Cloud-Based and Hosted Access Control: Opportunities for Dealers/Integrators

Joan Engebretson, Slayton Solutions

Cloud-Based and Hosted Access Control: Opportunities for Dealer/Integrators

Joan Engebretson, Slayton Solutions

Introduction

The purpose of this white paper is to introduce security dealer/integrators and other interested parties to cloud-based and hosted access control in a vendor-neutral manner and to outline opportunities for dealer/integrators in this area, particularly the opportunity to earn recurring monthly revenue (RMR) for installations that traditionally would not have RMR associated with them.

Information for this white paper came from conversations with people involved in this market, including manufacturers, cloud providers, and security dealer/integrators, and from their websites and support materials.

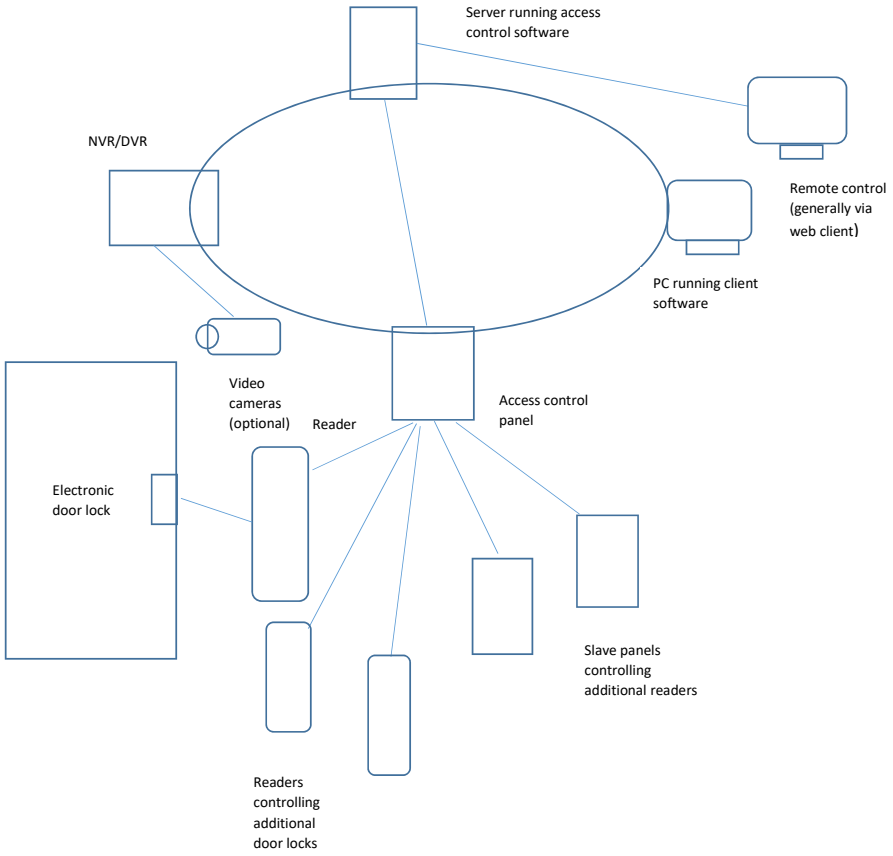
The cloud access control market is seeing strong growth, according to market research firm IHS Markit, which forecasts global sales of cloud-based access control to exceed $530 million in 2018 and to reach $1.8 billion by 2025. Sources interviewed for this report estimate that 5 percent to 12 percent of new access control jobs are web-based or hosted.

Definitions

Different people may use the same term to mean two different things. In this section, we will clarify how we will use terms such as "cloud," "hosted," "managed" and others.

Traditionally all equipment for access control systems was installed at the customer premises. Key components include a server running access control software, one or more computers running client software, readers, door locks, a master control panel, and in some cases, slave

Figure 1. Premises-Based Access Control



panels controlled by the master control panel. When slave panels are used, each slave panel is responsible for controlling one or more readers. Unlike other types of security systems such as intrusion protection or fire alarm systems, access control systems traditionally have not had recurring monthly revenue associated with them – although some customers might sign on for annual maintenance and service contracts.

With hosted and web-based access control, the server running access control software is not located at the customer premises but instead is owned and operated by the dealer or a third party. Customers avoid having to purchase, operate and maintain their own server and software.

The dealer or third-party cloud service/hosting provider typically collects a monthly fee on a per-door basis for providing the service. If a third-party provider is involved, the dealer reselling the service typically passes on the monthly fee to the customer, usually with a markup. (More information about this can be found in the section titled "Economics of hosted and web-based access control.")

Hosted Services

The cloud-based software supporting a cloud-based access control offering may be the same client/server software that an end user could buy from manufacturers such as AMAG Technology, RS2 Technologies or others. Some central stations or other companies that operate data centers use this approach to offer access control services. Importantly, some companies that use this method to deliver hosted services have done software development of their own to add capabilities not included in the software as delivered by the manufacturer or to overcome limitations traditionally associated with moving software designed for the customer premises to a remote location.

When software designed for the premises is moved to a remote server, that server typically will support multiple end users. With this option, end users can still interact with the system using a computer with client software but rather than connecting to the server software over a local area network, connection is over a wide area Internet/IP connection.

If end users are primarily responsible for adding and deleting users, adjusting schedules and other functionality, the offering is often described as a "hosted" service. If the dealer or a third party takes on those responsibilities (at the direction of the customer), the offering is often described as a "managed" service. Web-based services described in the next section also can also be offered as a managed service.

At least one company – Cloud 9 – offers hosted services on a wholesale basis to security dealer/ integrators using client/server software. The dealers then resell the services to their customers, eliminating the need to create, manage and maintain their own hosted offerings.

In this paper, we will use the term "hosted" services to encompass services that rely on traditional client/server access control software running on a server operated by the dealer or another outside party.

Web-Based Access Control

As an alternative to hosted services, some companies have developed access control software designed specifically to run in a remote data center and not available in a premises-based version. Examples of companies offering these options include BluBØX, Brivo Systems, Feenics, Kastle Systems and Paxton Access.

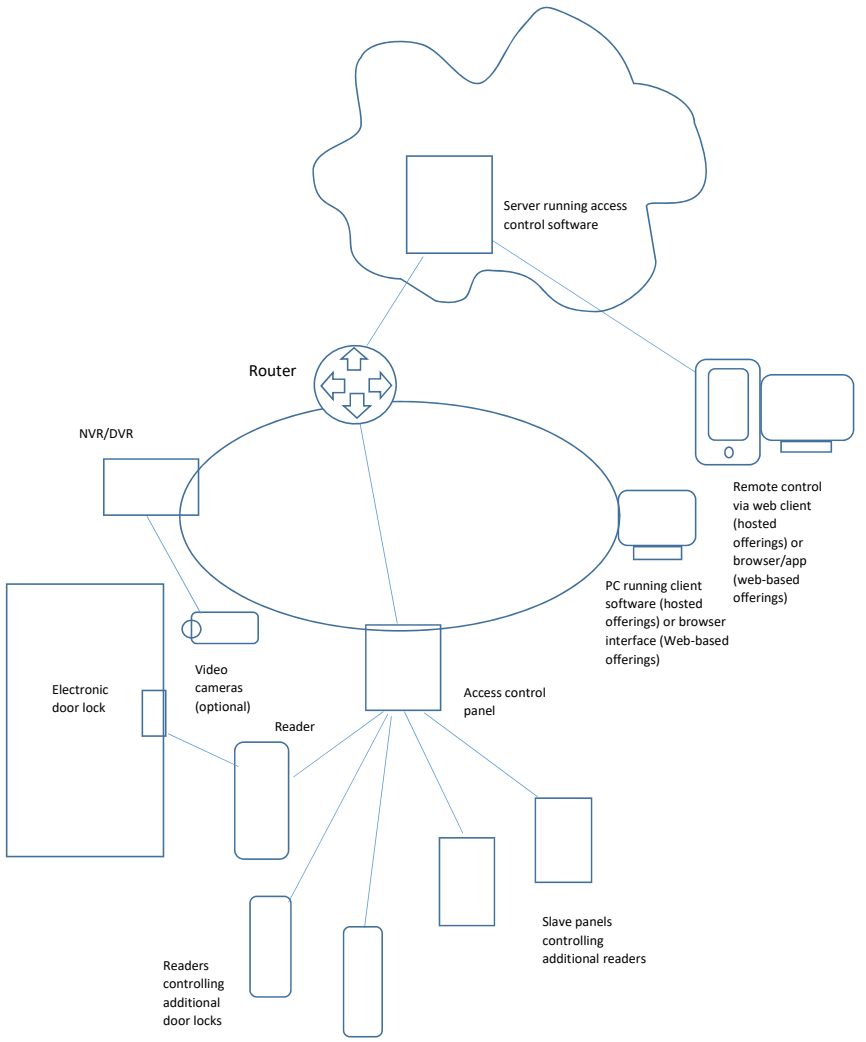
Unlike offerings based on traditional access control software, offerings designed for the cloud do not use a client-server approach. End users and/or dealers interact with the service via a browser interface or app, eliminating the need to use a computer onto which client software has been loaded.

We will use the term "web-based" to describe these services. The term "software as a service" (Saas) or, more specifically "access control as a service" (ACaaS) also could be used to describe these services.

Some developers of web-based access control offer services on a wholesale basis to security dealers, while others sell directly to end users. Wholesale offerings may include a special interface for the dealer, which the dealer can use to support managed services.

Some developers may have offerings in more than one category. For example, Honeywell offers premises-based access control, a client/server-based offering designed to be deployed in a hosted environment and a web-based cloud access control offering.

Figure 2. Hosted and Web-Based Access Control



Sales Trends

Based on the terminology used for this report, managed services currently generate the majority of cloud-based access control revenues, according to IHS Markit. But non-managed services, including hosted and web-based access control, have a larger share measured by systems sold, IHS Markit says.

NIST Cloud Definition

The National Institute of Standards and Technology (NIST) defines cloud infrastructure as "a collection of hardware and software that enables five essential characteristics," including:

- on demand self-service
- broad network access
- resource pooling
- rapid elasticity
- measured service

A purist would argue that hosted or managed services based on traditional access control software do not meet this definition because they do not support "rapid elasticity." For example, the party offering hosted and managed services based on traditional access control software typically purchases software from the manufacturer supporting a maximum number of doors, which means that service cannot be rapidly scaled once that number has been reached.

Not all customers are concerned about details such as those, however. To many of them, cloud-based access control is a service that moves access control software to a remote data center.

Benefits of Hosted and Web-Based Access Control vs. Premises-Based Solutions

In comparison with premises-based solutions, customers get a range of benefits from either hosted or web-based access control, such as:

- they convert some capital expenses to operational expenses (an approach that may be preferred by some customers, and which may be more easily approved by financial decision makers within the customer organization)
- overall cost savings (see details in Economics section)
- fewer in-house resources that must be dedicated to access control
- more time to focus on their core business
- software functionality can be updated more regularly, thereby keeping system more up-to-date
- convenience features such as remote locking/unlocking for authorized users
- ease of running reports
- enhanced convenience for multi-location enterprises

There also are some significant benefits to dealer/integrators of hosted and web-based access control versus premises-based systems, including:

- RMR, which in turn may help increase company's valuation should the owner someday want to sell
- easier to install and maintain in comparison with a premises-based system
- helps build ongoing relationship with the customer

Benefits of Web-Based Access Control vs. Hosted Access Control

Companies that offer web-based access control state the following benefits in comparison with hosted services:

- The customer does not need computers with client software installed on them.
- Working with customer's IT department may be simpler (because a port does not have to be opened as required by some client/server offerings designed for a local area network – see details in "Client/server vs. web architecture" section).
- Customer remote access to the system (via a browser or app) may provide more sophisticated functionality and may be simpler to implement in comparison with remote access to a hosted solution (see "Remote connectivity to access control systems").
- Some cloud service providers also offer cloud-based video surveillance or cloud-based versions of other systems, which may support a wider range of capabilities in comparison with what can be obtained using a hosted approach (see "Integration with other types of systems").
- It can be less risky for dealers, who would have to invest in servers and software licenses based on system capacity in order to offer a hosted solution, and would then have to recover those costs through sales to individual customers. Selling web-based access control services (or using a resale approach to hosted services) lets the dealer use a pay-as-you-grow approach.
- System may have greater redundancy as data center infrastructure is likely to be redundant, while options delivered from a central station or some other facilities may not have the same level of redundancy. A dealer opting to offer hosted services can make the decision to build redundancy into that offering but doing so may add to cost and complexity.

Benefits of Hosted vs. Web-Based Access Control

There are some instances in which a hosted approach can provide benefits not available from web-based offerings, such as:

- Customers are less likely to have to replace existing control panels (see "Compatibility with existing equipment").
- Some customers may be wary of purchasing from some web-based access control providers out of single-source concerns.
- Customers wanting to outsource full management of their system may find a wider variety of hosted options available to them, in comparison with web-based offerings, although some web-based offerings are available as managed services.

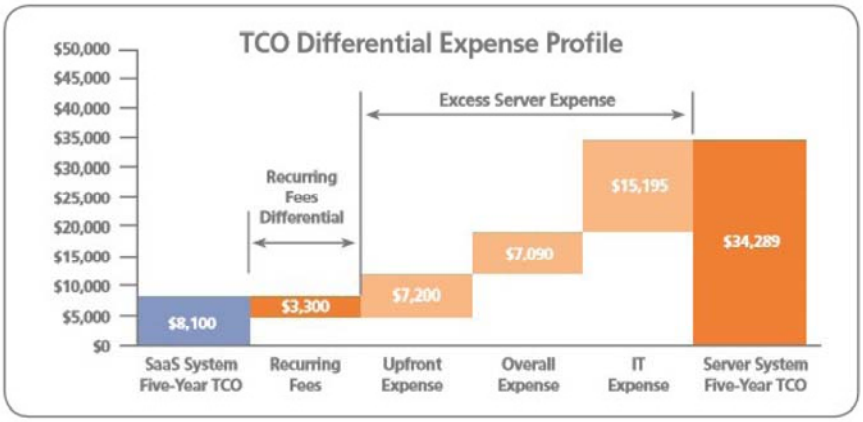
Economics of Hosted and Web-Based Access Control

Sources interviewed for this white paper said hosted and web-based access control services (not managed) cost in the range of $9–$30 per month, while managed offerings cost in the range of $15–$50 per month.

Web-based access control provider Brivo Systems estimates the total cost of ownership of web-based access control for an enterprise customer over a five-year period at $8,100 in

comparison with a total cost of ownership of $34,289 for a premises-based system.

Figure 3: Total Cost of Ownership – Web vs. Premises-Based Access Control



Source: Brivo Systems

Total savings result from savings in capital expenses, IT expenses and in other areas. Hosted access control offerings would provide some of those savings. But according to Brivo, the savings are not as large because considerably more work is required on the part of the hosting service provider to manage the system, even when it is not sold as a managed service and customers are still required to add and delete users, etc. That suggests that hosted services either will be costlier for the end user or less profitable for the dealer in comparison with web-based services.

Dealers opting to deliver hosted access control services also must purchase software based on expected capacity prior to recouping any of those costs through sales to individual customers. Depending on the manufacturer, dealers also may be required to pay an annual software support fee equal to about 12–20 percent of the license cost, sources said.

Target Markets for Hosted and Web-Based Access Control

Target markets for hosted and web-based access control fall into two broad groups, according to people interviewed for this white paper.

One group includes enterprises with multiple locations. The benefits of moving to the cloud are particularly appealing for those enterprises because the cost and resources required to support a premises-based approach are magnified when multiple locations are involved. Retail businesses also tend to be good candidates for hosted or web-based access control because such businesses are unlikely to have dedicated technical staff at each location. In addition, these companies tend to experience high levels of employee turnover, increasing the importance of access control while also complicating ongoing management of access control systems.

The other key target group is small- and medium-size enterprises that do not have technical staff. Doctors' offices, retail outlets, commercial offices and property management companies are just a few examples of the kinds of small- and medium-size enterprises to whom the idea of web-based or hosted access control is likely to appeal.

Technical Issues

Compatibility with Existing Equipment

With premises-based access control, a customer's panel generally must be from the same company providing the access control software. Therefore, providers of hosted services must adhere to that approach when they move the software to the cloud.

Web-based access control providers, by definition, create their own access control software. Some of them also offer control panels, which customers generally are required to use. This means that customers with existing premises-based access control systems would have to purchase one or more new panels in order to move to cloud-based services from those providers. Another concern is that some business customers are wary of purchasing services with such restrictions because they try to avoid purchases that are only available from a single supplier.

If instead the customer were to move to a hosted approach, there is a strong possibility that the customer would be able to find multiple hosting providers offering software from the existing manufacturer.

Not all web-based access control providers require customers to use their panel, however. Some web-based access control providers work with open hardware, specifically control panels developed from Mercury Security, with whom the cloud providers have made business and technology agreements. Several major access control manufacturers and numerous smaller manufacturers private label Mercury panels for all or part of their line, which means that customers retrofitting existing Mercury-based systems can keep their existing equipment. Before the Mercury panel can be used, however, software changes to the panel typically must be made to enable two-way web-based communications.

Those cloud providers that support Mercury panels also may be able to support panels from some equipment manufacturers that are not Mercury-based after a component board in the existing panel is replaced with one that is Mercury-based. However, there are some panels that cannot be converted to operate as Mercury panels, in which case all existing panels would have to be replaced.

Client/Server vs. Web Architecture

Traditional access control servers were designed to communicate with client software over a local area network. Because the software was not designed for communications over the Internet, client software located at the customer premises may not be able to communicate with a remotely located server over the Internet unless logical ports are opened up on the customers' routers and port forwarding is established. IT management may be unwilling to do that out of security concerns.

Access control offerings that were designed specifically for the cloud do not run into these issues because they were designed for two-way communications over the Internet and use Internet addressing conventions. If a cloud provider requires dealers to use the provider's own control panel, that panel can be designed to call out to the cloud upon installation, thereby establishing two-way communications. For those cloud providers that use Mercury panels,

the solution is to change the OEM code in the panel, thereby putting new capabilities into the panel, including the same sort of immediate dial out to the cloud upon installation.

It's important to note that at least one access control manufacturer that uses client-server software – RS2 Technologies – has devised a method to eliminate the need to open software ports and set up port forwarding in order to use its software to support a hosted offering. The company achieves this by giving dealers the option of having communications initiated by either the server or the panel.

Another advantage of web-based access control services is that client software does not have to be loaded onto a computer or other device in order for the computer or device to communicate with the access control system. Instead authorized users can use a browser interface to communicate with the system, offering greater flexibility in terms of how customers use the system. Some web-based access control providers offer smartphone apps with the goal of simplifying the user interface but these apps should not be confused with client software.

Remote Connectivity to Access Control Systems

Both web-based and hosted access control systems may offer authorized users the ability to interact with the systems from remote locations – a useful capability if, for example, an administrator wants to delete an employee from the system outside of usual business hours.

Hosted offerings based on a client-server architecture generally provide remote connectivity using web client software and may require the establishment of a virtual private network (VPN) connection in order to connect the end user to the system. However, at least one manufacturer – RS2 – supports remote control of some functions via a browser interface.

Authorized users remotely connecting with web-based access control systems designed for the cloud may do so using a smartphone app, web browser or both, depending on the provider, and generally do not require a VPN. The providers also may offer remote control of a broader range of functionality in comparison with hosted access control providers.

For example, offerings designed for the cloud may support alerts pushed from the system to authorized users. If a door remains open longer than a specified time (suggesting someone may have propped it open), the system may be able to automatically send an alert to specified administrators. In contrast, the web client software that provides connectivity to a hosted server may not support alerts pushed to it from the server. Instead, all communications may have to be initiated by the users. However, hosted offerings may be able to provide similar functionality by, for example, sending automatic alerts via email.

Another concern related to remote access to hosted systems is that certain functionality – such as an interface with a premises-based video surveillance system – may not be supported or may require the remote user to connect using a computer with a thick client installed on it. A thick client is more complex software with a wider range of functionality.

Integration with Other Types of Systems

Some customers like to have their access control system integrated with other systems such as video surveillance, elevators, heating/ventilation/air conditioning or other types of systems. An integrated access control and video system, for example, might logically associate a camera at a door with the access control reader at that door, enabling video images to the camera to be recorded or even sent to authorized users when a credential is presented at that door. Depending on the customer's preference, video also could be sent only in certain circumstances, such as when a door remains open more than a certain amount of time.

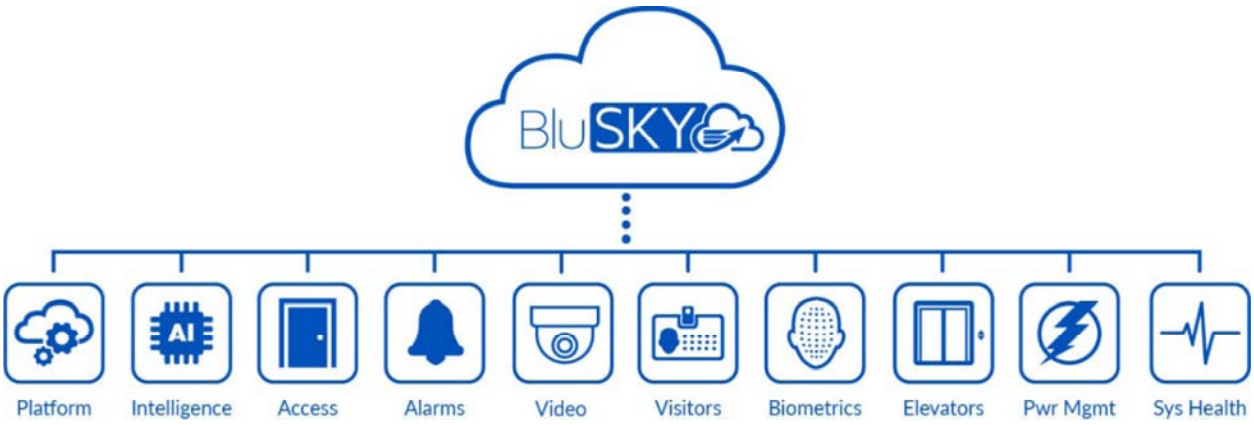
Manufacturers of premises-based access control systems typically make agreements with specific manufacturers of digital or networked video recorders (DVR/NVR) or other types of systems to undertake software development with each other to enable their systems to be integrated.

With hosted services, the access control server that needs to exchange information with the DVR/NVR, IP camera or other device is located in a remote location rather than at the customer site, which poses some challenges. For example, authorized users may have to have special "thick client" software on their computers in order to use functionality provided through the integration of the two systems and may not be able to obtain the full functionality that they could obtain with a premises-bases system.

Some providers of web-based access control services also have reached agreements to integrate their cloud-based services with premises-based systems such as DVRs/NVRs or wireless door locks from specific manufacturers. In addition, some providers of web-based access control services also offer web-based versions of other services such as video surveillance, building management or others.

In some cases, the cloud provider may have developed the software internally. In other cases, the web-based access control provider may have made a partnership with a video surveillance, building management or other software development company that offers a web-based option.

Figure 4: Some Web-Based Access Control Providers Offer Multiple Cloud Services



Source: BluBØX

In either case, the web-based offerings may be more tightly integrated in comparison with integrations involving premises-based DVR/NVRs, etc. For example, the end user may be able to access and control a wider range of functionality via a single app or browser interface. The additional web-based offerings also may offer extra-value capabilities such as video storage.

In contrast, integrated systems that use hosted or web-based access control but rely on premises-based video, building management or other systems are more likely to require the end users to use separate interfaces to interact with the two different systems.

Another integration option available to providers of web-based access control is known as cloud-to-cloud integration. This approach involves connecting the cloud supporting the access control service with another cloud that supports another type of system.

Web-based access control provider Kastle Systems, for example, has undertaken custom integrations on behalf of some accounts to connect the Kastle cloud, which supports access control and other functionality, with other cloud-based systems such as building management systems.

Cloud-to-cloud integration can enable a single interface to control multiple systems. In addition, it eliminates the need for the web-based provider to house and maintain the systems to which the access control software is integrated.

The Future of Cloud-Based Access Control

Some traditional manufacturers of access control systems designed for installation at the premises have avoided launching their own access-control-as-a-service offerings using either a hosted or web-based approach. But as cloud-based access control becomes more popular, that is likely to change. Generally, security manufacturers try to avoid competing with their dealers, but even if the products that manufacturers launch are offered only on a wholesale basis, the impact could be substantial – particularly considering that the manufacturers' cloud offerings may be designed to overcome traditional shortcomings of client/server systems.

Should that happen, hosted offerings based on that manufacturer's software may remain viable, but differentiation through custom software development is likely to become increasingly important. And dealers that have not yet launched hosted offerings but are considering doing so will want to carefully weigh the likelihood of their chosen manufacturer launching a cloud service and whether reselling the manufacturer's cloud offering might be a less risky alternative.

For web-based access control providers – and dealers who sell those services – the question will be whether they can stay a step ahead of any traditional manufacturers that opt to launch web-based offerings.

A range of technology developments are important to keep an eye on as various players look for ways of differentiating their offerings in an increasingly crowded marketplace.

We are likely to see a greater emphasis on tight integration with other systems such as video management or building management systems as a means of simplifying customers' interface with the integrated systems. Expect to see more partnerships between web-based access control providers and providers offering other types of web-based systems.

Cloud-to-cloud integration also is likely to become more commonplace moving forward and could be an important differentiator for web-based access control providers that embrace the concept and the dealers that sell the services of those providers. Dealers will want to pay attention to developing standards that aim to simplify the process of integrating cloud services from multiple cloud providers.

Wireless locks also are an important development area. As locks begin to take on functionality traditionally associated with separate readers and even access control panels, some people interviewed for this white paper envision a day when access control systems might consist primarily of wireless locks that communicate with the cloud. Sources noted, however, that such systems are likely to have a premises-based gateway device to provide security for multiple locks, eliminating the need to embed that functionality into each lock and potentially offering a more effective solution.

Summary

The cloud access control market is seeing strong growth as enterprises seek to minimize capex and minimize the need to install and maintain premises-based equipment. Offering cloud access control presents new recurring revenue opportunities for security dealers, as payment is generally made on a per-door, per-month basis. Traditionally, access control system installations have not had RMR associated with them.

With cloud access control, the software and server supporting the system are located in a remote data center operated by a dealer or a third-party provider. There are two basic types of cloud access control – hosted and web-based.

Hosted access control uses software and servers originally developed for use at the customer premises but moves the software and server to a remote location. It also retains the client/server approach initially developed for the system, and therefore may require client software on any devices to which the system connects. Additionally, it may require customers to open ports and enable port forwarding on their routers. If a customer retains responsibility for administering the system, it is considered a hosted service. If the hosting provider takes on that responsibility, it is considered a managed service.

Web-based access control uses software designed specifically for operation in a data center cloud and therefore authorized users can access it through an app or browser interface, eliminating the need to install client software or to open software ports or to enable port forwarding. With web-based access control, the customer may retain responsibility for system administration or the dealer may offer a managed service by using a dealer portal to interface with the web-based system.

Advantages of web-based over hosted access control include eliminating the need for customers to use computers with client software installed on them, fewer concerns on the part of the customer's IT department, and potentially easier integration with other systems and simpler remote connectivity for end users.

Advantages of hosted access control over web-based access control include avoiding potential risk of a single-source solution, which may be an issue with some cloud providers; less

likelihood of having to replace existing control panels, and greater likelihood of finding a fully managed solution.

In the future, we are likely to see more manufacturers of traditional access control systems moving to a web-based approach. In addition, we may see tighter integration of cloud-based access control systems with other cloud-based systems – and some of these integrations may be based on a cloud-to-cloud approach, especially as standards mature to support that approach. Another trend to keep an eye on is a move to minimize the amount of equipment required at the customer premises through the use of intelligent wireless locks.

Joan Engebretson has been writing about technology since 1992. Previously she was a product marketing manager for security system manufacturer Ademco, which was later acquired by Honeywell. Engebretson has been a regular contributor to *Security Distributing & Marketing Magazine* since 2004, and has a BA in journalism and an MBA from the University of Michigan.

In 2001, Engebretson won a gold award from the American Society of Business Publication Editors for her commentary. In 2009 she won Best Online Column in the Min Editorial & Design Awards.

APPENDIX: Companies Researched for this Report

Alarm.com
Tysons, VA
https://www.alarm.com/

AMAG Technology
http://www.amag.com/en-US/Resources/White%20Papers/

Blubox
Andover, MA
http://www.blub0x.com/

Brivo Systems
Bethesda, MD
https://www.brivo.com/

Cloud 9
http://www.cloud9acs.com/

Dynamic Security, Inc.
Edison, N.J.
http://www.dynamicsecurity.org/

Feenics
Ottawa, Ontario
http://www.feenics.com/

Honeywell Systems
Louisville, KY
http://www.honeywellaccess.com/

IHS Markit
London, U.K.
https://ihsmarkit.com/

Kastle Systems
Falls Church, VA
http://security.kastle.com/

Kingdom Security
La Porte, TX
http://www.kingdomsecurity.org/

Lenel/United Technologies Corporation
http://www.lenel.com/

Paxton Access Inc.
Greenville, S.C.
http://paxton-access.co.uk

RS2 Technologies LLC
Munster, IN
https://rs2tech.com/RS2WebApp/

Tyco/ Software House
Westford, MA
http://www.swhouse.com/