



Your Guide to Building a Scalable Security Program



Your Guide to Building a Scalable Security Program

Security manufacturers throw around the term “scalable” a lot these days, but few dive into what scalable really means for modern organizations and their security programs.

As leaders oversee organizational change, growth, and in some cases, shrinkage, implementing a flexible strategy will become critically important.

This eBook discusses how physical security teams can address the scalability problem across their organization, answering questions like:

- What do we mean by “scalable”?
- What strategies are included in building a program that’s truly scalable?
- How should a security team approach growth?
- What technology considerations must be considered?
- How can teams work together to leverage technology and reach scale?

What Do We Mean by “Scalable”?

It’s not enough to create a “fix it and forget it” security program. Not only do the needs of the organizations shift, but growth (or even shrink) is inevitable.

“Scalable” refers to the capability of a system, process, or technology to handle growth or increased demand without compromising performance, efficiency, or quality. To put it simply, scalability refers to the ability of a solution to expand or adapt to accommodate larger workloads, higher volumes of data, or increased complexity without requiring significant changes to its underlying architecture or design.

As we define scalability further, a few characteristics become important:

Flexibility. Scalable solutions are designed to be flexible and adaptable, allowing them to accommodate changes in requirements, resources, or usage patterns over time. Security teams see fluctuations not only in the amount of incidents they handle, but also in budget,

technology acquisition, and staffing levels, which requires flexibility across all facets of the program.

Efficiency. Scalable security systems are efficient in using resources such as available data or technology, to identify areas of excessive resource usage or waste in an effort to meet growing demands.

Reliability. Scalable security solutions maintain high levels of reliability and availability, ensuring consistent performance and service delivery even under increasing data load or incident levels.

Manageability. Scalable security solutions are manageable and easy to adopt across the program, allowing for seamless deployment, monitoring, and maintenance across large or distributed environments.

Cost-effectiveness. Scalable security enables organizations to optimize resource allocation and minimize costs associated with scaling a program, creating value for the organization, and minimizing the additional investments in accounting for growth and expansion.

Building a security program with scalability in mind is a critical consideration in the design and implementation of systems, processes, and technologies to ensure they can effectively meet the evolving needs and challenges of businesses and organizations.

How to Approach Growth

For many security leaders, growth has a trickle-down effect. Expansion through mergers and acquisition or organic growth, in addition to decreases in facility or employee count, directly impacts the security program. Whether it's an increase or decrease in size, workload, or scope, these leaders must be prepared to adapt their strategies and approaches to efficiently manage security risks while maintaining operational efficiency.

Here are some ways security leaders can approach growth:

- **Assess the here and now:** Begin by looking at the current state of your security program, including the resources, capabilities, processes, and technology infrastructure. Understanding existing strengths, weaknesses, and areas for improvement can help inform planning for the future.
- **Align with the business:** This might be one of the most important considerations to make, but ensuring security leaders understand the organization's growth objectives, priorities, and risk tolerance levels is critical to the success of a security program. The most successful security leaders will be able to align security strategies with business goals to ensure security investments and planning are enabling the company's growth initiatives.

- **Invest in scalable solutions:** It goes without saying in an ebook about scalability but we thought we'd spell it out here: Invest in solutions that offer flexibility and can adapt to the changing needs of the organization. Closed systems that aren't able to integrate fully with new technologies will severely limit the security team's ability to seamlessly manage the security portfolio.
- **Optimize processes:** Reviewing security processes and workflows – or investing in a platform that can streamline this for you – can improve efficiency and effectiveness for your security team. Identifying opportunities for automation and standardization can allow for scaling as business needs change.
- **Collaborate across departments:** Preparing for growth initiatives requires extensive communication across departments, including leadership teams, human resources, legal, IT, facilities, and many other stakeholders ensure that security priorities, challenges, and requirements are effectively communicated and integrated.

Adopting these approaches helps put security teams in the driver's seat, effectively managing periods of growth and change without compromising the safety and security of the organization.

Technology Considerations

As security leaders navigate investments in new technologies that achieve some of the approaches listed above, such as aligning strategy with business goals, optimizing processes, and cross-departmental collaboration, there are several considerations to make.

1. **Take a look at how technology can support (or even hinder) future growth.** For example, when making a buying decision around access control systems, security leaders have to consider the number of users, number of credentials, server requirements, facilities, hardware end points, and software features. As these items are being addressed in an RFP or in conversations with a vendor, security leaders must ask themselves, "Is there a scenario where my program will outgrow the system's capabilities in any of these areas?" If so, the answer might be to select a different solution.
2. **Security leaders must consider interoperability.** We talk a little about this above, but the importance here cannot be overstated: integration is key. The ability to leverage multiple point solutions, such as access control systems and video surveillance cameras – regardless of manufacturer – provides growing companies with the ability to scale quickly and more efficiently than ever before. Centralizing the ability to pull these

solutions into a single security operations management platform allows security leaders a better view of their security programs in a current – and even future – state.

3. **Cloud-based solutions can provide the ultimate scalability factor**, providing flexibility and accessibility advantages compared to traditional on-premise systems. Cloud-based, or Software-as-a-Service (SaaS) platforms, can easily scale up or down based on changing needs, accommodate distributed environments, and provide remote access and management capabilities, making them well-suited for scalable physical security deployments.
4. **Data-driven insights and analytics can drive decision-making beyond security**, making technology investments that provide these critical. Automated workflows, event-triggered alerts, and AI-driven analytics can streamline security processes, improve threat detection capabilities, and reduce manual intervention, enabling security teams to manage larger environments more efficiently.
5. **Centralized management of technology investments can create cohesion for security teams**. Centralized management and monitoring of physical security systems across multiple locations or facilities enables personnel to efficiently oversee and control security operations, access controls, and incident response activities. Being able to manage security in a single platform provides security leaders with the ability to assess staffing levels, streamline training, allocate resources effectively, and scale to additional sites and/or solutions as needed.

Achieving true scalability, or “expandable with a purpose,” takes planning and coordination from security leaders alongside the broader organization.

How Your Organization Can Scale with HiveWatch

The **HiveWatch® GSOC Operating System** allows security teams to bring together information, data, and technologies into a single platform, orchestrating existing security programs, leveraging intelligence, automation, and predictive threats that improve overall security posture, reduces noise and complexity, and delivers more intelligence across the organization.

HiveWatch was purpose-built to address the security industry’s scalability problem and does so in a few ways:

1. **Brings together disparate systems.** Security teams are able to bring together their disparate systems into a single security operations management platform. There is no need to rip-and-replace old systems as you acquire additional buildings, locations, or businesses with legacy hardware.
2. **Reduces false alarms.** Security professionals know, the more sensors you have, the more (false) alarms that will alert. As organizations scale, their noise only becomes worse. HiveWatch analyzes your data to determine the most accurate and productive path forward, layered with machine learning to dedupe excess noise.
3. **Stores security assets.** As programs scale, so do the floorplans, standard operating procedures (SOPs), and site information. With HiveWatch, everything is stored digitally and is only a click away – keeping everything in an easily accessible location that can be globally updated quickly when needed.
4. **Can be the right solution for you from the beginning.** Not all organizations are ready for the commitment of a full solution such as the HiveWatch® GSOC OS. This is why Command Center was created. The HiveWatch® Command Center assists the security team in detecting, triaging, responding, and investigating security incidents, while offering a scalable option for organizations as they grow.

The Command Center streamlines field resource-to-operator communications, centralizes the storage of standard operating procedures, optimizes incident workflow, and aids in incident management and response. While the Command Center doesn't ingest access control incidents or video feeds, it does allow security teams to leverage a cohesive vision for the program, enabling better communication with field resources and emergency services.

As organizations identify the need to gather more data about incidents using access control, video, and other intelligent sensors, Command Center customers can easily scale to the HiveWatch® GSOC OS.