How a Federated Identity Service Turns Identity into a Business Enabler, Not an IT Bottleneck

Add Agility, Flexibility, and Responsiveness into Your Enterprise

Delivering Identity the Way Your Business Demands It

Business is all about adaption and change, so being able to easily reorganize people, processes, and resources is essential to productivity and growth. **More agile identity management is the key ingredient for the success of your initiatives, from the tactical to the strategic level**. Whether you're adding a business unit, taking advantage of a cloud application, or orchestrating a billion-dollar merger, an agile identity management system is purpose-built to dispatch the right people to the right applications with the adequate privileges, while guaranteeing secure access.

However, actually implementing these changes can mean a host of customization pains, stalled projects, and lost opportunities. In a world of fragmented and distributed identity silos, most identity deployments lead to increased project costs, higher risks, and redundant efforts. **Reorganizing, assigning, or reassigning secure access to resources must be done at the speed of your business**—not at a stop-and-go pace hindered by ad-hoc and homemade tinkering.

No matter your initiative—extending secure access to newly deployed applications, expanding to the cloud, or reorganizing business units to integrate new populations—each has direct impacts on the identity infrastructure. Depending on your approach, your identity system **can represent a major business bottleneck** —or, with the right tools, it can help to **accelerate the growth in your organization, add in needed agility, and bring new objectives and services within reach**.

Why do You Need it? Business Drivers Behind an Identity Integration Layer

Integrating for Tactical and Strategic Enterprise Initiatives

Every physical change in your enterprise has a counterpart in the identity world. Whether a tactical or a strategic move, leveraging existing identity systems to support a change in your business is often necessary. For example, after an acquisition, you have an entirely new workforce, organization, and set of applications that need to be absorbed into an existing system. You need to be able to give new populations the autonomy to continue to work productively, while integrating them into your system and extending access to crucial services. However, decentralized and fragmented infrastructures significantly impede large-scale integrations. Without a common source of identity and group information, incorporating or reorganizing populations is costly, time-consuming, and requires extensive customization.

Supporting New Application Demands and Cloud Opportunities

The rise of the new—new business initiatives, new applications, and new delivery mechanisms, such as the cloud—is putting stress on already overtaxed identity infrastructures. New applications require potentially different user population subsets, different attributes, and a different structure than what your current identity infrastructure can deliver. Applications typically require a single source containing all relevant information about users accessing the application, in their expected format. However, in a distributed environment, this data source typically does not already exist, so deploying a new application means that a project is delayed, or goes way over budget. As many identity systems currently stand, it is often simply too expensive to reach new partners and channels. You want flexibility to execute new projects as they arise—without unexpected delays or costs due to the fragmented identity system.

Defending Against Increased Security Threats

An increasing threat landscape makes securing your environment even more business-critical. Identity is the true foundation of security—before you can grant someone access to something, you need to know who they are, and that their access is warranted. Before you can even think about SSO, security tokens, and federation, you first need a functional system for authenticating and authorizing users—and this is increasingly difficult to deliver in today's fragmented identity infrastructures.

You need a solid foundation on which all other security means can rely, one which offers additional information about each user's roles, access rights, location, or other pertinent information.

Keeping Growing Maintenance Costs in Check

Huge maintenance costs are dominating IT budgets. Supporting and maintaining a distributed environment is costly in terms of time and resources, thanks to a multitude of complexities. With each identity store comes the need to provision access, reset passwords, synchronize accounts, and potentially set up single sign-on. In many cases, simple tasks like setting up user accounts in Active Directory take weeks or even months. The cost and time associating with maintaining redundant and legacy identity stores is a roadblock between you and new identity initiatives.

Enabling Better Governance and Data Quality

Increased regulation and compliance drives the need for better governance and data quality. For reporting, for business intelligence, or especially if you face a security breach, you need to know who accessed what and when—but how do you that when you have a myriad of identity sources and authentication silos, including Active Directory domains and forests, databases, LDAP, or legacy mainframes? Plus, the possibility of duplicate user accounts means that your infrastructure has incomplete and potentially inaccurate data about users. As if that's not enough, defining and enforcing permissions across sources with different policies is also a challenge within a distributed environment. This structure limits your ability to audit. What you need is not necessarily a physically centralized system, but rather a logical, central view of users and administrative activities across all data sources, so you can see what actions, on which sources, everyone is performing, and present that data to business intelligence tools for analysis. When you have a logical access and management point, it makes it easy to see if you're not in compliance, so that you can better govern your identity data—and skirt any compliance issues.

Fragmented Identity Means Delivery Bottlenecks, Lost Opportunities, and Ever Increasing Costs

No matter what your strategy, the success and adaptability of your business relies on the ability to reorganize, people, processes, and resources. Unfortunately, for multiple reasons, the reality of your identity infrastructure is a fragmented, distributed, heterogeneous system, rife with silos. Most of today's infrastructures are the result of many mutually-incompatible identity systems and directories, cobbled together over a period of years. This led to an explosion of identities, stored in proprietary applications, with no standardized naming system. As a result, the business objectives we looked at earlier are out of reach due to these challenges:

- A distributed, fragmented infrastructure impedes the ability to integrate systems for authentication and authorization purposes.
- Inconsistent and redundant or contradictory user data means you can't identify a user across systems—much less deliver single sign-on.
- Lack of a comprehensive identity view means extensive customization and a potential increase in security vulnerabilities.
- Significant people and financial resources required to support and maintain decentralized, fragmented, and inconsistent large-scale directories with multiple licensing and maintenance fees.

A fragmented infrastructure means considerable financial impacts for your business:

Impact	Financial Impact
Increased deployment time for new applications and population integrations.	▲ Lost Revenue x Number of Days Delay ▲ Employee Hours to Manage Multiple Applications
Project halts due to failed integration effort and missed deadlines.	▲ Lost Revenue x Number of Days Delay ▲ Opportunity Costs
Increased user setup time or postponing new projects.	▲ Lost Revenue x Number of Days Postponed ▲ Employee Hours to Set Up Account x Number of New or Migrated Accounts
High support and maintenance costs due to redundant identity stores.	▲ Separate support teams to manage each identity store
Duplicate user accounts in various systems.	▲ Increasing license costs ▲ Increased administrative hours

Without planning and support from an identity framework, overcoming these challenges within today's fragmented infrastructures can be a never-ending effort of costly and brittle point-to-point integration efforts.

Federated Identity Service: An Identity Integration Spectrum to Meet Evolving Demands

There's a better way—you can **reflect changes in your physical world through a virtualization layer.** A federated identity service based on virtualization is capable of injecting this level of flexibility into your existing identity infrastructure. It is an integration layer that gives you a central access and management point for all identities, no matter how or where they are stored, enabling quick and easy redistribution of users. Identities can be **added, moved, or changed** without impacting users or applications, and at the speed of your business, instead of slowing initiatives through the **sunk cost of ad-hoc custom coding**.

Objectives	Goals	Required Platform Capabilities
Smoother integration and acquisition.	Help simplify user profile issues related to the decentralized and fragmented identity environment.	▲ Create multiple, customizable data views. ▲ Resolve duplicate identities. ▲ Integrate with various data sources, including directories, databases, and web-based applications.
Decreased support and maintenance requirements.	Integrate with existing applications.	▲ Integrate with application for authentication and authorization. ▲ Expose various types of interfaces (e.g. LDAP, ODBC, JDBC, etc.).
Improved governance.	Align with current technology standards.	▲ Migrate from one environment to another. ▲ Support a common and scalable architecture, yielding traceable events.
Leverage existing infrastructure.	Facilitate identity source consolidation with new and existing sources.	▲ Migrate users without impacting their application access. ▲ Allow applications to authenticate users from multiple directories.

No matter your business objective, a federated identity service enables you to save time, money, and hassle

A Flexible Integration Layer for an Incremental and Progressive Approach

No two identity deployments are the same. Different approaches are required for different integration efforts, depending on the objective, the scale, and the complexity of the initiative. More than a simple "point solution," a federated identity service is a complete platform that addresses the entire spectrum of integration needs—one that grows along with you as your business evolves and changes. It is the only solution that can take you all the way from lightweight identity aggregation to complete integration, with one global identity set.

1. Identity Aggregation for Lightweight, Proxy-based Integration

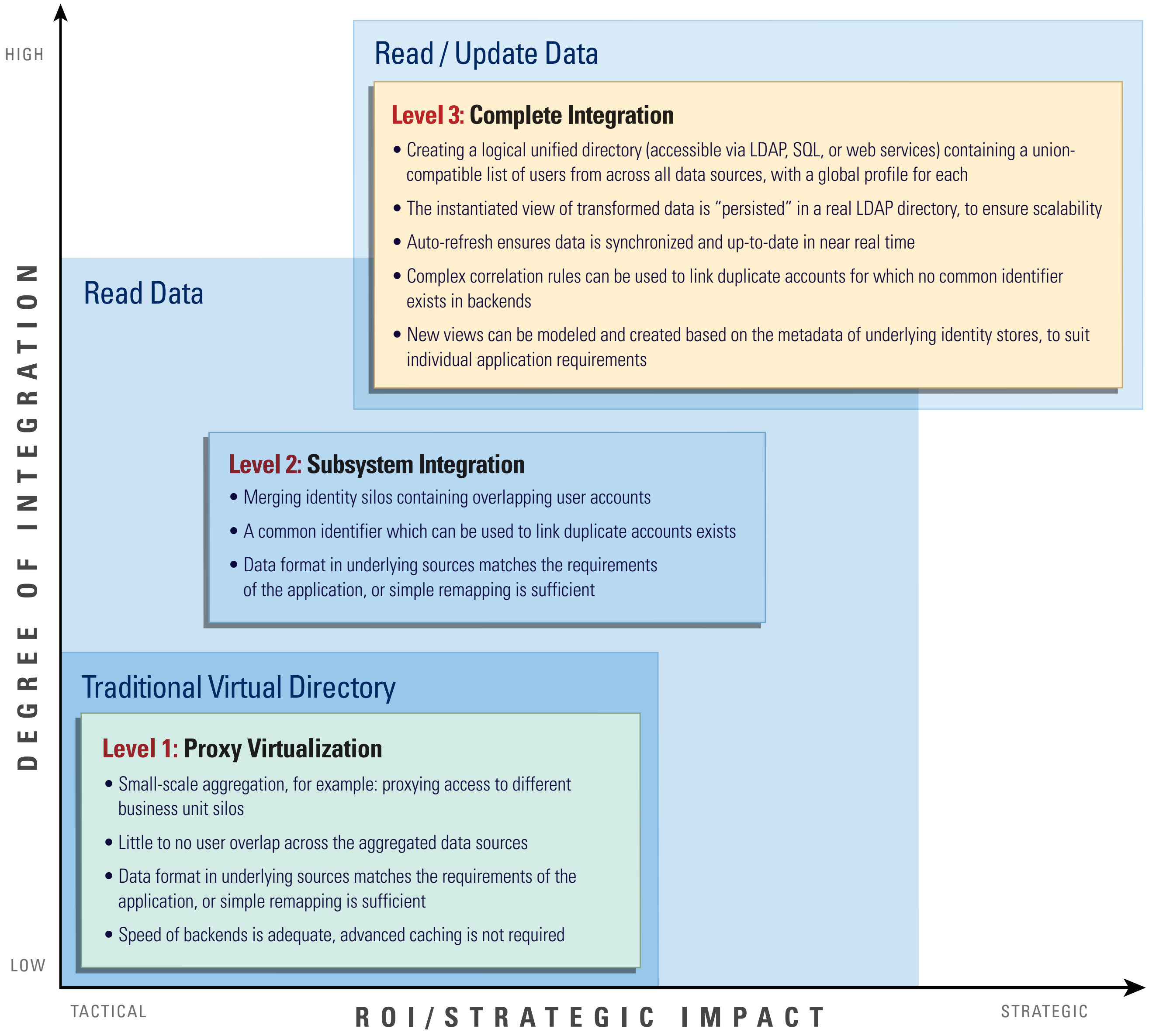
Multiple identity systems are regrouped within a common root, yet remain clearly separated. Each subsystem of identity is kept as-is, but a common "directory umbrella" regroups access, and a virtualization layer proxies security requests to the appropriate subsystem. The management of each subsystem remains unchanged.

2. Subsystem Integration

Difficulties can arise when duplicate user accounts for the same identity exist across subsystems. One common example for subsystem integration is the need to authenticate users across different Active Directory domains and forests. In order to present a single, complete view of each user to consuming applications, the integration layer needs to be able to link those overlapping accounts as if they belong to a global logical directory. Once the identities are disambiguated, flexible identity views can be built around the newly-defined hierarchy, without affecting the underlying directory hierarchy.

3. Complete Integration for a Fully Integrated, Absorbed System

To enable new services, you often need a complete list of identities from across many disparate sources—such as LDAP directories, Active Directories, SQL databases, and web services—presented in the format the service expects to see. This is typical of mergers and acquisitions, which insert new identity silos into an already fragmented identity infrastructure, while adding the requirement of granting secure access to new users. RadiantOne's unique ability to extract and understand the metadata from underlying repositories allows it to combine and re-model data endlessly, adapting your existing resources to suit new view requirements.



Read / Update Data

Level 3: Complete Integration

- Creating a logical unified directory (accessible via LDAP, SQL, or web services) containing a union-compatible list of users from across all data sources, with a global profile for each
- The instantiated view of transformed data is "persisted" in a real LDAP directory, to ensure scalability
- Auto-refresh ensures data is synchronized and up-to-date in near real time
- Complex correlation rules can be used to link duplicate accounts for which no common identifier exists in backends
- New views can be modeled and created based on the metadata of underlying identity stores, to suit individual application requirements

Read Data

Level 2: Subsystem Integration

- Merging identity silos containing overlapping user accounts
- A common identifier which can be used to link duplicate accounts exists
- Data format in underlying sources matches the requirements of the application, or simple remapping is sufficient

Traditional Virtual Directory

Level 1: Proxy Virtualization

- Small-scale aggregation, for example: proxying access to different business unit silos
- Little to no user overlap across the aggregated data sources
- Data format in underlying sources matches the requirements of the application, or simple remapping is sufficient
- Speed of backends is adequate, advanced caching is not required

Unlike traditional virtual directories, RadiantOne's Federated Identity Service can accommodate any level of identity integration and volume

The RadiantOne Federated Identity Service

While you have several choices in virtual directories, only Radiant Logic brings you the world's first complete federated identity service based on virtualization. The RadiantOne Federated Identity Service is an integration layer that gives you **a central access and management point for all identities,** no matter how or where they are stored, enabling **quick and easy redistribution of users on demand**.

By virtualizing and transforming disparate identity repositories, the RadiantOne Federated Identity Service abstracts the complexity out of your identity infrastructure to **present one complete, coherent image of your identity data to applications**. Now applications have a single source which they can access to use for authentication and authorization, and data can be changed in the backends without impacting users or applications. This means that reorganizing your infrastructure is as easy as *point-click-done*—**and suddenly identity is no longer a bottleneck, but a valuable tool to the business.**

Technical Advantages of a Federated Identity Service

Technical Features	Business Benefits
Remodel directory trees to a common namespace.	▲ Enables your users to be searched across systems, enabling cross-application and cross-domain **single sign-on** to quickly extend access to new user groups.
Virtualize groups and dynamically create new ones based on attributes from multiple systems.	▲ Identities immediately **gain access to resources—without a disruption in service** due to administrative bottlenecks.
Provide multiple views of identity information stored across existing systems in application-specific formats.	▲ **Avoid expensive and timely customization** to adjust ever changing application demand.
Build a global profile using attributes from multiple identity sources.	▲ Leverage attributes for **finer-grained authorization**, and build groups on the fly.
Safely expose true identities to external applications and partners through a secure virtual layer and standard federation protocols.	▲ **Take advantage of SaaS applications**, without the security risks of sharing credentials across the firewall.
Persistently cache views of your transformed data, and auto-refresh when changes occur.	▲ **Scale to millions of users** without hard-coded synchronization.

Business Benefits to Drive ROI:

- ▲ Reduce the need for expensive and time-consuming customization projects.
- ▲ Turn identity into a business enabler, not a business bottleneck, creating revenue by supporting more new initiatives.
- ▲ Develop inter-company and cross-company affinity across heterogeneous systems.
- ▲ Allow a single view of identity data in order to adhere to internal or external regulations governing identity data.
- ▲ Reduce the impact of changes on end users.
- ▲ Quickly give the right people access to the right resources without adding complexity for the user.
- ▲ Eliminate the need for your IT department to manage multiple directory systems from multiple vendors, all of which are providing similar services to the enterprise.

About Radiant Logic

Radiant Logic, Inc. is the market-leading provider of identity virtualization solutions. Since pioneering the first virtual directory, Radiant Logic has evolved its groundbreaking technology into a complete federated identity service, enabling Fortune 1000 companies to solve their toughest identity management challenges.

Using model-driven virtualization technology, the RadiantOne federated identity service builds customizable views from disparate data silos, streamlining authentication and authorization for identity management, context-driven applications, and cloud-based infrastructures.

Organizations in a wide range of sectors rely on RadiantOne to deliver quick ROI by reducing administrative effort, simplifying integration tasks, and enabling future identity and data management initiatives.

Contact Us

To find out more about Radiant Logic, please call us at **877.727.6442**, email **info@radiantlogic.com**,
or visit **www.radiantlogic.com**.