

A Guide to Moving Physical Security Into the Cloud

White paper

The use of cloud is rising across the globe as more organizations look to reap the benefits of a flexible and scalable service-based business model. The growth of cloud-based business functions and increase within the cloud services market is making way for security-as-a-service (SaaS) options that typically have been unavailable up to this point -especially for growing small to medium-sized businesses (SMBs).

The numbers support this trend, with numerous research and marketing firms reporting double digit growth in some instances for cloud services and products, as well as IT spending driven by the cloud:

\$214.3B

2019 PROJECTED WORLDWIDE
PUBLIC CLOUD SERVICES MARKET

\$466B

2020 PROJECTED IT SPENDING

- Gartner predicts that the worldwide public cloud services market is **projected to grow 17.5%** in 2019 to total \$214.3 billion, up from \$182.4 billion in 2018.
- Gartner also predicts that IT spending will reach \$3.8 trillion in 2019 - an increase of 3.2% over 2018, dominated by enterprise software spending, which is projected to grow 8.5% from 2018 to 2019, and another 8.2% in 2020, for a **total of \$466 billion**.
- A survey by RightScale in 2018 found that for SMBs, the **average spend on cloud services is about \$120,000** per year and at least 13% of SMBs still exceed \$1.2 million in annual cloud spending.
- Year over year, **the fastest-growing cloud services are serverless** (up 75%), according to the same survey.

This evolution has been triggered by the consistent adoption of cloud-based services in both security and other business units. The increase in spending is due in large part to the SaaS approach, which shifts the burden of data maintenance and infrastructure spending to integrator partners looking to incorporate recurring monthly revenue (RM) into their business model.

However, there still exists a sense of uncertainty about cloud-based security and a lack of knowledge about the advantages it provides to end users across a broad spectrum of markets. This white paper is a guide to all aspects of cloud-based services for growing SMBs, including:

- The benefits of the technology
- Common misconceptions
- Choosing the right kind of cloud-based service
- Ideal markets for cloud adoption
- Best practices for cloud implementation

WHY CONSIDER THE CLOUD FOR VIDEO SURVEILLANCE?

Cloud-based video surveillance is emerging as a viable option for physical security and video management across a number of vertical markets. But the cloud hasn't always been seen as such. For most of us in the security and IT industries, over the last few years, the term "cloud" has evolved from unknown or vaguely understood technology into a comprehensive service that can provide significant value. The cloud has proven to be a highly functional, flexible, and convenient method for SMBs to leverage as part of their strategies to protect and modernize their facilities.

When properly secured and managed, the cloud enables businesses to not only enhance operations, but also create a proactive and reliable data strategy to mitigate risk and make intelligent decisions. The cloud provides numerous benefits, including:

Centralization. One of the most advantageous components of the cloud is its ability to allow the appropriate users to access information from anywhere at any time and from a range of connected devices. All pertinent data is aggregated into one platform, and in the event of a crisis - security or business related - stakeholders can obtain the most relevant and up-to-date information in minutes for an immediate and informed response.

Scalability and Flexibility. Video is a valuable tool for any SMB when it comes to streamlining business operations and identifying the most prominent risks facing the organization. As an SMB grows or its technology systems become more advanced, using a cloud solution to store and manage video data allows for rapid adjustment and agility, reducing the complexity that might come with expansion. With the cloud, business owners can gain more insight into daily operations and ensure all organizational and security goals are met on both a day-to-day basis and into the future.

Data Security. While the security of data in the cloud is a highly discussed issue, the fact of the matter is that with proper protocols in place, the cloud can actually enhance data protection. End users can reduce their security footprint through the cloud, and by utilizing practices such as vulnerability testing, password etiquette, software patches, and encryption, sensitive data can be protected from bad actors. Additionally, public cloud providers have invested significant funds into ensuring their networks are protected and that their services provide the utmost uptime - it's critical to the business model to do so. This approach enables SMBs to have peace of mind that security and reliability are taken care of.

Automatic Updates. The cloud takes the burden off of limited IT departments when it comes to system management, as upgrades and security fixes are automatically installed. Cloud services are therefore exceptionally beneficial for organizations with a small - or nonexistent - IT team, as it takes maintenance and operational concerns out of their hands.

Cost-effectiveness. The investment in a cloud services model can be much more affordable than a hardware-based model. Deploying a cloud-based solution substantially reduces an upfront capital investment, introducing more of a service-based arrangement instead where users pay for the amount of video data, storage, and add-ons they use.

COMMON MISCONCEPTIONS

Over the last 10 to 15 years, the cloud has consistently gotten a bad rap for a myriad of reasons, including security concerns, usability, management, and unreliability. However, as the technology becomes more advanced and innovators learn more about what it means to design a product or service with security at its core, that view of the cloud is changing for the positive. When considering cloud, it is important to distinguish myths from facts.

Myth #1: The cloud is not secure.

This is probably the biggest misconception about the cloud that many integrators and manufacturers hear from potential users. Security of the cloud is imperative for top cloud service providers, such as Google Cloud Services or Amazon Web Services; their businesses depend on it. When a cloud service provider does not provide the proper protocols to protect data, it can be potentially dangerous for users. Using a public cloud service is often more secure than on-premise solutions that may be outdated or have unmet protocols in place. Public cloud services have protocols in place to ensure data is encrypted and protected from the moment it's collected to when it's transmitted via the cloud.

Myth #2: Cloud is only for SMBs.

While many Video Surveillance-as-aService (VSaaS) providers today focus on the SMB market, many providers target the mid- and enterprise-level markets. As VSaaS offerings mature and gain more functionality, they will become more attractive to enterprise-scale customers; especially those organizations that have a large number of distributed sites that require reliable monitoring and security management (with the benefit of scalability).

Myth #3: Cloud uses too much bandwidth.

One of the biggest concerns for customers looking to move to a cloud-based video system is bandwidth. While these concerns are valid with the amount of data that needs to be transferred from the cameras to the cloud. VSaaS providers and camera manufacturers are continuously implementing ways to limit the amount of bandwidth used. Compression technologies such as H.265 and smart codecs can limit the amount of bandwidth used. Additionally, the ability to upload video to the cloud based on a schedule can be used in an effort to limit the bandwidth used during business hours when other critical business systems are running.

Myth #4: Cloud security is too difficult to manage.

In contrast to on-prem solutions, cloud security is actually much simpler to manage. On-prem solutions can be hardware-heavy, requiring multiple racks of servers, cables, power sources, cooling mechanisms and much more space. And all of these elements, once in place, must be updated regularly, usually by on-site staff. Hardware is also prone to failures, which can mean a disruption in service and in some cases, the inability to access critical data. Cloud-based services, however, require little to no hardware,

and maintenance can be done remotely. This means that as vulnerabilities are discovered, they can almost immediately be addressed. Similarly, built-in failsafes in place in the event of an outage of a data center so that if one site goes down, the information is saved in another location until service can be restored (in most cases, these failsafes are so effective, users never notice a delay in service).

Myth #5: You need someone on staff who is specialized in cloud security.

Many cloud services on the market are built with ease-of-use in mind, utilizing an intuitive, customer-centric platform by which to control the system. While it can be beneficial to have staff that specialize in cloud security, the simplicity of cloud allows system integrators to be an ideal partner for delivering and supporting cloud services. Part of the appeal of working with an integrator partner to implement a cloud-based service is the fact that these teams are uniquely qualified to train and work within the parameters identified. Integrators often possess the knowledge necessary for networking and working within the cloud, which is ideal for companies that may lack IT resources with this expertise.

Myth #6: Traditional IT servers provide more control.

This myth is the result of misinformation about how the cloud can benefit organizations. On-premise hardware failures, for example, can cost organizations lost data and information, while cloud-based solutions have the advantage of networked backups. IT pros may also want to retain control over the protocols in place to protect on-site data, but this requires a significant amount of staff and resources that can already be strained by high demand within an organization.

OPTIONS FOR INCORPORATING CLOUD

Most SMBs are likely familiar with traditional, on-premise surveillance solutions. These require organizations to use proprietary architecture to run the solution within its own data center. All security operations and monitoring therefore take place in house, allowing SMBs to benefit from a strong sense of reliability and freedom. Additionally, there are a number of SMBs that prefer to be in control of all decision-making and data handling, which makes an on-premise solution ideal for customized configuration that is unique to the organization's needs.

However, organizations that are interested in incorporating the cloud into their overall security posture have three options to consider:

Private Cloud

Some organizations choose to deploy their own storage systems in-house, implementing cloud computing and storage technology.

Usually, this is managed via internal resources, which can be costly and require exceptional IT knowledge and a dedicated management team. Private cloud offers the usability, scalability and flexibility for which cloud is known, and is a viable option for those businesses looking to adopt cloud technology (but on their own private network to limit access to outside users).

Private cloud, however, is not without its limitations. As previously mentioned, staffing can become a problem, as the oversight and management of this storage solution requires extensive training and knowledge of the best practices for protecting data being transmitted. In general, private cloud systems have a higher cost of ownership as a result of the hardware investments that need to be made and maintenance costs.

Public Cloud

The public cloud refers to the delivery of hosted services over the internet, making it possible to shift the storage and management responsibility to a service provider or into the hands of the end user. The public cloud is an optimal surveillance solution for SMBs looking to experience scalability and flexibility

when it comes to streamlining video and business operations, as well as identifying the most prominent risks facing the organization. If an SMB is looking for a way to centralize surveillance and data management, the public cloud is an excellent choice. Cloud solutions also provide automatic updates and a long-term relationship with the integrator for continued support, which can be helpful for SMBs that need extra assistance. Public cloud providers include Google Cloud, Amazon, or Microsoft (to name a few).

However, the public cloud may not be the best option for SMBs that don't have the bandwidth required for streaming footage. The cost of streaming video 24/7 can certainly add up, and if a business demands extensive live viewing, an on-prem solution could make more sense. Additionally, while the security of data transmitted to the cloud can be ensured through practices such as encryption, if an SMB has to follow strict compliance regulations, such as GDPR or FDIC requirements for a bank or financial institution, or isn't fully confident in cloud security, shifting to this method may create apprehension.

Hybrid Cloud

Hybrid cloud models allow for a mix of on-premise, private, and/or public cloud services. For simplicity's sake, Forester Research defines hybrid cloud as "one or more public clouds connected to something in my data center. That thing could be a private cloud, that thing could just be traditional data center infrastructure.

Workloads and data are then able to move freely between the various pieces, creating an advantage for SMBs that are looking for a balance between the two aforementioned options – and a solution that is tailored to their needs. For example, if demand increases and exceeds the limits of an SMB's on-prem solution, the cloud solution can take over. Additionally, many headquarter locations are a good fit for an on-premise solution, which can make sense for the business. However, the addition of satellite offices across a city, state or even country, might require fewer cameras generating less data. In this case, the addition of cloud services functionality can save a business significantly on the cost of server hardware and installation, while offering a breadth of additional advantages like scalability.

A hybrid cloud solution may not be the right fit for an organization if it requires extremely high speeds and data transfer, as it can create integration and capability issues. Hybrid cloud models also still require cloud expertise and management through an IT team, which may not be readily available within the organization.

CUSTOMER USE CASES FOR THE CLOUD

Cloud-based services are growing in popularity among all kinds of SMBs and enterprises because of the scalability, flexibility, and ROI they provide. However, several market segments in particular stand to benefit significantly from their use:

Retail and Hospitality

In today's economy, retailers are concerned about more than simply loss. Their success depends on excellent customer service, effective merchandising, and maximizing both online and offline sales opportunities as the industry evolves. Now more than ever, it is paramount that retailers implement multifaceted solutions to improve both security efforts and business operations. Utilizing technology that not only provides forensic evidence for investigations of a specific incident (such as a theft or slip-and-fall claim), but also takes video data and applies certain analytics capabilities to provide insights, can help provide a retailer or hospitality-focused business with valuable insights that can guide business optimization.

In today's economy, retailers are concerned about more than simply loss. Their success depends on excellent customer service, effective merchandising, and maximizing both online and offline sales

opportunities as the industry evolves. Now more than ever, it is paramount that retailers implement multifaceted solutions to improve both security efforts and business operations. Utilizing technology that not only provides forensic evidence for investigations of a specific incident (such as a theft or slip-and-fall claim), but also takes video data and applies certain analytics capabilities to provide insights, can help provide a retailer or hospitality-focused business with valuable insights that can guide business optimization.

By using integrated analytics with video stored in the cloud, retail businesses can predict and prevent incidents with intelligent data analyses. Users can create custom alerts based on a specific set of potential triggers or vulnerabilities, allowing an immediate response and the ability to mitigate a situation before an incident occurs. For example, the order in which customers are situated throughout a store at any given time can provide increased insight into the effectiveness of operations and the possibility of security threats. A video cloud service can also leverage heat maps to indicate dwell times, such as when an employee lingers in stock rooms, parking lots, or other areas outside of normal business hours. This can then prompt a notification for possible theft or tampering, allowing managers to dispatch a swift response to the scene.

Additionally, heat maps can determine crowd levels and customer traffic patterns, delivering intelligence around which areas of the store are attracting the most interest. This data can be used to augment marketing efforts, as well as reducing shrink, especially in the event of extensive dwell times in aisles featuring high-priced merchandise.

Property Management

Property management companies are responsible for multi-tenant complexes, office buildings, or other spaces where people live and work, which can be challenging for safety and security initiatives. These entities must often enforce strict policies, making improvements and monitoring potential issues for numerous sites. These companies are an ideal fit for a cloud-based security service because of the need to address incidents that may arise at any geographically dispersed location without the resources to have an operator watching all of the cameras 24/7.

Common areas, such as parking lots and garages, gym facilities, stairwells, and indoor and outdoor recreation areas, require a unique approach to security, and can benefit from video surveillance in the cloud coupled with customizable analytics that can determine dwell times to indicate loitering, usage information for certain areas of a building, and potential threats (such as a suspicious car in a no-parking area). This kind of customizable alert can create a valuable tool for managers looking to maximize security investments while also gathering actionable insights to help in decision-making, such as staffing levels at a particular location.

Professional Services Firms

Typically consisting of lawyers, architects, financial services and advisors, engineers, real estate offices, and other client-centric businesses, professional services firms are an ideal fit for cloud-based security. These firms often serve clients across multiple office locations and as a result, have a unique set of challenges with regards to accessibility, flexibility, and the protection of their distributed business locations.

Cloud-based video surveillance is ideal for this market for a number of reasons, including centralization, which allows multiple locations and branches to be monitored from a single cloud-based platform. With cloud-based video surveillance, operators are in complete control of authorizing specific users, user groups, camera views, recordings, and more. Additionally, operators have the ability to manually schedule maintenance at any location when it's most convenient for that business site.

Professional services firms can also benefit from a fully customizable solution that allows security leaders to tailor alerts based on different characteristics, such as someone in a restricted location within a building or loitering for longer than a set amount of time in a parking garage. Additionally, scalability in this market is crucial as new locations or franchises are opened and needs change. Cloud services allow this growth to happen without the addition of costly hardware and infrastructure in a new location. Instead, security leaders are able to add cameras to a location, plug them into a gateway and almost instantly access the camera feeds from a remote platform, and view that location's video feed alongside all other locations (as opposed to sometimes days worth of installs for an on-premise location).

Finally, within this space, ROI is a critical component of decision-making for technology improvements, and the cost savings over an on-premise solution that requires regular maintenance and updates (as well as a costly up-front investment) are significant.

IMPLEMENTING A CLOUD-BASED SERVICE

Despite the adoption of cloud-based services in multiple areas of organizations (think about how you save files, conduct business, and communicate with coworkers), many of these same businesses have resisted the adoption of the cloud for physical security. For those organizations ready to take this step, there are several things to keep in mind before implementing cloud-based video surveillance.

Evaluate the business and its needs. Evaluating the business model is an important first step. There are a number of questions that should be answered before pursuing a cloud-based physical security service: How many locations need to be incorporated? How many cameras per location need to be integrated into the system? Are there insights that can be captured that would help a business streamline operations? What level of support is needed?

Determine usage. Typically, SMBs incorporate video surveillance into their locations to help provide forensic evidence in the event of an incident. In most cases, live feeds aren't being watched by an operator at all times because these businesses might lack the resources to do so. Additionally, in retail and hospitality environments, there are limited to no regulatory requirements linked to the amount of time video is retained for future use. Conversely, for a bank or financial institution, retention requirements for video data is set forth by governing bodies, such as the Federal Deposit Insurance Corporation (FDIC). For institutions to remain compliant with FDIC regulations, the requirements include "maintaining a camera that records activity in the banking office."

Find a good partner. Many SMBs typically have limited IT staff with specialized expertise for something like implementation of cloud-based physical security. For these businesses, finding the right integrator partner can set a business up for success. When evaluating partners, it's important to identify whether a partner has a strong working knowledge and training of core networking infrastructure. These partners must also be able to provide insight into proper bandwidth levels (discussed next) and the ability to provide ongoing support for users.

Discuss bandwidth. Bandwidth refers to the volume of data handled and can be defined as the "data transmission rate of data across a network," according to Webster's Dictionary. This is a crucial step in determining the right kind of cloud-based service needed to meet an organization's needs. Low bandwidth can cause issues with how much data the network can handle at one time, significantly reducing the user's ability to access critical data when it's needed. Working with the right integrator partner can help an organization determine the bandwidth needed to meet its needs (and recommend internet service providers who might be more suited to deliver the right levels).

Identify support resources needed. Working hand-in-hand with an integrator partner, it's important to determine the level of support that will be needed within the organization using the service. For many, the service-based model can help ensure high levels of oversight over the system – beyond the regular security updates – to include regular monitoring. To determine this, users have to identify who will be responsible for using the system. This will help give partners a better idea of what's needed by way of support.

Customize your data sources and plan. In short: find a platform that will mold to your business model. Each organization's needs are unique, so it's critical to search for a cloud-based service that can be tailored to individual needs, whether a facility requires all cameras to run analytics through the cloud or just some of them (as well as determining the types of analytics required). It's also critical to look for a partner that only provides a plan that far exceeds the needs of an organization. The solution should be agile enough to meet all of these needs and more.

IN SEARCH OF: THE RIGHT CUSTOMER

SMBs face so many challenges in the markets they serve: dispersed locations, networking issues, numerous employees and management functions, and the challenge of finding security solutions that work within specific parameters. Cloud-based options are emerging as a useful tool for companies this size, while manufacturers aim to provide intuitive, user-centric experiences within these solutions.

For most SMBs, the focus shouldn't rest on being glued to a monitor and watching what's going on at each location; instead, leadership should have the freedom to remain vigilant about business operations and honing in on potential issues that may arise. The goal for these leaders is to shift to the mindset of being proactive rather than reactive when incidents occur and needs arise, which can be achieved through the implementation of cloud-based physical security services.

The Arcules service bundle, which includes VSaaS, Access Control as-a-Service (ACaaS), and built-in security and business analytics, provides advanced management of video surveillance data, and access control in one unified solution for SMBs wanting to take control of their time, efficiency, costs and scalability. The Arcules service works by seamlessly integrating with thousands of surveillance cameras, bringing multiple business locations into a single view and correlating data across video and access control sensors. Arcules puts consumers in the driver's seat for the security of their own facilities.

Click here for a demo and to find out more about how today's growing businesses can benefit from cloud-based services.