

SaaS Adoption Breeds Compliance Challenges

By Darren Platt

The increasing use of Software as a Service (SaaS) is quietly imposing a seismic change on how organizations will control and audit access to sensitive information that resides in the Internet “cloud.” This change is bringing major new risks and security challenges.

While it takes an act of Congress to change compliance regulations, the increasing use of Software as a Service (SaaS) is quietly imposing a seismic change on how organizations will control and audit access to sensitive information that resides in the Internet “cloud.” This change is bringing major new risks and security challenges.

SaaS was just emerging when the Sarbanes-Oxley Act (SOX) was enacted in 2002, and in 2003 when the Privacy Rule and Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) became effective. Meanwhile, SaaS was barely on the radar in 1999 when the Gramm-Leach-Bliley Act (GLBA) was passed into law.

Today SaaS usage has become mainstream among companies of all sizes. By 2010, 65% of U.S. companies with more than \$100 million in yearly revenue are forecasted to be using SaaS.¹ Today, half of all large enterprises have two or more SaaS applications in use.²

SaaS is not immune to compliance

The SaaS revolution has made cloud-based applications mission-critical for customer relationship management (CRM), enterprise resource planning (ERP), and human resources (HR). Mission-critical SaaS is typically delivered with a multi-tenant architecture and over the Internet where it is vulnerable to a host of threats.

- SaaS CRM applications contain key contact information for customers as well as order histories, credit,

billing, and banking details, all related to core financials and governed by SOX.

- SaaS ERP and sales force automation (SFA) applications house critical internal operational and financial data as well as sensitive information about suppliers and distributors. All of this information includes financial details that flow through the SOX-covered general ledger.
- SaaS HR applications contain confidential privacy data about employees such as compensation, banking accounts, and health care records. Most employees have information in HR systems governed by HIPAA for health care and GLBA for consumer financial information about banking, credit, 401K, and insurance relationships. SOX can also govern executive compensation information in HR systems that span salaries, bonuses, and stock options.

Other popular SaaS applications house different types of sensitive information whose confidentiality and integrity must be protected. Content management and business process outsourcing systems often include intellectual property critical to current and future revenues, confidential government regulatory filings, legal actions, and operational documentation for company processes and procedures. Collaboration applications may include confidential company information about strategic products or services, marketing or sales plans, and competitive positioning.

Sensitive information is leaving the building

Companies today operate a mix of internally deployed and externally hosted IT resources and applications. While SaaS usage is rising dramatically, on-premise enterprise software applications, many of which have a long operational history

1 M. West, B. Guptil, et al, “Enterprise Ready or Not: SaaS Becomes Mainstream, 2008,” *Saugatuck Technologies*, http://www.siia.net/ondemand/2008/simplified_compliance_for_saas_and_cloud.pdf.

2 L. Herbert, B. Martorelli, “SaaS Clients Face Growing Complexity, 2008,” *Forrester Research*, <http://www.forrester.com/Research/Document/Excerpt/0,7211,45700,00.html>.

The burden of regulatory compliance remains on the owner of the data.

and have been invested in heavily, will continue to play a central role indefinitely.

That being the case, companies of all sizes must manage, secure, and audit access to their sensitive information – whether it resides inside or outside their firewall – in order to comply with regulatory mandates. This demands new skills, capabilities and architectures.

While applications provided by SaaS vendors may handle the processing of medical claims, credit card transactions, employee information, and other sensitive information on their servers, the burden of regulatory compliance remains on the owner of that data. That owner is the organization that gathered the data in the first place and is now using a third-party SaaS application (the custodian).

To date, regulatory mandates do not make exceptions or allow provisions for non-compliance caused by the operators of SaaS and Internet-based applications. Data owners are required to maintain the prescribed standards for confidentiality, control, and security over sensitive and confidential information, regardless of whether the IT infrastructure is operated by the data owner or a third-party application provider.

Access control and audit

Most SaaS and outsourced application providers offer baseline security mechanisms that include perimeter firewalls, intrusion detection and prevention, anti-malware, and physical security to protect their customer's information. However, most regulatory mandates require regular monitoring of all authentication, access, and activity on systems that contain sensitive information, regardless of location.

For organizations that need to manage compliance requirements across a wide mix of SaaS providers, complexity escalates proportionally with each new Internet application used. One of the primary reasons for this is that each SaaS provider uses its own identity management system and has limited ability to customize and tailor its controls for individual companies using their service. According to Forrester Research, among the biggest obstacles cited by companies deciding against SaaS usage are integration with existing enterprise infrastructure and security.³

For example, strong or two-factor authentication, which is a requirement for some applications and data, may not be available for SaaS applications. In addition, active real-time 24x7 monitoring of access and authorization for sensitive information inside a SaaS app is difficult or impossible. That's because SaaS application providers do not provide their cus-

tomers with an audit trail of activity by their end-users, and in some cases the SaaS provider does not even log activity. In the event that the SaaS provider is auditing all user activity, the only time a customer is given access to logs is when the Service Level Agreement (SLA) is violated.

Meanwhile, SaaS identity controls can be difficult to integrate with those already deployed inside an organization's network. Conversely, authentication and access controls inside a company's firewall are difficult to extend outside to the SaaS domain.

The result of maintaining and managing two or more heterogeneous identity infrastructures (one inside the firewall and one or more outside the organization) weakens security and increases risk. Standalone identity silos with non-integrated controls, uncorrelated log data, inconsistent policies, duplication, and redundancy increase the probability of a breach.

Technology alone is not the answer

Privacy and security regulations require owners of protected information to manage and secure access to data across geographically dispersed communities, processes, and technologies. This increases costs and lengthens time frames for implementing access controls and deploying SaaS applications.

Initial attempts at solving the enterprise identity compliance problem have applied a technology fix: buy software. Technology alone is a high-risk approach for authentication, access, and authorization, since these involve people and processes not just technology.

Consider identity federation. It has been deployed, using the Security Assertion Markup Language (SAML) standard, to address identity integration across multiple Internet domains using single sign-on (SSO) functionality. However, neither federation nor SSO meets compliance requirements. While SSO delivers process benefits by easing user access to multiple applications with one authentication, by itself it does not strengthen authentication and access control.

Efficiently managing authentication, access control, and authorization processes is beyond the scope of federation software, which requires lengthy custom integration to deliver coarse-grained, inflexible "one size fits all" SSO. As a result, federation creates legal and liability issues that must be contractually addressed between organizations to specify access and authorization limitations.

Similarly, two-factor authentication technologies often are deployed to meet requirements for strong authentication, such as the guidance issued by the Federal Financial Institutions Examination Council (FFIEC) for consumer online banking.⁴ It requires careful planning to meet compliance requirements, including a process for managing the authentication technology across its life cycle.

Frequently, mapping compliance requirements to security controls will channel multi-factor authentication invest-

3 Ibid.

4 http://www.ffiec.gov/pdf/authentication_guidance.pdf.

ments to less-costly approaches that are friendlier to people and processes. This has been the case with the FFIEC guidance for Internet banking which has seen a broad adoption of multiple password mechanisms, with each password originating from a different source. More expensive hardware-based “what you have” or “what you are” authentication methods often exceed compliance requirements. In these situations, resources are better spent in addressing compliance requirements for access (where you can go) and authorization (what you can do).

Moving security to the cloud

So what’s the answer? One possible solution is to move security into the cloud. Viewing compliance events such as authentication, access control, and authorization from within the network cloud provides a unique and privileged top-down perspective. Using this approach, all events enforced from within the cloud are centrally monitored and logged, regardless of location. This delivers enormous benefits for enforcing one set of compliance policies across the enterprise and multiple SaaS providers.

Cloud-based access management enforcement and auditing also eliminates the need to normalize incompatible data generated by heterogeneous identity systems used by individual SaaS providers. With one world view, IT departments can avoid orphaned accounts and other security blind spots associated with trying to keep tabs on users who are members of multiple SaaS access management systems. A centralized, cloud-based identity management system unifies many monitoring and logging functions, recording from the cloud the actions of internal and external users accessing applications anywhere. This nails compliance regulations on policy enforcement and audit trails.

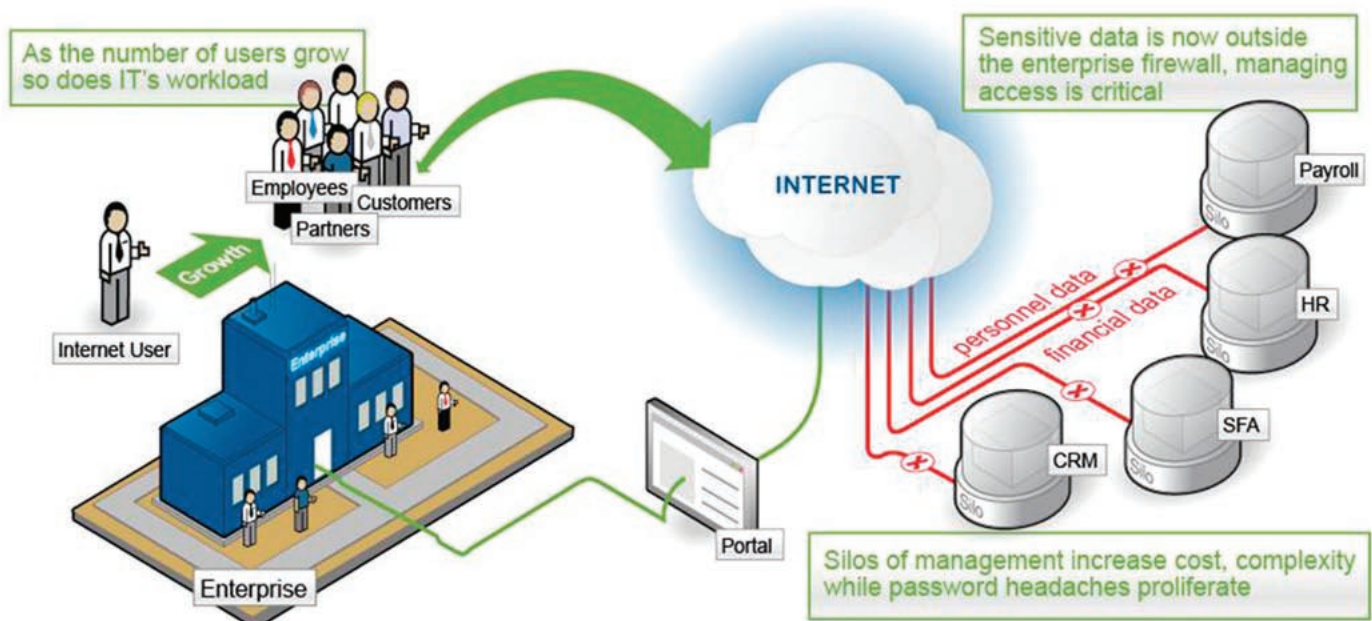
An additional benefit of centralizing access management and compliance in the cloud is the ability to apply the flexibility

and cost-saving benefits of virtualization to identity management challenges. For example, the complexity of integrating scattered user identity repositories to protect applications is a huge expense. This is a natural target for virtualization, which can be used to simplify the layers of physical and logical complexity created by these data stores. Meanwhile, virtual applications can automate the management of the logical links inside cloud-based virtual identity systems to improve security and streamline policy enforcement for regulatory compliance.

Deployment models

Getting security into the cloud is all about integration. The most practical approach is to extend enterprise investments in systems like Active Directory, LDAP and other identity and access management (IAM) infrastructures to work with applications that reside in the cloud like Salesforce.com, Workday, ADP, and others. By bridging security that is already in place within the firewall, it is possible to extend security to the cloud. This can be accomplished by deploying an appliance or Web service within the enterprise network and using an enterprise portal as a SSO gateway to the cloud applications. This enforces access policies, while auditing all activity as it moves through the gateway.

The second approach for moving security into the cloud is to provide IAM for applications that are built on cloud platforms like Amazon’s EC2. In this case, the application stack is running on a third-party platform accessible over the Internet. This architecture requires a stand-alone security system to provide access control, authentication, SSO, audit, and user management. Here an identity cloud can be implemented to act as a proxy that users pass through before they access the cloud application. By using a network-delivered architecture, similar to Postini’s secure messaging proxy, it is possible to get all the core security needed *for the cloud from the cloud*.



The role of standards

Standards are key to scaling anything on the Internet. To date the security standards that have been most successful in the enterprise and between enterprises are SAML, HTTP/S, and LDAP. SAML is the core federation standard for achieving SSO and trust between organizations. The more SAML is used the easier it becomes for both enterprises and SaaS providers to be connected for SSO.

However, most applications on the Internet today have not yet deployed SAML, primarily due to lack of budget or expertise. It is far more common to find applications that use logon forms within the web page itself. When users authenticate to these websites they are using HTTP running over SSL or HTTP/S. Leveraging the ubiquity of HTTP/S is the fastest way to get SSO and integration without changing the application itself.

As standards like OpenID become more widely deployed, they will facilitate access management interoperability between cloud applications, but currently they lack the trust needed for commercial use.

LDAP is the core standard for querying user information such as authentication, attributes, and roles. For example, Active Directory, the most widely deployed user store technology, supports LDAP, as do most other enterprise directories. The most efficient mechanism for cloud applications to securely access LDAP directories within the enterprise perimeter is through Web services. Another approach is to maintain a hosted LDAP directory in the cloud using a secure data center. This approach has the advantage of serving as a hub to which many applications can connect without imposing the management overhead of backup, restore, monitoring, etc.

Elements of cloud-based security

The following features are characteristic of a new model for handling access management from the cloud and meeting regulatory compliance for SaaS.

Virtualized identities

Setting up virtualized identities requires the ability to automate the discovery of who users are and what access attributes are associated with each user for each of the applications, either behind the firewall or SaaS-based. Ideally, the automated tool would point to the IP address of a server hosting a repository of user attributes. The user attributes represent a group needing an authentication and access policy for a protected application. The schema discovery and collection tool would communicate securely over an encrypted VPN tunnel or SSL session.

Once selected, the attributes are automatically mapped logically to the compliance policy, governing access for the group contained in the schema. The repository is queried each time a user invokes the authentication or access policy to check the status of the user, and the logical link remains effective until the policy is deleted or retired. Unifying and logically map-

ping user attributes from distributed repositories saves hundreds of man-hours needed to manually locate, normalize, and integrate user information to deploy a more traditional identity software approach. Virtualized identities respond to the flex and flow of business and its ever-changing sets of application end-users.

Visual policy development and mapping

Visual tools enhance clarity and understanding while simplifying and speeding up the task of creating and managing role-based compliance policies across their life cycle. Developing and deploying authentication and access policies to support compliance can be a series of time-consuming tasks – locating user attributes, writing policy statements, and deploying into policy enforcement points. Visual tools for complex tasks result in stronger security compared to a patchwork of logs, spreadsheets, and scattered audit data.

Unified logging and reporting

Managing identity in the cloud enables the establishment of a centralized, normalized, comprehensive audit system that can process volumes of authentication and access event logs from the top-down vantage point. This creates a single audit log store for multiple physical and logical locations and networks, user repositories, and protected applications. Distributed user repositories, protected applications, and policy enforcement points generate incompatible logs that can take many hours to acquire and normalize. A cloud-based access management system puts all of this critical audit functionality in one consistent file type, secured in a central location. This makes all authentication and access audit information easy to access, which results in stronger security and less costly compliance.

Conclusion

Ultimately, moving access management to a cloud-based model reduces the cost and complexities associated with using multiple SaaS applications by centralizing authentication, access control, and authorization, as well as audit logs, at one control point. This approach to access management has the singular ability to cross over from the SaaS side into the enterprise applications behind the firewall, integrating all access management into a centralized and automated command and control center.

About the Author

Darren Platt is CTO of Symplified, a provider of on-demand identity services. He co-authored the AuthXML specification, which served as a foundation for the SAML identity federation standard. He may be reached at darren@symplified.com.

