SMART INTEGRATION. BETTER SECURITY.

Comprehensive approach for physical and digital spaces

SIEMENS

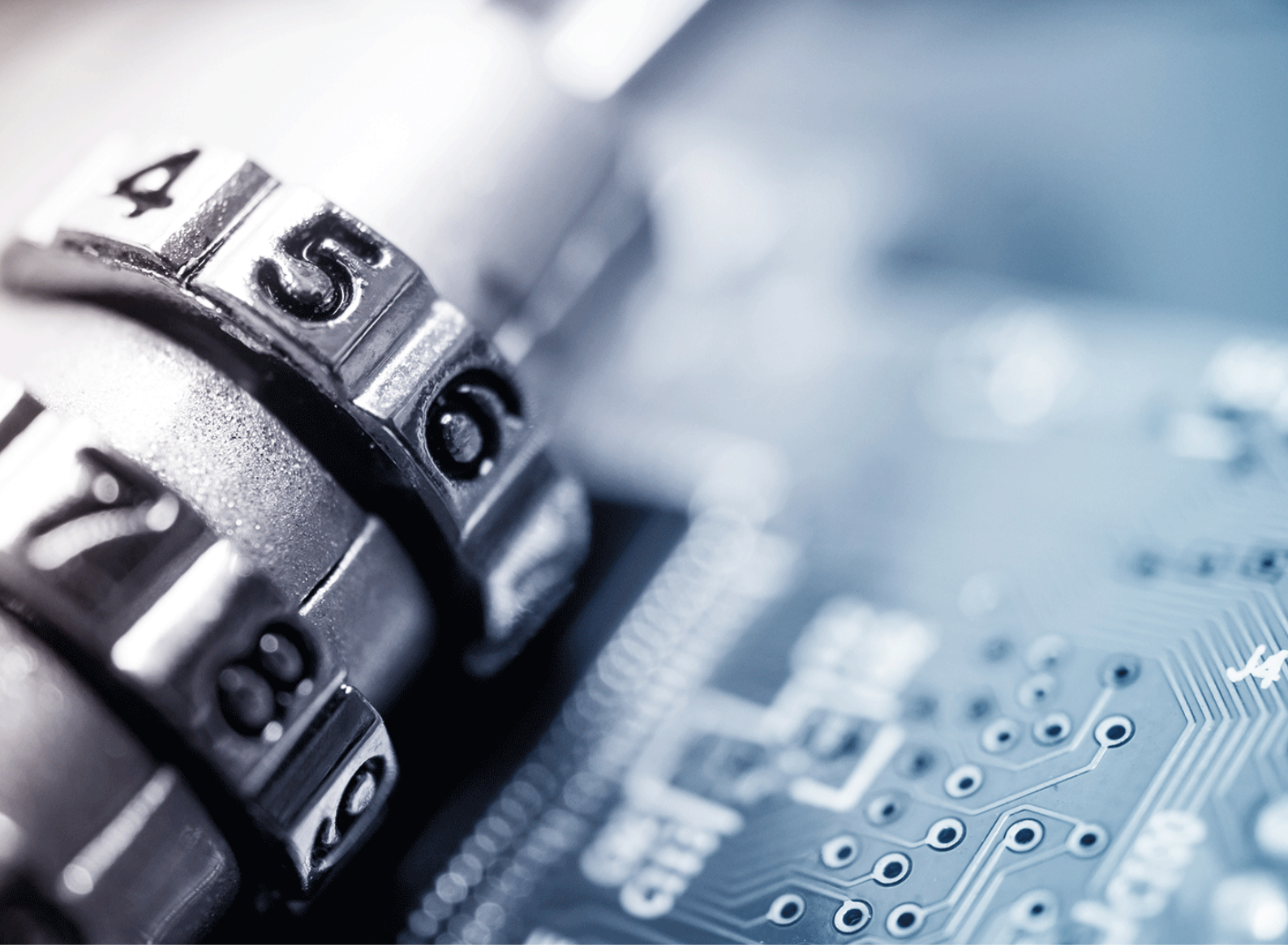

Table of contents

What value can a security system bring?

Over the last decade, the security landscape has been evolving in fundamental ways. Where once security systems were primarily based on cameras, access readers and other electronic devices focused on protecting physical spaces, they have become software-based, securing both physical and digital spaces. Today, for most organizations, security encompasses even more – it's now also about bringing added value to the organization.

The first in a multi-part series, this white paper explores the different types of value organizations are looking for their security solutions to provide. It uncovers some of the barriers of a siloed approach to security, both in smart buildings and in facilities where security is a part of the critical infrastructure. It also describes how taking an integrated approach to security can offer air-tight protection for people, property and information while delivering data that can enhance operational efficiencies, improve user experience, strengthen cyber security and more.

Risk mitigation is only the beginning.

Different buildings have different sets of security needs. Operators and users of today's smart buildings typically see security as a necessary investment and are looking for simplicity and ease of use. For facilities where security is a part of the critical infrastructure, such as airports and power plants, a 360-degree security experience is required to ensure business continuity at all times.

Most buildings and facilities aim to mitigate risks

Whether you have a smart building or a critical infrastructure facility, a range of stakeholders may be involved in security decision-making, including building owners, facility managers, IT managers and security managers. Each of these stakeholders has their own priorities, but they can all rally around one common interest: mitigating risks.

According to a global security market study by Kunde & Co 2020, among the above-mentioned security decision-makers across the US, Australia, Germany, France and Italy, 67 % see security as an enabler to mitigate risks. This means protecting assets, creating safe and healthy environments, safeguarding company image and brand reputation, and increasing employer peace of mind.

Security decision-makers want to reduce risk-related events:

- Reduce breaches
- Reduce number of injuries and casualties
- Reduce response time in case of event
- Address security information efficiently
- Recover faster from an incident
- Minimize risk of cyber-attacks

However, at least some security stakeholders believe their security solution should be able to go beyond risk mitigation. The same study shows that 33% believe their security solution should also create efficiencies, for example, by understanding traffic in an office building and improving room utilization or by helping increase employee productivity.

Top five pain points when it comes to risk mitigation:

1. Avoid security system errors or breakdowns
2. Ensure cyber/network security
3. Work within budget constraints
4. Integrate security systems with the building management system
5. Integrate different security system

Different buildings have different security needs

Smart buildings:

- See security as a necessary investment
- Ease of use is a high priority
- Operational efficiency is important
- Looking for added value
- Looking for integrated solution

vs

Critical infrastructure:

- Security is a first priority
- See security as a 360-degree experience
- Operational efficiency is important
- Security is linked to revenue streams
- Business continuity is critical
- Looking for integrated solution

Threats of disparate security systems

Differing stakeholder priorities often results in the organization taking a segregated, siloed approach that prioritizes disparate security systems. These systems struggle to work together to reduce breaches, injuries, response times, and the risk of cyberattacks. As a patchwork of systems and software, they are unable to create valuable efficiencies on their own.

"Many organizations have already digitalized and integrated most of their operational tools and systems. Security should be part of this," says Rami Bayram, Head of Security Center of Competence, Siemens Middle East and Asia Pacific. "With security systems that work independently, response times are longer. This can put people's lives or assets on the line. Without an integrated view of the facility, it can be hard to identify threats and understand their potential for harm." At the same time, integrating security systems with other digital systems reduces human work for facility management, security management and IT teams alike.

Integrated security and the value of data

The aforementioned study also shows that 31 % of decision-makers see security as an integral part of the building management system, and 27 % prefer one unified security platform. With security that is fully integrated with the BMS or SCADA system, organizations can get more insight into how people are using the building.

"There is great value in this intelligence as it can create more efficient and cost-effective building operations," says Rami, Head of Security Center of Competence. "By combining security data, like pedestrian traffic and access control points, with HVAC, lighting, fire safety and other building management data and visualizing it, trends will start to emerge. The more you know about the usage trends within your building, the more efficient it can become."

Enhancing operational efficiencies

Analyzing access control data lets building operators cut heating, cooling or power when rooms are not in use. Spaces can be rented out if they are not needed. Faulty equipment can be easily identified. There are many ways that security data can optimize the efficiency of buildings and facilities. The data can also be used for commercial purposes. For example, retailers can organize their stores based on shopper traffic and behavior.

Security data can also help teams work more efficiently. In the case of law enforcement, organizations leverage security data to save time reviewing evidence. "We have essentially saved the department over 2000 hours of manual labor in physically collecting and storing video evidence. The ROI is there for us in terms of the efficiency," says an IT manager from a law enforcement organization.

We have essentially saved the department over 2000 hours of manual labor in physically collecting and storing video evidence. The ROI is there for us in terms of the efficiency.

IT manager, law enforcement

Improving user experience

In smart buildings, many of the ways humans interact with the building are automated. Data from an integrated security system can help enhance this interaction by identifying areas that need improvement. Perhaps a building's cafeteria has high-traffic periods that need to be managed. Or the restrooms are too busy in the afternoon. Security analytics can help identify and correct these issues so building users have a better experience.

"Buildings are no longer passive concrete blocks. They are alive and interacting with us. If we can collect and analyze data about these interactions, we can improve usability," says Rami.

Strengthening cyber security

Integrating your BMS or SCADA system and your security system can also help strengthen cyber security. Cyber challenges can be multifaceted and can range from insider threat, ransomware attacks, opportunist threats, and hacktivism to terrorist-related cyber threats, all of which affect people, technology and business continuity. With a holistic view of the space between physical and cyber security challenges and the interactions among technology, people, processes and communication, cyber threats become easier to mitigate and downtime can be minimized.

"The financial and human costs associated with downtime should not be underestimated. Evacuating even a mid-sized office for a few hours could incur losses in the range of USD 10,000. For airports, data centers or financial buildings, this number can quadruple. And when it comes to hospitals with intensive care units where lives are on the line, the cost is way beyond financial."

What to look for in a holistic, integrated security solution

1. Look for a unified offering with an open, modular composition of applications, tools and services. This offers product flexibility and makes integration and scale-up simpler.
2. Ensure the solution offers business continuity in case of an event.
3. The solution should offer incident and command & control systems, access control, video surveillance, intrusion detection, alarm, analytics, information and operation management.
4. Look for a solution partner with both building management and digital security expertise.

Need more information about Security analytics? Learn more.

"

Choosing a partner with building and infrastructure management expertise can help you ensure that all aspects of the facility are integrated with your security solution, from automation to fire protection to energy management to other systems.

Rami Bayram, Head of Security Center of Competence for Siemens Middle East and Asia Pacific

Smart integration. Better security.

Smart buildings and facilities offer new levels of data-driven and sensor-enabled performance through deep system integration, predictive and condition-based maintenance, optimized efficiency, increased resilience and security, and better operations. Traditional security systems hold organizations back from experiencing the benefits of smart buildings.

An integrated security system can help you better understand your operations by detecting valuable events that go far beyond security – safeguarding people and assets while simultaneously powering better business performance.

Want to discuss integrated security with us?

Get in touch here

Published by
Siemens Switzerland Ltd

Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
6300 Zug
Switzerland
Tel +41 58 724 24 24

For the U.S. published by
Siemens Industry Inc.

800 North Point Parkway
Suite 450
Alpharetta, GA 30005
United States

Smart Infrastructure combines the real and digital worlds across energy systems, buildings and industries, enhancing the way people live and work and significantly improving efficiency and sustainability.

We work together with customers and partners to create an ecosystem that both intuitively responds to the needs of people and helps customers achieve their business goals.

It helps our customers to thrive, communities to progress and supports sustainable development to protect our planet for the next generation.

siemens.com/security

Status 02/2022