data highlighted where there were more alarms - the "noisiest" areas - where having a guard made the most sense to proactively address incidents.

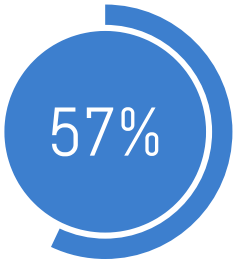
### *A/B testing at multiple sites*

With data-driven decision-making as a central theme in the company's HiveWatch® GSOC OS deployment, security leadership performed A/B testing of the platform across two GSOCs. One utilized the platform and the other did not, then they compared the data, which found the following:

- *Root cause found on 30% of false alarms in the first 60 days*: Through the data provided by device health monitoring within the HiveWatch® GSOC OS platform, the customer was able to have their systems team address the root cause of 30% of their false alarms within the first 60 days.
- *Addressing false alarms freed up 57% of operators' time*: Prior to implementing the HiveWatch® GSOC OS platform, the customer had so many incoming alarms, they determined the organization would need six times the number of operators they currently had per day to respond to every alarm as they scaled.

- *Time to resolve from 15 minutes to less than 1 minute*: The customer reported that prior to leveraging the platform, there was a 15-minute average time to resolve an incident, from acknowledgement to closure. This means that from the moment the alarm was sent to operators and evaluated for whether it was a false alarm or an actual event, it took 15 minutes or more for operators to resolve the issue. After implementing the HiveWatch® GSOC OS, the weekly average is now sub-1 minute.

### *GSOC achieves 57% more efficiency*



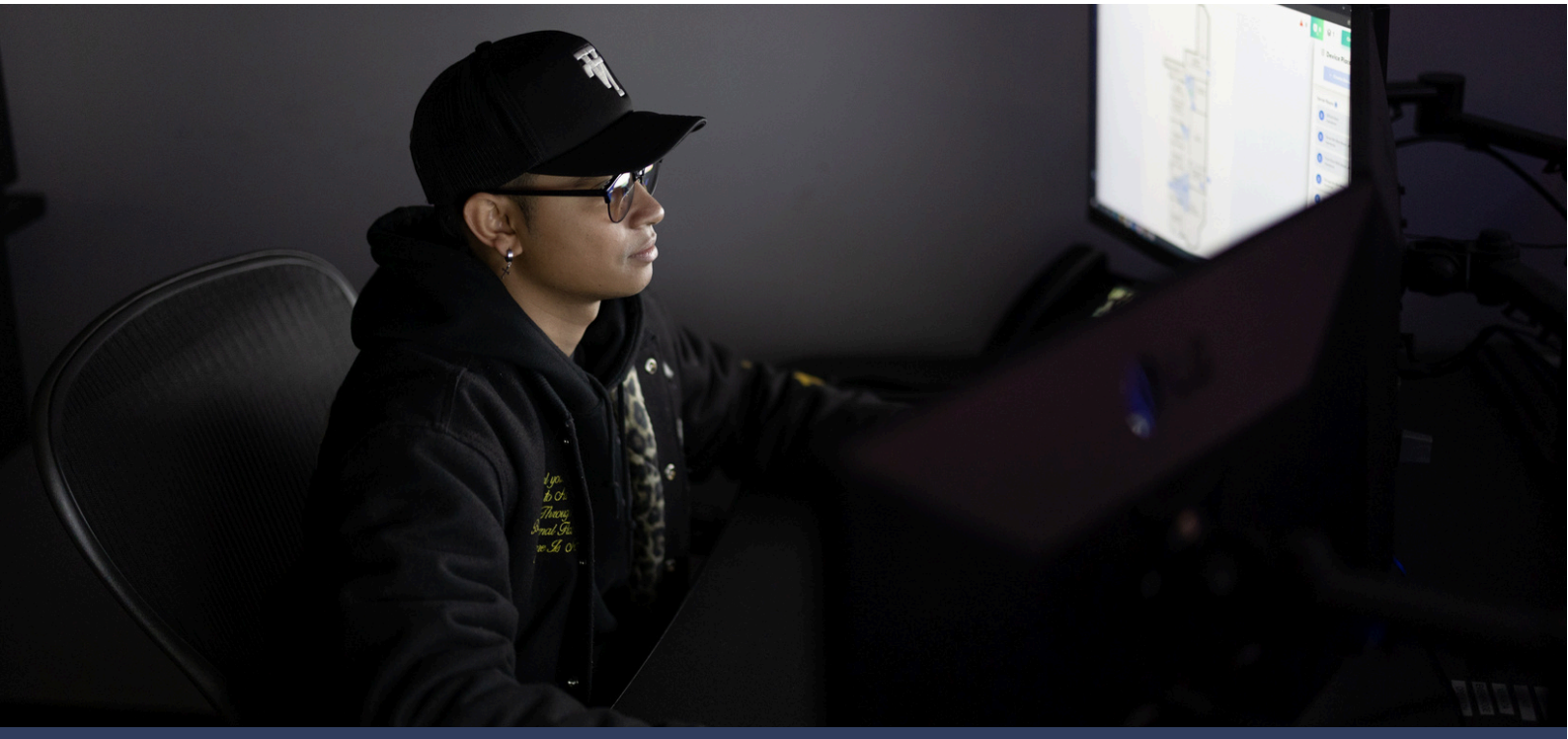

One of the biggest findings was the HiveWatch platform's contribution to the company's overall business goals. The platform helped the GSOC operators become 57% more efficient, shifting from primarily reactive to a more proactive approach to physical security. This means the team now has more time to devote to strategic work that's directly tied to business growth and scale.

"The reality is, your GSOC doesn't have to be a cost center, it can be used to drive revenue rather than spend it," Schonfeld said. "When you're operating in a reactive way, you have to increase headcount to address all of the incoming alarms and incidents. If you're able to reduce the number of false alarms that have to be addressed, you have more capacity to provide proactive, strategic planning and execution that adds value from the GSOC."

### *Dispatch based on geolocation in metros*

One of the biggest challenges the company faced was having physical assets across a wide geographic area that weren't facilities. As a logistics company, when they had an incident in the field, it was difficult to integrate field operations with the security infrastructure they had in place.

Working with HiveWatch, the company wanted to see where their assets were and have the ability to route the correct staff to the location, giving them a quick way to navigate to the scene. With the scalability of the platform, HiveWatch was able to deliver this level of visibility for operators that encompassed their needs and layered data-driven insights to determine patterns and potential improvements that could be made to the company's operations.



HiveWatch

### *Customizable, integrated SOPs*

Integrating SOPs into the platform saves the company's operators valuable time navigating through written binders and resources for how to respond to any given situation. This method of integration represents a shift from an analog approach to more digitization, which prioritizes workflows to optimize response and save time and resources.

Additionally, having SOPs readily available saves the company a significant amount of time in training, allowing their GSOC staff to be up and running quickly. Traditionally, security operators have a high rate of turnover, so being able to onboard in less time can mean significant cost savings.

### THE FUTURE

By correlating data together, identifying broken sensors, and providing the company with more information to make better decisions about their security program, HiveWatch was able to change how the entire company views security.

"The bigger question was whether HiveWatch could derive more value from the company's security program and the answer is a resounding 'yes,'" said Schonfeld. "Security leaders have a hard time getting the organization to shift their view of physical security as a cost center rather than a valuable business driver. In this instance, HiveWatch was able to find areas where the business could save resources and time, and backed it up with data to prove it. **Cost savings over a 3-year period of $28 million is significant to any business, especially a startup.**"

# Intelligent, efficient, and scalable security

## About HiveWatch

HiveWatch solves some of the physical security industry's biggest and most frustrating challenges including false alarms, tailgating, integration of disparate security technologies, lack of data and analytics, and operational inefficiencies.

The **HiveWatch® GSOC Operating System** allows security teams to bring together information, data, and technologies into a single platform that improves their overall security posture, reduces noise and complexity, and delivers more intelligence across the organization.