Life Is On | Schneider Electric

Security Management: Is the Cloud a Viable Option?

by Steven Turney

Executive summary

Many building owners, facilities managers, and security personnel are considering moving their enterprise security management systems to the cloud. With other enterprise applications already in the cloud, they want to achieve similar benefits while ensuring the best and most secure solution for their company. This white paper presents practicable considerations for moving to the cloud, with recommendations on how to evaluate cloud-based security management solutions.

Introduction

A widely discussed topic in organizations around the world today is whether or not the cloud is a viable, secure solution for enterprise applications.

There is still a lot of debate on this issue, especially when it comes to critical applications like security management solutions. It certainly is the right choice for many companies – and even a business necessity, in some cases – but it may not be right for every organization.

Like with any change in infrastructure, security managers and building owners must weigh the benefits and risks of moving to the cloud before incorporating it into their security management strategy.

To help with this process, this white paper offers an overview of security management market trends as well as recent research on what other companies are doing today with their security operations (**Figure 1**). It also offers insights and guidance on why organizations move their security to the cloud, and the value of such a move.

Figure 1

Many companies are moving their enterprise security management systems to the cloud.

In particular, this paper answers some of the most pressing concerns that building owners and security managers have regarding the cloud, including topics such as:

- What does the cloud offer in relation to in-house capabilities for security management?
- What kind of performance can be expected? Will services be compromised, especially in critical areas like building security alarms?
- From a cybersecurity perspective, is there increased risk in the cloud?
- What kind of capabilities does a cloud-based security management solution offer? Can a company expect robust, innovative functionality?
- Does the cloud offer a future-proof path?
- What kind of provider is needed in order to deliver a high-quality cloud solution?

With the information here, those responsible for their organization's security can intelligently decide if moving to the cloud is the right strategic move for their company.

The cloud is the future for many

Many organizations already have several enterprise solutions – such as email and voicemail services, human resources (HR) systems, customer relationship management (CRM), and data storage – in the cloud. In fact, a *2016 State of the Cloud Survey* found that 95% of the IT professionals who responded said they are already using the cloud.[1] And in its *2017 Predictions* report, Forrester Research says the cloud is no longer an adjunct technology bolted onto a traditional infrastructure and that the cloud market will accelerate this year.[2]

Similar trends are evident in the security management market as well. A recent study polled [3] IT and security executives in a wide range of industries who had purchasing authority for their company's security management solutions. As shown in Figure 2, the research report, *Security in the Cloud*, found that over 50% of the respondents already host their security management in the cloud.

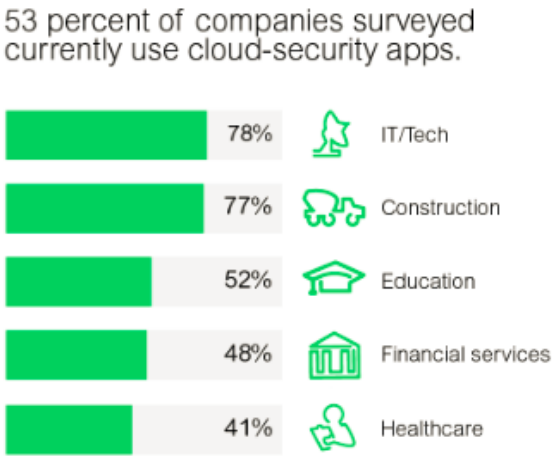


Figure 2

Over 50% of survey respondents representing a variety of business segments currently use cloud-security apps.

What kind of benefits are the people in this study experiencing? According to the respondents' antidotal comments, many are taking advantage of the innovative technology and opportunities that the cloud offers at a low total cost of ownership. Some believe it is the wave of the future and an actual necessity for their business. One respondent, a chief information officer, even shared that the cloud was one of the best strategic moves for his or her company, with ROI proven time and again.

A common theme in the commentaries in this research was how well the cloud is working for the respondents' companies, with convenience showing up as an often-mentioned benefit, along with versatility, flexibility, and efficiency.

Benefits like this are achievable because cloud providers are typically on the forefront of technology innovation, and they manage updates for customers, including deployment and maintenance of software and hardware environments. Cloud providers also have extensive computing resources and can provide high levels of redundancy. In addition, they can also easily deliver extra processing on demand and scale systems quickly as business needs change.

---

[1] *Cloud Computing Trends: 2016 State of the Cloud Survey*, Right Scale, 2016. http://www.rightscale.com/blog/Cloud-industry-insights/Cloud-computing-trends-2016-state-cloud-survey

[2] *2017 Predictions: Dynamics that Will Shape the Future in the Age of the Customer*, 2017, https://go.forrester.com/wp-content/uploads/Forrester-2017-Predictions.pdf

[3] *Security in the Cloud*, Morar Consulting, sponsored by Schneider Electric, December 2016.

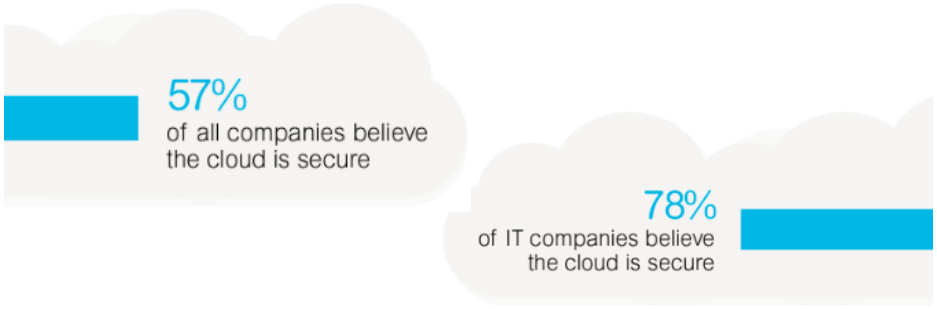
Thus, companies can take advantage of reduced onsite overhead costs, easier system deployment, decreased strain on internal resources, greater compatibility with existing onsite systems, and the future-proofing of their investments.

Is the cloud secure?

The *Security in the Cloud* research found that security – and threats like hacking and the protection of data – remains a major concern that could impede a move to the cloud. However, 57% of the overall respondents, and 78% of the ones from the IT and technology sector, believe the cloud is secure, a sentiment that was reiterated often in the antidotal comments (**Figure 3**).

Figure 3

Current research indicates a growing belief that the cloud is secure.



Utility companies are typically highly conservative about changes in information systems infrastructures and new emerging technologies, especially when it comes to building security. But an IDC Energy Insights report[4] found that the cloud addresses the concerns of organizations like these in security-conscious industries with critical privacy-sensitive environments. For instance:

- 74% of the utilities companies surveyed indicated that a public cloud is their dominant, long-term platform strategy to meet IT needs.
- 87% recognized the value of cloud services to provide better business continuity and disaster recovery than traditional technology.
- 82% considered total cost of ownership as the single most important consideration for choosing a cloud service.

  76% recognized that cloud providers can offer better cybersecurity than that offered by their own organization's IT security team.

Why a move to the cloud is a viable choice

In the *Security in the Cloud* survey, over 95% of the organizations encourage the adoption of new technologies, and hence, 36% of these companies feel their security systems are future ready. However, over 60% of them indicated that their security systems require improvements, with nearly 10% noting that their systems need major improvements (see **Figure 4**).

[4] http://www.continuitycentral.com/index.php/news/technology/266-news7575%0A

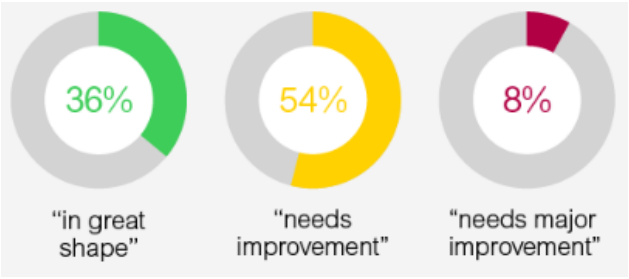


Figure 4

Survey results indicate how respondents rate the state of their security systems.

For companies like these, where security management improvements are imminent, it makes sense to consider the cloud, especially if they want to achieve these benefits.

1. **Capitalize on an existing and increasing cloud presence**. Many companies already have made a strategic choice to have enterprise applications like data, email, HR, and CRM in the cloud. Because the payoff is evident and proven, adding additional applications such as security management to their cloud presence is simply a way to extend benefits like cost-effectiveness, flexibility, and convenience.
2. **Take advantage of the latest in security**. Cloud service providers typically have the latest in cybersecurity tools in place, which can help mitigate the risk of attacks. In fact, the authors of a recent PricewaterhouseCoopers study, the *Global State of Information Security 2017*,[5] say, "We believe that cloud computing services are foundational to the integration and management of the many moving parts of a threat-management program."
3. **Provide anywhere, anytime accessibility**. When it comes to solutions like building security management, an advantage that the cloud provides is real-time visibility into an entire organization via mobile access. Whether onsite or on the go, security teams can get insights into all their facilities, assets, and systems from virtually anywhere, any place, and anytime. From a smart device or laptop, building managers and security personnel can make clear, informed decisions in real-time to more effectively manage their facilities.
4. **Increase innovation and performance**. The cloud typically provides companies with the latest, most evolved technology, and enterprise building security management is no exception. With a move to the cloud, organizations can take advantage of leading-edge innovation that provides high performance, mobile access, and easier maintenance, deployment, and scalability.
5. **Lower the cost of ownership**. Another attractive benefit of the cloud is the considerable savings companies can realize because of a lower total cost of ownership. Cloud implementations only require a minimal upfront investment because secured servers – as well as development, support, and maintenance – are managed by the service providers. A company's cost savings are extended even more because cloud-based security can typically be integrated with other building management systems (BMS), as well as fire alarm and lighting control systems. This approach optimizes an organization's investment in their existing technology while providing an overall better performing building.
6. **Future-proof security environments**. And finally, because of the innovation and cost savings of a cloud implementation, an organization's investment in the future is greatly protected. There is no need to plan and prepare for massive updates and upgrades of existing systems, or extensive build-outs to replace outdated technology. The cloud provider takes care of all of that, with systems that are continually up-to-date and at the forefront of evolving technology.

[5] PwC, *Global State of Information Security 2017*, http://www.pwc.com/gsiss

Note: To fully realize the benefits listed here, it's best to go with a top-tier cloud provider, such as Amazon Web Services, where there are proven layers of redundancy and security.

The key requirements for cloud-based security management

Like any technology solution, an investment in an enterprise security management solution requires due diligence, as not all cloud-based offerings provide the same functionality.

For a security management solution, it's advisable to go with a cloud solution that addresses these key requirements, as well as any other that are company-specific.

- **Open solutions**. An open solution provides peace of mind in knowing the investments made in a security management solution today will be future-proof. Additionally, an open solution provides maximum flexibility in how a solution is deployed, with simplified integrations and reduced development costs through the leveraging of industry protocols and hardware.
- **Mobility and remote access.** As mentioned earlier, anywhere, anytime accessibility is one of the reasons that companies move the security operations to the cloud. Mobile solutions provide facilities and security personnel with immediate insights and alerts from video monitoring, intrusion detection, access control, alarm management, and building management operations. The most advanced mobile solutions include a simplified user interface for easy access from laptops, tablets, or smart phones using internet protocols from any location at any time (**Figure 5**).

Figure 5

Mobile solutions deliver immediate insights and alerts from sensors and systems.

- **Solution security**. A cloud solution should meet stringent security requirements and government regulations, and consequently, only grant authorized personnel access to the system. A multilayered solution that is designed for the cloud, with SSL and TSL encryption, can protect communications between controllers, workstations, and mobile devices. Two-factor authentication can help ensure access to only those authorized users.
- **Real-time information**. Up-to-the-second information, with a current and holistic view of security operations, is a critical component of a building security solution. As events, transactions, alarms, and other instances are occurring, security teams can see synchronized updates without any latency or delays through capabilities such as push notifications.
- **Simplified integration and user experience**. In the *Security in the Cloud* survey, almost 80% of the respondents indicated that it was important to integrate security with other building and IT systems. An advanced building security management solution can bring together disparate security systems such

as access control, intrusion detection, mass messaging, and video surveillance into an easy-to-use interface. It can also simplify integration with other building systems for enhanced security and more efficient operations through a variety of open-standards-based options such as BACnet, RESTful API, and other web services.

- Enterprise control. With data storage and applications in the cloud, organizations can monitor and even control local and remote facilities seamlessly without the need for local servers. Cloud solutions give operators full control of systems from a single station – or even multiple stations at the same time in the case of redundant security operation centers – whether on site or on the go.
- Reduced operating costs. A cloud solution can help reduce day-to-day operating costs by leveraging the benefits of a provider's services. This eliminates the need for proprietary hardware, software, or servers locally or anywhere. For instance, by taking advantage of intuitive user interfaces, an organization can reduce personnel training costs while off-the-shelf devices and universal protocols can simplify support and maintenance. Even more cost savings can be realized when companies can use existing hardware with new software and controllers.

Conclusion

While cloud-based solutions are not for every company or every situation, there are clear benefits when considering moving building security management to the cloud. Innovation, security, cost savings, and other key opportunities are strategic motivations for many organizations.

Companies can make the right decision by working with trusted experts in the industry to evaluate the benefits for their specific organization. All options can be considered, and with the right information, an intelligent decision that is aligned with an organization's corporate strategy can be achieved.

About the author

Steven Turney has been with Schneider Electric's security line of business for over 18 years and is responsible for developing security strategies within Schneider Electric's North American Buildings business. He is an active member of ASIS International and has worked within the security industry for more than 20 years. Steven's expertise includes developing security solutions that mitigate risks and building a successful sales organization.