Shared responsibility is implied with software as a service (SaaS): vendors are responsible for ensuring services remain available and are not breached, while customers are responsible for safe use of those services. Current SaaS options are often insufficient on their own. Enhanced security visibility is needed by customers to uphold their responsibilities.

**ARE YOU SEEING GAPS?**

The sustained and massive growth of SaaS is unquestionably changing the IT industry. A significant change has been driven, and not only by managers in search of competitive service options. It also comes from users introducing personal services into the workplace. IT departments have no choice in this evolution. They must actively adapt by finding and applying controls for SaaS users in order to maintain or improve data protection. In other words, identifying responsibility for safety, as data passes into a SaaS provider’s environment, should be on the forefront of executive priorities.

Agility of the cloud service providers and their economies of scale, not to mention their ability to leverage broad-based experience and innovations, make it hard for any organization to resist the pull of SaaS. However, many factors are important beyond up-front-price considerations. Just as buying a pass for a month of train rides versus buying a car, the assessment of risk in SaaS is less about obvious cost calculations and more about finding and preparing for dangerous gaps.

Unfortunately, it is far too easy for customers to be unintentionally blind to serious factors. The SaaS model not only transforms service delivery, it also changes the equation for information security visibility, speed, and intelligence. How do decision makers clearly anticipate responsibility for environments they can’t oversee and receive no warnings from? And how do they measure and mind the most important gaps?

**WHO IS RESPONSIBLE?**

To put the technical issues simply, SaaS trust requires customer verification that controls are effective. In many cases, the SaaS provider does not encourage or provide the necessary verification. Does a service provider, for example, have the tools and incentives to distinguish a customer CEO user account from an imposter? When a breach of confidentiality happens, a SaaS provider may only say “we couldn’t tell it was not you.” Even if a SaaS provider could reliably see a difference between a real and false CEO, it may not be bound by any agreement to notify and give assistance.

There also is a maturity curve to security in service organizations. Which providers get more scrutiny and by whom? One might assume small SaaS startups are the weakest. Yet, if you follow the news, you will find even the largest providers are leaving customers scratching for hints of compromise. In 2010, Google had perhaps the most high-profile SaaS user safety case. A service reliability engineer with high-level access to children’s data was caught stalking by parents. Google did not detect the risk. Yet, after four serious cases were brought to its attention, Google fired the employee.
A SaaS provider may offer enhanced security capability for additional cost, but that does not resolve the need for a view across all providers. The importance of visibility expands quickly as SaaS grows in usership: how can companies centrally illuminate and manage all types of security gaps, across all relationships? Choosing one provider may lead to data being spread to multiple providers and outsourced access. Integration with a SaaS provider may also leave excess permissions or dormant accounts. In many cases, a contractor will be given full admin user access, then left open/shared even after work is complete. Should a SaaS provider be knowledgeable and responsible to alert the customer of admin account use after contractors no longer need access?

**AN EYE ON PROVIDERS**

The answer to these questions lies in our past. We can take lessons from risks we have faced before to prepare for those we face today. Without the right precautions, it turns out the cloud can actually increase business risk and be less secure than traditional IT. But with the right precautions, cloud can be more secure than ever.

Searching the web for controls in traditional IT brings up a standard set of suggestions. Compliance requirements have been documented for decades and, despite refresh and renewal, there exists a solid body of evidence for what constitutes due diligence. An audit trail, for example, is considered a requirement in IT because it is essential to understanding who did what, where and when.

Cloud providers have upturned this situation. Search the web for controls in cloud and the first ten results will be for wildly different topics. The reason for this discrepancy from traditional IT is not easy to explain here, but we can boil it down: a shift in control from devices and networks to just control of users.

Using our audit trail example from above, a SaaS provider takes over device and network responsibility, which leaves the customer to take increased responsibility over user monitoring. There are many clear cases where customers are not aware of this shift and also do not have the right people, tools, or procedures to maintain appropriate levels of data security in SaaS. Rather than replace or remove IT, SaaS can actually transform the role. There is emerging a new and expanded responsibility of enabling controls across all data services everywhere, including those external to the organization. But is there a better way to measure risk relative to each provider?

**SAAS-AWARE SOLUTIONS**

Once illuminated, the problem is simple and our goal is to find equally simple yet effective solutions. When a user logs in from China for the first time ever, how does a SaaS provider ensure the person using credentials is the right person? Perhaps geographic information makes that a loaded question. Knowing a user is in China gives away more information than knowing only they are a CEO. The likelihood of valid user location is a big step up in probability estimation. Reliance on a singular secret (e.g. password) creates a significant gap when using service providers because probabilities are changed from enterprise IT. Someone who simply steals a SaaS secret is indistinguishable from a true owner.

Simple and stronger solutions are available, fortunately so we do not have to rely upon secrets as the only form of authentication. Ask a HIPAA compliant service provider, for example, if they do not require more than a soft token for medical records in detecting the difference between a doctor and an identity thief. They should tell you multiple factors are available for authentication and active monitoring of success and failure. They should also offer real-time, detailed logs that are visible to the data owner. However, you are unlikely to get these answers.
If you do not have detailed logs, what happens when a doctor creates a sensitive file, such as “patientX-cancer_diagnosis.doc”? Would a SaaS provider be able to report in detail every person who performed a directory listing and saw just a filename?

We see an immediate need for SaaS customers to have more intelligent and faster visibility into all communication related to their own data. Collecting behavior data and looking for signs of aberration and exceptional risk greatly reduces the chance of fines and data loss. SaaS providers will usually offer only basic visibility of credentials being used (e.g. authentication success/fail), even when there is need for more.

Detection of fraud and abuse, as well as regulatory compliance, are clearly cases calling for a gap fix. Customers require visibility into behavior shifts and subtle changes of their own user accounts in order to prevent falling into a service gap. Back to our underground analogy, imagine a train that checks whether you have a valid ticket but has no way of alerting you as you plunge into a giant hole.

Data collection and monitoring has to be improved in order to see such gaps; we will improve the value of authentication by creating better records of actions. This is a real-world, pressing customer problem to solve. Already, we see attackers in the wild take SaaS credentials from a victim system and impersonate users in zero time on completely separate and disconnected systems.

We have left behind the standard perimeter defense-in-depth model and the tradeoff is holistic: giving up physical control, we have gained a robust-by-design application infrastructure that comes with a SLA. However, responsibility for security is now shared: users are accountable and liable for their activity. It is therefore imperative to ensure that users have purview into activity within SaaS applications and are able to react to compromised and unauthorized usage.

CONCLUSIONS

There is a shared responsibility implied in service provider management: The provider will protect your assets, and you will use the service safely. Migrating your data from on-premise applications into a SaaS relationship means taking responsibility for gaps along the way. Your SaaS provider is responsible for ensuring infrastructure remains available and is not breached, and you are responsible for services being used with authenticity.

Consider a decision to move money from your home safe to a bank vault to improve security. Your money might be in a more secure place because the bank invests in more controls than you would in your home. However, these controls are really just a different approach rather than a complete replacement for what you need. You do not surrender control. As the primary threat to your assets becomes someone stealing your credentials, defense requires a different set of tools and approaches than what you used before. Be prepared: mind the gap.