Delivering Identity and Context as a Service

Provide Smarter Security, Better Services, and Breakthrough Data Management through Virtualization

Table of Contents

Introduction

Delivering smarter security and more customized services are at the top of any IT agenda. But while these goals may appear quite different from a business and technical perspective, they share a lot under the surface. In fact, **both would be easier—and cheaper—to achieve with a common infrastructure—what we call an identity and context service.**

Now, this idea may seem a bit paradoxical at first glance. After all, different teams—with diverging backgrounds and separate budgets—traditionally handle these targets. Why would the directory-focused security unit and the database-driven data management crowd want—or need—to rely on a shared infrastructure? What exactly is an identity and context service? And **how would such an infrastructure serve these two very different groups, with their very separate and specific agendas?**

We'll address all these questions throughout this paper, but let's begin by looking these two seemingly unrelated sectors. First, we have the primarily LDAP-based field of identity management (IdM), which is concerned with **managing all your constituents to secure your organization.** Then we have the SQL-intensive field of data management, which, within its sub-disciplines of master data management (MDM) and customer data integration (CDI), is aimed at **providing greater agility and more targeted services** to your most important constituents: customers.

These worlds are not usually seen through the same lens—in fact, they don't even speak the same language. But they do share one essential need: whether you're ensuring security or looking at customer interactions across the enterprise, you must:

- **Find a way to identify users across all your fragmented systems.** This global identification system is the basic building block of many initiatives, whether they fall under the heading of identity management or customer data integration.
- **Once you can identify users, you also need a way to view the full range of their activities from inside all your application silos,** because that's the knowledge that drives smarter access policies, more responsive customer service, and higher-value offerings tailored to your customers' wants, needs, and particular delights.

And in the end, isn't that what really drives your business? It may feel like a cliché at this point, but it's still the phrase every company lives and dies by: ***KNOW YOUR CUSTOMER***. This capability is vital for securing your organization—after all, you need a common identity to authenticate users across systems, and as many attributes as you can gather to authorize them.

But it's also essential for your business: **the more you know about your customer, the better you can serve them—and the more you can sell them.** So when we talk about the demands of identity management, they are also the needs at the heart of any master data management/customer data integration initiative:

> *"MDM and CDI create new opportunities and ways to drastically improve customer experience and increase top-line revenue. Indeed, many new and established* ***enterprises are looking to differentiate themselves from the competition by significantly increasing customer satisfaction and improving customer experience.*** *Having an accurate and complete system of record for customer information allows enterprises to gain new and more actionable intelligence into the customer's buying behavior and thus allows companies to* ***create and offer better and more accurate personalized products and services."***
>
> - Alex Berson and Larry Dubov, *Data Management and Customer Data Integration for a Global Enterprise* (McGraw-Hill, 2007)

After all, everything comes down to **identity**—*who is this person and what do I know about them?*—and context—*how does this person relate to other people, objects, or services within my enterprise ecosystem?* Thanks to these common requirements, we believe that breakthrough technology developed for the identity management field could also be **the key foundation of a more flexible, nimble, and cheaper CDI effort.**

This approach is the result of abstracting two services:

- A common identity service for subjects, people, or objects shared across applications and disparate data sources.
- A dynamic context service that pulls contextual data from virtualized applications using **smart query federation** and an understanding of **metadata**, and delivers infinite new perspectives into this once-siloed information.

Rather than delivering a single, static view of the world, this system—an Identity and Context Virtualization service—promises one truth about the reference, one common way to identify subjects across systems, and the ability to link those subjects to any specific context contained in application silos. Such an approach offers richness and flexibility, as well as **another key advantage: in a system that can be seen and shared by everybody, security and privacy are built in**. By combining identity integration and context management with smart virtualization, you're building a modern data management infrastructure—one where security is a core feature, not an afterthought.

The Goal: Secure Your Infrastructure & Deliver a 360° View of Your Customers

The need for a global system of identity is not limited to the world of security or directories. Whether you need to **build a single view of your customers** or you're trying to **deliver rich context-driven services by extracting information from existing silos**, you need a global view of identity and context that allows you to enforce security and make updates at the local level.

Although the initial challenge is managing identity for security and privacy, **the existence of identity and data silos—and the difficulty of integrating across them—affects every aspect of your business information.** As enterprise IT has matured, more of your business-critical data is being managed in specialized application silos. While silos are excellent at collecting, maintaining and organizing information locally for a specific domain, integrating data across them is a huge technical challenge.

This **lack of coordination across silos has high costs for your enterprise:**

- Data fragmentation and missing insight into critical business processes
- Reduced productivity and higher costs
- Inconsistent or poor service in areas such as customer support, logistics, and workflow
- High risks in critical activities, such as healthcare, defense, security, and intelligence

We view identity and context as a service, enabling enterprises to **get a complete and contextual view of their information**—essential for targeting cross-sell and upsell opportunities, and improving operational efficiency. The same virtualization platform that enables enterprises to manage identity globally, while enforcing security locally, can also **deliver both identity and context as a complementary service for many of your other initiatives.**

Identity Crisis: The Current Fragmented Landscape

While a better understanding of your customers and other users is essential for both security and strategic reasons, there are technical complexities that have made such a goal more difficult—and expensive—to achieve. Since the user is the core of any initiative, let's begin by taking a brief look at the limitations of today's identity landscape.

Today's identity infrastructures are—in a word—broken. Critical information is siloed in diverse stores and applications, so what you know about a user is scattered across disparate systems with no easy way to retrieve it and put it all together. Even the basic task of authentication—identifying users from across data silos to grant them access—has become a nearly insurmountable burden.

These days, most organizations face an unappealing choice: either live with the current patchwork of identity silos or undertake a costly and almost impossible effort to centralize identity across these systems. The diversity of identity representation presents a huge technical barrier. Differences in APIs and protocols add to the complexity. Simply accessing and gathering identity information across data silos is already a challenge. And in a system with multiple distributed applications, **just keeping information up to date can be a synchronization nightmare.**

We believe that abstracting identities through **advanced virtualization is a better, more flexible option** than either building a monolithic application that's costly and difficult to manage, or dealing with a series of identity silos that are expensive and nearly impossible to bridge. And we'll explore how such model-driven virtualization works from a technical perspective in the final section of this paper.

Now that we've laid the groundwork for the underlying technical challenges, let's consider the larger picture of identity—who your users are and how they relate to your company and its products, services, and people, enlarging our focus from the security-minded landscape of IdM to the customer-centric terrain of CDI.

Beyond IdM and Security: Toward a World of Integrated, Context-Driven Services

In today's business environment, change is the only constant. When marketing occurs in real-time, and answers are expected at a moment's notice, **flexibility and responsiveness are your organizations' highest priorities**. Unfortunately, as we outlined above, typical identity infrastructures are mazes of application silos and identity protocols, making it tough to adapt.

To build a more flexible system, best practices dictate that we offer identity as a common, interoperable service. In this kind of architecture, multiple applications delegate functions such as identity management to a set of common services, **allowing the application to focus on its specialized tasks**. Beyond streamlining security for SSO and better authorization, this approach allows enterprises to meet shifting demands by flexibly shuffling their product and service offerings. Creating one shared version of identity is the key enabler for better segmentation, customization, and personalization—all key components of CDI initiatives.

Such customized offerings require an understanding of your customer that is not possible in the current chaos of application and data silos. The unique value of a common identity service is that you can now have **a global view of customers, employees, and partners, allowing you to change and reassign services and product offerings as needed**. By externalizing identities and their context into a service, such information can be flexibly and intelligently provided to a variety of applications, allowing each application to focus on its own core competency.

Begin with Identity: Build a Common Identifier from Across Systems

If identities were stored in a single repository, finding a unique user would be a relatively easy process. Unfortunately, this is almost never the case. Typically, there are many user stores for all the different constituents—employees, partners, customers, suppliers—in your enterprise. These data sources can range from LDAP to SQL, and even web services. **Most companies, both large and small, find themselves managing a variety of disparate data stores, without the means to integrate them**. The only solution for such a multifaceted infrastructure is to combine these resources into a unique "logical list" that works with existing identity silos. Sophisticated virtualization unifies disparate data sources and identity profiles into a single namespace, all delivered to your applications in real-time.

Then Add Context: Pull Information Dynamically to Create a More Complete Picture

Just as advanced virtualization can externalize identity out of data sources and represent it in the form of LDAP for security, it can also **liberate contextual data from the constraints of data silos—and make it accessible to business people**. With groundbreaking context virtualization capabilities, companies can **publish information directly out of their existing data silos and then share this data across the enterprise**. Context virtualization delivers a single version of the truth, where all systems can be linked and represented in a common model that is updated in real-time—giving you a **360-degree view of your customers and their context.**

As you can see, delivering identity and context as a service will not only renew and extend your security infrastructure, it could also drive customer data integration efforts, as well.

Use Cases: Why Identity and Context Matter

Now let's explore the reasons why externalizing identity and context out of application silos and delivering them as infinitely consumable services is a good choice for your business.

Ensure Advanced Security

Intelligent authentication, fine-grained authorization, and single sign-on capabilities all require externalizing identities out of applications. For security across your directories, databases, and web services—as well as enabling claims-based security across the cloud—you need one global view so your web access management (WAM) tool can authenticate different categories of users. More and more, your users need to connect to applications outside of the firewall and in the cloud. **As more services integrate with the cloud, the need to externalize identities into a common, easy to manage, and secure identity service is even more pressing.**

In addition, to provide up-to-the-minute, fine-grained authorization, you need quick access to attributes from all of your sources. If you can rapidly extract attributes from all your data silos, you can better secure your resources and offer new services. However, without a global view, managing customers, employees, and partners in the cloud would be at best a management headache, and at worst, a security catastrophe in the making. But there is much more to this story besides the security aspects.

Improve Business Agility and Provide More Targeted Services

Beyond the critical security reasons, the opportunity to better serve your customers is what compels enterprises to externalize identities from their data silos. By removing the responsibility for identity management out of applications and putting it into an interoperable identity and context service, **your applications can now focus their core competencies—and you can better serve your customers.**

In today's business and internet environment, your customers expect a seamless, no-hassle experience. **Imagine that your customers sign on only once, and immediately receive an individually tailored experience**, accessing services and offerings from across the enterprise and the web that reflects their preferences. An intelligent identity and context virtualization service enables this vision to become a reality, and helps your business to get ahead through better customer responsiveness.

Support Essential Business Strategies

In a time where differentiation, adaptability, and customer focus are essential business values, it doesn't make sense that the sources for all activities—the identity and contextual profiles of all users and customers—are spread across incompatible and siloed applications. Unfortunately, this is the reality for most organizations.

In their book on MDM and CDI, Berson and Dubov describe four essential reasons to know your customers better. Let's examine the impact of fragmentation on these key strategies, looking at the promise—and the pain—of building better customer relationships.

Use Case 1: Enhance Customer Experience

Customer experience is rapidly becoming a key differentiator for the savvy, agile organization. But **it's tough to deliver a great experience to individual customers when you don't know what makes them unique**. All customers expect an intuitive, hassle-free experience when buying products from your site or stores. They want the right information delivered in a timely fashion. And they want customer service issues to be handled quickly and efficiently. But beyond these basic expectations, there's a lot of room for really enhancing an individual's experience of your company. The more you know about a particular person, the better you can target cross-sell and upsell opportunities, ensuring that your marketing feels more like a conversation between trusted friends, rather than a mass, impersonal pitch made by a faceless corporation.

Use Case 2: Improve Customer Retention and Reduce Attrition

It's the holy grail of business: keeping customers satisfied so they stick around and keep spending. After all, **it costs a lot less to keep a customer happy than to attract a new customer**. Spending less on retention, while maintaining strong customer loyalty, is essential. Retention is driven by several factors—customer experience, as we describe above, and customer loyalty and service, which we'll examine below. But as we know, it's tough to deliver on any of these, given our fragmented data structures and the lack of visibility into customers and their ever-shifting contexts within your corporation.

Use Case 3: Increase Revenue by Building Customer Relationships

Product lifecycles are getting shorter. Competition is heating up. And even the costliest items are becoming commoditized. All this puts increasing pressure on your relationship with customers. It's no longer enough to take a transaction-based approach to customer relationships. Now, as Berson and Dubov say, *"the strategy involves the* ***notion of acquiring, understanding, and servicing the customer in the context of his or her relationships with the enterprise."*** To move from an accounts-based focus to a customer-centric focus, you need to be able to identify not only your customer, but also his or her context across your enterprise.

Use Case 4: Speed Customer Service with Just-in-Time Delivery

Imagine you're calling your cable company for customer service. You need to change your address, add another phone line, and also get some help resetting your network. Now imagine your all-too-common frustration when one person, using a single system, can't help you with all those needs. **What the customer doesn't, and shouldn't, know is that behind the scenes, there's a patchwork of different systems**—often cobbled together as the result of mergers or acquisitions—that are each responsible for some small part of the puzzle. There's no unified system where a service rep can make all the changes, or find all the information you need. From the customer's perspective, this makes no sense.

Customers expect service, not excuses. They have no idea how tangled your underlying infrastructure is, or how fragile the integrations are between all your disparate systems—and they should never have to deal with that.

The customer-driven enterprise is all about making accurate data available to users and applications more quickly, and providing excellent service as soon as it's needed. After all, customer service is a fact of life for companies—even the best organization needs to be responsive to the inevitable questions and issues. But problems don't have to hurt your relationship with customers. In fact, **great service is another opportunity to deepen and strengthen your relationship** with them. Done right, it's your chance to learn more about what a customer wants and needs, so you can deliver a more targeted, loyalty-inducing experience.

Now that we've considered the business reasons for abstracting identity and context and offering them as key services, let's take a deeper look at the technical challenges behind the goal of securing your infrastructure and enhancing your customer relationships.

The Technical Challenges: Managing a Diverse & Fragmented Infrastructure

A considerable set of technical challenges lie between a flexible identity and context service, and your current fractured infrastructure. Application silos, originally designed to be locally administered, now hold mission-critical data that cannot be easily consumed by the solutions that need it. Identities stored in the cloud complicate the issue even more. Because each application contains its own separate list of users, identities are locked inside these applications silos, divided by distinct protocols and identity representations.

As you add users due to new initiatives, mergers, or acquisitions, your user lists must be constantly updated. To perform secure authentication and authorization, your applications want to look to one standards-based directory. However, with multiple user stores belonging to a myriad of applications, identities are scattered across disparate user lists—each with its own access protocols.

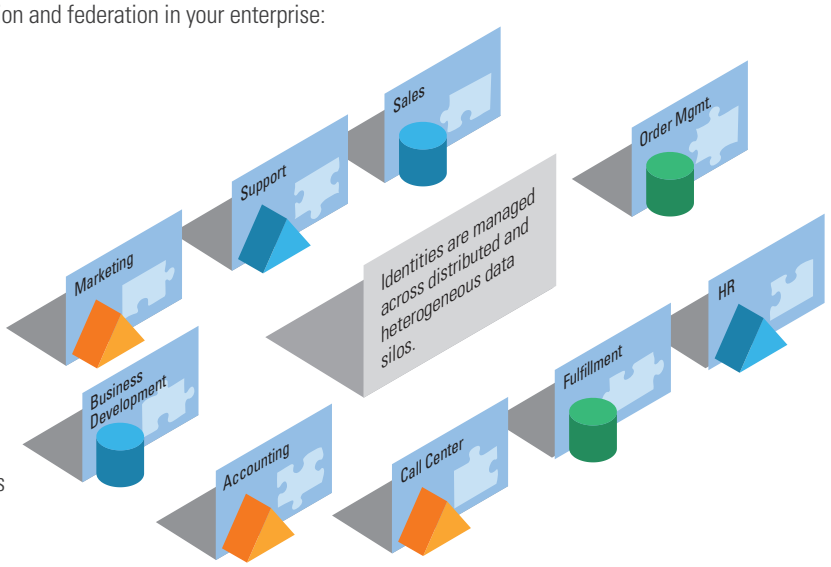
There are two dimensions to the challenge of identity integration and federation in your enterprise:

Multiple Security Domains:

- Multiple access protocols (including LDAP, SQL, and web services)
- Multiple security means and authentication methods (passwords, tokens, and certificates)
- Multiple authorization policies (roles, rules, groups)

Diverse Data Structures:

- Recognize and synchronize the same user across various systems
- Applications must read and understand different schemas from directories, both standard and proprietary, plus relational databases and web services

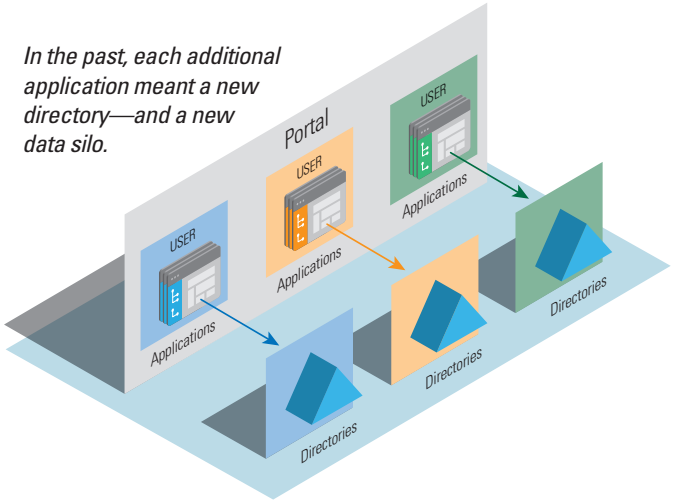


What you need is a complete identity profile, offering a unified view of context and attributes. But how can you create this single picture of your users and customers when their attributes are stored in different protocols and locked in identity silos?

A Heterogeneous and Tightly Coupled World of Applications and Identities

These problems began with the evolution of the directory as a storage structure. Directories were originally created as a means of turning identity into an external service, as had been done previously with other application functionalities. However, directories quickly became too inflexible and highly specialized, with the addition of each new service also requiring a new identity store. In the end, each application contained its own user store, creating an array of inflexible user lists, each of which must be maintained separately.

In the past, each additional application meant a new directory—and a new data silo.



Disparate Identity Structures, Competing Identity Protocols

Fast-forward to today's complex architectures, and identities are still represented in any number of ways. They can be found in Active Directory, relational databases, LDAP directories, or stored in the cloud. Unfortunately, all these different identity protocols act as a virtual tower of Babel, preventing your applications from working together easily or sharing information and functions between them.

Within such a siloed system, authentication is tougher than it needs to be because a user might have conflicting entries across silos. Synchronization is also increasingly difficult as you expand services or population size. If attributes are scattered or locked in application silos, each with its own protocol, your synchronization and security processes cannot access them. Inflexible, static, and hard-coded group membership also hinders authorization policies. In short, **these messy and overlapping user stores make it impossible to deliver the seamless and integrated experience you hope to offer your customers.**

Different Systems, Different Identifiers

Whether you're looking through the IdM or CDI lens, **the lack of a common identifier across data silos is a major problem in your infrastructure**. Your user or customer might appear multiple times across your system—and possibly with a different username or spelling each time. Identity management projects often require a common global identifier across systems to enable high-value targets such as single sign-on (SSO) or provisioning. Meanwhile, for better customer management, you need a common system of reference that maps the local customer identifiers within each silo to all the others, so you know which records, from which data sources, refer to which customers.

In CDI, this process is referred to as "customer entity resolution," although it's called "identity correlation" in the IdM world. Identities can be stored in many formats within the field of identity management, but they're traditionally stored in LDAP or a proprietary directory such as Active Directory. In data management, information is mainly stored in databases, so MDM/CDI efforts are mostly a matter of federating SQL data. Despite these differences, **both IdM and CDI require a common global identifier to see into all your systems and identify data**, whether it's user names or any other attribute or object. And both disciplines benefit from a virtualized layer that enables you to see into those systems and create a unique way to identify data. So the same structure that's at the heart of IdM initiatives could also form the core of your CDI efforts, as well.

The Over-Centralized System

One possible response to the diversity of protocols and the lack of a common identity is to create a centralized identity repository for the enterprise. This addresses the problem of synchronizing and normalizing diverse data. But let's say you could gather all the information you need, and harmonize it to achieve "one version of the truth." What kind of profile would you build? How would you define a single structure that could serve many purposes? How many attributes would you include? And who would own and manage all that data? As many organizations have found, **centralizing too much can mean an unmanageable system of synchronization**, or lead to a global system that's always outdated due to synchronization lag.

With your identities centralized, you also run the risk of over-centralizing and missing key attributes of identity from specialized applications, such as an HR or CRM system. Such an monolithic application quickly becomes unmanageable, reminding identity architects of why we need originally designed specialized applications—to reduce risk and create the best features for a given, narrow function.

Neither the chaos of identity stores nor a single, centralized application provides the flexibility and responsiveness that your enterprise requires. The only solution to these challenges is to **create a common identity service by externalizing and virtualizing identities out of application silos**. Such an identity service, coupled with a unified query system that pulls attributes from silos and organizes them contextually, delivers the unique views your applications need.

Common Integration Challenges at the Local Source Level

Here, we'll briefly examine three common use cases that are current challenges in your quest for better security and data management. We'll also see that **these challenges represent unique opportunities for a quick win with a high ROI**—thanks to an identity and context service. We'll also explore later how those how these intermediate steps could be leveraged to build a complete identity layer, delivering context-aware services to your customers.

1. From AD to LDAP: Integrating Proprietary and Standard Directories

Employee identities are often stored in proprietary directories such as Active Directory because it's essential to Network Operations and Administration. Meanwhile, external users are stored in a standards-based LDAP directory. The result is **a schism between your internal and external users—creating a headache for ensuring portal security** or granting access to cloud-based services. Web access management packages often have limited support for more than one directory, particularly when it comes to user search capabilities. To further complicate the problem, your WAM expects a more or less a standard LDAP structure, which constrains all the Microsoft-specific features and functionality of AD.

2. From SQL to LDAP: Mapping Databases into Directories

To securely authenticate and authorize all your users, you need quick access to your customer database, where those identities are stored and managed. However, SQL is not the fastest engine for authentication, and its very slow "join" function severely inhibits authorization capabilities, creating a traffic jam when you need to bring these identities in your infrastructure. **You need a way to map your SQL identities to the expected LDAP format**, so consuming applications can "read" them.

3. From Application Endpoints to Identity Federation: Delivering Identity and Context in the Cloud

Once disparate resources are pooled in a federated cloud infrastructure, your authentication hub now faces the issue of fragmented identification: how to identify users across heterogeneous data sources and check credentials via different methods, such as passwords, keys, tokens, and certificates. While federation security pathways cover a lot of ground, they cannot effectively scale all the way into each separate identity source. Identity providers need a way to **reach into endpoints to virtualize and authenticate identities out of disparate data repositories**.

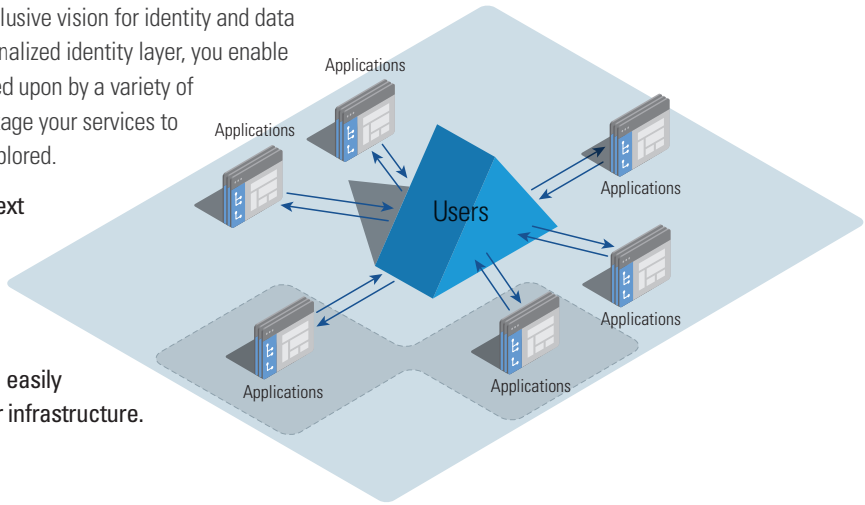
An additional challenge in the authorization domain is the division of work between Identity Providers (IdP) and Relaying Parties (RP). The key enabler for authorization at the level of the RP is a rich and fast attribute server. For a complete picture of your user, the server should be able to associate identity and context—but that means reaching across a heterogeneous mix of data silos.

We'll delve further into the technical details of solving these issues in future white papers, but the remainder of this paper will look at how an identity and context service based on model-driven virtualization solves these challenges in an efficient and cost-effective way.

The Solution: Model-Driven Virtualization and Identity and Context as a Service

A complete service-oriented architecture has been an elusive vision for identity and data architects. By supporting your application with an externalized identity layer, you enable on-the-fly recombination of services, which can be called upon by a variety of applications. At any time, you can easily offer or repackage your services to pursue any of the business strategies we've already explored.

As a key part of this architecture, **an identity and context service integrates and then delivers representations of users and the context that surrounds them**. By supplying identity information in a flexible and customizable way, applications can quickly pull the data they need from one logical source, allowing you to **easily add new applications and new populations into your infrastructure.**

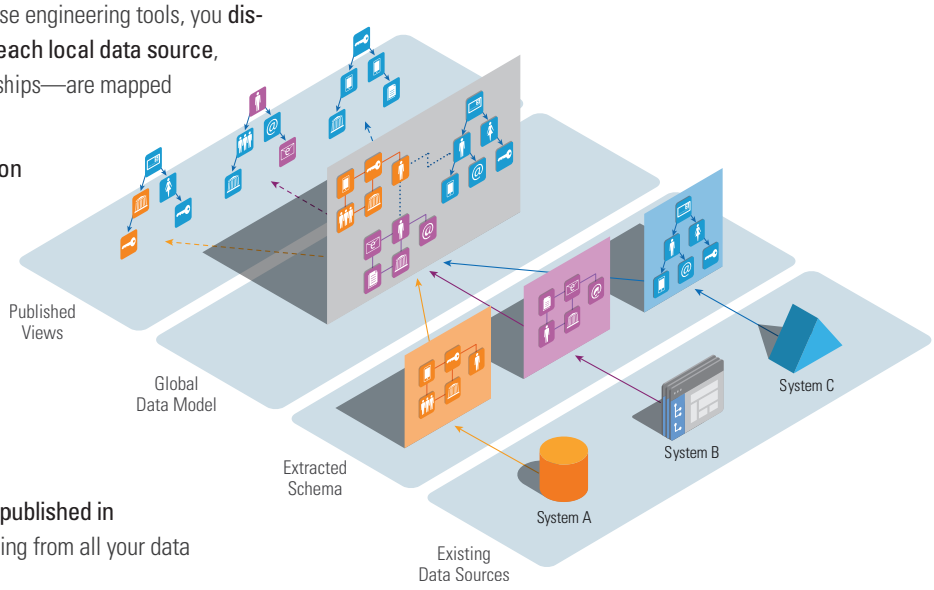


With an identity and context service, applications can dynamically access the information they need, without centralizing identity storage.

Model-Driven Virtualization: Building Your World View

Model-driven virtualization is the essential tool for externalizing and projecting identities into a service, while leaving underlying sources untouched. A model-driven identity service understands the formats of each data source and builds an **external, virtual global identification system.** Once this global virtual identity is in place, you can build contextual views of a user by leveraging a common federated query system, along with metadata extracted by automated reverse engineering. By externalizing the specific data models of each data silo and associating the users and subjects them into different contextual hierarchies, an identity and context service delivers the appropriate and unique views your applications need. Model-driven virtualization works in four steps:

1. First, with the support of automated reverse engineering tools, you **discover and extract a schema model for each local data source**, where objects—along with their relationships—are mapped and virtualized.
2. **Local models are linked through common identities into a global model.** Relationships are the key enablers to link the identity of a subject to its relevant application context.
3. **These links expose the attributes needed** for finer-grained, context-driven authorization and context-aware applications.
4. **Identity can by linked dynamically, and published in customizable views**, with attributes coming from all your data sources.



Streamline Authentication and Authorization

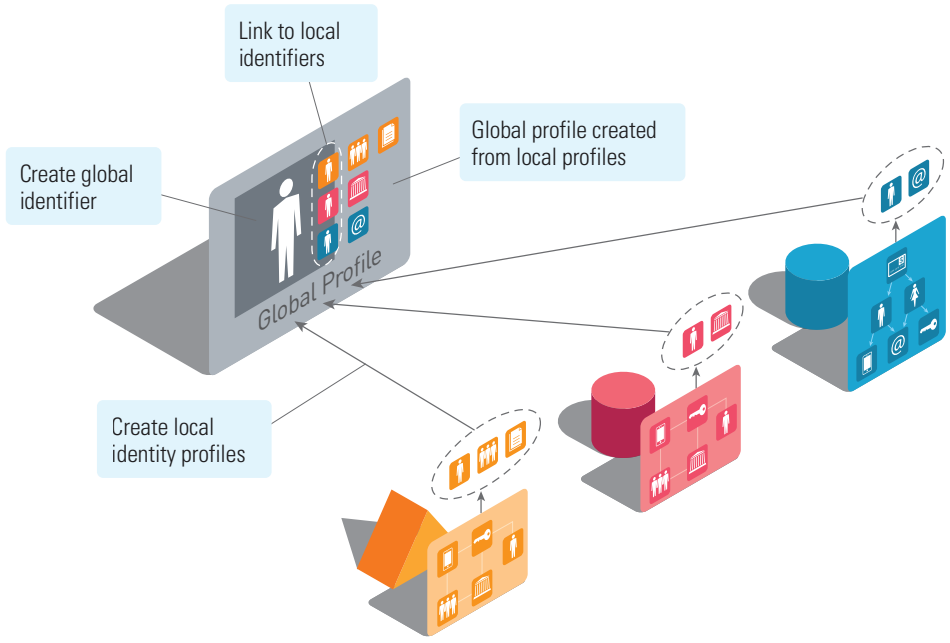
With a model-driven approach, the identity and context service can flexibly deliver identities out of silos, and present them to your WAM packages and applications. Such a service streamlines authentication in a variety of ways:

- **Simplifies identification:** Aggregating users from multiple data sources allows applications to search one common namespace to find user.
- **Increases flexibility:** Credential checking can be handled by the virtual directory or delegated to the underlying source.

Virtualization improves authorization by providing a **common searchable schema**. Such a schema:

- **Aggregates profile information** into one global profile to deliver more context about a user. Because more attributes are readily available, finer-grained, more nuanced policies can be enforced.
- **Offers more flexible group definition** by aggregating and mapping existing groups to build new attribute-based group definitions with dynamic membership.
- **Presents multiple hierarchical views** derived from existing static trees.
- **Feeds your policy server required user attributes** via a standards-based protocol.

An identity and context service joins attributes from across disparate data silos to build a global profile of each user or customer. This global profile can be fed to your WAM package for fine-grained, attribute-based access control solutions.

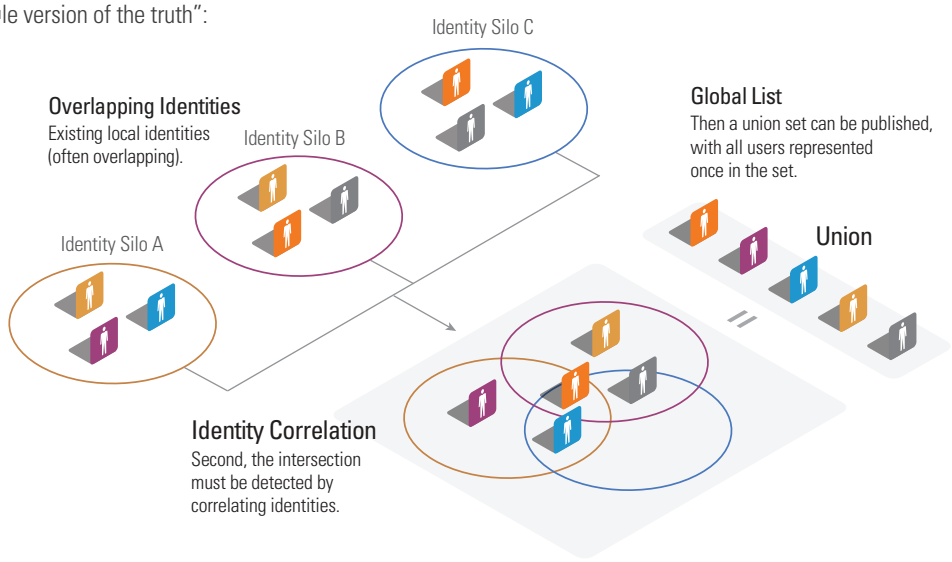


Create a Global Identifier Across Systems

Now let's look at what happens when a user shows up more than once within your sources. Before you can perform model-driven virtualization, and achieve this flexible identity service, you need to first locate the subjects, people, or objects that are shared across all your data stores. A common identity is the necessary foundation for both advanced security and complex customer management initiatives. Rather than imposing one monolithic view of your data, model-driven virtualization enables a single shared truth by creating a common way to identify subjects across your system.

Two key operations enable you to create a "single version of the truth":

- **Object synchronization** keeps identity data coherent across your enterprise.
- **Identity correlation** creates the unified view of identity data across multiple systems necessary for a complex infrastructure, identifying intersections and eliminating overlaps. If you have "dirty" data—with many users spread across several backends, no common identifier, and little overlap of attributes—you will need to create a global unique identifier for common use in your system.



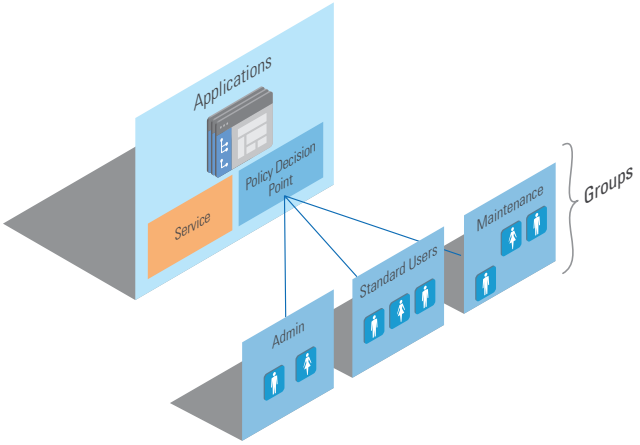
All of a particular user's entries in your directories, databases, and web services can now be identified by this **common global identifier**. And unlike most CDI efforts, where you're limited to SQL, an identity and context virtualization service enables a global identifier across directories, databases, and web services.

Thanks to the global identifier, your applications now believe that all the data from your disparate identity system is located in one place, with one access point—yet you still avoid the over-centralization trap.

Build Flexible Groups and Roles for Better Authorization

With your identities extracted out of silos and into an interoperable service, you can flexibly dispatch users into groups based on attributes and their context. **Advanced virtualization enables dynamic group membership—instead of hard-coding users into groups, you can populate groups as you go, based on whatever attributes you choose**. This is an essential asset for creating fine-grained authorization policies.

Your application can offer various services based on authorization policies that you define through the user's role or group membership. Because group membership is automatically assigned or removed based on the user's attributes, administrators are no longer responsible for endless manual group management, or for granting (or failing to remove) inappropriate access.



With an identity and context service, you can build and modify groups on-the-fly, without hard-coding.

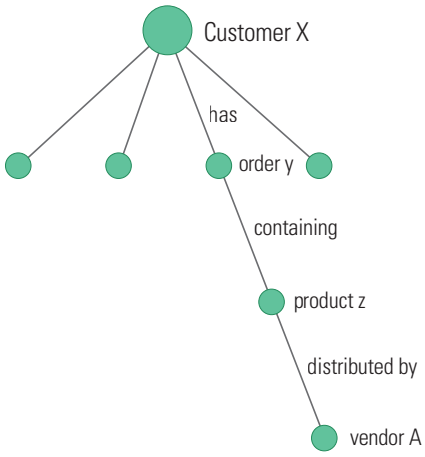
Get Context on Demand via Hierarchies

One critical objective of MDM/CDI efforts is to understand the relationships among reference entities throughout your enterprise. As we've already explored, successful CDI means being able to deliver different views of your enterprise's data to meet varying business needs. A context service makes a critical and unprecedented contribution to CDI: **by leveraging metadata through hierarchies, you can deliver an infinite variety of contextual views into your processes.**

Let's take a closer look at the role of hierarchies, especially when it comes to relational databases. Why are hierarchies important? As any practitioner of CDI knows, once you develop a customer's profile, the next step is to organize that person's profile around classifications such as households, or groups. **Context in a customer's profile comes from the classification and regrouping of the customer—and any form of classification is based on an implicit or explicit hierarchy.**

Let's look at an example of the "1:n" relationship between customers and their orders. Using SQL, you can navigate from customers to orders, and back again, via joins. So for each customer, you can easily find the potentially "n" corresponding orders. Or vice versa—for a given order, you can quickly locate which customers ordered it. But you should notice that semantically, we always pick one direction to interpret information—whether we go from customer to order, or from order to customer, **our interpretation is "oriented."** When you navigate a 1:n relationship, you are creating a simple hierarchy. If you repeat and cascade this operation across many relationships, you get a system that becomes increasingly specific. Implicitly, you are navigating a context tree that grows deeper and more detailed about a given subject.

Another way to look at this is to consider a "left join" between two objects as a sentence linking subject to object. Coming back to our example, we could say that: "customer X places order Y." Navigating relationships between objects is like publishing related sentences that link those entities. These sentences tie a subject to other entities/objects/services, **describing a "context" stored in the data silos** about a given user.



Relational models can generate infinite hierarchies, revealing the richness contained within your data—but at a cripplingly slow speeds. **An identity and context service, however, gives you the best of both the SQL and the hierarchical worlds.** You can store data in SQL, capturing attribute richness and relationships, but extract and publish hierarchical views in LDAP (or any other NoSQL), leveraging a well-established hierarchical engine—all without hard coding. Thanks to this contextual insight into relationships, your business can more effectively focus its marketing strategies, and better serve its customers. **With an identity and context service linking your backend sources, you can deliver context on demand, and at a faster speed than SQL alone.** HDAP, our Big Data Directory, becomes an essential asset to your infrastructure.

Deliver Your Views Quickly with HDAP

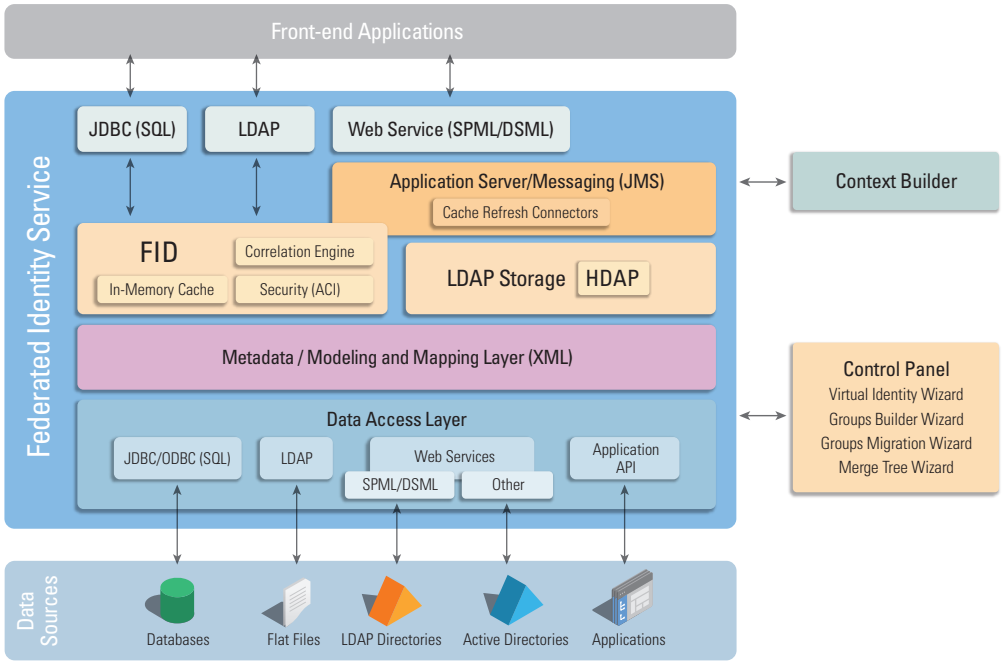
Virtualizing a slower source—such as a database or web service— into a service not only makes it compatible with your best security and MDM practices, it can also dramatically improve speed and performance. High user and data volumes, as well as complex use cases, demand a highly scalable storage that is automatically refreshed when data changes—RadiantOne's Big Data Directory, HDAP, provides this. With a storage layer that's based on big data technologies, complete replicas of your backend data are stored and delivered at high speeds. HDAP guarantees that your applications can access an always on, always available and up-to-date external replica of your virtualized sources—even if your actual data source is down or slow.

RadiantOne's Identity and Context Virtualization Platform

Although you have several choices in identity virtualization tools, **only one gives you a full-spectrum identity service—plus context on demand.** RadiantOne's Identity and Context Virtualization platform, built to handle advanced security challenges, can also provide a solid foundation for all your customer management initiatives. It's the only solution featuring **model-driven virtualization technology**, enabling you to build complete virtual and external replicas of your data storage.

The RadiantOne virtualization platform includes both our federated identity service and our Identity Correlation and Synchronization Server (ICS) for identity correlation, all fine-tuned to give your enterprise both a global and contextual view of your users, customers, and partners. Our identity service aggregates and correlates identities from across systems—both yours and your partners. This enables you to pull all the contextual attributes needed to quickly **deliver customized offerings with a single sign-on across trust realms, creating a fluid, individualized experience for your customers.**

Identity & Context Virtualization Engine



About Radiant Logic

As the market-leading provider of federated identity systems based on virtualization, Radiant Logic delivers simple, logical, and standards-based access to all identity within an organization. The RadiantOne federated identity service enables customizable identity views built from disparate data silos, driving critical authentication and authorization decisions for WAM, federation, and cloud deployments. Fortune 1000 companies, including General Electric, Wells Fargo, Monsanto, NBC Universal Media, and Intel, rely on RadiantOne to deliver quick ROI by reducing administrative effort, simplifying integration, and building a flexible infrastructure to meet changing business demands.

Contact Us

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