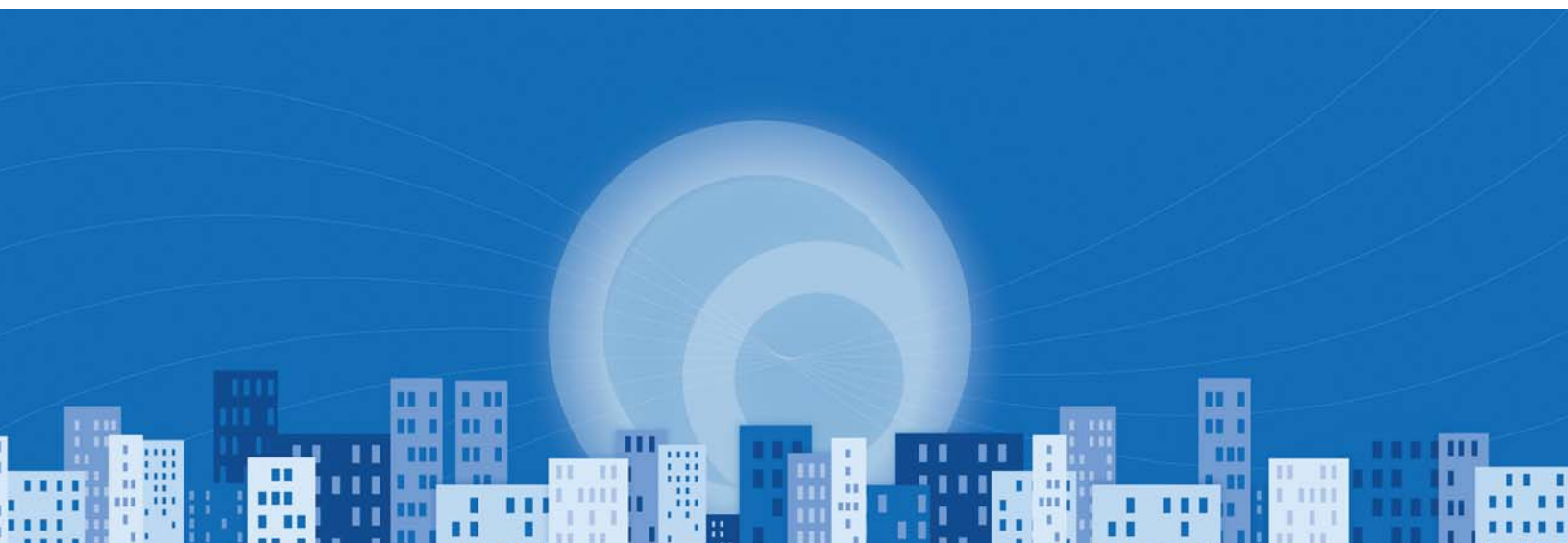


Security as a Service

Software as a Service Meets Physical Security

WHITE PAPER



Introduction

In the decade or so since widespread adoption of Internet, Web-based application services and pay-per-use business models have established Software-as-a-Service (SaaS) and cloud computing as the dominant new paradigms for software deployment and delivery. During the same decade, the physical security market finally caught up with the IT market's adoption level of IP networking technology and ushered in numerous IP-based products of its own, from cameras to control panels to browser-based user interfaces. These two technology trends have converged with the broader marketplace evolution to a service-based economy in which vendors increasingly take on roles formerly performed by the end user.

The result—like numerous other business application domains—is that physical security is now moving “to the cloud” and using SaaS to meet changing customer and market expectations. In some cases, these services are consumed directly by end-users, while in other cases they are accompanied by a “managed service” offering that layers human expertise on top of the underlying technology base. In both cases, users enjoy the benefits of being freed from technology ownership and seeing more rapid deployment of new features.

The following Executive Summary of the full study of the same name provides highlights of our conclusions regarding the ongoing adoption of SaaS within the security market.

Why SaaS?

Software-as-a-Service has emerged in the second half of this decade as the single most important trend in the computing industry. IT publications and Web sites and even the popular business press have been dominated for the past year or two with talk of SaaS and “cloud computing.” Numerous articles quote the almost revolutionary fervor of its proponents and predict the end of installed software as we know it.

Consider the following SaaS facts:

- The federal government has declared that SaaS is the best way to remedy their own expensive and inefficient IT procurement cycles, and has charged the GSA with maintaining a “SaaS storefront” on behalf of all federal agencies;ⁱ
- 75% of companies surveyed by IDC are planning to use one or more SaaS applications in their businesses;ⁱⁱ
- SaaS is reportedly the driving force behind the world's 60 fastest-growing software companies;ⁱⁱⁱ
- Annual growth rates for SaaS are estimated at 40% for 2009, despite the current economic climate;^{iv}
- Gartner, Inc., predicts that the SaaS market will continue to grow at least 22.1% per year^v and that by 2011, 25% or more of new software systems will be delivered as SaaS applications.^{vi}

In *The Big Switch: Rewiring the World, from Edison to Google*, Nicholas Carr reports that the SaaS industry has been growing at over 20% per year already^{vii} and now represents an annual market of approximately \$8-10 billion in the US alone. He further argues that the trend toward consuming software “on demand” rather than owning it is a paradigm shift comparable to the centralization and “on demand” provision of electrical power several generations ago.

SaaS products are available in vertical markets from CRM to accounting to ERP and almost every field where installed software was once dominant. What's interesting about this phenomenon is that the success of the technology and business model is not limited to just one type of application. Market penetration for SaaS seems to be growing rapidly regardless of the underlying function it performs. Among the most frequently cited reasons for this steep adoption curve are:

- low cost of ownership
- ease of deployment
- lack of IT resources in customer organizations
- avoidance of capital expenditure

For the security practitioner, all of these issues will sound like familiar customer concerns. But what, exactly, is SaaS, and how does it achieve these results?

SaaS and the Cloud Defined

One can find numerous definitions of SaaS in the literature today. Confusing matters further, the related trend of "cloud computing" is often referred to in the same breath, sometimes interchangeably. It's important to have a basic understanding of these terms, but rather than produce yet another definition, we've chosen to condense recent NIST work into two succinct uses for the context of this study:

Cloud Computing	Software-as-a-Service
A model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. ^{viii}	A <i>delivery model</i> for cloud computing, provided to the consumer to use the applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser. The consumer does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities. ^{ix}

Application to Physical Security Market

Setting aside the particulars of Internet technology, it's easy to argue that SaaS is nothing new to the physical security market.

The humble alarm monitoring station has exhibited many of the core characteristics of the SaaS model for several decades now:

- common computing infrastructure,
- shared across multiple client organizations
- no end-user capital investment
- pay-as-you-go monthly fees

By all measures, this model has been tremendously successful—for customers and business owners and for the industry as a whole. The curious fact is that with all the success of this model, it has not spread further until recently.

And this is where Internet technology becomes highly relevant. Alarm monitoring succeeded as a pre-Internet centralized computing model for several reasons: low bandwidth requirements; a relatively simple computing task; no direct application access by end users; and little need for systems integration with other IT infrastructure. The modern enterprise security system is not so lucky. Today's security applications have fundamentally changed since the industry's wholesale conversion to IP-based

products: high bandwidth requirements, complex processing and storage, end users who want to access every conceivable type of data, and a desire for interoperability with identity management and other IT systems.

Even with these dramatic increases in the technical profile of the relevant applications, the security market is still set to see more general SaaS applications succeed where the alarm model has been succeeding for many years. The key predictors for this success are that SaaS:

- leverages a common computing infrastructure across larger user groups, to the economic benefit of all;
- offers an on-demand computing model in which you only pay for what you use;
- frees the consumer of an application from owning and maintaining the underlying technology; and,
- replaces up-front capital expenditures with flat, subscription-based operational expenses.

Multi-tenancy as Breakthrough Technology

To better understand this bold prediction, we need to look at what it is about SaaS software architecture that has changed the outlook for centrally-hosted security applications. It is in a word: multi-tenancy.

The core idea of multi-tenancy is that “all users and applications share a single, common infrastructure and code base that is centrally maintained”.^x Just as a building’s structural architecture will differ depending on whether it is designed for a single occupant or multiple tenants, so too will a software system’s design differ depending on whether it is intended to be used by a single “tenant” or multiple tenants. In this model, cost savings are achieved both through commonality of hardware resources, as well as sharing licensing and operating expenses more efficiently across a large population of users.

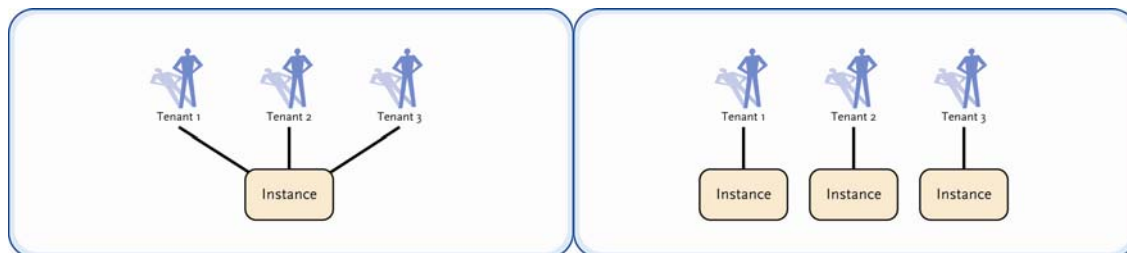


Figure 1. Multi-tenant vs. Single Tenant Software Architecture

Multi-tenancy stands in sharp contrast to the practice of simply deploying a stack of client-server systems in a data center and calling it a hosted service. In its “Four Level SaaS Maturity Model,” Microsoft categorizes this approach as the “lowest level” of SaaS maturity, or roughly equivalent to the “traditional application service provider (ASP) model of software delivery, dating back to the 1990s,” which “offers few of the benefits of a fully mature SaaS solution.”^{xi}

This stack-a-box or hide-the-server approach to providing remote software services is simply a case of what many observers call “cloud envy.” And it has the net effect of trapping service providers and customers into a costly cycle of maintenance and replacement. Doing the math, it becomes obvious that the overall solution is still saddled with the same cost structure as if it were located at the customer site. Except for the fact that someone else is managing the system, the stack-a-box approach is no different than the legacy approach to application ownership.

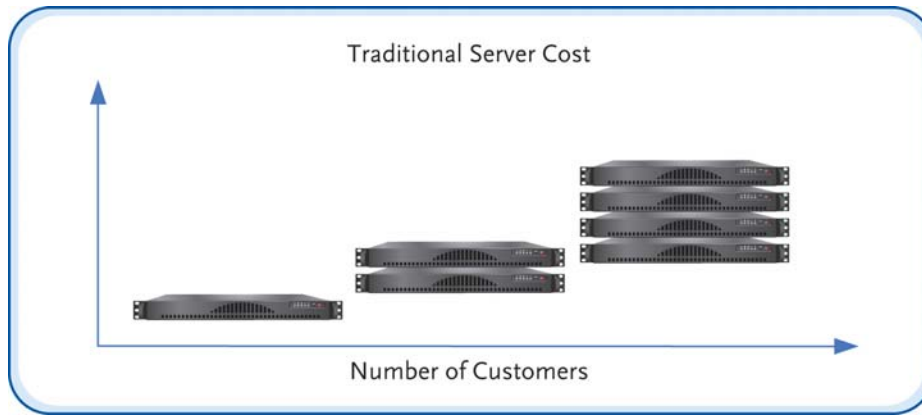


Figure 2. The Economics of the "Stack a Box" Approach

SaaS Adoption Drivers

In the broader IT market, SaaS has found many adherents for many different types of application services. The reasons for adoption vary by industry and application type, but a number of common trends emerge as reasons for adopting the SaaS model. Chief among adoption drivers are ease of deployment, flexibility, lower costs, and ease of use, as described in a landmark study published by *Information Week*,^{xii} and confirmed in a more recent study by Gartner.^{xiii}

The reasons for deploying SaaS for physical security are in many cases virtually the same as elsewhere in the IT world. Those drivers are listed in the left column in Table 1. In addition, there are also reasons unique to the physical security driving SaaS adoption in the industry, as shown in the right column. These have much more to do with the geographically distributed nature of many corporate security applications, the history of technology cycles within this market, and the class of solutions that have been deployed up until now.

Table 1. SaaS Drivers for IT and Physical Security

Top SaaS Adoption Drivers in IT	Additional SaaS Drivers in Security
Total Cost of Ownership	Span of Control
Rapid Deployment	Quality of Service
Capital Conservation	Anywhere Management
Obsolescence Avoidance	Distributed Software Updates

In the full version of this white paper, each of these drivers is fully elaborated upon in terms of its contribution to decision-making and its relevance to security buyers. For the sake of brevity in the current context, we describe only Total Cost of Ownership in additional detail here.

Total Cost of Ownership

Of all of these reasons, Total Cost of Ownership (TCO) is usually cited as the predominant reason for choosing the SaaS model. No surprise there: we all know that no matter what buyers say, cost is always a major factor behind any purchasing decision.

One can find extensive studies on the relative TCO of various software and hardware solutions through most of the IT industry. In the world of physical security, however, such analytical tools are less frequently applied—this, ironically, in an industry know for cost-conscious customers and hard-won justifications for capital expenditures.

Beyond stiff capital outlays, recent studies have established that the largest part of application and server ownership costs actually exist 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 conclude that only 15% of the lifetime cost of server ownership is captured by the initial purchase price, which means that your \$1,000 server can actually cost you over \$6,600.^{xiv}

In the case of physical security, our own study finds 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.

The graph below shows the conclusions of a study which concluded that a SaaS solution enjoyed an advantage of nearly \$26,000 (or 76%) over the server-based solution.^{xv}

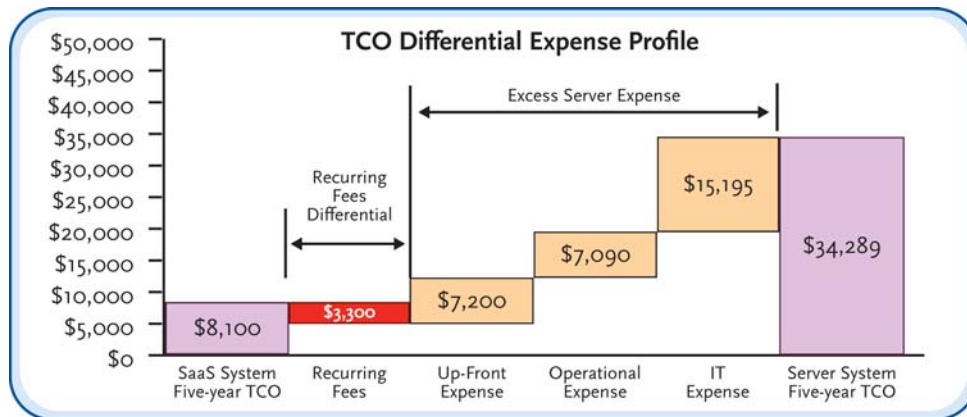


Figure 3, SaaS Cost Advantage over Server-Based Systems

The conclusion here, as in similar studies, is that savings accrue to buyers through economies of scale in the process of outsourcing non-strategic technology. Not available at the time of our original study was data describing additional savings that accrue from outsourcing of potentially numerous compliance requirements. Initial calculations indicate that for certain classes of business, these savings would easily match the “hard” savings from hardware and software.

Industry and Market Fit

Whether in the security industry or the broader IT market, there is no shortage of aaS's. Within physical security alone, a recent proliferation of XaaS offerings has provided a constant stream of new entries for the acronym-of-the-month club. What are they and what do they mean for physical security? Are they really new, or are they simply a “cloud-washing” of otherwise traditional applications?

The most general, of course, is the broad trend toward Security-as-a-Service, which is the title of this paper, and a catch-all for the whole genre of new entrants. But there are also any number of niche monikers which have been summarized in the table below to provide a sense of the recent diversity of offerings:

The Moniker	What it Means
MVaaS	Managed Video as a Service: an online offering that links together multiple DVRs into a unified whole accessible from a Web browser, with value-added analytical functions.
HVaaS	Hosted Video as a Service: a DVR-free online offering that provides central storage and management of streaming IP video.
VaaS	Video as a Service: How this differs from the other two is anyone's guess.
ACaaS	Access Control as a Service: a centralized online access control service in which applications and databases reside within a hosted facility.
PaaS	Platform as a Service: The provision of a common, hosted application development and deployment environment for SaaS offerings.

And the list could go on. The point here is that many vendors are in a big hurry to identify their applications as Something-as-a-Service. In reality, some of them are—or will be—SaaS applications, but it's often hard to “see the cloud for the marketing fog.”

Security Market Segments for SaaS

In an earlier section of this Executive Summary, we looked at general reasons for the adoption of SaaS in the physical security market, and how they compare to drivers in the IT world at large. What we found is that there are many strong similarities. Even more interesting is how these factors have actually played out in the marketplace, and where SaaS has been successful to date.

The following figure provides one way to look at the data along two principal axes.^{xvi} The vertical axis looks at customer tolerance for capital expenditure vs. their preference for purchasing goods and services as an operating expense. The horizontal axis describes the customers' physical assets in terms of geographic concentration or dispersion.

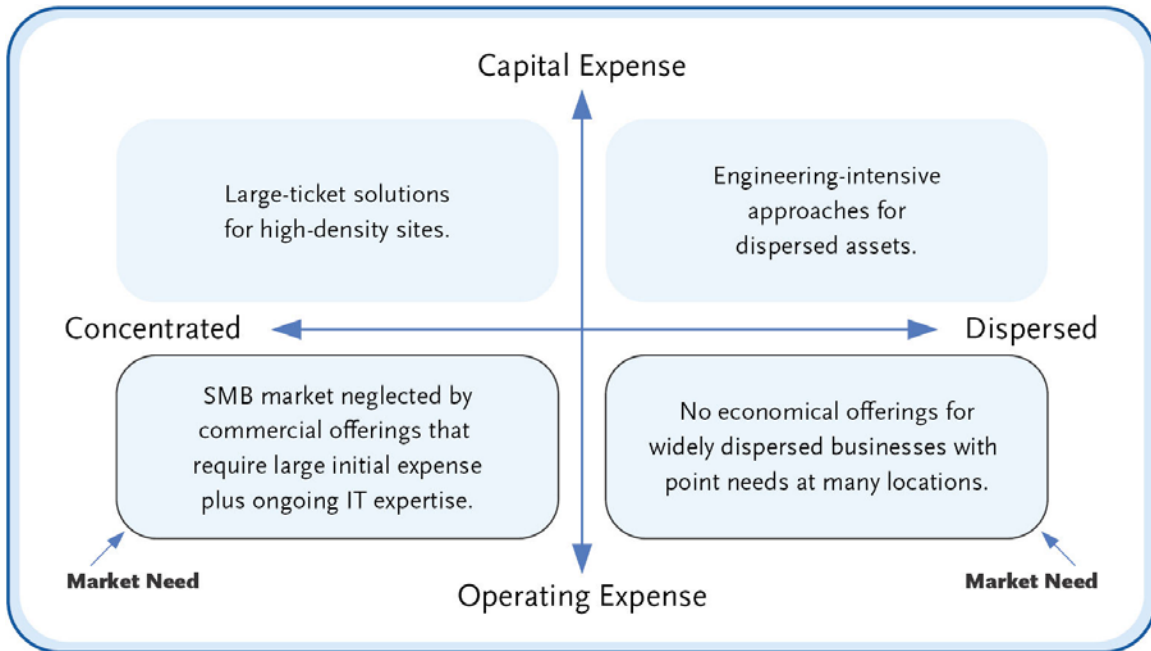


Figure 4. SaaS Market Fit Favors both SMB and Dispersed Enterprises

As shown by the “Market Need” indicators, the strongest fit for SaaS security applications occurs in two primary market segments: the Small and Medium-size Business (SMB) market (lower left), which has no appetite for extensive IT infrastructure; and the widely dispersed enterprise (lower right) that benefits most from centralization while minimizing per-site investment.

The SMB Phenomenon

The early success of SaaS in the SMB segment has been documented extensively in the trade press. The appeal is obvious. Even without a credit crunch, small and mid-size companies do not want to spend precious capital on large-ticket IT purchases. Nor do they wish to hire lots of IT staff to babysit a roomful of servers and applications. Many businesses in this category implicitly follow Jack Welch’s famous dictum that, “You shouldn’t have something in your back office that exists in someone else’s front office.” In fact, it is no longer unusual for small and mid-size companies to be able to meet all their IT needs through SaaS providers. Some actually establish “zero footprint” as a stated goal of information management. What it may surprise more industry observers to learn, though, is that this phenomenon is moving further up-market, with name-brand IT companies still choosing to outsource non-strategic IT functions—like access control and video—to SaaS providers who can bring the whole service with no IT distraction.

The Widely Dispersed Enterprise

The more recent success of SaaS in larger enterprises is also noteworthy in the industry—even for traditional “seat-based” licensing models of traditional corporate applications such as ERP, accounting, or CRM systems. We are seeing the same phenomenon in the security market, most notably where an organization has property assets with wide geographic dispersion. Examples of this phenomenon include: retail, property management, and many federal applications. The key to understanding this outcome is to evaluate the difference in cost and complexity of establishing one’s own far-flung security network versus simply piggybacking onto the Internet. The use of SaaS connection models—when properly executed—results in zero-configuration installations for most local network architectures, and no additional infrastructure spending or IT coordination.

An Alternative View

An alternative depiction of the market portrays SaaS strengths against the two other dominant modes of deployment within the IP access control segment: Embedded, a low-end solution in which the entire application resides in a “control panel” or similar embedded device; and Appliance (server), which provides a more robust offering than Embedded but without the built-in geographic reach, multi-tenancy or distributed availability model of SaaS.

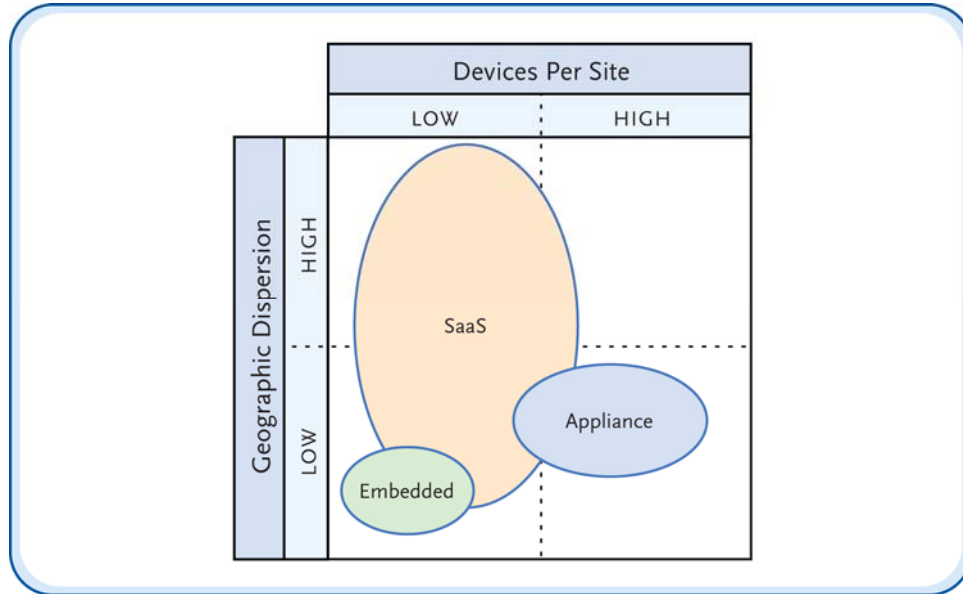


Figure 5. Deployment Modes and Market Fit

The point here is not that one model is better than another *across the board*; rather, it is really a question of *suitability for intended purpose*. Each of the dominant models has a clear role in the overall security ecosphere. Embedded solutions have eliminated the need for thick-client PCs every bit as much as SaaS has, and they are some of the cheapest solutions on the market, with at least half a dozen exemplars of the category currently for sale. But they won’t support a thousand sites. By the same token, appliance (or server-based) systems still serve the highest end of the enterprise market with the richest feature sets available, but they require sophisticated implementation exercises when stretched around the globe.

Managed Services is not SaaS

No discussion of SaaS is complete these days without a reference to “managed services” and how the two compare. Managed services is an older term which is frequently conflated with “as-a-Service” offerings that have since come into the marketplace along with other Internet technologies. It’s important to understand the differences or else one misses the importance of the SaaS market success.

The primary distinguishing feature of managed services is not a particular technology, but rather the involvement of human agents who perform various services on behalf of customers. In fact, hiding the underlying technology from customers has often been the whole point of managed services—based on the premise that the technology was simply too user-unfriendly for anyone but highly trained technicians to operate. These types of managed services will probably go the way of the switchboard operator as products with greater ease-of-use continue to be developed. In many application domains, this simplification has already come about with the advent of the modern GUI. Keeping such interfaces from end users is simply holding them hostage, and surely is not a model that will stand the test of time among informed end users.

That said, the value-added side of managed services is clear where the provision of a 24x7 staff provides a true benefit to the end user. The most obvious example of this type of service is any type of monitoring, which frees customers from having to pay their own staff around the clock. Another example is cyber-security services, where a managed service provider who is watching cyber threats across the entire Internet is in a better position to advise a client on the severity of a threat, and respond with an effective counter-measure. There are also cases where for insurance or risk management reasons, a company may wish to transfer a task—and the accompanying liability—to an outside managed services entity.

In none of these cases, though, is the technology really what managed services are all about. These services predated the arrival of cloud computing and SaaS, and many still use older technologies to perform their missions. Could they provide it better with SaaS? In many cases, yes, because of better connectivity or better availability or some other measure of service quality. Or it may be that managed service providers could simply reduce their own costs with SaaS. In most cases, though, the end user won't know—until they find a need to work with their managed service provider and pull some control back into their own organization. And that's when the technology will begin to matter for this sector.

Illustration: SaaS in Physical Security Today

Brivo introduced SaaS into 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 in Figure 6, the SaaS applications connect to a variety of on-premise security equipment ranging from cameras to control panels and other sensors.

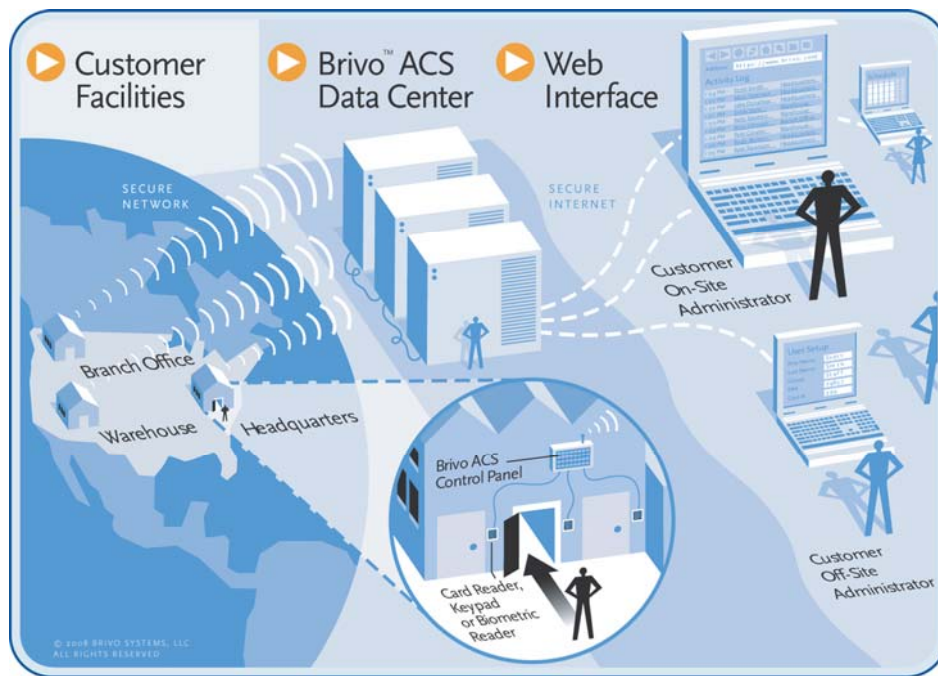


Figure 6. SaaS Access Control Overview

This architecture eliminates 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 US provide redundancy and disaster recovery capability, with SAS-70 audits to provide assurance on information security and compliance concerns.

Conclusions: Where will the SaaS Security Market Go?

Trying to understand where SaaS technology will go in the overall security market can take us in two different directions for an answer: one is toward the past, particularly for an industry that's already "been there" with a similar model; the other is toward the future, as already represented by the IT industry, which tends to lead the security field by a few years.

The past tells us that the centralized computing model works for those within the industry, that it can be packaged in many different ways, and that it can scale from the entrepreneur who starts his own RMR business to the largest players in the industry. The past also tells us that end users find the pay-as-you-go model and the possibility of ancillary managed services an attractive combination. That security is a 24x7 business doesn't hurt, because the prospect of managing applications or events in the middle of the night will always be something that end users will pay to outsource.

The future tells us that an unprecedented number of IT market segments are moving toward SaaS, encompassing applications that would never have been seen outside a corporate firewall just a few short years ago. Even the federal government—not usually known for its *avant garde* technology stance—has given SaaS a ringing endorsement as a way to control costs and speed deployment. All in all, it's safe to say that at least for several of the markets we've identified in our own studies, there are strong, compelling technological and financial reasons that we will see even more accelerated and expanded adoption of SaaS applications for the physical security industry.

"The future is here. It's just not widely distributed yet."

~ William Gibson

Notes & Bibliography:

- ⁱ Gautham Nagesh, "GSA to launch online storefront," 15 July 2009, [Nextgov](http://www.nextgov.com/nextgov/ng_20090715_3532.php?oref=rss?zone=NGtoday), 1 September 2009 <http://www.nextgov.com/nextgov/ng_20090715_3532.php?oref=rss?zone=NGtoday>.
- ⁱⁱ Alex Goldman, "IDC: SaaS Growth Coming," 27 March 2009, [Datamation](http://www.datamation.com), 3 September 2009 <itmanagement.earthweb.com>.
- ⁱⁱⁱ Matt Asay, "The Open Road," 15 April 2009, [CNET](http://www.cnet.com), 3 September 2009 <http://news.cnet.com/8301-13505_3-9919868-16.html>.
- ^{iv} Patrick Thibodeau, "SaaS Still on the Rise, Despite Down Economy," 9 February 2009, [ITworld](http://www.itworld.com), 3 September 2009 <<http://www.itworld.com/saas/62311/saas-still-rise-despite-down-economy>>.
- ^v 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).
- ^{vi} "Gartner: SaaS Market Heats Up." September 28, 2006 *ebizq*, <http://www.ebizq.net/news/7314.html> (January 20, 2008).
- ^{vii} Carr, Nicholas. *The Big Switch: Rewiring the World, from Edison to Google*. New York: Norton & Company, Inc., 2008.
- ^{viii} National Institute of Standards and Technology, "Computer Security Resource Center," 19 August 2009, [NIST.gov](http://www.nist.gov), 1 September 2009, <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>.
- ^{ix} *ibid*
- ^x Salesforce.com, "Multi-Tenant Platform," 5 Sep 2009, [salesforce.com](http://www.salesforce.com), 5 Sep 2009 <<http://www.salesforce.com/au/platform/why-ondemand/multi-tenant-platforms/>>.
- ^{xi} Microsoft Corporation, "Architecture Strategies for Catching the Long Tail," April 2006, [Microsoft Developer Network](http://www.microsoft.com), 1 October 2009 <<http://msdn.microsoft.com/en-us/library/aa479069.aspx>>.
- ^{xii} *Information Week*, CMP Publications: April 2007.
- ^{xiii} Sharon Metz, et al., "User Survey Analysis: Software as a Service, Enterprise Application Markets, Worldwide, 2008," Gartner, Inc, 2008.
- ^{xiv} "Total Cost of Ownership Reduction with VMware," [VMware.com](http://www.vmware.com) http://www.vmware.com/vmwarestore/newstore/tco_login.jsp (March 10, 2008).
- ^{xv} 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
- ^{xvi} The underlying data on adoption trends is based on customer trends from Brivo Systems' seven years of serving the security market with SaaS applications.