Dispelling 5 Common SaaS Myths

WHITE PAPER

CFOs have clearly bought into the value of software as a service (SaaS), as evidenced by research firm MarketsandMarkets' prediction that the market for financial applications in the cloud will grow nearly 25% annually to more than $29 billion by 2021.[1] Business agility and the availability of powerful analytical tools are just two of the many drivers of this trend.

But IT managers don't always share their colleagues' enthusiasm, particularly at small and midsize businesses that have historically managed IT internally. As guardians of their organizations' precious data assets, IT managers are instinctively cautious and may believe that giving control of servers and critical applications to a cloud provider is risky. Security, systems management, compliance and performance are also often cited as concerns.

These concerns are largely overblown, with many of them rooted in outdated perceptions. Commercial SaaS has greatly matured in the more than 20 years it has been available. The value proposition is compelling: cloud providers enjoy economy-of-scale cost savings that they pass on to their customers as subscription or usage-based prices. The same economics also enables them to provide security, availability and data protection that exceed the capabilities of all but the largest enterprises.

This paper helps financial professionals address five of the most common myths about the cloud in general, and SaaS in particular, so that they can build a collaborative approach to cloud adoption with their IT partners.

TechTarget | Custom Media

sage Intacct

Myth 1: Moving to the cloud means losing control.

Few businesses would say that managing computing infrastructure, installing and testing applications, applying updates and securing against cyberattacks is a core competency. For cloud service providers, however, expertise in these areas is essential to their business. They have spent two decades building world-class proficiency.

Cloud platform and SaaS providers unburden customers from the tedious and often risky details of managing infrastructure and applications. They provide reliable and scalable service and keep current with all the latest updates and patches. Contracts and service-level agreements (SLAs) guarantee specified levels of reliability, performance and availability. All other control rests with the customer, who owns the data and gets the benefits of speed, agility and flexibility without the cost and complexity of managing infrastructure and applications.

An often unspoken but valid concern is that the IT function will be marginalized if control passes to a cloud provider. That is never the case. Bettercloud reported that 78% of organizations expect at least 80% of their business applications to be SaaS by 2022, more than double the 38% today.[2] As companies grow, their usage accelerates; Blissfully says companies with 250 to 1,000 employees use an average of 124 SaaS applications compared to 72 for companies with fewer than 50 users.[3]

IT plays a vital role in selecting and integrating vendors, managing data, monitoring SLAs and maintaining vendor relationships. IT's value shifts from configuring equipment to powering the business, making the function more critical and strategic than ever.

Myth 2: Cloud security is questionable.

This myth is rooted in one misperception and one out-of-date perception. The misperception is that the record number of breaches of data stored in the cloud in 2019 casts doubts on cloud security.[4] The reality is that these breaches of public cloud data stores are almost always the result of user error rather than security failures.

Public cloud operates under a shared responsibility model in which infrastructure security is provided by the cloud vendor while customers are responsible for application and data security. Unfortunately, many customers don't understand this distinction. Enterprise Management Associates found that 53% of the IT and security professionals it surveyed believe infrastructure as a service (IaaS) providers are accountable for most or all public cloud security.[5]

Cloud infrastructure operators are working to simplify administrative complexity to reduce mistakes, but they can't guard against ineffective access controls or simple human error, which is responsible for nearly 90% of data breaches, according to Willis Towers Watson.[6]

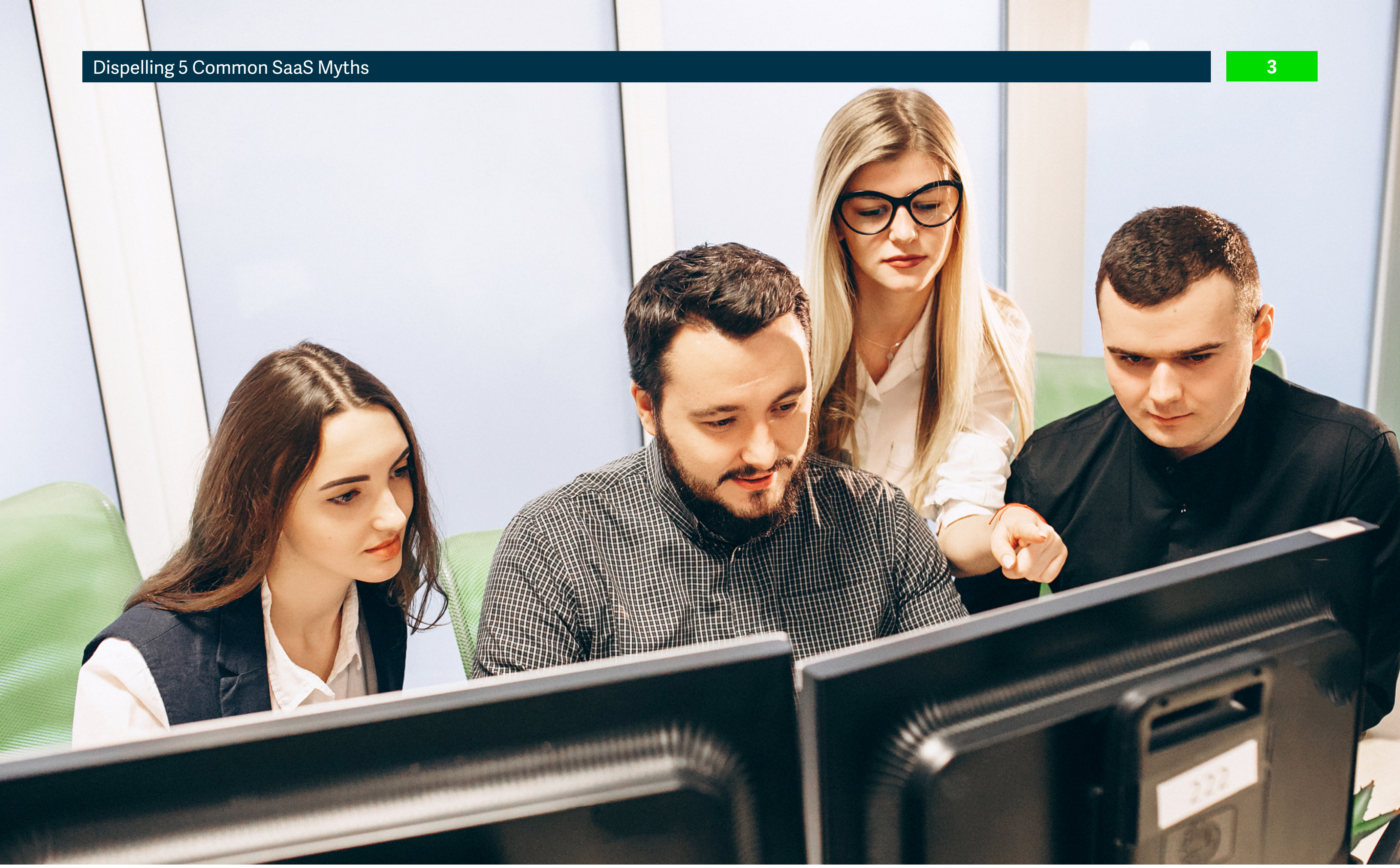
The outdated perception goes back to the early days of public cloud, when occasional security incidents occurred as major providers were building their infrastructure. The reality is that there hasn't been a publicly reported breach of a major cloud infrastructure provider since 2010.[7] Over time, cloud providers have built protections that exceed those of the world's largest enterprise data centers. They spend billions of dollars annually on security and can afford to hire top talent. Recent studies have shown that security has gone from being a negative to one of the best reasons to move to the cloud.

> Recent studies have shown that security has gone from being a negative to one of the best reasons to move to the cloud.

SaaS providers deliver even greater peace of mind because their involvement extends to the application level. SaaS companies make it a priority to keep current with patches and ensure that strong access controls such as multifactor authentication are in place. They use world-class backup and recovery practices for data protection. These companies know that a breach would cause a catastrophic loss of customer confidence and so take every possible preventive measure.

Myth 3: SaaS offers no scalability or availability guarantees.

The reality is that no one can ever guarantee availability on-premises or in the cloud because of the number of factors that are beyond the hosting provider's control. That said, for the reasons listed above cloud companies are much better equipped to provide reliable availability. They employ the best protections against such disruptions



as regional outages and denial-of-service attacks and use state-of-the-art failover and backup practices that few of their customers could afford. Cloud SLAs also provide customers with remedies when service levels aren't met.

Cloud vendors over-provision infrastructure to avoid scalability issues. For example, the Sage Intacct cloud data center contains more than 10,000 CPUs and more than 100 terabytes of RAM to handle more than 1 million application request per day. Workloads are constantly monitored to ensure that they never exceed 33% of capacity, providing customers with both high scalability and performance.

Myth 4: Cloud applications can't be customized.

This may have been true of some very early SaaS applications, but modern instances are extensible by design.

Customizing packaged applications is a controversial practice. Modifications to the code can introduce dependencies that invalidate support agreements and limit customers' ability to stay current with new software releases. The process is labor-intensive, requires extensive testing and even then can't be guaranteed to be reliable.

Cloud software providers rely upon extensible platforms for customization and application program interfaces (APIs) integration. An extensible application can be extended without modifying its original code base using platform-as-a-service tools, plug-ins and/or modules. For example, an insurance company might use extensions to add custom fields to its invoices without altering the underlying invoicing functionality of the host application.

APIs are documented interfaces and protocols that specify how software components interact with each other. They enable custom features and companion applications to be safely "plugged in" to the core application. For example, an expense reporting application can be integrated with a core accounting system using published APIs without requiring code modification on either side.

Both techniques make customizations both more reliable and persistent. For example, some Sage customers are still using API-based customizations that were built in 2001. Sage handles more than 1 billion application API calls per month.

Another benefit of APIs is that they enable SaaS providers to extend functionality through ecosystem partners. For example, customer relationship management systems like Salesforce.com or bill payment applications like Bill.com can be integrated with the core finance system in just a few clicks. Customizations are up to date with the latest regulations and patches and bug fixes are applied rapidly.

Myth 5: SaaS won't meet my compliance needs.

Maintaining compliance with laws and regulations is a complicated process that requires expensive expertise. Few companies would call it a core competency.

While some rules and jurisdictions preclude the use of SaaS by requiring data to be kept on-premises, most regulatory scenarios can be readily accommodated. In fact, companies are usually better off using software partners with vertical industry expertise than attempting to manage compliance themselves.

For example, many companies spent millions of dollars to become compliant with the ASC 606 revenue recognition accounting standard, which went into effect in 2018. Sage Intacct was preparing its accounting software three years before the rules went into effect, and was fully compliant more than a year before the deadline.

By choosing a SaaS provider with a strong track record in the customer's industry and a robust partner ecosystem, users can rely upon third-party experts to improve compliance. SaaS customers benefit from a far more abundant choice of options in this respect than users of packaged applications.

Sage Intacct was preparing its accounting software three years before the rules went into effect, and was fully compliant more than a year before the deadline.

Conclusion

Innovation in the software industry has clearly moved to the SaaS model as the mass migration noted at the outset of this paper proceeds. Nearly every new software company that has launched over the past five years uses a SaaS delivery model and many vendors of legacy applications are now actively encouraging their customers to migrate. For customers seeking the agility the digital business demands, SaaS is no longer an option but a mandate.

We hope this paper has dispelled some of the common misperceptions. Having this up-to-date information in hand should better prepare finance and IT professionals to approach the SaaS decision with confidence.

[1] "Finance Cloud Market by Solution (Financial Reporting and Analysis, Security, Governance, Risk and Compliance), Service, Application, Deployment Model, Organization Size, Vertical, Region - Global Forecast to 2021," MarketsandMarkets, December 2016.

[2] "2017 State of the Saas-Powered Workplace," Bettercloud, 2017.

[3] "2018 Q1 SaaS Trends Report," Blissfully, 2018.

[4] "2019 MidYear QuickView Data Breach Report," Risk Based Security, 2019.

[5] "Security Megatrends," Enterprise Management Associates Research, January 2019.

[6] "Almost 90% of Cyber Attacks are Caused by Human Error or Behavior," ChiefExecutive.net, March 2017.

[7] "Microsoft Cloud Data Breach Heralds Things to Come," PCWorld, December 2010.