SECUREAUTH

Making Passwordless Possible

How SecureAuth is eliminating passwords while improving security and user experience

Table of Contents

SECUREAUTH

Abstract

What do the breaches at Target, LinkedIn, and Home Depot have in common? Compromised passwords.

In fact, compromised passwords and credentials were used in nearly two thirds of reported data breaches in 2015. What's more, it is painful for users and drives up helpdesk costs. Trying to shore up passwords by adding a second factor, such as Knowledge-based answers (KBAs), One-time passcodes (OTPs) via Text/SMS, and hardware tokens, can significantly increase the burden on users and your budget, but cannot deliver the security needed against modern cyber threats.

The time has come to say farewell to the password. Fortunately, there is a better way. This technical brief explores how to finally implement secure passwordless authentication — while also streamlining the user experience and controlling costs.

SECUREAUTH

Introduction

The password may not be the root of all evil, but it is undeniably the root of many serious problems for organizations today. The top two drawbacks alone are sufficient reason to kill the password: the serious risk of breaches and the high costs. According to Verizon's 2016 Data Breach Investigations Report (DBIR), 63% of confirmed data breaches involved the use of weak, default, or stolen credentials. Organizations often try to mitigate this risk by implementing stronger password complexity and requiring more frequent password changes. Unfortunately, that approach does far more to increase helpdesk costs and user frustration than it does to actually improve security.

With No Password, There Are No Password Resets

If we take a typical 5000 user organization and assume one helpdesk call per user per month, so 12 calls a year. That means 60,000 helpdesk calls a year. Let's assume 30% of those are for password resets, which means we have 18,000 password reset calls a year. Let's also assume each call costs the organization $35 (We've seen anywhere from $20 to $70), we get an annual cost for password resets at $630,000.

Calculate your savings with our Password Reset Calculator
www2.secureauth.com/Password_Calculator

Some organizations try to salvage the password by buttressing it with additional authentication factors, such as a hardware token or a one-time password (OTP) delivered by email or text/SMS. But these factors are less than ideal from a user experience perspective, and token-based authentication in particular is notorious for high costs. More important, however, is the fact that vanilla two-factor authentication simply cannot deliver the security organizations need today. For example, KBAs can easily be social engineered, and OTPs delivered to a mobile phone are vulnerable to man in the middle attacks, when phone fraud prevention techniques are not used. We have seen many well-documented cases of breaches in which OTPs were stolen from mobile devices or directly from the carrier network.

"In the midterm to long term, the combination of passive biometric authentication and contextual authentication will provide sufficient trust, without the need for a "gateway" authentication event using passwords or tokens (given some mechanism to reliably identify jailbroken or other untrustworthy endpoint devices) and perhaps without an explicit claim of identity (that is, no need to enter a user ID)."

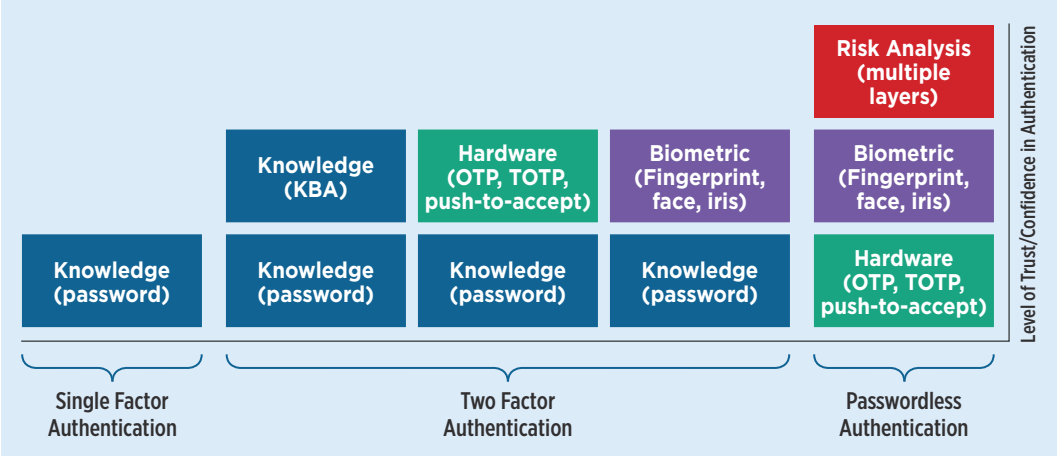
— Ant Allan & Tom Scholtz, Take a People-Centric Approach to Simplify IAM, Foundational, Nov 2015

Moving beyond the password

The problem, as Gartner analyst Ant Allan noted at the 2015 Gartner Security & Risk Management Summit in London[1], is that counting factors is not a reliable indicator of trust. In particular, if you base authentication on a password (something you know), adding a second or third knowledge-based method (such as a PIN or your mother's maiden name) adds very little security. Adding methods based on something you have (such as a hardware token) is better, but it is still not enough.

The solution, he argues, is to add biometric data. By combining hardware and biometric data, organizations can achieve a level of trust far beyond a knowledge-based factor like a password alone, or even a password plus a hardware token. In fact, Allan said, "If we had enough contextual data, we could allow log in without a password."

This is exactly the passwordless future that SecureAuth delivers today.



How SecureAuth's passwordless authentication works: a high-level view

The anatomy of an attack

To understand why contextual information is so critical to improving security, we need to step back and get the bigger picture. How can a single compromised password lead to massive data breaches like those experienced by Target, Anthem, and Home Depot? Simply put, it gives attackers the foothold they need. By gaining access to the corporate network, often through its weakest link, attackers can begin to move laterally and elevate their level of access, often by compromising more and more powerful legitimate credentials or creating new ones from scratch. Then the attackers can move freely and complete their mission to steal intellectual property, destroy data or encrypt it for ransom, or do other damage. And, according to the Verizon DBIR, the vast majority of the time (92.9%), they do all this in less than an hour.

But in that hour, the organization has multiple opportunities to thwart the attackers. The key is to spot the suspicious authentication attempts and block them, without putting unnecessary hurdles in the way of all the legitimate login attempts that are the lifeblood of your business.

SECUREAUTH

[1]SC Magazine: Minimise friction to maximise user satisfaction for user authentication – Sept 2015. http://www.scmagazine.com/minimise-friction-to-maximise-user-satisfaction-for-user-authentication/article/438575/

Adaptive authentication

That's what SecureAuth's advanced risk analysis (adaptive authentication) is designed for. SecureAuth's adaptive authentication blends a variety of risk checks for determining a user's aggregated risk score that determines how a particular authentication request is handled. Here are the risk checks SecureAuth can take into account:

- **SecureAuth Threat Service** — The SecureAuth Threat Service is a combination of multiple threat intelligence, information and blacklisted IP addresses for the industry's most advanced protection from today's threats including APT, Cyber Crime, Hacktivism as well as anonymous proxies and anonymity networks, such as Tor.
- **Device Recognition** — SecureAuth can determine whether the device is recognized and associated to a known user.
- **Geographical Location** — SecureAuth can determine if a request is coming from a known good location, where an organization has employees, partners, or customers.
- **Geo-velocity** — Using a user's geo-location and login history together, the solution can calculate improbable travel events, such as attempting to log in from a distant location only minutes after logging in locally (a good indicator that credentials have been stolen).
- **Directory Lookup** — Check group membership and user attributes, credentials created by attackers often lack appropriate group membership and other attributes.
- **Geo-fencing** — Determine if access requests come from within or outside a geographic barrier set by the customer.
- **Phone Number Fraud Prevention** — SecureAuth can negate the security flaws with one-time passcodes sent via SMS/Text with ability to block carrier networks, number class (e.g. virtual, landline, mobile), and mobile phones numbers that are involved in phone porting fraud. Also offers sophisticated spam and denial of service prevention to reduce number of OTPs.
- **Identity Governance** — We can take an access rights score from SailPoint IdentityIQ and utilize that score in determining the riskiness of access requests.
- **User & Entity Behavior Analytics** — We can check if behavior is outside the norm with integration with Exabeam, which helps SecureAuth determine anomalies in user behavior.
- **Behavioral Biometrics** — SecureAuth can gather keystroke dynamics and cursor movements with a particular user on a particular device and stop authentication attempts that fall outside established behavioral templates.

Individually, any one of these techniques may not provide sufficient protection against attackers, but when layered together, they can offer the industries' best level of protection and is very effective at preventing attackers from gaining a foothold and moving laterally within the organization.

Stolen credentials are rendered useless to attackers because multiple of these risk check will raise concerns and organizations can auto-require a multi-factor authentication step to prove validity or deny access requests outright.

Flexible authentication workflows

Of course, if adaptive authentication were to block every authentication attempt that received a non-zero risk rating, it would be unusable. But SecureAuth's adaptive authentication is flexible, enabling you to tailor the authentication workflow for different groups of users. For example, you can set a higher acceptable risk value for users who have few rights to sensitive data, and a lower acceptable risk value for users with privileged levels of access, such as IT administrators, financial employees, or pharmacists who can dispense controlled substances.

Moreover, you are not limited to the binary choice of either allowing or denying a given authentication attempt; you can also set a middle risk range where you step up the authentication requirements. For example, employees do travel, so instead of outright denying an authorization attempt for an otherwise low-risk employee who is logging in from a new location, you can instead challenge that user to provide any one of 25+ multi-factor authentication methods. In this way, you limit the inconvenience of multi-factor authentication to only a small number of legitimate authentication attempts and rarely if ever deny them, while consistently putting either high hurdles or complete roadblocks in the path of would-be attackers.

Not all users are created equal. SecureAuth lets you determine the authentication workflow and thresholds for individual users, groups, or applications.

Broad coverage is critical

Most organizations have multiple points of authentication; for example, users might have to log on to particular machines, at the VPN, to individual applications, and to data stores. Attackers look for the weakest part of the network as their foothold. For example, in the 2014 JPMorgan breach — the largest breach in financial services history — attackers gained access to the network by using the stolen login credentials for a JPMorgan employee to gain access to a particular server where two-factor authentication had not been deployed.

Accordingly, the best practice is to deploy SecureAuth widely across the enterprise and not just in a few pockets or selected departments. The greater number of applications and systems that are covered using a passwordless authentication approach, the greater the chance of eliminating an attacker from gaining a foothold or moving laterally inside your network.

How SecureAuth's passwordless authentication works: the details

Getting started

As noted above, SecureAuth offers multi-layered adaptive authentication, over 25+ different authentication methods, and flexible authentication workflows. You can use the default workflows, or tailor the workflows to your unique environment by specifying which authentication methods are to be used and at what level of risk a given type of user logon should be allowed without an MFA step, stepped up to a multi-factor authentication step, and at what level an access request should be denied outright.

User enrollment

Adaptive authentication begins with a one-time enrollment action for each user/device pair. This is not to be confused with the provisioning of a user account and assignment of permissions; that is handled by your organization's identity and access management processes. Rather, SecureAuth is cataloging established users and their devices for future authorization attempts.

Enrollment is a two-step process:

Step 1: You provide the user with a one-time code in one of the following ways:

- Send it to their phone by SMS (the phone number is protected using SecureAuth's Phone Fraud Prevention)
- Send it to them by email, which provides protection against OTP brute force, and OTP flooding.
- Have an automated system call the user and provide a one-time code orally
- Have an authorized staff member provide a one-time code in person

Step 2: The user uses the one-time code to enroll the SecureAuth Authenticate mobile application on their iOS or Android mobile device.

Throughout even the enrollment process, adaptive authentication techniques are being used to detect and mitigate risk in case an attacker is trying to enroll!

Day-to-day authentication

Once a user has enrolled their mobile device, the adaptive authentication workflow described earlier is used anytime the organization requires them to authenticate. The process is as follows:

1. The user provides his or her username to the application or VPN.
2. The user receives a login request notification from the SecureAuth Authenticate app.
3. The user provides his or her fingerprint as an initial form of biometric authentication. A valid fingerprint grants the user access to the SecureAuth Authenticate app. An attacker attempting to use a stolen device will be stopped here. Note: a PIN number could be used as an alternative if a fingerprint sensor is unavailable on the device.
4. The user accepts the authentication request using Push-to-Accept.
5. SecureAuth's adaptive authentication calculates the risk associated with the authentication attempt, based on the type of user and the factors you established during system setup. Depending on the thresholds you specified, one of the following will happen:
    - If the risk is sufficiently low, the authentication attempt will be approved without requiring any additional authentication step.
    - If the risk is moderate, the workflow can step up and request that the user provide an additional authentication method. Legitimate users will be approved, but attackers will be stopped.
    - If the risk is too high, the authentication attempt will be denied. Again, the attacker will be stopped.
    - If the risk is too high, the authentication attempt can be redirected to a honeypot or safezone for further observation

Why SecureAuth?

SecureAuth is uniquely positioned to enable organizations to embrace passwordless authentication. We have already explored several of the key features:

- Adaptive authentication
- Flexible authentication workflows
- Biometrics (fingerprint on a mobile device)

But SecureAuth also offers flexible deployment options:

- You can move toward passwordless authentication at your own pace. For example, you can continue using passwords with adaptive and multi-factor authentication and when confident you're protected, phase out passwords.
- You don't have to rip and replace. SecureAuth IdP plays nicely as part of the security ecosystem. SecureAuth IdP installs right into your environment, tying to your enterprise directories, applications, and VPNs, and using the same user accounts, profile information and policies you use today. SecureAuth even works with your hardware tokens.

And SecureAuth beats the competition:

- No other vendor provides as many authentication methods as SecureAuth (25+)
- SecureAuth offers more risk-based adaptive authentication checks than any other vendor.
- Very few other vendors offer flexible workflows for varying authentication requests
- Very few other vendors support as much technology as SecureAuth, meaning it's easy to deploy and TCO is low.
- SecureAuth costs the same or less than most solutions on the market.

Conclusion

As Ant Allan noted at the recent Gartner conference, designing user authentication systems for applications is often seen as a trade-off between security and the user experience. SecureAuth also rejects this idea. With SecureAuth, you can secure your network and data while streamlining the user experience — and you'll also eliminate the high costs of helpdesk calls for password resets, hardware tokens, and lost productivity. It's a win-win-win. Welcome to the passwordless era.

SECUREAUTH

8845 Irvine Center Drive | Irvine, CA 92618

p: 1-949-777-6959 | f: 1-949-743-5833 | **secureauth.com**