SECURITY AS A SERVICE

Is subscription-based the future of physical security?

SIEMENS

Table of contents

What potential does subscription-based security hold?

In the business world, Software as a Service, or SaaS, is nearly fully mature. Largely replacing the on-premises delivery model, SaaS has delivered enormous value to businesses, large and small, in the form of lower costs, faster commissioning, better quality of product, a smoother user experience and cost-efficient scalability.

These kinds of benefits are not only available in the software realm, they have also proven popular in the physical security world through Security as a Service. As smarter, more connected security and communications devices become more ubiquitous along with global networks, enterprises can access a world-class level of physical security, with new capabilities, across their properties without a serious CAPEX investment.

The adoption of Security as a Service is on the rise, proving that companies don't need or want to be 100 % dependent on their internal departments to deliver high-quality security services. Just as SaaS has proven to be an enabler for IT, freeing up costly IT resources to focus on value-added activities, Security as a Service is freeing up facilities and security departments to provide higher valued services at lower cost.

But what are the barriers to entry for Security as a Service? Why is it experiencing this surge in popularity? And what does the future hold for this relatively new offering? Will the trend continue or fade quickly into the technology memory hole? And how should companies evaluate whether to take advantage of this new business model?

This whitepaper explores these questions and more. It provides security decision-makers with insights into the risks and opportunities around Security as a Service and details on how it provides value. It also explores current trends in technology that may shape the future viability of Security as a Service. And, finally, it offers tips on how to choose the right partner.

Read on to explore if Security as a Service is right for your business.

The future demands flexible security management systems

Over the past several years, the technology industry has been dominated by flexible consumption models, also known as as-a-service models. Whether it's subscription-based music such as Spotify or software used in business such as Microsoft 365, subscription-based models are widely known for enabling more flexible, customized and efficient user experiences.

What is Security as a Service?
Security as a Service is a full-service approach to access control, video surveillance, perimeter protection, intrusion detection, security management and analytics. It includes planning, hardware, software, updates, upgrades and services in a subscription model and can be deployed on-premises, in the cloud or be hosted. Security as a Service enables access to your security system from anywhere, anytime, from any device, so you're ready to react quickly to security incidents.

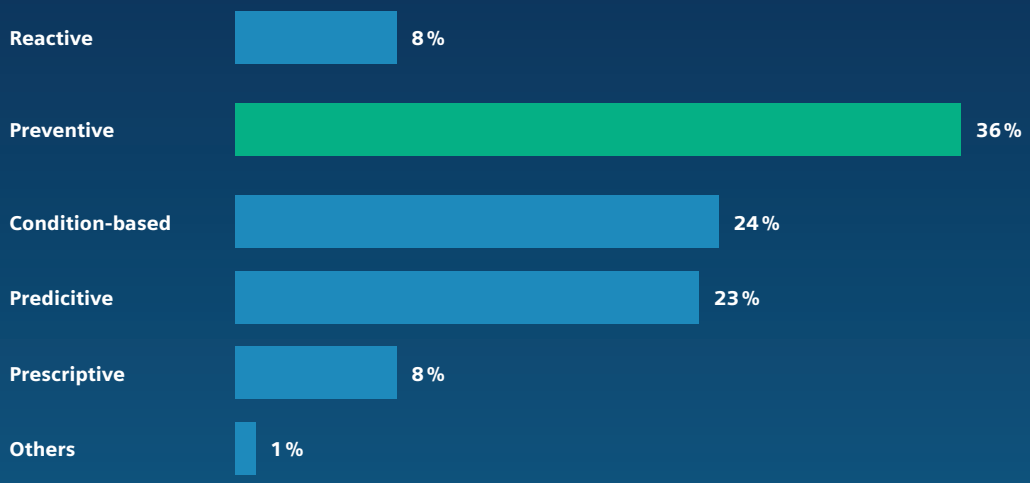
Although slower to be adopted than other as-a-services, Security as a Service is becoming more prevalent for businesses across the world. According to a recent market study of building owners, facility managers, IT managers and security managers across the US, Australia, Germany, France and Italy, 74% of companies will likely adopt an as-a-service-based payment model for physical security solutions in the near future. And 5% have already adopted one.

"We see many customers investigating as-a-service models," says Rich Reidy, Senior Director of Security Solutions & Services for Siemens Americas, "trying to make budget decisions that will allow them to move from an asset-based security system to a serviced-based one. I think the pandemic has shown that we can – and need to – rely on remote connectivity for basic business functions, and as 5G gets more established, companies will see greater opportunity in as-a-service models for building and employee security."

Preventive security as the preferred service model
The study also shows that preventive security is the most popular security type provided as a service (compared with reactive, condition-based, predictive and prescriptive security). Preventive security has become especially prevalent in smart buildings because the more devices that are connected to the network, the greater the pressure on the IT infrastructure. More and more companies are taking preventive measures to protect themselves from vulnerabilities in the network, and this becomes more efficient through as-a-service models.

"As-a-service models provide automatic updates of the security system, which is key to preventive security," explains Rich. "This may be one of the reasons this is the most popular type of security delivered as a service."

According to a global survey conducted by Kunde & Co, **74 %** of companies will likely adopt an as-a-service-based payment model for physical security solutions in the near future. **5 %** have already introduced such a model.



Kunde & Co, Global Security Market Study, 2020

With 36 %, preventive maintenance is the most popular security type delivered as a service.

Why Security as a Service is gaining ground

Instead of focusing on hardware and software ownership, Security as a Service applies the service delivery model to lower the costs of physical building security. It combines mobile, wireless, and cloud technologies into a service system that transforms the economics of building security while improving flexibility, convenience, capabilities and user experience.

Because it's run on a subscription-based model, Security as a Service requires no capital investment up front, freeing you up to invest in your core business. And, because human security expertise is included, along with automatic software updates and system maintenance, your IT staff is freed up to focus on IT and not security. With no gaps on a human level, this also reduces exposure to security risks.

The benefits of Security as a Service:

1. Customers can focus on the core business by outsourcing their full security needs
2. Automatic system updates reduce complexity and increase security
3. Users get exactly what they need, how they need it
4. No up-front investment in products and personnel
5. Predictable costs set by the contract
6. Flexibility – fixed price includes scaling system up and down
7. Leverage cloud-based technology

Use case: Burda Druck Nürnberg GmbH & Co. KG

A company for individual communication and printing solutions (a venture of the Hubert Burda Media group of 12,900 employees) required a Physical Security Information Management (PSIM) system to increase on-site security. As they had few security resources in house, they needed a full-service approach to help meet all standards and individual requirements. Requiring no CAPEX investment, their Control as a Service solution offers predictable operating costs and flexibility should they need to scale the system. It ensures high business continuity thanks to high system availability and allows the company to focus on its core business.

Obstacles to faster adoption of Security as a Service

Even though the adoption of Security as a Service is at an all-time high, it has been slow-going compared to other as-a-services. One of the biggest obstacles to a faster adoption is the prevailing mindset. Traditionally, when we talk about security systems, we think of tangible devices such as alarm systems, video equipment, computer hardware and the software that it runs on. For Security as a Service to be even more widely adopted, this mindset will need to change.

"When you own a car, for example, it becomes your asset, and you need to invest in its maintenance to optimize its value," Rich Reidy explains. "When you lease a car, it is not your asset – you pay a monthly fee to use it and when your needs change, you exchange it for one that matches your needs. Security as a Service is like leasing a car instead of owning it. All the service and maintenance, or updates, are included and it can't depreciate in value. Because as your business needs change, so can your Security as a Service agreement. But decision-makers need to accept the service model to experience the benefits."

IT infrastructure integrity

Another major obstacle to the adoption of Security as a Service, especially for IT managers, is the question of IT infrastructure integrity. As security cameras, sensors, access control systems and other security devices are connected to the internet, they present opportunities for the system to be hacked. IT managers need to be reassured that increased connectivity does not threaten the integrity of the IT infrastructure.

"It's important that the physical security devices comply with the business's IT governance," says Rich, "and that the physical security system is seen as an integrated part of IT infrastructure."

It's important that the physical security devices comply with the business's IT governance, and that the physical security system is seen as an integrated part of IT infrastructure.

Rich Reidy, Senior Director of Security Solutions & Services for Siemens Americas.

The question of cloud security
For cloud-based or hybrid solutions, cloud security is another common barrier. IT managers, security managers and facility managers are asking: "How safe can my solution be if it is cloud-based?" The answer is that a cloud-based security solution can be just as secure as an on-premises solution.

"The key to a secure solution is updated software and firmware. On-premises solutions are often based on legacy systems that, due to outdated passwords and other system gaps, can hold a range of security risks. Cloud-based security includes constant automatic updates, making it, in many cases, more secure than on-premises solutions," Rich explains.

As more and more enterprises rely on data and cloud-based data storage, cloud-based Security as a Service models are becoming more relevant and more secure. Still, some businesses prefer to run their Security as a Service on-premises, as it gives them an added sense of control over their data.

The next three years
Despite these obstacles, 89% of decision-makers accept the idea of remote connection from their security provider and 71% believe they will adopt a cloud-based technology to host and process security data within 3 years.

Top 3 obstacles to the adoption of Security as a Service

1. **Ownership vs. service-based mindset**
2. **Questions about IT infrastructure integrity**
3. **Cloud-based network security concerns**

"

89 % of decision-makers accept the idea of remote connection from their security provider. 71 % believe they will adopt a cloud-based technology to host and process security data within 3 years.

Kunde & Co, Global Security Market Study, 2020

The future of Security as a Service

In the past, security was about maintaining workflow and traffic through the building and augmenting the physical guards on-site. But as building owners have become more tech-savvy, digitally managed security spaces have become a major component of the overall business – bringing real operational and commercial value rather than just ongoing business costs.

Future security systems need to find ways to connect multiple devices and services and identify how to drive building efficiencies, effectively reducing a building's costs. Security as a Service is a reliable and cost-efficient method of achieving all of this, and, at Siemens, we believe the future looks bright for this solution.

Five trends point to subscription-based security

1) The ownership mindset is changing
Although the ownership mindset remains a barrier in the physical security market, this is changing as digital natives become decision-makers. This generation is pursuing freedom from ownership, not only in terms of music and media, but also in terms of cars, homes and other once self-defining assets.

"Asset ownership comes with certain constraints," adds Rich Reidy. "Once you invest in that asset, you are responsible for insuring and maintaining it. Consumers and professional decision-makers around the world are freeing themselves of these constraints – and this is largely enabled by the rise of subscription business models. It's only a matter of time before the ownership mindset changes in security as well."

2) Service expectations are increasing
Across all markets and realms, consumers and professional decision-makers are conditioned to expect seamless delivery of services regardless of the service, provider or channel. They seek on-demand services that are fully aligned with the challenges they face, and they only want to pay for objects and services they actually use.

"As IT managers, security managers and facility managers continue to experience the benefits of seamless services in other contexts, they will naturally expect the same from their security solution. Security as a Service takes the burden of security management off the company in a cost-effective manner. We expect more and more organizations to seek the benefits in the coming years."

3) Security focuses on prevention
In the world of security, the focus is moving from reaction to threats to prevention of threats. This is driven by the uptick in hacking and data breaches along with the availability of data and surveillance technologies that enable prevention.

"The value of preventive security solutions is becoming clearer to businesses who experience security events and realize how costly even the more benign security threats can be," says Rich. "As-a-service business models are the most cost-efficient delivery method for preventive security, so we see this as another clear indication that Security as a Service will only rise in popularity."

4) Businesses look to get value from their data
Hyper-connected and mobile populations using immersive and cloud-based technologies have led to an explosion of data. There are new layers of information built around everything we do, which brings new opportunities in terms of physical security.

"Customers are always looking to get value from their business intelligence," says Rich. "Building planners of the future are challenging the industry to find out how to leverage data to make processes more efficient and minimize operating and maintenance costs. By surfacing the available data and providing valuable business insights about their buildings, we're helping customers do that – and again, the as-a-service business model is the most efficient way to deliver these benefits."

5) 5G strengthens connectivity
5G is being rolled out in regions across the world. The technology is not just about higher bandwidth and lower latency; it is also a wireless revolution that will enable robotics, automation, IoT and many more industry applications to further drive enterprise digital transformation.

"The growth in IoT adoption is driving the total number of connected devices. Some IoT applications, such as smart building and location tracking that require large numbers of sensors in a small area, are reaching the maximum capabilities of existing wireless technologies. With IT supporting stronger connectivity and more robust IT infrastructures, I think it will encourage the further adoption of integrated security solutions delivered as a service."

About a third of 924 enterprises interviewed have more than 1,000 devices connected in their IoT deployments.

Kunde & Co, Global Security Market Study, 2020

Digitally managed security is getting better every day

Investments in security technologies have steadily risen over the past several years. As a result, businesses and public buildings usually have more than one security system installed. They rely on powerful security management systems that combine all of them into one user experience. This makes security management much simpler for facility managers, receptionists, or other non-experts with responsibility for security.

"Comprehensive security management systems today take advantage of the latest technologies to heighten security while simplifying security management for users. Our Siveillance Suite, for example, comprises a comprehensive range of security solutions and systems – from intelligent video surveillance, access control and identity management to intrusion detection and perimeter protection, up to industrial command and control center technology."

When delivered as a service, security management systems are also scalable according to customer needs. This is particularly useful in large enterprises where employee turnover averages around 10%. In organizations where turnover is high or change is constant, Security as a Service is the easiest way to scale the system up or down while managing costs.

The right partner is important

When considering different security partners, it's important to choose one with building and infrastructure management expertise as well as cyber security know-how. This will help ensure that all aspects of the facility are integrated with your security solution, from automation to fire protection to energy management. And it will help ensure that cyber security is inherent to the planning and execution of your system. Look for a Security as a Service solution that ensures the integrity of your IT infrastructure and is customized to your distinct user needs.

How to choose the right partner for Security as a Service

1. Work with a partner with knowledge and domain know-how of automation, digitalization, and electrification in compliance with international standards
2. Look for solutions that meet the strictest physical and digital security requirements:
   – Building security
   – Entry points
   – Room utilization
   – Communication
   – Data protection
   – Access control
   – Consistent monitoring
3. Ensure full optimal and secure interaction among all components: products, processes and technical solutions
4. Look for a solution that includes consulting covering technological, procedural and personnel elements and comprehensive services throughout the lifecycle of the assets

Safe and intelligent: Security as a Service

Because we live in the era of digitalization, we're future-oriented. Our Security as a Service solutions arm our customers against both existing and potential cyber and physical security challenges.

For Siemens, Security as a Service is fundamental to providing a flexible, cost-effective and future-proof security for our customers, no matter their size or needs. Ultimately, when it comes to both physical and cyber threats, we're committed to safeguarding the only thing that matters to you – security as the foundation of your business.

Want to discuss Security as a Service 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