At your service.

The end of disruptive upgrades, lower TCO and allowing IT to shift to more strategic projects just skim the surface of the Software-as-a-Service model benefits.

By Bill Bulkeley

Software as a Service (SaaS) is an element of cloud computing that is growing rapidly. IDC notes that the SaaS market reached $13.1 billion in revenue in 2009, and forecasts that the market will grow to $40.5 billion by 2014, at a compound annual growth rate of 25.3%.

Many midsize organizations are at the forefront of adopting SaaS — and for good business reasons. Many may view it as the great equalizer to acquire enterprise class systems.

Indeed, many midsize businesses are deciding to adopt SaaS wholeheartedly because they have become more comfortable with the idea of hosting vital company data or even e-mail archives outside their own data centers. Still, security remains one of the primary concerns about cloud-based services.

While there are several factors that attract IT managers to adopt SaaS for their organizations, one of the most important is cost savings. The SaaS model is all about cost-effectiveness and ease of use, compared to the more costly alternative of buying packaged apps and hardware. "SaaS generally offers the most compelling TCO (Total Cost of Ownership) for small to midsize companies," says James Decker, senior manager of cloud/software strategy at Dell.

Buying software as a service means that a company doesn't start paying for a seat license until the software is needed for an employee. IT managers no longer need to guess how many users will need an application and acquire a few extra licenses in case growth is sharper than planned. They don't have to buy extra servers and software or expand a data center in anticipation of future needs. If operations shrink or a division is closed, the software bill drops immediately with each employee. "With subscription-based pricing, they pay for what they use," says Decker.

Using integration-services software, such as that provided by Dell, companies potentially can link and integrate applications in the cloud more simply than they could integrate legacy systems that sit entirely in their own data centers.

Another advantage is that SaaS features are continuously improved for free as part of the subscription price. That assures that employees are using state-of-the-art software without having to go through the periodic trauma of disruptive upgrades. Because the software is in the cloud, IT doesn't have to worry about installing patches or upgrades on every user's laptop and desktop.

All this brings up another major manpower advantage for IT leaders: They can shift their staffs' focus to more strategic projects for the business instead of spending time on maintenance and implementation tasks.

IT staff as strategists.

When the more mundane IT tasks are taken care of, IT managers are also able to focus on business needs and be more responsive to C-level executives. But that means IT workers "need to understand how the sales team operates," Decker says.

In many midsize businesses, for instance, functions like sales have already moved to SaaS for customer relations management (CRM) applications like Salesforce.com. IT managers are finding SaaS applications that they can apply to their own operations, improving the core efficiency of the IT department, which in turn helps improve the efficiency of the business.

The key is figuring out "what is in it for the IT professional?" says Matthew Keeler, senior manager, SaaS and cloud-based services at Dell. He says that companies like Dell provide SaaS tools that make it simple to architect how data will flow between applications inside the corporation and in cloud-hosted applications. Such tools eliminate "a huge barrier to adoption" in midsize businesses, he says.

Dell's "current offerings are focused on IT management" rather than business applications, Keeler says. Specifically, Dell provides SaaS to simplify integration projects and to centrally manage users' client systems and business-critical data.

SaaS tools can also be applied to one of the thorniest IT problems: managing user devices. Desktops, often scattered in branch offices, and laptops that travel with salespeople and executives are hard to keep track of and update. IT-focused

SaaS offerings, such as those from Dell, help to automate the task of managing software and encrypting data on laptops.

Capabilities like enforcing encryption of laptop data are convincing many IT managers that the security benefits of SaaS outweigh the risks. One CIO for a midsize healthcare provider that employs home healthcare nurses recently said he worried about them having patients' private health information on their laptops. This CIO said he solved the problem for mobile laptops by requiring that the entire disk be encrypted so that if it is lost, nothing can be read. "As the business benefits of SaaS continue to gain proof points, SaaS adoption among midsize businesses will continue to accelerate," says Keeler.

Bill Bulkeley is president of Green Line Research, a Boston-based company specializing in reports in the high-tech field.

SaaS security concerns fast fading.

"Security of the public cloud is a key concern" for IT managers who are considering SaaS, says James Decker, senior manager of cloud/software strategy at Dell.

Many IT managers are uncomfortable having corporate data and applications outside their own data center where they maintain physical security and data security.

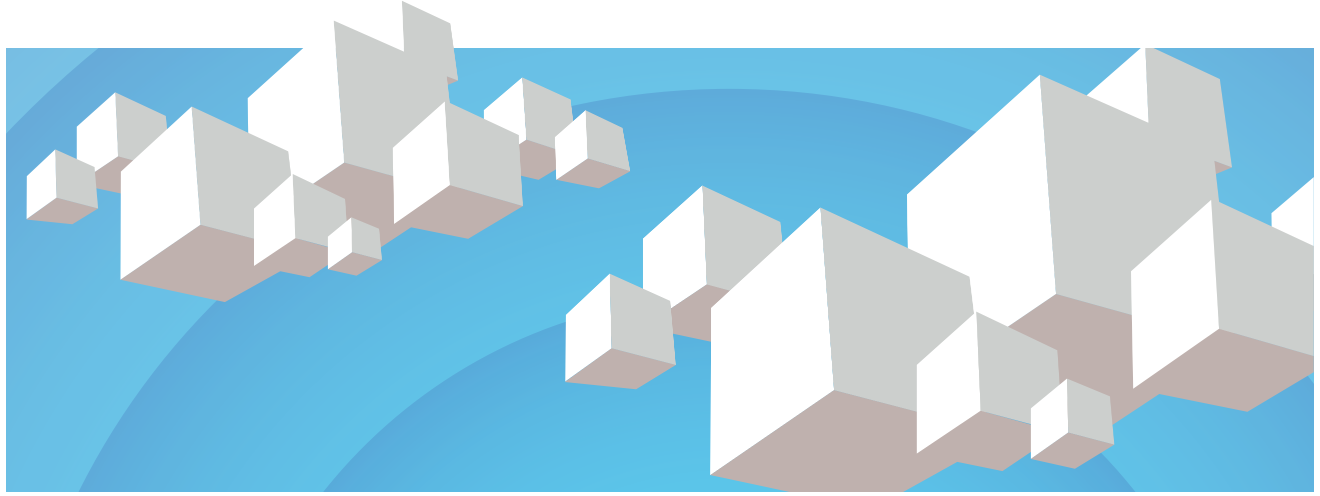
Once data is in a cloud, by definition, the data owner can't control which server it is on or which networks are used to access it. The efficiency benefits of SaaS are only produced when the capacity of servers in the cloud is shared among applications and is expanded or contracted to meet growing or shrinking demand.

As SaaS providers improve their security, many midsize companies are concluding they can deal with the security risks of SaaS as easily as they can with their internal legacy systems.

Indeed, Jeff Kaplan, managing director of ThinkStrategies, says: "The fact is that one of the benefits of the SaaS model when it's implemented properly is that everyone gets to share the level of security and reliability expected by the most demanding of customers."

Kaplan notes that banks, insurance companies and even the U.S. Department of Defense use SaaS for some applications. He says the key for IT managers is to require a service-level agreement from any SaaS supplier specifying user-access controls, backup and recovery measures and regular security vulnerability tests.

Decker notes that in some ways SaaS applications have improved security because they make it easy for IT to enforce encryption standards on all company data. Still, it can be inconvenient for workers using many different SaaS applications because they usually have to log into each one separately.



Dell steps up with SaaS solutions.

"In our SaaS portfolio today, we're focused on IT management," says Matthew Keeler, senior manager, SaaS and cloud-based services, at Dell. To help IT, Dell offers services that help integrate various SaaS offerings together. It also helps them manage user devices and business-critical data.

Using Dell Integration Services, IT departments can build and deploy new applications in hours by integrating different data and software with cloud-based applications. Then they can monitor all the business processes on a Web-based dashboard that shows the flow of information and can help spot bottlenecks. Since it's SaaS, they don't have to install or maintain any software products or worry about hardware capacity. And pricing is based on the number of integration connections needed for the application.

Dell also offers IT Management SaaS to help the IT department track and manage Windows-based PCs, wherever they may be. The solution provides continuous control and visibility of distributed assets. It automatically discovers and manages the PCs, whether they are connected by an internal network, a virtual private network or even over the public Internet.

That information enables IT to use the application to identify potential security problems and enforce enterprise policies. It can also locate unauthorized software on remote PCs that might cause security problems. It can enable data encryption to secure sensitive data.

"All those things are designed to make the life of an IT manager easier," Keeler adds.