OPTIMAL IdM
Identity & Access Management

The Emerging Identity Consolidation Need

– It's All About The Applications!

Identity Chaos is Handcuffing Your Enterprise Cloud Potential

Imagine unrelenting security threats exploiting gaps from scattered user identities across your network and applications. Duplicate accesses leaving audit finding remediation unfinished for years. Simple new hire onboardings requiring risky elevation of privileges.

Let the identity hero emerge to tackle your enterprise security, compliance and transformation priorities magnified across a complex application ecosystems.

This identity chaos is painfully familiar for most modern enterprises. Increased cloud and mobility adoption only fragment identity stores further across applications, platforms and regions. Without reining it in fast, substantial business opportunities will only vaporize through lost data, customers, and resources one breach at a time.

But what if a simple platform could magically weave together those disconnected directories, databases and cloud apps - to allow one dashboard providing instant visibility across your identity anarchy? A solution allowing easy controls enforcement spanning all those chaotic stores in one sweep rather than hoping fragmented efforts might mesh randomly over time.

This whitepaper reveals how a purpose-built system delivers this unified identity fabric to drive convergence of your hybrid IT disorder. Exposing business risks, efficiency drains and simplified cloud migrations pathways are made possible once your access sprawl is tamed.

Let the identity hero emerge to tackle your enterprise security, compliance and transformation priorities magnified across a complex application ecosystems. Let's start by taking a look at some of the common issues causing identity chaos.

The Hybrid IT Complexity Issue

Modern enterprises operate in extremely complex technical environments. Most have hybrid infrastructure spanning on-premise data centers, multi-cloud platforms, SaaS applications, and more. With regional operations, redundancies are built across stacks. Divested businesses also leave abandoned infrastructure. This multiplicity introduces tremendous complexity for IT administrators. Fragmented systems with data and configuration sprawl make managing basic operations highly chaotic.

Identity Chaos Impacting Businesses

At the core of the IT complexity lies identity chaos. As infrastructure evolves rapidly, user stores and access controls fail to keep pace. Employees end up with identities and credentials straddling various directories and databases. Account lifecycles go uncontrolled. Entitlement risks and dormant users pile up within stores, obscured from oversight. Audits trigger fire-drills versus clean compliance reports.

Growing Data Breaches Due to Hacker Exploits of Gaps

The business impact of these identity gaps is accelerating. Account takeover and insider threats are rising as fragmented identity environments provide exploitable seams for hackers and bad actors. Forging of privileged access has enabled various headline-grabbing supply chain attacks recently. Positive Technologies' research highlights ~80% of data breaches involve compromised user identities. Purpose-built cyberattacks leveraging identity loopholes will sharply rise.

Need for Unified Identity Fabric

To address fundamentally, there needs to be a unified identity fabric that weaves together disparate sources like AD, LDAP and clouds. Consolidating identities into 'golden profiles' is pivotal for governance. Federation must percolate ongoing changes across stores in near real-time. This allows centralized policies while retaining existing infrastructure. Only an integrated identity platform can deliver the foundation for robust access management demanded of digital businesses.

Disconnected Directories and Siloed Applications

Fragmented identity directories and siloed applications create massive blind spots within user access environments. Some examples of disconnected identity data stores:

User Stores Tied to Line of Business Applications

For historical reasons tied to mergers or decentralized culture, often different business units manage own applications along with closely held user stores. This causes identity duplication and ineffective access reviews.

Cloud App Identity Stores with Disjointed Attributes

With SaaS apps like Salesforce, Workday or Office 365, new stores emerge rapidly. But integration challenges exist in propagating admin changes back to authoritative on-premise sources. Attributes diverge causing business workflow disruption.

EMEA AD Environments vs Americas ADs

Multinational companies maintain Active Directory Forests in each region. But the identity administration consoles end up inconsistent for people changes and access management over time. Conflicts arise requiring manual resolution.

Legacy Systems with Identities Not Maintained

Mergers, decommissioned apps or forgotten platforms still retain identities. Associated entitlements are challenging to map and contain for compliance needs allowing threats to linger due to identities left adrift.

Proliferation of Duplicate Profiles

Due to the fragmentation, it is common for employees and contractors to end up possessing multiple profiles - directly contributing to risks of improper access and exploitation by malicious actors.

This paints an unfortunate picture of how disconnected identity systems can enable enterprise risks. The downstream costs grossly outweigh any perceived flexibility gains. So it begs the question, what are your current key identity chaos or access sprawl pain points?

Failure of Traditional Approaches

With established approaches failing, new architecture principles may be needed for identity consolidation in complex environments. Some key drawbacks with existing techniques:

Limitations of Point Identity Management Tools

Legacy IGA tools solve for enhancements within an identity store itself. Focus is on governance capabilities for say Active Directory or Azure AD management. But gaps emerge in integrating distributed domains to derive unified views of user access.

Syncing Only Replicates Chaos

Legacy sync connectors extend chaos by duplicating disjointed identities across stores. This speeds up access but fails to resolve underlying fragmentation that weakens security. Replicating such disorder leaves the crux unaddressed.

Migration Untenable for Most

A greenfield migration into a fresh identity store brings forced disruption, massive costs and extended timelines - often impractical for global companies. Re-platforming workflows dependent on legacy stores brings risk of breaking business capability. The effort overwhelms most IT shops.

A Virtual Identity Integration Fabric Emerges

A radically different integration fabric has emerged that can federate identity stores to derive one consolidated view spanning distributed sources virtually.

This virtual identity platform helps consolidate identities across sources without needing migration or replication burdens:

- ***It federates stores at a virtual identity layer rather than physically moving stores***
- ***Provides consolidated identity governance while retaining data residency***

Essentially, this integration fabric offers a purpose-built access governance system fitting complex legacy constraints.

The Uniform Identity Vision

Golden Profile Vision Across Environments

The ideal vision is a 'Golden Profile' consolidating attributes into a centralized source of truth for each identity entity. The underlying platform homogenizes the divergent representations of users and entitlements from disparate stores onto shared virtual profiles. The integration layer federates ongoing updates to propagate changes to dependent systems smoothly. Such unified, auto synced profiles eliminate risks from duplication and fragmentation while boosting agility.

Secure Identity Governance Use Cases

Some compelling use cases made possible for security teams with golden profiles include:

One click revocation of user access spanning integrated apps

Access certifications encompassing systems in hybrid estate

Unified reports covering access risks across identity fabric

This allows CISOs to govern the expanded digital attack surface from one dashboard in tandem with business needs.

Lower Total Cost Shaped by Consolidation

For CFOs, consolidated identity platforms enhance IT productivity multifold. Streamlined access workflows and pruning duplicate accounts result in substantial savings from licensing and operational efficiencies. Staff no longer need to manage access in discrete systems. Convergence unlocks massive reduction in overall total spend needed for identity management.

With the unity identity vision framed, what use cases or metrics matter most to your executive team on the identity unification front?

Optimal IdM's VIS delivers a specialized identity integration platform explicitly designed to connect disjointed identity stores.

Bridging The Identity Divide with The Virtual Identity Server

As elaborated earlier, the limitations of existing identity tools in managing access across fragmented landscapes are apparent. A purpose-built virtualization fabric helps fill this gap specifically.

Optimal IdM's Virtual Identity Server (VIS) delivers a specialized identity integration platform explicitly designed to connect disjointed identity stores. VIS provides the tailor-made bridge for streamlined access governance across distributed user stores, applications and policies.

Here are several reasons that make VIS the platform uniquely capable of helping your business conquer disconnected identity chaos and associated risks amplified in complex hybrid environments.

Purpose Built for Application Consolidation

VIS delivers specialized identity virtualization capabilities tailored to directly consolidate identities and entitlements across application environments. Legacy tools falter at unifying access views spanning on-prem directories with modern SaaS apps or IaaS platforms. VIS federates stores at the identity layer through custom adapters uniting previously siloed sources.

Unified Real-Time View Across Stores

Via high performance identity bus, VIS proxies access requests between apps and underlying stores while retaining data residency. This allows consolidated visibility and policy enforcements across integrated fabric in near real-time without migration burdens.

Compliance Visibility, Reporting Simplicity

For auditors, VIS offers unified dashboards and controls not possible in fragmented identity estates full of blind spots. One console simplifies access reviews, anomaly detection and risk analytics across hybrid infrastructure thanks to aggregated identity data.

Flexibility Maintained Via Federation

Mergers, decommissioned apps or forgotten platforms still retain identities. Associated entitlements are challenging to map and contain for compliance needs allowing threats to linger due to identities left adrift.

The Critical Need For Identity Federation That VIS Enables

It is abundantly clear that the scattered identity landscapes within modern hybrid environments introduce tremendous business risks. Key takeaways include:

- ***Enabler for Enhanced Security***
  Consolidating identities and access governance controls protects organizations comprehensively. It eliminates blind spots hackers prey on. Automating access lifecycles enhances data and system protection.

- ***Boosts IT Productivity via Automation***
  Unified identity platforms with built-in synchronization tremendously enhances administrator productivity. It collapses overlapping tasks into standardized workflows on integrated profiles minimizing manual processes.

- ***Core for Effective Digital Initiatives***
  For enterprise digital transformation plans involving deeper ecosystem integration, identity federation is pivotal. Consolidated identity fabrics speed up partner onboarding, vendor access and M&A consolidations substantially, saving project costs.

As emerging architectures like zero trust mature, the underlying verification powered by authoritative golden sources will rely on platforms as delivered by VIS. Unified identity consolidation solves foundational access challenges needed to unlock the next frontier of enterprise security and agility goals.

Conclusion

As enterprises aggressively adopt cloud platforms and embed deeper digital integration across lines of business, distributed user stores become a norm. The resultant identity chaos poses very real threats for data security, operational agility and audit complexity.

Legacy tools prove limited in managing these heterogeneous environments with fragmented access controls. Federation of identities, without disturbing current infrastructure, emerge to be a critical capability.

The Virtual Identity Server from Optimal IdM delivers a purpose-built identity consolidation fabric tailored to the unique needs of complex hybrid IT models. It collates and synthesizes identities and entitlements into instant consolidated views - providing the foundation for next generation access policies spanning ecosystems.

For enterprises committed to enhancing security posture, improving compliance and reducing identity management costs simultaneously - platforms like VIS that create uniform identity records are pivotal. They save IT teams thousands of hours wasted reconciling attributes spread disorderly across stores.

By standardizing with a federated architecture early, you can avoid runaway identity chaos that will only exponentially snowball and handcuff enterprise goals. The time for consolidated identity access governance is now.

Contact Optimal IdM at
info@optimalidm.com or visit us at www.optimalidm.com/VIS.