



# Licensed or SaaS?

Picking the right model can save money, reduce risks, and boost productivity

Undoubtedly the hottest trend in software today is the rise of software-as-a-service (SaaS), also known as hosted or ASP.

Established companies like IBM, Oracle, Microsoft, and SAP have all announced hosted offerings to counter Web-based firms like Google and Salesforce.com.

Converts to SaaS claim that it can deliver lower costs and less reliance on IT. And for some applications, SaaS may well be the right choice.

But how does SaaS stack up for information-gathering and analysis systems designed for surveys, evaluations, 360 reviews, and tests?

Is SaaS always the best model for these applications?

This white paper examines five areas where SaaS may still be questionable:

- ◆ total cost of ownership
- ◆ system availability
- ◆ data security
- ◆ vendor lock-in
- ◆ workflow and productivity.

An enterprise must choose carefully between licensed software and SaaS to achieve lower costs over time, tight security over mission-critical data, and productive results from any new information-gathering and analysis system.

	Year 1 TCO	Year 2 TCO	Year 3 TCO	Year 4 TCO
Scenario A: Steady use of SaaS (\$50 @user, 100 users)	\$60,000	\$120,000	\$180,000	\$240,000
Scenario B: Growing use of SaaS (\$50 @user, 250 users by end of Year 3)	\$64,950	\$151,050	\$273,150	\$417,600
Scenario C: Licensed software (unlimited users, hardware and IT staff extra)	\$200,000	\$240,000	\$280,000	\$320,000

**Figure 1: SaaS versus Licensed Software Total Cost of Ownership (TCO)**  
(sample data, not based on any specific software vendor)

### Total Cost of Ownership

Software vendors are quick to say it's cheap to get started with SaaS: as little as \$50 a month per user.

But while the initial monthly fees are low, over time a customer may end up paying *more* than if they'd simply bought the license the traditional way.

It's a lot like leasing a car. Sure, the monthly payments may be low, but you just keep on paying forever.

Let's do some quick back-of-the-envelope comparisons, as shown in Figure 1. These numbers are just examples, not based on any specific software vendor.

As shown in Scenario A, suppose an enterprise signs up 100 users for a SaaS application for \$50 a month each. Over the first year, that costs \$5,000 a month, or \$60,000 a year.

Extended in a straight line, by the end of Year 2 the total cost of ownership is \$120,000. By the end of Year 3, it reaches \$180,000. And by the end of Year 4, it's \$240,000.

Now suppose events unfold according to the more realistic Scenario B. The SaaS application is popular, and more users want to sign up for it. Over three years, the user base grows steadily to 250. By the end of Year 3, the total cost of ownership is now close to \$275,000.

That's about the same as paying \$200,000 for a software license with unlimited users, plus 20 percent annual support for three years, as shown in Scenario C.

And by Year 4, the total licensed cost is well below the SaaS version. The shaded cells in this table show how the more expensive option changes from licensed to SaaS over a few short years.

This doesn't allow for the expense of in-house servers and IT staff, which are eliminated in SaaS. But these factors likely balance out by Year 4 as well.

And if the SaaS application costs more than \$50 a month, or attracts more than 250 users, the TCO for SaaS ends up even higher even sooner.

If you sometimes doubt that SaaS by definition equals lower costs, you're not the only one. Many analysts are beginning to say the same.

For example, Burton Group analyst Lyn Robison recently told *Red Herring* magazine that "the cost of using SaaS could be greater than signing licensing and support deals. Over a long period of time, those monthly or yearly subscriptions could compound into greater total cost of ownership."<sup>1</sup>

<sup>1</sup> "Sassing SaaS," *Red Herring*, April 9, 2007, p. 14.

The bottom-line on the bottom-line?

Don't assume that SaaS automatically saves you money. Over the long haul, it could cost more. Do the math, and make sure to project three to five years out to see where you could end up.

### **System Availability**

SaaS proponents often say this new model transforms software into a utility, like electricity, that's there whenever you need it. But what about when it's not there?

Even the most well-established SaaS vendors, Google and Salesforce.com, have struggled to keep their applications up.

Salesforce.com has faced embarrassing service interruptions, including much-publicized outages on December 20, 2005, and in 2006 on January 6 and 30, February 9, and April 6.

Even after massive efforts to upgrade its infrastructure and recode its software, a related site ([www.salesforce.com/appexchange](http://www.salesforce.com/appexchange)) unexpectedly shut down and locked out the company's development partners for two days in March, 2007.

Google customers suffered at least three service outages from the premium version of Gmail in March, 2007. Companies paying for this service apparently went without e-mail for two full business days.

These failures mean Google did not meet the 99.99% uptime guarantee in its service level agreement.

To maintain goodwill, the company had to offer 15 days of free service to its paying customers.

If SaaS vendors as experienced and well-staffed as Google and Salesforce.com suffer serious lapses, what about smaller, less established firms?

Many IT managers agree that these availability problems give SaaS an inherent weakness; in fact, they represent an Achilles heel for this business model.<sup>2</sup>

Even 99.99% uptime means an estimated 60 hours of downtime during business hours every year.

That's a full business week and a half without that application — and all the data your staff have loaded into it. Can your firm really afford that?

### **Data Security**

How secure is SaaS, especially for storing strategic corporate information?

This question is especially worrisome for any system devoted to gathering and analyzing sensitive information through surveys, questionnaires, and appraisals.

For instance, such a system could be used to research customer satisfaction, including any intentions to seek out alternate suppliers.

It could be used to gather product or service quality evaluations.

Internally, it could be used for HR purposes, such as employee performance and salary recommendations, 360-degree reviews, or to document reasons for leaving the company.

How comfortable are you with having all this information transmitted beyond your firewall over the Internet, and then stored off-premises by someone else?

Do you have any competitors who might enjoy a sneak peek at this information?

How much damage would it cause your firm if this data was ever compromised?

---

<sup>2</sup> "Google Apps' Gmail Faces Downtime Problems," IDG News Service, March 27, 2007.

As shown in Figure 2, an enterprise using licensed software installed behind its own firewall has little to risk from an information-gathering and analysis system. All your data, directory information, and in-house survey responses are under your own watchful eye.

But as shown in Figure 3 on the next page, each link in the chain outside your own firewall adds another possible point of failure. Using any SaaS system means that hackers can potentially intercept IDs, passwords, and demographics from any user, as well as survey responses from any respondent.

Many experts observe that people are the weakest link in this chain. And SaaS simply exposes your data to more people.

“Savvy technologists have painstakingly developed information-security solutions to minimize the risks connected with the use of computers, yet left unaddressed the most significant vulnerability, the human factor,” writes convicted hacker turned security advisor Kevin Mitnick.<sup>3</sup>

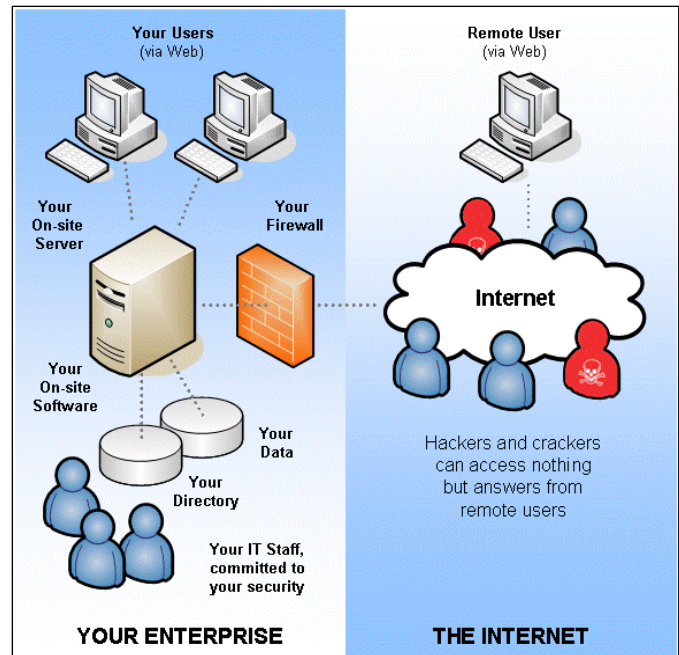
In chilling detail, his book presents more than 50 plausible scenarios for how easy it is to penetrate just about any company and pilfer its data.

The data security issue should give any prospective SaaS buyer pause. The more mission-critical the application, and the more sensitive the data, the more risky it is to choose SaaS.

### **Vendor Lock-in**

The story goes that anyone displeased with a SaaS vendor can just unplug and shift to another. But this vastly understates the pain of switching vendors.

<sup>3</sup> “The Art of Deception,” Kevin Mitnick, Wiley Publishing, 2002, page 23



**Figure 2: Security in the Licensed Model**

Every enterprise makes a major time investment in any new IT system, whether it’s licensed or delivered as SaaS.

For example, your SaaS users will need to learn the system, and set up options or preferences to suit their work habits.

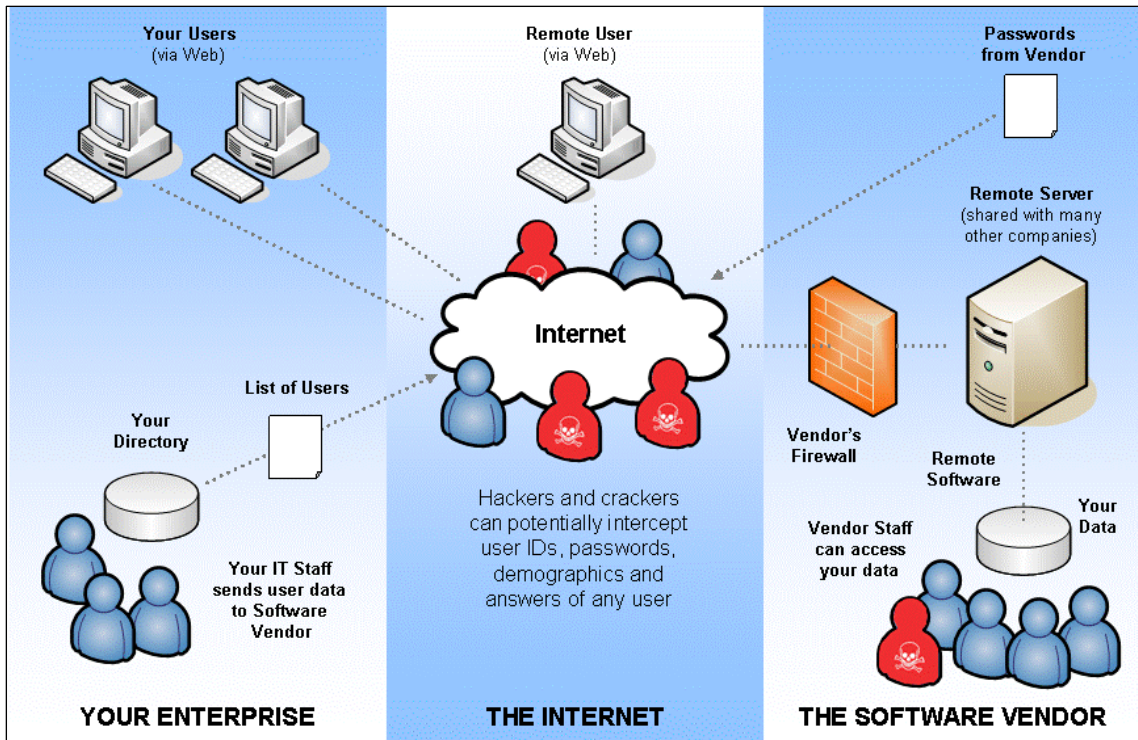
And they will input vast amounts of corporate data. These efforts represent a time investment of many person-weeks.

Unplugging from an unsatisfactory SaaS vendor may sound easy, but what about all that time? And even worse, what about all that data?

The reality is that selecting an IT vendor is never a flippant decision, and deselecting one is never quick and painless.

### **Workflow and Productivity**

Licensed software integrated into an enterprise infrastructure can save a lot of time through streamlined workflows and better productivity.



**Figure 3: Security in the Hosted Model**

The arm's-length architecture of SaaS can only slow down the productive use of these applications. For example, look at all the information exchanges in Figure 3.

**Selecting survey lists:** To set up a survey, a list of respondents and e-mail addresses must be prepared and sent to the SaaS host. With a licensed application residing on-site and properly integrated, these lists could be extracted by managers without any IT support.

Under SaaS, IT will have the added chore of extracting a multitude of lists for different purposes, and sending these to the SaaS vendor.

**Filling in background questions:** No one wants to answer mundane survey questions like their name, gender, department, employee number, and so on.

An on-site application well-integrated with enterprise systems can fill in all these fields automatically. Then a survey can focus on fewer and more useful questions,

save every respondent time, and enjoy a better response rate.

Yet a SaaS system without permission to look up this data in the HR or customer files will need to ask everyone all these questions.

**Increasing use of portals:** Many firms have invested in employee portals.

Licensed software running behind the firewall can leverage this investment by presenting surveys, appraisals, and 360-degree reviews through a portal.

This will add value and "stickiness" to any portal, as employees find yet another useful purpose for it.

But no SaaS application running outside the firewall can likely be granted this kind of access to an employee portal.

**Support for single sign-on (SSO):**

Requests for forgotten passwords eat up a large chunk of time from any help desk.

SSO schemes enable employees to sign in once when they first arrive at their workstations. From then on, the system will authenticate their identities as they access further software, portals, or Web services.

Yet a SaaS application will be outside any SSO scheme. This means employees will have to remember yet another set of log-in credentials.

**Integration with dashboards:** Many enterprises are also moving towards dashboards that display an ongoing readout of key performance indicators.

An internal system can feed results from information-gathering exercises directly to business information dashboards.

This integration is very likely beyond the scope of any SaaS application.

### ***Is SaaS Ever Preferable?***

Of course, there can still be times when SaaS is preferable.

For instance, suppose executives are pressing for enterprise feedback without backing a capital investment in a new information-gathering system that would make this exercise feasible.

Or perhaps IT is understaffed and not delivering adequate support, so that line managers are effectively on their own.

In cases like these, the low entry cost and quick deployment of SaaS may well outweigh any longer-term limitations.

There is no black-and-white answer to the question of whether SaaS is suitable; this question must be answered in the context of each enterprise and every department.

## **Conclusions**

This white paper has highlighted five areas where the SaaS business model may not be appropriate for information-gathering and analysis systems.

1. SaaS is not necessarily less expensive than licensed software, especially if an application runs three years or more and attracts a sizable user base.
2. Even the most well-established SaaS vendors experience frequent service interruptions.
3. Data security remains a critical issue, especially for highly sensitive information taken outside the corporate firewall.
4. Vendor lock-in may not be lessened with SaaS. Switching IT vendors always generates pain.
5. Without the benefit of integration behind the corporate firewall, workflows may be less productive for systems running as SaaS.

For all these reasons, enterprises must choose carefully between licensed software and SaaS.

Making a careful decision between licensed software and ASP is the best way to get the lowest costs over time, minimize risks, maintain tight data security, and see optimal results... especially from any new information-gathering and analysis system.