SaaS Adoption Requires A New Approach To Information Security
Complacency And Confusion Pose Threats In An Increasingly Popular Delivery And Consumption Model
Table Of Contents

Executive Summary .................................................................................................................. 1
SaaS Applications Are Here To Stay ..................................................................................... 2
Comprehension Of SaaS Security Responsibility Is Outpaced By Adoption..................... 4
IT Is Complacent With Legacy Security Protections — And That’s A Mistake............. 4
SaaS Calls For A New, Integrated Approach To Security ................................................. 5
Key Recommendations ........................................................................................................ 6
Appendix A: Methodology .................................................................................................... 7
Appendix B: Supplemental Material .................................................................................... 7
Appendix C: Demographics/Data ........................................................................................ 7
Appendix D: Endnotes ........................................................................................................... 8

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester’s Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2014, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com. [1-PBG77X]
Executive Summary

The advent of software-as-a-service (SaaS) application adoption has the potential to produce dramatic benefits for businesses across industries, not the least of which is the ease and flexibility of access to the information needed for productivity. Combine this benefit with the increasing popularity of bring-your-own-device (BYOD) and “shadow IT” practices (IT solutions deployed without the approval or involvement of the IT department), and the march is on toward a truly anywhere, anytime, any-device workforce. With this increased flexibility, however, come increased risks to the security of critical data and business communications as users deploy SaaS applications on unmanaged devices and over non-corporate networks. Now, more than ever, it is imperative that firms understand the true nature of these risks and have strategies in place to proactively combat them.

In January 2014, Adallom commissioned Forrester Consulting to evaluate IT decision-maker attitudes toward security in the context of SaaS, BYOD, and shadow IT, and to assess the steps decision-makers are taking to confront these concerns while supporting the needs and desires of the business. To further explore the subject, Forrester tested the hypothesis that a gap in understanding exists in enterprise IT between knowing where the responsibility for SaaS security controls begins and ends and what SaaS vendors are responsible for versus the enterprise that consumes these services.

71% of security decision-makers say they understand their accountability for SaaS security, but this figure diminishes significantly when specific aspects such as liability and division of responsibilities are dissected.

In conducting in-depth surveys with 150 IT professionals responsible for information security, Forrester found a high level of SaaS adoption, as well as permeation of shadow IT practices. While some respondents indicated that they use security solutions specifically geared toward SaaS applications, far more displayed a false sense of security in older technologies unsuitable for such use. Furthermore, the study found evidence of confusion regarding the division of security responsibility with regard to SaaS. Looking forward, respondents expressed interest in more advanced security capabilities tailored to this new era of IT.

KEY FINDINGS

Forrester’s study yielded four key findings:

- **SaaS adoption cannot be ignored.** SaaS applications are now included as a prominent piece of IT portfolios across industries. Furthermore, in addition to applications supported by IT, a crop of shadow IT applications introduced by individuals or lines of business are also a large piece of the equation, presenting business opportunities and insights, as well as new and heightened security risks.

- **IT decision-makers have a false sense of comfort with existing controls for SaaS security.** The security decision-makers we surveyed expressed confidence in the ability of their existing controls, such as firewalls and VPNs, to protect digital assets in SaaS applications. This confidence is ill placed, however, as SaaS adoption and BYOD are conjoined, introducing new vulnerabilities that legacy security tools simply don’t address, such as those used in data protection and configuration management.

- **Many SaaS customers do not understand the division of security responsibilities.** Despite an overarching sense of confidence in their comprehension of SaaS security responsibilities, security professionals struggle with the specifics of their contractual agreements and mistakenly place the onus of usage integrity and data loss prevention on their SaaS providers.

- **IT security is a shared responsibility best addressed by seamless integration of SaaS provider and customer tools.** Security is no longer the sole domain of IT departments; it is instead a shared responsibility between multiple stakeholder groups (including, but not limited to, IT security, business stakeholders, IaaS providers, and SaaS providers) as new technologies take hold. Seamless integration of security tools on both the user and cloud provider sides, with advanced capabilities such as behavioral analytics, are often viewed by forward-thinking security professionals as components of a solution to this challenge.
SaaS Applications Are Here To Stay

It’s no longer appropriate to look forward to the cloud computing future. We’re well into the era in which we’re no longer tied to our data centers or our desks, as various industries increasingly embrace the “anytime, anywhere” mentality of work. Many companies are ramped up to this state and expanding their cloud strategies, and many more are racing to catch up to cloud computing.

Software-as-a-service (SaaS) applications are no small part of this evolution, and their benefits are many. Information workers now have easy access from practically anywhere to a variety of capabilities far beyond those provided in early ERP and CRM use cases. Today, many companies count on these “on-demand” resources for productivity, file sharing, and IT service management purposes, and the upward trajectory of adoption across myriad use cases is clear (see Figure 2).

Key among the effects of this fundamental shift for IT and security professionals include:

FIGURE 1
Shadow IT Is Seen As A Permanent Fixture Of The Modern Organization

“Please indicate which of the following statements you agree with the most.”

<table>
<thead>
<tr>
<th>Statement</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shadow IT is here to stay and cannot be ignored</td>
<td>43%</td>
</tr>
<tr>
<td>Shadow IT provides significant opportunities to the firm to improve its security posture</td>
<td>33%</td>
</tr>
<tr>
<td>Shadow IT must be blocked</td>
<td>10%</td>
</tr>
<tr>
<td>Shadow IT can provide stronger security than our organization can on its own</td>
<td>5%</td>
</tr>
<tr>
<td>Shadow IT can be ignored, it’s just a fad</td>
<td>5%</td>
</tr>
<tr>
<td>None of the above</td>
<td>4%</td>
</tr>
</tbody>
</table>

Base: 150 US IT decision-makers with responsibility for SaaS security
Source: A commissioned study conducted by Forrester Consulting on behalf of Adallom, February 2014

FIGURE 2
SaaS Is Proliferating Across The Application Landscape

“What are your firm’s plans to use software-as-a-service (SaaS) to complement or replace the following applications?”

<table>
<thead>
<tr>
<th>Application</th>
<th>Plan to complement with some SaaS within two years</th>
<th>Plan to replace most/all with SaaS within two years</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaboration software</td>
<td>23%</td>
<td>13%</td>
<td>1,052</td>
</tr>
<tr>
<td>Business process management (BPM) software</td>
<td>19%</td>
<td>10%</td>
<td>520</td>
</tr>
<tr>
<td>Customer relationship management (CRM) software</td>
<td>18%</td>
<td>11%</td>
<td>1,135</td>
</tr>
<tr>
<td>Project portfolio management (PPM) software</td>
<td>18%</td>
<td>10%</td>
<td>549</td>
</tr>
<tr>
<td>Learning management software</td>
<td>16%</td>
<td>12%</td>
<td>637</td>
</tr>
<tr>
<td>ePurchasing software</td>
<td>16%</td>
<td>11%</td>
<td>456</td>
</tr>
<tr>
<td>Content management software</td>
<td>16%</td>
<td>10%</td>
<td>965</td>
</tr>
<tr>
<td>Product life-cycle management (PLM) software</td>
<td>15%</td>
<td>10%</td>
<td>451</td>
</tr>
<tr>
<td>Business intelligence software</td>
<td>17%</td>
<td>8%</td>
<td>1,081</td>
</tr>
<tr>
<td>Human capital management software</td>
<td>14%</td>
<td>11%</td>
<td>766</td>
</tr>
</tbody>
</table>

Base: software decision-makers using the software in question and planning to replace the software with most/all SaaS or are planning to complement the software with some SaaS
A proliferation of BYOD. As the lines between work and personal life blur, so do those between our work and personal devices. An employee may be more content to update a report curling up on the couch with her tablet than setting up a bulky laptop in the dining room, underscoring the bring-your-own-device (BYOD) phenomenon. As this practice becomes more and more common, it is critical to ensure that it poses no threat to sensitive data.

The emergence of departmentalized SaaS. As individual lines of business learn of new apps that boost productivity, better serve their customers, enable mobility, and are available as-a-service, they are increasingly circumventing formal IT provisioning processes that they view as ineffective or slow. Chief information security officers (CISOs) in turn learn of subsequent vulnerabilities after the service is in place and often have no opportunity to vet or sanction the apps.1

The need for a firm grasp on security responsibilities. With so many digital assets, and even infrastructure components, being placed outside the four walls of the organization, there is a new and heightened imperative to understand which party is responsible for which aspect of workload configuration and network security.

Despite the challenges and risks, IT professionals view the rise of shadow IT, a reliable precursor to accelerated SaaS adoption by individual lines of business, as a development with staying power. Many IT professionals also acknowledge that shadow IT practices can help improve their own policies and operations (see Figure 1). Survey respondents agreeing with this latter sentiment expressed that shadow IT behavior can help them understand which services IT should prioritize sanctioning or supporting (54%), which services represent the most risk (50%), and even how to rethink the role of IT security (38%). It is no surprise that only a minor portion of respondents thought that shadow IT should be blocked (10%). Instead, respondents said that proactively responding to the challenges of shadow IT is more important. Respondents also said that shadow IT could potentially help them develop an understanding of what types of services users and lines of businesses were turning to shadow IT because IT had failed to provide them with what they needed (36%).

FIGURE 3
Security Professionals Believe They Understand SaaS Provider Contracts But Express Confusion Around Specifics

<table>
<thead>
<tr>
<th>Question</th>
<th>Strongly agree</th>
<th>Agree</th>
<th>Neutral</th>
<th>Disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Thinking about the management of your organization’s security controls, how well do you understand the division of responsibility between you and your cloud services provider(s) as stipulated in the contract(s) governing your relationship(s)?”</td>
<td>24%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“Please indicate your level of agreement with the following statements regarding responsibility boundaries between SaaS providers and the on-premises environment.”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SaaS providers make unrealistic or overstated security claims</td>
<td>39%</td>
<td>32%</td>
<td>20%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Limits of liability are hard to find or understand</td>
<td>39%</td>
<td>27%</td>
<td>24%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>Contractual agreements (MSA, SLA) are not clear</td>
<td>19%</td>
<td>30%</td>
<td>40%</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>It is hard to identify the boundaries between our organization’s on-premises infrastructure and security measures versus those of the SaaS provider</td>
<td>42%</td>
<td>30%</td>
<td>21%</td>
<td>4%</td>
<td></td>
</tr>
</tbody>
</table>

Base: 150 US IT decision-makers with responsibility for SaaS security
Source: A commissioned study conducted by Forrester Consulting on behalf of Adallom, February 2014
Comprehension Of SaaS Security Responsibility Is Outpaced By Adoption

To securely implement SaaS products and take full advantage of the benefits they afford, it’s not enough to know what threats and vulnerabilities this delivery and consumption model presents. It’s also critical to hold a firm understanding of which party is responsible in the event of a breach. The combination of this new technology and its unique vendor-customer relationship, however, makes this easier said than done.

› IT decision-makers are confident in their general contractual understanding. In our research, a sizable 71% of respondents claimed to completely or mostly understand the division of security control responsibility as stipulated by their contracts, with only 6% claiming to have limited or no understanding (see Figure 3).

› Knowledge of specific security responsibilities is much hazier. Despite an overall positive attitude toward their contractual obligations, survey respondents were less self-assured when asked about specifics. A mere 21% disagreed with the notion that SaaS providers make overstated security claims, for example, and only 25% believed the boundaries between their on-premises infrastructure and those of SaaS providers were reasonably identifiable (see Figure 3).

› Ambiguity dominates the vendor/customer security dynamic. Just as, if not more, notable in our data were the consistently large groups of neutral responses to questions around specific SaaS security statements and questions. Between one-quarter to one-third of those we surveyed neither agreed nor disagreed with assertions of unclear service-level agreements (SLAs) and limits of liability (see Figure 3).

› Popular perceptions of vendor liability are false. Nestled among the confusion is an overarching sense that SaaS, IaaS, and PaaS vendors bear the responsibility for a data breach, with 86% placing the onus on those parties. This misunderstanding leads to a mistaken sense of complacency among adopters. Upon looking carefully at a contract with a cloud provider, one will often find “best effort” or “no direct liability” clauses that prevent the vendor’s customers from holding it directly liable for any data loss for which the customer is custodian or owns. The Cloud Security Alliance guidance version 3.0 agrees: “When data is transferred to a cloud, the responsibility for protecting and securing the data typically remains with the collector or custodian of that data.”

IT Is Complacent With Legacy Security Protections — And That’s A Mistake

Once armed with a concrete and objective grasp of accountability in the face of a SaaS security compromise, IT professionals need to look in the mirror and make an honest evaluation of how vulnerable their entities are and what they can do to protect their digital assets. Protocols and policies play fundamental roles in preventing data loss, but with a firmly ingrained “anytime, anywhere” mentality among the modern workforce, and an explosion of applications to enable them, policies won’t be enough. Security technologies are ultimately what keep the wolves at bay when the organization’s understanding of risks is fuzzy.

The risks that public cloud services introduce are fundamentally different from those you’ve seen in the past. By default, you do not control the cloud provider’s environment in terms of configuration management, network security, identity and access management, privileged identity management, data protection, security incident and event management (SIEM) integration, intrusion detection/prevention, etc. The very nature of how knowledge workers access these applications, and the devices on which they do so, presents a host of susceptibilities that simply aren’t addressed by the safeguards you’re used to, and good luck convincing your SaaS vendor to provide insight into the steps it takes to combat them or grant a view of their security logs. According to our data, these differences are not well understood, and there is widespread confusion and dangerously false senses of security among IT professionals.

› IT decision-makers overwhelmingly believe their existing controls to be effective for SaaS. A whopping 92% of respondents to our survey indicated a belief that their existing security controls are either effective or very effective in protecting their digital assets in SaaS applications.

› Perimeter and endpoint protections are erroneously credited as protective. Not only do a vast majority of respondents put faith in their legacy controls, but the
controls they cited are outdated perimeter protections such as firewalls (35%) and virtual private networks (VPNs) (29%) (see Figure 4). Unfortunately, security professionals with this mindset are rolling the dice with their sensitive data. Perimeter and endpoint protections can largely protect against threats that are well understood, but they provide minimal protection against new, emerging, and largely unknown threats; they are ineffective when the endpoint is unmanaged and off-premises.

SaaS Calls For A New, Integrated Approach To Security

Modern risks to digital assets are very real. Companies experiencing data breaches and employee misuse of authority to commit fraud are legitimate concerns that can produce catastrophic results such as sanctions, fines, and loss of goodwill. Outdated technologies and ubiquitous confusion toward what the threats are, how to combat them, and even who is accountable, amplify the murky nature of protecting modern digital assets. The use of hardcoded, rules-based policies and legacy protection tools is largely ineffective when trying to mitigate the risks associated with SaaS. However, security professionals need not fear, as the policies, capabilities, and general approaches to adaptation to this new IT era are proven and implemented at many forward-thinking firms.

› Treat security as a shared responsibility. Less than a quarter of survey respondents indicated information security as a core competency of the IT organization. Our data also showed that 40% had a more evolved view of shared responsibility across all stakeholders, including lines of business and cloud providers. Work collaboratively with your SaaS vendors to ensure you have a comprehensive understanding and purview into the security of your users and data.

› Knock down security silos through integration. Disparate security tools from your organization, SaaS providers, and elsewhere can operate at odds with each other and lead to poor experiences among end users, thereby inviting the potential for additional workarounds using sanctioned applications. Consider standards-based, seamless integration of these protections to streamline end user benefits without impacting the goals of your business partners.

› Embrace behavioral analytics. No longer the sole domain of credit card providers on the lookout for fraudulent charges, modern behavioral analytics capabilities can detect abnormal activity based not just on standards, but also according to the individual end user’s behaviors and habits. This emerging approach is particularly valuable given the ultra-accessible nature of SaaS, as protections “learn” the work habits of individuals and detect potential threats before they pounce.
Key Recommendations

Forrester’s in-depth survey of IT decision-makers with SaaS security responsibilities at enterprise organizations yielded several important guidelines to keep in mind as you consider your approach to protecting your digital assets:

› **Evaluate your protection gaps in the context of common fallacies, misconceptions, and false senses of security around cloud computing.** As-a-service delivery and consumption models are fundamentally different from those that have been used in the past. The whirlwind pace of SaaS adoption has made it easy to miss key facets of these models’ security capabilities and, just as importantly, liabilities for end users. Making the effort to comprehensively review your contracts and security capabilities will empower you to make well-informed decisions on how to protect yourself and save your firm major headaches down the road.

› **SaaS adoption is here to stay and needs to be managed.** The departmentalization and consumerization of IT is not a fad, and it’s now more crucial than ever for technology professionals to include lines of business and individual contributors in the decision-making process and enable them with the capabilities they need to stay competitive. Just as importantly, firms need clear, forward-thinking policies and technologies that are up to the task of addressing the new and evolving risks associated with sanctioned applications.

› **Seek SaaS-focused solutions.** Tried and true legacy perimeter and endpoint protections, having served their purpose in on-premises, controlled environments, are simply not designed with the threats and vulnerabilities of cloud environments in mind. Relying on these technologies alone in the context of new computing models is not only inadequate, but irresponsible. You must look beyond your current security portfolio for proper solutions designed to address the security gaps overlooked by many cloud consumers in their vendor contracts.
Appendix A: Methodology

In this study, Forrester conducted an online survey of 150 US-based organizations to evaluate attitudes and practices regarding SaaS security, along with steps being taken to confront related concerns while supporting the needs and desires of lines of business. Survey participants included decision-makers in IT and security management and leadership roles. Questions provided to the participants asked about their SaaS security practices and beliefs, their understanding of contractual agreements with SaaS vendors, attitudes toward shadow IT, and desired SaaS security capabilities. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in January 2014 and was completed in February 2014.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH


Appendix C: Demographics/Data

FIGURE 5
Company Size And Roles

“Using your best estimate, how many employees work for your firm/organization worldwide?”

- 20,000 or more employees (Global 2,000) 33%
- 1,000 to 4,999 employees (Large) 33%
- 5,000 to 19,999 employees (Very large) 33%

“Which title best describes your position at your organization?”

- Manager (manage a team of functional practitioners) 40%
- Vice president (in charge of one/several large departments) 13%
- Director (manage a team of managers and high-level contributors) 31%
- C-level executive (e.g., CIO) 15%

Base: 150 US IT decision-makers with responsibility for SaaS security
Source: A commissioned study conducted by Forrester Consulting on behalf of Adallom, February 2014
FIGURE 6
SaaS Application Deployment Footprints

“Which SaaS application(s) does your organization have deployed in the enterprise?”

<table>
<thead>
<tr>
<th>Application</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer relationship management (CRM)</td>
<td>63%</td>
</tr>
<tr>
<td>Enterprise resource planning (ERP)</td>
<td>53%</td>
</tr>
<tr>
<td>Productivity apps</td>
<td>48%</td>
</tr>
<tr>
<td>File sharing and content management</td>
<td>45%</td>
</tr>
<tr>
<td>ITSL/ITSM</td>
<td>20%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>

Base: 150 US IT decision-makers with responsibility for SaaS security
Source: A commissioned study conducted by Forrester Consulting on behalf of Adallom, February 2014

Appendix D: Endnotes
