EBOOK

Elevate Your Physical Security to Match Your Cybersecurity

HiveWatch | TechnologyAdvice

What is Security Fusion?

In today's climate, businesses ranging from corporate giants to small family shops are struggling to combat an uptick of multi-faceted security threats. These attacks often come from numerous directions and have specifically worsened since the onset of the pandemic. What's more, hybrid work models have created a distributed workforce, which has exponentially increased the complexity and urgency of detecting and responding appropriately to a security breach in a timely manner. These threats can include:

- Insider threats to data and assets
- Targeted, online attacks
- Seemingly random online attacks
- Physical attacks on and disruption to supply chain and facilities
- Attacks by former employees, contractors, or partners
- Orchestrated attacks by nation-states or their proxies

What's clear from this list is that some threats are physical. They rely on actual people to approach a facility or employee. We also know that many of today's threats take place online, carried out by actors that are never seen or heard. Most threats, however, blur the line between the physical and virtual. That being said, most organizations are not well prepared to defend themselves against these looming physical attacks. Instead of utilizing integrated security technologies, they try to solve their problems with unscalable and expensive human operations, guards, and/ or disparate systems which create noise and inefficiencies, to monitor these threats.

Meanwhile, forward-thinking organizations are investing heavily in their cybersecurity efforts by implementing smart software designed to detect and remediate all manners of online threats. Security operations centers (SOCs) and network operations centers (NOCs) staffed with cybersecurity analysts that surveil supplemental threats and catch data anomalies are now commonplace.

The strongest approach to securing a business's assets is through **Security Fusion** – the unification of these siloed physical and cyber security systems that allows for the analysis of data, program design, team performance, and the monitoring of disparate systems. To provide maximum protection today for your people, assets, facilities, and brand, your cybersecurity (both IT and network security) and your physical security systems need to share data and communicate effectively.

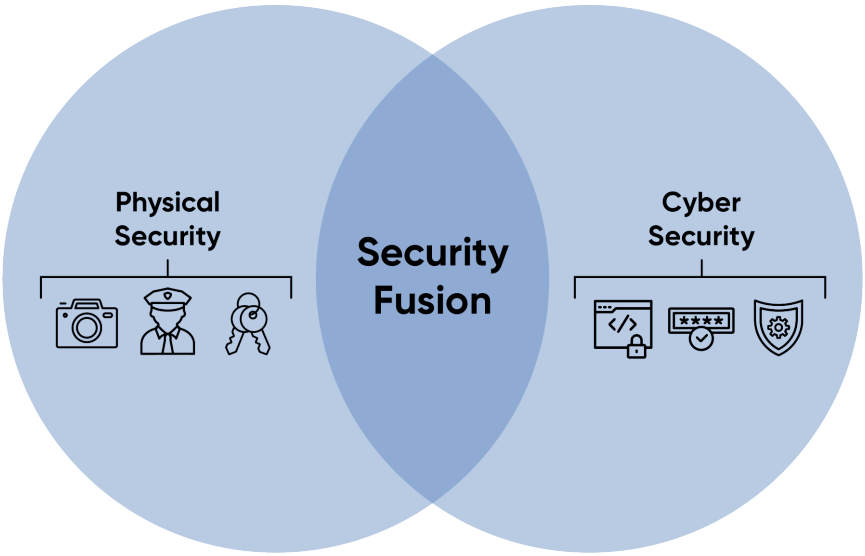
Consider a situation where someone uses a thumb drive to remove sensitive corporate data or intellectual property from a machine in a

company's facility. The data is an electronic asset, but the perpetrator of the attack breached the physical facility to orchestrate their attack and data exfiltration. Information from the facility's access control system should identify whose credentials were used to gain access to the premises. The corresponding video surveillance footage will detail the whereabouts of said person, or identify if it was a case of "tailgating," where someone walks in behind an employee with a credential. The same is true for an attacker that uses a thumb drive to maliciously or unintentionally install malware on a corporate system.

When organizations can use data from both their cyber and physical security systems together, they get better visibility into the anomalies that indicate malicious activity. This helps proactively improve detection because the anomalies create a signature that indicates suspicious activity, much in the same way early antivirus measures worked in cybersecurity.

Threats that crossover between the physical and cyber realms require a coordinated response. When you have visibility into data from both cyber and physical security systems, you are much better positioned to identify attacks like these and remediate them more quickly. This visibility is particularly effective against insider threats, because insiders are often able to evade some security measures, but cannot evade them all when they operate in sync.

Security Fusion requires that organizations bring all of their security teams to the same level. Today, it's likely your SOC and NOC are several levels ahead of the Global Security Operations Center (GSOC) your physical security team is running.



What does your organization's security look like today?

Your organization's cybersecurity strategy likely includes a NOC and a SOC. These two centers use different tools, but will have some amount of coordination and sharing of knowledge and data. They are often working together to some degree because the two teams likely roll up to the same executive leader, such as the CISO, CSO, or CIO.

The ever-changing nature of attacks and the increasing sophistication of attackers means cybersecurity is still very hard work. In recognition of this, the cybersecurity industry has shifted in recent years to increase its focus on quickly detecting and remediating attacks instead of a strategy of pure prevention. A strategy for cyberdefense designed around a NOC and SOC that share information and communicate doesn't mean an organization is airtight when it comes to its cybersecurity, but it does demonstrate a high level of maturity in the cybersecurity program. If your organization isn't at this point yet, it likely aspires to reach it soon.

When it comes to physical security, your organization likely already has a GSOC in place, or is working toward one. But even in large organizations with well-funded and thoughtfully designed physical and cybersecurity programs, the GSOC often remains disconnected from the SOC and NOC in terms of tools, data, and the leadership structure.

Physical security programs rarely generate the data and metrics that help determine the effectiveness of cybersecurity programs. It's more difficult to measure ROI for physical security, plan your spending, and plan for the future. Some organizations will increase their spend after an incident, for example. Other organizations will overspend in an effort to prevent an incident using the lack of an incident as their measure of ROI.

If this situation sounds familiar to you, then the first step your organization needs to take toward achieving security fusion is bringing your GSOC up to the same level of your NOC and SOC in terms of the tools at its disposal, the data it collects and analyzes, and its visibility into the various systems and facilities covered by your physical security program.

Your physical security program likely relies heavily on human guards, access control and video surveillance systems. The guards, however, rarely have access to data of any kind beyond security cameras. The access control data is likely disconnected from other sources of security data, such as those that feed into the SOC and NOC.

With a new paradigm of hybrid and remote work emerging today, a holistic view of security is more important than ever. Office environments

where the same people pass through at 9 and 5 every day are becoming increasingly rare. Your teams are likely distributed across geographies and faces aren't as familiar as they once were, thus exponentially increasing the complexity of both protecting the company and providing a duty of care to its employees.

To get a holistic view of your organization's security, you need visibility into the details around who takes actions and where they take place. Then you combine this information with data from your cybersecurity tools and paint a much more accurate picture of your threats and defenses.

Raise your physical security to your cyber standards

The future of security is fusion, but the current state is siloed. Technology leaders typically have physical security operations siloed because their legacy systems are out-dated. These systems are incapable of talking to each other and don't communicate with their cybersecurity and other corporate tools.

On the cyber side, many of the challenges around orchestration, behavioral analysis, and anomaly detection have been solved. Now it's time for forward-thinking organizations to bring their physical security up to this level and embrace fusion.

Visibility is essential to how the SOC and NOC work – both as independent entities and as partners. Together, they have visibility into network traffic and infrastructure. They can monitor access to applications and data. They can grant or remove access to networks and devices. Your Global Security Operations Center lacks this visibility. Each piece of your physical security program stands independent of the rest. A guard patrolling a facility, the data from the access control system, and the surveillance cameras are disconnected from one another.

It's time for a physical security strategy that orchestrates and analyzes data like you do in cybersecurity.

HiveWatch is a cloud-based platform that takes the data and orchestration commonly found in cybersecurity strategies and brings them to your physical security program. Like the tools used daily in the cyber realm, HiveWatch works to reduce the noise and make it easier to analyze threats and determine a response.

With HiveWatch, your business still owns its GSOC and builds and manages its physical security program. HiveWatch is added to your

existing GSOC to bring new capabilities and orchestration to the systems you already have in place. Your team of security analysts and experts remains in control, and because HiveWatch uses a cloud-native approach, your GSOC team can work from anywhere or in a traditional operations center.

With this level of information sharing and orchestration in place, HiveWatch can help correlate data and identify anomalies, such as when cyber tools identify an employee opening an electronic document in one location while physical security detects the employee who just accessed a building in a different location.

Businesses that are still in the process of building their GSOC and physical security program can outsource their monitoring with HiveWatch's vGSOC, a virtual outsourced GSOC. As their internal resources mature, these businesses can upgrade from the vGSOC to the HiveWatch Operating System software, and put their own team in charge of monitoring.

Today's threat landscape extends across the physical and cyber worlds. While businesses have invested heavily in their cyberdefenses and built out SOCs and NOCs with modern tools and data sharing, physical security is still far behind.

HiveWatch delivers the capabilities your GSOC needs to rise to the level of your cybersecurity strategy via the cloud, as part of your physical security program and with your team in control.

To learn more about HiveWatch, visit: hivewatch.com.