Call Us Today
(717) 620-3042

507 N. York Street
Mechanicsburg, Pennsylvania 17055

SIX REASONS WHY CLOUD-BASED ACCESS CONTROL IS RIGHT FOR YOUR COMPANY

Your guide to asking the right questions while selecting a Cloud-based access control system

WHAT IS CLOUD-BASED ACCESS CONTROL?

Before we begin asking the questions relevant to selecting a Cloud-based access control system, we need to define exactly what it is. Simply put, it is an access control system where the login/management server lives in the cloud as a Software-as-a-Service (SaaS) model. In a traditional access control model, local card readers, locks, sensors, etc. are connected to reader interface boards. These reader interface boards then communicate to an on-site server where all programming, system management, maintenance and back-ups take place. In the Cloud-based model, this main server is moved to the "cloud".

The cloud is a data center environment that shares computing resources and utilities. When a management user logs into the access control system to make changes, they are logging into the server in the cloud instead of a server that they own and manage at their facility. All other features of the access control system remain the same as with the traditional model. This document will outline the reasons why hosting your access control server in the cloud is advantageous to a company.

#1 NO LOCAL SERVER

On-site servers are the bane of just about every company's existence. They require a safe, secure and clean environment. They require redundant power. They require application software updates as well as operating system updates. They require virus protection and firewall protections from outside hackers. They require backups. And they require in-house expertise; an IT professional who knows how to do all these things. In short, they are expensive and time consuming to maintain.

This is one of the best advantages to selecting a Cloud-based access control system. All the items listed above are eliminated. With this solution, there is no local headend or on-site server. The server is now located in a remote data center and operated by the access control manufacturer. The data center has redundant power and internet services. Remote backups are performed to hot servers in real-time. Virus protection and firewall maintenance is constantly updated. And your data is in a distributed format so that there is no longer a single point of failure in your system.

#2 LOWER UPFRONT INSTALLATION COSTS

The cost of moving into a new space can be overwhelming. And installing a full-featured stand-alone access control system in your office can add dramatically to those costs. When you decide to go with a Cloud-based access control system, the initial upfront installation costs are much lower. In many cases, 30%-50% lower than a traditional system. The main reason is that you are not purchasing a local server and software. This is a significant cost related to a stand-alone access control system. The second reason is that connection to the data center servers is offered as a SaaS product (Software as a Service), which is now being referred to as ACaaS (Access Control as a Service). This allows much of the installation costs to be spread out over the extended subscription costs of the service.

#3 ACCESS THE SYSTEM FROM ANYWHERE

We've already established that your data now lives in redundant servers in the cloud. And those servers are connected over the Internet to the local access control data gathering panels located in your facility. So how do you access your data and your systems administration functions? By simply opening any web browser, from inside or outside your company's network, and pointing to the access control cloud servers. The process is the same whether you are sitting at your office desktop computer, on your laptop in your home, or from your smart phone while on vacation. There is no dedicated PC needed or client software required. Once you point to the cloud server from your browser, you enter your secure credentials and you have access to all your company's access control system, limited only by your administrative permissions. Once you've securely gained access to your company's data, and you have the proper administration level, you can perform all the necessary system administration functions such as:

- Add/delete cardholder/user access
- Run reports on card activity
- Set up alerts or automated reporting
- Perform remote door functions – locking/unlocking
- Perform a system lockdown

If you don't have the internal resources to perform your own systems administration, your installing integrator will provide you with these services through your Service, Maintenance/Monitoring contract. Simply email your request such as add/delete a user and your request will be performed remotely and confirmed with you. If you have an immediate request such as unlocking a door, you can call the support number and have an operator perform the function for you in real time.

#4 SCALABILITY

There is nothing more difficult in business than planning your future growth. Having an access control system that is scalable without major additional costs is key. With Cloud-based access control, you never have to worry about software license restrictions, server capabilities, or headend controller upgrades. Adding additional doors is very linear. For every 2 doors that you install, a new reader interface module is installed at your facility and connected to your network. There can be an unlimited number of reader interface modules installed with no additional headend system hardware or software needed. These boards connect to the Cloud-based servers and are configured by your installing security contractor.

In addition, the bandwidth required on your network for the transmission of these reader interface modules is very low.

The latest card reader and credential technologies can be installed and upgraded at any time. Whether you are looking for standard proximity, smart card integration, biometrics, or encrypted Bluetooth, they are all compatible with the reader interface modules and are easily scalable and upgradable. Many users are now integrating a combination of smart proximity card technology along with virtual credentials that allow smart-phone use to unlock doors by users.

#5 ONE CARD/CREDENTIAL SOLUTION

When a tenant moves to a new office location, they often find that the base building management company has an existing card access system that controls the common doors, elevators, and parking gates for the building. The base building often refers their "preferred" security contractor to the new tenant. This can lead to highly inflated prices to the new tenant and being locked into a system that doesn't fit the tenant's needs.
With a properly designed Cloud-based access control system, you can install your own system on your tenant doors and utilize the base building cards/credentials provided by the landlord. After all, you don't want to, or ever need to, carry multiple cards.
This approach allows you to control your own facility without having to be tied into the base building's system. Your installing security integrator will work directly with your landlord to get a list of all credentials issued to your company for base building access and will upload that information into your system so that it can they can be programmed accordingly.

#6 SERVICE, MAINTENANCE & MONITORING

The key to successful ongoing operations, after an installation is completed, is a comprehensive service and maintenance plan. Access control systems are essentially living, breathing systems that get constant use, wear and tear. It is inevitable that mechanical parts will eventually wear out, shift out of alignment, or break. And as Murphy's Law would have it, it always happens at the end of a work day, on a weekend, or just before an important open house. To ensure the most uptime possible, it is vital that a 24/7 service/ maintenance agreement with real-time diagnostics is provided. Your installing security integrator will provide you with the appropriate service agreement. This provides for unlimited phone support, 24/7 response to on-site issues, real-time email updates of service status, advanced replacement of parts, priority dispatching over non-agreement customers, regularly scheduled preventative maintenance visits, and real-time system monitoring at the data center level.

With real-time system monitoring, you are oftentimes notified that you have a problem before you even know about it. If a reader interface module goes off-line, a runaway alarm occurs, a power outage happens, or a high-level invalid transaction is being performed, you will be alerted by the system.

The scheduled preventative maintenance visits are critical to keeping your system running smoothly so that service interruptions and inconvenience is kept to a minimum. At these visits, power levels will be checked, back up batteries tested, door locks examined, and reader function tested on all doors. A properly structured service and maintenance agreement gives you the comfort of knowing that the system is operating at peak performance and that you get quick response when it's most important to you.

ABOUT BLACKCSI

BlackCSI is a Pennsylvania integrator specializing in electronic access control, voice over IP and structured cabling systems installations. BlackCSI has been installing and servicing Entry-Master security control systems since 2008 and is the most experienced integrator of Entry-Master systems in the Pennsylvania area.