WHITE PAPER

Transform Identity from Roadblock to Business Enabler

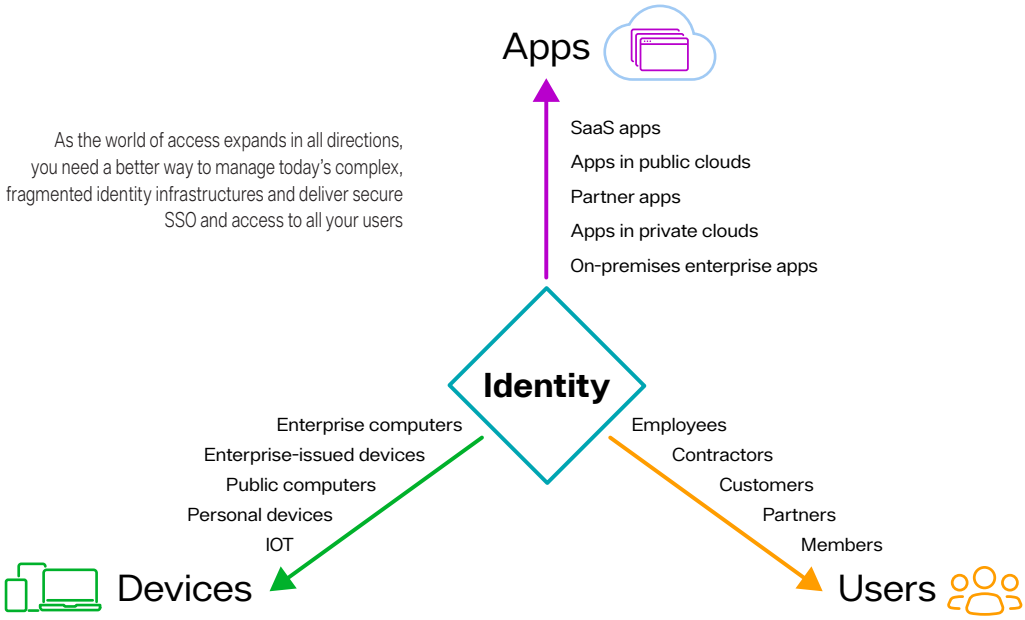
Delivering the Exact Version of Identity Your Security Demands

Business is all about adaptation and change, so being able to easily add or reorganize people, processes, and resources is essential to productivity, security, and growth. More agile identity management is the key ingredient for the success of all your initiatives, from the tactical to the strategic.

Whether you're adding a business unit, taking advantage of a cloud application, or orchestrating a billion-dollar merger, a flexible identity management system is purpose-built to dispatch the right people to the right applications with the appropriate 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 secure access to resources must be done at the speed of your business—not at the stop-and-go pace of ad-hoc tinkering.

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

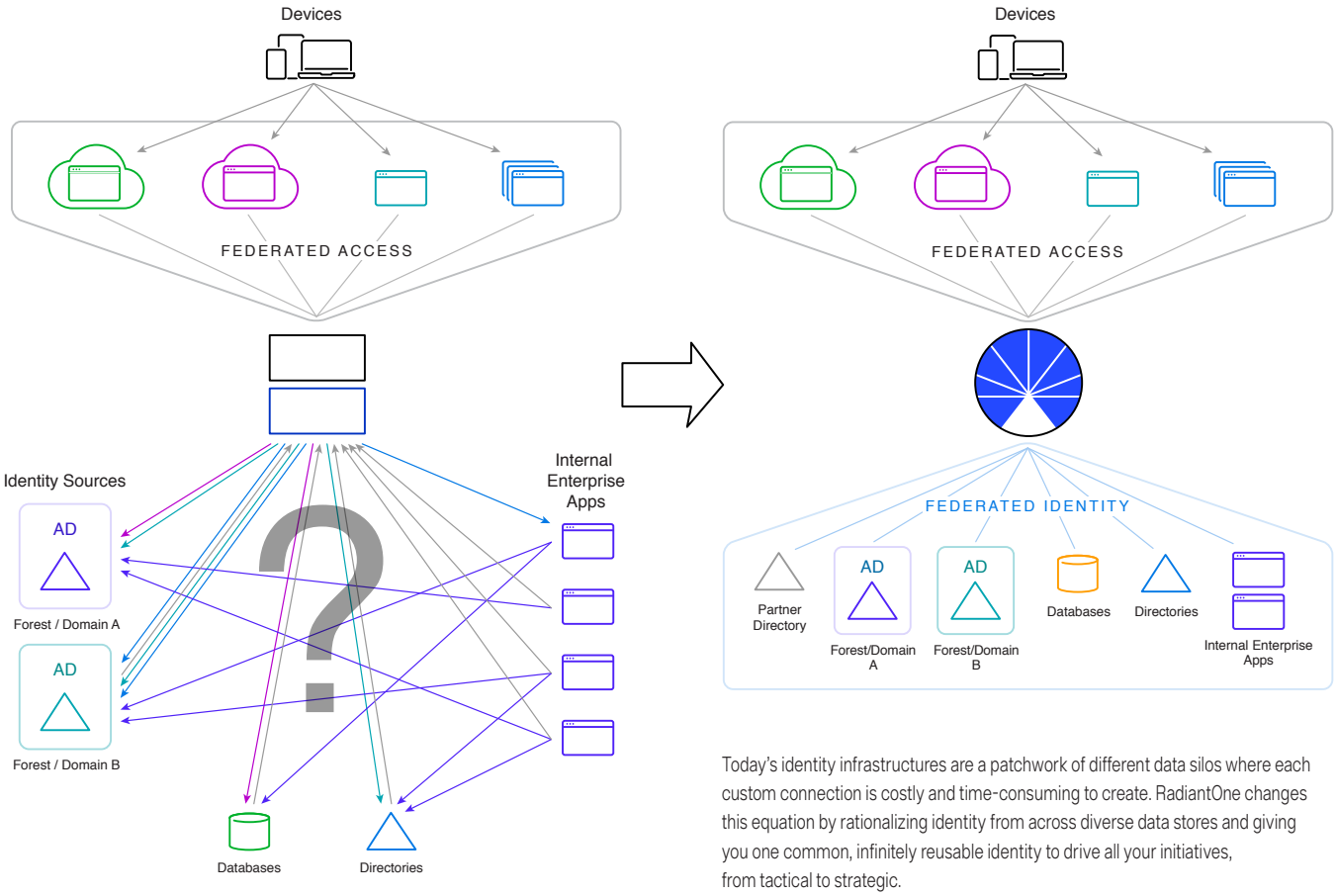


Business Drivers for Identity Enablement

New business initiatives, applications, and delivery mechanisms are putting stress on already overtaxed identity infrastructures. New applications often require additional user populations, different subsets of users, 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 its expected format. However, in a distributed environment, this rationalized data source typically does not already exist, so deploying a new application often means project delays or budget overruns. As many identity systems currently stand, it is often simply too expensive to reach new partners and channels. You need flexibility to execute new projects as they arise—without unexpected delays or costs due to the fragmented identity system.

Support Secure Access and SSO to Web and Cloud Applications

Securing access to an expanding portfolio of web and cloud applications is a top priority for most sizable organizations—after all, these applications help you do business better, and access alone is not enough if it's not secure. But how do you give users—from employees to partners and even customers—secure access and single sign-on, given the complexity of today's existing identity infrastructures? Whether you're trying to deliver traditional SSO for your web access management solution, or extend access and SSO to cloud applications, you need a way to reduce complexity with an integrated identity system.



Today's identity infrastructures are a patchwork of different data silos where each custom connection is costly and time-consuming to create. RadiantOne changes this equation by rationalizing identity from across diverse data stores and giving you one common, infinitely reusable identity to drive all your initiatives, from tactical to strategic.

Defend Against Increased Threats

An increasing threat landscape—including identity theft, hacker attacks, and malware—makes securing your environment even more business-critical. Identity is the true foundation of security; you can't grant or deny access without knowing who your users are, and whether their access is warranted. Before you can even think about SSO, security tokens, and federation, you must have 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. But many users have multiple accounts—and as many passwords to remember—making it difficult to figure out who's who, much less guarantee secure access.

Integrate Essential Enterprise Initiatives

Every physical change in your enterprise has a counterpart in the identity world. No matter the project, leveraging existing identity systems to support a change in your business is often necessary. 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 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.

Shrink Maintenance Costs

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 associated with maintaining redundant and legacy identity stores is a roadblock to delivering new identity-driven initiatives.

Enhance Governance and Data Quality

Increased regulation and compliance demands drives the need for better governance and data quality. For reporting, business intelligence, or security breaches, you need to know who accessed what and when—but how can you achieve this across a myriad of identity sources and authentication silos, including Active Directory domains and forests, databases, LDAP, APIs, and other legacy stores? The possibility of duplicate user accounts means that your infrastructure has incomplete and potentially inaccurate data about users. Defining and enforcing permissions across sources with different policies is also a challenge within a distributed environment. This structure limits your ability to audit.

With a logical, centralized view of users and administrative activities across all data sources, you can see what actions, on which sources, everyone is performing and present that data to business intelligence tools for analysis. Such a logical access and management point makes it easy to see when you're not in compliance, so you can better govern your identity data—and skirt any compliance issues.

Fragmented Identity =

- ✔ **Delivery Bottlenecks**
- ✔ **Lost Opportunities**
- ✔ **Spiraling Costs**

The success and adaptability of your business relies on the ability to reorganize people, processes, and resources. But 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 years. This led to an explosion of identities, stored in proprietary applications, with no standardized naming system. As a result, your business objectives are difficult to achieve quickly because:

- A distributed, fragmented infrastructure impedes the ability to integrate systems for authentication and authorization.
- Inconsistent, redundant, or contradictory user data means you can't identify a specific user across all systems—much less deliver single sign-on.
- Lack of a comprehensive identity view means extensive customization and a potential increase in security vulnerabilities.
- Significant human and financial resources are 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 to your budget:

Increased integration time for new applications and populations	• Lost revenue x number of days delay • Employee hours to manage multiple sign-ons to applications
Project stops or slowdowns due to failed integrations 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 x new or migrated accounts
High support/maintenance costs for redundant identity stores	• Separate support teams to manage each store • Increased license costs • Increased administrative hours

Without planning and support from a smart identity framework, overcoming these challenges can be a never-ending effort of costly and brittle point-to-point integrations.

An Identity Integration Spectrum to Meet Evolving Demands

There's a better way—you can reflect changes in your physical world through advanced identity virtualization. Our Intelligent Identity Data Platform based on virtualization is capable of injecting this level of flexibility into your existing identity infrastructure. Instead of slowing initiatives through the sunk cost of ad-hoc custom-coding, identities can be added, moved, or changed at the speed of your business without impacting users or applications.

The key to security lies in knowing exactly who your users are and what your organization knows about each one—even if that essential information is scattered across different data silos. RadiantOne strengthens your security by pulling together a comprehensive view of all your users with no duplications, and gathering additional information about those users' roles, access rights, location, or other pertinent information.

identify users, while RadiantOne manages credential checking across the disparate identity systems, using their individual access protocols and data formats.

This shields the consuming applications from the complexity of the backend—and your business from unwarranted access. And by joining each user's disparate duplicate accounts to each other, RadiantOne creates a global profile that can be used to feed fine-grained attribute-based authorization engines.

With RadiantOne, you can also flexibly define groups and memberships, making it easier to reshuffle access to services and functions. With this granular-level control, access is automatically altered when people change departments or leave the company, preventing security breaches by disgruntled ex-employees.

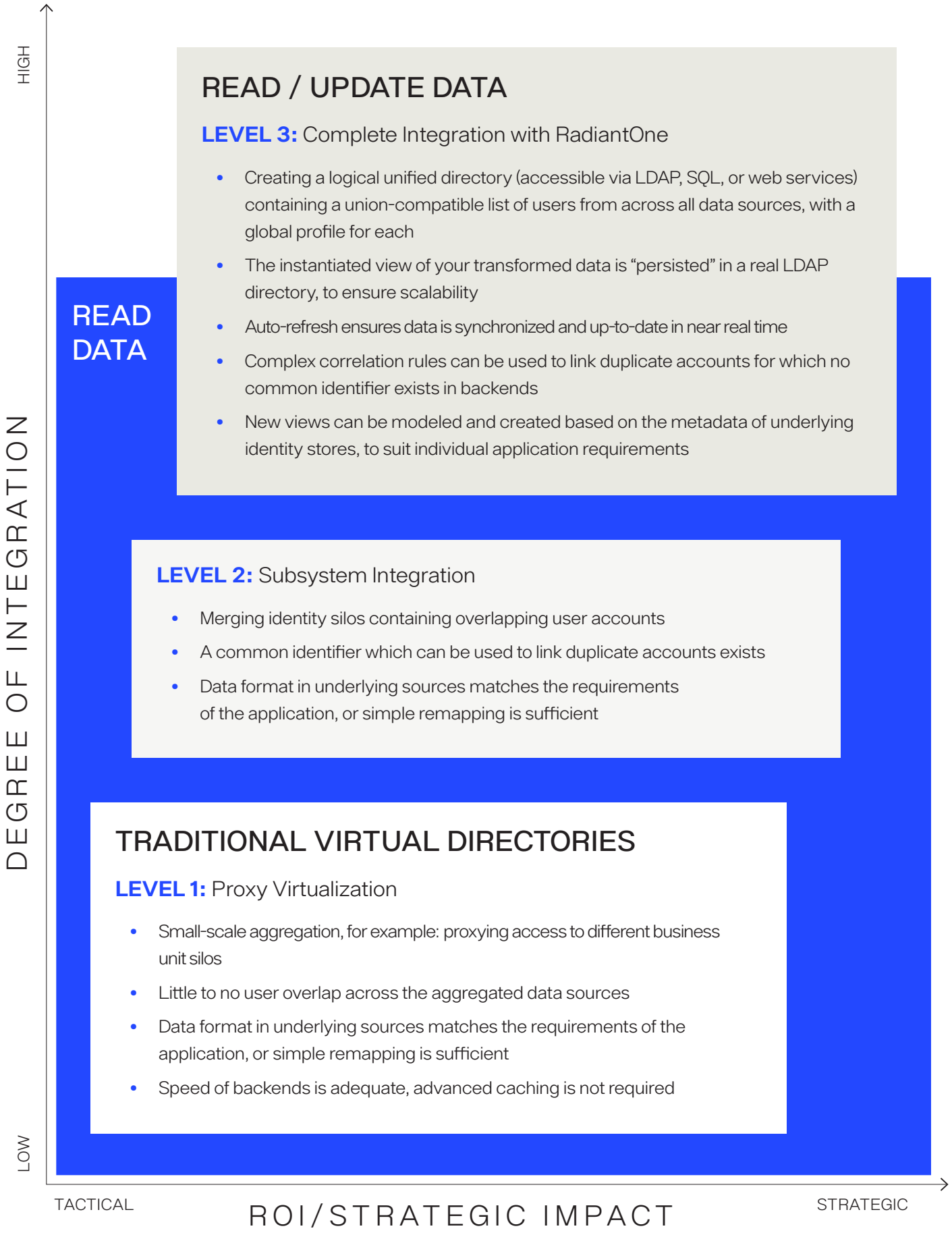
Objectives	Goals	Required Platform Capabilities
Smooth integration and acquisition	Help simplify user profile issues related to the decentralized and fragmented identity environment	• Integrate with application for authentication, SSO, and authorization • Create multiple, customizable data views for authorization • Resolve duplicate identities • Integrate identities from multiple directories, databases, and web-based applications
Decrease support and maintenance requirements	Integrate with existing applications	• Expose various types of interfaces (e.g. LDAP, ODBC, JDBC, etc.)
Improve 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, RadiantOne Saves You 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," RadiantOne 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 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 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.



Unlike traditional virtual directories, the RadiantOne Intelligent Identity Data Platform can accommodate any level of identity integration and volume.

RadiantOne Intelligent Identity Data Platform

Only Radiant Logic brings you the world's first complete intelligent identity data platform based on virtualization. RadiantOne 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, RadiantOne 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 they can access to use for authentication and authorization, and data can be changed in the backends stores without impacting users or applications. So 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 RadiantOne

Technical Features	Business Benefits
Remodel directory trees to a common namespace	Enable your users to be searched across systems, allowing 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 to ever-changing business demands
Build a global profile using attributes from multiple identity sources	Leverage attributes for finer-grained authorization, and build groups on the fly
Safely expose 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 hundreds of millions of users and queries without hard-coded synchronization

Drive ROI with RadiantOne Intelligent Identity Data Platform

- Reduce the need for expensive and time-consuming customization projects
- Turn identity into a project enabler, instead of a bottleneck, by supporting more initiatives
- Develop inter-organization affinity across heterogeneous systems
- Create a single view of identity so it's easier to comply with internal and external regulations governing identity data
- Reduce the impact of changes on end users
- Securely 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

RADIANT LOGIC

About Radiant Logic

As unified identity market leader, Radiant Logic provides the cornerstone for complex identity architectures, creating a single source of identity truth. Radiant connects disparate legacy/cloud data sources, speeding the success of single sign-on, M&A integrations, identity governance/administration, cloud directory deployments, and hybrid/multicloud environments for Fortune 1000 and government agencies.

Learn more at radiantlogic.com