Solution Brief

Passwordless Authentication

SecureAuth's Solution to a Passwordless Organization

SECUREAUTH

The password has long been a thorn in the side of users and organizations alike, and it is also the root of many serious and costly problems. According to Verizon's 2016 Data Breach Investigations Report (DBIR), weak, default, or stolen credentials were involved in 63% of confirmed data breaches, including the large, highly publicized breaches at LinkedIn, Home Depot, and Target. To improve security, organizations often require stronger password complexity and more frequent changes, but this often leads to poor user security practices, such as writing passwords down or using the same password for multiple applications, and increased costs because users forget their passwords and have to call the helpdesk for resets. Organizations also lose productivity when users use passwords to log in separately to multiple applications each day to do their jobs. Many organizations feel they have to sacrifice security for user convenience, but SecureAuth has a unique solution. Welcome to the passwordless era.

Benefits

+ Compromised credentials are useless to attackers
+ Less daily disruptions for users
+ Greater protection than password + 2FA
+ No passwords means no time-consuming and costly password reset calls
+ Less time spent logging in leads to more productivity
+ Infinite workflows create a tailored experience for users

What would you trust more?
A human generated password OR a combination of biometric + push-to accept + risk analysis?

Protecting Identities without Requiring a Password

A Better User Experience

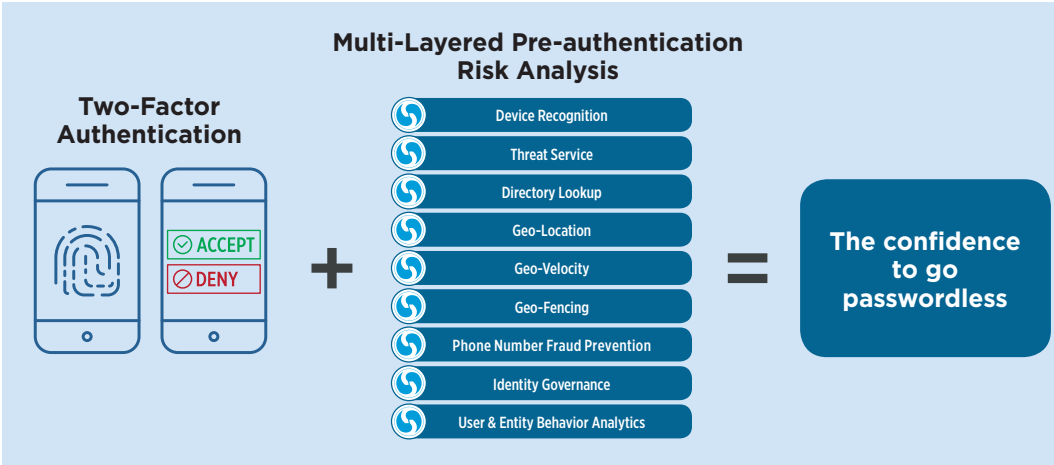
Imagine how happy users will be when they don't have a password to remember, change, enter over and over, or mistakenly give to attackers!
No password combined with the convenience of single sign-on (SSO) means users authenticate just once a day with a username & a quick fingerprint biometric coupled with a two-factor authentication (2FA) method like Push-to-Accept.

Security in Layers = Greatest Identity Confidence

2FA alone may not provide the protection and identity confidence organizations need. In addition to 2FA, SecureAuth offers Adaptive Authentication, which acts like a protective barrier, analyzing every access request for anomalies.

Cost Savings & Productivity Gains

You could see a 30% or larger drop in helpdesk calls, because users who don't have passwords never need password resets. Additionally, removing the password can generate significant labor cost savings: Saving each user just 3 minutes a day by not having to repeatedly enter passwords to access resources can make a significant impact on productivity over the course of a year.



SecureAuth Corporation **Tel:** + 1 949-777-6959 www.secureauth.com

Password + 2FA is NOT Enough

Supplementing a username and password with 2FA can provide a false sense of security. Knowledge-based questions and answers (KBAs) can be socially engineered fairly easily with the wealth of personal information publicly available via social media. One-time passcodes (OTPs) delivered via SMS/text or email can be intercepted, and in fact, the National Institute for Standards and Technology (NIST) no longer recommends SMS/text-based OTPs because of security flaws. RSA and Gemalto hard tokens have been compromised by attackers in the past. Therefore, security-conscious organizations need to look beyond 2FA for access control and protection against cyber attacks.

Security in Layers = Greatest Identity Confidence

Multi-Layered Risk Analysis

Pre-authentication risk checks provide the confidence to go passwordless.

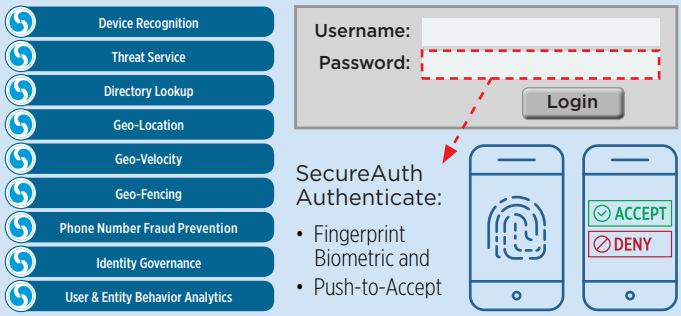
Layered risk checks provide a protective barrier against attacks

Instead of interrupting every user for multifactor authentication, SecureAuth silently makes multiple pre-authentication risk checks — such as device recognition, IP reputation, threat intelligence, geo-location, and geo-velocity — and requires another factor only when sufficient risk is present. The risk level can be tailored to the type of user; for example, you can apply more scrutiny to remote users and anyone who has access to sensitive resources. This super strong security streamlines legitimate access while blocking attackers, even those using stolen valid credentials.

How Does Passwordless Work?

SecureAuth replaces the password with a fingerprint biometric to secure our SecureAuth Authenticate mobile app, and requires a Push-to-Accept 2FA step. Combine this with our multilayer adaptive authentication risk checks, and you can identify your identities with confidence — without a password.

Passwordless Authentication



Cost of the Password

No Password = No Password Reset Calls

Most industry leaders agree that 20–50% of helpdesk calls are for password resets and each call costs in the range of $15–$70. If an organization has 5,000 users, each user makes one password reset call per year, and 50% of those users need to make a second password reset call, there are 7,500 calls each year. If each call costs $40, the organization spends $300,000 per year on password reset calls! Going passwordless eliminates those calls and therefore those costs.

Calculate your savings at www2.secureauth.com/Password_Calculator

Labor Cost Saving and Productivity Gains

Eliminating passwords and gaining SSO and self-service tools can easily save each user three minutes a day – which adds up to millions of dollars in labor cost saving. Saving 3 minutes a day on each of the 240 working days in a year equals a 12-hour savings per user per year. At an average employee cost of $40/hour, the organization could save $480/year/user. Multiply $480 by the number of users (5,000) and our sample organization gets a labor cost savings of $2,400,000!

Calculate your savings at www2.secureauth.com/Password_Calculator

Ready to go passwordless?

Visit secureauth.com and talk to a product expert or request a demo to see it live.