What is identity and access management (IAM)?

Discover what identity and access management (IAM) is and how it keeps an organization's data and resources secure.

Explore secure access

What IAM is and what it does

Regardless of where employees are working, they need to access their organization's resources like apps, files, and data. The traditional way of doing things was to have the vast majority of workers work on-site, where company resources were kept behind a firewall. Once on-site and logged in, employees could access the things they needed.

Now, however, hybrid work is more common than ever and employees need secure access to company resources whether they're working on-site or remotely. This is where identity and access management (IAM) comes in. The organization's IT department needs a way to control what users can and can't access so that sensitive data and functions are restricted to only the people and things that need to work with them.

IAM gives secure access to company resources—like emails, databases, data, and applications—to verified entities, ideally with a bare minimum of interference. The goal is to manage access so that the right people can do their jobs and the wrong people, like hackers, are denied entry.

The need for secure access extends beyond employees working on company machines. It also includes contractors, vendors, business partners, and people working on personal devices. IAM makes sure that each person who should have access has the right level of access at the right time on the right machine. Because of this, and the role it plays in an organization's cybersecurity, IAM is a vital part of modern IT.

With an IAM system, the organization can quickly and accurately verify a person's identity and that they have the necessary permissions to use the requested resource during each access attempt.

How IAM works

There are two parts to granting secure access to an organization's resources: Identity management and access management.

Identity management checks a login attempt against an identity management database, which is an ongoing record of everyone who should have access. This information must be constantly updated as people join or leave the organization, their roles and projects change, and the organization's scope evolves.

For added security, many organizations require users to verify their identities with something called multifactor authentication (MFA). Also known as two-way verification or two-factor authentication (2FA), MFA is more secure than using a username and password alone. It adds a step to the login process where the user must verify their identity with an alternate verification method. These verification methods can include mobile phone numbers and personal email addresses. The IAM system usually sends a one-time code to the alternate verification method, which the user must enter into the login portal within a set time period.

Access management is the second half of IAM. After the IAM system has verified that the person or thing that's attempting to access a resource matches their identity, access management keeps track of which resources the person or thing has permission to access. Most organizations grant varying levels of access to resources and data and these levels are determined by factors like job title, tenure, security clearance, and project.

Granting the correct level of access after a user's identity is authenticated is called authorization. The goal of IAM systems is to make sure that authentication and authorization happen correctly and securely at every access attempt.

The importance of IAM for organizations

One reason IAM is an important part of cybersecurity is that it helps an organization's IT department strike the right balance between keeping important data and resources inaccessible to most but still accessible to some. IAM makes it possible to set controls that grant secure access to employees and devices while making it difficult or impossible for outsiders to get through.

Another reason that IAM is important is that cybercriminals are evolving their methods daily. Sophisticated attacks like phishing emails are one of the most common sources of hacking and data breaches and they target users with existing access. Without IAM, it's difficult to manage who and what has access to an organization's systems. Breaches and attacks can run rampant because not only is it difficult to see who has access, it's also difficult to revoke access from a compromised user.

While perfect protection unfortunately doesn't exist, IAM solutions are an excellent way to prevent and minimize the impact of attacks. Instead of restricting everyone's access in the event of a breach, many IAM systems are AI-enabled and capable of detecting and stopping attacks before they become bigger problems.

Benefits of IAM systems

The right IAM system brings multiple benefits to an organization.

The right access for the right people

With the ability to create and enforce centralized rules and access privileges, an IAM system makes it easier to ensure that users have access to the resources they need without making it possible for them to access sensitive information they don't need. This is known as role-based access control (RBAC). RBAC is a scalable way to restrict access to only the people who need that access to perform their role. Roles can be assigned based on a fixed set of permissions or custom settings.

Unhindered productivity

As important as security is, productivity and user experience are also important. As tempting as it might be to implement a complicated security system to prevent breaches, having multiple barriers to productivity like multiple logins and passwords is a frustrating user experience. IAM tools like single sign-on (SSO) and unified user profiles make it possible to grant secure access to employees across multiple channels like on-premises resources, cloud data, and third-party applications without multiple logins.

Protection from data breaches

as easily be hacked or shared.

Data encryption

One of the reasons IAM is so effective at elevating an organization’s security is that many IAM systems offer encryption tools. These protect sensitive information when it’s transmitted to or from the organization and features like Conditional Access enable IT administrators to set conditions such as device, location, or real-time risk information as conditions for access. This means the data is safe even in the event of a breach because the data can only be decrypted under verified conditions.

Less manual work for IT

By automating IT department tasks like helping people reset their passwords, unlock their accounts, and monitoring access logs to identify anomalies, IAM systems can save IT departments time and effort. This frees up the IT department to focus on other important tasks like implementing a Zero Trust strategy throughout the rest of the organization. IAM is essential to Zero Trust, which is a security framework built on the principles of verifying explicitly, using least privileged access, and assuming breach.

Improved collaboration and efficiency

Seamless collaboration between employees, vendors, contractors, and suppliers is essential to keeping up with the pace of modern work. IAM enables this collaboration by making sure that not only is collaboration secure, it’s also fast and easy. IT administrators can also build role-based automated workflows to speed up the permissions processes for role transfers and new hires, which saves time during onboarding.

IAM and compliance regulations

Without an IAM system, an organization must manually keep track of every single entity that has access to their systems and how and when they u that access. This makes manual audits a time-consuming, work-intensive process. IAM systems automate this process and make auditing and reporting faster and much easier. IAM systems enable organizations to demonstrate during audits that access to sensitive data is being governed properly, which is a required part of many contracts and laws.

Audits are just one part of meeting certain regulatory requirements. Many regulations, laws, and contracts require data access governance and privacy management, which are what IAMs were designed to help with.

IAM solutions make it possible to verify and manage identities, detect suspicious activity, and report incidents, all of which are necessary for meeting compliance requirements such as Know Your Customer, transaction monitoring for Suspicious Activity Reporting, and the Red Flags Rule. There are also data protection standards like General Data Protection Regulation (GDPR) in Europe and Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act in the United States that require strict security standards. Having the right IAM system in place makes it easier to meet these requirements.

IAM technologies and tools

IAM solutions integrate with a variety of technologies and tools to help make secure authentication and authorization possible on an enterprise scale:

- Security Assertion Markup Language (SAML) – SAML is what makes SSO possible. After a user has been successfully authenticated, SAML notifies other applications that the user is a verified entity. The reason SAML is important is that it works across different operating systems and machines, which makes it possible to grant secure access in a variety of contexts.
- **OpenID Connect (OIDC)** – OIDC adds an identity aspect to 0Auth 2.0, which is a framework for authorization. It sends tokens containing information about the user between the identity provider and service provider. These tokens can be encrypted and contain information about the user such as their name, email address, birthday, or photo. The tokens are easy for services and apps to use, which makes OIDC helpful for authenticating mobile games, social media, and app users.

Benefits of IAM systems

integrates with the provider so that the user has access without creating a separate account.

Implementing IAM

IAM systems affect every department and every user. Because of this, thorough planning before implementation is essential for a successful IAM solution deployment. It's helpful to start by calculating the number of users who will need access and compiling a list of the solutions, devices, applications, and services the organization uses. These lists are helpful in comparing IAM solutions to ensure they're compatible with the organization's existing IT setup.

Next, it's important to map out the different roles and situations the IAM system will need to accommodate. This framework will become the architecture of the IAM system and form the basis of the IAM documentation.

Another aspect of IAM implementation to consider is the solution's long-term roadmap. As the organization grows and expands, what the organization needs from an IAM system will shift. Planning for this growth ahead of time will ensure that the IAM solution aligns to business goals and is set up for long-term success.

IAM solutions

As the need for secure access to resources across platforms and devices grows, the importance of IAM becomes clearer and more imperative. Organizations need an effective way to manage identities and permissions at enterprise scale that facilitates collaboration and increases productivi

Implementing an IAM solution that fits into the existing IT ecosystem and uses technology like AI to help IT administrators monitor and manage ac across the entire organization is one of the best ways to fortify your organization's security posture. To learn how Microsoft can help you protect a to any app or resource, secure and verify every identity, provide only necessary access, and simplify the login process, explore Microsoft Entra and other Microsoft Security solutions.

Learn more about Microsoft Security

Microsoft Entra

Protect identities and resources with a family of multicloud identity and network access solutions

Learn more >

Azure Active Directory

Keep identities and data safe while simplifying access. Azure AD is becoming Microsoft Entra ID

Learn more >