OPTIMAL IdM
Identity & Access Management

Identity Fabrics and The Evolution of Identity:

From Problematic to Programmatic

Background:

Today's businesses are faced with managing massive amounts of identities from many sources that need to go many places in many ways. Managing access via traditional methods increases cybersecurity risk and decreases speed of business. A new approach called Identity Fabrics has emerged to help organizations handle one of the thorniest problems spawned by the shift to digital business.

Your business no longer has boundaries. With the adoption of the cloud, the embrace of SaaS, the evolution into multi-cloud, and the growing reality that every business is a software business, managing identity and access is today's top cybersecurity challenge. Malware may get the headlines, but IT people know the real risk is losing control of privileges. An over-privileged user or a thief with privileged credentials can do a great deal of damage over an extended period of time.

Malware may get the headlines, but IT people know the real risk is *losing control of privileges.*

Managing identities has always been challenging, but at least they were managed in-house, where there was a high level of control. That is no longer true. Identities come in from different services, such as directory services, federated identities, and social network IDs, and all of these identities need to integrate with outbound federation, web SSO, and other consumers of identity information.

But while boundaries around the edges of a business have blurred, there are more boundaries than ever on the inside. A company may have different directories to meet regulatory requirements or for other logical business reasons. Or, it may have acquired or merged with other companies and kept the absorbed companies' directories in place because the effort of integration was greater than the reward. But managing identity across these siloed directories adds increases headcount, adds cycles to the IT workload, and creates security gaps.

The legacy way of handling identity – where enterprises sync users to different apps and drop large files of user data, often using FTP, doesn't make sense in a digitally-transformed business. With identities coming from everywhere and taking so many different forms, businesses need a robust, flexible backend that standardizes them – without impacting users and or creating work for IT.

A more efficient way of handling identity is emerging. An Identity Fabric system connects many sources of identity information to many consumers of identity information, validating digital identities once for consumption by all.

Identity Fabric: A Modern Architecture Built Around Capabilities

An identity fabric architecture enables an organization to manage identity-related tasks like authentication, access control, and integration, through no-code workflows that ingest information from all platforms, process it, and route it to the services and apps necessary to fulfill the user's request.

Its power is in its flexibility. An Identity Fabric based system can handle requests from any source, including external identities, federated identities, APIs, directory services, databases, etc., and route them to an equally diverse array of identity consumers. An identity only has to be authenticated once and from there can be used without any limits other than those imposed by identity policies.

Identity isn't getting any easier

Straegize now, roll out when ready

The work of managing identities across silos is abstracted away from platform or vendor-specific solutions. Businesses don't have to re-tool their existing infrastructure and tech stacks, and they don't have to rewrite their apps or undergo painful migrations.

Since there is no need to rewrite apps or move platforms, the costs of identity-related projects is greatly reduced, as is time-to-market. Once in place, APIs do the heavy lifting, so admins are free to focus on their core jobs and the business has more resources available to devote to growth.

An Identity Fabric architecture provides visibility into the identity system and provides authentication regardless of the infrastructures involved – on-premise, private clouds, public clouds, and multi-clouds are all accommodated, and identity information is continually updated and always consistent.

An Identity Fabric supports stronger cybersecurity by enabling the consistent enforcement of policies across infrastructures, and across distributed apps as well, while also making advanced identity controls such as multi-factor authentication (MFA) and passwordless easier to implement.

Understanding Identity Fabrics

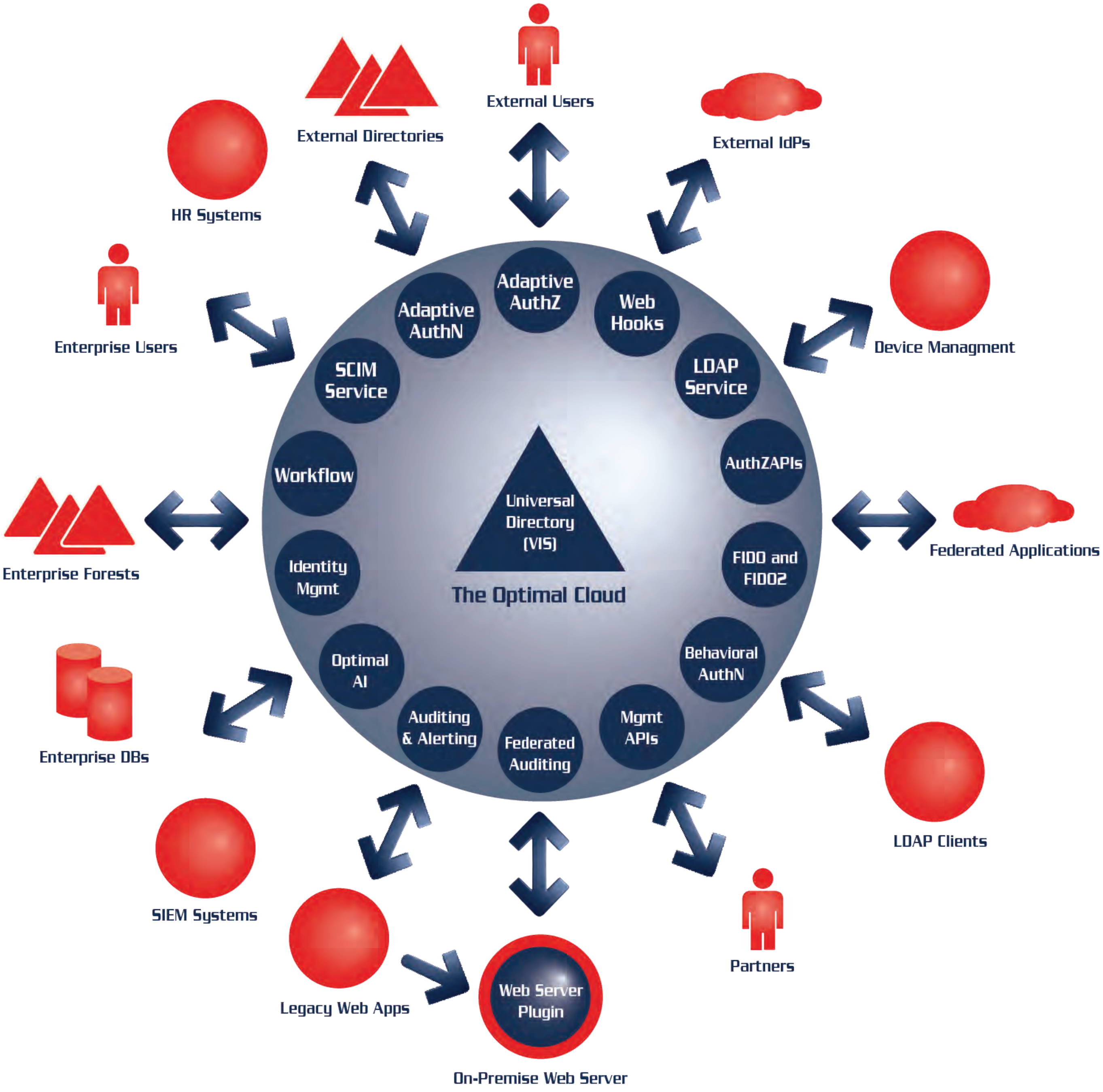
An Identity Fabric is a comprehensive model for architecting the delivery of identity services in the enterprise. Its components are a collection of API-enabled services and underlying directories that reside in the cloud between producers and consumers of identity requests. These components work together to deliver seamless and controlled access for all users to every service.

An Identity Fabric focuses on capabilities rather than a particular set of tools. While an Identity Fabric will include the pillars of IAM, which are access management, privileged access management (PAM), and identity governance & administration (IGA), these are complemented by additional capabilities, such as identity lifecycle management, multi-factor authentication, adaptive authentication, and virtual directory services. Because of its modular nature, an Identity Fabric is flexible, scalable, and customizable. It can also be implemented in phases, rather than one big push.

How Identity Fabrics Work

The Identity Fabric architecture receives requests from digital services through an API layer. A requester may be a person or group, or it may be a federated identity solution, API, directory service, database directory, etc.

The request is sent to an “identity API layer,” which passes it along to access management, IGA, and PAM solutions that handle things like identity federation, access governance, identity relationships, privileged access, and more. Other tools and services, such as MFA, may interact with the identity information at this point as well. Then containers of API-enabled microservices pass the request to all of its destinations, which may be a one or more other digital services, a SaaS, an API, or any other consumer of identity information.


External Directories
External Users
External IdPs
HR Systems
Enterprise Users
Device Managment
Enterprise Forests
Federated Applications
Enterprise DBs
LDAP Clients
SIEM Systems
Partners
Legacy Web Apps
On-Premise Web Server
Web Server Plugin
Adaptive AuthZ
Adaptive AuthN
Web Hooks
SCIM Service
LDAP Service
Workflow
AuthZAPIs
Universal Directory (VIS)
The Optimal Cloud
Identity Mgmt
FIDO and FIDO2
Optimal AI
Behavioral AuthN
Auditing & Alerting
Federated Auditing
Mgmt APIs

Solving The Silo Directory Problem With VDS

Silos aren't going away. Businesses will continue to acquire other businesses and continue to leave the acquired companies' directories in place because it's less expensive and easier to do so. More partnerships and more SaaS will evolve, and the rise of no-code and the citizen developer will result in more apps developed in-house that contain their own directories.

These highly-fragmented user populations have to constantly be synced to many places – and anything that's in sync can become out of sync. So while businesses are striving to accelerate their speed of business, syncing users is holding them back.

Organizations should be addressing this problem now by gaining the ability to create a way to authenticate identities once, in accordance with industry standards, and re-use them infinitely with their owners' consent. New use cases and identity groups should be able to be spun up quickly and made available everywhere they need to be, without human intervention. If a business can achieve this, it doesn't have to worry about silos.

And the way to achieve this is with a virtual directory service (VDS).

A virtual directory service makes multiple directories act like a single directory. Optimal IdM Virtual Identity Service (VIS) is middleware that proxies traffic between connected directories on the backend and can be managed through a familiar LDAP tool or the Optimal IdM console. All directory silos can be accessed and managed in real-time, letting administrators create connections and access policies, search all directories, and perform other admin functions the same way they do now.

Optimal IdM VIS Advantages

Efficiencies	Results
No synchronization necessary	Data is always consistent
No data flowing across the network	Data is always up to date
No database storage required for directory identity data	Management is minimized
Deployment in as little as 15 minutes	Security is strengthened

Optimal IdM VIS uses real-time 'joins' cached at the proxy layer to connect data between discrete directory services and feed them to apps and users as a single LDAP proxy. Advanced features include Virtual Group Manager, which allows group memberships to span multiple domains without the need for forest trusts. Group members can be either static or dynamic. Optimal IdM VIS presents a consolidated view of identity information to the services and apps that need to consume it.

Optimal IdM VIS In The Real World

Optimal IdM VIS is the world's first cloud-hosted virtual directory server and is used in the some of the largest companies in the world.

State Agencies

One of the common uses of Optimal IdM VIS is to allow apps that are not multi-forest aware to work in siloed environments. For example, one state government has separate forests for each of its agencies, such as its Department of Motor Vehicles and Department of Revenue, because the state wants centralized authentication and authorization in each one. But the state also uses a leading voicemail solution that is not multi-forest aware, so it can only communicate with one forest. When the state wants to send a voicemail to all of its agencies, the voicemail solution can't do it – but Optimal IdM VIS makes it possible. The voicemail solution thinks it is connecting to one forest, but in reality, it's connecting to VIS, and VIS is proxying the message to twenty or thirty Active Directory forests.

Global Enterprises

Optimal IdM VIS supports geographically distributed forests seamlessly without any caching or syncing. It can combine live data from multiple sources and merge it with the data in an Active Directory (AD) so the data appears to be coming only from the AD. Customers can lock down which applications can perform specific actions, so a business can, for example, connect its Secure Web Gateway(SWG) to its AD forest, but only let the SWG authenticate users and look up groups – but never see its computer accounts or unnecessary security information. In addition, Optimal IdM enables consistent auditing and logging across applications, processing results into a consistent format.

Academic Institutions

A US-based university had three forests across three separate campuses and needed a solution to help with their applications that were not multi-forest aware. They could have implemented Optimal IdM on-prem, but chose the cloud-hosted option. All they had to do was tell Optimal IdM which forests to connect to and provide credentials, and Optimal IdM did the rest. The school didn't have to do any integration, migration, or ripping-and-replacing to make its multi-forests appear as one to the rest of its ecosystem.

Optimal IdM VIS at a Glance

- The world's first cloud-hosted virtual directory service
- Live in data centers on 4 continents
- Connected to over 200 identity providers
- Serving more than 500,000 users

  4 levels of authentication
- 11,000+ federated applications
- 100-200 apps deployed each month
- More than 100 million authentications performed each a month

Can Identity Really Be This Easy?

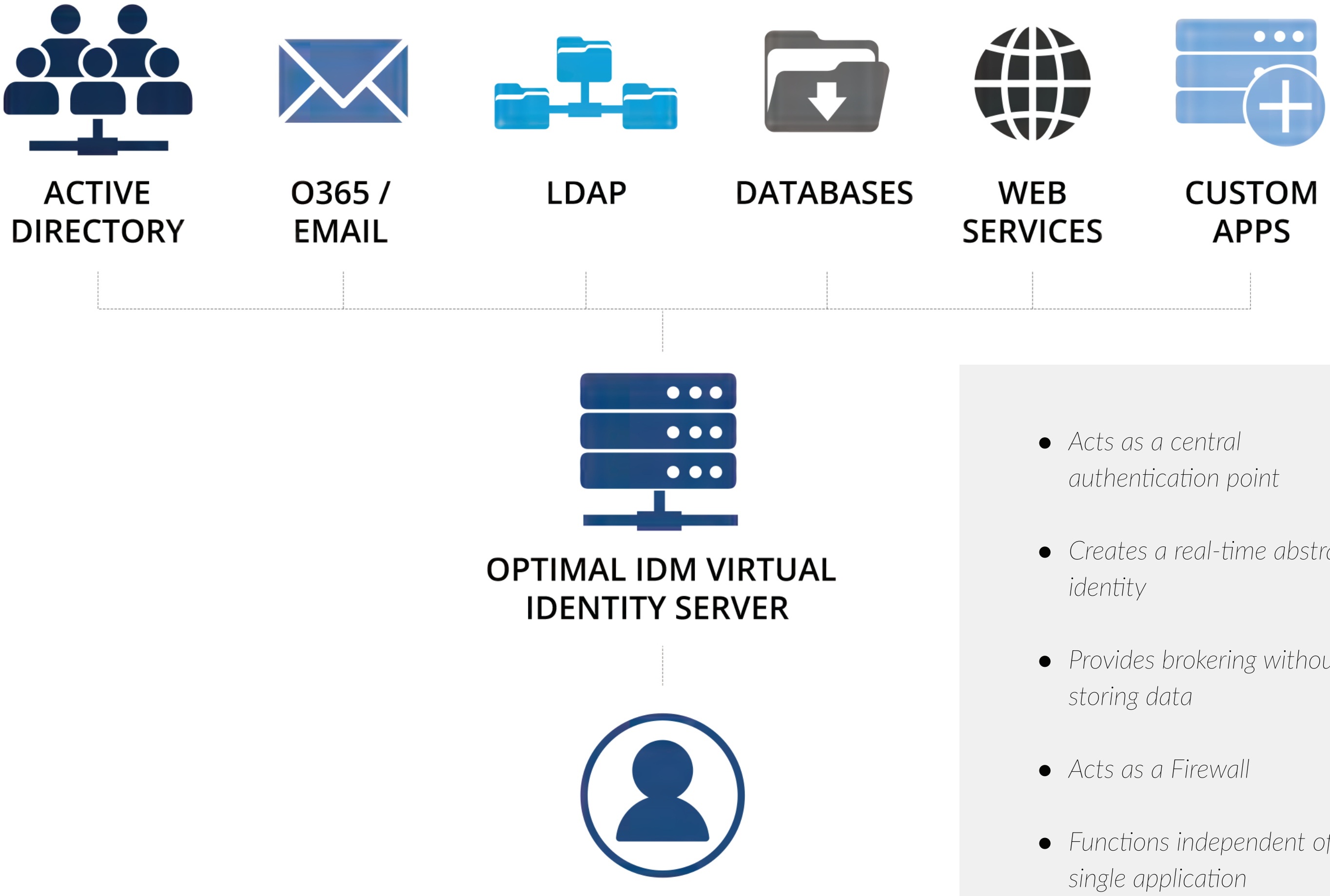
Optimal IdM VIS provides cloud-based reports that are written to a private database and are available via the browser. These reports can be filtered and exported, and raw files are available to feed into the Optimal Auditing System.

Security measures are baked into Optimal IdM VIS. Each customer is hosted on a private dedicated server, so if one customer is hacked, the others are not affected.

And because Optimal IdM is a fully-managed service, customers don't need their admins to do the configurations. Optimal IdM experts do 100 percent of the configuration, load balancing, maintenance, monitoring, etc. Updates are performed by Optimal IdM, and backups are made before each update, even if the customer has multiple environments.

Automatic scalability eliminates capacity concerns – Optimal IdM has the elasticity to meet even extraordinary needs. When COVID hit, a US state unemployment agency that was using Optimal IdM VIS was able to scale from

VIS – 1 IDENTITY FROM 1,000'S OF APPLICATIONS



- *Acts as a central authentication point*
- *Creates a real-time abstracted identity*
- *Provides brokering without storing data*
- *Acts as a Firewall*
- *Functions independent of any single application*

The Speed Of Business? Pedal To The Metal!

The pandemic taught business leaders that it was worth investing in agile technologies, that their teams are able to adapt to anything, and that there are still some sticking points to work out. Identity is the biggest of those, because traditional identity solutions cannot gracefully handle the vast numbers of external identities that are being created or route them to the equally vast number of places they need to be sent for consumption.

Identity Fabrics address that problem by applying known technologies and tactics to a complicated issue. APIs, automation, no-code, and cloud-hosted services are here to stay, and decision-makers should be taking steps now to incorporate them into their identity strategies.

Innovation doesn't have to be risky. Optimal IdM has proven identity services, delivering more than 100 million authentications each month across 4 continents to over 500,000 users.

Talk to Optimal IdM today and find out if you're ready to start your journey toward an Identity Fabric.

Talk to Optimal IdM today

and find out if you're ready to start your journey toward an Identity Fabric.