Solution Brief

SecureAuth Access Management

Adaptive Authentication | Multi-factor Authentication | Single Sign-on | Self-service

Better Protection Starts with Better Intelligence

Breaches continue to litter headlines and have increased 40% annually, yet on average, organizations protect roughly 60% of their resources with multi-factor authentication (MFA). This leaves roughly 40% of their resources protected with only a password. Identity has fast become the primary security weakness at most organizations. With cyber attackers increasingly bypassing MFA, it's time to better protect your workforce and customer identities and secure the access control gap.

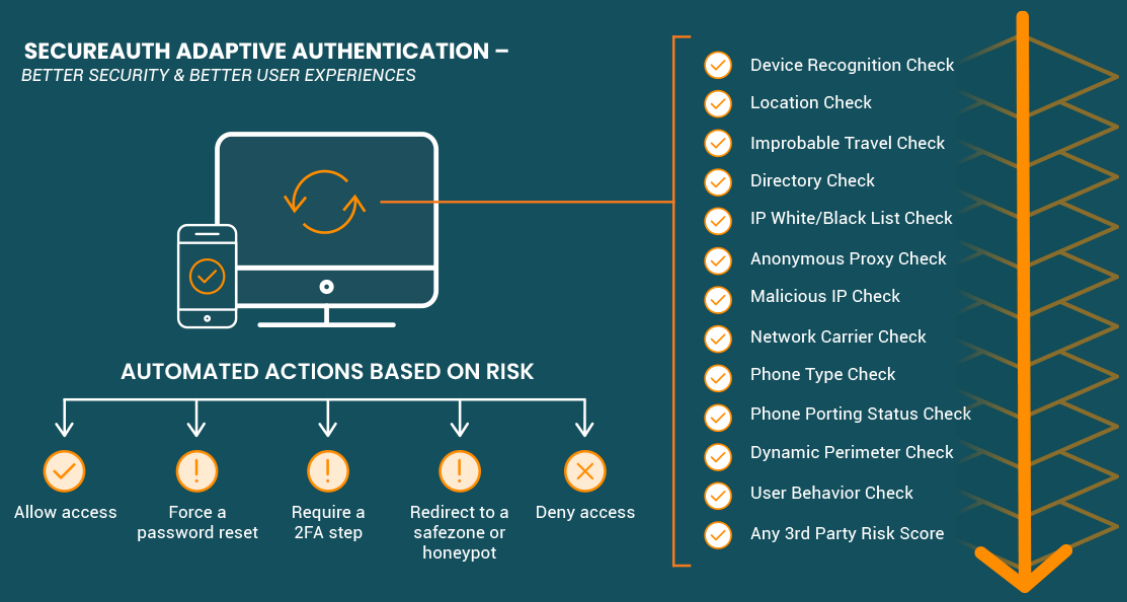
Adaptive Authentication

Build Identity Trust & Remove User Authentication Disruptions

Knowing more about the identities accessing your systems can stop attackers from gaining entry with stolen credentials and bypassing MFA. By analyzing multiple characteristics around device, location, IP address, and behavior, it becomes clear if an identity is known or unknown and the appropriate access decision can automatically ensue. For example, if you want to employ phone-based authentication it's critical to check the carrier, phone type, and porting status to ensure an attacker hasn't compromised the device. The more you know, the more you can trust and when trust is high you can safely remove authentication disruptions like MFA steps.

SecureAuth Benefits

- **Gather identity intelligence to make better access** decisions by analyzing device, location, IP address, and behavior to verity who wants access
- **Increase security without impacting users** with more pre-authentication risk checks than any other vendor
- **Deliver the right access control** with nearly 30 MFA methods to choose from
- **Tailor authentication experiences** for different user types and systems
- **Maintain productivity & reduce help desk calls** with user self-service tools
- **Improve user experience** and remove password fatigue with single sign-on
- **Optimize existing security investments** with our standards-based architecture
- **Simple administration** with reusable objects enables build once and reuse often with changes propagating automatically



Strengthen Security with Intelligence

Our cloud-based analytics and administration employs a big-data approach with machine learning to deliver the identity intelligence and risk checks required to ensure strong security and maximum usability for all your identities.

> *"The end users love the new system. When they're on premise, they don't even have to be prompted for their credentials, however if they take that same device off network, they're automatically prompted for credentials. It's really a nice solution and a lot of time people don't even realize they are using it"*
>
> — **Matt Johnson, Manager, Server Engineering, Houston Methodist Hospital**

Multi-factor Authentication

MFA is an important step in strengthening your organization's access security. With nearly 30 authentication methods ranging from mobile push notifications to desktop app generated OTPs to biometrics, the SecureAuth Identity Platform provides maximum choice. This flexibility ensures your authentication workflows are tailored to any use case, providing the right access control every time. We fit right into your environment, tying to your enterprise directories and delivering secure access for all resources — on-prem, cloud, and even homegrown applications.

User Self-service

You can't afford to tie up your helpdesk with a never-ending stream of requests or require users to wait for help. With the SecureAuth Identity Platform, you can enable your users to securely reset passwords and update their profile at any time without assistance. Users can even self-enroll devices for initial MFA roll-out. The self-service process ensures high user productivity while slashing helpdesk costs.

Calculate your savings - www2.secureauth.com/Password_Calculator

Simple Administration

Administering strong security and good user experience for your workforce and customer identities can be complex but it doesn't have to be. We provide you the flexibility to easily build, reuse, and modify security policies and settings, risk tolerances, system configurations, and user experiences. Save time by centrally modifying objects, templates, and settings and when changes are final they auto-populate globally throughout your environment.

Single Sign-on

As digital transformation continues the number of passwords users have to manage grows, impacting user experience and productivity and putting security at risk. SecureAuth SSO enables you to give each user a single set of credentials to remember and manage, streamlining secure access to on-prem, cloud, VPN, and legacy resources while eliminating stored, passed, or synced credentials. Multi-factor and adaptive authentication options ensure only authorized users can single sign-on. Time savings gained by deploying single sign-on can be significant.

SecureAuth Access Management Delivers:

- The most adaptive authentication risk checks
- Flexible authentication workflows
- Deployment freedom
- Customer self-service options
- Intelligent Identity Cloud
- The most multi-factor authentication
- A wide range of federation protocols
- Simple Administration

The intelligence dashboard delivers turn-on-and-go reporting of key metrics