UNITED STATES ▾

TODAY'S TOP STORIES

What is IAM? Identity and access management explained

IAM products provide IT managers with tools and technologies for controlling user access to critical information within an organization.

By David Strom

CSO |

APR 8, 2021 2:00 AM PDT

IAM Definition

Identity and access management (IAM) in enterprise IT is about defining and managing the roles and access privileges of individual network entities (users and devices) to a variety of cloud and on-premises applications. Users include customers, partners and employees; devices include computers, smartphones, routers, servers, controllers and sensors. The core objective of IAM systems is one digital identity per individual or item. Once that digital identity has been established, it must be maintained, modified and monitored throughout each user's or device's access lifecycle.

[Find out how IAM solutions from CA and Oracle compare. | Get the latest from CSO by signing up for our newsletters.]

Thus, the overarching goal of identity management is to grant access to the enterprise assets that users and devices have rights to in a given context. That includes onboarding users and systems, permission authorizations, and the offboarding of users and devices in a timely manner.

However, part of the problem are the users and their love/hate affair with their passwords. We all have too many passwords, making the temptation to share them across logins – and the resulting security implications – an issue. A Forrester survey from August 2020 found that 53% of information workers store their passwords insecurely. Another March

2021 survey of US consumers by Transmit Security found that more than half of them stopped using a website because their login process was too complex. Clearly there is work still to be done in this area.

IAM systems provide administrators with the tools and technologies to change a user's role, track user activities, create reports on those activities, and enforce policies on an ongoing basis. These systems are designed to provide a means of administering user access across an entire enterprise and to ensure compliance with corporate policies and government regulations.

"Identity has become more important since COVID has made physical boundaries irrelevant," says Andras Cser, VP and IAM analyst with Forrester Research. More businesses have moved toward remote users and have also given users outside the organization greater access to their internal systems. "With digital transformation accelerating, identity has become the cornerstone of customer acquisition, management, and retention," he says. COVID-caused disruption has surfaced weaknesses in many organizations' IAM architecture and greatly accelerated IAM evolution, according to Gartner's latest 2021 Planning Guide for IAM report. "The economy now relies on IAM."

This may be why IAM spending is up. According to a March 2021 study of more than 1,300 executives sponsored by Ping Identity, about "70% of global business executives plan to increase spending on IAM for their workforce over the next 12 months, as a continuation of remote work increases demand on IT and security teams." They also found that more than half of the companies surveyed have invested in new IAM products since the pandemic began.

How IAM works

In years past, a typical identity management system comprised four basic elements:

- A directory or identity repository of the personal data the system uses to define individual users

- A set of tools for adding, modifying and deleting that data (related to access lifecycle management)
- A system that regulates and enforces user access
- An auditing and reporting system

Regulating user access has traditionally involved authentication methods for verifying a user's or device's identity, including passwords, digital certificates, hardware and smartphone software tokens. These latter forms of tokens first emerged in 2005 and now can be found on both iOS and Android smartphones with apps from Google, Microsoft, Cisco/Duo, Authy and numerous other IAM vendors. More modern approaches include biometric elements and support for the Fast Identity Alliance (FIDO).

In today's complex compute environments, along with heightened security threats, a strong username and password doesn't cut it anymore. The most notable change has been the addition of multi-factor authentication (MFA) into IAM products. Today, identity management systems often incorporate elements of biometrics, machine learning and artificial intelligence, and risk-based authentication.

IAM's role in the organization's security stack

IAM plays a series of critical roles at several places in an organization's security "stack," but it isn't often thought of that way because these roles are spread out across different groups, such as development teams, IT infrastructure, operations managers, the legal department and so forth. "IAM teams are no longer making all the related decisions about IAM," said Gartner in its planning guide.

First, IAM techniques are just the beginning of managing a secure network. They requires companies to define their access policies, specifically outlining who has access to which data resources and applications and under which conditions they have access.

Many companies have evolved their access control policies over time, and the result is that they have overlapping rules and role definitions that are usually outdated and, in some cases, provisioned incorrectly. "You have to clean up your identities and revoke all the extra privileges that users don't need so that you don't migrate a mess," says Cser. "This means spending more time on upfront design."

Second, IAM has to connect with all parts of the business, such as integration with analytics, business intelligence, customer and partner portals, and marketing solutions. "Otherwise, IAM quickly becomes irrelevant," says Cser. Gartner recommends that IAM adopt the same continuous value delivery model that many DevOps cloud teams use to deliver their software. That isn't how many enterprise IT shops have approached IAM in the past, however.

Next, IAM goes beyond protecting users to include authenticating non-human entities such as application keys, APIs, and secrets, agents and containers. Gartner recommends making these items "first-class citizens" and says they should be managed appropriately with cross-functional teams to bring together every stakeholder. This is one area where IAM is evolving rapidly, as evidenced by the acquisition of Auth0 by Okta earlier this year.

Finally, IAM needs to be tied closely with adaptive authentication and MFA tools. Authentication used to be thought of as a binary go/no-go decision at the moment of login, such as signing into a VPN. That's old-world thinking. Today's IAM needs more granularity to prevent account takeovers and subtle phishing attacks. Gartner recommends rolling out adaptive MFA to all users and having an evolving authorization model that safely enables remote access. This both increases trust and improves overall usability, and as Gartner's planning guide states, "adaptive access is just the beginning of smarter authentication solutions. Most of these products don't have fraud detection based on passive biometric collections or support digital signatures and identity orchestrations. These protections that are needed thanks to new and more sophisticated account takeover attack methods."

What IAM means for compliance

IAM systems can bolster regulatory compliance by providing the tools to implement comprehensive security, audit and access policies. Many systems now provide features designed to ensure that an organization is in compliance.

Many governments require enterprises to care about identity management. Regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley and HIPAA hold organizations accountable for controlling access to customer and employee information. Identity management systems can help organizations comply with those regulations.

The General Data Protection Regulation (GDPR) requires strong security and user access controls. GDPR mandates that organizations safeguard the personal data and privacy of European Union citizens and businesses. Various US states have enacted similar privacy laws. To comply with these laws means you need to automate many aspects of IAM, and to ensure that your workflows, processes, access rights, and applications stay in compliance.

IAM open standards

The good and bad news about IAM is that there are numerous open standards to track and to leverage. These standards are a great starting point, but as Gartner mentions in its planning guide, organizations need to go beyond embracing particular open standards and be more nuanced about how to adopt these standards and be more effective at managing access. “For example, the IAM team should develop best practice documents on how these standards are integrated and used across all applications, devices, and users,” the guide said.

Authorization messages between trusted partners are often sent using Security Assertion Markup Language (SAML). This open specification defines an XML framework for exchanging security assertions among security authorities. SAML achieves interoperability across different vendor platforms that provide authentication and authorization services. SAML isn’t the only open-standard identity protocol, however. Others include OpenID, Web Services Trust (WS-Trust) and WS-Federation (which has corporate backing from Microsoft and IBM), and OAuth, which let a user’s account information be used by third-party services such as Facebook without exposing the password.

The biggest change in identity standards since 2013 has been the adoption of FIDO among a variety of IAM vendors, device makers and operating systems. It provides approaches for eliminating passwords entirely, using a variety of hardware security keys, biometric methods and smartphone profiles.

What are the challenges and risks of implementing IAM?

Despite IAM's presence up and down an organization's security stack, it doesn't cover everything. One issue is how users' "birthright access" policies evolve. These are the access rights that are given to new users when they begin working at a company. The options for how new employees, contractors, and partners are granted this access touch on numerous different departments, and "delegating this to the right people and managers becomes an issue," says Cser. "IAM systems should be able to detect access rights changes automatically, but they often don't."

This level of automation becomes important, particularly if we consider automated on and offboarding of users, user self-service, and continuous proof of compliance, Steve Brasen, research director at EMA, wrote in a blog post. Manually adjusting access privileges and controls for hundreds or thousands of users isn't feasible. For example, not having automated "leaving" processes (and auditing them periodically) will almost guarantee that unneeded access rights haven't been completely revoked.

You can't do this with Excel spreadsheets or other manual methods," says Cser, "but underlying complexity of user onboarding hasn't gotten any better over time, even as IAM products have gotten better at handling workflows and business processes."

Second, while zero trust networks are all the rage right now, the issue is being able to continuously monitor these trust relationships as new applications are added to a corporation's infrastructure. "We need to watch what people are doing after they login and look at behavior baselines. There are lots of false positive opportunities, such as if a user broke their finger," that can mess up these trust relationships, says Cser.

Next, the relationship of IAM and single-sign on (SSO) needs to be carefully orchestrated. According to Gartner, "The goal is to get to one integrated SSO system per user constituency that can mediate access to all of the generations of applications the organization uses. Note that this doesn't necessarily mean using one SSO tool across the entire organization."

Next, the grand unification of IAM with customer-centric IAM has begun, as witnessed by Okta's Auth0 acquisition. As long as these are seen as two separate efforts by security professionals, IAM will always be playing catch-up.

Next, IAM teams need to be conversant with multiple cloud architectures. See examples of IAM security best practices for Amazon Web Services (AWS), Google Cloud Platform and Microsoft Azure. Integrating these practices with an organization's network and applications infrastructure will be challenging and bridging the security gaps among these cloud providers won't be easy.

Finally, IT managers need to build in identity management from the start with any new applications. Cser suggests carefully selecting a target app that can be used as a template to pilot any IAM and identity governance and then expand to other apps across the enterprise.

What IAM terms should I know?

Buzzwords come and go, but a few key terms in the identity management space are worth knowing:

- **Access management:** Access management refers to the processes and technologies used to control and monitor network access. Access management features, such as authentication, authorization, trust and security auditing, are part and parcel of the top ID management systems for both on-premises and cloud-based systems.
- **Active Directory (AD):** Microsoft developed AD as a user-identity directory service for Windows domain networks. Though proprietary, AD is included in the Windows Server operating system and is thus widely deployed.
- **Biometric authentication:** A security process for authenticating users that relies upon the user's unique characteristics. Biometric authentication technologies include fingerprint sensors, iris and retina scanning, and facial recognition.
- **Context-aware network access control:** Context-aware network access control is a policy-based method of granting access to network resources according to the

current context of the user seeking access. For example, a user attempting to authenticate from an IP address that hasn't been whitelisted would be blocked.

- **Credential:** An identifier employed by the user to gain access to a network such as the user's password, public key infrastructure (PKI) certificate, or biometric information (fingerprint, iris scan).
- **De-provisioning:** The process of removing an identity from an ID repository and terminating access privileges.
- **Digital identity:** The ID itself, including the description of the user and his/her/its access privileges. ("Its" because an endpoint, such as a laptop or smartphone, can have its own digital identity.)
- **Entitlement:** The set of attributes that specify the access rights and privileges of an authenticated security principal.
- **Identity as a Service (IDaaS):** Cloud-based IDaaS offers identity and access management functionality to an organization's systems that reside on-premises and/or in the cloud.
- **Identity lifecycle management:** Similar to access lifecycle management, the term refers to the entire set of processes and technologies for maintaining and updating digital identities. Identity lifecycle management includes identity synchronization, provisioning, de-provisioning, and the ongoing management of user attributes, credentials and entitlements.
- **Identity synchronization:** The process of ensuring that multiple identity stores—say, the result of an acquisition—contain consistent data for a given digital ID.
- **Lightweight Directory Access Protocol (LDAP):** LDAP is open standards-based protocol for managing and accessing a distributed directory service, such as Microsoft's AD
- **Multi-factor authentication (MFA):** MFA is when more than just a single factor, such as a user name and password, is required for authentication to a network or system. At least one additional step is also required, such as receiving a code sent via SMS to

a smartphone, inserting a smart card or USB stick, or satisfying a biometric authentication requirement, such as a fingerprint scan.

- **Password reset:** In this context, it’s a feature of an ID management system that allows users to re-establish their own passwords, relieving the administrators of the job and cutting support calls. The reset application is often accessed by the user through a browser. The application asks for a secret word or a set of questions to verify the user’s identity.

- **Privileged account management**: This term refers to managing and auditing accounts and data access based on the privileges of the user. In general terms, because of his or her job or function, a privileged user has been granted administrative access to systems. A privileged user, for example, would be able set up and delete user accounts and roles.**Provisioning:** The process of creating identities, defining their access privileges and adding them to an ID repository.

- **Risk-based authentication (RBA):** Risk-based authentication dynamically adjusts authentication requirements based on the user’s situation at the moment authentication is attempted. For example, when users attempt to authenticate from a geographic location or IP address not previously associated with them, those users may face additional authentication requirements.

- **Security principal:** A digital identity with one or more credentials that can be authenticated and authorized to interact with the network.
- **Single sign-on (SSO):** A type of access control for multiple related but separate systems. With a single username and password, a user can access a system or systems without using different credentials.

- **User behavior analytics (UBA):** UBA technologies examine patterns of user behavior and automatically apply algorithms and analysis to detect important anomalies that may indicate potential security threats. UBA differs from other security technologies, which focus on tracking devices or security events. UBA is also sometimes grouped with entity behavior analytics and known as UEBA.

More on identity and access management:

- Microservices for IAM: container security and personal data
- What is identity management? IAM definition, uses, and solutions
- The best identity management advice right now
- What is SAML, what is it used for and how does it work?
- What is OAuth? How the open authorization framework works

Next read this

- *21 best free security tools*
- *How to rob a bank: A social engineering walkthrough*
- *8 things CISOs want to hear from XDR vendors*
- *How to write a cyberthreat report executives can really use*
- *7 most common ways to fail at DevSecOps*
- *Top cybersecurity M&A deals for 2021*
- *What's next for encryption if the RSA algorithm is broken?*

David Strom writes and speaks about security, networking and communications topics for CSO Online, Network World, Computerworld and other publications. He can be reached through his web site, or on Twitter @dstrom.

Follow 👤 🐦