Moody's Analytics

Whitepaper

Author

Yann Delacourt
Director-Product Management, Enterprise Risk Solutions, Moody's Analytics

Contact Us

Americas
+1.212.553.1653

Europe
+44.20.7772.5454

Asia-Pacific
+852.3551.3077

Japan
+81.3.5408.4100

Best Practices for SaaS Security

Security concerns about Software as a Service (SaaS) in the banking and financial services sector have less to do with technology than with business culture, governance, and compliance

On-premise or cloud? And if cloud, what kind of cloud? An on-premise system is like being the owner-occupier of a house. You are uniquely in charge of security. But what quality of security technology can you actually afford? SaaS, by contrast, is like a multi-tenant system, where a landlord or facilities manager provides security with specialist assistance. That means you have outsourced responsibility for building access control to a manager with the latest, multi-level access technology, and the best security skills. At the same time, you control who can and cannot enter your own part of the building.

Which do you prefer?

After many years of skepticism and hesitation, banks are increasingly opting for the multi-tenant option. SaaS is now driving a disruption in the global financial services IT landscape. Banks were held back because of a misconception that the cloud, and in particular the public cloud, is insecure. That misconception has changed rapidly, but banks are still well advised to proceed with caution. Banks, which have a long standing culture of high security, want to be sure that the SaaS vendors and cloud infrastructure providers they work with are as committed to security as they are themselves.

Cost is a major driver of migration to the cloud. All banks interviewed in a recent survey by Moody's Analytics stated that they were migrating to the cloud to minimize IT costs, including the cost of data centers, hardware, staff, legacy systems, and expensive software licenses.

Yet, cost is far from being the only reason to migrate to cloud. Many banks want to achieve greater business agility through the flexibility and scalability that cloud deployments provide: the ability to upscale and downscale IT services as and when required. Others believe that cloud deployments allow them to develop products faster and meet customer demands in a more timely manner. Cloud is also seen as a lever for innovation, partnering with cloud vendors to co-develop products and services.

What is SaaS? And what is the cloud?

Definitions differ, but there are essentially three degrees of computing over the cloud: Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

IaaS vs PaaS vs SaaS: Where the value goes

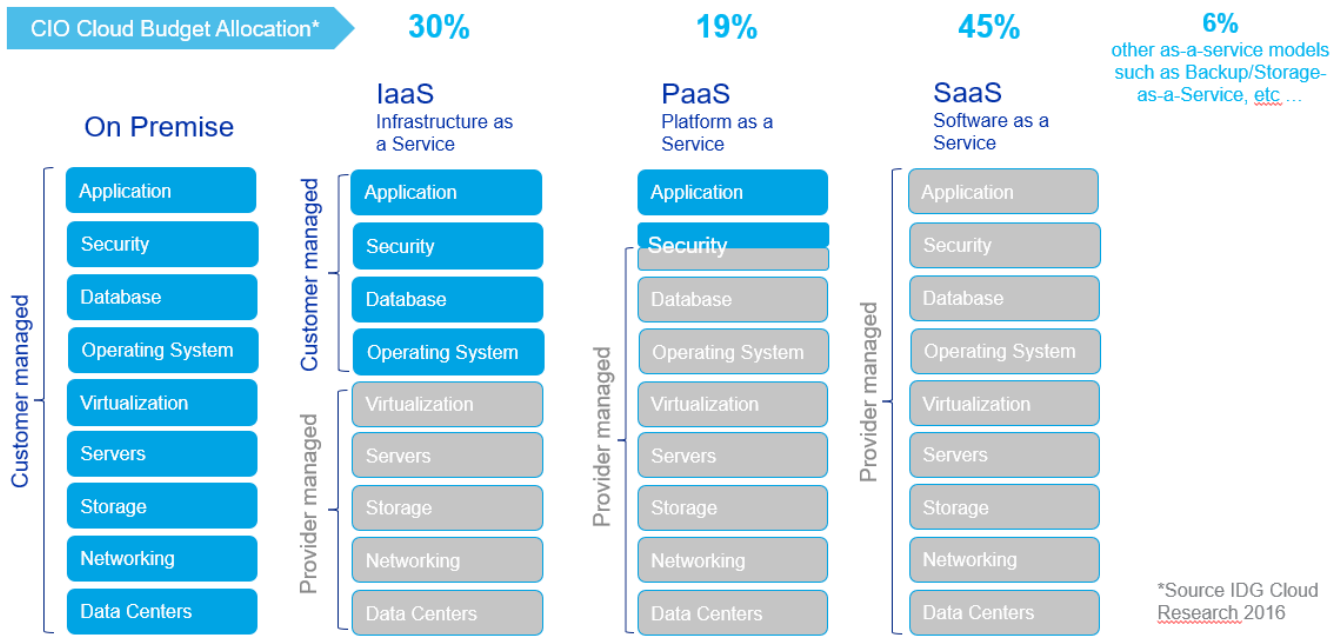

Figure 1: Software as a service provides the greatest value and ROI of cloud-based models, and therefore attracts the larger budgets.

IaaS means simply using a private cloud infrastructure. The applications, operating system and database remain the bank's responsibility, and the bank retains the security expertise almost entirely in-house. With PaaS, the service provider typically makes both the operating system and database available. The bank is responsible for applications alone, so the security burden is reduced in proportion. With SaaS, the vendor offers the entire IT stack including applications, and the bank is relieved of the burden of IT security in its entirety. The bank not only eliminates a good deal of operational risk but also benefits from shared costs and the technical skills that a specialist IT service vendor can provide.

It is hardly surprising then, that most banks (57% according to the recent Moody's Analytics survey) regard SaaS as the cloud model of choice because it delivers the greatest ROI. However, if an adequate SaaS offering for a particular class of application is difficult to find, many still opt for PaaS model.

Using SaaS services over the cloud means not having to maintain infrastructure or manage software upgrades. SaaS makes it easy for banks to remain current with regulatory updates to software and be at the forefront of technology due to more frequent product releases. Finally, banks are increasingly aware of the reduced operational risk that cloud deployments provide and the greater business continuity.

The regulators' view

One of the greatest fears within the banking community is the regulatory scrutiny if data becomes compromised in a security breach. In recent years, cloud providers have improved significantly, working with banks, regulators, and industry bodies such as the Cloud Security Alliance. Security has become less of an obstacle and indeed regulators now regard SaaS deployments as more secure than many banks' own data centers. In addition, Saas deployments deliver other benefits such as reduced operational risk, business continuity and auditability. Financial regulators are increasingly using cloud technology themselves.

The outsourcing of business-critical functions by banks is itself now subject, in many jurisdictions, to specific regulation. Banks that do outsource business-critical functions by placing them into a public cloud still look to retain the ability to assess, supervise, and enforce provider performance. They manage risks contractually, and maintain the security of, and access to their data. This approach has become all the more important with the implementation of more extensive data protection laws across the globe.

To remove any possible future uncertainties, banks must define a due-diligence framework and service delivery guidance covering the following five areas:

- Access and audit rights that ensure SaaS implementations meet the same standards that are currently expected of on-premise systems.
- Location of data and data processing that ensures data is not moved from one region to another, contrary to some demands.
- Mitigation of risks associated with the outsourcing stack – for example the risks associated with a non-mature vendor going out of business, or changing business focus.
- Contingency plans that provide, for example, strategies to move to another vendor or to reinternalize applications.
- Regulators' assessment and security audit of the cloud service providers

Regulators are currently considering the development of a legal framework to assess the security measures and processes of cloud providers such as Amazon and Microsoft. The IT security technology to achieve such a framework is in place, the main issue is transparency into that security. To satisfy regulators, customers, and the general public, banks must be in a position to know precisely what security measures are being used and how safe they are. Transparency requires a track record of protecting sensitive data, based on a close partnership between the SaaS service provider, responsible for security in the cloud, and the provider of cloud infrastructure responsible for security of the cloud.

The Seven Pillars of SaaS Security Wisdom

There are critical security issues and best practices that banking executives must consider when transferring regulatory compliance systems and processes to SaaS deployments, or deciding between SaaS providers. The checklist for evaluating SaaS vendors should include both the bank's existing requirements based on company-wide practices, and SaaS-specific security requirements as well.

There are seven pillars to SaaS-specific security and it is important that each vendor is scrutinized in detail on both their own security and that of their cloud infrastructure partner. In this section, we describe good security practices.

1. **Access Management:** Who can access your cloud deployment and what permissions do they have? The vendor must provide a unified framework to manage user authentication through business rules that determine appropriate user access based on organizational role, the system accessed, the data requirements, and workflow assignments, independently of the device used.
2. **Network Control:** Security groups control who can access specific instances across the network. For more granular control, this can also include jump servers and network access control lists (NACL). An optional layer of security for a virtual private cloud, acting as a firewall for controlling traffic in and out of one or more subnets.
3. **Perimeter Network Control:** Perimeter defense has traditionally been about controlling traffic flowing into and out of a data center network. The primary technology that underpins perimeter protection is a firewall, which filters out potentially dangerous or unknown traffic that might constitute a threat based on a set of rules about the types of traffic and permitted source/destination addresses on the network. Most organizations also deploy further levels of perimeter protection such as intrusion detection and prevention systems (IDS/IPS), which look for suspicious traffic after it has passed through the firewall.
4. **VM Management:** Ensuring your infrastructure is secure requires frequent updates directly to your virtual machine. Staying up-to-date requires a significant investment in ways to identify the latest threats and patches available in the market. A SaaS provider continuously performs these tasks on standardized VM images and third-parties used in its software. Therefore, the time between a breach and the resulting patch is reduced.

5. **Data Protection:** The most important practice of all is the SaaS provider's methodology for preventing a data breach, primarily by using various methods for data encryption both at rest and in transit. Best practice solutions offer customers the option to control their encryption keys so that cloud operations staff cannot decrypt customer data. They also deploy encryption technology for data at rest, which provides options for building a hierarchy of client-side and server-side encryption for a high level of security, with separation of duty at the various levels of the hierarchy, customer control, and full audit trails. All this becomes more important with the stringent safeguards required for personally identifiable information (PII).
6. **Governance and Incident Management:** Certain types of incidents must be captured, reported, and tracked to closure, and there must be procedures in place for investigating any potential security breaches.
7. **Scalability & Reliability:** One of the biggest features of the cloud is the ability to increase capacity of existing hardware or software by adding resources as and when needed. Vertical scaling is limited by only being able to get as large as the size of the server. Horizontal scaling means the ability to connect multiple hardware or software entities, such as servers, so that they work as a single logical unit. This kind of scale, however, cannot be implemented at a moment's notice, so a cloud computing vendor must build a considerable amount of horizontal redundancy into the infrastructure to ensure continuity of service. A content delivery network or content distribution network (CDN) provides further robustness through a geographically distributed network of proxy servers and their data centers. Finally, there must be a disaster recovery (DR) plan in place for replicating data and services in the event of a natural or human-induced regional disaster.

Isolation and Separation across Cloud Operation Activities

The other important consideration is how well the SaaS vendor and its cloud services partner isolate the operations of their various customers. To return to our shared tenancy analogy: the facilities manager gives the tenants access to the building (or specific parts thereof). But each tenant has their own apartment or separate office space. In the context of cloud-based IT, this is best achieved through virtual private clouds (VPC). These enable you to launch resources into a virtual network that you have defined, and which closely resembles a traditional network that you would operate in your own data center. Each SaaS service is made available in its own VPC, maximizing isolation.

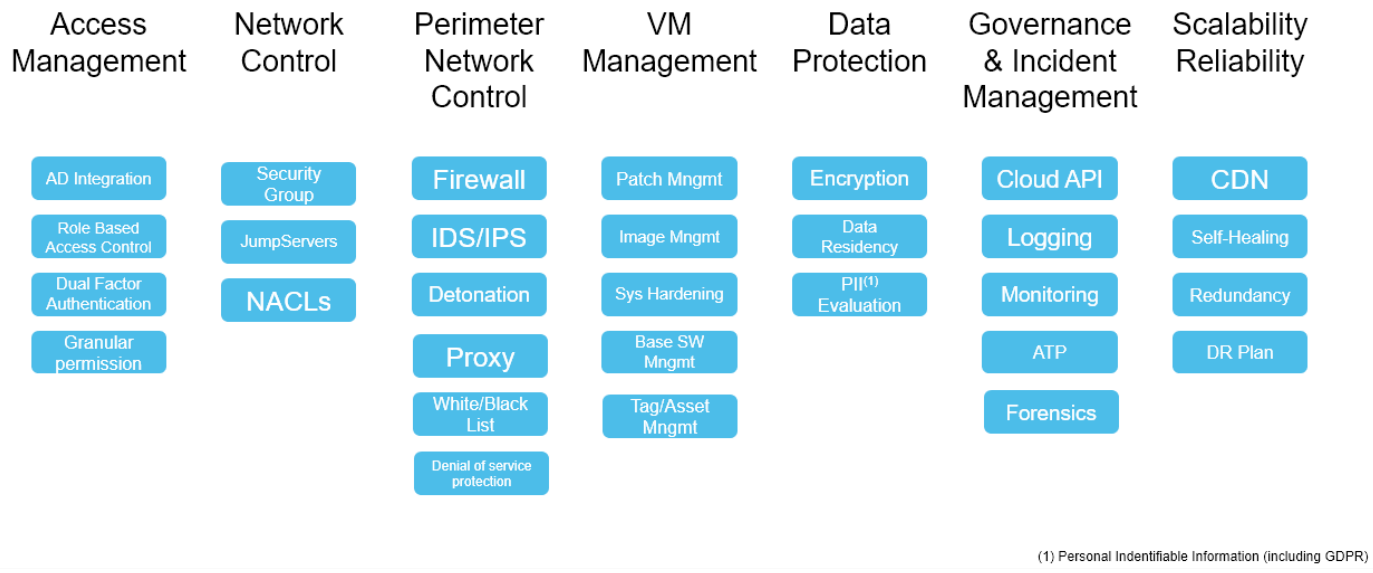

Figure 2: The Seven Pillars of SaaS security

Security is further enhanced by introducing the separation of duty within the SaaS vendor's operational teams – the practice aimed at preventing one team from having too much control.

- Separate accounts in charge of operating the infrastructure, with responsibility for reliability, availability, scalability, and hardening.
- Separate accounts in charge of securing access to each perimeter in production, with responsibility for secured access, network isolation, and access control.
- Separate accounts in charge of continuously evaluating the security of production independently of other accounts, with responsibility for identifying security breaches if any, identifying unexpected access and governing overall practices.

Certifications

Finally, when choosing a cloud services provider, it always pays to ask about certification and see the documentation. Key general compliance certificates include SOC 1 and SOC 2, ISO 27001 but there are many relevant certificates in different branches of financial services. For example, AWS, has some 3,500 separate controls, and keeps track of these controls with a Master Controls Set mapped to the various external compliance standards for regular audits. Many of these, together with guidance on how to achieve compliance in various jurisdictions, are publicly available on the AWS Artifact service.

Conclusion

SaaS technology holds the promise of lower cost and more agile performance in a host of critical financial and regulatory areas in the banking sector. These applications usually involve managing sensitive information on customers, regulatory compliance, and other areas of the business. With the right technology and best practices, SaaS can be far more secure than on-premise applications and the bank has many options for retaining control over the security infrastructure, such as the encryption of customer data.

CONTACT DETAILS

Visit us at **moodysanalytics.com** or contact us at a location below.

AMERICAS
+1.212.553.1653
clientservices@moodys.com

EMEA
+44.20.7772.5454
clientservices.emea@moodys.com

ASIA (EXCLUDING JAPAN)
+852.3551.3077
clientservices.asia@moodys.com

JAPAN
+81.3.5408.4100
clientservices.japan@moodys.com

BP54140