

SaaS Expands Into Identity Management

BY STEPHANIE HAGOPIAN

As business environments become more and more complex, the demand for continual growth and constant change keeps mounting to dizzying heights. If your organization struggles with never-ending shifts in infrastructure, as well as major structural overhauls due to mergers or acquisitions, you are certainly not alone. Expansion seems to be a driving force for success these days, which puts overwhelming pressure on every organizational unit to cut costs, lower budgets and manage people, processes and projects with fewer and fewer resources.


One of the most significant expenditures for organizations stems from the challenge to own and operate various software applications in order to keep up with frequent advances in technology. The idea being that the latest and greatest technology will keep an organization relevant in a highly competitive market. While there's never any argument that the functionality embedded in these solutions are essential to successfully operate a growing business, the cost of the software itself, the related hardware environment needed to host the solution, and the people required to run it all contribute to a significant and worrisome financial burden. As a result, companies are starting to search for viable alternatives to some of the more traditional business models that will ease some of their financial woes without sacrificing technology in the process.

We're seeing it more and more. Help desk calls are answered by people in entirely different countries and programmers are developing software 5,000 miles away from the actual company who owns it. It is a steadily growing trend to see organizations no longer own and manage software internally, but to let a trusted third-party securely operate a solution instead. And, there's a good reason for this tactic; it allows an organization to gain the functionality it needs without the burden of licensing, implementing, managing or updating that software.

Commonly termed Software as a Service (SaaS), remote software management boasts many benefits, including increased service levels, lower long-term investment costs, shorter time to value, improved business continuity and disaster recovery, better access to advanced product functionality, and less risk.

With the incredible success of companies like Salesforce.com, it was only a matter of time before every type of technology would try to adopt a similar model. Identity Management as a Service is the newest evolution of this trend. As an integration-based technology, it has the overall benefit of integrating application technology silos into a cohesive platform to manage business processes, allowing organizations to function more securely, effectively, efficiently, and profitably.

Stephanie Hagopian is the director of business development in NetworkingPS' Security Management Services Practice. Visit www.networkingps.com for more information.

 MORE INFO

For more on SaaS, read the remainder of this article.

 AUDIO FILE

Additionally – there is a third article available in an audio format

SaaS Expands Into Identity Management

By Stephanie Hagopian

(This is the second half of this article. The first half can be found in the print and interactive versions of TechNews.)

Identity Management as a Service is a fully hosted and managed web-native identity management solution that allows an organization to take advantage of the latest generation of identity management (IdM) technology without the financial burden of owning the software itself. Like any traditional IdM solution, a hosted service provides organizations with the ability to manage the entire employee lifecycle and automate the management of identities, access rights and resources across multiple IT applications and business processes.

When it comes to Identity Management as a Service, the benefits are fairly straightforward. Traditional IdM implementations can become both expensive and time-consuming, especially if your organization doesn't have qualified resources on staff to integrate and manage the solution in a production environment. Although a proper skill set is still essential to any successful IdM project, it is highly unlikely that additional staff will have to be hired for your impending project if it is being incorporated into your organization as a service.

Mainly, it is most important that your organization makes sure to have the proper business and technical analysts available to identify the necessary IT and business requirements for all relevant stakeholders, as well as an individual who will relay the organization's goals, business processes, and security policies to the third party who will be responsible for managing your solution. If the nature of your business demands far less staff members who are prepared to handle these technical and process-related functions, then these functions can be off-loaded by a consulting firm as long as the proper sponsorship is in place -- and access to both the required system and people resources is allowed. In some cases, it might even make more sense for your organization to outsource all of your technical activities, in which case, the IdM consulting firm would require access to all of these providers as well.

Identity Management as a Service is really ideal if you have a small to medium business that has either never had an IdM solution in place before, or is looking to replace a solution that has excessive overhead. In either scenario, the newer and less customized the platform or application, the more ideal it will be for a hosted IdM model. Ideally, you'll want all of your applications and back-end systems to eventually become part of a service-oriented architecture, so cross-domain workflows and data integration can be more easily achieved.

No matter what the nature of your company, there are 10 key questions that should always be considered when investigating a service provider to host your identity management environment:

1. Always be sure to inquire about the service level agreements (SLAs) that will be put into place. SLAs can make or break a hosted offering, so be aware that the SLAs directly support your institution's goals and objectives.
2. Fully explore the liability ramifications of outsourcing your identity management operations. How will this affect your compliance regulations and requirements? Do you or your vendor have any compliance or measuring tools available to mitigate any noncompliance issues? Will the vendor provide periodic compliance reports or scorecards?
3. Think about how much control you really want regarding how the service should be implemented. Will you define all the requirements, or will your customers be involved as well? How many of these decisions do you wish to be in the hands of the actual service provider?
4. Carefully plan and define exactly how you will interface with the service provider. Define integration points and standards between you, the service provider, and any third parties, as well as determining how internal administrators will control and monitor those access points. Make sure the vendor has a high privilege account management feature to achieve this type of fine-grained administrative access.
5. Consider what applications you will wish to integrate into the solution. Will this only involve web-based applications, or will mainframe and web services also be incorporated?
6. Security is a huge concern for most companies when it comes to any outsourcing endeavor. Make sure your security model is fully defined and that the service provider can abide by all the requirements in that security model. Find out what policies the provider has in place for controlling access to systems containing client data. Also find out what their best practices are for screening and hiring employees. As many service providers run a multi-tenant software infrastructure within their data centers, be sure to find out what safeguards will be put in place to protect you from other tenants.
7. Be sure to clearly understand how much business disruption might arise from this service. Make sure your provider is using a software solution that can be fully configured and tested outside of a production environment, so applications won't have to be taken offline, and can be remotely deployed to keep service levels intact. Clearly define who will assume risk if there are availability or performance issues.
8. Fully explore just how viable it would be to take the solution in-house eventually. Does the technology support an easy transition, should the need arise?

9. Does the vendor have a solid and qualified history with identity management deployments? This is a question relevant to both your initial deployment and any future shifts to an in-house framework

10. And don't forget the age-old question, "How much is this going to cost me?" Hosted identity management is a subscription-based service, but find out if it is going to be user-based, usage-based or a flat rate. Also inquire how often you will be billed and if there are any extra costs for implementation and/or customizations.

If all of these issues are addressed and fully evaluated by both you and your service provider, identity management as a service can be leveraged to deliver a low-cost solution with high ROI and automated business and IT services for your entire enterprise.

Stephanie Hagopian is the director of business development in NetworkingPS' Security Management Services Practice. Visit www.networkingps.com for more information.