Secure Cloud Applications Without Disrupting Your Enterprise Identity Infrastructure

Deliver a Federated Identity Service Based on Virtualization for Single Sign-On Across Your Enterprise and Cloud Applications

More companies are moving to the Software-as-a-Service (SaaS) model, taking advantage of specialized new services without the cost and hassle of developing or managing them in-house. But securing these applications is another story. While the cloud is expanding enterprise capabilities, it's also putting a strain on your existing identity infrastructure. When your business adds cloud-based applications into the mix, what was already a tough job—**separating identity and access management from the applications themselves**—becomes even harder.

According to Gartner analyst Gregg Kreizman in his paper, *Enterprise Options for Federated Single Sign-On to the Cloud:* "Gartner inquiry data and search analytics show clear trends that **mobility and cloud computing are stretching and breaking traditional IAM processes and infrastructure**. The same IAM functions are needed for the cloud; however, they are just not readily available as mature, abstracted or brokered services."

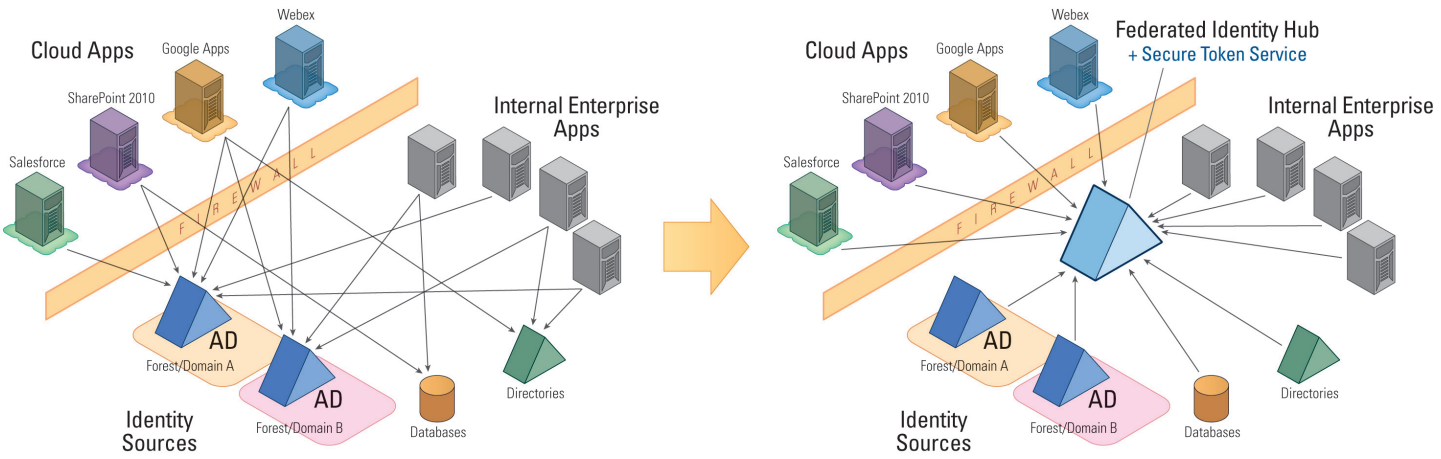
If you were starting from zero, hosting your identity in the cloud would be easy. But most companies have heavy investments in Active Directory, along with a variety of disparate data sources and legacy applications. While cloud-hosted identity services might be a great option for greenfield deployments, **pushing an already-complicated infrastructure to the cloud can be a security and synchronization nightmare**.

Today's companies face a difficult decision: whether to disrupt their current system and start fresh on the cloud, or find a way to **evolve and extend existing identity infrastructures to meet new challenges, today and in the future**. None of these challenges are new—they're the main drivers toward a better, common identity service. Such a service is already essential for securing internal applications, and new cloud-based applications only add more urgency and greater value.

The Challenge: Adding Cloud Applications To Your IAM Infrastructure is Difficult

For most enterprises, the cloud deepens a number of existing challenges. Even if you're only dealing with internal applications, **you need to secure a complex heterogeneous environment with multiple identity sources and applications**. To achieve this, you must manage the multitude of different authentication/authorization methods and requirements that are part of such a disparate environment. And finally, you have to keep your user data up to date—even when it's spread across systems and into the cloud. Given today's complicated enterprise identity landscape, how can you:

- Provide simple, secure and user-friendly access to cloud-based applications?
- Administer appropriate security policy when password protocols and authorization requirements differ for every application?
- Ensure that data is up to date everywhere—and that your picture of each user is complete, no matter where attributes are stored?



Without a federated identity service, authenticating users across different silos and applications can be chaotic

A federated identity service creates a local identity hub for authentication, authorization, and profile management

Authenticating and Authorizing Across Fragmented Identity Silos

SaaS vendors are specialists in delivering a given service, whether that's CRM, payroll, or some other cloud-based tool, but when it comes to access and identity management, they provide a relatively generic interface that cannot take into account the intricacies of your current system. **While many SaaS vendors claim that it's easy to integrate their products with your enterprise identity infrastructure, that's not the whole story**. In fact, they grapple with the same challenges you face with securing internal applications, including the need to integrate identities from across a variety of disparate sources.

First, you have to **go the "last mile" into disparate enterprise endpoints to authenticate users and collect identity information for authorization**. For most companies, this is tough enough within the enterprise itself, with its heterogeneous mix of existing identity and authentication silos, including multiple AD domains and forests, other LDAP directories, databases, and applications. Adding access to cloud-based apps only increases the complexity.

Taming the Tangle of Security Means, Credentials, and Protocols

Once you've gone into your silos, you have to **transform the proprietary security means generated by your existing infrastructure** into a vendor-appropriate industry standard format and deliver it to the cloud-based application. However, **these applications might use one of many different methods of authentication**, such as name/password or federation/token.

Even when cloud apps support more modern standards, such as SAML & WS-Federation, adding cloud-based applications still creates an identity challenge. For example, **SAML-based security tokens come in many vendor-specific flavors** and each application has very specific expectations of what the payload contains and how it will be formatted. Even if a user could be authenticated by a local security source, you must map the data from the format of the internal user profile to the specific attributes of the security token expected by a given Saas application/service.

Keeping User Profiles in Sync When They Exist in Many Places

This challenge does not stop at the authentication layer. In many cases, you must also **create identity profiles of all users within the cloud-based application itself, and keep those profiles synchronized with the authoritative sources** within your enterprise. And finally, to provide specific services based on your users and their activities and relationships, you must pull relevant SaaS-specific context from the cloud-based profiles and reflect that information within your internal systems.

None of this is easy, as many enterprises are learning. In fact, cloud-based applications take the usual hassle of authentication, authorization, and profile management across disparate systems, and add an additional layer of complexity—or ten. So **how can you ensure security and deliver the experience your users expect across your enterprise and in the cloud?**

The Solution: One Virtual Identity Service to Unify Your Entire Identity Infrastructure

What you need is a way to **federate your identity, delivering a single point of access for all your applications**, no matter what they do or where they're located. RadiantOne virtualization delivers **identity as a complete, on-premise service**, giving you a local identity hub for all your applications, whether they're enterprise, web-based, or in the cloud. With an identity service, cloud applications can authenticate users against the authoritative sources within your organization—and your **essential identity data doesn't have to cross the firewall** every time you synchronize user accounts. RadiantOne gives you all the tools you need to federate identity and **achieve SSO with your SaaS apps**—all without having to reinvent your infrastructure.

A Common Point of Access for All Your Applications

With RadiantOne, you can overcome the primary challenges of identity and access management for the cloud. **A virtualized identity service shields cloud-based applications from the complexity of your backend sources**. Such an identity service enables you to create custom views of data that span enterprise and SaaS systems, and deliver data via different protocols based on the application's requirements.

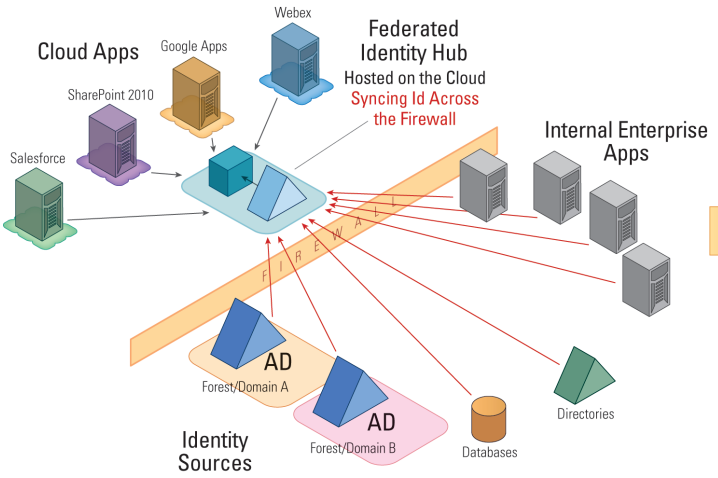
Through a virtual abstraction layer, RadiantOne brings together identity and context information from your cloud-based and physical sources, enabling **a global view of your customers, partners, and employees**. No matter what the model, such a federated identity hub is essential to securing the cloud. While creating a single point of access is the main challenge in securing your SaaS applications, you must also consider the location of such a hub: either in the cloud or on-premise. Where to host this infrastructure depends the needs—and demands—of your current installation.

Disrupt or Evolve? Why an On-Premise Solution Provides a Better Foundation

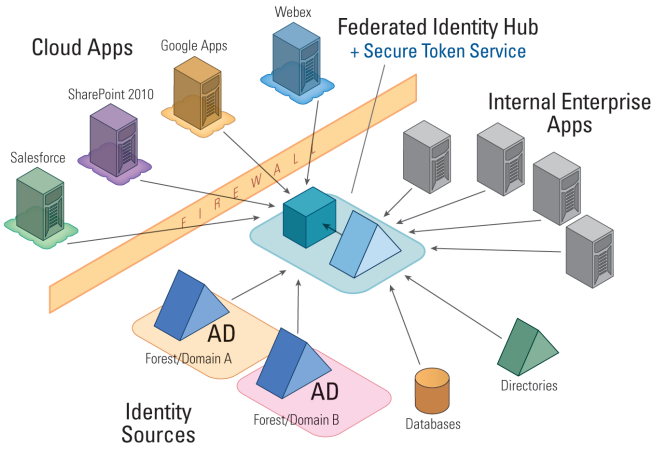
If you're starting from scratch with **a greenfield deployment, it makes sense for identity to be hosted in the cloud**—basically, you're securing your SaaS applications using another cloud-based service that's contracted out to a third-party vendor. And if you're a smaller organization looking to authenticate against your Active Directory employee base, then federating locally using ADFS (Active Directory Federation Service) might be the best choice—after all, it's built right in to the system, so it's cheap and designed to work with your AD.

However, most larger enterprises have a complex infrastructure with identities spread across many heterogeneous sources, along with a multitude of legacy applications that rely on those sources. For those organizations, **a move to cloud-based identity would be extremely disruptive**, and cannot be undertaken without some intermediate identity federation steps.

An approach such as ADFS could be a first step, but unfortunately, ADFS only enables access for a subset of your users—those stored in Active Directory. **You need a more complete solution: an identity service based on virtualization** which can integrate diverse data sources and security protocols, covering the different user populations—such as employees, customers, and partners—which need authentication and authorization.



For enterprises with established infrastructures, hosting identity in the cloud can be disruptive and less secure, since identity must be synced across the firewall



With an on-premise identity hub from RadiantOne, companies can evolve their identity infrastructures for the cloud—without risking the security of their information

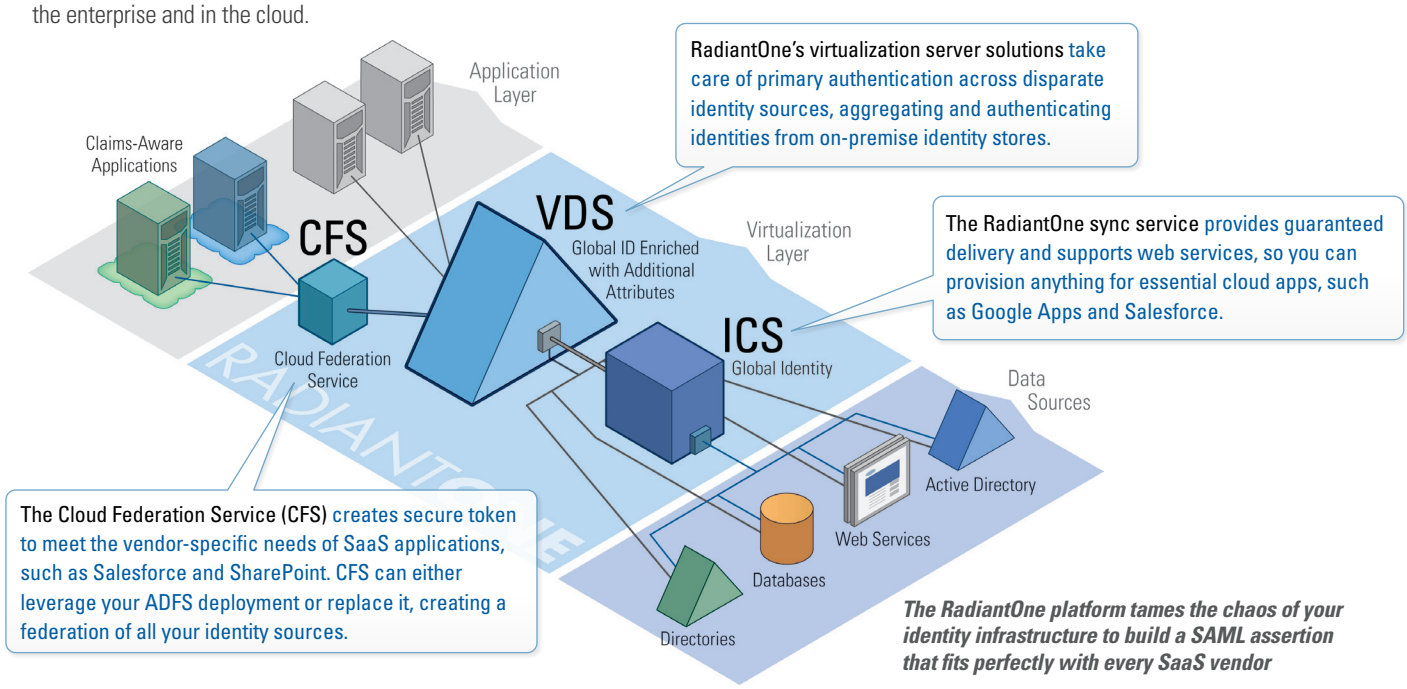
A Complete Identity Service—with the Future Built in

If you're a larger organization with heavy user volumes and complex, entrenched systems, it's essential to establish **a flexible infrastructure that solves your internal challenges and lets you evolve your identity to encompass the cloud**. While a move to cloud-based identity may be part of your long-term identity strategy, beginning with an on-premise deployment is safer and easier for the current needs of most enterprises. Virtualizing and federating your identity allows you to **deploy a fully secure solution behind the firewall, while preserving a path to the cloud**, should you decide to move your identity toward a hosted model over time. Such a solution gives you stability and flexibility, so you can secure any applications you want today—no matter where they're based—and grow into new paradigms and architectures as they emerge.

Go beyond a narrow SaaS security point solution that simply pushes your identity fragmentation to the cloud. Deliver a complete, federated identity service that allows your identity infrastructure to respond easily to changing requirements, whether that means adding new data sources or applications, expanding your user populations after a merger or acquisition, or **extending your identity securely to take advantage of the cloud**.

The RadiantOne Platform in Action

RadiantOne has all the tools you need to deliver a single point of access for cloud applications, support federated single sign-on, and unify identity across the enterprise and in the cloud.



The RadiantOne platform tames the chaos of your identity infrastructure to build a SAML assertion that fits perfectly with every SaaS vendor

The Benefits of RadiantOne for Cloud-Based Infrastructures:

- **On-premise solution:** RadiantOne virtualization federates your identity and delivers it as an on-premise service, giving you a local identity hub for all your applications, whether they're in the enterprise, on the web, or in the cloud.
- **Authentication across AD domains and forests:** One logical, transparent way to integrate Active Directory, without having to manage multiple trust relationships. RadiantOne can either work with your existing ADFS infrastructure or replace it entirely.
- **Easier SSO across all sources:** Give your SaaS applications a single source for identity data—without building customized connections to multiple AD domains/forests, LDAP directories, databases, or applications.
- **Better user experience:** With single sign-on, your users can sign in once, then access applications across the enterprise or in the cloud.
- **Enhanced security and authentication:** Credential checking stays local, so passwords/credentials are not sent over the Internet and any needed synchronization is reduced.
- **Smarter, finer-grained authorization:** RadiantOne makes it easy to create dynamic groups based on attributes, and populate these groups with users coming from multiple sources.
- **Intelligent administration and audit:** Manage identity globally, across all your identity sources, while delegating credential checking to the local level.
- **A more flexible, scalable system:** With RadiantOne virtualization, you can add new user stores to your infrastructure without disrupting the existing system.
- **Simpler synchronization:** Keep all your sources current when needed, with transparent and automated sync services, featuring real-time event detection and a message queue for guaranteed delivery.