Solution Brief

Move Beyond Two-Factor Authentication

2FA is not enough to secure today's modern organization

Highlights

Complete Identity Protection

+ Improve protection beyond just a password with 25+ MFA methods
+ Protect beyond MFA with the industry's most pre-authentication risk checks
+ Stop attackers with stolen credentials and innovative ways to defeat MFA methods

User Approved Experience

+ Only require an MFA step if risk present
+ Empower users to go Passwordless with high identity confidence
+ Reduce authentication time further with single sign-on
+ Tailor the authentication process to different users and resources

More Than Authentication

+ Remove password fatigue with single sign-on (SSO) across on-prem, cloud, and homegrown resources
+ Improve productivity and reduce helpdesk costs with self-service password reset and MFA enrollment
+ Deploy on-premises, in the cloud, or a hybrid of the two

Attackers can Bypass Popular Two-Factor Authentication Methods

Two-factor authentication (2FA) is a great first step toward better identity and access security. 2FA is definitely an improvement over password-only authentication. The problem is, 99% believe 2FA is the best way to protect identities and access. Yet, knowledge based Q&A can easily be social engineered, hard tokens have been compromised in the past, popular push notifications have been routinely falsely accepted, and one time passcodes delivered via SMS/text can be spoofed. Attackers are only going to evolve and learn to defeat more 2FA methods. Organizations need additional security layers, but don't want to cause daily disruptions and annoyance among their user populations.

99% 99% of IT decision makers think 2FA is the best way to protect identities

42% 42% of IT professionals worry 2FA will disrupt user schedules

Many 2FA methods can be bypassed by attackers

OTP via SMS/email	Phone fraud is on the rise
Tokens	High cost, Low UX; compromised in the past
Knowledge Based Questions	Easily phished or found on social media
Push-to-accept	User conditioned to accept when not authenticating

The Challenges

+ On average, 44% of assets are only protected by a password
+ 81% of 2016 data breaches involved the use of weak or stolen credentials[1]
+ Perception that 2FA alone provides near impenetrable protection
+ Users hate authentication disruptions

Supplement 2FA Protection AND Improve User Convenience

SecureAuth + Core Security offers 25+ multi-factor authentication (MFA) options to match your use case, providing protection beyond passwords alone. Because attackers can bypass some 2FA methods, SecureAuth provides multiple pre-authentication risk checks that provide context to any access request, checking things like device recognition, IP reputation via multiple threat services, geographic location, behavioral biometrics, and phone number fraud (to name just a few). This adaptive authentication runs behind the scenes for seamless access and ensures you can easily identify legitimate access while denying attackers — even those using stolen credentials and innovative ways to defeat MFA methods.

1 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

"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

Maximum Security and Usability

Protection in layers = Greatest identity confidence
2FA alone is not enough. Adaptive authentication is an additional safety net that does not inhibit the daily routine of users and is nearly impossible for attackers to bypass. Additionally, the threat data collected via multiple risk checks can be shared with the SIEM or SOC for correlation with other organizational threat data to pinpoint genuine threats in a sea of alerts and potential problems.

Users Only disrupted if Risk Present
Instead of interrupting users for a 2FA step at every access request, adaptive authentication enables you to allow access for low risk requests without an 2FA step, require 2FA for medium risk, and deny or redirect for high risk — delivering the most user-friendly authentication experience.organizational threat data to pinpoint genuine threats in a sea of alerts and potential problems.

Eliminate Passwords from Authentication

With 25+ authentication methods ranging from SMS to telephony to email to push notification and more, coupled with adaptive authentication risk checks, SecureAuth + Core Security can uniquely provide the confidence to eliminate the password from the authentication process. Users will love that they no longer have to remember, change, and enter passwords. You are thrilled that users can't write down, unknowingly share, or be phished out of their credentials. Imagine the helpdesk call reduction and cost savings too.

Enhance User Convenience with Single Sign-On

The number of passwords users have to manage grows daily, putting security at risk. SecureAuth + Core Security enables you to give each user a single set of credentials to remember, streamlining secure access to on-premises, mobile, cloud, VPN, and legacy resources while eliminating stored, passed, or synced credentials. If the identity is compromised, adaptive authentication ensures the attacker will be challenged with multi-factor authentication and/or denied access. Time savings with single sign-on and passwordless authentication can be significant.

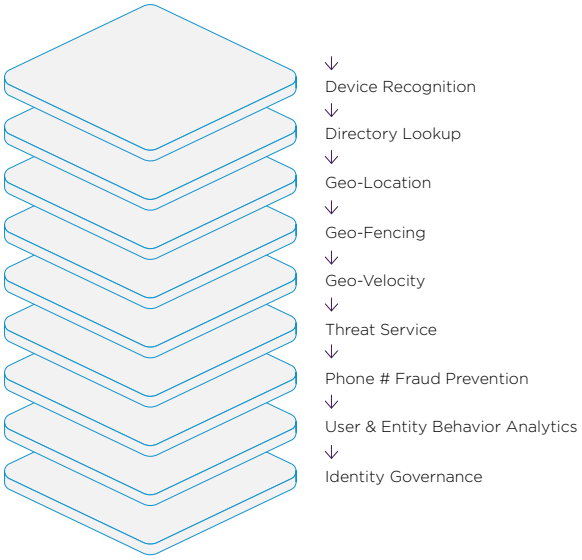
Calculate your savings with our online calculator -
www2.secureauth.com/SSO_Calculator

Reduce IT Workload with User Self Service

You cannot afford to tie up your helpdesk with a never-ending stream of requests to reset passwords and unlock accounts, or to idle valuable employees while they wait for access to job-needed resources. With SecureAuth + Core Security, you can enable your users to securely reset their own passwords and unlock their own accounts at any time without assistance from the helpdesk. Users can even self-enroll for initial multi-factor authentication. The process takes less than a minute, ensuring high productivity while slashing overhead costs.

Calculate your savings with our online calculator -
www2.secureauth.com/Password_Calculator

SecureAuth adaptive authentication risk checks:



Password Reset Calculator

Step 1. Calculate Number of Help Desk Calls

Total Number of Employees:
5,000
(Editable Field)

Average Number of Help Desk Calls Per Employee, Per Year:
12
(Editable Field: META Group estimates 1.75 calls/month or 21/year per user)

Average Number of Help Desk Calls Per Year:
60,000

Step 2. Calculate Number of Password Reset Calls

Percentage of Help Desk Password Reset Calls:
30 %
(Editable Field: Gartner estimates 20-50% of all calls are for password resets)

Total Number of Password Reset Calls Per Year:
18,000

Step 3. Estimated Cost Per Password Reset Call

$ 35.00
(Editable Field: Cost estimates typically fall between $15-$70 per call)

Annual Password Reset Call Cost Savings: $630,000