Deloitte.

Digital Identity
Identity is the fabric of the digital economy

Digital transformation is reshaping identity management. When corporate networks had discernable perimeters, an organization conferred trust on a circle of known individuals by issuing user names and passwords. With that badge of trust, sitting in front of a desktop or laptop, the individual "user" could access resources.

Fast-forward to today. Consumers and employees alike expect seamless connectivity to data and services, whether those resources are neatly tucked behind corporate walls, sitting in the cloud, or—more likely—traversing multiple entities. They use devices of their choosing and have little patience for lumbering authentication. Whether they're working from an airport, filing medical claims, ordering food, sharing photos, or remotely managing their home alarm system, they expect their information to be secure. Organizations are increasingly reliant on the data they share and on their willingness to engage digitally. Failure to win trust and provide an easy user experience can be the difference between a well-performing business and a laggard. Managing identities is no longer a back office IT and compliance function—it's an essential business enablement function at the heart of the digital economy.

Managing digital identities is more complex and resource-intensive than ever. Deloitte Risk and Financial Advisory's Digital Identity services offer the feature-rich capabilities and configurability of traditional, on-premise solutions, with the agility of the cloud, leveraging our industry depth, accelerators, and track record of delivering effective identity solutions.

Digital Identity is a broad suite of managed identity services delivered via best-of-breed technologies to help manage organizations' identity governance and provisioning, identity management, privileged access management, single-sign-on, and risk-based multi-factor authentication. With licensing and hosting terms built in to the service, organizations can focus on their core business rather than managing large complex Identity and Access Management environments.

Digital Identity is designed to help you solve your identity challenges and can help reduce the potential boundaries to adoption by establishing a platform for identity innovation that helps your organization achieve its vision and frees your people to focus on what's core to your mission.

Cloud adoption has spurred cloud-based identity management platforms offered both by legacy identity and access management vendors and new entrants to the market. Cloud options replace monolithic, connector-heavy frameworks with application programming interface (API)-based architectures. They promise elastic scale, pre-built integration with other cloud applications, subscription-based pricing, and accelerated client onboarding times. They can also alleviate the staffing burden many organizations suffer trying to train and retain qualified Identity and Access Management specialists, and can save direct and indirect costs compared to on-premise solutions.

Beyond the obvious efficiency gains, though, cloud-based identity management is likely to provide better options for addressing digital identity needs of the future. Identity models themselves are becoming more user-driven, enabled by analytics that process the rich troves of data available on the internet. Federated digital identity models will become the norm for managing identities that must be shared across multiple inter-dependent organizations. Done well, a move to the cloud can help innovative organizations both improve digital identity management today, and establish a platform for future advancement.

It is tempting to hope that managed identity services will be "turnkey"; but there are limits to how much digital identity management can be commoditized. Each organization has particular challenges and requirements. Identity solutions must continue to adjust to the expanding threat landscape and changing compliance pressures.

Rather than providing business agility, most cloud-based services force clients into a multi-tenant platform with "cookie-cutter" functions that sacrifice the ability to customize and integrate with legacy applications and platforms. Providers typically offer limited integration support, placing a heavy burden on the client to manage integrations themselves, or engage professional service firms to build custom extensions and drive associated changes in supporting business and support processes.

As a result, cloud-based identity offerings can suffer from the same challenges associated with legacy enterprise Identity and Access Management: business value can be delayed for months or longer while the new platform is deployed; the organization gets locked into its vendor relationship through expensive license costs; and the burden falls to the client to staff and support many aspects of the solution.

supports your digital transformation

Digital Identity combines the rich features of today's cloud solutions without sacrificing the customizability of on-premise solutions. We accomplish this through single-tenant deployments and best-of-breed technologies in the cloud, which are tailored to each client and supported by a global team of identity management specialists who can leverage the technical depth and breadth, industry knowledge, and risk management perspective of our broader Cyber Risk Services practice.

Beside providing common baseline capabilities [see "Core service capabilities" sidebar], Digital Identity is designed to:

- Find the right mix of technology-based solutions, whether highly customizable single-tenants or demonstrated cloud/Software-as-a-Service (SaaS) offerings, while still owning the identity challenge at a business process level

- Support third-party access requirements

- Deploy at the scale, performance, and availability standards for consumer identity requirements

- Offer API-based integration for clients that wish to control the user experience

- Shape use cases to help you address your own profile of business risks and strategic business objectives

- Alleviate compliance challenges

- Provide end-to-end services to onboard you to the platform, and full integration services to extend into your environment as needed

- Utilize an agile "devSecOps" model to help evolve your deployment and rapidly adapt as new threats, standards, and business needs evolve

- Integrate with other Deloitte Risk and Financial Advisory managed service offerings to leverage digital identity data in the context of threat management, third-party risk management, and other services

- Leverage Deloitte Digital to develop highly personalized user engagement vehicles

Core service capabilities

Access certification: Automate compliance-mandated identity governance procedures to regularly certify access assigned to a user, on either a scheduled or ad-hoc basis

Access request and approval workflow: Empower an end user to request IT access not automatically granted.

Consumer identity management (business-to-consumer): Provide frictionless registration, enrollment, and access for consumers, while protecting data privacy and enforcing their data-sharing choices

Identity life cycle management: Publish user changes, such as onboarding, move/transfer, leave, and termination, to various digital identity providers, such as enterprise or cloud directories

Identity proofing: Utilizing industry-leading technology to verify and authenticate a user's identity
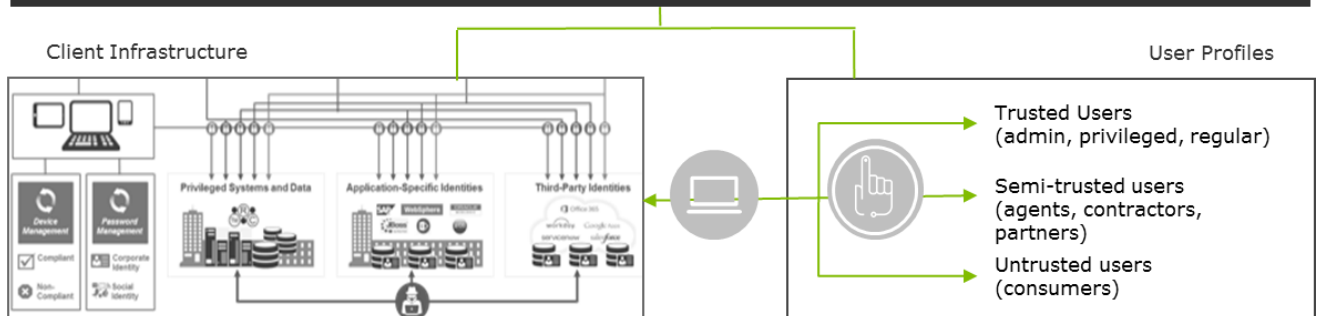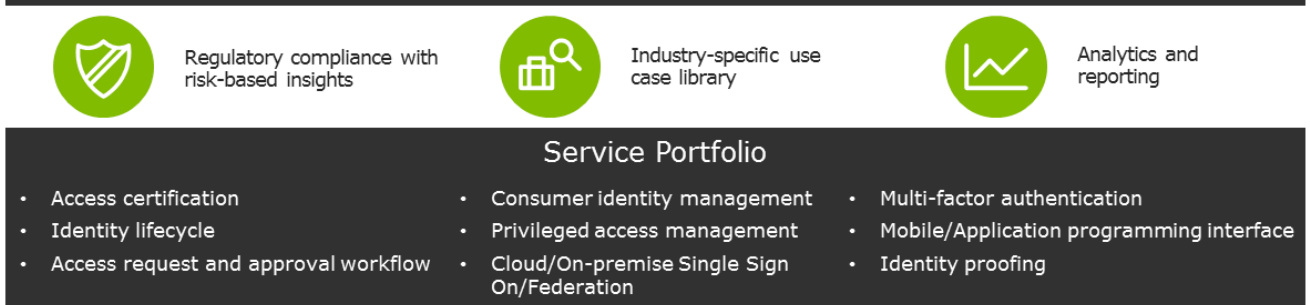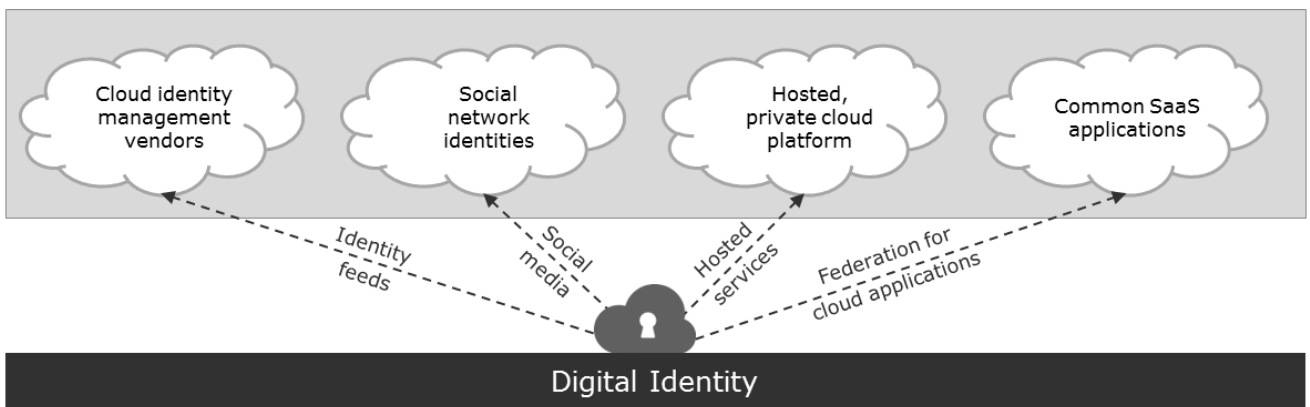
Federation (business-to-business): Help organizations and their third parties to trust identity claims and assertions, avoiding the need to manage third-party accounts, reducing duplicative end user password/profile management, and reducing multiple sign-ons

Multi-factor authentication: Help to establish more trust in an identity through hard/soft tokens and one-time passwords and passive factors, such as behavioral biometrics and device risk assessment

Privileged access management: Lock down privileged identities and sessions, reducing risks associated with lost or stolen "elevated privilege" credentials and hard-coded application passwords

Mobile and application programming interface: Manage data from desktops to devices, as the markets shifts to an API-based economy

Technology framework

Digital Identity

- Regulatory compliance with risk-based insights
- Industry-specific use case library
- Analytics and reporting

Service Portfolio

- Access certification
- Identity lifecycle
- Access request and approval workflow
- Consumer identity management
- Privileged access management
- Cloud/On-premise Single Sign On/Federation
- Multi-factor authentication
- Mobile/Application programming interface
- Identity proofing

Client Infrastructure

User Profiles

Trusted Users
(admin, privileged, regular)

Semi-trusted users
(agents, contractors, partners)

Untrusted users
(consumers)

Why choose Deloitte Risk and Financial Advisory's Digital Identity?

Achieve better digital transformation faster. We leverage our regulatory and industry-focused library of accelerators, built through years providing identity management solutions across hundreds of clients, to accelerate compliance, and help your businesses move faster, more securely.

Balance business risk and opportunity. Business can't slow down just because change creates new cyber risks. As your organization connects in new ways with customers, partners, and employees, Deloitte Risk and Financial Advisory is here to help your digital identity capabilities keep pace with business needs through business integration and process organization.

Reduce costs without compromise. Reaping the cost benefit of cloud solutions doesn't have to come at the expense of functionality. With the same features you'd expect from an on-premise solution, we support both cloud and legacy applications while freeing your in-house talent to focus on what differentiates you in the market.

Step into your own future. If you're like most organizations, your Identity and Access Management program is not where you'd like it to be. You may need help maturing supporting processes; you may be undertaking digital transformation objectives; you may be facing rapid growth or changes due to mergers and acquisitions. Wherever you're starting from, we're here to help you build a strong foundation and help you evolve to keep pace with your business of tomorrow.

Take action today! Request a briefing
Visit us at www.deloitte.com/us/cyberrisk

Deloitte Risk and Financial Advisory contacts:

Emily Mossburg
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
emossburg@deloitte.com

Michael Wyatt
Managing Director | Cyber Risk Services
Digital Identity Leader
Deloitte & Touche LLP
miwyatt@deloitte.com

Vik Bansal
Managing Director | Cyber Risk Services
Deloitte & Touche LLP
vbansal@deloitte.com

Irfan Saif
Principal | Cyber Risk Services
Deloitte & Touche LLP
isaif@deloitte.com

Secure.Vigilant.Resilient.™

To grow, streamline, and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what's most important to your organization, you must invest in cost-justified security controls to protect your most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A Secure.Vigilant.Resilient. cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

BEING SECURE means having risk focused defenses around what matters most to your mission.

BEING VIGILANT means having threat awareness to know when a compromise has occurred or may be imminent.

BEING RESILIENT means having the ability to regain ground when an incident does occur.