Identity and Access Management (IAM) Best Practices

Identity and Access Management (IAM) has become an essential element of security plans for many organizations. To reap the most security benefits, it is imperative that companies ensure that their IAM tools and processes are set up correctly. In this article, we will share 11 identity and access management best practices your company should adopt to establish a strong security posture. By the end of this article, you'll know the next steps to take to incorporate **IAM best practices** into your security strategy.

1. Adopt a Zero Trust Approach to Security

Many companies have applications, platforms, and tools that are designed with implicit trust features. Implicit trust means that if users have access to your network or log in to a tool, the system "remembers" them and doesn't always prompt the user to verify their identity again. These lax access permissions can pose a major risk to your organization's security stance if an unauthorized entity gains access to your system via a remembered credential.

A Zero Trust security model relies on these core principles: never trust, always verify; assume breach; and apply least-privileged access. By adopting a Zero Trust model and services that work with IAM, companies can always guarantee users are who they claim to be before allowing access to company resources. This constant authentication supports IAM best practices by reducing the risk of unintentionally allowing access to unauthorized users

IAM t ogether because Zero Trust architecture ensur ollowed whenever and wherever a user need: l access management best practices. Zero Trust's foundational rule of applying least-privileged access helps define access policies, while IAM tools simplify and streamline the authentication process to allow the right access without interrupting workflows.

Curious to know how improving infrastructure access can improve your organization's bottom line? Try our Access ROI Calculator to find out!

2. Identify and Protect High-Value Data

Protecting your most valuable data involves limiting who can access it as much as possible —but, to limit access, you first need to know where your most valuable data is stored and how it is used.

Companies identify high-value assets (HVAs) — including data and the systems that house them — based on what data would pose the biggest threat to the organization if it was lost or compromised. This often includes sensitive data like confidential trade secrets or customer and employee PII. Once you've identified your high-value data, it's important to see where it's stored and what applications and tools have access to that data. These HVAs are often stored in the cloud, so it's critical to Azure, GCP, and AWS IAM best practices to keep your data secure.

From there, use access control best practices and policies to limit access to that data and deprovision access from users who don't need that data to do their daily work.

3. Enforce a Strong Password Policy

Your IAM technologies are only as strong as the identity management best practices and policies that support them. If your team is leveraging single sign-on (SSO) tools, it's critical that each user's password is strong, unique, and difficult to guess to support password and IAM best practices. Passwords must be complex enough to deter cyberattacks, frequently changed, and not used for multiple sign-on requirements.

Even if your company uses Multi-Factor Authentication (MFA) alongside SSO tools, that doesn't mean you can overlook password policies and assume your resources are protected. Instead, set up an audit schedule to regularly review user password strength and continuously make users change their passwords.

4. Use Multi-Factor Authentication (MFA)

User authentication is an essential component of effective identity and access management best practices. After all, if you can't guarantee a user is who they claim to be, you may be putting your data at risk and unintentionally allowing access to an unauthorized user.

Login credentials alone aren't enough to validate a user's identity; companies need an additional step to ensure the person logging in with those credentials is the authorized user. MFA tools simplify and automate the authentication process by requiring two or more forms of validation to confirm a user's identity.

MFA tools often use a combination of these methods to authenticate identity:

- Biometric authentication (e.g., fingerprints or facial recognition)
- Possession authentication (e.g., sending a one-time password to a user's personal device)
- Knowledge authentication (e.g., answering security questions)
- User location or time data

5. Automate Workflows

IAM tools offer IT teams many opportunities to use automation to make your organization more secure. Automation reduces manual errors, streamlines workflows, and supports compliance and governance needs.

Common tasks like creating accounts, changing passwords, and provisioning or deprovisioning access for personnel changes can easily be automated with IAM technology. These automations support best practices for access control, helping the company stay protected against insider threats when employees leave while also simplifying the transition for new employees or those transitioning into a new role.

Automation also makes it easy to log, audit, and generate reports on a regular schedule for compliance requirements. This eliminates one of the most manual tasks many IT departments commonly deal with.

Ultimately, automation helps companies cut down on help desk requests, save time and money, and better leverage the capabilities of their IAM tools.

6. Adopt The Principle of Least Privilege

One of the most common roles and permissions best practices is applying the principle of least privilege. IAM least privilege encourages organizations to restrict access and permissions as much as possible, without interfering with users' daily workflows.

Role management best practices should be used to define the minimum amount of privilege users in each role need to perform their work. In addition to this role-based access control, organizations can also leverage attribute-based access control to further define the permissions necessary across different departments. However, the goal is to regularly audit usage, reduce unnecessary standing permissions, and grant system function permissions to limit capabilities wherever possible.

It's especially important to limit administrative and change capabilities to ensure single admins don't have excessive permissions they don't need. Divide responsibilities to avoid over-provisioning access to certain people and adopt privileged access management best practices (PAM).

7. Enforce Just-in-Time Access Where Appropriate

In some circumstances, the principle of least privilege doesn't provide the necessary flexibility that certain situations require. For instance, a help desk associate may need temporary elevation of privileges to troubleshoot a customer's urgent ticket. One way to enforce identity and access management best practices, yet still support the principle of least privilege without compromising user experience, is by leveraging just-in-time access.

Time-limited access makes it easy to elevate permissions temporarily, without giving excessive authority or access to a user who may not need it regularly. These granular permissions are available with disposable or one-time-use credentials, allowing sufficient access without altering your overarching user access provisioning best practices and policies. The temporary access method is especially valuable for users outside your organization who may require periodic access to a system, like vendors or partners.

8. Leverage Both Role-Based Access Control and Attribute-Based Access Control Policies

Using role-based access control (RBAC) and attribute-based access control (ABAC) together can facilitate robust user access management best practices.

RBAC determines access based on a user's role, giving the same access to everyone called a "third-party vendor," "administrator," or "manager" based on their title. This ensures that users have the minimum privileges necessary to perform their work depending on their level. But, using RBAC alone often requires IT teams to do more manual provisioning to provide access to additional tools beyond the fundamentals, which can get challenging as a company's tech stack expands.

ABAC uses policies to define access based on filters and attributes assigned to users. For example, every employee in the marketing department may need access to a project management tool that employees in other departments don't. However, using ABAC exclusively can be unnecessarily complex when creating too many attributes to define users.

Combining RBAC and ABAC can help automate provisioning and deprovisioning as users join the company, leave the organization, or change roles. Setting up these access control policies is an essential element of IAM implementation best practices.

9. Regularly Audit Access to Resources

Even with strong policies around access control, over-provisioning remains a problem for many organizations. Auditing is one of the fundamental IAM best practices to build into your overall IAM strategy to maintain the principle of least privilege.

Organizations are constantly adding new tools and applications to their tech stack, and employees may believe they need access to all these tools to perform their work. However, as teams streamline their workflows using those tools, IT commonly finds orphaned accounts that employees aren't using. By auditing usage logs and access permissions regularly, IT teams can deprovision access and reduce their attack surface.

Limiting access is part of IAM security best practices, but the only way to consistently track what access users really need is through regular audits. Create an auditing schedule in your IAM strategy to make sure your team prioritizes this important security procedure.

10. Centralize Log Collection

Many IAM tools automatically generate logs, and these logs are valuable tools to help your team meet compliance requirements, audit usage, and strengthen IAM policies. However, not all teams think to centralize where they store their logs.

Rather than pulling logs from multiple locations, many companies store logs on the cloud for easy reference. In an increasingly hybrid work environment, storing logs on the cloud instead of on-premises is often a more convenient and affordable way to keep logs available and accessible. But, when centralizing log collection, companies must consider current cloud IAM best practices to keep valuable log data secure without limiting accessibility.

11. Adopt IAM Solutions That Work With Existing Tools

Using the right tools can make applying identity and access management industry best practices much easier for your organization. There's no need to force a round peg into a square hole; instead of making IAM solutions fit your existing tech stack, search for the right solutions that already support your existing tools and applications.

Some tools may need to be reconfigured to support IAM technology. However, IAM implementation best practices recommend that you limit how many reconfiguration projects need to be done to integrate IAM technology. Even as you search for the right tools to support your tech stack, you can start identifying and adopting user account management best practices for your organization long before you have the tools to automate it. Defining those policies early will make it easier to set up your IAM framework and systems later.

Make IAM Best Practices Standard in Your Organization

The identity and access management industry is always evolving, but there are some fundamental IAM best practices that can support your organization as your IAM strategy grows. These best practices are great ways to help you build out your IAM framework and further strengthen your security posture.

If you're wondering how to start implementing IAM within your organization, our IAM guide offers valuable information to help you get started. StrongDM can also help your organization start implementing identity and access management right away with our comprehensive Infrastructure Access Platform.

Want to see how StrongDM takes the guesswork out of your IAM implementation? Contact one of our experts today for a free no-BS demo.

by Andrew Magnusson
Director, Global Customer Engineering
StrongDM

6 min read

Last updated on:
February 23, 2023

⤓ **Get the IAM eBook PDF**

Found in:
Identity And Access Management

StrongDM manages and audits access to infrastructure.

- Role-based, attribute-based, & just-in-time access to infrastructure
- Connect any person or service to any infrastructure, anywhere
- Logging like you've never seen

Get a demo

About the Author

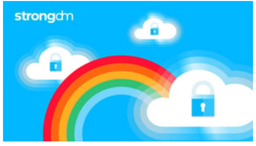
Andrew Magnusson, **Director, Global Customer Engineering,** has worked in the information security industry for 20 years on tasks ranging from firewall administration to network security monitoring. His obsession with getting people access to answers led him to publish Practical Vulnerability Management with No Starch Press in 2020. He holds a B.A. in Philosophy from Clark University, an M.A. in Philosophy from the University of Connecticut, and an M.S. in Information Management from the University of Washington. To contact Andy, visit him on LinkedIn.

♥ this post?
Then get all that StrongDM goodness, right in your inbox.

You May Also Like

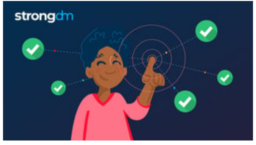
What Is SCIM Provisioning? How It Works, Benefits, and More
In this article, we will define SCIM and cover the basics of SCIM security. You'll learn what SCIM stands for, how SCIM provisioning works, and why SCIM SSO is essential. By the end of this article, you will have a clear understanding of what SCIM means and how auto-provisioning via SCIM streamlines cloud identity management, increases employee productivity, and reduces IT costs.

Top 7 Identity and Access Management (IAM) Solutions for 2023
In this article, we'll compare the top IAM solutions: StrongDM, CyberArk Identity, Okta, BeyondTrust, ManageEngine AD360, Saviynt, and Twingate. We'll explore what business needs identity and access management solutions address, and review the pros and cons of each. By the end of this article, you'll know how to choose the right IAM solution for your organization.



Cloud Data Protection: Challenges, Best Practices and More
Cloud data protection is an increasingly popular element in an organization's security strategy. In this article, we'll explore what cloud data protection is, why it's important, and the best practices to follow when migrating to the cloud. By the end of this article, you'll understand the benefits and challenges of adopting a data security strategy for cloud environments.

Centralized and Decentralized Identity Management Explained
In this article, we'll define centralized identity management and explain the difference between centralized and decentralized identity management models. We'll explore what centralized access control is, how it works, and how centralized access management handles provisioning, authentication, and authorization. By the end of the article, you'll know how to choose between centralized account management and decentralized models to prevent cybercrime and streamline provisioning workflows.



What Is Automated Provisioning? Benefits, How It Works & More
In this article, we'll explain the concept of automated provisioning and how it's used in identity and access management. You'll learn about the importance of automated provisioning in an organization's IT management and its benefits to businesses and system administrators. By the end of this article, you'll have a deep understanding of automated provisioning and how it works.