

Symplified Expands Its Cloud Identity Vision with Sync, Virtual Directory and Identity Vault

Abstract

On July 28, 2010, Boulder, Colorado-based Symplified, an innovator in solutions for easing the adoption of cloud computing and hosted resources through more seamless integration with an organization's existing approach to identity management, announced three new capabilities for managing and synchronizing user identities regardless whether they reside in on-premise resources or with a cloud computing or hosted technology provider. Symplified Sync extends the use of Microsoft Active Directory to cloud and hosted environments. SinglePoint Virtual Directory enables user data normalization, transformation, attribute mapping and support for a wide range of LDAP and RDB data stores and identity federation endpoints between businesses and their cloud computing or hosted service providers. Symplified Identity Vault provides a cloud-based directory service that enables businesses to securely use their hosted or cloud services as user directories.

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts see these new capabilities as part of an expansive vision for identity management in and for cloud-based resources that distinguishes Symplified as an early leader in the emerging and vital field of security for cloud computing, making tangible strides toward defining security for the cloud when many others simply talk about it.

Background and Context

The concept of cloud computing has taken the IT world by storm in the last few years. The emergence of technologies such as virtualization that enable effective resource consolidation and abstraction, and Web Services that support highly flexible resource integration, have together combined to transform long-standing models of hosted services into something much more responsive to the needs of businesses of all sizes. Large enterprises gain immediate access to an ideal complement of infrastructure, modular application services, or fully complete hosted applications as SaaS (“Software as a Service”) without having to fight seemingly endless battles against the burdens of legacy systems, or making high-risk investments in products and their long-term maintenance. Small businesses, meanwhile, gain immediate access to a level of technology and technology integration that is often simply beyond their grasp. All this comes with a measure of support provided on an ongoing basis by the service provider. For the price of a subscription, businesses are relieved of many of the most onerous aspects—and costs—of IT support.

But there is one factor above all others that gives organizations pause when considering the cloud or hosted alternatives. That factor is security. Finding after finding makes clear that security and its many implications are top issues that must be resolved before cloud computing will become widely penetrated. In the 2010 EMA Research Report, *The Responsible Cloud*,¹ security, risk and compliance management was the top decision factor in choosing a cloud computing technology or provider. At 54% of all respondents surveyed, this was the most frequently mentioned factor by far, 12% of the next most significant concern (performance and manageability), and the *only* decision factor cited by a majority.

In EMA's 2010 Research Report, *The Responsible Cloud*, security, risk and compliance management was the top decision factor in choosing a cloud computing technology or provider.

¹ EMA Research Report, *The Responsible Cloud*, January 2010, available at <http://www.enterprisemanagement.com/research/asset.php?id=1652>

A number of initiatives have arisen to address this lynchpin concern, but in some cases, the bulk of outcomes have mostly been more talk about the lack of security for cloud computing and what should be done, rather than what *can* be done.

Symplified, however, has not sat idly on the sidelines of this discussion. As one of the first pure plays to recognize the need for an identity foundation for cloud security, Symplified differentiated early with an actionable way to extend single-sign-on to hosted services that did not depend on a service provider's pre-existing support for a specific approach to identity integration. Rather, it introduced a readily adopted hosted identity service that provided the linkage with service providers, in concert with an on-premises appliance, the Symplified Identity Router, when needed to interface safely with the customer's identity resources.

This strategy enables organizations to safely link internal identity management with popular hosted services such as Salesforce.com, Google Apps, and ADP personnel management services with minimal impact. The approach has been particularly popular with organizations who want to extend single-sign-on to cloud and hosted services, but who (understandably) fear the risk of taking on overwhelming costs or burdens of identity management deployments that often challenge even the most capable enterprises.

The Symplified strategy is predicated on becoming the foundation of trusted resources that link the enterprise with its cloud computing assets and hosted service providers, and to that end, the company has embraced an expansive vision of the kind of "identity fabric" that foundation entails. This has led to the next logical and expected steps after integrated single-sign-on as a primary essential—identity resource integration and the introduction of user management. Single-sign-on takes advantage of identities that already exist in a given resource such as a directory. Identity integration breaks down silos that isolate identity resources, while user management addresses the lifecycle of user account creation and provisioning, modification, termination and synchronization across multiple resources.

Event

With the introduction of Symplified Sync, the SinglePoint Virtual Directory, and the Symplified Identity Vault, Symplified advances into three areas of identity integration between the enterprise and the cloud that will be of immediate value in extending the capabilities of single-sign-on across cloud and hosted environments, and which lay a foundation for further innovation to come:

- **Synchronizing Active Directory user management with the cloud: Symplified Sync** – Microsoft's Active Directory (AD) is one of the most common internal resources for unifying identity management within organizations of all sizes. The ability to extend its usefulness to cloud environments was an early advantage of single-sign-on solutions for cloud and hosted services. But without the ability to synchronize user account attributes, changes or terminations, its usefulness is limited.

With the introduction of Symplified Sync, Symplified now embraces these aspects of ongoing Active Directory user maintenance. When user accounts are created, modified or terminated in AD, Symplified Sync propagates those changes to its supported service providers automatically and transparently. Symplified Sync also allows AD attributes to be mapped to those of the target resource at the cloud or hosted provider, which improves the consistency of identity policy management across both internal and external cloud or hosted resources.

With the introduction of Symplified Sync, the SinglePoint Virtual Directory, and the Symplified Identity Vault, Symplified advances into three areas of identity integration between the enterprise and the cloud that will be of immediate value, and which lay a foundation for further innovation to come.

Initially, Symplified Sync will support Google and Salesforce.com, with additional cloud services to be added over time.

- **Harmonizing identity resources across the enterprise and the cloud: SinglePoint Virtual Directory** – Regardless whether on premises or at the hosted or cloud provider, the integration of identities across various disparate resources such as LDAP directories and relationship databases (RDBs) often challenges identity deployments. Different identity stores function differently, and may store attributes in dissimilar ways. Virtual directory technology is one way to overcome these technology silos and unify identity and policy management between identity stores.

Recognizing the value of this technology in linking enterprise identity with the cloud and hosted services, Symplified has introduced the SinglePoint Virtual Directory, providing normalization, data transformation and attribute mapping across a wide range of LDAP and RDB services as well as cloud-based resources. This eliminates the often schema-breaking need to consolidate directory systems into a single architecture, or to write custom code just for integrating identities between specific applications. It also allows for greater consistency in policy management, regardless whether via Active Directory for internal personnel, an LDAP directory for partners of Web applications, or Salesforce.com for customers.

- **Security for cloud-based identity stores: Symplified Identity Vault** – Symplified also recognizes that there are three cases in which an organization would prefer to manage a user identity store such as a directory in a cloud or hosted environment: organizations that rely primarily on cloud-based applications, those who lack an on-premises directory infrastructure, and those who are migrating identity management to a cloud environment or service provider. In each case, Symplified offers the Symplified Identity Vault as a way to leverage hosted identity resources such as Salesforce.com and Google as their identity store.

Essentially, the Symplified Identity Vault sits between the customer's applications and Salesforce.com or Google, enabling organizations to use these highly available resources as user directories. This helps eliminate "directory sprawl" that multiplies management burdens by requiring organizations to build out new directory structures—and their management burdens—just to support new applications or portals for partners or customers.

EMA Perspective

With the introduction of these three new capabilities, Symplified begins to stake out the components of a comprehensive identity fabric for cloud computing and hosted resources. With Symplified Sync, Symplified further extends Active Directory to hosted, cloud or third-party environments through synchronization that helps keep identity and access policies current. With SinglePoint Virtual Directory, Symplified eases the integration of disparate identity stores and a more seamless extension of identity to the cloud. Perhaps most provocative of the three in the near term is the Identity Vault, which turns the focus in the opposite direction, toward organizations that would prefer to extend service provider identity resources into the enterprise and beyond, for multiple use cases. This follows Symplified's announcement of Symplified Trust Cloud for Amazon EC2 this past May, and suggests the outlines of hosted identity management in the future.

These new capabilities open the door to Symplified's further investment in user management, and an anticipation of the company's wider scope of provisioning and account lifecycle management harmonized with both cloud-based and legacy identity resources that seem sure to come—capabilities that will be anxiously awaited by Symplified customers and IT-as-a-service providers alike.

These capabilities highlight the level of investment Symplified is willing to make in a comprehensive approach to unifying identity in the cloud with identity in the enterprise—and more. What is often overlooked in the discussion of cloud security is its critical foundation—identity. Organizations voice high concern over the safety of confidential data in the cloud, but what is that safety based on? Simply put, it is the ability to distinguish authorized from unauthorized access to sensitive information at the heart of the issue, and this fundamental depends directly on identity.

The unification of identity offers substantial promise for simplifying security policy management, making it more consistent as well as more effective across multiple resources. By recognizing this fact, and maintaining its competitive edge with offerings that widen the scope of identity unified across the enterprise and its cloud computing resources, Symplified backs its audacious slogan of “the cloud security company” and carries the fight into a level of action that many still only talk about.

Organizations voice high concern over the safety of confidential data in the cloud—but what is that safety based on? Simply put, it is the ability to distinguish authorized from unauthorized access to sensitive information at the heart of the issue—and this fundamental depends directly on identity.

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter (http://twitter.com/ema_research).

2137.081210