



Finding the Right Security Tech Stack to Fit Your Organization

If you're part of a physical security team that's already realized the importance of a security tech stack – congratulations – you're ahead of the curve.

The term “tech stack” refers to a way of visualizing how technologies are layered on top of one another to create a functioning solution. When used properly, a tech stack provides order when there seemingly is none, ensuring that each component interacts seamlessly with the next to deliver the desired outcome.

While some Google searches may deliver a more cyber-focused approach to security tech stacks, this ebook focuses on physical security, which encompasses the technologies and infrastructure designed to secure physical assets. It's meant to serve as a practical guide for organizations looking to implement effective measures that match their specific needs.

DEFINING THE SECURITY TECH STACK









Security Tech Stack (noun) / [si-kyoor-i-tee tek stak]

All the physical devices, infrastructure, and technologies leveraged by an organization to manage its entire security operation

"When designing a comprehensive protection plan for our new facility, we need to carefully evaluate our physical security tech stack to ensure it provides robust protection against unauthorized access, theft, and other relevant threats."

Every organization's security tech stack is unique, designed to meet specific security needs, operational goals, and regulatory requirements while reflecting the distinct challenges and priorities of the organization's environment.

Elements of a security tech stack are the everyday tools security teams use to monitor, manage, and respond to security incidents. Security tech stack elements may include, but are certainly not limited to:

-  **Perimeter protection:** Perimeter fencing, perimeter intrusion detection systems (PIDS), bollards, LiDAR/radar sensors, drones, manned security
-  **Access control:** Physical access control systems, personal identity and access management (PIAM) software, biometric readers, turnstiles, visitor management, mobile credentials, badging
-  **Video surveillance and monitoring:** Surveillance cameras, video management systems (VMS), recorders, video analytics
-  **Intrusion detection:** Alarm systems, panic buttons, motion sensors, glass break detectors
-  **Environmental monitoring:** Fire alarm control panels, smoke detectors, water sensors
-  **Communication:** Emergency notification systems, security information and event management (SIEM) software, smart mustering, dispatch systems
-  **Incident response and management:** Security operations centers (SOCs), incident reporting systems, crisis management software, open-source intelligence
-  **Maintenance and compliance:** Self audits, compliance management software, system health monitoring software, policies and procedures

The ordering of the physical security tech stack in this way (bottom up) reflects a logical progression from outermost defense layers to the uppermost policies that guide the implementation of each physical security layer. This ordered approach ensures that each component builds upon the previous one, creating layers of defense and response capabilities that collectively enhance the security posture of the facility.

FINDING THE RIGHT SECURITY TECH STACK FOR YOUR ORGANIZATION

Choosing the right security stack for your organization is similar to the hiring process. Each candidate must be evaluated by both the value they would bring to the organization as well as based upon the organization's current and future needs. You wouldn't hire a candidate solely based on their qualifications without considering how they fit into your team's dynamics and long-term goals. Similarly, selecting the tools to build your security tech stack solely based on their features without evaluating their compatibility with your organization's existing infrastructure could lead to an operational breakdown.

To help guide your decision making, ask yourself the following questions:

What kind of organization is this?

Start by identifying where your organization falls on the Compliance-Complexity matrix:

Organizations with **high complexity**, in their technologies, size, number of locations to secure, etc., are likely to result in a high number of manual security processes.

There may be automation tools present, but getting each technology in a complex environment to communicate with one another often requires manual data entry, resulting in increased administrative overhead and potential for errors. This can lead to operational inefficiencies and hinder the organization's ability to adapt swiftly to emerging threats. Enacting change within complex enterprises can also be challenging due to the segmentation of teams and facilities.

Highly complex organizations may benefit from a security tech stack that prioritizes integration, scalability, and identity management processes to reduce the administrative burden across multiple systems.

Organizations with **low complexity** may have the same number of layers in their security tech stack, but with far less endpoint devices.

Organizations with **low complexity** can focus on straightforward implementation of essential security measures such as access control, basic video surveillance, and intrusion detection. These solutions are typically easier to deploy, manage, and scale as the organization grows.

Enacting change within these organizations tends to be more straightforward, enabling quicker decision-making and the faster deployment of new tech.

Organizations with **high compliance** will rely largely on local, national, and industry regulations to build their security tech stack.

In highly compliant environments, technologies within each layer may already be predetermined, e.g., NDAA compliant cameras mandated within government buildings or the use of access control required within cannabis dispensaries.

While this limits an organization's flexibility, it also ensures adherence to legal and regulatory requirements, minimizing the risk of non-compliance penalties and legal challenges.

Organizations with **low compliance** may not be bound by many regulations, if any at all, increasing flexibility when choosing tech stack solutions.

In this case, organizations have the freedom to prioritize operational efficiency, cost-effectiveness, and specific security needs without the constraints imposed by regulatory requirements.

Conversely, organizations with low compliance may face challenges in establishing standardized security protocols across different locations. Without regulatory frameworks to guide their security tech stack choices, these organizations rely more heavily on internal policies to guide its security posture.

What risks are my organization is exposed to?

The most important thing an organization can do when building or making significant changes to their security tech stack is to conduct a risk assessment. Many organizations may ignore this step because of cost limitations, however, without a comprehensive risk assessment, you cannot accurately evaluate where you need to focus your security efforts.

If your industry faces specific risks to people or assets that are not adequately addressed by broad frameworks, a generalized application of controls may result in insufficient protection. For example, if you work in warehousing, dangerous machinery is often moving alongside personnel. In this case, your security tech stack will need to include technologies focused on protecting people in both designated walkways and operational zones.

Start by identifying your high-value assets most worth protecting and work backwards from there.

Your people likely come in at No. 1, so based on your known risks, what do they need protection from? That will look different depending on what type of organization you are. The risks facing today's warehouses are going to be much different than those facing today's schools.

Similarly, organizations with outposts in the Middle East and Asia face different concerns than those with a single North American outpost. During times of political unrest, government buildings and retail stores are a common target of public discontent. And vehicle ramming incidents seem to disproportionately affect airports, temporary events, and storefronts.

Building your security tech stack therefore requires a tailored approach that considers the unique risk profile of each environment and incorporates adaptable solutions to effectively mitigate those risks. And while it is not possible to anticipate a black swan event, such as COVID, organizations can make educated guesses about the risks they are facing. To do so, it takes the right balance of social listening, situational awareness, research, and strategic foresight.

Where is my organization today and where are we going?

Beyond analyzing your organization's risk factors, it's important to be honest about the current state of your organization. Consider:

Permanent infrastructure – Your organization may not be willing to invest in new technologies that don't integrate with its existing operating systems or those that can't be deployed in the cloud.



Geographic limitations – If you are working on a critical infrastructure site in a remote location where there is no access to high-speed internet, this will certainly limit the kinds of technologies you can deploy.

Lifecycle of current security tech stack – Perhaps your physical access control system is facing end of life. Or you just invested tens of thousands into a new video surveillance system with analytics at the edge. Before rushing to rip and replace or introduce new technologies, evaluate how you can extend the value of your existing investments by integrating them with upgraded solutions, enhancing their capabilities, or phasing them into a broader strategic plan.

Realistic level of investment – It seems obvious, but the scale and scope of your security tech stack will be largely influenced by your budget. E.g, is your organization more CapEx focused or OpEx focused? Understanding your financial constraints allows for prioritization of investments that deliver the greatest impact on security posture and operational efficiency.

Future state of the organization – For example, if you plan on adding new locations, you will want to ensure that your security tech stack was built with scalability in mind. What's more, you will want to think about the effect your security tech stack will have on your organization. Many organizations today push for a security tech stack that is fully on the cloud. But while the cloud offers lots of benefits, a fully cloud operation will have a large draw on your internet connection, potentially limiting solutions' efficacy and degrading the performance of other systems.

What does the rest of my organization need?

You and your team won't be the only stakeholders when it comes to your organization's security tech stack. Be sure to consult the following departments prior to making an investment in new security technologies:

Information Technology: Given the cohabitation of cybersecurity and physical security, it is essential to ensure that new security technologies align with existing IT infrastructure, cybersecurity policies, and data protection measures.

Consulting with your organization's IT team early in the tech stack building process ensures a holistic approach. One that not only integrates physical and digital defenses but also promotes cybersecurity across all systems to minimize vulnerabilities.

Will the solution be deployed on cloud, on premises, or a hybrid? Has the proposed application undergone penetration testing? Be prepared to answer such questions and work with your IT team to ensure your physical security tools don't become a cybersecurity risk.

Legal: Consulting with your legal department is especially critical within highly compliant organizations. Your legal team will need confirmation and documentation that all deployed solutions follow the applicable regulatory and industry requirements.

The good news? They also have an appetite for solutions that decrease your organization's liability in the event of an accident and will likely advocate for products that detect and deter such incidents.

Human Resources: Your HR team has a lot to gain and a lot to lose when it comes to physical

security. HR teams will concern themselves with privacy policies and the user experience provided by your security tech stack. But, when done right, physical security technologies can also introduce automation into existing workflows, in turn reducing the number of manual tasks that tend to overburden employees.

This then allows HR teams to reallocate labor resources to more strategic roles. For example, a visitor management system can enhance efficiency at reception, allowing staff to focus on delivering exceptional customer service. A security revolving door equipped with access control and installed at an employee only entrance can similarly allow guards to focus on more mission-critical tasks.

Consulting with other internal departments when building your security tech stack also increases organizational buy-in.

Gaining buy-in from other departments will not only increase compliance with any existing policies but also introduces opportunities to transform security from a cost center into a value driver.

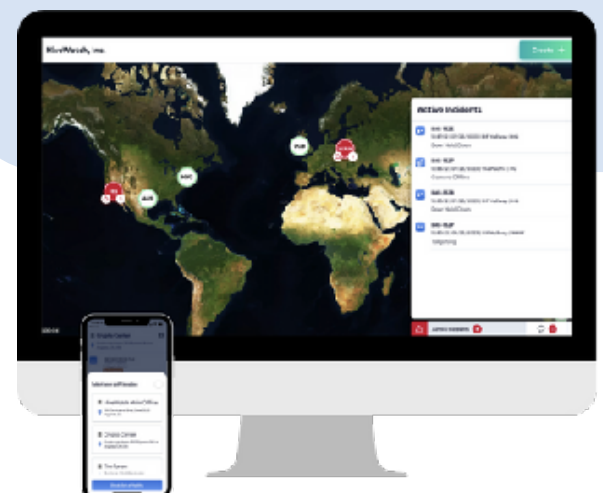
Look for solutions that offer additional business intelligence to increase buy in from other departments. For example, your facilities management team would love to use the data provided by your access control system to gain insights into building occupancy and usage. Your marketing team may benefit from video analytics that provide heat mapping or line crossing.

These insights can enhance operational efficiency and decision-making across departments, demonstrating the broader organizational benefits of integrated security solutions beyond their traditional security functions.

QUESTIONS TO ASK YOUR VENDOR

Your diligence and inquiry sets the tone for the deployment of your security tech stack.

- Can you please provide your license, insurance, and qualifications?
- What are other companies like mine doing?
- What solutions can you recommend that have been tried and trusted?
- Why do you and other customers like about this recommended solution?
- How well does this solution communicate and integrate with others?
- How does this solution integrate (what are the shared attributes, what data does it utilize, etc.)?
- What can I expect of the post-installation experience and who should I contact for troubleshooting?
- Can you provide any referrals for me to speak with?





3 TIPS TO MAKE A “GOOD” SECURITY TECH STACK GREAT

- 1. Listen to the people who use it** – Getting feedback from those actually using the technologies in your security tech stack provides valuable insights into potential issues, areas for improvement, and practical challenges. This is especially critical in areas of high turnover, ensuring every team member is not only actively utilizing the tools you are providing, but doing so to its fullest capabilities.
- 2. Don't buy a solution for every pain point** – If there is a problem, install something to solve it. This seems like pretty sound logic; but if you buy a point solution to solve every security problem you are having, the management of all this technology becomes overwhelming. Not only from a cost and administrative perspective, but from a cybersecurity perspective too. More endpoint devices create even more vulnerabilities in your network. You can actually solve many security problems at once if you...
- 3. Consolidate your security tech stack** – Every technology you add to your portfolio expands your security tech stack, but as mentioned, can lead to increased headaches. When you consolidate your tech stack, you both limit your deployments while also implementing a single source of truth. Imagine being able to manage your entire security tech stack – from access control, to surveillance, sensors, incident reporting, compliance, and beyond – in just a few clicks.

CONSOLIDATE YOUR SECURITY TECH STACK WITH HIVEWATCH

In the hierarchy of your security tech stack, HiveWatch lives at the top.

Think of HiveWatch as a UFO, beaming up all the data from all your various security technologies and consolidating it into easily digestible outputs. **With HiveWatch, it's possible to go from managing upwards of 20 technologies down to just 2-3. Deploy guards and field resources, remotely dial 911, track incidents, store all standard operating procedures, correlate access and video events, and so much more – all from one platform.**

In one instance, a large global financial firm was facing significant challenges with its outdated, on-premises access control system. Frustrated with its limitations and inefficiencies, the firm considered ripping out the existing system and investing \$10 million in a complex overhaul that would involve multiple new tools for access control, visitor management, and surveillance. The plan included replacing their existing cameras and expanding their tech stack by six different solutions. However, this approach risked creating additional complexity and escalating costs.

HiveWatch stepped in to assess the situation and proposed a more cost-effective and streamlined solution. By updating the existing access control system to the latest version, the firm could leverage enhanced features and capabilities that addressed many of their concerns without a complete overhaul. From there, the HiveWatch solution was implemented to bring the existing access control, video, and new visitor management solution together to be managed under one platform. This approach preserved the existing infrastructure while significantly reducing costs and complexity.

To put it simply: HiveWatch provides you with an easy-to-use, end-to-end tech stack that's equipped with the security management tools you need without the additional overhead.



Ready to see it in action? Request a demo at hivewatch.com/demo



HiveWatch