Understanding Cloud Services for Access Control

**Lose some hardware.
Gain new advantages.**

Introduction

Cloud computing has been a hot topic in recent years, initially for storing assets such as shared files and backups, then for accessing remote computing services, and most recently for using cloud-based software that doesn't even get installed on your computer. Today, cloud services are starting to be offered for security applications.

What is this all about? Why is "the cloud" such an exciting topic, and what could it mean for security organizations and specific security applications such as Access Control? Is it more secure and reliable, or is it less secure?

This paper will explain what all the fuss is about, first by explaining cloud services in general, then by focusing specifically on Access Control. By explaining how cloud services change the way Access Control can be implemented, we will gain insight on the potential gains of this technology for an important security application, but will also better understand several potential pitfalls and how to avoid them.

Cloud Services

For the purposes of this paper, the term "cloud services" will be used to describe the combination of one or more distinct, but related functions, including for example:

- "cloud storage" for holding or storing data
- "cloud computing" for making use of remote processing power,
- "SaaS", or "Software as a Service" for making use of remotely located software

The cloud itself is the entire network infrastructure and the large number of connected data storage and processing devices. From the user's perspective, it isn't clear exactly where the data is being stored, and the user may not care. In reality, of course, it is stored somewhere –

but depending on the type of service and the resources available at that moment, data may be stored in more than one location, or even split between locations.

The first thing to know about these new cloud services is that these functions are not new at all – they were invented in the 1960's in the early stages of developing the ARPANET, which formed the basis for the Internet of today. Cloud storage was offered commercially as early as 1983 by consumer internet pioneer CompuServe, and by the mid-1990's AT&T was offering additional services positioned as an "electronic meeting place".

Several factors have made today's landscape much more fertile for cloud services of all types. Some of the most important of these factors include;

- Increases in the capacity of storage devices such as hard drives
- Decreases in the cost of storage devices such as hard drives
- Technical advances in storage strategies such as drive striping, error correction, and others
- Improved server hardware and software to allow more efficient use of shared resources among multiple users simultaneously
- And perhaps most important of all, improvements in network access, speed, and reliability that have been broadly deployed

Without these important technical enablers, cloud based services could not be available broadly today.

#52293605

The Nature of Cloud Services

There are several characteristics of cloud services that stand in contrast to standard on-premise computing, including:

Accessibility: This characteristic is the most significant driver for cloud services. The primary point of these services is their easy access and connectivity from anywhere, at any time – thereby disconnecting the historical link between the physical location of the computer and the user of that device. After implementing cloud-based services, any user who has access to a connected data network can access and use the stored information and resources.

Cost sharing and shifting: Making use of cloud computing resources, depending on the specifics of the agreement, normally shifts what would have been up-front capital costs for hardware and software into lower ongoing operational costs. Companies have realized financial benefits by spreading out their costs, and moreover, have been better able to quickly increase or decrease their computing usage and costs as their needs change.

Reliability: The recent standard for computing has been using a desktop or portable computer, usually with a connection to a network. Much of the software being used, and the data, documents, images, and other materials used are stored locally on that computer hard drive or other storage device. While this may seem comforting to the user ("I know where my data is right now") it actually creates many risks due to the potential for a single point of failure in the storage device, processor, or almost any other power or critical processing chain element. In contrast, centralized data centers can be equipped with strong, redundant backup power and storage systems, and multiple computers can be connected to provide computational backup as well. In this way, the systems that provide the cloud services can be far more reliable than even a collection of individual computing resources.

Backups: As mentioned above, data centers can be better equipped to improve reliability versus on-premise computing resources. The same also applies to backup processes. It is difficult to ensure that a number of individual workers will properly back up their programs and data to protect them against loss and other hazards. In contrast, centralized data centers can have strict backup procedures to ensure that data is backed up and stored in a timely and secure manner in case it is needed.

Software Updates and Patches: As is the case for backups, it is difficult to manage a dispersed set of computing resources to ensure that all necessary updates, patches, and fixes are applied across an organization. By centralizing and formalizing the update process, compliance and security can both be dramatically improved.

Cyber and Physical Security: And, similar to the updates section above, a centralized location can be protected with strong logical and physical protections, ranging from fortress-style physical walls and barriers, to strong logical firewalls. These measures also prevent events such as theft, or damage due to fire or flood as a result of the increased level of protection at the central site. The scale of centralized data centers makes these improved protections feasible, where they would be difficult to justify for on-premise computing resources. Communications between system elements can be encrypted at all times, further improving the security posture of the system.

Benefits of Cloud Services for Access Control

By now it should be clear that depending on the specifics of a business case, organizations can access a range of benefits by using cloud services. Here are several of the key benefits of cloud services specifically for access control applications:

Lower up-front costs:

In the past, new access control installations required a large capital expense at the start to buy all the hardware, software, cabling, and installation labor to deploy a complete system. For medium-sized installations, the total budget could easily be in the range of $50k to $100k, which is easily enough to have a budget impact.

In contrast, using a cloud-based access control system would shift the cost from a front-loaded capital expense to a more manageable recurring monthly operational expense; starting as low as $30/mo depending on the size of the project.

Deployment speed:

Another benefit of using a cloud-based access control system is the speed with which new installations can be deployed. This is particularly true for installations that can make use of wireless door lock hardware, or where the access control panels and door hardware are already installed.

In these cases, there is a very minimal requirement for network connectivity, so it is relatively easy to work with existing limited infrastructure, or add a small amount of infrastructure to support the new application. For common small installations, with only 4 or 5 controlled doors, it could potentially be as simple as setting up a WiFi router – and that may be the only IT infrastructure you need for access control. Without the need for local servers, operating systems and software, installation becomes much faster and easier.

Greatly improved accessibility:

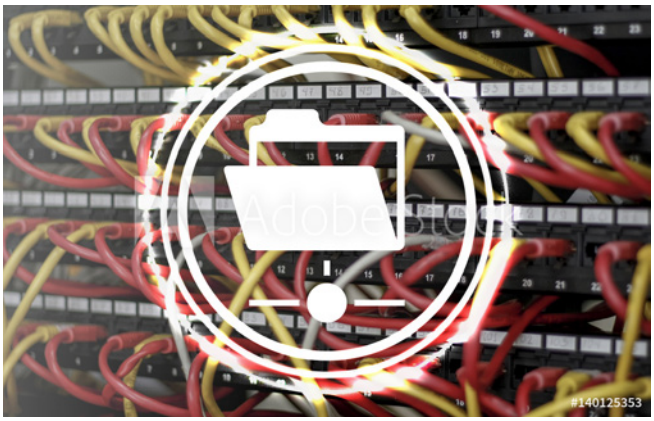
As was described above, the system can be administered by the responsible security staff from anywhere, at any time, that they have network connectivity. This functionality does not depend on VPN connectivity, so any available network access device can be used if needed, without any prior software installation or setup. This allows security staff to take any necessary access control action immediately.

Improved reliability and security:

As described above for general cloud services, using centralized data centers provides several advantages in terms of power assurance, physical protection, system and data backups, software updates and security patches, and other maintenance factors over and above what can typically be achieved with on-premise systems. This is a particular advantage for mission-critical security functions such as access control.

If there is a failure, the most likely issue will not be the central data center – instead, it will be internet connectivity. In these cases, users will not have access to management functions that are hosted at the data center location – to add a new user, for example – until the internet connection is restored. The on-site door controllers will continue to operate with the most recent set of instructions until connectivity is restored to accept new updates and management changes. If any amount of management downtime is unacceptable, then there are ways to provide backup connectivity (via cable or cellular systems, for example). As shown below, data centers also have provisions for backup operations in multiple cities that make the true backup situation even better.

And, for security, every communication between every element of the system can be encrypted. During setup, the best systems let the administrator select the level of encryption desired. The result is that the cloud-based system often has better security than even the internal network of most businesses.



Minimal required IT support:

By using centralized data centers to provide data storage and processing functions, the need to support and maintain local equipment is also largely eliminated. Since many organizations, and particularly smaller teams, do not have excessive IT department staffing, most welcome the chance to assign existing staff to other higher-priority tasks.

Clearly, this combination of cash flow advantages with real operational advantages makes the use of cloud-based access control an attractive option for consideration.

Traditional Access Control System

Here is a high-level view of a typical On-Premise Access Control system. Please refer to Figure 1 to see the system elements and their primary connectivity.

In the diagram, everything on the left-hand side would normally reside at the organization's location, up to the firewall that stands at the connection to the Internet in the outside world.

Starting in the upper left-hand corner, administrative workstations are the day-to-day computers that system administrators would use to enroll and remove staff and others into or from the access control system, take action to set rules, and generate and review any necessary reports. These workstations are connected by the internal network infrastructure (LAN) to a server room, where the access control servers are located. System client software must be installed on these workstations, making them the only places where authorized staff can manage the system, enroll and remove authorizations, and perform other administrative tasks.

Three server functions must be supported. The first is a database server to store the system settings, enrollees, and rules. The second is the application server itself, which runs the access control system software, accepting instructions from the administrator and updating the door controllers. The third is an optional web server that allows for remote access to the system.

The servers are connected to the door controllers through the facility LAN. The door controllers respond to individual access requests at the doors and open the locks for authorized staff and visitors.

Remote access is provided by a combination of webserver or VPN connection. Webserver access requires a SSL certificate for data encryption where VPN access has encryption built-in. Both scenarios require firewall and port setup before remote access can be granted.

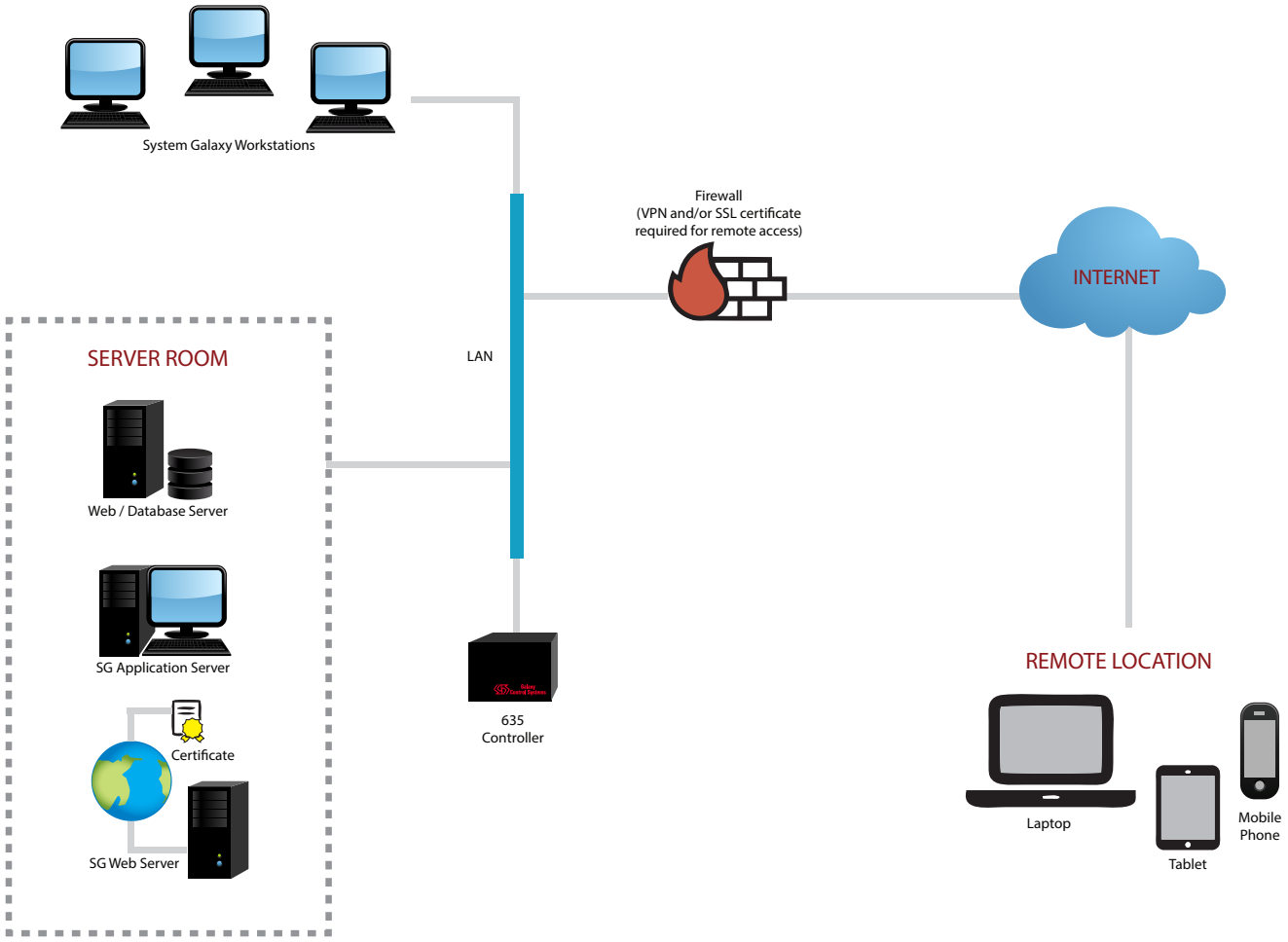


Figure 1: Typical On-Premise Access Control System

Cloud-Based Access Control System

Here is a high-level view of a typical Cloud-based Access Control system. Please refer to Figure 2 to see the system elements and their primary connectivity.

As was the case in the previous diagram, everything on the left-hand side would normally reside at the organization's location, up to the firewall that stands at the connection to the Internet in the outside world. The door controllers and locks are always located on-site in both arrangements. Note that in this case, in contrast to the previous example, there is no server room equipment located at the user site.

Instead, any local computer with LAN connectivity can be used to administer the system. The user interface, and all the enrollment, rules, and other functionality is exactly the same as the on-site version.

Instead of making use of on-site servers, the

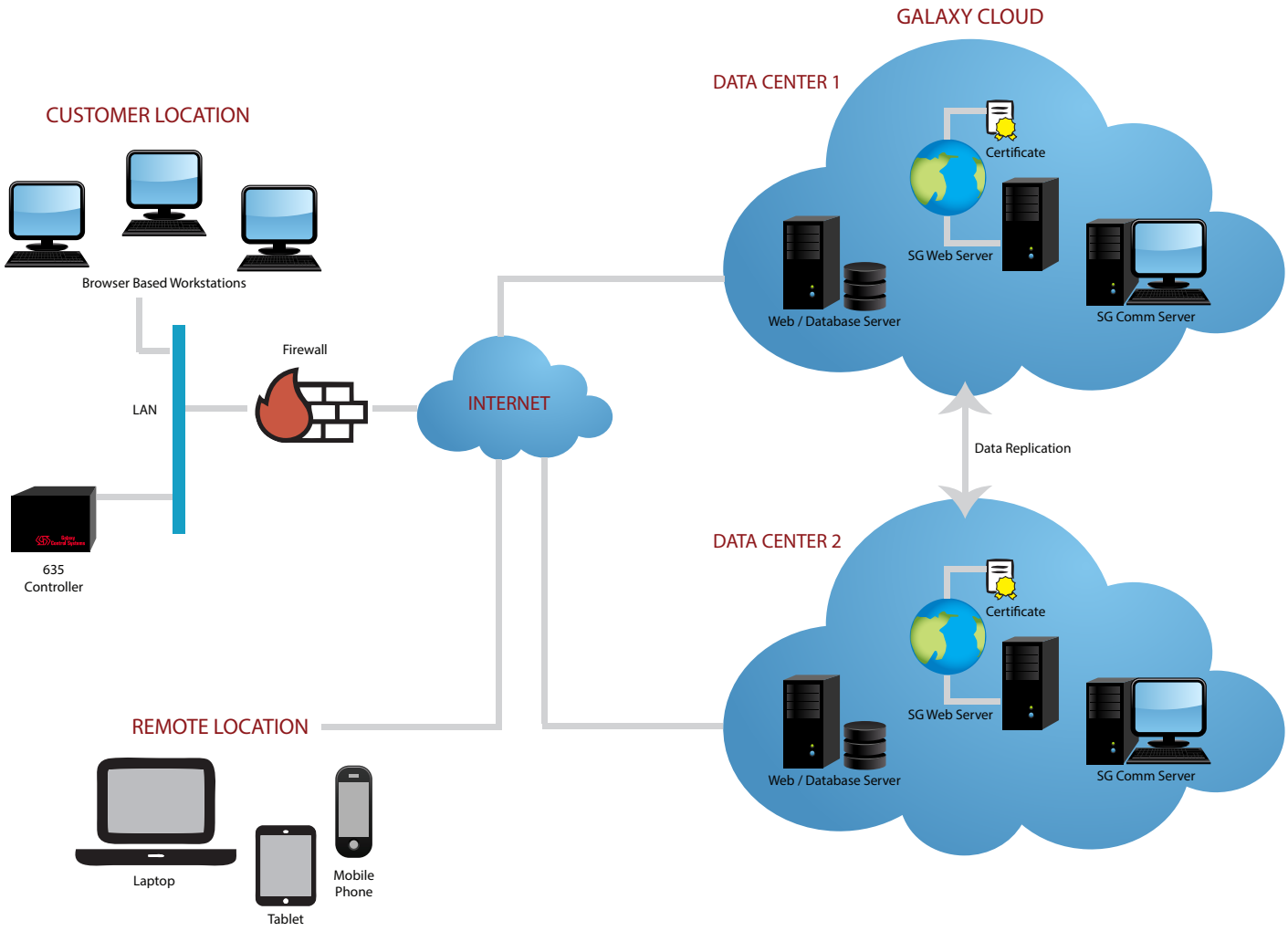


Figure 2: Typical Cloud-Based Access Control System

cloud based system makes use of servers located at a remote data center to provide the same access control system functionality, so the same three server functions are shown: a database server, an application server, and a web server – but in this case the web server is not optional.

Also note that in this typical system diagram, a second backup data center is indicated. This second center mirrors the data held in the first center, in real time, to serve as a backup in case the first center has any type of failure. In practice, the level of backup redundancy can be set to match the business needs of the end user customer.

Lastly, note that because the system makes use of a web-based interface, remote users with proper authentication can access the system from anywhere they can reach the internet, and do not require any specific software installed on their device beyond a normal web browser.

Decision Factors

Implementing a new access control system is an important step to provide safety and security for an organization. Here are some factors to consider before deciding on the right approach for your team:

Up-front cost: Installing a new access control system, or even significantly upgrading an existing system, can be a line item on most company budgets. Even smaller systems can require an up-front capital investment. If the business case allows, the use of a cloud-based access control system will shift most of the capital requirement into a monthly operational expense instead. In most cases, a multi-year agreement will be required.

IT staffing: If the current IT staff has the capacity to accept new tasks, then this may not be a significant factor. They can take care of hardware and software maintenance, updates, patches, and similar ongoing tasks. If the IT staff is already fully occupied with important tasks, or there is no IT staff at all, then going with a cloud-based access control system removes the need for any additional internal IT support. The only internal need will be for the system administrators, the HR department for example, to register new staff in the system and make similar updates.

Need for Accessibility and Reliability: As was described, cloud-based systems deliver advantages over traditional systems with regard to accessibility and reliability. And, it is important to note that in a cloud-based system, remote users have exactly the same functionality available to them as internal users. Evaluating how important these factors are to the organization's operations will give further insight into how much weight these factors should receive in the decision process.

Conclusion

Cloud services may be new to the security industry, but they have been well established in other industries and represent an increasingly important alternative to traditional on-premise hardware and software solutions. For several reasons, Access Control is an ideal application for this technology, and it should be considered for any major upgrade or new installation going forward. If the decision is to proceed with a cloud-based implementation, work with a well-established company to choose the right level of security and the right data center locations, and the project is likely to be a success.

Galaxy Control Systems
3 North Main Street
Walkersville, MD 21793

galaxysys.com
orders@galaxysys.com
info@galaxysys.com

Phone: 1.301.845.6600
Fax: 1.301.898.3331