Solution Brief

SECUREAUTH® IDENTITY PLATFORM

ADAPTIVE ACCESS MANAGEMENT FOR PORTAL SECURITY

Increase security without increasing user disruptions

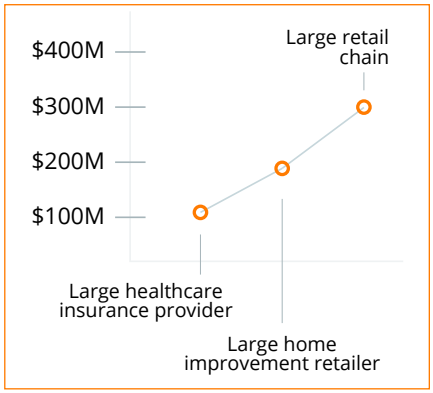
The Dilemma: Security versus User Experience

Organizations embarking on digital transformation initiatives through business and consumer portals need to provide the best possible user experience while protecting systems from unauthorized access. This can be a delicate balance. Portals are attractive to cyber criminals due to the volume of users, and breaches rose roughly 40% again last year.

For a successful outcome, the login experience must be painless for users. However, low-friction experience cannot be at the expense of security. SecureAuth is uniquely positioned to offer both frictionless user access and the strongest authentication available.

Breaches are expensive:

+ Large healthcare insurance provider has paid out $115 million.
+ Large home improvement retailer is nearing $180 million.
+ Large retail chain is close to $300 million.



The Challenges

+ Stopping attackers who are attempting to bypass two-factor authentication
+ Providing quick and painless authentication users don't mind
+ Reducing helpdesk calls - keeping visitors on the portal vs seeking IT help

Highlights

Access Protection

+ Improve portal protection beyond just a password with 25+ MFA methods
+ Protect beyond MFA with risk checks around device, location, IP address, & behavior
+ Secure access for all users — customers, partners, employees

User Experience

+ Tailor the authentication process to different user types and risk levels
+ Eliminate MFA steps for low-risk access requests

More than Authentication

+ Simplify access and remove password fatigue with single sign-on (SSO)
+ Enable 24/7 support and reduce helpdesk calls with self-service tools
+ Choose hybrid, on-prem, or cloud deployment

Greatest Portal Security and User Experience Together

The SecureAuth® Identity Platform uniquely offers the best of both worlds — the industry's best identity security AND a great user experience. Multiple pre-authentication risk checks around device, location, IP address, and user behavior coupled with nearly 30 multi-factor authentication (MFA) methods provide a layered defense system that is nearly impossible to penetrate, even with stolen credentials and ways past certain MFA methods.

Instead of constantly interrupting users for a MFA step, adaptive authentication enables you to allow access for low-risk requests without MFA, require MFA for medium risk, and deny or force a password reset for high risk — ensuring the most user-friendly authentication experience. 90% of the time SecureAuth users are not required to take an MFA step.

Protection You Need... Usability Users Want

- Device Recognition Check
- Location Check
- Improbable Travel Check
- Directory Check
- IP White/Black List Check
- Anonymous Proxy Check
- Malicious IP Check
- Network Carrier Check
- Phone Type Check
- Phone Porting Status Check
- Dynamic Perimeter Check
- User Behavior Check
- Any 3rd Party Risk Score

Industry's most pre-authentication risk checks elevate access security

Greatest Identity Protection

Multi-Factor Authentication
Nearly 30 supported methods = user choices

Adaptive Authentication
More pre-authentication risk checks than any other vendor

Threat Detection
Pinpoint real threats vs. false positives

Greatest User Experience

No Risk = No MFA Step
Require an MFA step only if risk is present

Single Sign-On
Reduce the password burden

User Self-Service
Reset passwords, unlock accounts, enroll devices without IT involved

Customer Portal | Partner Portal | Employee Portal

Greatest Access Protection

Protection in layers = Greatest identity confidence

The reality is that attackers can use real-time phishing, malware, text & voice call interception, phone fraud, and more to bypass MFA today. Adaptive Authentication adds a protective barrier by analyzing characteristics around device, location, IP address, and behavior for risk. Detecting threats across multiple vectors ensures you can easily identify legitimate users while denying attackers — even those with stolen credentials and ways around MFA.

Greatest User Experience

Only disrupt users if risk is present

Instead of interrupting users at every access point for an MFA step, you can remove authentication disruptions when trust is high. Recognize the device, location, IP address and behavior, why force an MFA interruption? Of the 617 million authentications SecureAuth processed last year, 90% did NOT have to take an MFA step because little to no risk was present. With a large group of users accessing your portal, single sign-on ensures users can move easily among multiple apps, and self-service capabilities improve productivity while minimizing helpdesk costs.

The stakes are high - if interacting with your portal is not easy, users will switch to alternatives, resulting in lost revenue. The SecureAuth Identity Platform uniquely delivers the right blend of security, user experience, and user self-service options to ensure the right balance for your portal project.

Learn more about how The SecureAuth Identity Platform can help — visit
www.secureauth.com/solutions/use-cases/portal-security