IDMWORKS

Identity at the Speed of Business

www.idmworks.com

IDENTITY AT THE SPEED OF BUSINESS

For the past five years, digital transformation has been at the forefront for nearly every business, from the fortune 100 to smaller family-run companies. For many, these initiatives hit hyperdrive in 2020 as businesses grappled with a digital-first engagement model dramatically accelerated by COVID-19.

- Employees went fully remote for most companies and many will never return to a full in-office experience
- Consumers moved to a near 100% digital consumption model and analysts predict much of that behavior will not change in the years to come
- All organizations large and small needed to adopt new strategies to handle the ever-changing landscape of new employee requirements, broader partnerships, and exponential growth in digital touchpoints

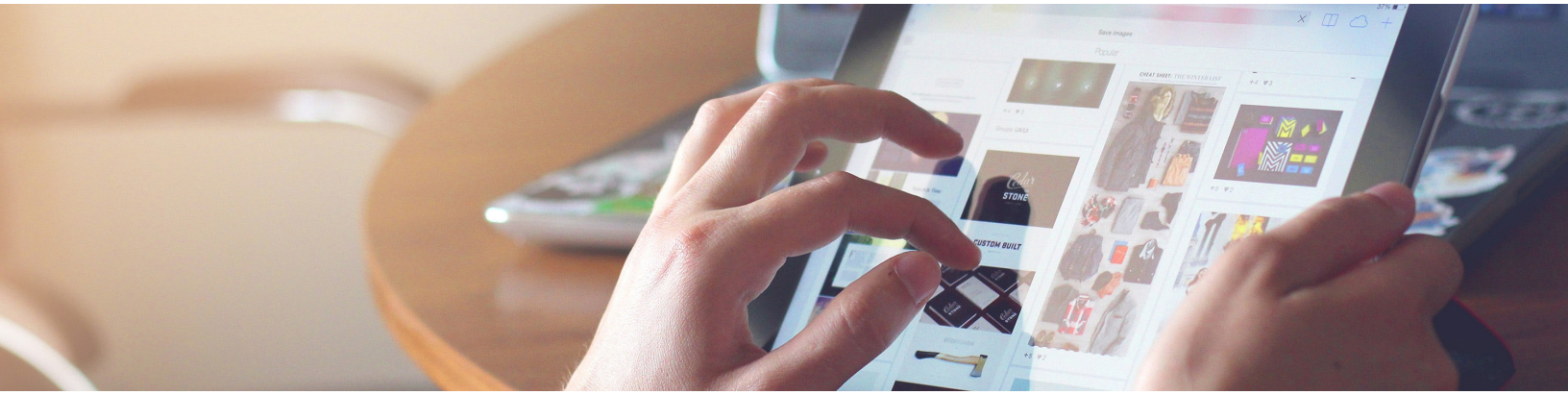
How is this central to a conversation about identity? Because a modern identity program underpins every digital interaction. The lack of a program to address internal, external, and non-human identities at many organizations exposed several weaknesses and raised questions about these companies' ability to survive and thrive in a digital-first environment. Specific areas of the challenge have included:

- The complexities of securing enabling and securing a remote workforce
- Inability to rapidly onboard and off-board employees
- Inability to execute digital customer engagement at scale (or at all)

These gaps illustrate the need for the underlying identity program necessary to support today's rapidly evolving identity and access requirements.

IDENTITY 101

In its most simplistic form, identity management ensures the right individuals have the right access to the right digital resources at any time, from any location, and on any device. Taken a step further, users need to have the ability to access the information they need via an appropriately secure method of authentication that adjusts dynamically based on the sensitivity of the resource and associated risk of access. AND if that isn't enough, you have to be able to provide forensic details that cover all aspects of every identity's interaction from the creation of that identity through its termination.



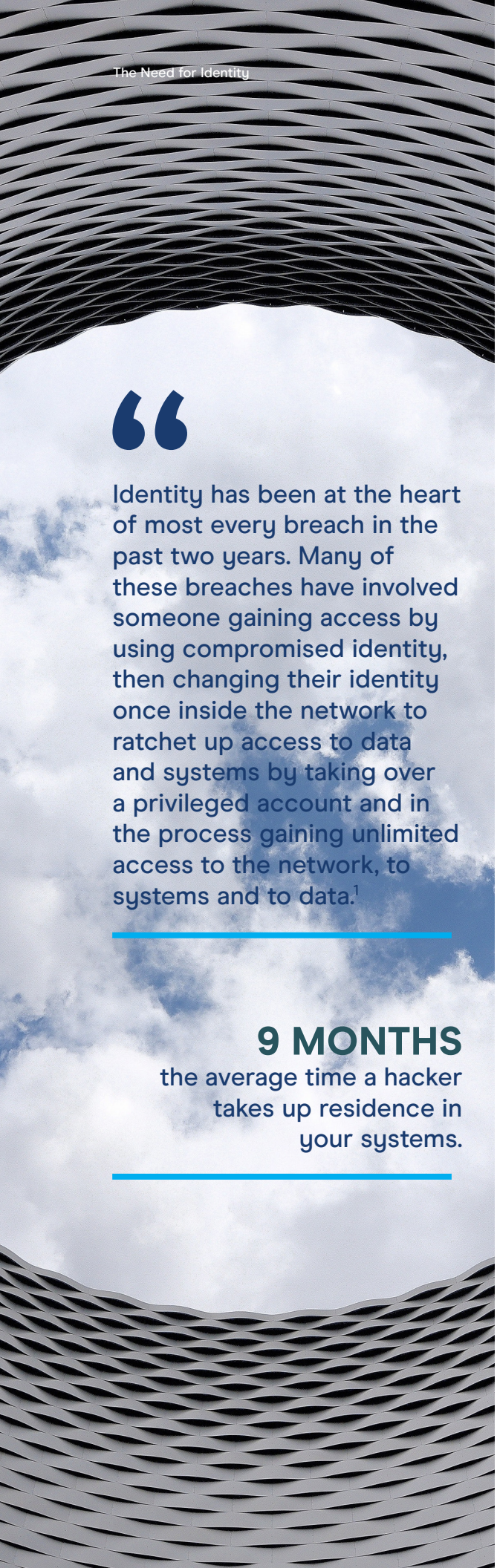
Authentication
is the process of confirming the correctness of the claimed identity.

Authorization
is the approval, permission, or empowerment for someone or something to do something.

Auditing
is an official examination or verification of accounts and records.

A comprehensive identity program will address the need to ensure appropriate access to resources across your organization's entire attack surface and meet your compliance requirements. At its core, an identity program must build a foundation addressing critical security areas including Access Management (AM), Single Sign-On (SSO), Multi-Factor Authentication (MFA), Identity Governance and Administration (IGA), and Privileged Access Management (PAM).

On its face, solving identity challenges might seem straightforward. It isn't. Beneath the surface of each core identity area, there are hundreds of tendrils of IAM functionality, often provided across several different vendors, all of which must work together seamlessly to provide the right levels of protection for your organization. Larger organizations have spent millions, if not tens of millions, trying to solve this problem.



> Identity has been at the heart of most every breach in the past two years. Many of these breaches have involved someone gaining access by using compromised identity, then changing their identity once inside the network to ratchet up access to data and systems by taking over a privileged account and in the process gaining unlimited access to the network, to systems and to data.[1]

9 MONTHS
the average time a hacker takes up residence in your systems.

THE NEED FOR IDENTITY

Why is a modern identity security practice critical? Because identity is everywhere; every digital service, every application, every connected device, every smart object has its own identity. The ability to control and audit those identities is central to security, and security is central to business growth.

Now more than ever, identity is the center point of a robust security program. IN many cases, hackers aren't really "hacking" into businesses. They're employing simple attacks or otherwise exploiting weaknesses in an identity and access management program. These weaknesses allow a bad actor the ability to log in, access critical systems and data, and potentially create additional exploits over time.

Why bother breaking a back window when a homeowner leaves the key under the fake rock next to the front door?

What does this mean?

It means that if your organization has any users (employees, partners, customers, devices) connecting to applications, you have an identity problem. A problem that is increasingly complex as the number of applications, users, and amount of data grows exponentially because you have to satisfy the growing demand for instant access to any application on any device. This is compounded by rapidly evolving regulatory mandates like CCPA, HIPAA, GDPR, PCI, and others which carry legal risk and financial penalties for non-compliance.

[1] *PwC, Global State of Information Security, Richard Kneeley, 2017*

Avoiding cyber threats isn't the only focus of an identity program. A poorly designed identity program is a security risk, but it's also a significant source of frustration for users. Without the right identity management solutions, employees can't gain access to the applications they need to do their job, partners can't work with you, and your customers can't easily access the products or services you sell. Unfortunately, many organizations have defaulted to ease access at the expense of strong security, increasing the risk of data breaches.

TechVision Research says, "Identity Management is the foundation for "real" digital transformation; the secure, flexible and adaptive IT infrastructure that every company, government agency, and institute of higher education strives to achieve." Yet industry data indicates that 75% of IAM projects deliver results that are less than expected.

Why? Because identity security is complex, it touches the whole business, and it isn't solved by a single vendor. Identity management isn't a project. Identity management is a long-term, holistic program that requires specific expertise in the unique complexities of the identity and access management market.

AT ITS BEST, THE MOST SECURE, SOPHISTICATED APPROACH TO MANAGING IDENTITIES ACTUALLY DELIVERS A BETTER USER EXPERIENCE, OFFERS MORE OPPORTUNITIES FOR DIGITAL ENGAGEMENT.

THE EVOLUTION OF IDENTITY

Over the past decade, we've seen the introduction of Cloud-Based Services, Multi-Tenancy, and variations on hosted delivery models. We've seen the move from on-premises computing to hybrid computing environments, to Cloud-Based data centers.

We've seen the introductions of hundreds of unique products and offerings to address the frustrations surrounding Identity Management. Yet all of these advances have not addressed the single most important aspect of the identity problem - how to build, implement, run, and manage an identity program that keeps pace with business needs.

In the last year, COVID transformed our behavior, as consumers and employees. We've accelerated the adoption of digital engagement by a "decade in days." This rapid change in behavior has also progressed the requirements of the ever-changing identity marketplace faster than we ever have before. There's an explosion of new IAM solution categories and vendors, changes to how traditional IAM vendors deliver their services, and continued move away from the old IAM monolithic platform approach in favor of IAM micro services-oriented solutions. The appetite for a single-stack solution is waning in favor of a compilation of best-of-breed technologies purpose-built to tackle specific subsets of IAM functionality or to solve specific use cases. But this approach creates a highly complex, expensive to buy and difficult to manage identity program. It brings us full circle back to the crux of the identity challenge.

The ability to build, implement, run, and manage an identity program is out of reach for all but the largest enterprises because successful identity programs requires:

Keeping pace with the speed of business requires identity services that are easy to consume, bring the best set of services together to match specific business needs, and evolve over time as business needs change. Simply stated, modern business requires consumable, managed identity services paired with intelligence and visibility across a holistic identity program.

[2] *McKinsey & Company, How COVID-19 is changing consumer behavior –now and forever, June 2020*

A NEW APPROACH: CONSUMABLE IDENTITY AS A SERVICE

IDMWORKS' approach is to provide a simple foundation to an identity program covering core IAM value propositions of user lifecycle management, governance, privileged access management, and access and authentication to applications & resources.

The IDMWORKS identity platform is built using industry-leading technologies delivered as a low-cost, reliable service from a cloud-based, vendor-endorsed environment that has the ability to grow from a core set of applications into a broader set of applications and endpoints over time.

IDMWORKS MIDaaS gives every organization the ability to establish a best-in-class identity program that addresses the most critical underlying use cases:

IDMWORKS MIDaaS gives every organization the ability to establish a best-in-class identity program that addresses the most critical underlying use cases:

- Identity Lifecycle (Joiner/Leaver)
- End User Access Management (SSO)
- Advanced End User Authentication (MFA)
- End User Self Service (Password and Access Request)
- Privileged Access Management (Admin Account Controls)
- Identity Governance (Recertification and Auditability)

IWith a fully managed identity program, your organization will have the flexibility to focus on your business because the underlying complexity of Identity Management is provided to you as a service. The benefits of a consumable identity program include:

- Addresses core identity use cases with minimal support from your team
- Eliminates the need to host/manage/support the system
- Delivers a fully-staffed, 24x7 identity team comprising the brightest identity experts in the industry
- Saves you the cost of highly compensated identity professionals (who are nearly impossible to find)
- Ensures an always-updated identity infrastructure (no need to manage updates, patches, or upgrades)

The potential benefits of a consumable, managed identity as a service managed services environment for IAM are no longer out of reach. The right identity partner will be with you for the long haul -- they will help you from initial assessment to your identity strategy, to selecting the right mix of vendor solutions, to implementation & day-to-day management, to benchmarking performance, and back to taking in new business requirements and evolving your program over time.

ASK THE
IAM EXPERTS

Company Address
IDMWORKS
2200 Segovia Circle
Coral Gables, FL 33134

Phone & Fax
Sales: (888) 687-0436 ext. 1
Support: (888) 687-0436 ext. 6

Online Info
Email 1: sales@idmworks.com
Website: idmworks.com

IDMWORKS