

# SaaS — TCO

How Web-hosted Software-as-a-Service (SaaS)  
Lowers the Total Cost of Ownership (TCO)  
for Electronic Access Control Systems.

WHITE PAPER



## Introduction

Total Cost of Ownership (TCO) is a well-studied discipline within IT at large, but its results have seldom been brought to bear on the world of electronic access control. Now that the Internet-based Software-as-a-Service (SaaS)<sup>1</sup> model for access control management platforms is, in many cases, replacing the traditional server-based approach, integrators and end users alike need to evaluate which is the most cost-effective solution for their organizations.

Until recently, it has been common for buyers to think of system cost in terms of one-time, up-front server and software expenses. However, it has become a well-established fact that the largest part of PC or server ownership cost actually lies in ongoing operational expenses, maintenance, and support agreements. This is particularly true of computer systems providing infrastructure services such as access control, because they must be held to a higher standard of availability and performance than ordinary office equipment.

## Summary Results

Our studies find that for most classes of applications, the SaaS model for security management platforms is the clear operational and financial winner, due primarily to the economies of scale introduced by hosted application services. It also provides significant availability and redundancy advantages over most server-based systems, which translates directly to increased business value.

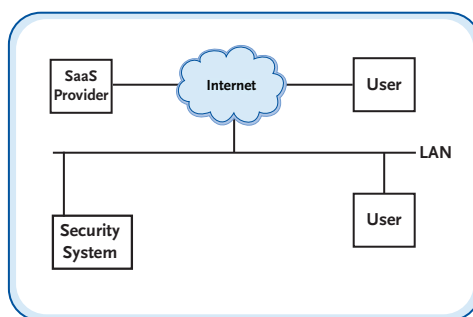


Figure 1: SaaS Architecture

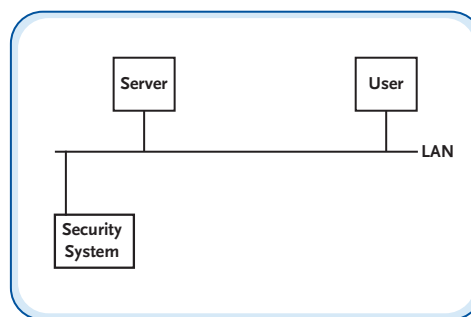


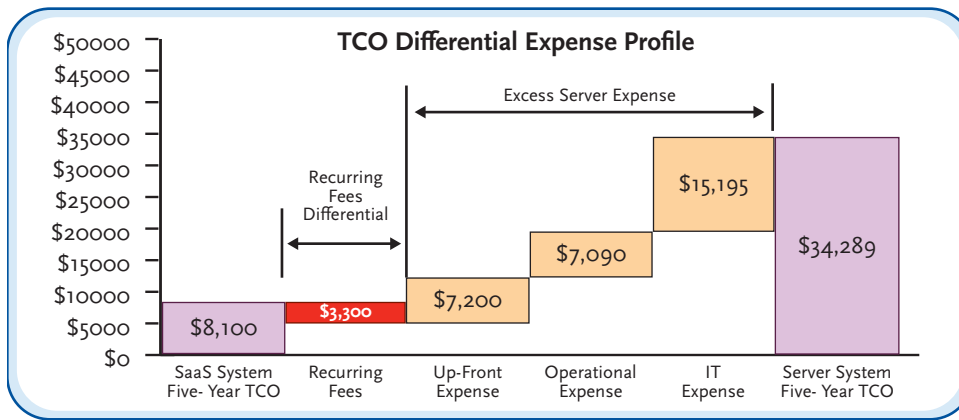
Figure 2: Server-based Architecture

Figure 3 shows the conclusions of our study, which demonstrates that for the systems we modeled, the SaaS solution enjoys an advantage of nearly \$26,000 (or 76%) over the server-based solution.

Only 15% of the lifetime cost of server ownership is captured by the initial purchase price, which means that your \$1,000 server actually costs you over \$6,600 .

For the systems we modeled, the SaaS solution cost \$26,000 less over 5 years while providing a higher grade of service.

<sup>1</sup> Note that during the history of centrally hosted software solutions provided as a service, SaaS has also been referred to as the ASP (Application Service Provider) model. Both names refer to the practice of providing software to end users from a centrally hosted system, rather than from on-premises servers with installed software licenses. The significant difference between SaaS and ASP models is that SaaS applications are generally required to be native, multi-tenant Web applications.



**Figure 3: SaaS cost advantage over server-based system**

Figure 3 shows the relative cost advantage of the SaaS solution over a traditional server based system. The first column (on the left) shows the five-year TCO of a SaaS solution for a single six-reader reader site. The next column (in red) shows the cumulative monthly expense of the SaaS fees, which actually count as a negative against the SaaS solution as compared to an installed server. However, this small deficit is quickly outweighed by the next three columns, which represent expense categories that are borne only by the server solution. The net effect is that these categories add up to a much higher TCO for the server-based system.

Note that the SaaS savings are achieved without factoring in the IT expense or business impact of server downtime, which can be considerable for many types of enterprises. When these additional cost factors are added, the cost effectiveness of SaaS solutions is even more dramatic.

The following pages will examine the cost factors and methodology that led to our results.

## Cost Factors

To perform a cost comparison between traditional server-based and SaaS security management platforms, we examined the following categories of operational expenses:

- Initial installation costs such as hardware and software license purchases, as well as labor expenses for provisioning control panels, servers, or other software systems.
- Recurring fees, including SaaS subscription fees, server software licensing, and hardware and software maintenance agreements.
- Operational expenses such as electrical power, rack space, and disaster recovery sites.
- IT staff costs, including routine maintenance, troubleshooting, patches for server-based systems, and the cost of upgrades and replacements.

Many additional factors are often included in a complete TCO analysis, but we found that these vary so widely from organization to organization that they could not be

When the effects of server downtime are added, SaaS savings are even more dramatic.

Servers require ongoing IT staff attention, including preventive maintenance, troubleshooting, OS patches, application upgrades, and security administration.

<sup>2</sup> VMware, Inc, "Reducing Total Cost of Ownership with VMware Server Software"

included in a meaningful generic model. Thus, we excluded such considerations as:

- Organizational cost of server downtime, including lost productivity and explicit cost of IT and security staff time to remediate failed systems.
- Business risk cost of system unavailability, including lost revenues, liabilities due to service level agreements, and loss of good will.

While evaluating the possible costs incurred from these factors would certainly have strengthened the case for SaaS, we found the outcome of the analysis more than compelling enough, even without these additional categories of hidden expenses.

The costs of procuring and installing lock hardware, readers, sensors, control panels, wiring, and other common items were assumed to be equal across both server- and SaaS-based systems. In other words, all TCO differences between the two types of security management platforms were the direct result of IT and operational expense factors, not the specific model of control panel, reader, etc. that were used.

## Methodology

Within this framework, our methodology for establishing the expense of every relevant management platform line item in our TCO model was to work from the following documented sources:

- Actual quotations from integrators to end users for various types of system installation, or, equivalently, from published price lists available in the industry. These were primarily used for calculating initial system installation expenses.
- Published studies or other reference data on the cost of various types of IT services and/or staff time. These were helpful in determining staff costs for server-based systems.
- Published rate structures for publicly available services, such as electrical power, rack space, and off-site backup services.

**The initial purchase is usually only 5% of the total cost of owning and maintaining a program.**  
- Microsoft Corporation<sup>3</sup>

## Case Studies & Examples

Two composite case studies were used as examples for the purposes of this article.

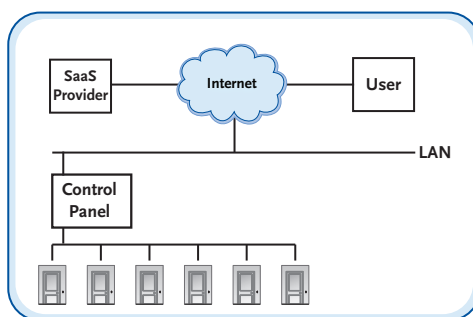


Figure 3: Single-site SaaS

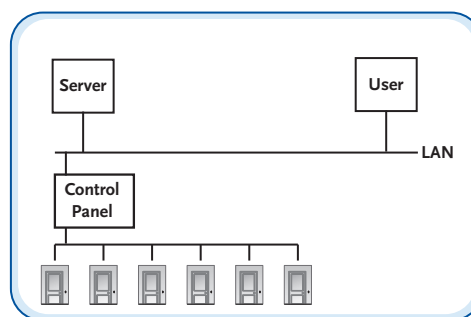


Figure 4: Single-site Server-based

<sup>3</sup> Microsoft Wages Campaign Against Using Free Software, The Wall Street Journal, December 9, 2002

The first case study is a single-site access control system with a total of six doors. In this case, all of the access control equipment is installed at one geographic site, with any related servers or other computing equipment also located at the same site. The second case study is a two-site system with six doors per site, requiring a common access control system across both. For the server-based system, the redundant servers are collocated at one of the controlled sites. In this case, an IP network between the

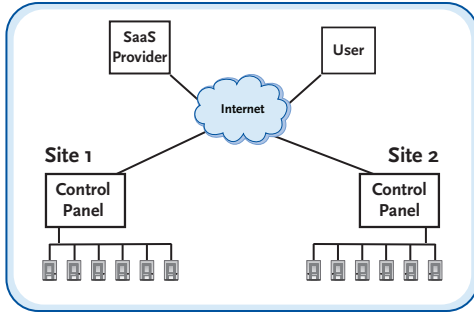


Figure 5: Multi-site SaaS

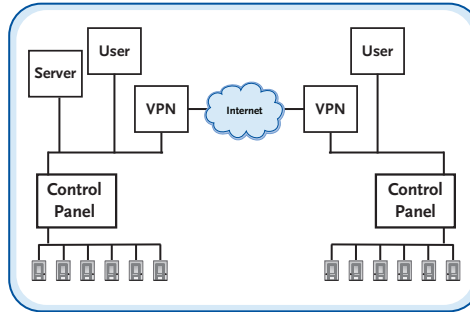


Figure 6: Multi-site Server-based

sites is assumed to use a VPN running over the public Internet in order to provide a common network topology for communications between the control panels and the servers. For the SaaS solution, no VPN is actually required, as it is sufficient that both sites allow their respective control panels to access the SaaS provider’s online Web services.

## Up-front Costs

Up-front costs for the single-site systems were quantified for four areas, with the following results:

System Installation Expenses	SaaS	Server-based
Installed cost of control panels and related hardware	\$3,200.00	\$3,200.00
IT staff expense, including initial consultation, network configuration, firewall settings	\$100.00	\$800.00
Installed cost of servers	\$0.00	\$4,400.00
Cost of software licenses: <ul style="list-style-type: none"> <li>• Application license</li> <li>• Operating system</li> <li>• Database</li> <li>• Middleware</li> <li>• Backup storage</li> </ul>	\$0.00	\$2,100.00
<b>TOTAL ONE-TIME EXPENSES</b>	<b>\$3,300.00</b>	<b>\$10,500.00</b>

Table 1: Single-site up front costs

Most SaaS applications can be deployed and put into production much faster and for a fraction of the cost compared to a traditional software solution.<sup>4</sup>

<sup>4</sup> Software-as-a-Service; A Comprehensive Look at the Total Cost of Ownership of Software Applications,” Software-as-a-Service Executive Council, September 2006

Staff time for the server-based system included the initial consultation for server installation, establishing networking parameters for server system and related control panels, and assessing firewall policy impact and making needed adjustments for remote access to the security management platform. The SaaS platform, by contrast, used DHCP on all control panels, thereby eliminating the need to assign static IP addresses or perform other network management tasks. It also required no changes to the firewall, as it used an existing “outbound 443 allowed” policy. Remote access to the access control application is a baseline capability of the SaaS model.

The cost to install servers for the server-based model included two security-grade redundant servers (to offer similar redundancy to the SaaS solution, which is intrinsically redundant), as well as one-day installation and set-up time on site. With the SaaS model, of course, there is no on-site server installation, which eradicated these costs.

Software license fees for server-based models included all required licenses for applications, middleware, database, and the operating system. These costs are all built in to the monthly fees for SaaS services, which means that there is no additional up-front charge for any of these items.

**Remote access via the Internet is fundamental to the SaaS architecture— it’s built into the solution.**

## Recurring Fees

Recurring fees for the single-site systems were identified for three areas, with the following results:

Recurring Fees	SaaS	Server-Based
Annual recurring service fees	\$960.00	\$0.00
Annual software maintenance	\$0.00	\$150.00
Annual technical support fees	\$0.00	\$150.00
<b>RECURRING ANNUAL FEES</b>	<b>\$960.00</b>	<b>\$300.00</b>

**Table 2: Single-site recurring fees**

Monthly subscription fees are the hallmark of the SaaS model, whereas they cost zero for an installed server-based system. Retail rates for these services vary considerably depending on whether any additional services are bundled in (e.g., 24X7 telephone support, concierge services, etc.). In this analysis, a market average for basic subscription services was used.

Annual software maintenance fees—typically charged to entitle users to ongoing software upgrades—are free in the SaaS model, as upgrades to Internet-based SaaS services are part of the core value proposition of such services.

Technical support fees for access to telephone support are required by most organizations, but tend to be included or bundled into the monthly subscription fees of SaaS vendors. This is important because technical support is a major differentiator between SaaS products and traditional software licensing models. The reason is that SaaS providers incorporate ongoing support into their business model. Traditional

**Annual software maintenance fees are free in the SaaS model as are automatic software updates.**

software providers, on the other hand, either try to avoid it—because it’s an unreimbursed expense—or charge large annual support fees.

## Operational Expenses

Operational expenses (non-IT) for the single-site systems identified as relevant to the TCO model were primarily related to energy—an increasingly visible cost of computing infrastructure.

Operational Expenses	SaaS	Server-based
Electrical power for server	\$0.00	\$709.21
Data center power expense for cooling, delivery, backup, air handling	\$0.00	\$709.21
<b>OPERATIONAL EXPENSES</b>	<b>\$0.00</b>	<b>\$1,418.42</b>

**Table 3: Single-site operational expenses**

The primary power consumption expense is based on redundant servers, with 2 X 400 W power supplies, 365 days x 24 hours, and an average cost of \$0.1012 per KWH for commercial power. Note that there is no associated power consumption for a SaaS security management platform, as all applications and databases are off-site and included in the monthly subscription fee. A redundant configuration is used for this calculation to compare fairly with the redundancy offered by an enterprise-grade SaaS provider.

The additional expense of delivering this power to the servers assumes a PUE (Power Usage Efficiency) of 2.0 for a well-run data center, which implies that every watt consumed for IT equipment is matched by an additional watt for uninterruptible power (UPS), chillers, air handlers, and power distribution equipment.

In the data center, power and cooling costs more than the IT equipment it supports.<sup>5</sup>

## Ongoing IT Expenses

Ongoing IT expenses proved to be a significant component of overall annual and lifetime costs, as show below:

IT Expenses (Recurring)	SaaS	Server-Based
Rack space for server	\$0.00	\$720.00
Redundant offsite data backup	\$0.00	\$239.40
Server management annual	\$0.00	\$1,200.00
Budgeted server upgrades/ replacements	\$0.00	\$880.00
Allocated IT support staff cost	\$0.00	\$0.00
<b>IT EXPENSES</b>	<b>\$0.00</b>	<b>\$3,039.40</b>

**Table 4: Single-site IT expenses**

One of the key issues in IT today is that normal operating expenses consume way too much of the annual budget—61% in most organizations.<sup>6</sup>

<sup>5</sup> Christian L. Belady, P.E., Hewlett-Packard, Electronics Cooling Magazine

<sup>6</sup> Tom Pisello, IT Business Edge, <http://www.itbusinessedge.com/blogs/tom/?p=107>

Rack space to house two redundant 1U servers was estimated based on the lowest commercially available cost for which we could find pricing data.<sup>7</sup> Again, rack space is calculated on the basis of redundant servers in order to compare fairly with redundancy provided by an enterprise-grade SaaS provider.

Most—if not all—SaaS providers include remote backup to a disaster recovery data center. In the interest of creating a fair basis for comparison, the cost of an off-site backup of all data was added to the server-based solution at the lowest available commercial rate.

Server management cost was budgeted on the low end at one hour per month for the server-based system, with fully loaded labor rates at national averages for IT personnel. Such costs are avoided when using a SaaS provider.

Our estimation of server upgrade or replacement costs reflect likely or planned server upgrade requirements, totaling these costs over a 5-year period—a much longer lifespan than most servers enjoy in today's IT environment. Many systems require upgrades over this time span due to mandatory operating system and security upgrades, as well as product obsolescence.

**Remote backup and disaster recovery are built into SaaS offerings, while they pose considerable extra expense for self-hosted server designs.**

## Single-site Summary

The following table summarizes the findings presented above and estimates the annual recurring fees for both solutions by multiplying the fees to their five-year totals.

Expenses Category	SaaS	Server-based	Period of Expense
Up-front expense	\$3,300.00	\$10,500.00	One-time
Recurring annual fees	\$960.00	\$300.00	Annual
Operational expenses	\$0.00	\$1,418.42	Annual
IT expenses	\$0.00	\$3,039.40	Annual
<b>TOTAL 5-YEAR COST OF OWNERSHIP</b>	<b>\$8,100.00</b>	<b>\$34,289.10</b>	<b>5 Years</b>

**Table 5: Single-site TCO comparison**

The cost savings of using a SaaS solution for access control are clearly dramatic—and probably far greater than most observers would have expected. Many server-based systems appear to be less expensive to own and operate than the SaaS, so where exactly did the costs grow beyond expectations?

A few things to remember about this analysis is that in the interest of a fair comparison with a SaaS offering, the server-based solution that we modeled was likely more powerful than many deployed in smaller businesses, and offered more services, such as redundancy, off-site backup, automatic upgrades to applications and system software, as well as full technical support.

**To compete with SaaS, a server solution must offer redundancy, offsite backups, automatic upgrades, and disaster recovery.**

<sup>7</sup> An alternate method is to work from the build-out and operating costs of a data center housed in one's own facility. This method gives similar or even higher results because most companies cannot build and operate a data center as efficiently as a collocation facility. For a discussion of build-out and cooling expenses, see Computerworld, "Data Centers Get a Makeover," November 2004.

That said, these are all important service level differentiators that buyers would do well to consider. Redundancy, for example, would seem to be a primary requirement for a system that is used in the protection of life and property, and a small cost to pay considering the lives and assets at risk. By the same token, off-site backup of data storage is routine for most corporate systems, but often neglected for access control systems. The cost of re-entering thousands of employee credentials and identifiers would be enormous in the event of a data center loss. Automatic application upgrades—available with most SaaS subscriptions—continue to add to the value of the initial purchase and prevent obsolescence or potential compliance issues that face aging systems.

The server-based solution used in this comparison was also presumed to be supported by data center-grade uninterruptible power, environmental conditioning, and data center-quality rack space (as opposed to sitting under someone’s desk). These items represent costs frequently overlooked or left as “overhead” in the often hasty comparisons presented during the purchasing cycle.

Nonetheless, even with “downgrades” to the quality of service used to price out the server solution, it has approximately \$26,000 of cost disadvantage that it would have to overcome during the five-year lifecycle in order to compete with the SaaS solution.

**The cost of re-entering thousands of employee credentials would be enormous in the event of a data center loss.**

## Multi-site Impacts

The data presented thus far have primarily addressed the single-site case. Qualitatively, the SaaS solution fares even better in a multi-site application, primarily due to additional cost penalties that the server-based solution must pay during initial setup of VPNs, along with higher ongoing IT expenses due to the complexity of managing the security management applications over a far-flung network. The SaaS solution is at home in this environment because, as a Web application, it is intrinsically multi-site from the inception.

Table 6 shows the same analysis we performed for the single-site system, but with the new values to reflect a multi-site system connected via a VPN. The same comments and analysis regarding quality-of-service and comparable feature sets between the SaaS and server-based systems apply here as well; in the interest of a fair comparison, the multi-site server-based system was configured to meet the same availability, redundancy, and disaster recovery standards as most SaaS offerings would provide.

**Qualitatively, the SaaS solution fares even better in a multi-site configuration.**

	SaaS	Server-based
<b>Up-front Fees and Expenses</b>		
Installed cost of control panels and related hardware	\$10,000.00	\$14,000.00
IT staff expenses, including initial consultation, network, configuration, firewall settings	\$200.00	\$2,400.00
Installed cost of servers	\$0.00	\$4,400.00
Cost of software licenses	\$0.00	\$2,100.00
<b>TOTAL UP-FRONT EXPENSES</b>	<b>\$10,200.00</b>	<b>\$22,900.00</b>
<b>Recurring Annual Fees</b>		
Annual recurring services fees	\$1,920.00	\$0.00
Annual software maintenance	\$0.00	\$500.00
Annual technical support fees	\$0.00	\$500.00
<b>RECURRING ANNUAL FEES</b>	<b>\$1,920.00</b>	<b>\$1,000.00</b>
<b>Operational Expenses (Recurring)</b>		
Electrical power for server	\$0.00	\$709.21
Data center power expense for cooling, delivery, backup, air handling	\$0.00	\$709.21
<b>OPERATIONAL EXPENSES</b>	<b>\$0.00</b>	<b>\$1,418.42</b>
<b>IT Expenses (Recurring)</b>		
Rack space	\$0.00	\$720.00
Redundant off-site data backup	\$0.00	\$239.40
Budgeted server upgrades/replacements	\$0.00	\$880.00
Allocated IT support staff cost	\$0.00	\$400.00
<b>IT EXPENSES</b>	<b>\$0.00</b>	<b>\$3,439.00</b>
<b>TOTAL ANNUAL EXPENSES</b>	<b>\$1,920.00</b>	<b>\$5,857.82</b>
Up-front expenses	\$10,200.00	\$22,900.00
Recurring annual fees	\$1,920.00	\$1,000.00
Operational expenses	\$-	\$1,418.42
IT expenses	\$-	\$3,439.40
<b>TOTAL 5-YEAR COST OF OWNERSHIP</b>	<b>\$19,800.00</b>	<b>\$52,189.10</b>

Table 6: Two-site TCO comparison

## Conclusions

As we have shown, our studies indicate that using a SaaS solution for a security management platform—specifically electronic access control—provides major, demonstrable cost savings. In addition to ease of installation and ease of use, the market's increasing awareness of the cost benefits of SaaS are driving the substantial growth in the installation of such systems.

These findings have several implications for system integrators and end users. The first is that—other things being equal—both groups would be well advised to calculate the relative cost of any proposed access control solutions before make a decision on what to offer a customer (in the case of integrators), or what to ultimately buy (in the case of end users). We have made our mathematical model and data sources publicly available so that anyone can perform the same comparisons that we did.

The second implication is that the savings provided by SaaS for access control can also be extended to other security services, such as hosted video, intrusion detection, remote monitoring, and many others. This is an important implication for the vast majority of business owners, as most businesses are not large enough to be able to absorb the cost of dedicated server solutions into a larger IT infrastructure. What this means is that such business owners can expect to enjoy enterprise-grade service levels at lower TCO points than at any time in the history of electronic security.

## The Business Impact of Downtime

The savings provided by SaaS access control solutions discussed throughout this white paper are all obtained without factoring in the IT expense or business impact of server downtime. A natural question to ask is, What does the picture look like if these costs are included? After all, server failure and downtime is a real phenomenon that businesses experience on a daily basis.

The short answer is that when these additional cost factors are included, the effectiveness of SaaS solutions is even more dramatic. However, the actual dollar impact on any given business depends on many factors beyond the scope of this study. For example, the cost impact on a \$1 million business will be much less than the cost impact on a \$1 billion business. The time and expense of restoring a server and any lost data will vary greatly depending on whether a company is using an in-house IT staff which can respond immediately, versus using contract IT providers who may not be able to arrive and fix the problem immediately.

What's clear, however, is that the costs can be very large, and are unpredictable when compounded with other factors: according to one study, "down-time costs accelerate in a non-linear fashion every hour."<sup>8</sup>

<sup>8</sup> Iron Mountain White Paper, "The Business Case for Disaster Recovery Planning: Calculating the Cost of Downtime."