AVIGILON™

HOW CLOUD-NATIVE SOLUTIONS CAN ENHANCE PHYSICAL SECURITY AND CYBERSECURITY CONVERGENCE

with Avigilon Alta Cloud Security

MOTOROLA SOLUTIONS

Security Convergence Overview

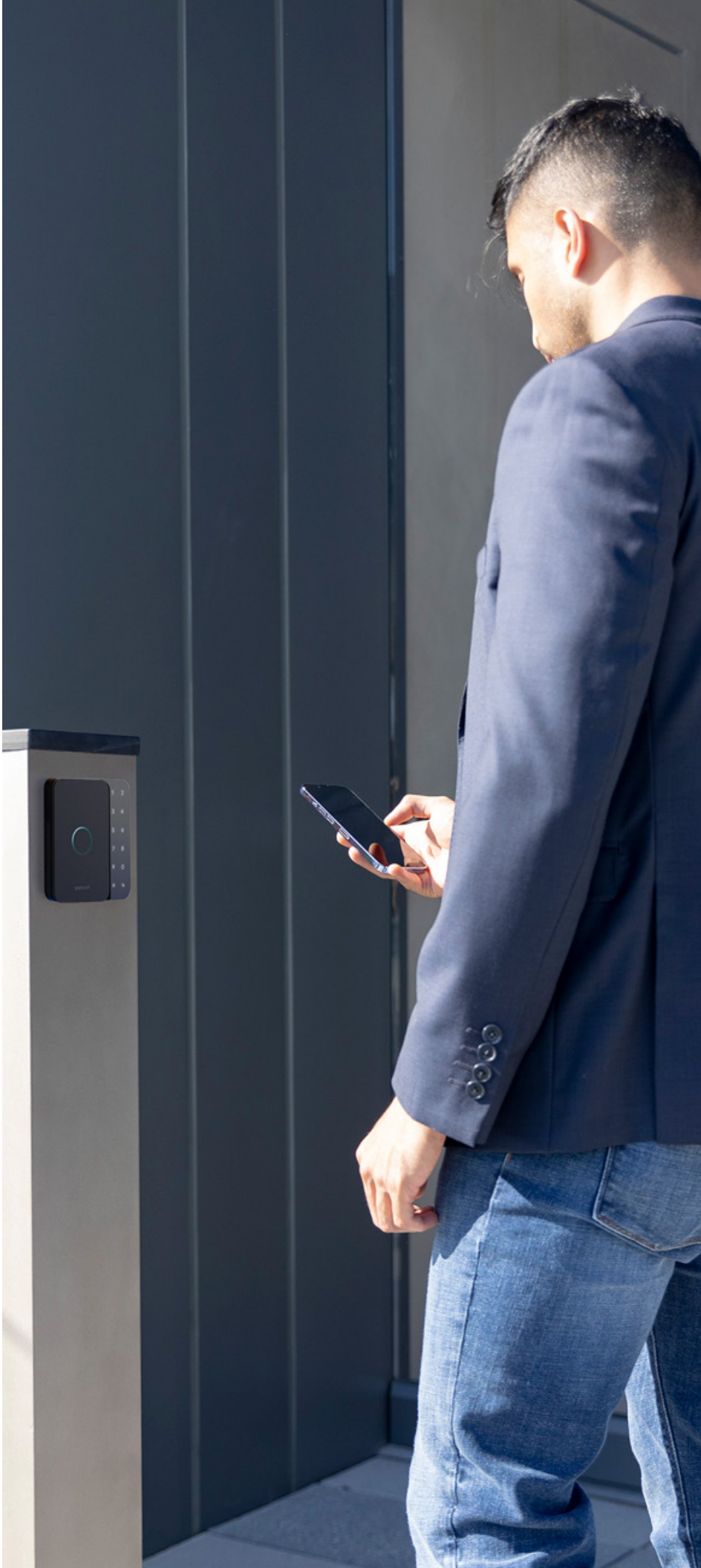
In security, two areas that traditionally served distinctly different sectors, physical security and cybersecurity, are now merging at a fast rate. What used to be a squarely physical security responsibility or risk now affects cybersecurity, and the reverse is also true. A compromised physical security system can be used as an attack vector for an organization's cybersecurity; cybersecurity vulnerabilities can be exploited by bad actors and used to take over a physical security system. As the lines between the two continue to blur, organizations that keep these areas separate will have a harder time ensuring overall security.

On the other hand, organizations that take a holistic approach to security by converging these two areas can create a powerful, unified system that works seamlessly to fortify security on all fronts and provide a complete view of security operations. This guide will cover the differences between cybersecurity and physical security, the importance of converged security, and provide best practices and tools to streamline management and optimize both physical security and cybersecurity.

Physical security versus cybersecurity

Physical security refers to the measures put in place to safeguard an organization's physical assets, including the building, equipment and people. The most common example of protecting a physical asset is guarding a building from unauthorized access. This can be accomplished by a combination of methods, including installing proximity readers, alarms and cameras at entry points to ensure that every individual entering the building has proper authorization and deter unauthorized individuals from attempting to gain entry.

Cybersecurity, on the other hand, is the integration of technologies to protect computer systems and networks from digital attacks orchestrated by hackers and cybercriminals. In a digital world, it is crucial to have measures to protect confidential information and sensitive data, as breaches in this area can disrupt business operations on a massive scale.



Why security convergence matters

The adoption and integration of the Internet of Things (IoT), including things like IP cameras and connected sensors, means that physical systems and networks are becoming increasingly interconnected. The once separate functions of physical security and cybersecurity are separate no more. In an IoT-connected organization, a cyber attack that exploits a weakness in network security could be used to access and gain control of a physical security system. Conversely, attackers can exploit blind spots in a physical security system to enter a building and access an organization's network systems from the inside.

When cybersecurity and physical security operate separately, the lack of a comprehensive security view can leave organizations blind to the signs of a cyber attack or a security threat. As a result, attacks and breaches are more likely to occur and continue longer before being detected. This can lead to severe consequences, such as exposing confidential information, financial damages and disruption of business operations. In some cases, cyber attacks may lead to critical services being denied to people who need them most.

To build a successful security convergence strategy, an organization should begin by implementing measures to limit access to physical spaces and put cybersecurity tools in place to restrict access to sensitive information. Physical security guards the space where sensitive data is stored by restricting physical access; cybersecurity protects data kept in physical systems.

Some physical security components, such as RFID door locks for commercial use and video cameras, are common targets for both cyber attacks and physical security breaches. The right security convergence measures can prevent hackers from accessing these channels through the internet and prevent unauthorized individuals from entering a building with stolen credentials or stealing readers to access stored data.

Best practices for converged security

There is a lot of commonality between physical security and cybersecurity tasks: intrusion prevention, threat prevention, access management, fixing vulnerabilities and responding to incidents. Though each team's responsibilities for the above areas may look a little different, a converged security strategy requires both physical security and cybersecurity to work together seamlessly.

	CYBERSECURITY	PHYSICAL SECURITY
Intrusion prevention	Firewalls and encryption	Doors, turnstiles, guards
Threat detection	Networking monitoring	Video and access alerts, alarms, active monitoring
Access Management	Locks, readers	Multi-factor authentication, passwords
Fixing Vulnerabilities	Patch management, software updates	Hardware and software updates
Responding to incidents	Reporting and system audit logs	Reviewing video or access events, dispatching security personnel

The following best practices can help ensure a holistic security approach, ensuring both systems work together for a more comprehensive security view.

- Control access to physical spaces. Install access control readers, security cameras and physical security measures for all areas where sensitive data, proprietary information and intellectual property are stored. Installing these systems will also prevent unauthorized users from entering a building or gaining access to high-security areas.
- Harden and secure your physical security systems, following best practices for cybersecurity. This includes using multi-factor authentication (MFA) for users accessing the system, adhering to the principle of least privilege, ensuring systems software and firmware are kept up-to-date, active system monitoring and threat detection, and regular vulnerability testing.
- Set up a collaborative structure for your organization's security teams and IT experts to work together. This is crucial when training security teams to employ the right technology and for IT teams to ensure that converged systems run smoothly.
- Create an open communication system to encourage teams to collaborate and share information from their departments. Implementing the findings from these discussions can help facilitate convergence and strengthen overall security.
- Analyze data collected from converged systems to get a comprehensive view of security across your organization. Compiled data can provide a broader view of areas outside of security, such as business operations. For example, a visitor management system can detect patterns in the flow of visitors, and cameras can count people and analyze motion in an area. If an organization finds that there is heavy traffic in certain areas of an office or if the number of visitors is causing congestion, it may consider moving to a larger space.

Security convergence allows teams within an organization to quickly assess threats and respond accordingly to incidents. Irregularities can be spotted sooner, and teams have the complete picture of the information needed to respond immediately.

Benefits of the cloud for physical security and cybersecurity

Cloud-native solutions are one of the best ways to employ a converged security strategy, strengthening both physical security and cybersecurity. Cloud solutions streamline management, are highly flexible, scalable and can reduce operating expenditures.

Streamlined remote visibility and control

Today's distributed sites and hybrid workforces are driving the increase in cloud adoption. The increased flexibility in the workplace requires that cybersecurity and physical security systems provide more versatility without compromising safety. Cloud security systems allow organizations to streamline processes and manage security remotely.

With cloud systems, operators are able to grant or revoke access,

manage door access control schedules, issue guest access passes and adjust permissions from anywhere, at any time, and for multiple locations and sites. They allow security teams to observe video footage in real-time, arm or disarm alarm systems and oversee cyber activities.

Future-proof security

Yesterday's security systems can't be expected to meet today's security needs, much less address future requirements, unless they are continuously updated and managed. Many on-premises solutions require manual software and firmware updates and patches to maintain system security. Adding new features to address new use cases may require significant system changes. Best-in-class cloud-native solutions offer automatic over-the-air updates for firmware updates and new features. This improves operations and increases security, providing access to the latest technologies without in-person maintenance or disrupting work during business hours to update systems.

Seamless integrations for more comprehensive security

Systems working in silos are counterproductive to convergence. The best security happens when you have complete visibility to understand and assess threats and respond quickly. Cloud systems like Avigilon Alta have open API architectures, facilitating seamless integrations of video and access control with cybersecurity systems and other cloud software into one platform to provide converged security.

Infinite scalability

A cloud system is scalable and allows organizations to scale up or back, depending on their needs. Because new users, locations and sites can be added to a deployment with just a few clicks, purchase decisions can be made based on current needs as organizations that the system can grow with them. On-premise systems may require additional space to house new servers and specific software to be installed on local workstations. In contrast, cloud solutions rely on hosted services and web-based access to eliminate this hassle.

Reduced expenses

Security incidents can occur anytime, so security is a 24/7 job. Cloud systems make it easier to monitor security around the clock without needing dedicated security personnel present at a dedicated, on-site workstation or working after hours, reducing the cost of hiring extra staff while ensuring that security continues. Intelligent cloud systems can provide real-time alerts of abnormal behavior or anomalies, alerting teams to potential threats and allowing them to respond quickly from anywhere. Cloud security systems also enable easy, centralized monitoring across sites from one location if 24/7 monitoring is required.

Cloud solutions can also reduce costs by eliminating the purchase of some hardware and software by eliminating the need for on-site servers and custom software. Cloud systems offer hosted services so that security can be managed from a web browser or app. Expenses are shifted from capex to opex and spread out over time with the subscription models.

Convergence with security as a service (SECaaS)

Converged security requires a new organizational structure. A security as a service (SECaaS) provider can help simplify the process of streamlining management and maintaining both physical security and cybersecurity systems.

SECaaS providers allow organizations to outsource management of certain aspects of their security. The traditional method of managing security is challenging, requiring dedicated teams, specialized knowledge and continual investment in hardware and software, as well as time and resources to maintain systems. SECaaS solutions allow organizations to integrate systems into their infrastructure on a subscription basis, making it more cost-effective and ensuring it's always up-to-date. This streamlines management and improves efficiency while reducing expenses. Some SECaaS providers also offer managed services, which allows organizations to outsource system management responsibilities.

Physical security as a service (PSaaS) also falls under the security as a service umbrella. With PSaaS solutions, like the Avigilon Alta Cloud Security Suite, organizations can manage tools such as access control and video surveillance in the cloud. Security teams can manage door schedules, grant or revoke access, unlock doors remotely. They can view video, receive and respond to alerts, and investigate incidents via a web dashboard or mobile app. Like some SECaaS providers, PSaaS providers may also offer the option to outsource services, such as monitoring video, relieving internal teams of the responsibility.

Cloud security is the key to convergence

As the security landscape continues to evolve, convergence is only going to become more important for organizations looking to ensure the safety and security of their people, buildings, assets and data. Cloud-native solutions provide organizations of all sizes with a way to seamlessly unify their physical security and cybersecurity practices, providing a stronger, more comprehensive security solution while improving flexibility, scalability and operations while reducing costs.

Visit avigilon.com/alta to discover how the Avigilon Alta Cloud Security Suite can help take your organization's security to the next level.

To learn more, visit:
www.avigilon.com

MOTOROLA SOLUTIONS

AVIGILON™