Success in the Enterprise

Making SaaS Manageable

A Conformity White Paper

EXECUTIVE SUMMARY

In the ongoing quest to reduce costs and simplify IT, large enterprises are increasingly opting for software as a service (SaaS) as an alternative to traditional software investments. Consider the following recent online media reports:

- *InternetNews.com* (March 27, 2009) reported IDC's expectation that SaaS sales will grow at a rate of 40 percent in 2009. The report also specifically noted enterprise customers' potential eagerness to take advantage of SaaS' lower costs and ease of deployment.
- *TechWorld* (January 16, 2009) reported findings from a Forrester study showing double-digit growth in subscription revenue for SaaS vendors in 2008. The study also revealed that enterprises, rather than small and midsize businesses, are the largest users of SaaS.
- *itworld.com* (December 2, 2008) reported on a recent Gartner survey that indicated that nine out of ten companies in eight major countries worldwide planned to grow their use of SaaS in 2009.

The allure to the CEO, CFO and business executives is understandable: With a third party hosting the software, an enterprise can eliminate costs and complexities associated with installing and maintaining programs on multiple systems. For the CIO, however – who is charged with governance over enterprise IT systems, including software – it's more complicated.

Simply put, the issue is this: If a third party controls the software, data, and access, and the CIO no longer has the capabilities to directly monitor and manage software operations, how can the CIO fulfill his or her responsibility for governance, especially with regard to critical areas such as governance and compliance? It's a question that SaaS vendors must address if they expect to effectively compete and succeed in the enterprise marketplace.

This white paper examines the CIO's need to manage SaaS applications as part of the larger responsibility for systems management in the enterprise and looks at steps SaaS vendors can begin to take to meet this need.

SAAS MANAGEABILITY: THE KEY TO MOVING FROM MID-MARKET TO ENTERPRISE SUCCESS

Early adopters of SaaS technology have typically been small and medium-sized companies driven by business priorities to embrace the SaaS model of multi-tenant, third-party hosted software. SaaS offers these companies the obvious advantages of lower costs, with no large, single licensing fee; reduced on-site data storage requirements; and reduced need for IT personnel to handle monitoring and maintenance tasks. It is this last point that changes the game on the enterprise level.

In smaller organizations that adopt SaaS, there can actually be an advantage to IT doing less, from the standpoint of optimizing lean resources. Responsibility for adoption and management in such organizations is often shared with or wholly owned by empowered business owners. But in the enterprise environment, nothing could be further from reality. There, the CIO is ultimately responsible for the technology solutions that will enable the business. As part of this responsibility, he or she must be able to exert authority over technology to a far greater extent than the original SaaS model allows.

It's understandable that IT has been to a great extent overlooked by the SaaS model, in the interest of the business benefits that SaaS can offer – specifically for organizations that operate on a different scale and governance model than large enterprises. Now, however, the time has come for SaaS vendors to adapt to what the enterprise CIO requires. Those that don't adapt will lose crucial opportunities to those that do.

WHAT A CIO MUST DO – BUT CAN'T WITHIN THE EXISTING SAAS MODEL

The enterprise CIO has a number of global priorities. While these may vary somewhat from industry to industry, they will generally include the following.

- **Technology-enable the business:** The CIO's team provides the technical services that keep the business operating productively on a day-to-day basis.
- **Evaluate opportunities:** As technology opportunities and best practices emerge, it's the CIO's job to identify them and evaluate their usefulness to the enterprise.

- **Deliver capabilities for strategic advantage:** The enterprise IT executive must continue to analyze technologies that can deliver a competitive or strategic advantage. Enterprises rely on the CIO and technology teams to deliver in this area.
- **Maintain business continuity:** The CIO must ensure that IT systems that enable the business remain viable and functional, without interruption, in the event that the company's operations are disrupted. Business continuity includes managing service level agreements with internal and external customers.
- **Manage security and risk:** The CIO must carefully manage overall security, risk, and compliance across enterprise systems and solutions. This includes maintaining regulatory, license, and corporate compliance.

For the CIO, the problem with SaaS is that it fundamentally disrupts current approaches for delivering on these technology priorities – since the processes and data associated with them have moved, along with the software, beyond the organization. From the CIO's perspective, the *responsibility* for all these areas remains with the CIO's team – but the ability to *fulfill* the responsibility does not.

Specific Capabilities CIOs Need

There are a number of specific capabilities on which CIOs have traditionally relied in their efforts to fulfill the responsibilities outlined above; several key examples follow. As CIOs analyze cloud and SaaS offerings, they continue to find these capabilities lacking, which can negatively impact their endorsement of the offerings.

- **Performance and uptime validation:** To ensure adherence to terms of internal and external SLAs, and for business continuity planning purposes, CIOs traditionally use SNMPs, network probes, and dedicated network monitoring tools to gain visibility into complex solution performance and availability.
- **Usage and activity management:** CIOs rely on event monitors, data reporting, and event logs to monitor software and systems activity, providing a basis for tuning application and systems performance.
- **Compliance management:** Regulatory compliance requires that CIOs be able to monitor application access, changes to permissions, and other activities that affect compliance with regulations and policies – and to demonstrate compliance through data reporting and event logs.

- **Identity management:** The CIO enforces policy-driven identity in the enterprise by managing user profiles and permissions across applications and systems and by mapping policy to users and their roles.
- **Business process / integration:** CIOs are accustomed to integrating on-premise software applications into IT management processes and tools – such as directories that contain information on users, groups, and policies.
- **Security policy enforcement:** The CIO's team is responsible for securing all enterprise IT assets, including software, and typically accomplishes this using a variety of physical and virtual security tools.

FOR VENDORS: THE SUCCESS IMPERATIVE (AND THE PRICE OF FAILURE)

The enterprise is the next frontier for SaaS vendors, and preparation is the key to exploiting the opportunity. There are a number of steps SaaS vendors can take now to start to address CIO concerns about identity and systems management in an environment increasingly characterized by SaaS and cloud technologies. The remainder of this paper is dedicated to describing what vendors can do to get ahead of the curve on this issue.

Why is this so important *now?* There are several reasons.

1. Enterprise business will be won by the SaaS and cloud vendors who are first to demonstrate an understanding of CIO concerns and execute a strategy to address them.
2. If SaaS vendors don't make this a priority, legacy enterprise vendors will – and they already have the advantage of inroads into the enterprise with their on-premise applications. SAP and Oracle, for example, have both recently announced increased investments and renewed commitment to their SaaS-based offerings.
3. If SaaS vendors don't fill the systems manageability vacuum created by the SaaS model, CIOs and business owners will do it themselves. SaaS vendors can avert a future of cobbled-together legacy tools and processes in the enterprise by having the vision to address the problem now.

BEST PRACTICES: WHAT TO CONSIDER GOING FORWARD

Perhaps the toughest question for SaaS vendors who want to address enterprise CIO concerns about manageability is simply where to start. What kinds of information and data do CIOs need? How do you begin to provide access to it? Conformity proposes a set of best practices in several key areas that can help SaaS vendors who are thinking seriously about how to address CIO concerns.

General Best Practices

Before looking at best practices in specific areas, it's useful to consider how to approach them generally.

- **Be a part of the big picture.** Any SaaS vendor that is considering how to develop solutions to empower CIOs would do well to keep in mind that this is ultimately an issue of concern for the global SaaS industry. This is going to be the case whether those solutions involve APIs, event streaming, or any other capability described in the remainder of this white paper. While individual vendors do need to be concerned about taking steps that will help them establish competitive advantage in the enterprise market, no one vendor acting alone can eliminate the CIO-related barriers to adoption in this area. The best course requires taking a visible industry position on the topic, taking advantage of opportunities (including standards efforts, CIO consortiums, vendor working groups), and partnering with companies specializing in management solutions.
- **Be a part of the existing environment.** Solutions enabling SaaS management should interoperate with existing on-premise vendors and solutions – and not require CIOs to operate an entirely separate management infrastructure for SaaS applications. At the enterprise level, there are longstanding relationships and deployments in which the CIO and the organization as a whole are likely to have invested significantly over time. The answer is not to ignore this infrastructure, but to take advantage of it to simplify, rather than complicate, IT operations when SaaS is introduced into the enterprise.
- **Be a part of the future.** Solving CIO-related problems does not require adoption of the 1990-era technologies currently in use, as some enterprises may suggest. In fact, addressing the IT challenges requires use of existing "2010"-based technologies that better align with SaaS and cloud computing initiatives, while developing the next-generation solution set. SaaS ISVs are positioned to set the vision by addressing long-standing challenges with a new technology suite.

Best Practices: APIs

APIs are crucial for connecting CIOs with the information they need to gain insight into information that affects performance, identity and compliance and to integrate SaaS applications into existing IT infrastructures. This has already been a subject of significant discussion in the industry of late; for example, *Network World* reported recently (May 20, 2009) that an industry panel at the 2009 Interop IT Expo and Conference pointed to APIs as one of the keys to acquiring customers going forward.

One of the primary roles of an API in SaaS solutions is to fulfill the request / respond function in which IT management solutions can initiate a transaction request for a particular action, and the application can respond. SaaS vendors therefore need to think about what kinds of requests CIOs and IT owners are going to be require and how to address them.

Within this general context, Conformity suggests that vendors consider the following as a starting point for recommended best practices for APIs.

- Where appropriate, use secure APIs to enable full visibility into information needed to support the CIO's efforts to discharge the responsibilities described previously. Security models will ideally be customizable based on customer needs, sensitivity of data, and regulatory compliance in effect.
- To both simplify IT and meet enterprise security and compliance initiatives, specifically build APIs to support segregation of duties and unique permissions (rather than just enabling a shared default login as "admin" that gives the API "user" access to all data).
- Separately manage the API and the administrative users in terms of licensing, access rights, and auditing. This will improve security and audit capabilities for automated access while further discouraging users from risking security by sharing administrative seats, since seat cost will not be a factor.
- Address enterprise requirements for testing or modeling API interactions before committing to a SaaS deployment or migration. At the enterprise level, it's vital to be able to simulate the effects of new technology rather than risk disruption of critical operations in a real-world environment.

Best Practices: Activity Access

In activity access, action to provide information to a CIO is driven by the server initiating an event, rather than by the user initiating a request. The key to addressing this successfully is to think through what kind of business information, and the extent of the information, that needs to be provided.

With the importance of defining information for activity access in mind, Conformity suggests that vendors consider the following as specific best practices for access to information on user activity.

- In defining solution-generated events, design beyond user login to include activity by active users once they are logged in. For example, did a user who was logged into an application create new content within the app? Did he or she delete content? Was the deleted content critical? Was key information exported? This level of granularity is critical to enabling the CIO to maintain application security and visibility into important user actions.
- Provide both real-time event access and access to historical logs reporting on events that have already taken place, using a streaming model for real-time and critical events and using batch reporting for log access.
- Enable customers to prioritize events and information and categorize data in a way that makes it easily accessible to them. For example, a user should be able to query for specific event types that are of particular interest based on his or her role in the organization.
- Adopt a best-practice security model for real-time and batch data access, ensuring alignment with organizational security policies and government regulations including SOX, HIPAA, and PCI.

Best Practices: Performance / Probes

Being able to monitor performance and uptime is essential to the CIO for a number of reasons, from making sure that IT is meeting the terms of SLA agreements to planning for business continuity in the event that operations are disrupted. SaaS vendors need to think about how to deliver the ability to check performance and uptime to be sure applications are running at required performance levels at all times.

Conformity suggests that vendors consider the following as specific best practices for solutions related to monitoring performance and uptime.

- Provide on-demand probes that can be used to probe into performance and uptime of applications and components.
- Enable full visibility into information by allowing it to be included in external (customer-owned) dashboards, rather than just as part of the hosted login views.
- Enable access to information on the health of the customer's specific instance of the application and modules. Provide on-line enterprise visibility into their particular user's experience, versus uptime statisitics on the data center.

Best Practices: Back Office Visibility

At this point in the evolution of SaaS, there is no easy way for the customer to gain visibility into back office information, to speak of. But as the industry matures, and especially as it makes more significant inroads into the enterprise market, it is reasonable to expect that there will be increasing demand for easy access to business information on contracts, licensing, SLAs and other back-office areas. The time to start thinking about this is now.

Conformity suggests that vendors consider the following as specific best practices for visibility into back office information.

- Design solutions to allow access to information including contractual data, licensing, and SLA agreements between vendor and enterprise. Proactively notify customers of key events or contractual dates.
- Enable customers to track and manage all information and data that is relevant to these types of business information, including historical reference information.
- Look at how other industries have made visibility into this type of information a standard part of their business relationships. For example, communications service providers routinely enable customer access to online invoices that include detailed back office information.

Best Practices: Standards

Standards will ultimately be an important part of addressing all the areas discussed in this paper. But at this point in the evolution of SaaS, adequate standards have yet to emerge, even on the identity front. The lack of adoption and creation of needed standards has perhaps hampered the ability to proactively address the issues described here.

However, Conformity's view is that successful standards typically emerge *after,* rather than *before,* a particular issue is addressed by the industry. The challenge is therefore for the industry to develop models and approaches for APIs, activity access and so forth based on real-world experiences, and then for battle-tested standards to emerge from those models and approaches. Given this view, Conformity suggests that vendors consider the following as best practices.

- Play an active part in defining the set of needed requirements, rather than allowing technology vendors to convince the market to use their proprietary offerings or having customers standardize legacy practices in the absence of practices and standards.
- Start now: Don't wait for the best standard to be hashed out. While SAML, SPML, XACML, and other standards around authentication and access control may end up being an integral part of the answer, the first order of business is to make sure the industry has the appropriate models in place for satisfying end user requirements. Customers require working solutions to fully adopt SaaS applications, and will align with standards as they mature.
- Be mindful that standards need to be developed across the broadest range of capabilities, including user identity, event creation, event monitoring, credentials management, and federation.

CONCLUSION

An enormous market opportunity exists for SaaS and cloud-based applications in the enterprise. To capture this opportunity, SaaS vendors need to take the next step to ensure their services provide the management visibility needed to be truly enterprise-ready, and that they address the unique identity and systems management challenges created by the SaaS model. This is the first of a series of best practice white papers that Conformity will be publishing for SaaS vendor executives to help the industry meet the needs of enterprise CIOs and their teams. Please register at www.conformity-inc.com to subscribe for future white papers from Conformity, and to learn more about how we can help SaaS vendors address IT enterprise challenges.

ABOUT CONFORMITY

Conformity provides on-demand solutions that enable organizations to govern manage and control the software-as-a-service (SaaS) and cloud based applications proliferating across their environments. The Conformity platform enables organizations to centrally manage their SaaS applications, users and data, reducing security and compliance risk and providing visibility into operational costs associated with SaaS usage in their environments. Based in Austin, Texas, the Conformity team includes former executives and founders of pioneering companies in the systems and identity management software market. For more information about Conformity, please visit www.conformity-inc.com or email info@conformity-inc.com.

Provisioning SaaS Applications for the Enterprise
July 2009
Author: Scott Bils, Brian Kerns
Version: 1.0

Conformity
6300 Bridge Point Parkway, Building 1
Austin, TX 78730
U.S.A.

For More Information:
Phone: +1.512.795.5826
Fax: +1 512.795.5849
www.conformity-inc.com