SECUREAUTH
Welcome to Better Identity.

eBook

Tackling 3 of IAM's Biggest Challenges

Technology Proliferation, Seamless Integration, and Reducing MFA Friction

Get Started

Table of Contents

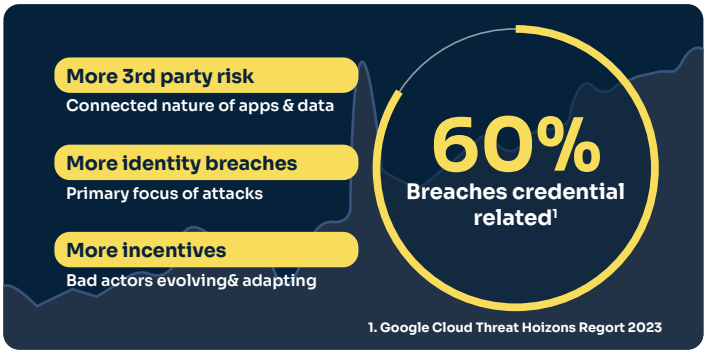
Executive Summary

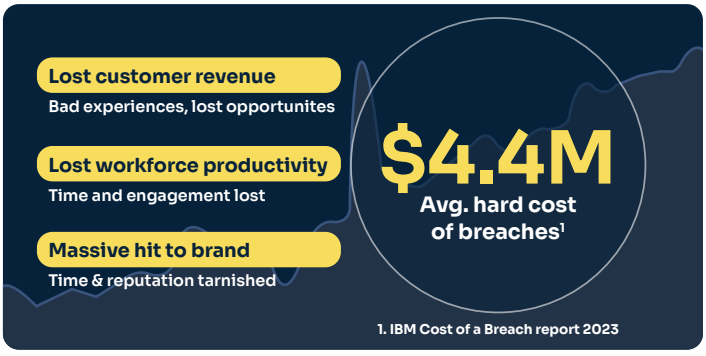
As your enterprise grows increasingly digital, securing user access to a myriad of applications and systems becomes more challenging—yet more critical—than ever. You're not just looking for security; you need a seamless user experience, too. With a growing number of devices, deployment models, and identity management systems, this task becomes more complex. To tackle these challenges head-on, you need advanced identity and access management (IAM) solutions that put both security and usability front and center. This ebook dives deep into the modern identity ecosystem and showcases SecureAuth's approach to creating a unified, secure access management system that works.

Introduction: Conquering the Identity Ecosystem

As your enterprise grows increasingly digital, securing user access to a myriad of applications and systems becomes more challenging—yet more critical—than ever. You're not just looking for security; you need a seamless user experience, too. With a growing number of devices, deployment models, and identity management systems, this task becomes more complex. To tackle these challenges head-on, you need advanced identity and access management (IAM) solutions that put both security and usability front and center. This ebook dives deep into the modern identity ecosystem and showcases SecureAuth's approach to creating a unified, secure access management system that works.

Breaches Exact a Heavy Toll...





But there's a way forward. By addressing every aspect of your IAM needs—securing and streamlining user access across all devices, deployment methods, and IAM components like Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Federation—you can create a unified experience. One where your users get secure, efficient access to what they need, no matter what's running in the background.

Understanding the IAM Landscape: Why Complexity Isn't an Option

The Pillars of Effective IAM

To secure user access while keeping things user-friendly, your IAM strategy must include these key components:

Single Sign-On (SSO)

Users log in once, accessing multiple apps without the hassle of logging in again. Simplified access means fewer credentials to remember, reducing frustration and boosting productivity.

Multi-Factor Authentication (MFA)

Adding extra layers of security—like one-time passwords or biometrics—ensures that users are who they say they are, beyond just a username and password.

Federation

Seamless access across al boundaries with a single identity, using protocols like SAML or OAuth 2.0. This is essential for cross-company collaboration.

These tools are critical for keeping your enterprise secure, but they also bring their own set of challenges—especially when you're juggling multiple protocols and technologies.

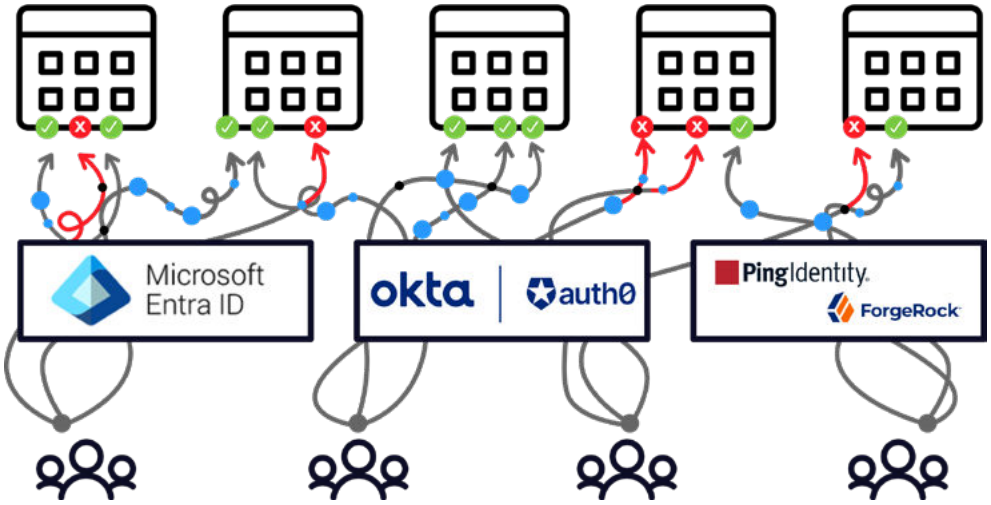
Tackling IAM's Biggest Challenges

The Strain of Technology Proliferation

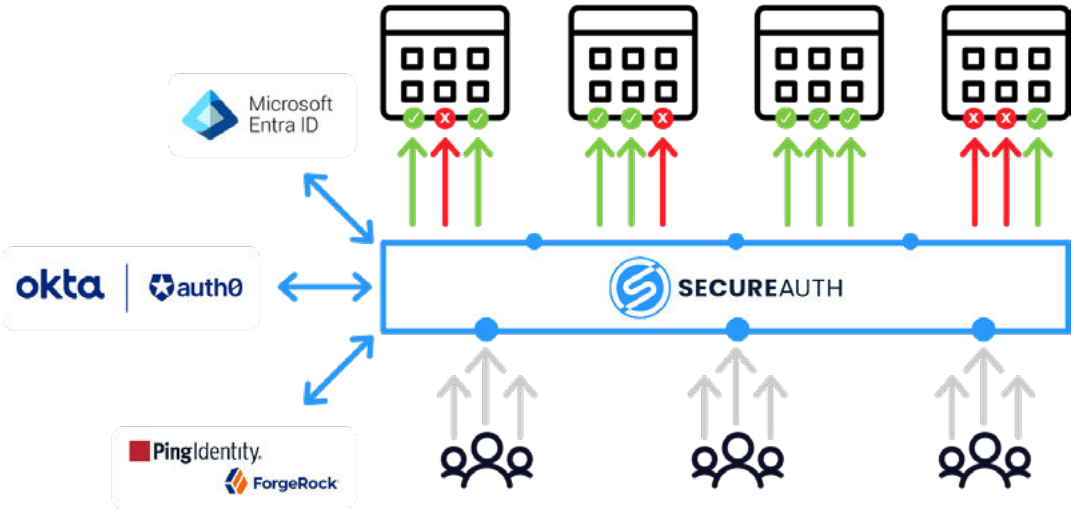
In many enterprises, the IAM landscape is a patchwork of technologies. Maybe you're using Microsoft Entra ID, Active Directory, Okta, Ping Identity, or others. Each supports different protocols, making it hard to provide a consistent user experience.

This tech sprawl leads to inconsistent security policies, fragmented user experiences, and increased costs as your IT teams struggle to manage it all. According to recent research from Forrester, today's IAM deployments are characterized by identity sprawl, creating security vulnerabilities that attackers can exploit, and gaps that hinder employee productivity.

SecureAuth offers a single, cohesive platform that ties together all the key elements of IAM—SSO, MFA, Federation, and more. The result? A simplified user experience, stronger security, and reduced IT overhead. With fewer logins and less friction, you lower the risk of security breaches and free up your IT team to focus on more strategic initiatives.



Current State of Multiple IdP Profileration



The Path to IAM Modernization

Migration and Integration: Seamless Transition, Stronger Security

Many organizations delay IAM modernization due to concerns over complexity, legacy system integration, and internal challenges. Whether it's M&A consolidation driving the complexity or technology proliferation over time, moving to a new IAM system can feel daunting, especially when consolidating multiple stacks. But sticking with a patchwork system only makes things harder to manage and secure.

SecureAuth eases the transition with a centralized portal that connects all your applications—regardless of their existing IAM systems. We'll get you into a unified system for all your employees in just weeks—no multi-year journey here.

You can migrate gradually, integrating with your legacy IAM systems during the transition. This phased approach reduces risks and ensures a smooth, disruption-free shift to a more unified, secure environment.

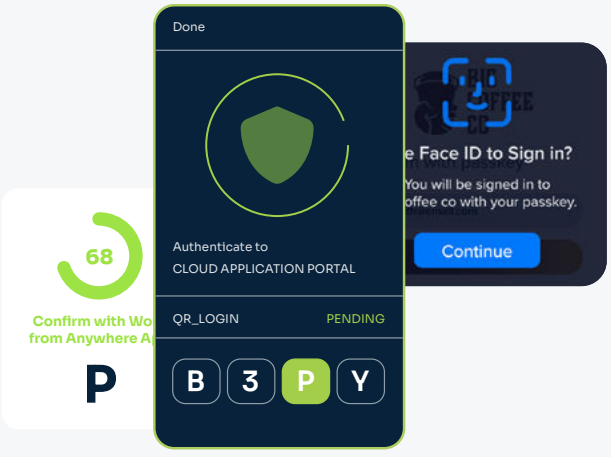
SecureAuth simplifies access and authentication, providing one portal for app access and authentication. With SecureAuth Workforce IAM solutions, you can modernize at your own pace without the "all or nothing" pressure.

Reducing MFA Friction: Security Without the Annoyance

MFA is crucial, but too many prompts can frustrate users, leading to reduced productivity and risky workarounds like password reuse. SecureAuth cuts down on unnecessary MFA prompts with an AI/ML-based risk engine that knows when MFA is truly needed. Less friction means happier users, fewer calls to the IT help desk, and overall cost savings.

Unnecessary MFA prompts can lower productivity by up to 12%

SecureAuth addresses the MFA friction challenge with adaptive and continuous authentication. This system adjusts authentication levels in real-time based on risk assessments. If a user's behavior matches their usual patterns and occurs in a trusted environment, they might not need additional verification. But if something seems off, SecureAuth steps in with stronger security measures.



Our risk engine evaluates factors like device fingerprints, geolocation, and behavioral patterns, giving you fine-tuned control over security without sacrificing user convenience.

Key Steps to IAM Excellence

Achieve a secure, frictionless user experience by transitioning to passwordless. Follow these steps for streamlined IAM success:

01 Implement SSO

Use a single set of credentials for all applications, reducing login fatigue and security risks.

02 Enable Federation

Ensure seamless access across multiple systems by integrating with other identity providers.

03 Integrate MFA

Strengthen security with multi-factor authentication, without overwhelming users.

04 Leverage Risk-Based Authentication

Dynamically assess risk with AI/ML to reduce unnecessary authentication prompts.

05 Apply Fine-Grained Authorization

Control access using role-based, attribute-based, and relationship-based models for better security.

06 Transition to Passwordless

Use biometrics or advanced methods to remove passwords entirely, improving security and user experience.

Secure, Simplified, Seamless—The Future of IAM

The digital landscape is evolving, and so must your approach to IAM. SecureAuth's unified access management solution is your key to conquering the complexities of today's identity ecosystem. By adopting advanced strategies like adaptive authentication, risk-based decision-making, and a path to passwordless access, you can protect your digital assets while offering a frictionless user experience.

The future of IAM is here. It's secure, it's seamless, and with SecureAuth, it's within your grasp.

About SecureAuth

With leading Identity and Access Management solutions from SecureAuth, organizations worldwide find it easier than ever to create digital experiences that are as welcoming as they are secure. Our AI-driven Risk Engine helps deliver dynamic – and often invisible – authentication and authorization for users, combined with a data privacy framework that protects their information and ensures their consent.

It all adds up to a virtual handshake at the digital door to your company. Making you more effective than ever at eliminating bad actors or incorrect authorizations. Keeping your employees engaged and productive. And delighting your customers so you can fuel your digital growth. Welcome to Better Identity.

Learn more at **SecureAuth.com**