SECURITY CONCERNS OVERCOME: CUSTOMERS MOVING TO SAAS

A Cloud Security Study

May 2016

INFO~TECH
RESEARCH GROUP

CONTENTS

3 **STAYING SECURE WITH SAAS**
Despite the wide prevalnce of point SaaS solutions, historically companies have been reluctant to move to the cloud due to security concerns.

5 **SAAS VENDORS TAKE SECURITY SERIOUSLY**
Info-Tech's current study shows a changing landscape in which internal IT organizations are recognizing that SaaS vendors' security is in fact better than their own.

10 **INSPIRING CONFIDENCE**
A defined process exists to assess the right SaaS fit within an organization and perform the requisite due diligence to migrate core enterprise applications to the cloud.

13 **PURCHASING SAAS**
Once a purchase decision has been made, the IT organization must prepare to ensure short- and long-term success.

17 **INSIGHT AND DUE DILIGENCE**
While SaaS vendors have recognized that security is paramount, and responded accordingly, organizations must still perform their own due diligence to ensure a good fit and validate claims.

STAYING SECURE WITH SAAS

The cloud has been the hottest topic in information technology for the better part of the last decade. Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and now a new wave of Anything-as-a-Service (XaaS) continue to drive adoption of what we collectively call cloud services. Adoption of these services has been growing exponentially in recent years, with a new study conducted by Info-Tech Research Group indicating that as many as 94% of organizations in the corporate sector report the use of at least one technology delivered via Software-as-a-Service (*Info-Tech Research Group SaaS Security Survey, 2016, n = 305*). Info-Tech sees this as a pivotal inflection point in overcoming what has been the greatest area of concern over implementing SaaS solutions: security.

The notion of giving up control of any production environment comes with potentially serious security implications. If a software environment creates, stores, or has access to any personally identifiable information, intellectual property, or other sensitive information, it can be perceived as a potential source of a crippling data leak. This fear has fostered persistent objections to the deployment of SaaS or other cloud solutions; however, new data is clearly demonstrating that it is time for those fears to be put to rest. The uncertainty has hinged on three key notions:

- IT can do a better job of protecting the system and data if it remains in full control.
- It's very difficult to properly vet a SaaS vendor's security controls and protocols.
- Multi-tenant environments provided by SaaS vendors can open up the organization's data to a wide variety of new attack vectors due to the proximity to data from other SaaS customers.

OVER

94%

of companies already leverage **Software-as-a-Service** somewhere in their organization.

For cloud evangelists, it is tempting to label these as nothing more than myths; however, it is important not to dismiss these concerns as baseless. There are some very real factors driving these concerns. But also, some very real data to satisfy even the staunchest objectors to the adoption of cloud services on the grounds of a perceived lack of appropriate security. Survey respondents cited Security, Performance, and Ease of Use as the top three drivers of SaaS adoption (*n=305)*. But the organization has to be able to trust in the vendor's security, and accept the reality that the security measures that these vendors take are often more robust than what the organization can deliver on its own.

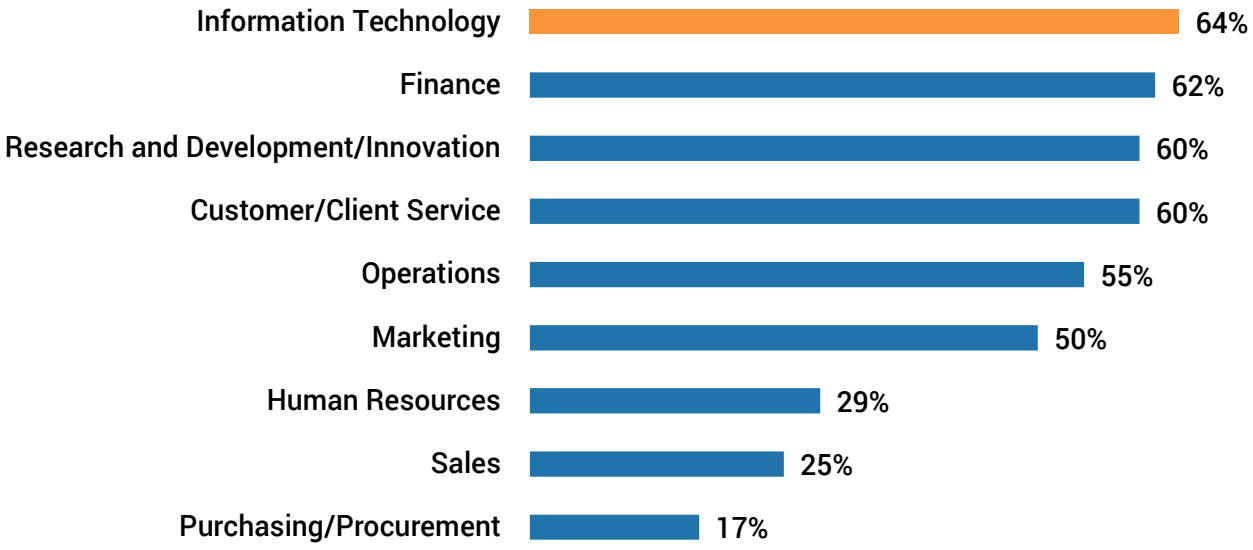
ON PREMISES	CLOUD
Security	Security
Ease of Use	Performance
Integration	Ease of Use

SAAS VENDORS TAKE SERCURITY SERIOUSLY

Security can be an expensive proposition, and protecting against every possible attack vector, both known and unknown (such as a zero-day vulnerability), requires a massive investment that many organizations simply cannot justify. SaaS providers, on the other hand, benefit from significant economies of scale through multi-tenancy models, allowing them to spread that investment over dozens, hundreds, or even thousands of different clients.

Their business is dependent on maintaining a strong reputation, especially as it relates to a strong security posture, making investment in security a top priority for the vast majority of providers. Recent data breaches of private companies have caused major problems for their brand integrity, but if those data leakages had impacted a major hosting provider, instead of retailers or entertainment companies, the damage could have been irreparable.

So where do concerns about SaaS vendor security come from? Oddly enough, it is not the security teams or even IT in general who doubt the capabilities of SaaS vendors. It is business users that are least confident in SaaS vendors' ability to keep their organization's data safe. Where 64% of IT respondents (*n=241*) rated their confidence in SaaS vendors to be high or very high, only 44% of respondents from all other departments (*n=64*) reported the same level of confidence.



Confidence in Saas security: Percentage of respondents rating SaaS security confidence high or very high

Could it be that IT's increased visibility into internal security controls makes them eager to off-load that component, knowing that they are unable to provide the same level of protection?

It turns out that this is, in fact, not the case. Participants who rate their confidence in cloud security as high or very high are actually 19% more likely to be confident in their own internal security, and deploy an average of 13% more security tools in their environments (n=141). This suggests that intimate knowledge of security internally does not result in a lack of confidence, but rather, demonstrates a deeper understanding of just how capable SaaS vendors are. In other words, those who truly understand security, know that they can trust SaaS vendors as much as, or even more, than they can trust their internal provisions.

When did people start trusting SaaS vendors this much?

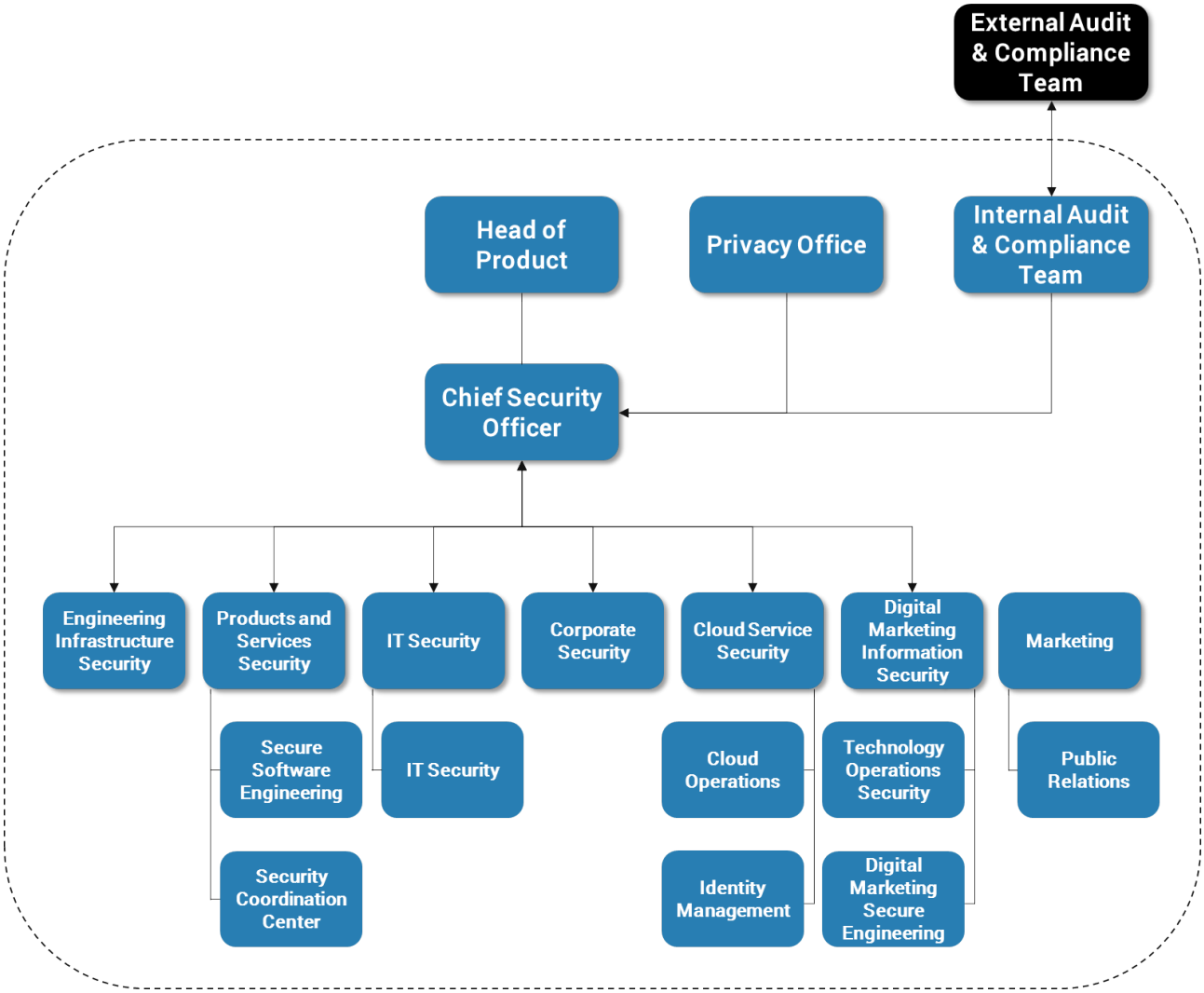
While not an overnight phenomenon, faith in SaaS provider security has accelerated in recent years to the point where it is no longer a barrier to adoption. According to 81% of respondents surveyed, that faith is actually now a driver. Cloud security has matured at a much faster rate than the security of internal IT teams. Based on the Spring 2014 Alert Logic Cloud Security Report, cloud vendors had a greater increase in self-initiated vulnerability scans of their networked assets than on-premises solutions from 2012 to 2013 ("Cloud Security Report–Spring 2014," Alert Logic, https://go.alertlogic.com/CSR2014P.html?PS=2nd%20Watch). The study also discovered that on-premises solutions were more exposed to certain types of attacks, such as malware and botnets, than their SaaS counterparts.

The second element that enables cloud security to be this effective is scale. The market for the cloud itself is expected to scale at a compound annual growth rate of 30% from 2013 to 2018 according to research from Goldman Sachs ("Roundup of Cloud Computing Forecasts and Market Estimates, 2015," Louis Columbus, Forbes, www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/#29080fa5740c). Enterprise IT spending was expected to grow at 5% CAGR over that same period. As cloud business continues to boom, SaaS providers will have the stable revenue and economies of scale to develop stronger, more consistent, and more comprehensive security features. With the push for IT to help drive business forward through technology innovation rather than commodity services, most IT departments will not have the budget, resources, or time to allocate to securing data as robustly as a SaaS vendor.

A view into a SaaS provider's security environment

For any established SaaS vendor, security provisions must be thorough and comprehensive to remain competitive in their line of business. Most of the prominent vendors have a large security team, with rigorous training, meticulously selected security products, and effective policies. A look at top cloud service providers in the world shows just how seriously they take the security of their offerings.

These vendors coordinate all security under their Chief Security Officer (CSO) or Chief Information Security Officer (CISO). That individual's office coordinates all product and services security initiatives. One of these vendors boasts over 500 experts in information, application, and network security.



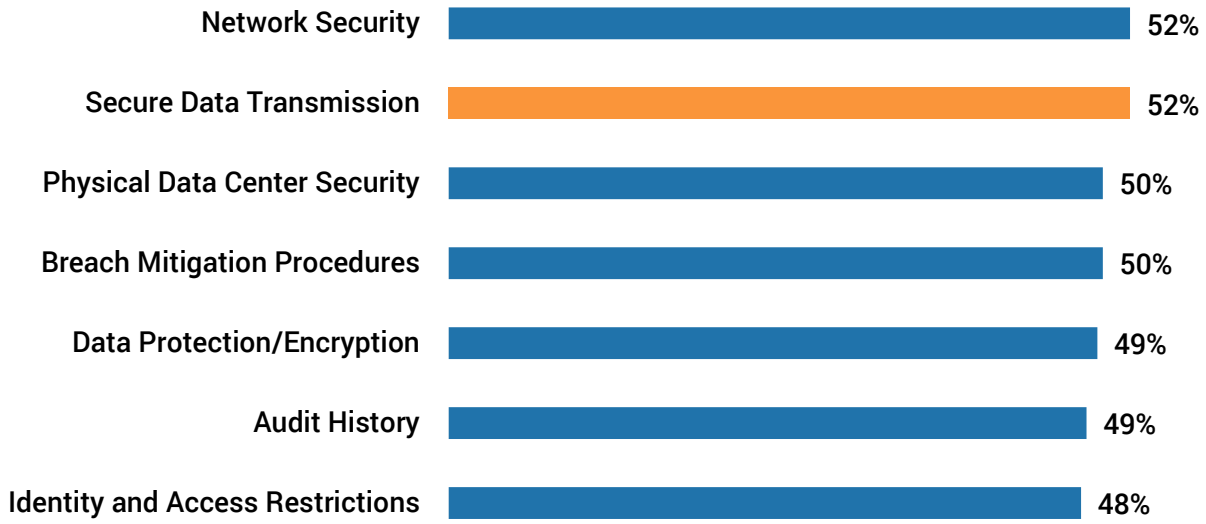
For these vendors, a secure product and services lifecycle consists of the following practices to help ensure that the applications they offer have implemented robust security measures, and that the data is protected when at rest:

- Provide security training and certification for product teams
- Perform product health, risk, and threat landscape analysis
- Conduct mandatory static analysis
- Develop secure coding guidelines, rules, and analysis
- Conduct secure complete stack
- Utilize big data for advanced threat detection
- Develop service roadmaps, security tools, and testing methods that guide the security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Provide secure architecture review encryption and penetration testing
- Conduct source code reviews
- Hold regular reviews for regulatory compliance

These vendors also protect customer data in transit through Secure Socket Layer (SSL) and Secure Shell (SSH) to manage the infrastructure connection. The larger vendors also offer degrees of managed services where they can take responsibility for the guest operating system, application software, and firewall for the infrastructure connection to help ensure secure end-to-end interfacing. This enables organizations to offload not just the data processing and storage, but even large portions of the transmission security to truly realize the benefits of a cloud solution.

These provisions do not go unnoticed among today's IT professionals who are well educated in security but also know their own limitations. When comparing their perception of internal security capabilities directly against those of SaaS vendors, IT respondents were 31% more likely to believe that SaaS vendors could do a better job of providing more secure data transmission, than their organization's own security provisions. This was second only to the belief in SaaS vendor breach mitigation procedures.

Reputable cloud vendors have all the tools in place to help secure data. They have the scale, the environment, the budget, and the people to stay on the bleeding edge of security. With regularity, they are launching new features that will further catapult them ahead of an internal IT team's security.



SaaS vendors are more capable: Percentage of IT respondents who perceive SaaS as more capable than internal IT

INSPIRING CONFIDENCE

It is clear that enterprise-class SaaS providers go to great lengths to provide the best security to their customers, but what about second- and third-tier providers? Chances are that most providers out there take security very seriously and will have the necessary provisions in place; however, it is important to thoroughly vet any vendor whose service may touch the organization's sensitive information. Especially in industries where it is a legal requirement to follow regulations such as PIPA, HIPAA, PCI, Sarbanes-Oxley and others, it is imperative to assess where any given SaaS vendor might have access to data that would fall under these regulations, and to ensure that adequate protections are in place. Failure to do so can result in significant financial penalties and irreparable damage to the company reputation and brand in the event of a data leak.

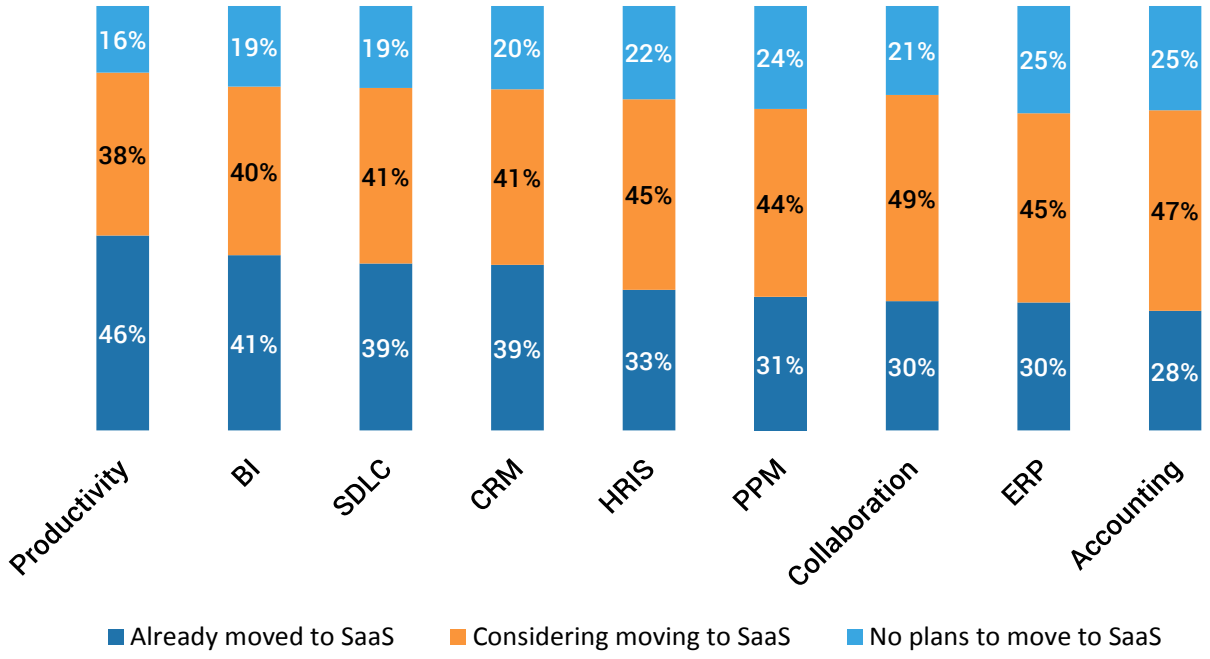
It's therefore prudent to take a process-driven approach in making the decision to move workloads into a SaaS environment. Info-Tech recommends the following three stage approach:

Determining the organizational risk profile

The data an organization can take to the cloud depends on business, compliance, and customer obligations. So, the regulatory environment, the data's importance and sensitivity, and the type of SaaS solution an organization intends to use all play a pivotal role in assessing its risk level. An organization must look at how the following elements will be impacted by SaaS adoption in order to define the risk:

- Business considerations
- Revenue
- Customer acquisition or engagement
- User satisfaction
- Time to market
- Cost of handling peak loads
- Regulatory compliance

Not surprisingly, respondents were least likely to consider SaaS for software that is more likely to contain sensitive financial data, such as accounting and ERP software. Interestingly, solutions that are more likely to create or house corporate IP such as productivity tools or business intelligence and analytics see the highest levels of adoption among participants. For them, financial data leaks are perceived as a greater risk than the potential for IP loss.



SaaS adoption by software type: Percentage of respondents who have moved named software type to SaaS

Requirements for access security control

In order to make an accurate decision on the suitability of moving workloads to SaaS, the organization must be honest with itself about internal capabilities. Though 67% of respondents rate their confidence in their internal security to be high or very high, Info-Tech identifies that there is an inflation of approximately six percentage points in the perception of internal security compared to the actual provisions taken. These organizations are in the most precarious situation of all, as in the realm of security, overconfidence can be a dangerous proposition. Knowing limitations, deficiencies, and gaps in security help ensure a realistic perspective of the overall security posture, but over-inflated confidence can create unnecessary areas of exposure.

While most organizations report having data protection and encryption, identity and access, and network security provisions, only about half have any

type of physical data center security, or conduct internal security audits, and even fewer—approximately one third—indicate that they have formal breach mitigation plans. A strong SaaS vendor, will have all of these technologies, will have certified their data center under ISO 27001, and will conduct regular penetration and vulnerability testing. Results are documented and, can be made available to security-conscious clients.

Evaluate vendors from a security perspective

Info-Tech Research Group recommends using the CAGI (Completeness/ Function, Auditability, Governability, and Interoperability) model for assessing a vendor's security prowess.

The organization must have a thorough understanding of the anatomy of a SaaS service agreement to evaluate a vendor for completeness. Within the customer agreement, data policies relating to data preservation, redundancy, location, verification of new data location, and seizure should be examined. An organization can be more certain that security is effective if the right data policies are in place.

The auditability of a vendor can be assessed by evaluating the vendor's abilities in self-auditing a breach, using their own tools or a third party incident response service. The audit data produced must enable forensic analysts to understand how any particular incident occurred, and what assets were compromised. The vendor should be able to provide high-level results of such an audit and describe implications to policies, procedures, and technologies that may require enhancements to avoid a similar incident from occurring.

Governability of a vendor can be assessed by checking to see how frequently and comprehensively a SaaS vendor monitors its environment. First and foremost, the vendor must monitor logs and performance. However, the provider should also monitor for malicious use, compromise, and policy violations. Depending on the organization's regulatory needs, the vendor may need to produce some or all of the following reports: a SOC 2 Type 2 report, ISO 27001 certification, CSA STAR certification, a PCI DSS assessment report, and a FedRAMP authorization.

Finally, an organization needs to think through how its data can be transferred safely to a new vendor or internally if the organization chooses to leave its SaaS provider. Interoperability is concerned with data, process integration, management capabilities, and business capabilities. If data cannot be transferred, an organization can find itself in a position where it needs to manually import data from its current vendor to the new vendor. This can cost the organization significant time and money.

PURCHASING SAAS

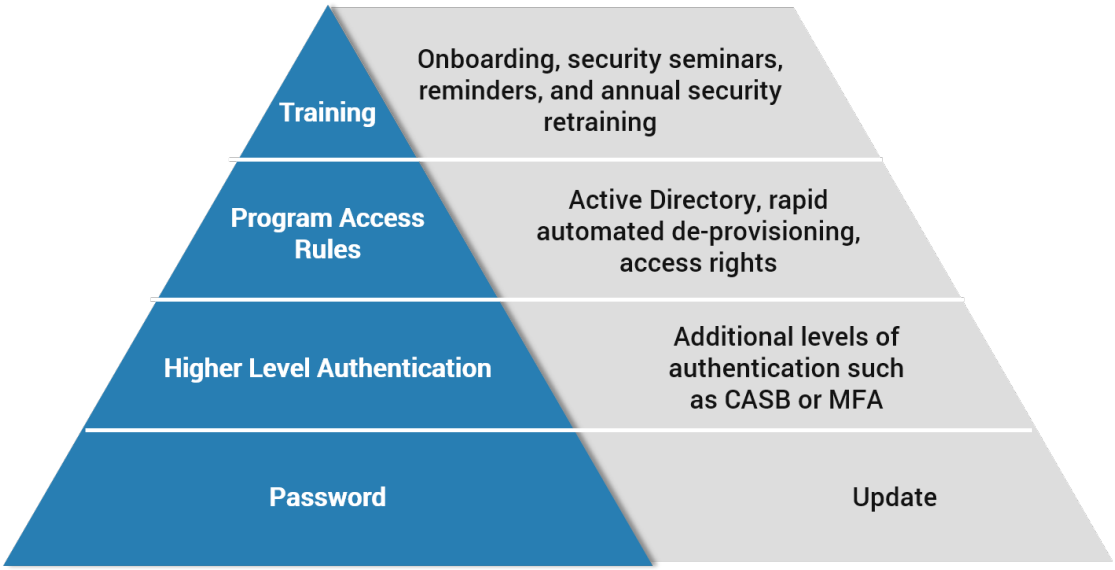
"Once an organization has procured a SaaS solution, it does not need to do anything more to secure its data, since it should leave all of that work to the vendor." This belief is surprisingly common; however, it cannot be further from the truth. There are indeed steps that an organization can and should take to further ensure that its data, clients, and business are protected.

An organization can add numerous processes that complement the cloud and make it more secure. Access, governance, and partner management are core areas that must be considered.

Assessing accessibility

Even if the appropriate security technologies are in place, many organizations fail to take critical steps to ensure that data cannot be leaked through other means. 60% of security incidents in 2014 were caused by employees according to the 2016 Data Breach Industry Forecast by Experian ("Cloud security: 10 things You Need To Know," Conner Forrest, Tech Republic, www.techrepublic.com/article/cloud-security-10-things-you-need-to-know). It's critical for a SaaS provider to consider the human element so that the actions of a malicious or careless employee don't put at risk the process and technology in place to protect the organization's data.

There are four elements that can help reduce the likelihood of an intrusion during access:



First and foremost, users should have a password with a minimum of twelve characters (upper and lowercase, special characters, and numbers). Additionally, the organization should have a policy wherein individuals must change their password regularly, at minimum every three months.

Second, the IT department should work to ensure that all departments utilize multifactor authentication. Authentication can be done through an RSA token, OTP over SMS or phone, smart card, PKI, and biometrics. Furthermore, firms can take advantage of risk-based authentication, for which the validation criteria depend on the type of transaction being performed within the application and the device identifier, geolocation, ISP, and heuristic information. These tools can be used as a second layer of authentication for when an individual accesses a VPN connection over an unsecure network.

Third, an organization must implement measures so that user access is restricted solely to the areas employees need for their role. These access rights must be easy to change. Additionally, should an employee leave the company, all access rights should be revoked automatically by cross-referencing against Active Directory.

Finally, where possible, employees should receive adequate training on proper security protocols. Because many breaches occur due to employee mistakes, it is vital that an organization educate its workforce. By taking these steps an organization can make it easier for an employee to remember what to do and increase the probability that its data will

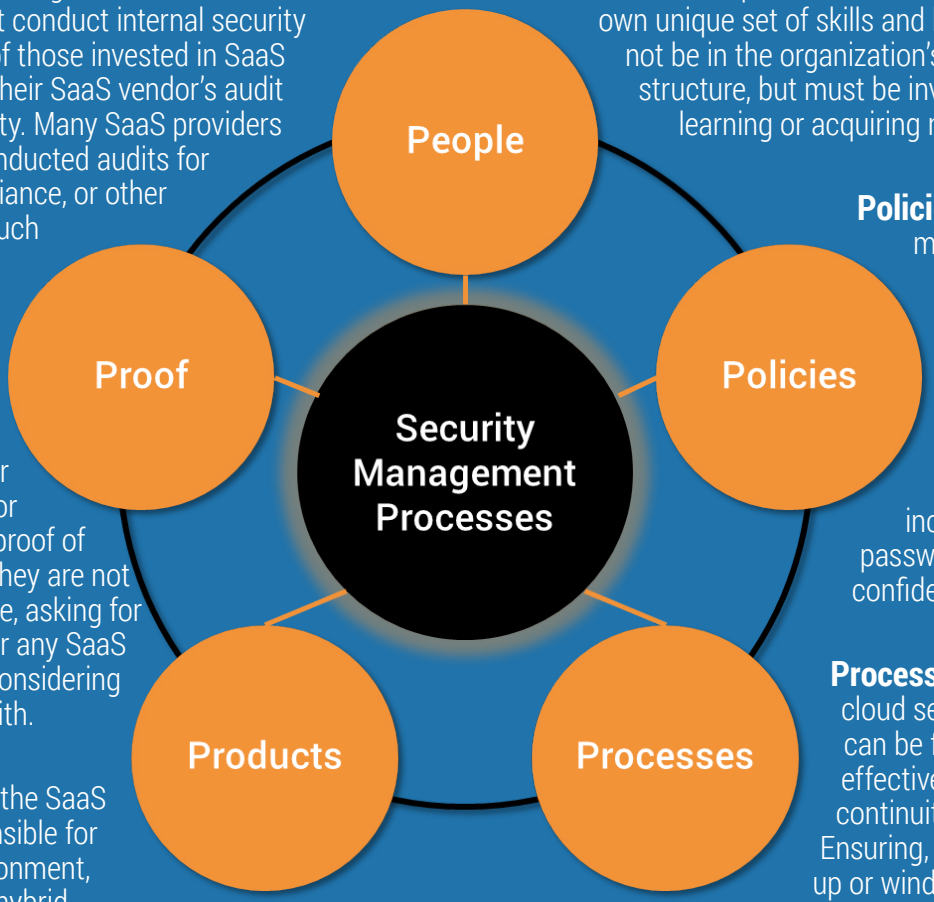
Assessing governance

Even the best laid plans can be laid to waste in an instant thanks to zero-day vulnerabilities and other attack vectors that are difficult, if not impossible, to prevent. Whether that vulnerability is exposed on the customer side or in the SaaS vendor's environment, establishing proper governance ahead of time will help to ensure that in the event of an incident, all parties act according to a defined plan, and surprises are kept to a minimum. Key elements of a proper SaaS vendor governance plan include immediate notification requirements, timelines for updates on the situation, and commitment to root cause analysis.

There are five fundamental areas that an organization will want to consider. These areas are people, policies, processes, products, and proof.

Proof: Security control effectiveness must be tracked to further hone cloud governance. 47% of all participants didn't conduct internal security audits, and 63% of those invested in SaaS did not consider their SaaS vendor's audit history as a priority. Many SaaS providers have regularly conducted audits for ISO, SOC 2 compliance, or other security testing such as penetration testing. Info-Tech recommends reviewing the vendor's publicly available information, either through the web or in brochures, for proof of these tests, or if they are not publically available, asking for copies of them for any SaaS vendor that it is considering doing business with.

People: Don't ask a mainframe programmer to manage SaaS relationships. Vendor management requires its own unique set of skills and knowledge that may not be in the organization's existing organizational structure, but must be invested in either through learning or acquiring new talent.



Policies: An organization must make sure it documents a set of security policies and procedures that must be followed depending on the situation that is present. These should include appropriate use, password construction, and confidentiality, to name a few.

Processes: Secure operation of cloud services and data transfer can be facilitated by deploying effective security and business continuity management models. Ensuring, for example, that wind up or wind down of any SaaS solutions is done according to a prescribed process will ensure that no important items are overlooked.

Products: While the SaaS provider is responsible for securing its environment, the trend toward hybrid environments where the customer may assume some of the data storage means that it too must deploy all the appropriate tools to help keep data secure.

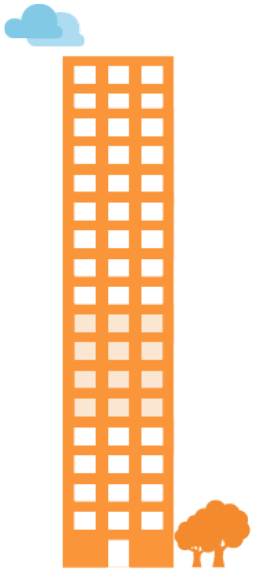
- System end-point security
- Next generation firewall
- Intrusion prevention
- Risk and compliance
- Security Information and Event Management (SIEM)
- Advanced malware
- Web and email security
- Data protection
- Mobile security
- Data center security
- Identity and access management

The importance of partner management

Adoption of SaaS technology shifts IT's delivery model from developing, maintaining, and supporting solutions, to managing contracts and relationships with vendors. It is imperative to maintain open lines of communication that promote transparency. Understanding the product update and release cycle, planned downtimes, and any changes in back-end frameworks or development languages ensures that there are no surprises that could potentially open up new vulnerabilities.

To manage the relationship effectively, organizations can take several steps. Exactly which of these steps need to be part of the relationship management process will depend on the scale and scope of what is being provided. For example, a purchase of only a few seats of a technology where no sensitive data or intellectual property will be housed might not warrant regularly scheduled updates and reviews. In every case; however, Info-Tech recommends starting with this list as a default, and working backward from there as the situation may require:

1. Define all the key points of contact at the vendor, from account management, technical support, and emergency to after-hours support.
2. Designate a person internally to manage, and be accountable for the relationship.
3. Set a clear escalation path commensurate with SLAs and other well-documented expectations.
4. Schedule regular updates with the vendor.



INSIGHT AND DUE DILIGENCE

There may never be a way to be 100% certain that every data asset trusted to the cloud is completely beyond compromise, but if followed properly, the tactics discussed in the previous sections may help the organization arrive at a more secure posture. Understanding the security capabilities of both of internal IT, as well as the SaaS vendors to whom your data will be trusted is an essential first step. Only then can the appropriate assessment, validation, and governance of the SaaS provider be established in order to keep data assets secure. Confidence in cloud security is not awarded blindly, but developed through a structured, rigorous approach to evaluating how, where, and by whom data will be secured.

INFO-TECH RESEARCH GROUP

Get the full report at:(TBD)
Statistics based on Info-Tech Cloud Security Survey, Jan 2016

Sponsored by Adobe