



A **Symplified** Best Practices Guide

Compliance for SaaS and Cloud Applications

Symplified
The Cloud Security Experts

Compliance Regulations Govern Sensitive Information in SaaS and Cloud Applications

» **Enterprise Growth Marks SaaS Maturity:** Mid-market companies were early SaaS adopters and have been using SaaS and cloud applications on a large scale for more than five years to deliver enterprise CRM, ERP and HR functionality. Today SaaS is mainstream as larger enterprises have adopted SaaS and a more sophisticated business-in-the-cloud model. By 2010, 65% of U.S. companies with more than \$100 million in yearly revenue are forecasted to be using SaaS¹. Today, half of all large enterprises have two or more SaaS applications in use.²

» **SaaS Applications Contain Sensitive Information:** The SaaS revolution has made cloud-based applications mission-critical, with a variety of confidential financial, operational and customer information governed by compliance regulations.

SaaS CRM apps 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 for its sensitivity to general ledger payable and receivable accounts.

SaaS ERP and SFA apps contain key 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 general ledger, which is a central part of core financials and governed by SOX.

SaaS HR apps contain many confidential details about employees, such as compensation, banking accounts and healthcare records. Most employees have information in HR systems governed by HIPAA for healthcare and GLBA for consumer financial information about banking, credit, 401K and insurance relationships. SOX can cover sensitive compensation information inside HR systems regarding executive salaries, bonuses and stock options.

Other popular SaaS apps also contain sensitive proprietary information whose confidentiality and integrity must be protected. Content management and business process outsourcing systems may 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 product or services, marketing or sales plans, and competitive positioning.

» **Compliance and Security For Internal and External Applications:** Companies today routinely operate with a mixture of internal and external IT resources and applications. They use enterprise software applications to manage specific parts of their business or strategic pieces of their IT architecture, usually those with a long operational history and large investment. Enterprise software apps inside the trusted network frequently are augmented, complemented or replaced by SaaS or outsourced apps on the Internet.

All companies, regardless of size, must manage and secure sensitive information they own on both sides of their firewall to comply with privacy regulations. Properly securing internal and external sensitive information to meet compliance requirements demands new types of skills, capabilities and architectures to effectively control without costly duplication and redundancies.

¹ Saugatuck Technologies, Enterprise Ready or Not: SaaS Becomes Mainstream, 2008, Michael West, Bruce Guptil, et al

² Forrester Research, SaaS Clients Face Growing Complexity, 2008, Liz Herbert & Bill Martorelli



» **Data Custodial Relationships on the Internet:** Privacy regulations recognize company ownership of the information they use to manage their operations and employees. As owners of information, they are required to protect the confidentiality and integrity of their information defined as sensitive, such as any personally identifiable information, healthcare information, consumer or customer financial information, and all data relevant to financial reporting. Companies in specific vertical industries, such as pharmaceuticals and communications, have specific requirements for protecting operational data.

SaaS vendors offer various types of automated business processes and services for information owned by another company – their customers. SaaS vendors' process medical claims and credit card transactions, manage employee information, benefits and retirement plans, acquire and dispose of assets, and manage core financial information.

Privacy regulations describe a data custodian relationship for SaaS and other vendors processing sensitive information for the owner of the data. Data custodians require access to sensitive information owned by a customer to perform their services. They are required to exercise due care in protecting the sensitive information for their customers, the owners of the data. Data custodian relationships, the due care to protect sensitive information, and the due diligence required by the data owner to verify proper procedures and controls, are described in privacy regulations and frequently covered in service agreements between the parties.

Meeting the compliance requirements of data owners and custodians has been the primary driver of double-digit growth in the identity management marketplace.³ Symplified's cloud-based On Demand Identity service offers a unique, top-down perspective with new efficiencies for enforcing compliance authentication and access policies, and in logging all user events.

Identity Requirements for Access Controls and Audit for SaaS Apps

» **Established Compliance Marketplace:** Compliance regulations make no exceptions for data owners using the services of data custodians to process or store sensitive information in SaaS and Internet-based applications. Data owners are required to apply the same standards for confidentiality, integrity and availability with a system of policies, procedures and controls for all sensitive and confidential information, regardless location.

Most SaaS and outsourced application providers offer baseline security defenses of perimeter firewalls, intrusion detection and prevention, anti-malware and physical security to protect systems hosting services and their customer's information. Managing security controls for perimeters, intrusions and anti-malware is a fast-growing market driven by established SaaS benefits of lower cost, and skilled and specialized expertise on demand 24X7. Managed security service providers offer professional services with expert knowledge of security and privacy requirements. The managed security services marketplace is forecasted to jump from \$1.3 billion in 2007 to \$2.8 billion in 2012, a compound annual growth rate of more than 17%.⁴

Many managed security service vendors, such as Qualys, Verisign, IBM, EDS, Verizon, AT&T and others, provide managed security services to relieve companies from the cost and complexity of operating defenses against baseline threats, or to uncover common vulnerabilities.

³ Forrester Research, Identity Market Forecast 2007-2014, Andras Cser et al

⁴ IDC, Managed Security Services 2007-2012, Irida Xheneti



» Standalone Identities – Costly and Unmanaged, Not Correlated:

Compliance regulations require regular monitoring of all authentication and access to, and actions taken with, sensitive information, regardless of location. The requirements levied by HIPAA, GLBA, the EU Data Protection Directive and SOX, with additional security requirements such as the Payment Card Industry Data Security Standard, require consistent user access monitoring with regular correlations of events to detect policy violations and trends in access attempts to protected information.

Companies facing this problem for a distributed mix of SaaS and Internet applications must augment the baseline identity capabilities offered by SaaS and outsourced vendors as custodians of sensitive data. Strong authentication may not be available, or is very expensive to deploy where required, and may violate restrictions against installing software or tokens on a client PC. Active real-time 24X7 monitoring of access and authorization for sensitive information inside a SaaS app is difficult or impossible. Further, SaaS and outsourced identity controls and procedures do not integrate with those already deployed inside the enterprise firewall. Similarly, authentication and access controls inside the trusted network are difficult to extend outside to the SaaS domain. Efficient identity operations based on economies of scale are impossible. The result is weakened security and increased risk, with standalone identity silos, non-integrated controls, uncorrelated log data, inconsistent policies, costly duplication and redundancy.

SaaS and Enterprise Identity Compliance Secures Users With Process and Technology

Privacy and data integrity regulations require owners of protected information to manage access controls and authentication to monitor their users, and perform regular audits of logs. These are major tasks spanning geographically dispersed people, processes and technology, and are significant cost items stretching deployment budgets and schedules for access and auditing controls for enterprise, SaaS and Internet applications.

A classic attempt to solve the enterprise identity compliance problems has been buying software and trying a technology fix. Technology alone is a high-risk approach for authentication, access and authorization, which includes users and therefore spans people and processes, in addition to technology. Technology alone does not provide a complete solution for problems spanning all three, often creating problems for people and process. Identity technology solutions also become very costly over the operational life of the solution, with lifecycle costs easily exceeding the initial identity software license cost by a factor of 4-5 times.⁵

Technologies such as federation have been deployed to address identity integration, usually as a type of single sign-on (SSO) functionality. However, neither federation nor SSO are compliance requirements. SSO delivers process benefits by easing user access to multiple applications with one authentication but it does not strengthen authentication and access.

Efficiently managing authentication, access and authorization processes is beyond the scope of federation software based on the Security Assertion Markup Language (SAML) standard. SAML was designed to link domains in a chain of trust and requires considerable custom integration and lengthy deployments to deliver coarse-grained, inflexible “one size fits all” SSO. Federation’s lack of access, authorization and audit functionality creates legal and liability issues that must be contractually addressed to specify access and authorization limitations and liabilities.

⁵ Burton Group, Provisioning Market 2008: Survival of the Fittest, Lori Rowland & Gerry Gebel



Similarly, multiple authentication technologies frequently 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. Authentication involves people and process, requiring careful planning for efficient and effective strong authentication to meet compliance requirements. A thorough understanding of security issues, including managing the authentication controls, frequently channels multi-factor authentication investments to less-costly methods friendlier to people and process.

The practical impact of the FFIEC guidance for Internet banking users has been the adoption of a less-costly mix of multiple passwords, with each password originating from a different source. Costly deployments of “what you have” or “what you are” multi-factor authentication methods may exceed the security need underlying the authentication compliance requirement while failing to address any part of access (where you can go) and authorization (privileges) compliance requirements.

Symplified is a Unique Compliance Solution for SaaS and Cloud-based Identities

» **Cloud Perspective Offers Privileged Vantage:** Viewing compliance events such as authentication, access and authorization from within the network cloud offers a unique and privileged top-down perspective. All events enforced from within the cloud are centrally monitored and logged. This allows Symplified to create a unified audit log and reports for all authentication, access and authorization events to support compliance policies enforced within our cloud-based service. Symplified’s unified cloud-based security and compliance extends to all downstream users and applications - internal and external users authenticating and accessing all enterprise, Internet and SaaS applications and resources.

The impact of this privileged position for compliance policy enforcement is enormous. Enterprises frequently deploy multiple monitoring solutions to enforce or log compliance events, such as authentication and access, in distributed locations. Symplified’s privileged cloud vantage unifies many monitoring and logging functions, recording from the cloud the actions of internal and external users accessing applications anywhere. Additionally, Symplified’s centralized policy enforcement logs all monitored activity into one unified log, eliminating the need to normalize incompatible data acquired from multiple locations.

» **Virtualized Identities Streamline Deployments:** Symplified’s innovative virtualized identity technology is an easy-to-use tool for building and strengthening compliance. Symplified’s virtualized identities allow you to 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.

Symplified’s patent-pending schema discovery tool, launched over an encrypted VPN tunnel to the destination repository, probes and presents the schema from which the authentication or access attributes can be selected to support the compliance policy. Once selected, the attributes automatically are 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.

Virtual identities and schema discovery represent significant breakthroughs for deploying identity management solutions and in developing compliance policies. Unifying and logically mapping user attributes from distributed repositories saves hundreds of man-hours needed to manually

locate, normalize and integrate user information to deploy an identity software solution. Business agility and changing conditions are easily accommodated.

» **Visual Policies Ease Management:** Visual policy development and mapping tools, such as Symplified's SinglePoint Studio™, are intuitive tools that enhance clarity and understanding. Symplified Studio eases and speeds the task of creating and managing role-based compliance policies across their lifecycle. 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, such as Studio, result in stronger security compared to a patchwork of logs, spreadsheets and scattered audit data.

Symplified's privileged vantage inside the network cloud, coupled with the innovative Studio policy development and management tool, unites policy development and enforcement for the enterprise in one location. Authentication and access policies to support compliance are deployed to all enforcement points on Symplified's SinglePoint network as the policy is saved and activated with a mouse click. Policies remain effective until deleted or inactivated.

Unified Logging and Reporting: Symplified's SinglePoint™ network is a cloud-based identity and compliance service, logging volumes of authentication and access events from the top-down vantage point. SinglePoint offers a single audit log for multiple physical and logical locations and networks, user repositories and protected applications.

A distributed network of user repositories, protected applications and policy enforcement points takes many hours to acquire and normalize information gathered from incompatible logs. Symplified puts all of this critical audit functionality in one consistent file type, secured in a central location. All authentication and access audit information is easy to access, strengthening security and compliance.

Start realizing the benefits of Symplified's innovative On Demand Identity now. Call Symplified today at 303.318.4188, Ext. 1 to schedule a free demo.

Symplified | The Cloud Security Experts, enables Enterprise 2.0 to adopt cloud computing by providing the security and identity infrastructure for the On Demand world. Symplified's revolutionary On Demand Identity™ is a network-delivered identity security service that eliminates the cost and complexity that has constrained identity software deployments.

Symplified's Cloud Access Manager™ single sign-on service eases multiple user logons with one convenient authentication. Symplified Web Access Manager™ is an affordable and easy-to-use unified Web access control service that strengthens Internet security and enhances business agility. Symplified's SinglePoint™ network eases the deployment and management of complex identity technologies.

The Symplified team brings decades of collective experience from solving the security and identity challenges of some of the world's largest enterprises to the new challenges presented by the shift to cloud computing and software-as-a-service.

Symplified, founded by the management team that created Securant, pioneered the Web access software market and was acquired for \$140M by RSA Security. While at Securant, founders Olden and Platt co-authored AuthXML which today is the core of the ubiquitous SAML standard. Symplified is applying this unique experience and heritage to the next generation identity and security problems facing enterprises today.

Venture funding was provided by Granite Ventures and Allegis Capital.
Visit us on the web at www.symplified.com.

