SECURITHINGS

# The Guide to Automating Physical Security Device Management

The Challenges and Opportunities of
Automation in Physical Security

# Automation is Inevitable

As organizations move towards digital transformation, automation is becoming a major focus, particularly within the enterprise.

Physical security teams are increasingly joining this trend, seeking out ways to automate the highly complex and dynamic nature of their work – particularly when it comes to managing and maintaining their vast and diverse fleets of devices. Yet all too often, physical security teams still find themselves contending with the same unscalable, manual work they sought to avoid with those very tools.

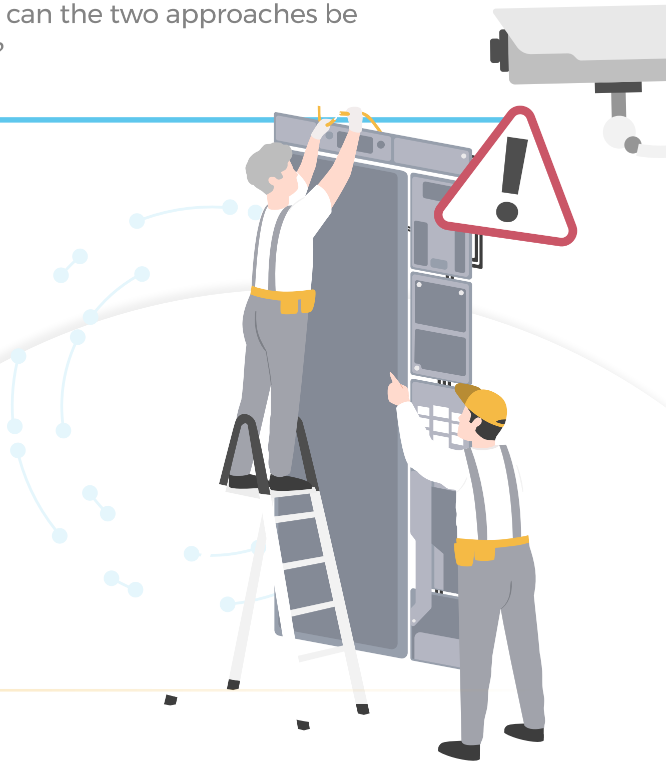
Why does this happen? And more importantly, what does it take for physical security teams to successfully automate their device management and maintenance?

To answer these questions, this guide presents the three fundamental criteria required for physical security teams to achieve the shift from manual to automated device operations.

By the end of this eBook, you will have a deepened understanding of how automation can transform your physical security operations – optimizing previously unscalable tasks, enabling your team to focus on more strategic objectives, and ensuring that your physical security is fully enterprise-ready.

## In the following pages, we will cover:

- Why are physical security teams faced with "impossible jobs" – and how can automation empower them to take back control?
- What are the key opportunities and use cases for automation in the operational management of physical security devices?
- What does it take to comprehensively automate the operational management of physical security devices, and what benefits can you achieve this way?
- Why is human involvement still necessary alongside automation, and how can the two approaches be integrated effectively?



# The “Impossible Job” Facing Physical Security Teams

Physical security teams face a range of challenges that make it particularly difficult to effectively manage their devices and ensure operational efficiency and compliance. To identify the areas where automation can make maximum impact, let’s analyze those challenges:

## Overwhelming complexity

Physical security teams often work with large fleets devices including IP cameras, access control panels, and a wide variety of other device types and management systems. Typical fleets of these devices include various models, produced by different manufacturers and running numerous firmware versions.

While it is critically important to manage these devices, the sheer scale and complexity of the task makes it prohibitively time-consuming and expensive to be conducted manually – especially when devices are distributed over a wide area and/or multiple sites, and especially given that physical security teams are usually resource-constrained.

## The scalability struggle

Exacerbating this already complex challenge is the fact that as organizations grow, so do their physical security needs. And when they grow suddenly – as in the case of mergers and acquisitions – the sharp jump in their physical security requirements can be exceptionally difficult to navigate.

It’s not just a case of having many more devices to manage. For example, particularly in the case of M&As, physical security teams will often inherit fleets of devices from manufacturers they weren’t working with until then, supported by unfamiliar management systems. Then they are left

with the complex, painstaking task of juggling these new devices and systems together with their existing ones, while they figure out a plan for eventually consolidating them (e.g. phasing some devices out, migrating others to existing management systems, etc.) Doing all that manually is virtually impossible – and in the meantime, those devices are vulnerable to a range of performance, compliance and cybersecurity risks.

## Keeping expenses in check

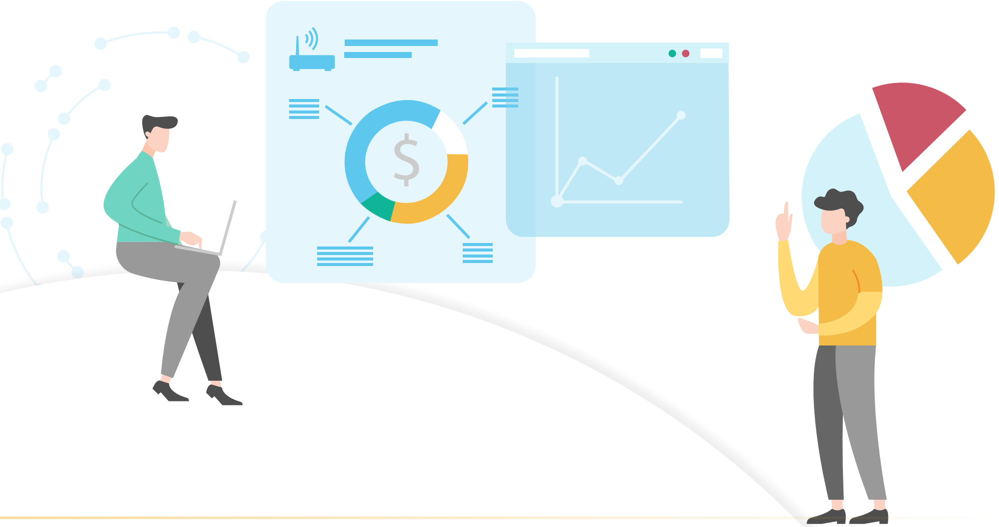
Cost-efficiency is a constant concern for physical security teams, which are often viewed as a cost center within organizations. Just purchasing and installing 1,000 physical security devices can easily cost $2 million to $3 million – and as mentioned, managing those devices over time is expensive. For example, the truck rolls on which many organizations rely for maintenance are costly, while communication difficulties and a lack of information can result in unnecessary work for IT and physical security teams, adding to ongoing costs.

Without enhanced communication, collaboration, and cooperation between physical security and IT teams, as well as with external partners such as systems integrators, organizations will continue to struggle to keep the inefficiency and expense of managing physical security devices down. And without a more cost-effective alternative to truck rolls, the physical work involved in managing those devices will continue to strain their budgets.

## Attracting (and retaining) talent and ensuring smooth transitions

As physical security needs continue to grow, organizations face a significant physical security workforce shortage, particularly in terms of qualified professionals with the required expertise. To ensure that their physical security is reliable, they need to attract and retain enough professionals with the necessary skills.

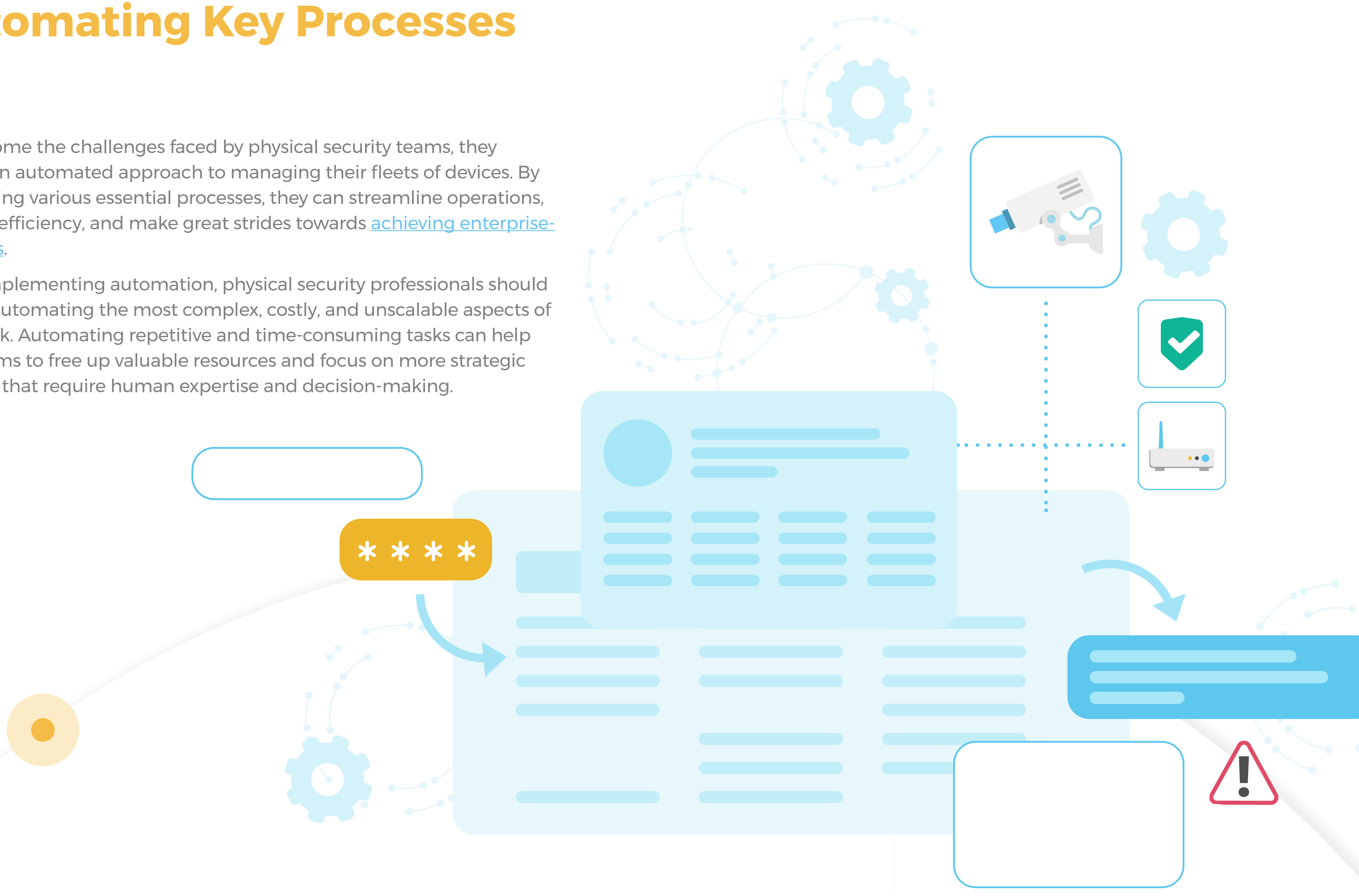
Adding to that challenge are changing demographics across the workforce. Millennials – now the largest generation in the U.S. – are especially attracted to companies that offer the latest and greatest technologies. That makes it particularly important for physical security teams to provide an environment that embraces automated tech and offers opportunities for skill development. Efficient automation is also an imperative for them as a crucial tool to help onboard new team members seamlessly and efficiently.



# Automating Key Processes

To overcome the challenges faced by physical security teams, they require an automated approach to managing their fleets of devices. By automating various essential processes, they can streamline operations, improve efficiency, and make great strides towards achieving enterprise-readiness.

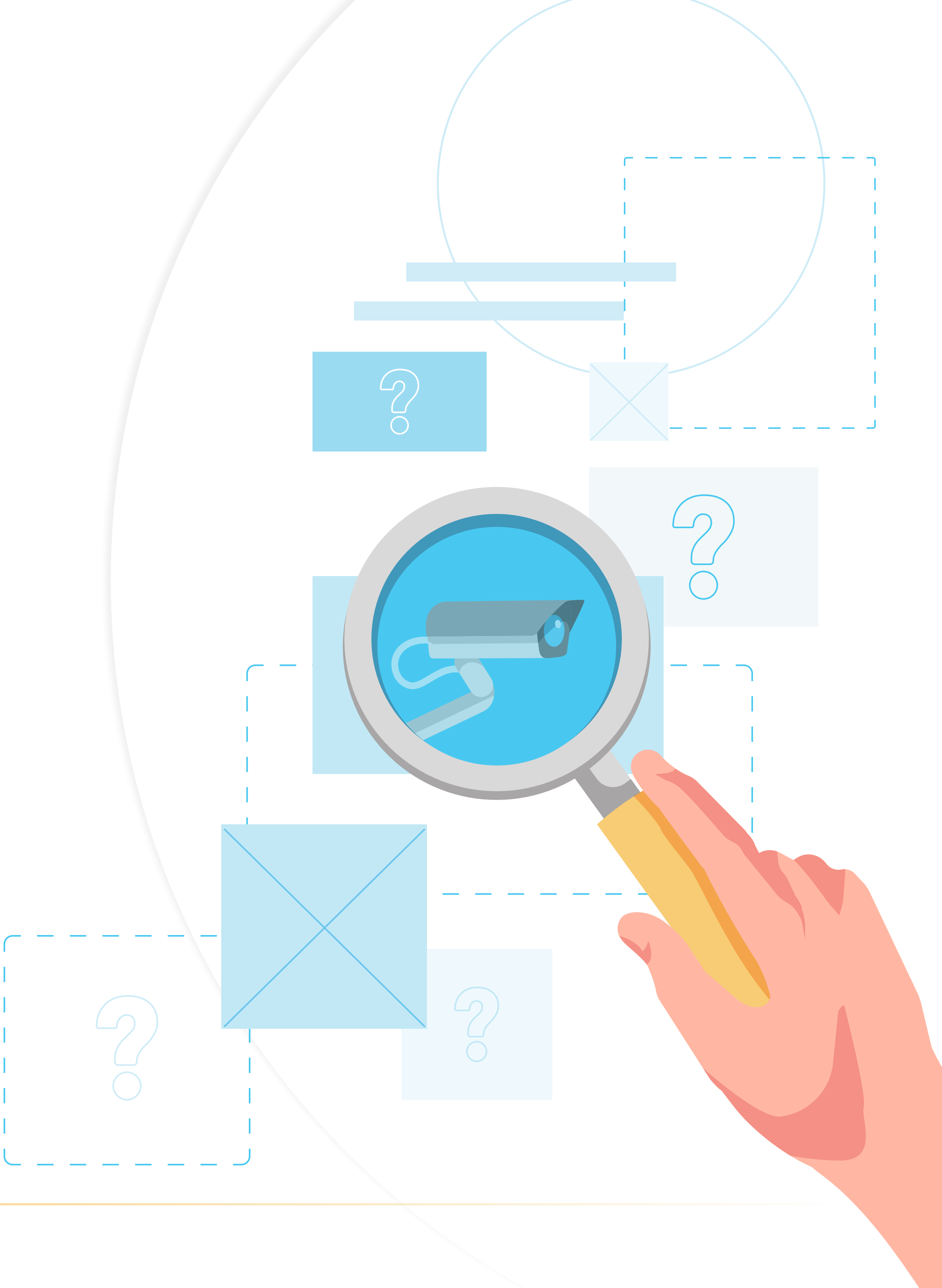
When implementing automation, physical security professionals should start by automating the most complex, costly, and unscalable aspects of their work. Automating repetitive and time-consuming tasks can help their teams to free up valuable resources and focus on more strategic activities that require human expertise and decision-making.



# Before we move on: a word about visibility

To effectively automate device management, physical security teams need to have visibility into those devices to begin with. Specifically, this requires real-time insight into the operational status and health not only of their physical security devices, but also of the surrounding ecosystem (management systems, related IT assets, etc.). This information is crucial for root cause analysis when issues arise, helping physical security teams to minimize downtime by diagnosing and resolving problems affecting their devices quickly and efficiently.

Visibility also plays a critical role in protecting physical security devices from cyber threats. To ensure that these devices are adequately hardened and maintained, organizations need information such as when each device last had its password rotated, how often passwords need to be rotated, when each device will reach its end of life, when certificates need to be rotated, which firmware version each device is running, and more. For firmware upgrades, having the necessary visibility is even more complex, as we'll see later on.



# Quantifying the Benefits of Automation

**Some of the most important physical security use cases for automation include:**

**Remote device restarts,** which can minimize downtime and ensure continuous functionality without the need for on-site intervention.

Our work with our own customers has shown that 70% of truck rolls can be replaced by remote device restarts.

**Certificate management**, which plays a vital role in securing communication channels and validating the authenticity of devices to protect them from threat actors.

Automatically managing certificates can make a powerful difference in helping organizations prevent data breaches, which cost an average of $9.48 million in the U.S., according to IBM's Cost of a Data Breach 2023 report.

**Firmware upgrades**, which can improve device performance and bolster cybersecurity by patching discovered vulnerabilities.

Automatic firmware upgrades can help organizations make sure their devices aren't vulnerable to cyberattack – a danger facing nearly 40% of security cameras as a result of running outdated firmware, according to Genetec.

**Password rotation**, which is a crucial part of hardening and maintaining physical security devices to protect them from cyber threats.

Some 15% of data breaches are carried out using“stolen or compromised credentials” (more than any other attack vector besides phishing), and these breaches take an average of 328 days to identify and contain (longer than any other attack vector), according to IBM’s Cost of a Data Breach 2023 report.

Our work with our own customers has shown that 70% of truck rolls can be replaced by remote device restarts.

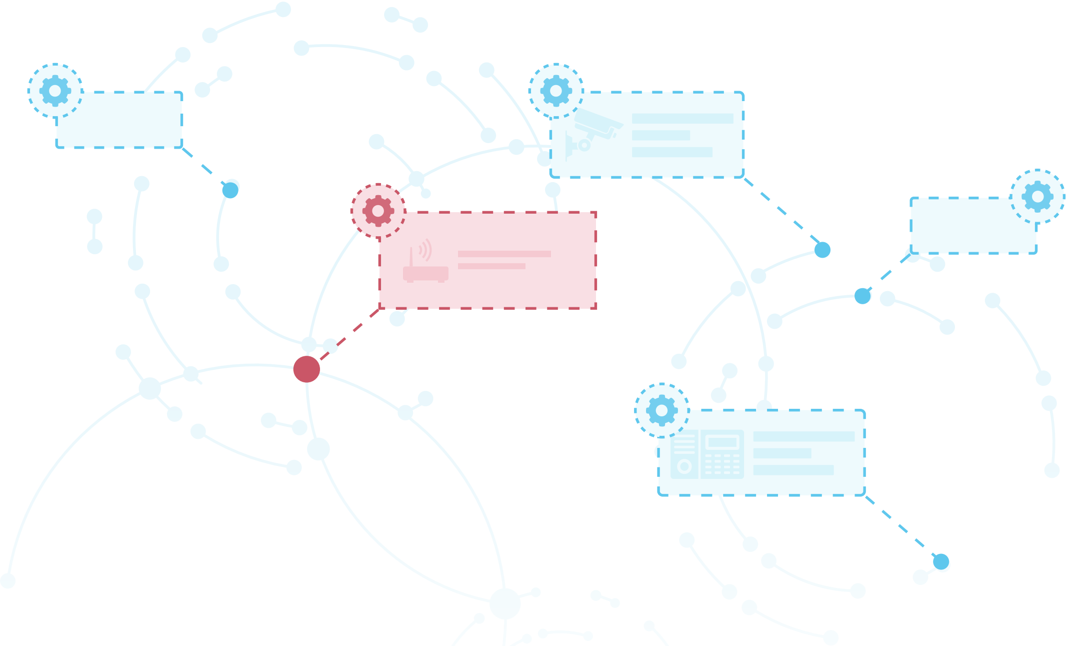
**End-of-life planning**, which can help physical security teams plan ahead in order to promptly replace devices before they become a cybersecurity liability as they stop being supported by new security patches.

Our data have shown that 15% of the physical security devices still in use are past their end of life, while an additional 40% are within 3 years of their EOL.

# The 3 Criteria of Comprehensive Automation

**There are no shortcuts to automation.** Limited or partial automation can alleviate some physical security challenges, but they won't solve them. In fact, in some cases an incomplete or partial automation "solution" can even make matters worse, by inadvertently introducing inconsistencies between various parts of an organization's physical security ecosystem.

To fully address your physical security pain points, it's important to take a comprehensive approach to implementing automation – particularly by considering the following three criteria.



## #1 Point Solutions vs. Comprehensive Layer of Automation

When considering ways to streamline the operational management of physical security devices, it's important to differentiate between point solutions and those that cover the entire process of operationally managing those devices.

Point solutions may offer automation in specific areas, such as password rotation or firmware upgrades. While this can be useful, it doesn't fundamentally transition your device management from manual to automated. It might offer some of the benefits of automation, but it will ultimately fall short of relieving physical security teams of unscalable maintenance tasks – leaving them to continue struggling in these areas.

Additionally, some organizations work with solutions that can automate a wider variety of processes, but only for a specific device manufacturer or management system. The problem with this approach is that device fleets typically consist of various devices from multiple manufacturers, which rely on multiple management systems. As a result, this approach is unlikely to let physical security teams realize the full possible benefit of automation – and can in fact cause or exacerbate siloes within the physical security ecosystem.

## #2 Device-Level Only vs. End-to-End Automation

Some automated tools focus solely on automating device-level processes, overlooking the importance of the broader ecosystem in which devices operate. This approach can introduce risks of device downtime or security breaches, especially when there is a lack of coordination between devices and their management systems.

For example, when rotating passwords for cameras, a device-level approach to automation does not guarantee that those cameras' video management system (VMS) will be updated accordingly. If the VMS is not updated, it can stop working properly with those cameras, creating a risk of downtime.

Similarly, organizations taking this kind of approach to automation may upgrade their devices' firmware in bulk, without first checking to see whether the new version is compatible with related equipment (such as a VMS) – also creating a risk of downtime. And if this happens to security cameras that have other technologies installed on them (such as license plate or facial recognition software), this kind of scenario can require a reinstallation of that software on every affected camera.

So in the best case scenario, device-only automation still leaves teams with a lot of manual work; while in the worst case scenario, it can lead to device downtime or other serious security and compliance issues – not to mention a major operational headache.

By contrast, a comprehensive approach to automation considers not only devices but also assets such as a VMS, network switches, and other relevant equipment – checking compatibility and then automating the process seamlessly on both the devices and their corresponding management system. This way, key steps such as password rotations and firmware upgrades can be coordinated properly across all assets, preventing incompatibilities that can lead to downtime. And since this coordination occurs automatically, it means that organizations don't need to spend valuable work time checking manually to see – for example – whether a firmware upgrade is compatible with a VMS.

# #3 Human Involvement and Collaboration

While automation offers numerous benefits, it is not meant to replace physical security teams. Instead, those teams can use automation in ways that empower them to shift their focus toward more strategic tasks and to generally improve their performance.

Human decision-making and involvement remain crucial when working with physical security devices, necessitating collaboration between different departments. In particular, collaboration between an organization's IT and physical security teams is crucial in order to help each team optimize its efficiency while boosting the organization's overall security. And there are situations where on-site repairs or troubleshooting require a human presence, highlighting the need for a hybrid automation approach.

To fully harness the benefits of automation, physical security teams should strive for comprehensive automation that encompasses the entire ecosystem in which their devices run. By combining thorough visibility with a comprehensively automated approach to managing entire fleets of physical security devices, organizations can take a holistic and effective approach to ensuring enterprise-ready physical security.

# Conclusion

Automation has become a vital tool for physical security teams, empowering them to streamline and enhance the operational management of their devices, and enabling them to focus their energies on strategic tasks rather than tedious, unscalable ones. Throughout this guide, we have explored the potential of automation to address inefficiencies, high costs, and reliability issues that can often plague security operations.

This use of automation presents physical security teams with opportunities to strengthen their enterprise-readiness across various critical processes – from remote device restarts to firmware upgrades, password rotation, certificate management, and end-of-life planning.

At the same time, it's important to recognize that automation is not a standalone solution. While it brings significant benefits, human involvement remains essential. Collaboration between IT and physical security teams and the need for on-site repairs underscore the importance of a hybrid approach that combines automation with human expertise.

By combining this approach to automation with heightened visibility into your physical security devices and their surrounding ecosystem, you can boost your efficiency, cost-effectiveness, and – most importantly – your overall security posture.

## SECURITHINGS: AUTOMATING PHYSICAL SECURITY DEVICE MANAGEMENT

SecuriThings automates physical security device management at scale. The SecuriThings solution provides real-time security and operational efficiency to improve system availability, organizational compliance and cyber protection — while reducing costs and streamlining future planning. SecuriThings' advanced technology provides automation, analytics and actionable alerts to keep fleets of physical security devices fully operational and secure. The solution is deployed remotely, in a matter of hours.

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

www.securithings.com

SECURITHINGS