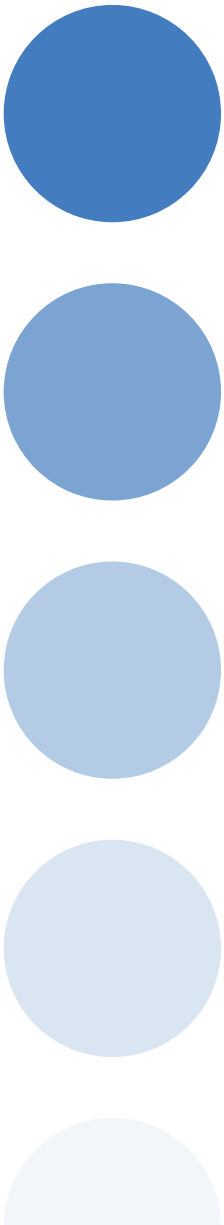
EBOOK

Physical Security Needs a Makeover: How to Approach Security Differently

HiveWatch

Table of Contents:



Introduction:

As security professionals, you've likely heard the phrase "but we've always done it that way." And if you're venturing into this eBook, your likely response is to wrinkle your nose and think to yourself, "But there's a better way!"

Physical security needs a makeover. There. We said it.

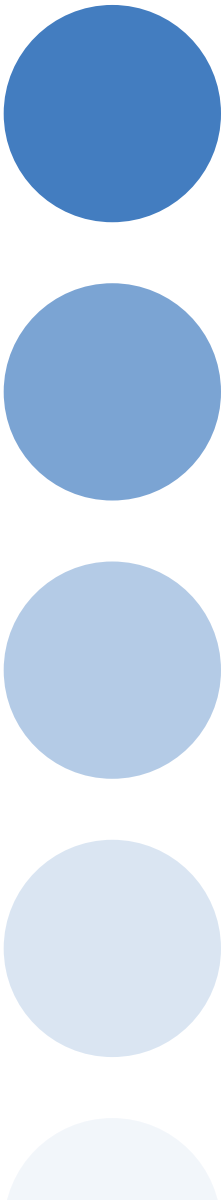
But we don't take this change lightly. Over the last several years, we've reviewed security from the framework of what works, what needs improvements, and what we can do to make the process easier for security leaders.

The answer? Data and making sense of it.

In this eBook you'll find a series of articles and facts that help build on the idea that there may be a better way to approach security – especially for security practitioners and operators.

This eBook should speak to those who question how the siloed systems that your organization has invested in work together to provide more streamlined information to leadership, how new technology needs to be open and able to ingest the data being collected, and how fusion is the way forward.

We hope you will enjoy the thoughts presented in this book.



Security Doesn't Scale

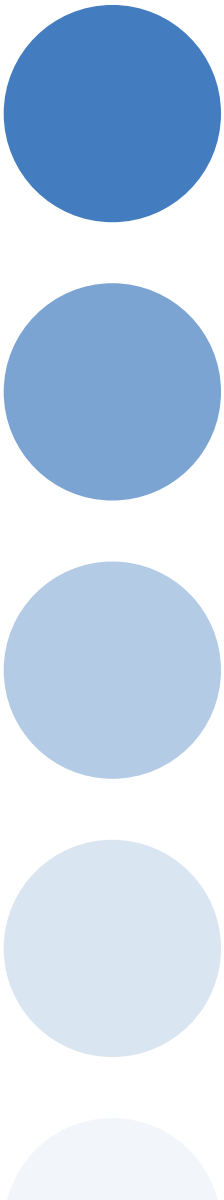
By Ryan Schonfeld

News flash: Security doesn't scale!

Now before you get offended and stop reading, consider where we are as an industry today and how much we've evolved over the past 5, 10, 15, 50 years. Sure, there has been great innovation across certain products:

- Camera resolution is higher than ever, at a price point that security leaders probably couldn't have fathomed fifteen years ago. Today, cameras are essentially IP computers that perform advanced edge processing and analytics.
- Analytics have progressed from being a buzzword thrown around to actually delivering on many of its promises.
- Organizations are continuing to replace their analog camera fleets with new IP technology, albeit at an alarmingly slow rate.
- Facial recognition, object detection & classification, biometrics, drones, counter-drone, access control, tailgate detection, weapon detection, gunshot detection, aggression detection...and the list goes on.

Yet, with all the amazing product and technological innovation our industry has seen, we haven't resolved a core problem. Security doesn't scale.



An Antiquated Industry

Everyone has heard the notion of "gates, guards, and guns." All of those are important elements to various security programs, and I make no assertions that humans can or should be removed from the loop. Security will always require humans at a certain level to understand context and nuance to make a rapid decision. In the end, we protect organizations' people, assets, and brands. Sometimes that can mean critical life and death decisions. So with all of the innovation we've seen, why can't we effectively scale programs that are operationally impactful and don't totally break the bank?

I started my career in law enforcement, one of the most antiquated professions I've experienced in my life. It's also far and away one of the most rewarding things I've ever done, but it never ceased to amaze me how technology wasn't used to improve operations, increase closure rates, and reduce the time to resolve events. Sure we had access to new gadgets and software, but everything stood alone and very rarely did one system feed another. So it was an endless cycle of better mousetraps.

New Tools

When I moved to the private sector, my first role was with a company that literally made its money from gates, guards, and guns. New tools in the guarding industry made patrols more efficient, tracked guard movement and compliance, and reduced paper reporting. Yet how many of those tasks

performed by the guard(s) really required a person to perform it? Why isn't the platform the guard companies sell to customers to track patrols, events, incidents, etc. linked to the systems the organizations use to run the rest of their programs? Aren't those metrics key in making decisions about your program?

Then, the real learning began as the security leader in a large Fortune 500 company. I started in investigations which used one platform to manage the workflows and data. The security team used an entirely different platform to intake reports and relevant functions. The camera system didn't talk to the access control system, the intrusion systems were standalone, and like many other companies, we had disparate camera, access control, and intrusion systems deployed at our facilities around the world. How do you build an effective global program with no standards? The options were a large capital project to rip and replace, or buy a Physical Security Information Management System (PSIM). Neither of these were a good option, further proving that security doesn't scale.

I left my corporate role to start a security consultancy to prove that security could scale if you took the right tech-forward approach. A core tenet was that companies shouldn't have to compromise their culture to have an effective program. We quickly started working with some of the fastest growing companies in history, yet the problem remained the same. There was great technology available to solve individual problems, but the systems were just that - standalone. Connecting disparate systems required server-heavy, high latency products that were brittle and took forever to deploy (PSIM). Once deployed, they took teams of people to maintain. There had to be a better way.

Unless a company is building a ground-up facility, much of their scale involves taking over spaces that were once occupied by others. This is a huge part of how big companies end up with so many different technologies.

The Solution

We set out to solve the problem of the connective tissue between disparate solutions - one that was:

- Cloud-based
- Easy and quick to deploy
- No major capital investment
- Intelligent enough to automate the majority of functions that require human capital today, while properly prioritizing and visualizing those events that truly require human decisions
- Capable of reducing the "noise" of constant false positives

I began assembling a team of all stars from places like Apple, Bird, Cisco, and NORAD to prove that security can scale.

Introducing: The HiveWatch® GSOC Operating System.

The Top 3 Benefits of Utilizing Machine Learning in Security

By Sean Mulqueen

Machine Learning (ML) should not be confused or used interchangeably with AI (Artificial Intelligence). ML is a subcategory of AI that uses algorithms to recognize patterns from data and automatically learn insights, allowing programs to become more intelligent.

ML ultimately should aim to remove the need for humans to do repetitive, low-value decision-making activities, like triaging false positives or system/device health ticketing.

Here are the top 3 benefits of utilizing ML in security:

1. Free up time for other strategic initiatives

Do your operators spend countless hours dealing with false alarms and faulty sensors? HiveWatch had one customer who, before adopting HiveWatch, calculated that they would need 6x the amount of operators they already had to be able to deal with all of the alarms coming in. By utilizing a system with ML, the data collected from these alarms can be processed to identify patterns and provide insights, taking the guesswork out of these alarms. Ultimately, this allows operators to be less reactive, giving them more time to work on strategic and proactive initiatives.

This, in turn, up-levels the position of operator, to analyst, which brings me to my next point...

2. Create lower turnover rates

Historically, the security industry has incredibly high turnover rates. Annual rates are anywhere from 100-300%. Recruiting & training new operators is expensive, timely, and stressful. This is why retaining employees, especially your operators, is so critical.

According to a recent Korn Ferry poll of 5,000 professionals, the top reason people look for a new job is boredom. Getting a job in security, which on the surface sounds fun, exciting, and challenging, and then sitting in a dark room all day clearing false alarms caused by birds - not exactly what you signed up for. ML can not only alleviate that boredom, but help up-level the job. With ML your operators are now analysts, fueled with the idea of career growth and opportunity.

3. Save money

Bringing it all together - ML ultimately saves organizations money. The combination of false alarms (a $3.2 billion industry issue), additional guard staff (ie: the 6x guards mentioned in the first point), and consequences of high turnover make the security organization a cost center.

Embracing New Technology in Physical Security

By The HiveWatch Team

As companies reflect on the continued impact of the COVID-19 pandemic and subsequent changes to business operations, the maturity and effectiveness of physical security infrastructure and data has become imperative to a successful transition to remote and hybrid work models. In particular, Cloud-based software solutions have proven critical to maintaining a strong security posture as travel and resourcing constraints limit the ability to monitor and manage security operations in-person.

Cloud-based security software that gives organizations the ability to access and control camera systems, monitor video feeds, conduct maintenance tasks, evaluate system health, and perform updates to firmware/software from remote locations have been identified as must-haves for maturing security organizations.

Answers from more than 2,000 security leaders give insight as to how the physical security industry is changing, with more movement towards the Cloud and an increase in investing in upgrades to legacy and/or disparate access control systems. A recent Genetec State of the Industry report showed that 45% of large companies (those with more than 1,000 employees) have already adopted cloud solutions.

An impressive 94% of survey respondents stated plans to deploy Cloud or hybrid-cloud solutions for their long term plans, a major increase from 2020 when 26% of those surveyed said they began implementing their cloud journey. 35% of respondents said the pandemic directly accelerated or triggered their Cloud strategy.

Christian Morin, Vice-President, Product Engineering and CSO at Genetec Inc, stated, “While many physical security departments were hesitant to consider cloud-connected solutions in the past, they now better understand the benefits these solutions bring and how it can help them to better utilize their resources to achieve their respective business goals while minimizing their overall operational complexity.”

The Challenges for Organizations

Security professionals looking to transition to a Cloud environment are generally worried about maintaining secure and compatible systems during the migration period. When considering a transition to Cloud or hybrid Cloud physical security environments, security professionals cite outdated infrastructure, cybersecurity vulnerabilities, and remote management challenges as their top 3 concerns. These challenges are only compounded as systems become more reliant on remote technology and devices continue to be spread across multiple networks.

Prior to the pandemic there was a traditionally slow trend to adopting Cloud-based software as it was often viewed as overly laborious since

applications have usually been built into in-house hardware and infrastructure with limited remote capabilities. This hesitancy to leverage cloud-based solutions has largely dissipated, however, as companies realize that security infrastructure requiring on-premise maintenance may not always be feasible. Even with the above challenges in mind, 47% of Genetec survey respondents indicated plans to begin or further deploy parts of their security solution to the cloud. Cloud-based technology offers a way for companies to meet new challenges, scale as needed, and readjust to changing circumstances or events where access can become limited.

"As we emerge from the pandemic, organizations will contend with three undercurrents; changes in the physical dimension of work as workspaces evolve into hubs for collaboration and cohesion, workflow automation of the mundane in a bid to drive productivity and retention, and board-level interest in achieving operational resilience through integrated risk management." said Pervez R. Siddiqui, Vice President, Offerings and Transformation, Genetec Inc.

Advantages of the Cloud

1. Adaptability and accessibility

The Cloud is reachable via internet access, from anywhere you can sign in, with many security solutions able to be controlled and managed through a computer browser or mobile device. Access is not limited to on-site locations, on desktops with dedicated software. Security personnel can manage the Cloud security solution from anywhere, offering more flexibility.

2. Reducing physical locations and real estate

Moving backend applications to the Cloud means the potential for better utilizing physical locations. Dedicated sites for security housing racks, cooling systems, and power hookups can be reduced and repurposed for other uses, giving companies the chance to mindfully maximize their real estate.

3. Updates can be done remotely

Cybercrime is a threat when the access to security systems can be done through the internet. Cloud architecture suppliers, however, know the threats to cybersecurity and will follow best practices to mitigate risk. Updates, patches, and system fixes are kept up to date and done automatically, as opposed to waiting for manual updates on most on-premise security systems. This could have the potential to make Cloud systems more secure, since they are updated on time to keep up with the latest security risks.

Migrating security systems to a cloud-based software, such as HiveWatch, gives organizations the ability to adapt as situations change. Key operations can continue despite limitations to physical access and circumstances, even when an unpredictable event occurs and the lasting impacts that it may have on businesses and activities.

In Physical Security, Data-driven Risk Assessments are Incomplete Without Device Data

By Rebecca Sherouse

As the global threat landscape evolves and security resources remain limited, security leaders have had to re-think historic approaches to security risk assessments to meet the demands of unpredictable threat environments and ever-changing business needs.

Forward-looking security practitioners are now leveraging data to conduct quantitative, data-driven risk assessments, reducing the need for global travel among their teams and resulting in real-time risk data that has a meaningful impact on security operations, business investment, and resource allocation.

As security functions take this leap and teams begin to leverage multiple streams of security data to measure risk, one pain point is proving harder to overcome than the rest: device data.

Device data tells security practitioners what kind of technical security controls are in place and how well those controls mitigate against any variety of security threats. While a standard site assessment might determine whether or not a site is equipped with a type of security system, it is only with device data that we can determine how well those systems are functioning. Without actionable device data, it is nearly impossible to accurately measure risks posed to company assets.

As HiveWatch teams work with our customers to untangle device data, some key trends have begun to emerge.

Here are the three most common reasons device data is difficult for security practitioners to leverage:

Disparate security devices are the norm

As many security leaders will tell you, it is not uncommon to have multiple security systems and device types monitoring assets at the same organization. Security teams often inherit disparate security systems across their portfolio, which results in noticeably different reporting capabilities and data types available from those devices. This variance in device type and subsequent data output makes it a challenge to collect, standardize, and analyze device data in meaningful ways.

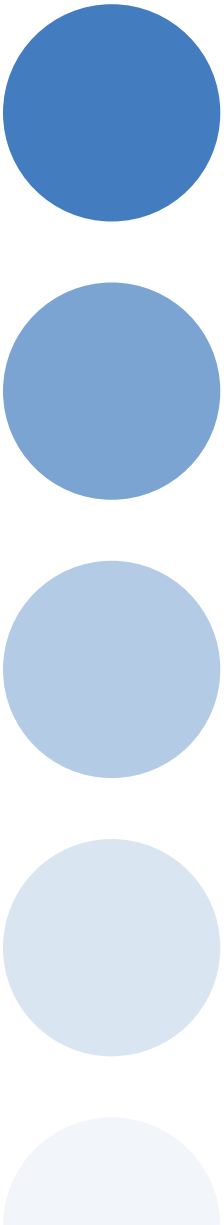
Devices are not appropriately configured to collect relevant data

For security practitioners with less technical knowledge, it is easy to assume that security devices are configured to collect as much relevant information as possible. This is not always the case however, and devices often require

unique configurations to optimize data collection and reporting capabilities. Security teams may be losing out on years of impactful security data if devices are not appropriately configured at installation.

Systems data is unstructured and overwhelming

Device data, in its unstructured, raw form is nearly impossible to manage without the support of technical resources to clean, query, and visualize the data. While there are proactive steps security professionals can take to ensure device data is usable, teams looking to leverage this data will always require the support of analysts to facilitate meaningful, quantitative security analysis on otherwise unruly datasets.



PSIM is Out. Fusion is In.

By Ryan Schonfeld

In a global security operations center (GSOC), operators are making decisions about the safety and wellbeing of assets and people. A lot of the challenges across security programs involve many of these decisions being made reactively, which can cause burnout and fatigue among operators and set security programs back from getting to the root cause of emerging threats.

The answer? A more tech-forward approach that fuses data together to create a more seamless, proactive, and effective response, also known as Security Fusion.

Here are some of the challenges that fusion can address:

The Old Way: Numerous systems that require management

In the past, organizations only had one option for integrating disconnected security applications and devices, which came in the form of a physical security information management (PSIM). But these solutions came with a high price tag and complex execution – not to mention minimal ROI.

The New Way: Data fusion

Aiming to integrate data from siloed security systems – think video surveillance, access control points, fire and intrusion alarms, etc. – into a holistic view that enables users to quickly filter de-noised threat information relevant to the organization, is the way forward. Using a Security Fusion Platform® like the HiveWatch® GSOC Operating System (OS) instead of a PSIM broadens the capability of security leaders to pull in additional data points to better inform decisions, such as intel platforms and situational awareness data.

The Old Way: Expensive rip and replace for PSIM

In many cases, implementing a traditional PSIM involves months of designing, building, and implementing a platform that is largely rooted in expensive, on-premise hardware.

The New Way: Scalable digital transformation

We live in an instant gratification society, and it's unfair to think that the same doesn't apply to a large corporation aiming to upgrade their physical security posture. Cloud-native platforms bring speed to the table, as well as the ability to properly scale as necessary and needed.

The Old Way: Too many false alarms

Security operators are constantly addressing which alarms are “real” and which are false alarms. Many of these false alarms are considered “noise.” It becomes crucial then to differentiate between what is noise, and what is intelligent information which can be researched and found viable.

The New Way: Addressing inefficiencies

Bringing in data from multiple sensors and fusing them together creates more intelligence for security operators who are then better able to direct resources to a specific location. Using machine learning, a Security Fusion Platform® pulls data from a company’s disparate monitoring systems and security sensors to provide operators the information to evaluate and respond to alerts without sifting through false alarms.

The Old Way: Sifting through incoming data

Sometimes in a SOC, there are multiple workstations that contain solutions that must be accessed separately as an alarm comes in. That’s not only inefficient; it’s dangerous.

The New Way: Data-driven decision-making

Centralized monitoring and intelligence changes the way security leaders process information. By incorporating machine learning technology into a platform that fuses multiple data points together to garner better information, decisions are more streamlined and effective. This can also help organizations to move corporate safety operations from reactive-only responses to designing proactive programs that identify threats before they happen.

Doing More with Less: 3 Considerations to Make to Optimize Your Security Programs

By Jenna Hardie

Here's the deal.

Budgets are tightening or staying flat. The recent State of the Industry report from Genetec found that 34% of respondents said their budgets were going to remain flat, while 16% said they were expected to decline. This leaves security teams wondering how they can optimize their programs while keeping budget considerations top of mind.

In one of our awesome webinars, we were joined by Bobby Louissant, Head of Technical Partnerships, Global Security, at Meta; Rebecca Sherouse, Director of Account Management & Security Advisory, at HiveWatch; and Gerardo Iglesias, Director of Physical Security, at Molina Healthcare. The discussion was moderated by Jon Harris, Sr. Product Manager at HiveWatch.

The group talked about the current landscape in physical security, driven by the need to maximize and streamline existing investments and operations to meet budgetary demands being placed on the organization.

Here are three considerations you should make when optimizing your security program with budget constraints in mind:

1. Start with an Assessment

You can't begin to optimize your security program without knowing what you have. You need to take a closer look at the data that's coming in, the risks you're addressing, and whether or not there are segments of the budget that require analysis.

"The initial physical security assessment is critical," said Iglesias. "Not every site should be cookie cutter...your security program should vary based on the business needs of the site along with what the ultimate goal of that site is there for. If you're in a high-crime risk area, along with a potential history of incidents, then more guards, cameras, and other technology may be necessary. There are ways for us to take a look at the overall design of each site and that's where the spend occurs – and where savings can be found."

Similarly, Sherouse pointed out that the security spending for pre-pandemic may need to be re-evaluated as hybrid and remote work has shifted, which might free up additional budget that can be made available for technology advancements

2. Involve Stakeholders at all Levels

Engaging stakeholders at all levels provides security teams with the ability to identify potential roadblocks to success related to physical security program implementation. The panelists agreed that building community within the security team by encouraging leaders to listen to the concerns of operators

and sharing those with executive leadership can help build morale. Doing so can also reduce turnover, which can be a drain on resources and affect budgets.

"Leadership has to establish a baseline with their teams and an understanding of what the move forward strategy is about," Louissaint said. Without it, he stressed that teams aren't empowered to make cost-cutting decisions that are aligned with overall business goals.

"It's more of a community approach rather than top-down," he said.

Molina Healthcare sites are often in less affluent areas, Iglesias said, which makes it important to weigh the input from employees about what they need to feel safe going to work each day. "It's not just you (as a security leader) approaching the finance committee; it's you with the stakeholders that support your vision that ultimately translates to better employee morale for those employees directly affected," Iglesias said.

"A lot of successful security leaders often partner with business continuity teams and crisis management teams to understand the various exposures of their assets to risk," Sherouse added. "Through that, they start to understand the risk level of various assets. Taking a risk-based approach to securing the business is a great first step."

3. Incorporate Technology Advancements

Once a security program combines risk assessments that affect the business, as well as input from key stakeholders, then decisions can be made about how to provide more comprehensive data-driven decision-making for security leaders with technology.

"One of the best resources we have in this industry is the data," said Louissaint. "Using that data is probably the best resource you have as a security leader to position your business in a manner where you can be prepared, or having to cut costs."

"I find that the rip and replace cycle that we all have found ourselves in our career is brutal and very difficult to justify to finance. You're only going to get one shot of going through that justification cycle," Iglesias said. To combat the cycle, he recommends layering artificial intelligence (AI) technology that allows operators to better manage incoming alarms by identifying false alarms, finding the root cause of the alarms, and being able to respond quickly and efficiently.

"Technology that leverages AI isn't inexpensive, but there's an ROI associated with it, especially in the security industry, where we're constantly being asked to do more with less resources," Iglesias said. "It's almost as if you have no alternative but to really start leveraging the technology that you've already deployed."

Security teams are taken a lot more seriously when risk to the business can be both qualified and quantified, Sherouse pointed out. "How do we quantify threat intelligence? How do we quantify the attractiveness of our particular

assets? And how do we measure the controls that we have in place, including device data, sensor data, all of that good stuff to give an accurate picture of our exposure that sets the groundwork for optimizing security programs?" she said.

New advancements fall into the following buckets, according to Sherouse: reducing administrative burdens, enhancing how we collect data, and then optimizing that data.

- Reducing administrative burdens: The mobile-first management and remote access technology advancements can be found here, even something as simple as mobile credentials. There's a tremendous amount to be said for the administrative burden that has been decreased with these advancements and continuing to look towards technology that can help us to do that in security teams is a really important one.
- Enhancing how we collect data: This encompasses the use of low-cost movable sensors that are emerging in the market; things like proximity sensors, lower cost technology to collect different data which can be an alternative to the rip and replace approach. These investments may not be long-term, but they can drive a ton of value and help gather more data for security teams.
- Optimizing the data: System centralization and ingesting disparate security devices and data from your cameras, access control, environmental sensors, and more allows leaders to visualize incoming data in a meaningful way. This is becoming a game changer. It takes some of the highly manual, time intensive tasks from operators, like clearing mass amounts of false alarms, and redirects these individuals to perform more meaningful tasks for the organization that provide more value to the business.

"If you're dealing with the pressure of cost reductions today, it's going to be hard to purchase an AI solution, but you should plan to work toward this goal," Louissaint said. (Hint: The HiveWatch ROI Calculator can help you figure out how the platform can save your organization time and resources. Contact us for more info.)

Security Fusion, Explained

By Jordan Hill

As HiveWatch has built a platform aimed at bringing together multiple streams of incoming data, we talk a lot about the term 'Security Fusion.' Now, we're defining it.

What is Security Fusion?

Security Fusion refers to the process of integrating and analyzing data from multiple sources to enhance situational awareness, improve decision-making, and support proactive security measures. This process typically involves gathering information from various security sensors and other sources, and then processing, correlating, and analyzing the data to support operational decisions.

Security Fusion Sources of Data

The main sources of data for physical security, when it comes to Security Fusion are:

- Video surveillance systems
- Access control systems
- Security personnel records
- Occupancy data
- Social media monitoring
- Public safety and law enforcement databases
- Risk intelligence
- Analyst-curated intelligence
- Executive protect
- Other Internet of Things (IoT) sensors

Security Fusion is important because it transitions security programs from a basket of individual technologies to an interconnected experience that improves operations for guards, operators, program managers, and security executives.

For guards, Security Fusion allows faster sharing of data around threats they are dispatched to and the collection of operational data to evaluate how they perform. For operators, when identifying potential threats, the cross referencing of all of these sources historically required a lot of time hopping between systems. This methodology is vulnerable to human error in detection and lacks automation that would allow operators to focus their time on real, active threats.

Security Fusion unlocks viewing all program data related to a specific incident in one interface, while also using that same multi system data to remove the clutter of false positives alarms, to ensure that only real alarms

reach the GSOC. This can be as simple as using data from the camera that overlooks an alarming door to verify whether an actual threat has happened.

For program managers, Security Fusion can also streamline analytical capabilities. Rather than pulling reports from each individual platform where you have to manually calculate a security program's performance, with Security Fusion, you can automate how you measure your program performance, so you focus more time on identifying and responding to the areas of your program that need improvement.

How HiveWatch Uses Security Fusion

At HiveWatch, our vision is to change physical security from an art into a science. That means connecting existing technology to speed up and automate redundant processes, while highlighting where gaps are. We want more "addressing business risk, impact, and threat frequency" and less "the way it's always been done."

We want program managers and security executives to spend less time managing the daily operations and more time improving their security program design.

This vision influences every aspect of how we build products at HiveWatch. When we design new features, we ask:

- How will this feature save operators or program managers time?
- How will this feature help a program manager or security executive identify gaps in their security program?
- How will this feature help a program manager or security executive map security concerns to the business?

At HiveWatch, we are committed to helping organizations not just achieve Security Fusion, but also reap the benefits it unlocks.

Request a Demo Today!