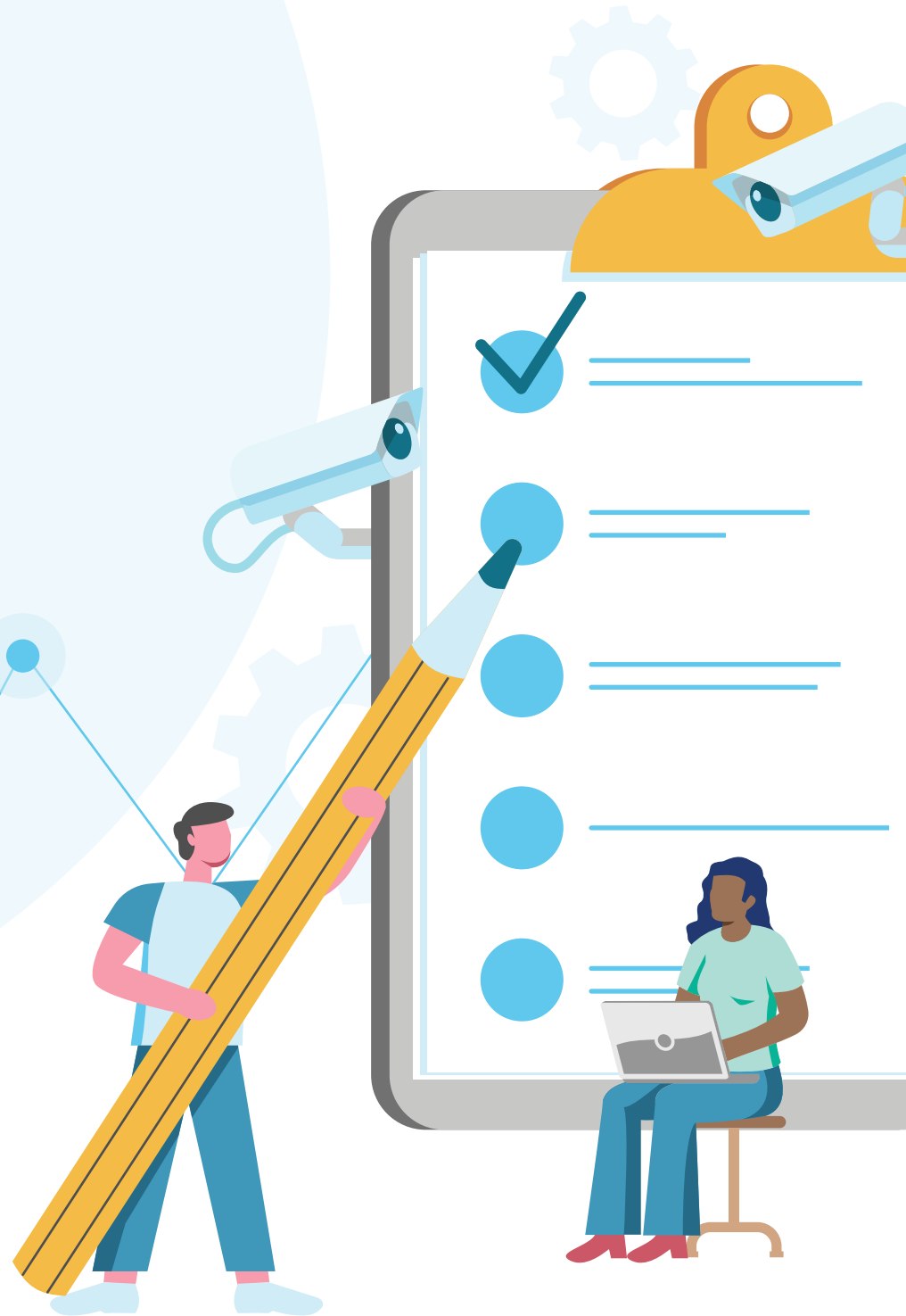


The Guide to Enterprise-Ready Physical Security

Optimizing the availability, cyber security, cost-efficiency and compliance of physical security devices



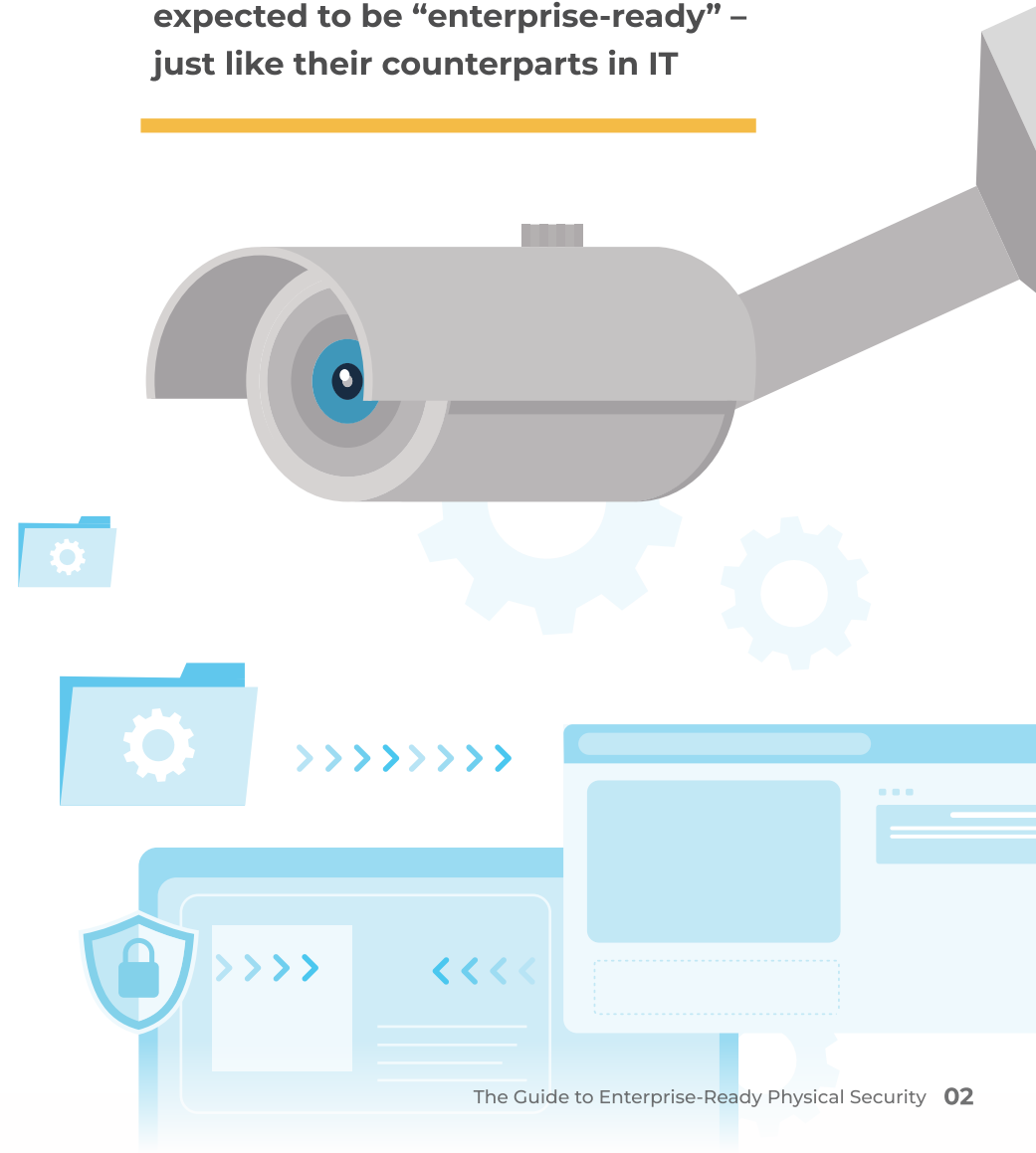
In a Digital World, Enterprise-Readiness is a Must

The physical security space today is largely dominated by IP-based devices, as the industry has shifted away from analog systems over the past several decades. These digital devices and systems are in many ways far superior to their analog predecessors, and physical security teams find themselves spoiled for choice with a vast, growing selection of advanced surveillance and access control systems, intercoms, alarms and other technologies like shooter detection, emergency power supplies and more.

But this new reality has also generated new, complex challenges. Today's connected physical security ecosystem is **inextricably linked to IT**, which in turn brings physical security under much greater scrutiny from both IT themselves, as well as from external auditors and other stakeholders. In fact, physical security is increasingly expected to be “enterprise-ready” – just like their counterparts in IT. This means physical security departments are increasingly held to IT standards and best practices, which in turn also places pressure on vendors to ensure their products are fully compliant.

In this guide we provide a checklist for all relevant parties – from the enterprises themselves, to the device manufacturers and management system vendors – as a framework to reaching an “enterprise-ready” state.

Physical security is increasingly expected to be “enterprise-ready” – just like their counterparts in IT



Why “Enterprise-Ready” Physical Security is so Crucial

Before we delve into how physical security can become enterprise-ready, it's important to establish why it is so important from a wider business perspective – and what exactly is at stake for organizations that aren't enterprise-ready. In general, there are five areas in which enterprise-readiness is critical for physical security:



Availability



Cyber Security



Compliance



Cost-Efficiency



Future Planning



Availability

Ensuring device availability is the most critical challenge for any physical security team – and particularly difficult with large, varied fleets of devices, especially when spread over large areas. This challenge is even more complex with IP-based devices, given the wider variety of potential causes of unavailability: from a physical problem with the device, to an interrupted connection with a management system, to network-related issues.

An enterprise-ready physical security device must be able to avoid downtime as much as possible. When a device does become unavailable, the relevant people must be alerted in real time, be able to rapidly identify the root cause, and take the necessary steps to fix it.



Cyber Security

Cyber security is quickly becoming a major concern for physical security teams. IP devices are often an easy target for cyber criminals – and once a malicious actor breaches a device, they can gain access to the entire network and cause untold damage. The [average cost](#) of a data breach is \$4.35 million (and rising), but a hack can also seriously damage a brand, undermine customer confidence, and have severe legal repercussions.

To ensure the enterprise-readiness of their devices, physical security teams must have visibility into the current cyber threat landscape, as well as into potential vulnerabilities in their devices and systems, and the means to harden their devices against those threats.



Compliance

Physical security teams are increasingly expected to comply with IT standards. These compliance requirements can be set both internally by the company, or by external auditors as per local or government regulations. In recent years, physical security teams across all industries have faced increased scrutiny, amid pressure to comply with government and international standards.

To be enterprise-ready, physical security teams must be able to ensure their devices and systems are fully compliant. This includes having visibility into the compliance status of all devices and the ability to correct any compliance issues – while also having the means to easily pull the necessary data for external auditors.



Cost-Efficiency

Despite their critical role, physical security is typically seen as a cost-center, which also requires the involvement of multiple internal teams and third parties. This makes cost-efficiency a key priority. Yet as physical security battles to keep up with the increased frequency, sophistication and cost of physical and cyber threats, all too often they find their precious budgets drained by endless break-fix cycles and other costly, avoidable maintenance tasks.


To be enterprise-ready, physical security teams need devices that enable them to work cost-effectively, and avoid wasting their budgets on preventable maintenance costs such as costly truck rolls.



Future Planning

Strategic planning is a critical ingredient for any enterprise-ready organization. One common example of this for physical security teams, that means planning when to replace outdated and unsupported devices before they reach their end-of-life (EOL) and pose serious cyber security and compliance issues. Yet EOL planning is incredibly difficult and ultimately unscalable, as teams must manually crosscheck EOL across multiple device types, manufacturers and models.

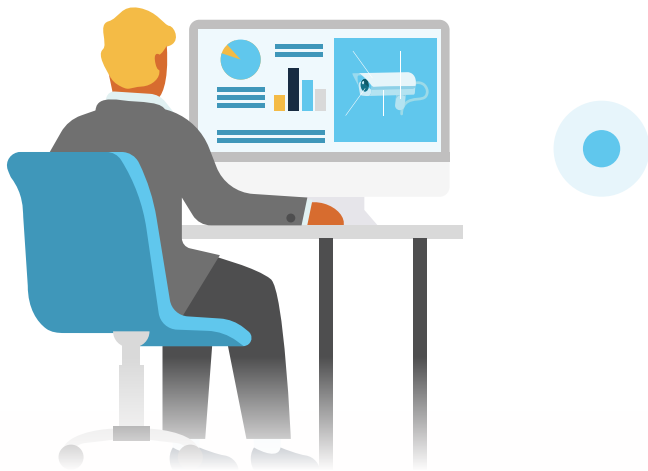
To be enterprise-ready, physical security teams must have visibility into the lifecycle of all their devices – across all device types and manufacturers – so they can effectively conduct future-planning and ensure their fleets of devices are always supported.



The Checklist for Enterprise-Ready Physical Security Devices

So what are the technical requirements for a physical security system to be “enterprise-ready”?

Based on our extensive work with IT and physical security professionals, as well as with leading device manufacturers, we’ve compiled a checklist of 8 requirements for physical security to reach an enterprise-ready state. We’ve made this list as practical as possible, by prescribing specific technical criteria you can implement right now.



#1 Operational Asset Mapping

To be enterprise-ready, critical device information must be readily accessible for monitoring, e.g. model, firmware version, serial number, end-of-life, warranty.

The ability to discover and add devices to management systems is the most basic criteria for managing and monitoring connected devices, as well as enabling cross-department collaboration. IT organizations possess countless tools for this, but for IoT devices – particularly in the physical security space – such capabilities are far less widely available.

#2 Configuration Hardening

To be enterprise-ready, it is critical to identify specific attack surfaces of the device or system and address any vulnerabilities in advance, and close off potential entry points to malicious actors, e.g. closing FTP access, shutting down unnecessary discovery protocols (Bonjour, UPNP).

Most physical security devices are not sufficiently hardened out-of-the-box against cyber attacks. Devices often don’t fully support the proper networking configuration requirements, come with weak default passwords, and possess other vulnerabilities.



#3 Health and Performance Monitoring

To be enterprise-ready, important performance data must be readily accessible for monitoring, e.g. Network utilization, recording status, PoE consumption.

IoT devices must be carefully monitored to ensure they have the resources to perform their tasks at any given time. This requires both real time access for ad hoc monitoring, as well as more advanced tracking and alert capabilities.



#4 User and Password Management

To be enterprise-ready, remote and automated management of users and passwords must be possible in order to enable critical tasks such as defining access and permissions, password rotation, rollback, and more.

The ability to remotely manage users and passwords is key to securing IoT devices. In physical security organizations, the ability to remotely add users, manage permissions, and rotate (and rollback) passwords in accordance with accepted IT standards is particularly critical, as these tasks are usually unscalable and therefore commonly neglected – leaving devices vulnerable.

#5 Remote Firmware Upgrade

To be enterprise-ready, physical security must have visibility into firmware versions across devices, when new versions are available, ensure compatibility with management systems and the ability to remotely update devices in bulk.

Each physical security device comes with its manufacturer's Operating System (OS), which must be regularly updated for optimal functionality, security and compliance. But as physical security teams lack the robust, established management tools used by IT to define when and how to deploy OS updates, these upgrades can only be carried out manually – which is unscalable.

#6 Certificate Management

To be enterprise-ready, devices should enable remote management of SSL and 802.1x certificates to ensure compliance and improve the cyber security posture of the devices.

Both physical security devices and their respective management systems typically include a built-in web server allowing to connect and communicate with them and between them. Best practice is to use both SSL and 802.1x for better network security – using default self-signed SSL certificates is not secure.

#7 Cyber Security (Detection & Protection)

To be enterprise-ready, physical security needs visibility into known firmware vulnerabilities, malicious processes, suspicious network connections and more, as well the means to manage vulnerabilities and mitigate potential attacks.

Cyber threats are constantly evolving, and physical security devices must be protected against new and emerging threats. Beyond initial Configuration Hardening (#2), devices must further reduce security risks by looking at the specific attack surfaces of the device or system to identify new threats and vulnerabilities, and closing any potential entry points to potential attackers.

#8 Detailed Log Collection

To be enterprise-ready, physical security teams need access to log information from each device for further analysis and investigation, and should be able to share this data with other relevant stakeholders.

Device system logs need to be reviewed for audit purposes (e.g. showing which user performed what actions on a device), as well as for technical diagnostics. In many cases, these logs are also utilized by other systems and tools for important purposes, including cyber security.

Unlock The Full Potential of Your Physical Security Investments

It's clear that enterprise readiness is the call of the hour – for end users and manufacturers alike.

Physical security teams who implement these steps will be well on their way to building reliable, secure compliant and cost efficient security systems. At the same time, they will empower themselves to stop putting out fires and take a more strategic, long-term view – maximizing their technology spend and effectively planning for the future. And of course, manufacturers who enable them to succeed will place themselves at the forefront of the market and gain a competitive edge.

About SecuriThings

Founded by leading security and IoT experts, SecuriThings empowers physical security teams and IT professionals to automate the operational management of physical security devices, while also ensuring full compliance and security within their organization. SecuriThings is trusted by Fortune 100 companies and is used by large enterprises such as technology companies, financial institutions, manufacturing companies, major airports, universities, hospitals and more. SecuriThings partners with key systems integrators and device manufacturers to provide unmatched insights, coverage and reliability.

For more information, please contact us at info@securithings.com.

www.securethings.com

