3 Arguments Against Enterprise SaaS That Fall Flat

By Jeffrey Vogel, Bulger Partners and Mike Kavis, Cloud TP

In the world of Enterprise Software, on-premises solutions are becoming rare. The economies of scale that comes with the cloud combined with the innovation and agility of fully SaaS ISVs has led to a world of primarily SaaS-based enterprise applications. However, there are vestiges, particularly with large conglomerate ISVs (Oracle, IBM, Microsoft, SAP), of classic on-premises solutions and deployments.

In this article, we explore some of the reasons for those vestiges, hypothesize on what motivates enterprise IT to support them, and decide whether there will be changes in the near-term that enable a complete transition to SaaS.

The Value of SaaS

The benefits of SaaS are easy to enumerate. Instead of investing large amounts of time and money on people and technology to build or deploy an application, enterprises can simply "turn on" a SaaS offering and pay for only the services that they use. The "pay as you go" model of cloud computing allows enterprises to get to market quickly at a very low cost of entry.

In addition, the need to continually sink money into the product for things like upgrades, additional features, and adopting new technologies goes away

as that responsibility shifts to the vendor. This also frees up resources to focus on other priorities and allows an enterprise to reduce the overall resource needs in certain areas. So why would an enterprise push back on SaaS?

Not in My House

Sometimes enterprise IT executives think their requirements are so different than those of other companies that they cannot be met by a SaaS provider. This thought process is often nothing more than a poor excuse that tends to fall into one of three categories:

1. **Customization/Configuration Limitations**
2. **Integration with legacy systems**
3. **Security Concerns**

Customization/Configuration Limitations

Most large companies accumulate a variety of proprietary processes over the years that can make it hard for SaaS solutions to succeed. Instead of revisiting why some of the non-value-add legacy processes exist, they often declare that no SaaS solution can meet the requirements of their application.

We have witnessed a company build an entirely new accounting system from scratch because they refused to change a small subset of business rules that really added no value to the company. They spent over two years building a homegrown solution, for an application that has many proven SaaS solutions readily available in the market place.

> "The reality is that today's SaaS applications are highly configurable."

To make matters worse, once it was implemented they had a long list of enhancement requests for capabilities like mobile, advanced analytics, and other features that would take months to implement.

The reality is that today's SaaS applications are highly configurable, often at least as configurable as their on-premises predecessors. Many of them have built-in rules engines, extensible workflow engines, standardized scripting languages, connectors to various third party solutions, single sign-on capabilities, drag-and-drop user interface customization, self-service administration, and much more.

It is not that these customization techniques are unique to SaaS applications, but rather a fortuitous coincidence that throughout the past 10 years while the cloud was evolving, so too were the aforementioned modern techniques for customizing applications.

For capabilities that are not a core competency of an enterprise, IT would be hard pressed to justify why the needs of the business could not be met with one of the leading SaaS solutions.

Integration with Legacy Systems

Most enterprises IT systems are built on stacks that span multiple technology eras, from mainframe, to client server, to three-tier web, to the cloud. In the early days of SaaS this presented great challenges, but over the years SaaS products have solved this issue with APIs to make integration simple and efficient.

In fact, many SaaS solutions come with out-of-the-box connectors to leading vendor solutions while also providing simple ways for enterprises to quickly build custom connectors to their proprietary solutions.

Furthermore, application integration and data integration vendors offer shrink-wrapped solutions for integrating hundreds of legacy and SaaS applications as well as extension capabilities for custom in-house applications.

Security

The biggest reason for resisting SaaS is concern over security. Many enterprises simply refuse to accept the notion of allowing sensitive data to live outside of their firewall. A study by Alert Logic in the spring of 2013 came to the following conclusions:

- The cloud is not inherently less safe than enterprise data centers.
- Attacks in external cloud environments tend to be crimes of opportunity, while those in enterprise data centers tend to be more targeted and sophisticated.
- Web applications are equally threatened in cloud and enterprise data centers.

> "What this report proves is that the security threats are the same, regardless of where the data resides.."

What this report proves is that the security threats are the same, regardless of where the data resides. What is even more interesting is that the success rate of penetrations from outside threats was much higher in enterprise data centers than in external cloud environments.

Based on this information, skeptics should dismiss the notion that data cannot be as secure in the cloud as it is behind the corporate firewall. We call this the "hypocrisy" of enterprise IT.

It is almost comical when people declare SaaS to be unsecure while their company transmits unencrypted email, staff members have company information on personal unsecured mobile devices, and a number of systems run on unsupported or unpatched versions of software on premises.

Major Security and Data Breaches

Since 2013 there have been many enterprise security breaches affecting hundreds of millions of customers. Not one of these breaches involved a SaaS provider.

If we look at some of the most recent security breaches (listed in the chart below), we should quickly realize that all of these nightmare scenarios took place in on-premises settings. Losses of sensitive data may not even be tied to IT itself. For example, at JP Morgan Chase a disgruntled employee posted personal information of 900 of the firm's wealthiest customers on the internet.

Increasingly, a large number of breaches are the result of insider and privilege misuse, leaks of information from paper documents, and lost or stolen devices and media.

Recent breaches at Target and Home Depot occurred within the physical Point of Sale (POS) infrastructure and had nothing to do with the cloud. The Sony hacks, orchestrated by North Korea, were a breach of an on-premises datacenter.

In June, hackers attacked the JP Morgan Chase corporate network, gaining access to the bank's data center to expose the personal information of 76M customers. Many of the other top data breaches of 2014 were focused around POS, ATM, and payments systems, none of which were cloud based.

As long as we have enterprise IT and

COMPANY	BREACH TYPE	PEOPLE AFFECTED
The Home Depot	POINT OF SALES	56M
J.P.Morgan	EMPLOYEE	900
JPMorgan Chase & Co.	DATA CENTER	76M
SONY	ON-PREMISE DATA CENTER	47K
TARGET	POINT OF SALES	70M
Adobe	INTERNAL SYSTEMS	3M

internet connectivity, on-premises systems will continue to be breached. With this in mind, can we take the security concerns about SaaS seriously, or is it simply cover for job protection within enterprise IT?

While the naysayers are decrying SaaS as unsecure, their businesses are demanding that IT become more agile. At what point do these ultra conservative claims regarding SaaS give way to the agility demands of the business?

Conclusion

There is a lack of compelling data to support the argument that SaaS solutions are less secure than on-premises, "behind the firewall" proprietary solutions. Couple that with the high costs of building and managing proprietary solutions and the demanding business requirements to deliver more quickly, it becomes clear that the postponement of SaaS as a viable enterprise option is a losing proposition.

We believe that over the next 5-10 years there will be a drastic reduction in the amount of behind the firewall on-premises applications and broad adoption of SaaS as the preferred delivery model. Even proprietary software will continue to shift to a SaaS model. Ultimately, those companies that continue to fight SaaS will struggle to stay competitive in today's demanding market. b

About the Authors

bulgerpartners

Jeff Vogel is a Managing Director at Bulger Partners.

He is co-head of the strategy consulting practice with deep hands-on expertise helping software companies manage growth, product, R&D and integration.

info@bulgerpartners.com
www.bulgerpartners.com

Cloud Technology Partners

Mike Kavis is a Vice President & Principal Cloud Architect at Cloud Technology Partners.

He leads the firm's DevOps and Internet of Things practices.

info@cloudtp.com
www.cloudtp.com