The Five Cs of Security as a Service

Why End-users Are Looking to the Cloud

WHITEPAPER

brivo®

Introduction

When you wake up in the morning and turn on the light, you probably don't think about the source of the power. As you switch on the television and start the coffee maker your thoughts are likely to be on the day ahead and not whether you have enough capacity to power the items you're using in your home. You're free of these worries because the power company has created a reliable service, shared among the whole community, that scales to your individual, immediate demands. The service is metered so you pay your fair share based on what you use.

The basic concept behind cloud computing is very similar to this. The Cloud is like a power plant for computing resources, ready to deliver what you need, when you need it. The Internet is like the power lines, a means to deliver the power reliably and efficiently to individual users. Many companies are creating Cloud services that you can use as you need them and pay for them as you consume them. There are already a host of capabilities grouped beneath the broad umbrella of cloud computing. These include sharing networks, computers, storage, and also software applications.

The main accelerant for the growth of these cloud services is the Internet. In the past ten years we have seen the Internet evolve from the dial–up-based "world wide wait" to the blazing fast medium for the exchange of data, audio, and video. The speed of the Internet, coupled with excellent reliability and security improvements, has made it the engine for innovation in the delivery of a wide range of services. Most of us use the Internet for much more than gathering information and sending email. We use it to manage our finances, coordinate calendars, purchase music, and back-up our files, amongst a host of other capabilities.

Software as a Service, or SaaS, is the moniker for software applications delivered via the Internet from companies such as Amazon, IBM, Salesforce.com, Microsoft, Google, and others. SaaS is contrasted with the traditional "shrink-wrapped" model for application delivery where the user installs and configures the software on a machine they own and maintain. Growth trends for SaaS are strong: Gartner, Inc., predicts the SaaS market will continue to grow at more than 22% per year[i] and that by 2011, over 25% of new software systems will be delivered as SaaS applications.[ii]

So why is SaaS emerging as the dominant computing model today? The answer is because of the way the technology directly addresses the key needs and concerns of consumers. We call these fundamental needs "The 5 Cs". This paper will explain The 5 Cs and detail how these business drivers apply to the adoption of SaaS in the physical security industry.

SaaS and Security Defined

We have said that cloud computing is sharing pooled resources via the Internet. SaaS providers create multi-tenant software hosted in the cloud with the following basic attributes:

- All applications, databases, and servers are hosted on the service provider's own infrastructure—typically at sophisticated outsourced data centers.
- The public Internet is used as the communication path from the SaaS provider to users, of course with appropriate security measures in place.
- Local users require no dedicated PCs or software applications; they gain access to the resources they need from a range of Internet-connected devices.

In the physical security world, the client/server model for delivery of applications has dominated most complex applications while an early analogue for SaaS, namely central station alarm monitoring, has dominated the less complex applications. Alarm monitoring is essentially a model for efficiently delivering pooled central resources to a group of users. The infrastructure, computers, and personnel in today's central stations are shared among a group of clients. Each client pays a small fraction of the cost they would bear if they had their own dedicated central station.

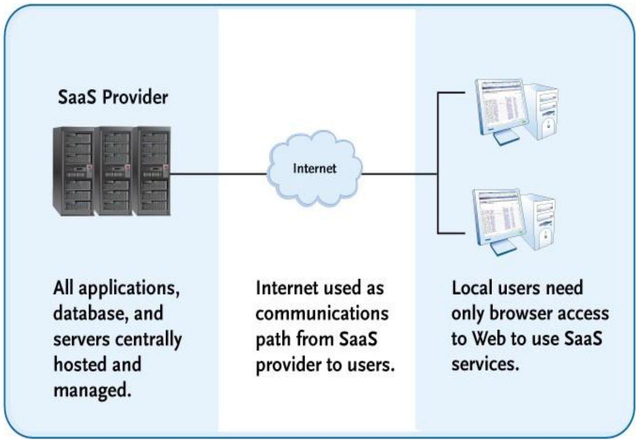
SaaS Provider
Internet
All applications, database, and servers centrally hosted and managed.
Internet used as communications path from SaaS provider to users.
Local users need only browser access to Web to use SaaS services.

Figure 1: Basic Architecture of a SaaS Solution

Security as a Service takes the central station model to a new level, providing unprecedented end-user control over system functions while preserving complete segregation of data. Leveraging multi-tenant software and efficient hosting environments, SaaS for Security drives costs down and service levels up.

The 5 Cs of Security as a Service

Physical and logical security are among the top priorities for most organizations today. Having a sound risk management plan for security is as essential as having a sales and financial strategy. However, security seldom contributes to the bottom line of an organization and, as such, Chief Security Officers (CSOs) and Chief Information Officers (CIOs) must find ways to ensure that their functions contribute as much as possible while consuming a minimum amount of resources. Each successful organization today is constantly asking how things can be done better at a lower cost. To understand the potential impact of Security as a Service, we will explore "The 5 Cs", five areas that are of strategic importance to all organizations.

Change

Organizations face a constantly changing array of pressures from multiple sources. Competitive threats, new regulations, financial uncertainty, technological shifts, and business risk all force managers to maintain a state of perpetual vigilance. Globalization and technological advancements have enabled new business models and competitors to spring up seemingly overnight. The ability of businesses to respond effectively to these pressures can be in itself a source of sustainable competitive advantage.

> It's not the strongest of the species that survives, nor the most intelligent that survives.
> It's the one most adaptable to change. – Charles Darwin

Savvy managers are taking cues from Darwin and are building lithe organizations with systems and infrastructure capable of responding to threats and capitalizing on opportunities with amazing speed. Today's CEOs look to their CIOs and CSOs for answers on how to be more competitive, not simply to deliver a service to the organization. Any CSO who fails to consider business agility and speed to market in their planning is likely to be consumed by a hostile business environment.

The SaaS delivery model supports these objectives by providing capabilities that can be rapidly deployed and retracted based on the changing needs of the business. In the context of physical security, SaaS applications allow CSOs to provision new security capabilities as needed and where needed without investing in the technology and human resources required to support the service. Also, since the SaaS model is built around ever-improving technology supported by monthly fees, CSOs can ensure their organization's access to the latest features without ever worrying about upgrade patches and hardware limitations.

Compliance

Corporate governance, risk management, and compliance with policies and regulations are in sharp focus for most organizations. It's not enough to express intent to follow regulations and policies, organizations must measure and transparently report on how completely they are being followed. Efforts to ensure consistent experiences for customers and to wring efficiencies from standardization are often competing with individual workers whose sense of privilege or creativity conflicts with the corporate standard. Getting it wrong in this area can have devastating consequences on the viability and competitiveness of any firm. Correspondingly, many organizations invest huge amounts of resources in auditing and assurance services to ensure compliance with standards and to evaluate controls.

In the context of physical security, compliance failures can result in data breeches, exposure to financial losses, denials of service, and even bodily injury to employees and visitors. The use of traditional physical security client/server architecture exposes company assets and personal information to constant threats. A typical corporate installation may have dozens of PCs each with access to security controls and sensitive personal information. Providing any assurance of how access to these resources is managed and what standards are being followed is a daunting task.

SaaS architecture greatly simplifies enforcement of polices and audits for compliance by providing centralized capabilities to establish standards as well as tools to track and report on compliance. Since a SaaS solution database is centralized, the cost for performing compliance audits is significantly reduced. Many SaaS providers are also able to provide evidence of internal controls certified by independent auditors, thus eliminating the need for a subscriber to incur these costs.

Cost

The survival of every organization hinges on its ability to deliver value for its customers. It's impossible to deliver high levels of value without addressing the cost structure for operating your organization. Referring back to the power example, what would it cost each of us to have a personal power generation plant for our homes? How much would the installation cost be and how much labor would be required to operate it and maintain the equipment? While it seems quite obvious that a personal power plant wouldn't make sense, most physical security applications are designed exactly in this way. Software and hardware are purchased with sufficient capacity to handle present and some portion of future needs. The equipment is installed, powered, and maintained with internal resources. Very often excess resources exist in the host computers and within each machine that is operating the client software. When you add up the total cost of ownership, you will most likely be quite surprised and less than pleased.

"You shouldn't have something in your back office that exists in someone else's front office."- Jack Welch

The SaaS-based Security as a Service model provides an excellent alternative to the traditional options, thus allowing organizations to focus on their core business. SaaS delivers outstanding economic value for the following reasons:

1. All users share a common computing infrastructure, to the economic benefit of all.
2. The cost model is scalable with users only paying for what they actually use.
3. The consumers of an application are free of all "back-end" management and maintenance expenses.
4. Up-front capital expenditures are replaced with flat, subscription-based operational expenses.

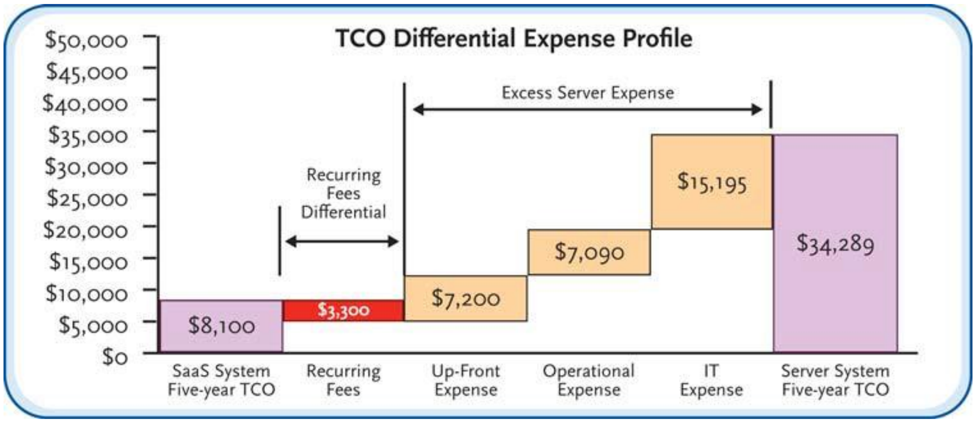

Figure 2: SaaS cost advantage over server-based systems

Beyond the excessive capital outlays for traditional options, recent studies have established that the largest portion of application and server ownership costs actually exists in ongoing operational expenses, maintenance, and support agreements. This is particularly true of computer systems that provide infrastructure services like security, because they must be held to a higher standard of availability and performance than ordinary office equipment. In one representative study, the authors concluded that only 15% of the lifetime cost of server ownership is captured by the initial purchase price. This means that your $1,000 server can actually cost you over $6,600.[iii]

In the case of physical security, our own study found that for a typical branch office or managed property scenario, the SaaS model for security management offers significant operational and financial savings. This is due to both upfront cost reductions and the economies of scale of hosted application services. This study determined that a Security as a Service solution enjoyed an advantage of nearly $26,000 (or 76%) over the server-based solution.[iv]

Continuity

Our collective experiences with events such as 9/11, Hurricane Katrina, and a host of other disasters and outages have brought into clear focus the need for redundancy and resiliency in the systems that support our organizations. It's not enough to ask how well we are protected or how many back-ups exist, we must also ask how fast we can resume operations if everything goes wrong.

Organizations routinely spend hundreds of thousands of dollars on hot-standby computers, back-up power sources, and disaster recovery locations to create resiliency in their physical security platforms. These measures are not only expensive; they are often reliant on internal computer networks that are likely to be severely challenged by any form of massive disaster. Further, if employees cannot get to the machines that operate the security platform, all the redundant measures will more than likely be fruitless. While security is certainly a high priority, if an organization's core revenue-generating capabilities are down, what will be addressed first?

Fortunately, the SaaS model provides numerous answers for these types of critical challenges. Multi-tenant SaaS services are normally hosted in highly reliable data centers with built-in redundancy. The best providers also employ separate disaster recovery centers to restore full operations if the primary center is disabled. Redundancy in the communication path is built into this model due to the Internet's capability to send information via a large number of routes. Even if broadband service is down, it's possible to establish the same communication paths via cellular cards and cellular-equipped access panels. Since no special computers or software are required to operate a SaaS-based physical security application, any computer connected to the Internet can be placed into service during an emergency.

The redundancy and disaster recovery capabilities of the SaaS model are even more remarkable when you consider that it's all part of the basic service, and is available at the same level of quality for consumers who want to secure one door or one thousand of doors.

Coverage

Organizations often find that the best way to accelerate profitable growth is through geographic expansion. Expansion comes with significant challenges, risks, and expenses. Management teams will be extended a bit further, as will scarce company resources. Solutions that provide good results in one location or at a small campus can become troublesome when multiplied for many geographically dispersed sites. Typically these latter types of installations expose the vulnerabilities, complexities, and hidden expenses of traditional client/server solutions.

Security as a Service solutions provide very clear benefits for organizations with geographically dispersed sites. The low initial costs and wide scalability of SaaS solutions give organizations access to world-class technologies with an economic model that promotes expansion instead of restricting it. Securely using the public Internet as a communication medium greatly simplifies the deployment of remote sites for IT departments. Best yet, the centrally hosted SaaS model provides all the central oversight and management needed in well-run organizations without requiring costly investments in dedicated infrastructure.

It's a small world, but I wouldn't want to have to paint it – Steven Wright

A SaaS-based security platform gives you the power to drop an access control point anywhere in world and have it configured, communicating, and controlling your facility in a matter of hours, and with complete synchronization to your master database and total audit capability from wherever you happen to be. With the complexity of local software and hardware configurations removed from the equation, installers with even modest training can successfully implement a SaaS-based physical access control solution.

Illustration: SaaS in Physical Security Today

Brivo introduced SaaS to the security industry in 2001. The company offers a hosted Security Management System that provides centralized access control, video surveillance, notifications, and related services. As shown below, the SaaS applications connect to a variety of on-premise security equipment ranging from cameras to control panels and multiple other sensors.

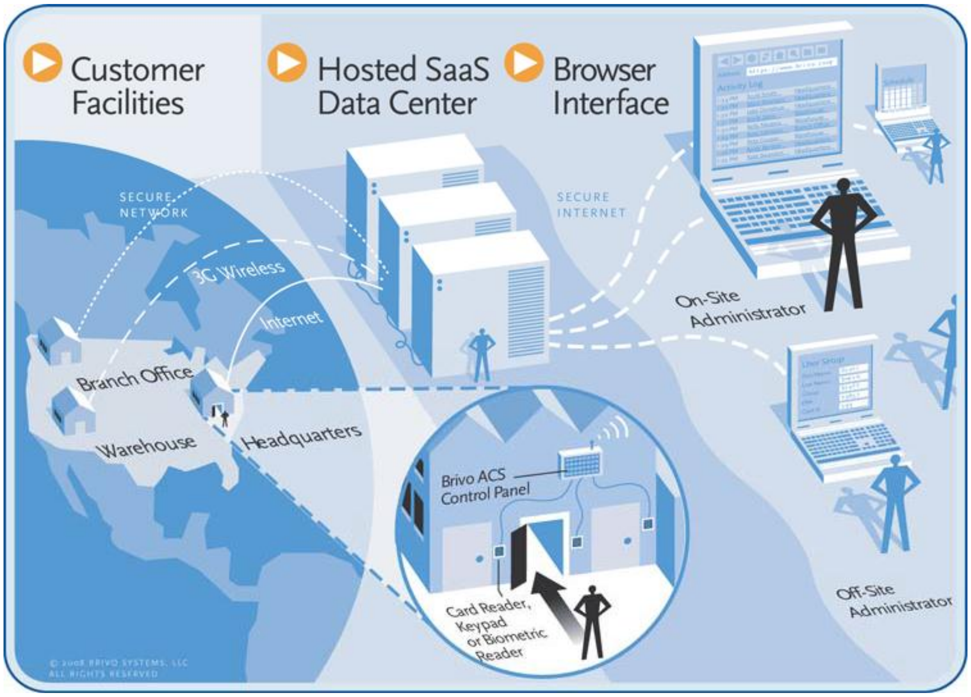

Figure 3: SaaS access control overview

This architecture does away with the need to have applications running at each secured property, which eliminates the expense and headaches of the local computing resources that have been the Achilles' Heel of legacy security systems. Instead, it relies on a centrally hosted platform for identity, device, and asset management; as well as all alerts, alarms, email notifications, and general reporting. Multiple data centers throughout the U.S. provide redundancy and disaster recovery capability, along with an SAS-70 audit capability to provide assurance on information security and compliance concerns.

Conclusions

Change, Compliance, Cost, Continuity, and Coverage; these are all fundamental considerations for an organization. For anyone challenged with evaluating and implementing technical solutions, these factors provide a useful lens through which to assess available options. With the past as our guide it is clear that the future will demand more flexibility, reach, and capacity more quickly and at lower costs. The Internet has already changed the way we live, learn, and communicate with each other. It is also changing the nature of software and how we interact with it. We are moving from static applications purchased in boxes to living cyber platforms shared with thousands of users, adopted as needed and discarded if not valued.

SaaS changes our relationship with software by allowing us to focus on what it does for us—not the infrastructure required to make it work. This change allows businesses to invest more in their people and in differentiating technologies and less on non-strategic functions.

SaaS also changes our relationships with software providers by creating a mutually dependant environment in which the seller of the service is fully committed to the customer's long-term outcomes. No one expects a customer to continue to pay for a solution that is not providing value to their organization. The Software as a Service model creates a vendor-vested relationship from the very start and places the consumer in a more powerful position. If your organization would benefit from rapid access to state-of-the-art technology delivered with minimal internal resource requirements, tremendous scalability, and predictable costs over time, then your organization should consider a SaaS-based option for your physical security needs.

Bibliography:

[i] Scheier, Robert L. August 20, 2007. "Your Data's Less Safe Today than Two Years Ago," InfoWorld, http://www.infoworld.com/article/07/08/20/data-is-less-safe_1.html (January 4, 2008).

[ii] "Gartner: SaaS Market Heats Up." September 28, 2006 ebizq, http://www.ebizq.net/news/7314.html (January 20, 2008).

[iii] "Total Cost of Ownership Reduction with VMware," VMware.com http://www.vmware.com/vmwarestore/newstore/tco_login.jsp (March 10, 2008).

[iv] Interested readers are referred to the full study, which can be found at: http://www.brivo.com/user_data/white_papers/1238089383_brivo_whitepaper.pdf

About Brivo

Brivo Systems LLC provides an online, open-system security management technology platform that empowers organizations to protect and remotely monitor buildings and perimeter entry points using the latest in Internet and wireless technologies. With Brivo's security management system, customers significantly expand their physical access control system by customizing functionality to exactly fit their needs and more effectively mitigate and manage security risk. The company's hardware products and software services enable businesses to control physical access to offices, warehouses, remote/unmanned buildings, as well as sensitive areas such as computer rooms, where real-time control and accountability of entry are critical. 2009 marks 10 years of Brivo making security simple for thousand of end users around the world.

brivo®

Call toll-free today for a demonstration 1-866-692-7486, option 1, email us at demo@brivo.com, or view all your options and make your choice at www.brivo.com/demo.

Brivo Systems LLC, 7700 Old Georgetown Road, Suite 300, Bethesda, MD 20814