

SaaS, The Cloud and the 'Big Bang'

Reinventing IT Management for
On-Demand Environments

A Conformity White Paper

EXECUTIVE SUMMARY

Questions around whether applications delivered via software-as-a-service (SaaS) or cloud-based models will 'go mainstream' have largely been answered, with the primary topic of discussion now shifting to 'how far' and 'how fast'. While offering clear operational and financial benefits over on-premise alternatives, organizations are finding that SaaS and cloud-based applications fundamentally explode their traditional models for governing and managing applications, users and technology resources. These organizations are finding that processes, approaches and tools developed for management of on-premise applications and infrastructure are not easily extensible to applications and data that have migrated outside the corporate firewall with SaaS. This whitepaper discusses the challenges and risks associated with re-integrating SaaS and cloud-based applications and resources into existing IT and financial management approaches and solutions, and proposes characteristics of a new class of management platform that needs to emerge.

According to Forrester Research, nearly 50% of enterprises are now using, piloting or considering use of SaaS applications.

A recent Conformity survey found that IT is now involved in managing or administering SaaS applications in 72% of multi-SaaS organizations.

SAAS IS HERE TO STAY

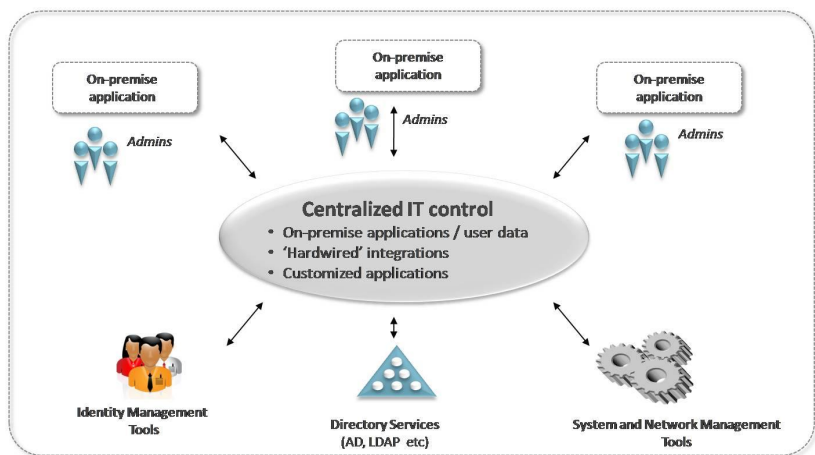
The question around adoption of applications delivered via a 'software-as-a-service' (SaaS) or cloud-based models has rapidly shifted from 'if' to 'how quickly' and 'how far'. The economic downturn has increased the attractiveness of SaaS and cloud-based applications to budget conscious executives, and is driving faster market adoption than even most analysts had expected. Empowered business users, unencumbered by traditional deployment costs and IT investments and restrictions associated with on-premise applications, continue to drive adoption of true 'best of breed' applications and solutions. SaaS adoption is now occurring in areas once reserved exclusively for on-premise applications, including mission critical applications such as ERP and HR in both small and large enterprises. Additionally, cloud-based services are moving below the application layer as Amazon, Google and other vendors offer organizations metered access to cloud-based servers, storage and infrastructure on-demand.

The accelerating adoption of SaaS applications and on-demand services is beginning to hit 'critical mass' in many organizations today, raising executive-level questions around how to most efficiently and effectively manage environments that are increasingly migrating outside the firewall. While the downturn has accelerated adoption of cloud technologies, it has not removed the organizational responsibilities for IT oversight, fiscal control and regulatory compliance. The first step in identifying the questions that need to be addressed is to examine the impact SaaS is having on 'conventional' IT management models.

THE TRADITIONAL IT MANAGEMENT MODEL

Most organizations adopting SaaS or cloud applications initially approach the IT management challenges by attempting to extend legacy infrastructure and processes. While acknowledging that IT environments and management models are as heterogeneous as the organizations that implement them, it is useful to examine some of the common characteristics of these models involving predominately on-premise applications and resources:

The Traditional IT Management Environment



As seen above, predominately on-premise environments that predate widespread adoption of SaaS and cloud-based applications are characterized by:

Centralized management – in many organizations IT has complete responsibility and accountability for governance and management of technology resources within the organization, including infrastructure, development and operations. This span of control has a

also included management and support of business applications, including COTS and homegrown applications and their associated users. This autonomous focus on IT governance and management has moved from optional to mandatory in the past decade due to the need for organizations to comply with information security requirements associated with SOX, HIPAA, GLBA, PCI and other regulatory acts and industry requirements. This has led to the adoption of best practice governance, management and control frameworks such as ITIL, COBIT and ISO 17799/27001/27002. Adherence to these process and control frameworks has increased the management visibility of IT governance and management, the centralization of accountability with IT, and the investment in on-premise management tools.

On-premise control – traditional IT management environments have also been characterized by full IT control not just of applications and data, but also the associated IT management tools and solutions. CIOs and IT organizations have been responsible for managing the full application lifecycle from deployment, management, monitoring and support through retirement, including the responsibility for managing users and associated permissions and access rights. Access to critical applications and data is controlled through IT management of user authentication, authorization and audit capabilities often through premise-based directory services tools (Microsoft Active Directory, LDAP) and systems and identity management platforms and point solutions. While in some cases BPO and outsourcing activities led to the transfer of infrastructure and assets to 3rd party service providers, these providers are acting as a proxy for IT, and still demonstrate full control (on-premise or remotely) of the IT stack.

'Hardwired' integration – finally, traditional IT management environments have been characterized by a high degree of integration. Services intensive deployment of broad enterprise application suites supplemented by custom application development led to tight integration between business processes and supporting applications. From an IT management perspective, these 'traditional' environments are characterized by tight integration of agent-based systems and identity management solutions into business applications, help desk solutions and directory services. This has enabled organizations to have significant visibility and control over the deployment and management of technology resources, enabled by the advantages of on-premise instrumentation of applications.

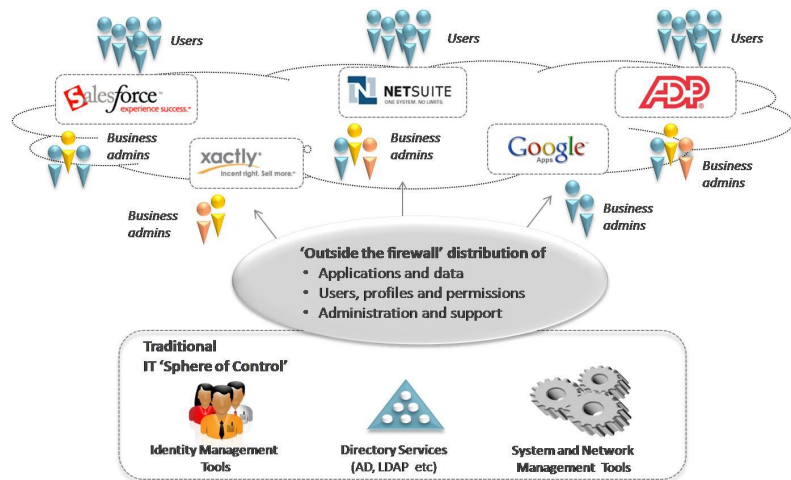
"My biggest challenge with SaaS? My team's complete loss of management visibility into what's going on out there..."

- CIO, Fortune 500 Financial Services

THE EXPLOSION OF THE TRADITIONAL IT MANAGEMENT MODEL

Turning the page forward, organizations that have been aggressive adopters of the SaaS model are finding that SaaS, cloud- and web-based applications are creating significant disruptions in the traditional IT management model. These disruptions are raising difficult, executive-level issues regarding not only accountability for management of on-demand environments, but exactly *how* they should be managed. While web-based applications are certainly not new to IT, migrating the application and control to third-party vendors outside the firewall is a new dynamic unique to SaaS.

The New Management Environment



As seen above, on-demand applications are fundamentally exploding the traditional IT management model due to:

Decentralization of management – due to their ease of configuration and deployment many organizations have virally adopted SaaS applications without IT awareness or oversight. In fact in a recent survey CIOs on average underestimated by 40% when asked how many SaaS applications had been deployed by their organizations. With little or no IT involvement, business users themselves have provided administrative support for the SaaS applications they've deployed. In these roles, business admins have taken on management and support responsibilities traditionally owned by IT, including ownership of:

- User provisioning, deprovisioning and ongoing permissions management
- Role and profile management
- Application customization and configuration
- Vendor and contract management

Even in models where IT has re-entered the SaaS management picture, administrative functions are often still delegated to business admins who possess greater knowledge and insight into the relationship between business processes, applications, roles and users. Though delegated, these models often require sophisticated process coordination between HR, IT and business units for management of users and access. Interestingly while in most cases business users maintain ownership of vendor and contract management issues, they often look to IT when issues arise around availability and SLA performance of external SaaS and cloud-based applications.

"We literally have no way of truly ensuring effective segregation-of-duties across the SaaS applications we have deployed today..."

- CIO, Technology Services Provider

Loss of control – along with the decentralization of traditional management outside of IT's sphere of control, SaaS is 'breaking' the traditional access and control IT has over the applications. In addition to the physical ownership of the applications, the migration and fragmentation of the following to each service provider is also critical from an IT management perspective:

» Data - along with the application itself, sensitive corporate data migrates outside the firewall with SaaS applications. Though the data has moved offsite to a third-party service provider, from a compliance perspective the organization is still solely responsible for the confidentiality, control and security of that data. With the migration offsite, organizations also lose centralized visibility (and the associated metadata) into what data is resident in what applications, an issue increasing in importance as SaaS penetrates mission-critical applications with financial reporting or information privacy concerns. The data visibility challenge is compounded by typical 'best-of-breed' SaaS approaches, where multiple ISVs host different portions of the business process and supporting information. While most SaaS ISVs ensure the integrity and security of their customers' data through adherence to SAS70 standards and best practices, organizations also need cross-application, business process-based visibility into data, including availability and security.

» Role and profile models – each SaaS application typically contains its own model and nomenclature for defining and managing organizational roles, application roles and profiles. These models are typically idiosyncratic to the vendor and problem set for which their application is optimized. For example, the organizational role model in a sales compensation application requires deep understanding of organizational reporting relationships and dependencies to correctly calculate commission payments. This company-specific data model may differ significantly from the native organizational model developed by the vendor for a CRM, ERP or HR application. This makes it difficult, if not impossible to propagate an existing single organizational 'system of record' role model that might be contained in existing HR systems or directory services across multiple SaaS applications.

In addition, each application typically contains different security and permissions models and constructs for administrators and users within the application - in fact in some SaaS applications the semantics behind 'role' and 'profile' is reversed from mainstream usage. In addition, the specific permissions and authorizations also can significantly differ across applications, as well as the granularity to which permissions can be applied. While some applications enable profile-based field-level control of create, read, update and delete (CRUD) actions, others enable manage of CRUD at only the highest level within an application, creating confusion and risk for adoption organizations.

» User authorization and credentials stores – data around application-specific user permissions and authorizations moves out of the organization to each specific service provider. The inability to centrally track, manage and control application users and associated permissions and privileges in many cases breaks the ability to monitor compliance and security best practices around segregation-of-duties, role-based access control (RBAC) and least 'privilege' concepts. In addition, each application typically provides its own user credentials store, which in traditional models was managed on-site through directory services or identity management solutions and tools.

"True best of breed should finally become a reality with SaaS. Unfortunately the management 'glue' just isn't there yet."

- CIO, leading data services vendor

- » Usage activity – in the SaaS model activity logs are also hosted offsite and do not leverage a common format or access model. While established logging and monitoring standards such as syslog and SNMP exist in the on-premise world, there currently are no analogous standards for SaaS or cloud-based applications. Not only are standards lacking, but the ability for SaaS vendors to provide access to log data for end-customers varies widely, and often requires manual requests. Without visibility into usage and access to event and activity logs, organizations are unable to effectively monitor and enforce policies, creating significant security risk and compliance exposure.
- » Availability / performance data - data on application availability and performance also moves 'outside the four walls' in on-demand environments, making it difficult if not impossible for IT organizations to assess and remediate application performance issues, and to effectively determine if vendors are complying with SLA commitments.

'Broken' integrations – SaaS applications have evolved as best of breed 'point solutions' that are focused on addressing a specific functional problem set. While multitenant SaaS models do generally provide customers a limited ability to customize a virtual instance of the vendor service, they have been architected to address specific problem sets or functional workflows, creating problems on two dimensions.

From a broad business process perspective, SaaS applications must be integrated into existing business processes through upfront manual configuration and ongoing management by line-of-business administrators with knowledge of processes, applications and users. While in some cases data integration can be handled through third-party solutions, the ability to manage SaaS applications and users in the context of a broad business process is nonexistent, especially where SaaS administrators are acting autonomously.

From an IT administration perspective a similar challenge emerges. Today many IT processes around application and user management are highly automated, supported by on-premise management solutions. Organizations are unable to administrate SaaS applications with on-premise systems and identity management systems. Many of these legacy solutions are agent-based and have not been instrumented for the challenges of SaaS deployments, and development of one-off customer SaaS gateways is not proving to be a cost-effective option. Finally, SaaS applications break organizational reliance on existing directory services and help desk / trouble ticketing solutions, forcing a change in fundamental processes to realize the full benefits of SaaS.

While platform-as-a-service (PaaS) offerings have emerged to help address application integration issues, these platforms have yet to exhibit the ability to effectively normalize metadata around business process and data models across applications. Also while robust cloud to cloud and cloud-to-premise data integration solutions and services are emerging, these are focused on the transactional, not the management and governance layer.

"Responsibility for managing SaaS applications has just been thrown in our lap. As we haven't been involved we have no way of knowing what users have what access to what. Talk about scary..."

- CIO, publicly-traded software vendor

THE SAAS MANAGEMENT CHALLENGE

The adoption of SaaS and cloud-based applications and their 'big bang' impact on traditional IT management models are forcing organizations to fundamentally rethink not just how they manage required processes and policies, but also the tools and solutions they must integrate. The challenge is not purely theoretical, and is fast becoming a business critical priority for enterprises that are facing:

- » Increased security and compliance risk – the breakdown in traditional approaches for monitoring and enforcing policy create significant security and compliance risks. Organizations have little or no ability today to implement best practices such as role-based access control (RBAC) least privilege and segregation-of-duties (SOD) and audit logging with and across SaaS applications. This is particularly true as adoption and penetration deepens to touch ERP, HR and other applications that contain sensitive financial or employee related data.
- » Suboptimal spend on SaaS applications, licenses – organizations without a centralized view into applications, users and licenses are finding they lack the ability to know if spend on SaaS seats and licenses is truly optimized, and if full business alignment exists between users, roles and actual application usage.
- » Increased operational costs – with application management and support activities now distributed among business users, organizations are finding that many application and user administration activities are highly manual, redundant and inefficient, resulting in unnecessary cost to the organization. This is creating particular challenges for CIOs who are being asked to do 'more with less' in today's economic environment.
- » Decreased agility – organizations that have become cognizant of the security, compliance and operational asset risks associated with an unmanaged SaaS environment in some cases are putting additional application deployments 'on hold' until more robust enterprise class governance and management capabilities for SaaS and cloud-based applications become available.

A new type solution is required for systems and identity management in on-demand environments. This solution must re-integrate best-of-breed applications, data and users in a fundamentally new way for manageability and enable organizations to answer four key questions around their on-demand environments:

1. Access – which employees, contractors and partners have access to SaaS applications, data and cloud-based resources, and how can they access it (e.g. mobile devices)?
2. Authorization – upon access, what specific authorizations do users have to SaaS applications? Are permissions and authorizations consistent with corporate policy and security best practices?
3. Activity – what have SaaS users been doing in the applications, and have activities been compliant with overall IT and corporate policies? Do we have the ability to audit user activity within applications?
4. Availability – are our applications and data available and do they appropriately support users and business processes? Where is our mission-critical data and how can we be assured of access continuity?

"SaaS adoption, particularly in the enterprise, is accelerating faster than is being widely reported. As the result, the demand for a new type of solution to help organizations manage multi-SaaS environments is also developing much quicker than expected."

- Jeff Kaplan, THINKstrategies

To answer these questions new types of solutions will be required that are architected around the unique systems and identity management challenges that on-demand environments are creating. While still nascent, several core requirements for a new class of solutions are emerging:

Business process integration – new management solutions must support the integration of SaaS applications into existing IT management processes and workflows. These solutions also must provide the ability to manage applications and users in context of overall business processes they support, and have business context 'awareness'. The SaaS model is enabling organizations to begin to realize the vision of 'best of breed' applications, freeing them from the 'lock-in' to broad on-premise application suites. A new management framework is required that will more effectively integrate SaaS applications into existing businesses process and workflow.

Data / integration normalization – to provide better visibility into SaaS applications and their usage, and to support business process integration, new solutions must normalize the data models and integrations provided by SaaS ISVs and cloud services. For example, to be effective in the areas of security and compliance management data models around users, roles, profiles and permissions must be developed that support and normalize the heterogeneous application-specific models in use today. In addition to underlying application specific data new solutions must provide normalization of exposed SaaS application APIs. This normalization will be able to abstract and normalize widely disparate data models and non-standard APIs provided by SaaS ISVs in this area of access control, and also provide visibility into application administration such as availability, events and usage activity. As the SaaS market matures standards may emerge to drive vendor convergence, but early adopting organizations need solutions that support and address SaaS vendor heterogeneity today.

Policy monitoring and enforcement – Organizations are finding they have little if any capability today to extend their on-premise control frameworks to SaaS and cloud-based applications and resources. New solutions must enable organizations to monitor and enforce policies across their deployed SaaS applications. These solutions need to leverage normalized cross-application role, profile and authorization models and streamline and automate the ability of organizations to monitor and enforce multi-vendor policy.

Collaborative management – Effective management of SaaS applications and users will require a more collaborative, cross-functional approach than is typically seen in traditional IT management models. Unlike on-premise management models, governance and management in SaaS and cloud-based environments will require federation among business users, IT, finance and even HR. In addition, as cloud computing breaks down organizational boundaries, external business groups will need to be incorporated into any model, allowing stronger management of partners, customers and auditors in the SaaS models. New SaaS management solutions will need to provide the workflow and collaboration tools required to address the management needs and requirements of a much broader user constituency to be effective.

Platform, not point solution – effectively federating governance and management of SaaS-centric environments will require collaborative management and process integration driven by normalized data models and vendor integrations. To be effective, new management solutions must provide a platform that leverages these common elements to holistically address the challenges inherent with managing SaaS environments, and not just address a piece of the problem in a vacuum.

Open standards and interoperability – while many standards around SaaS access management, authentication and authorization such as SAML, SPML, OpenID, Passport and others have been introduced, they have yet to gain the critical mass among SaaS ISVs. A SaaS management solution should provide the flexibility to support these emerging standards, but also provide immediate value to organizations looking to manage major SaaS applications with current levels of provided access and integration. The platform should also have the flexibility to integrate with enterprise environments and provide organizations the ability to extend their current infrastructure and standards. A robust SaaS management platform should embrace (versus supplant) existing on-premise systems and identity management solutions, directory services, help desk systems and access management / SSO solutions.

SaaS and cloud-based applications are truly driving a revolution in how applications and technology is being used in organizations today. It's now time for the management solutions to catch up. While existing on-premise infrastructure management solutions and point security tools such as SSO/access management will play a role in the 'brave new world' of SaaS management, organizations are rapidly finding that broad new approaches and solutions will be required.

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.



SaaS, the Cloud and the 'Big Bang'

April 2009

Author: Scott Bills

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

Copyright © 2009, Conformity, Inc. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.