DASHLANE

Identity and Access Management 101

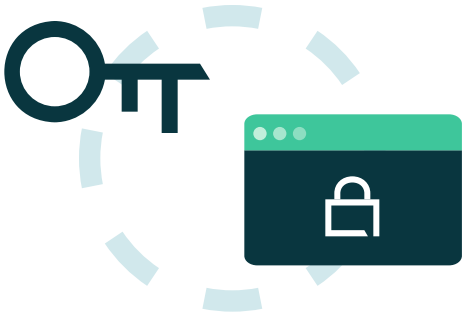
How IAM protects your data by managing user access

Assessing your cybersecurity capabilities without the right technologies is akin to measuring the size of an iceberg based on its tip.

You know you must explore the deep waters of integrated technologies, but you can see only what's above the surface. Since the COVID-19 pandemic has led to an increase in remote work, employees are now using their work credentials on personal devices and accessing work accounts from new places. What's needed is a real-time company-wide view of network connections and user activities.

Identity and Access Management (IAM) is key to achieving this kind of deep visibility. Gartner Research defines IAM as "the discipline that enables the right individuals to access the right resources at the right times for the right reasons."[1] In other words, IAM can help you flexibly—and securely—assign appropriate access to all your resources. It can also help you meet increasingly stringent compliance obligations.

With IAM, you can identify and gain insights into below-the-surface cybersecurity vulnerabilities. The technology can also help reveal emerging threats, support complex digital transformation initiatives, and strengthen compliance with new regulations and laws.



Logins are one of the most sought-after types of data, and 61% of data breaches across all sectors involve compromised credentials

Verizon, Data Breach Investigations Report, 2022

1. Gartner Research, Gartner Glossary: Identity and Access Management, accessed May 25, 2022

These capabilities aren't particularly new. What has changed is an intensified urgency to improve security in response to the COVID-19 pandemic. To combat the disease, companies sent huge swaths of employees home to work in a rapidly assembled—and often haphazardly secured—remote-work environment. As a result, there are more ways than ever before for hackers to try and access company data. Now potential targets include at-home technology like desktops, laptops, and tablets, all of which may be connected to an unsecured WiFi network.

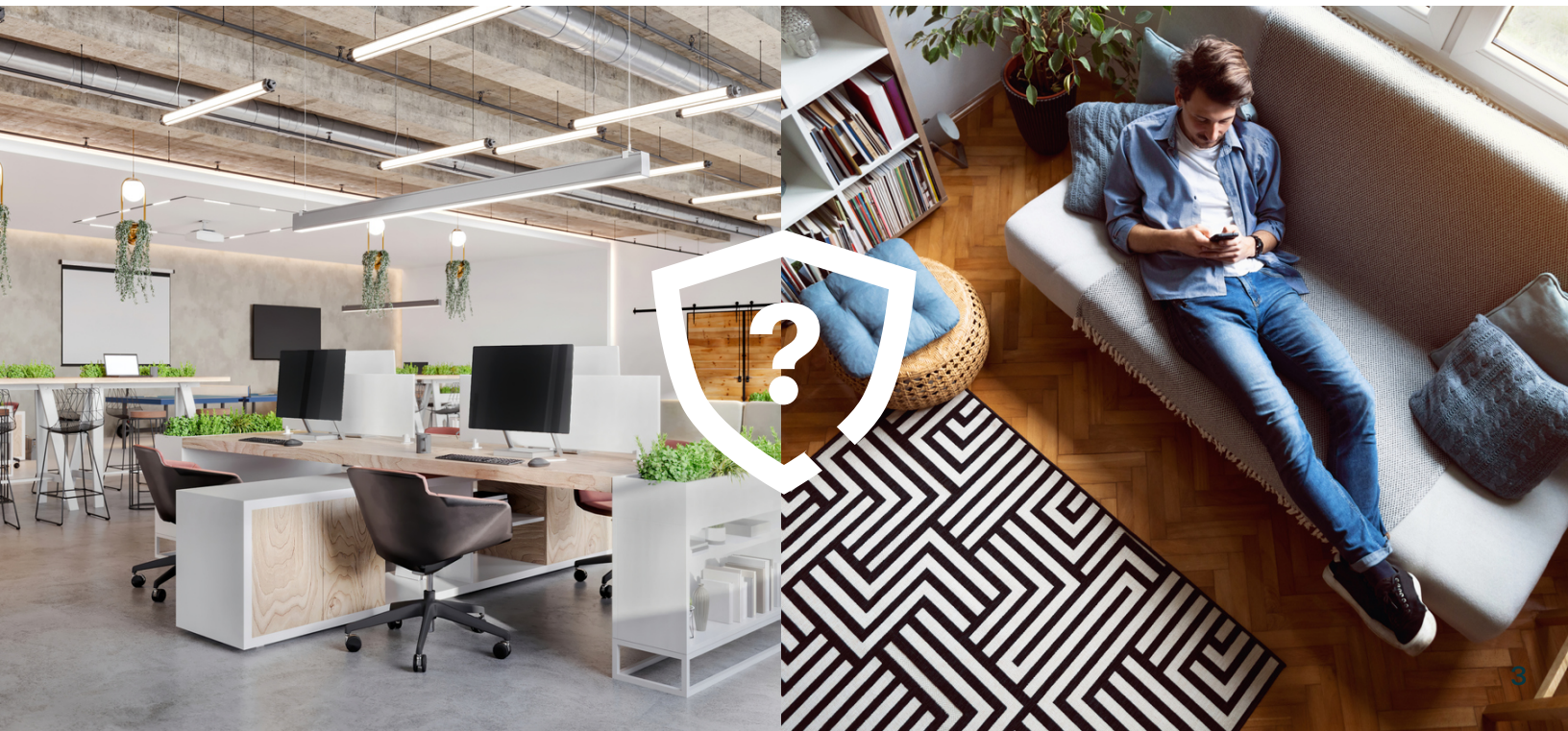
The use of personal equipment for work tasks has been multiplying for years as the bring-your-own-device (BYOD) movement went mainstream. But with the widespread COVID-19 remote-work mandates, the number of personal devices used on corporate networks has skyrocketed.

Furthermore, near-universal adoption of cloud computing and shared networks for remote access has increased the types and amount of information that businesses store, potentially putting more data at risk. At the same time, organizations must also consider regulatory legislation such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

$25.6 billion

The projected global IAM market size by 2027, a compound annual growth rate of 13.7% from 2022

ResearchAndMarkets, Identity and Access Management Market, 2022



Rising threats, rising costs

Threat actors, meanwhile, continue to lob ever-more dangerous malware over corporate firewalls.

A study conducted by IBM found that the frequency of incidents involving theft of credentials per company tripled from 1 to 3.[2]

The financial impact can be cataclysmic, particularly for smaller businesses. Median costs of incidents and breaches to businesses in 2020 were:

$7,000
for 1–9 employees

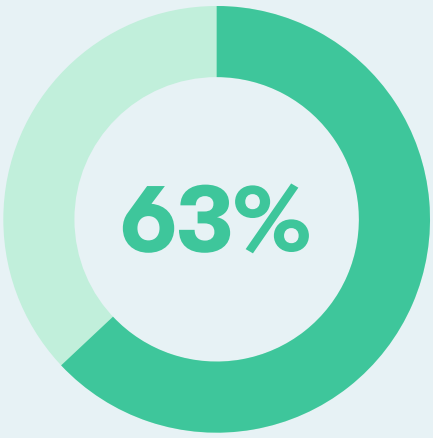
$50,000
for 50–249 employees

$17,000
for 10–49 employees

$133,000
for 250–999 employees

based on data from eight countries.[3]

Most businesses that have been breached say that the root of the problem is a lack of cybersecurity resources. Typically, this means insufficient personnel and budget, an inability to monitor for anomalous network activity, and deficient in-house security knowledge. Complicating matters, surveys show that 63% of employees reuse passwords.[4]



of employees reuse passwords across business and personal accounts

2. IBM, Cost of Insider Threats, 2020
3. Hiscox, Hiscox Cyber Readiness Report, 2022
4. Visual Objects, Employees & Cyber Defense, November 2020

Visual Objects, Cybersecurity Topics: Employees and Cyber Defense, 2020

Four primary domains of an IAM framework

An IAM framework typically encompasses four primary domains: authentication, authorization, user management, and a central user repository. Technologies like single sign-on (SSO) and multifactor authentication (MFA) are subcomponents of an IAM framework. Together, the domains and technologies provide the convenience of anytime, anywhere authentication for your teams.

1 Authentication

The employee provides credentials for access to an application or a particular resource and, once authenticated, the system creates a session. Most authentication tools include a password service that centrally maintains the user session and provides SSO for automated access to other business applications or resources.

2 Authorization

Determines whether a user has permission to access a particular resource. The system checks the resource access request against authorization policies stored in the IAM policy store. Authorization also implements role-based access control and can provide intricate access controls based on data like user attributes, actions taken, and resources requested.

3 User management

Comprises user management, password management, role/group management, and user/group provisioning. This area employs user lifecycle management throughout the lifespan of a user account and can delegate user management tasks across functional units to directly distribute workloads.

4 Central user repository

Stores and transmits identity information to other services and verifies credentials submitted from clients. The central user repository presents an aggregate or logical view of an enterprise's identities. Directory services, both meta-directory and virtual directory, can be used to manage disparate identity data from different user repositories. A meta-directory typically merges data from different identity sources into a meta-set. A virtual directory also delivers a unified Lightweight Directory Access Protocol (LDAP) view of consolidated identity information.

Taken together, these IAM features can help businesses centrally manage user roles, track activity, generate reports on that activity, and enforce policies and compliance obligations. IAM can also continually monitor connected systems to uncover suspicious behaviors that may signal cybersecurity risks and even identify incidents in progress.

Additionally, IAM can help resolve security gaps that can arise from a seemingly straightforward action, such as an employee promotion that requires a new set of access rights. If addressed manually, this update can be time-consuming and prone to human error. A modern cloud-connected system, on the other hand, automates the process and integrates changes across systems in a matter of minutes.

IAM also plays a critical role in helping streamline compliance with corporate policies and government and industry regulations: IAM creates automated, in-depth audit trails and metrics that help prove compliance and accelerate reporting.

For more information on Dashlane business plans, sign up for a trial or visit dashlane.com/business.

IAM terms you need to know

Authentication
A mechanism for the secure authentication of the identity of network clients by servers and vice versa, without presuming the operating system integrity of either.

Authorization
A process ensuring that correctly authenticated users can access only those resources for which the owner has given them approval.

Data governance
The specification of decision rights and an accountability framework to ensure the appropriate behavior in the valuation, creation, consumption, and control of data and analytics.

Directory services
Middleware that locates the correct and full network address for a mail addressee from a partial name or address. A directory service provides a naming service and extends the capabilities to include intelligent searching and location of resources in the directory structure.

Identity and access management
IAM is the discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. IAM is increasingly business-aligned, and it requires business skills, not just technical expertise.

Single sign-on (SSO)
SSO provides the capability to authenticate once, and be subsequently and automatically authenticated when accessing various target systems. It eliminates the need to separately authenticate and sign on to individual applications and systems, essentailly serving as a user surrogate between client workstations and target systems.

User provisioning
Creates, modifies, disables, and deletes user accounts and their profiles across IT infrastructure and business applications. Provisioning tools use approaches such as cloning, roles, and business rules so that businesses can automate onboarding, offboarding, and other administration workforce processes (for example, new hires, transfers, promotions, and terminations). Provisioning tools also automatically aggregate and correlate identity data from HR, CRM, email systems, and other “identity stores.”

Five benefits of IAM

If your business is driven by data—and most are—you're probably concerned about the rising cybersecurity risks to that information. IAM can help businesses protect data by automatically granting permissions, providing credentials, and using SSO for logging in to multiple applications. IAM delivers other advantages that include:

1 **Lower risk of data breaches**
With SSO and MFA, your employees no longer have to remember and type multiple passwords.

2 **Improved user experience and productivity**
Employees can securely access the applications and data they need from anywhere. This can improve the user experience and bump up productivity.

3 **Enhanced regulatory compliance**
IAM automates data access and privacy requirements by controlling who can access, use, and share data.

4 **Reduced IT costs**
IAM automates and standardizes many aspects of identity, authentication, and authorization management. It can, for instance, decrease help desk tickets for password resets and streamline onboarding and offboarding of users.

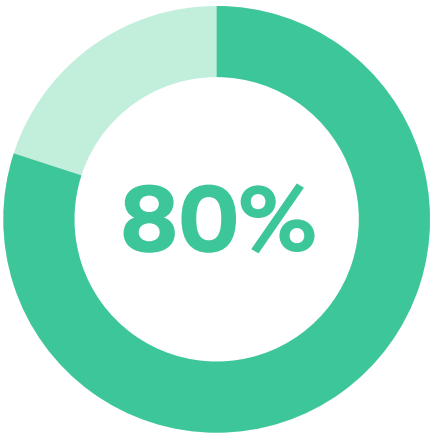
5 **Centralized management**
IAM centralizes and automates IT management, giving IT teams the flexibility to work in the office or from remote sites.

Key challenges to implementing IAM

Let's face it, IAM isn't easy to get right, nor is it a one-time technology deployment. Rather, an IAM deployment is a continuous initiative that should combine ongoing knowledge of IAM technologies with intricate planning and change-management expertise.

Many small- to medium-sized businesses (SMBs) lack the experience and financial resources needed to implement IAM. Consequently, SMBs often lag behind their larger counterparts in deployment of IAM. This disadvantage has not escaped the attention of hackers, many of whom are developing new threats that target smaller organizations.

No matter your company's head count, getting buy-in from business leaders and board members is critical to the success of an IAM initiative. Too frequently, executives dismiss IAM as "just an IT issue." In reality, a truly successful IAM program is aligned with enterprise-wide business goals and risks. As such, an IAM implementation requires not only technical expertise but also a deep understanding of business processes, operations, and regulatory obligations.

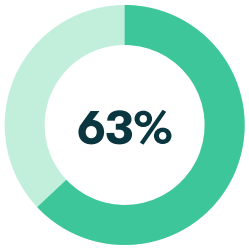


of organizations are pursuing digital innovation faster than they can improve their security practices to defend against cyberattacks

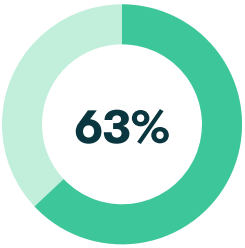
Dashlane, How to Safeguard Sensitive Data for Businesses, 2020

Finding IT employees with this knowledge can be difficult due to a global shortage of technology workers. SMBs continue to jockey for skilled, but scarce, IT security professionals. They are at a disadvantage, however, because they typically lack the deep pockets of larger companies that can pay a premium for top talent.

And then there's password security—or, more accurately, a lack thereof.



of employees are not concerned about storing their personal information on work devices.



of employees admit to using the same passwords for multiple work accounts.[5]

For more information on Dashlane business plans, sign up for a trial or visit dashlane.com/business.

5. Visual Objects, Cybersecurity Topics: Employees & Cyber Defense, 2020

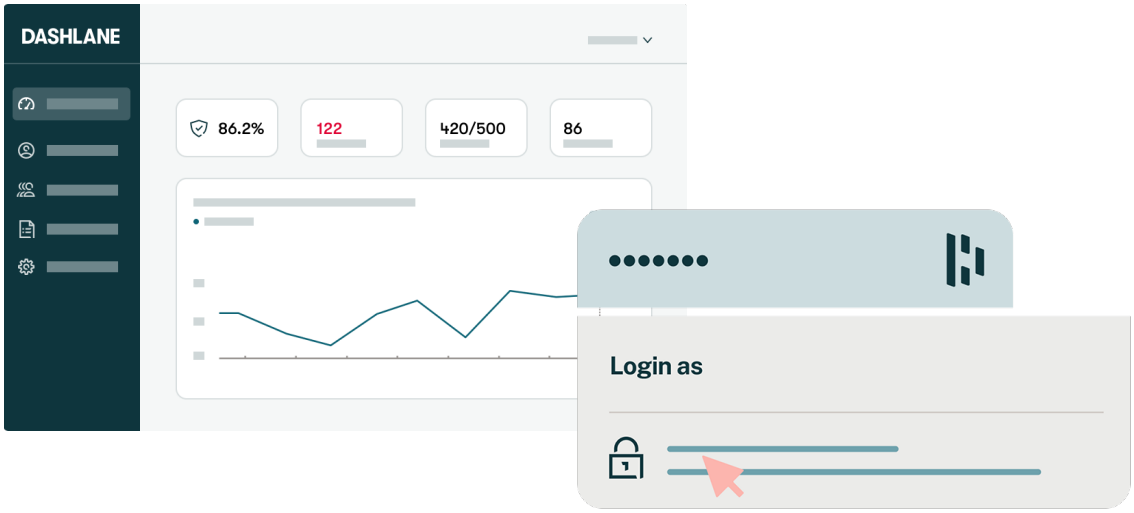
Why IAM is critical to securing your digital assets

Data is at the front and center of today's information-fueled business world.

IAM helps protect this data through an automated, integrated system that securely and remotely manages access and enterprise resources.

Digital transformation and the Internet of Things (IoT) have created a galaxy of connected physical devices that exchange data with other devices over the internet. These devices—which can range from smart-home security systems to wearable health monitors to autonomous farming equipment—may require technologies like access control and authentication to help ensure remote security. At the same time, connected devices typically require centralized remote administration because they are often scattered across multiple locations.

IAM reduces the complexities of access by combining all access policies into a unified system that provides a centralized and consistent way to manage users and accelerate adoption of new applications. IAM also significantly simplifies and automates business processes like user provisioning and account setup. The technology harnesses role-based permissions to give users the appropriate amount of access needed to efficiently do their job while keeping their business secure—the foundation for effective access control.

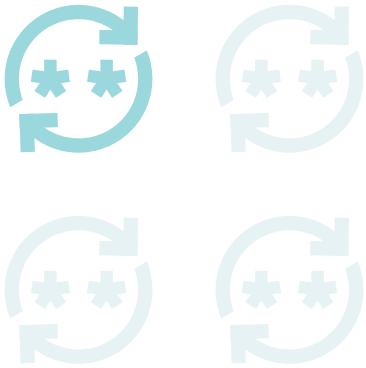


IAM gives IT administrators real-time visibility into employees' access rights and enables them to automatically adjust those rights based on changing roles or if an employee leaves the company. These automated access policies can help IT conserve time and resources, and free IT staff to work on more strategic and less repetitive security initiatives.

Centralized access rights management is one reason why businesses are opting for cloud-based IAM solutions over on-premise systems. Cloud-based solutions cost less, require fewer internal resources, and outsource security to providers that have built-in, sophisticated security capabilities.

Password managers can add new layers of protection

For many businesses, passwords represent one of the weakest links in security.



Yet only 25% of respondents to a Dashlane survey said they use an automated password management solution to keep track of their work account passwords.[6]

Password management solutions help employees generate strong, secure passwords that can be synchronized across multiple devices, whether desktop or mobile. When integrated with IAM solutions, a password manager can add new layers of protection across all accounts and cloud applications:

- A password manager can significantly improve an organization's cybersecurity by identifying and eliminating weak and reused passwords. IT gains greater visibility into all apps and services in use, including those directly installed by employees without the knowledge of IT, a practice known as shadow IT.
- Password management can enable employees to securely manage their own personal passwords.
- A password manager requires employees to remember only one password. It also simplifies tasks like generating new passwords and updating old passwords.
- A password manager can allow co-workers to securely share passwords while lessening the likelihood of a data breach.
- Password managers typically separate personal and business credentials to help make sure that employees don't leak or leave with sensitive business information and intellectual property.

6. Dashlane and Harris Poll, The State of Security in the Workplace, December 2020

IAM in action: The processes and technologies at work

An IAM solution assigns one digital identity to each individual person or a device. From there, the solution maintains, modifies, and monitors access levels and privileges through each user's access life cycle. Here's an overview of the process:

1. A system admin creates a profile in the user repository or database.
2. The admin configures the definition engine to assign roles and privileges to users.
3. IAM systems typically enable provisioning via role-based access control (RBAC) policies. Users are assigned one or more roles, usually based on job function and contextual information, and are automatically given access to applications required by those roles.
4. RBAC configurations also assign security and privacy regulations that the user must comply with.
5. The user is assigned an email address and is added to a preconfigured group, such as sales, that allows access to applications associated with that group.
6. The admin provisions the user, a process that specifies which apps and resources the user can access and what level of access the user has.
7. The user is added to a password management solution, and all attributes for the new user are securely transferred to the password manager.
8. When a user enters login credentials, their identity is checked against a database to verify that the credentials are correct.
9. The user now has automatic access to approved applications without having to sign in.
10. The IAM system begins capturing and recording user login events.
11. In the event of role changes or separation from the company, the IAM system manages the reassignment and/or removal of users' access privileges.
12. The IAM system generates reports that help organizations prove compliance with regulations, identify potential security risks, and improve IAM and security processes.

IAM should be business as usual

An effective, tailored IAM program can help you secure applications, as well as pave the path toward digital transformation. When implementing IAM, security teams should work closely with business leaders across the organization to make sure that the solution is aligned with business goals and spending priorities. Planning an IAM implementation will require a deep understanding of business and compliance processes, and not just technical expertise.

As you implement the IAM solution, anticipate unexpected issues and risks, and be prepared to reprioritize changes on the fly. The goal is to create an IAM program that can flex to accommodate the identity and access challenges of today—and tomorrow.

For many businesses, implementing a low-cost password manager represents a logical first step in securing user credentials and data.

For more information on how Dashlane can help you improve password security, read our white paper, Password Management 101: Why Passwords Are the Weak Link in Company Security.

About Dashlane

Dashlane is an advanced password manager for businesses that is as easy to use as it is secure. The award-winning solution fuses the security capabilities of IAM and password management to simplify and streamline data protection. Dashlane is built on a patented security architecture that integrates 2-factor authentication, single sign-on, and AES 256-bit encryption with powerful password management capabilities. Dashlane has empowered over 15 million users and over 20,000 companies in 180 countries to enjoy a simpler, more secure internet.

- LinkedIn
- Twitter
- Instagram
- Blog

dashlane.com

DASHLANE