

Conformity slips the covers off its SaaS user management platform

Analyst: Steve Coplan

Emerging from semi-stealth, **Conformity Inc** is starting to go public with details of its platform for management and governance of software-as-a-service (SaaS) application usage. The most immediate use of its technology is likely to be as a centralized access control mechanism, exploiting its ability to maintain visibility into user activity and integration with directories and application infrastructure. The demand for multi-SaaS federation is only beginning to show signs of life, which would suggest an uphill climb initially for Conformity, and the need to focus on more narrow use cases.

Over time, however, and if there is enough market momentum, Conformity could harness the management issues raised by SaaS adoption that are out of the scope of existing approaches, to drive a new type of infrastructure that mediates between the user and a business object, as provisioning once promised to achieve.

The 451 Take

To characterize Conformity simply as a SaaS user management vendor downplays the sophistication of its technology. We see plenty of pragmatism in its approach and its read of current market requirements, but the issue becomes whether the midtier masses adopting SaaS as a de facto application consumption model are the ideal audience for the depth the company is building into its platform. While this is by no means a fatal flaw – since we expect Conformity to have plenty of opportunity going after breadth as SaaS adoption in general gains momentum – it may have to wait a while until market requirements mature.

Context

Conformity was founded in 2007 by CMO Scott Bills (formerly at **Scalable Software**), CTO Roy Kipp (formerly at NAC vendor **Mirage Networks**, prior to its acquisition by **Trustwave**) and VP of engineering Rich Pusateri (formerly of **QuickArrow**). CEO Tom Smith, who served as **Countermind** CEO and later chairman, joined the company in March, after Conformity had secured VC backing. Conformity, based in Austin, Texas, closed a series A funding round of \$3m in January this year from **Guggenheim Venture Partners**, after subsisting on seed funding of about \$300,000, we believe. The company currently has 20 employees, including an offshore team in Pakistan.

Technology

In terms of our cloud services classification model, applications delivered through SaaS constitute the uppermost tier in the stack. This is distinct from 'platform as a service' – such as **Salesforce.com's** AppExchange, which would reside below the SaaS tier. 'Infrastructure as a service' consists of compute resources and storage that can be consumed dynamically and in a burst-y fashion. But rather than falling into the overly broad cloud-security category, Conformity is focusing on the management issues raised by horizontal SaaS application adoption as one outcome of the shift toward a cloud services model.

The technology challenge (and the corollary market opportunity) Conformity is focused on is the governance, authorization and user management of applications consumed through a SaaS model. Governance, by our definition, incorporates both compliance and security, while the Web delivery model implicit in SaaS has primarily raised concern about access control and authentication. Indeed, a few vendors such as **Ping Identity, TriCipher, Symplified** and **Nordic Edge** have spent some time thinking on maintaining a consistent user store across multiple SaaS applications, and the problem of tying authentication to enrollment (as well as de-provisioning). SaaS vendors, on the other hand, have built some authorization capabilities into their management capabilities, generally by harvesting logic such as attributes, or user information such as group membership, in order to specify access control permissions and rules.

Conformity has more of a telescoped view of the requirements – which is predicated on a secular shift toward more reliance on SaaS applications, increasing the absolute number used within an enterprise and broadening their user base beyond specific populations. As the shift gathers momentum, application usage and access will increasingly take place not only outside of the network perimeter, but also outside the sphere of customary IT management (and identity management infrastructure). As more applications are added, the more acute the problem becomes. Ping and others certainly view adoption of multiple SaaS applications as a catalyst for a centralized user store and single sign-on (likely delivered as a service in the cloud itself). Conformity, however, is hoping to live higher up the stack from these vendors, serving as a central point in the governance process, both capturing usage statistics by user, and serving as a central point of administration and repudiation.

For Conformity, the inflection point will come when enterprises realize they require a central point to aggregate the authorization capabilities and hooks provided by SaaS providers for a single application and a well-defined set of users across multiple applications and user sets. For the vendors focused on authentication and enrollment based on propagating changes from the enterprise directory to a local store, the impetus is likely to be more in the realm of operational overhead – or at least trying to maintain some level of access control while lowering the administrative load. As the number of users and applications grows, current ad hoc enrollment processes quickly become operationally intensive – new users and new applications must be added through a request process or automated through integration with a user directory.

This scenario of high administrative workload for extending access to resources is clearly analogous with the thrust behind enterprise provisioning. But where enterprise provisioning

has faltered in terms of breadth of connectivity, the issue with SaaS applications is the ease of connectivity, since it leads to decentralization. In a sense, what Conformity is aiming for is provisioning with integrated monitoring involving a platform interacting with services modules across an enterprise bus.

Products

In its first iteration of its SaaS management product – which is scheduled for early beta access in July, and to hit general availability in September – Conformity is aiming to address a more confined set of requirements, focused on access control. Access control, in this sense, amounts to providing a central point at which provisioning decisions to SaaS applications are captured, creating visibility into who has access to what, so as to ensure access decisions are consistent with policies across both SaaS and on-premise applications and can be easily incorporated into the audit process. Although Conformity is clearly intent on tight integration with identity management and views the actual process of role definition and management as a complementary activity, we believe the company is ultimately aiming to build a platform that will allow roles and permissions to be mapped to application function, wrapped up with compliance, reporting and workflow modeling.

For the near term, however, the company anticipates it can also advance down the path of providing usage analytics for understanding how users interact with SaaS applications, as well as determine whether license agreements are appropriate or whether more stringent service level agreements are required. Since most SaaS customers have limited direct visibility into usage patterns, Conformity anticipates that initially it can serve the purpose of providing the monitoring and reporting required for license compliance and variance, and potentially identity analytics.

In terms of its architecture, the Conformity product consists of a platform services tier and management module tier. At a high level, the platform services tier provides data integration and normalization, integration and policy monitoring. Interaction with and data extraction from SaaS application and identity management providers is through Secure Access Markup Language and Service Provisioning Markup Language. The platform also supports the WS-Federation protocol. The design principle behind the platform tier is to serve as a consolidated collection point for SaaS and on-premise application authorizations, identity management logic and systems management configurations. The normalized authorization and permissions then serve as the baseline for policy definitions and collaborative management workflow templates.

Above the platform services tier, Conformity is building modules for user management, compliance management, services management and process management. A stand-alone role and profile module is also in the works. The interaction and data exchange between the two tiers is implemented through an enterprise service bus that can operate as a service-oriented architecture or as XML messaging environment. Conformity anticipates the ESB will itself run as a cloud service.

User management, encompassing provisioning/de-provisioning and application-specific profiles, is the module that will probably get the most initial attention. However, the

architecture of the Conformity platform suggests far broader ambitions than the current use case scope – providing management and governance of how users interact with SaaS applications, with compliance, policy and process management overlays.

Competition

While we can't identify a direct competitor across the current landscape, particularly when Conformity's broader infrastructure ambitions as reflected in its architecture are factored in, there are several points of overlap that at some stage may develop into areas of direct competition.

As we noted in the technology section, we anticipate that the vendors concentrating on authentication and access control for SaaS – Ping Identity, TriCipher, Symplified and Nordic Edge – will more likely be complementary as opposed to competitive. Federated SSO cloud-based services will serve as a data and information source for the Conformity platform, and will potentially act as policy slaves to the Conformity policy engine, or consume workflows.

Over time, however, we anticipate that these vendors will look to migrate up the stack, assuming authorization and user management aspects – at which point, the balance will shift to direct competition. We see indications of that process already at Symplified, and believe that Ping and TriCipher are not far behind. With the incorporation of data normalization and richer workflow modeling, Symplified could expand into providing a more generalized set of identity management and governance capabilities.

There are distinct similarities in terms of architecture with **Fischer International Identity**, with its 'identity as a service' model that revolves around provisioning. However, Fischer is more focused on selling provisioning as a service into the midtier market, than with management of SaaS users. Again, over time, we expect the distance between the two to narrow.

Sonoa Systems could also be seen as complementary – and its Cloud Services Gateway could possibly even be an enforcement point. Sonoa's Cloud Service Gateway could be understood to reside at the 'edge' of the cloud, manipulating data flows as they traverse domains. Where we do see a point of overlap is in the area of SaaS API management. While Sonoa is currently front-ending SaaS APIs to provide scalability, the visibility into who is calling the API, and how, could be used to extend its analytics pitch.

At this point, we don't view the incumbents working on an identity services layer – **Oracle** (and its intended acquisition target **Sun Microsystems**), **Microsoft** and **CA Inc** – as direct competitors since the thrust of their efforts is building the infrastructure to allow applications to call out to logic repositories in order to make dynamic authorization decisions. But if we assume that Conformity is heading in the direction of providing a comprehensive provisioning and access management platform, and that identity management vendors will eventually have to devise a consistent approach to managing how users access SaaS applications, some degree of competition is inevitable.

SWOT analysis

Strengths	Weaknesses
Conformity has been built from the ground up to tackle the problem generated by a fundamental shift in how functionality is consumed, and potentially circumvents existing controls.	As the more modest use cases the company is planning for its beta participants illustrate, it could be ahead of the market – or even overshoot it. Plus, it has to deliver on the management platform it envisions.
Opportunities	Threats
Although actual revenue from identity management for SaaS has been elusive, we anticipate that the desire to lower operating costs in a tough economic environment through increased adoption of SaaS and cloud computing will drive the need for a more systematic user management platform, with automated decisioning and embedded governance controls.	Identity management vendors are well aware they have to find a way of managing SaaS users, but may be able to address the need through an identity services layer, with incumbents like Oracle and Microsoft (or IBM) tying the technology to their application infrastructure.

Reproduced by permission of The 451 Group; copyright 2009. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to:
www.the451group.com