ForgeRock

WHITE PAPER

MODERNIZING AUTHENTICATION WITH PASSWORDLESS

Healthcare's Cure For Password Security And Experience Woes

Never Login Again

Introduction

Passwords have been around forever, but their value as a means of securing access has diminished as attackers consistently find new ways to defeat them. Efforts to strengthen passwords using more stringent policies, adding a second authentication factor, and educating users about protecting themselves have been largely ineffective, as passwords remain the leading cause of successful cyberattacks and data breaches. Passwordless authentication offers a new approach — a lower-cost, easier, and more secure way to authenticate healthcare consumers, patients, members, providers, employees, contractors, and partners.

> The healthcare industry is the number one cyber crime target
>
> — **The ForgeRock Consumer Identity Breach Report**

Passwords, in one way or another, have been used to verify identities since the Roman Empire, when soldiers exchanged watchwords to distinguish friends from foes. Even today, healthcare organizations of all types and sizes remain heavily dependent on the concept of a memorized piece of information that immediately grants access to its holder.

While the password has never been ideal for identity authentication, the age of computing has introduced new and bigger challenges that make passwords even more problematic. The volumes of sensitive data generated and stored today, and the speed at which that data can be stolen or destroyed, are major concerns for healthcare organizations.

For years, the standard approach to dealing with the inherent security flaws of passwords has been limited to three categories: enforcing increasingly harsh password policies, deploying a second (and sometimes third) method of authentication on top of a password, and educating users about the dangers of social engineering and password misuse. Unfortunately, these security measures keep organizations at risk because of the increase in password-based attacks, resulting in more compromise. According to the Verizon 2022 Data Breach Investigations Report (DBIR),[1] 80% of cyberattacks were attributable to stolen credentials.

Why Passwords Are a Problem

1. Poor password hygiene

The most commonly used password in 2019 was 12345, followed by equally simple strings. When security policies prevent the use of such common strings, the problem is only slightly less alarming. Recent research among IT security personnel showed 49% of responders admitting to sharing passwords with colleagues to access business accounts, and 59% reported that their organizations' users rely only on memory to remember passwords while 42% say sticky notes are being used for that purpose.[2]

Passwords Are a Problem

Poor Password Hygiene
49% of users admit to sharing passwords with colleagues to access business accounts

Password-based Breaches
34% of healthcare data breaches come from unauthorized access or disclosure

Breaches Are Expensive
A data breach in the healthcare sector costs more than any other industry at $10.1 million

High Help Desk Costs
50% of all help desk calls are related to password resets ($70 per password reset cost)

Password-based Cyberattacks
The average ransomware payout in Q1 2022 for the healthcare industry was $211,259

2. Passwords-based breaches

The danger of passwords is clearly demonstrated by the Verizon 2022 Data Breach Investigations Report, which associated 76% of breaches to basic web application attacks, miscellaneous errors and system intrusion. Of the data that is compromised, 58% is personal, 46% medical, and 29% are credentials.

3. Passwords-based data breaches are expensive

The financial implications of data breaches resulting from compromised credentials are becoming dire. With an average cost of $10.1 million per healthcare data breach according to the Verzion 2022 Data Breach Investigations Report,[3], it is more critical than ever to prevent potentially devastating security incidents.

> *"Healthcare is the industry where the internal actor has figured prominently in breaches since we first began collecting and reporting data."*
>
> — Verizon 2022 Data Breach Investigations Report

> *"...in the second half of 2022, victims of healthcare data breaches had 28.5 million records exposed, which was an increase from 21.1 million in 2019."*
>
> — Health IT Security

4. Help desk password reset costs are increasing

IT and help desk teams have been trying to balance the enforcement of secure password policies with simplifying user experiences. The results, however, tend to be expensive and ineffective for improving protection. Password complexity requirements, once thought to be critical in preventing hacks, provide no defense against many common attacks. This approach is now regarded as an obstruction to productivity, security, and convenience. Moreover, since up to 50% of all help desk calls are related to password resets according to Gartner Group[4], and with Forrester Research estimating an average cost of $70 per password reset[5], strict password policies increase operational costs dramatically.

5. Password-based cyberattacks are growing

Ransomware has become one of the largest cybersecurity problems in the world since the start of the 2020 pandemic. Heatlhcare IT News reports that ransomware attacks on healthcare entities doubled from 2020 to 2021 in a poll of more than 5,000 IT professionals.[6]

One of the most common ways adversaries carry out ransomware attacks is using Remote Desktop Protocol (RDP) brute-force attacks, which account for up to 47% of ransomware attacks[7]. An RDP brute-force attack is fundamentally an authentication problem, and passwordless authentication would close down this attack vector.

Phishing is the other major problem in cybersecurity. In fact, the 2022 Verizon DBIR found that phishing came in as the top avenue of incursion in the general incidents they studied (67%). Phishing fundamentally targets a password and, once compromised, enables many downstream attacks. Removing the password removes the target that attackers are chasing the most.

*"According to IBM, **ransomware** attacks are **increasing** in their speed, especially when measuring the "time on target"*[8]

— Health and Human Services

Multi-Factor Authentication (MFA)

An improvement at a great cost

To bolster password security and to meet new regulatory demands, many companies have implemented multi-factor authentication (MFA) for patients, members, consumers, providers, employees, contractors, and third-party partners. MFA relies on a combination of two or more distinct proofs of identity, including something the user knows, something the user possesses, or something the user is, to fully authenticate a user.

MFA fatigue

With increased security comes higher levels of friction in the end-user experience. For example, a user who wants to log in to a business application or resource must enter the correct username and password, then take the action of accepting a one-time passcode (OTP) or push notification on their smartphone in order to complete that authentication process.

Basic MFA is the standard form of authentication most organizations deploy. Unfortunately, basic MFA lacks the intelligence to adjust the number of times extra steps are required from an end user. Frequently requiring these steps can lead to MFA fatigue, which attackers are actively trying to exploit through a method known as MFA prompt bombing. In this scenario, attackers repeatedly send MFA prompts in an effort to get a frustrated user to finally "accept" the prompt, granting access to an intruder.

In a 2020 update to its digital identity guidelines, the U.S. National Institute of Standards and Technology (NIST) states that authenticators leveraging phone calls and SMS messages to send unencrypted one-time passcodes (OTPs), once considered a legitimate channel, are now labeled "restricted."

MFA workforce blindspots

Due to the cost of MFA, its use within enterprise environments and internal corporate networks remains inconsistent and is often limited to the corporate VPN, according to the latest Mary Meeker Internet Trends Report[10]. Ponemon got a picture for the general use of MFA across different use cases in its 2021 State of Workforce Authentication report[11], and it is clear from the findings that MFA use across the enterprise varies widely from use case to use case.

MFA islands

When organizations have undergone significant change due to mergers and acquisitions, or due to incomplete coverage from one solution, they can find themselves with MFA implementations from various vendors. These solutions may have been selected at different times and to cover different use cases independently. The result is "MFA islands," which introduce a higher level of MFA complexity and increased management costs. End users are also burdened with the use of multiple authenticators or MFA factor methods as they authenticate throughout their user journey.

MFA security limits

With the growing adoption of MFA, a realization has emerged in the market that it is not foolproof and quite capable of being defeated with known attack methods, such as SIM swapping. After several successful attacks on seemingly secure out-of-band authentication factors, regulators started adding restrictions to MFA authentication methods. In addition to restrictions on OTPs, NIST has limited the use of biometrics as a standalone authentication factor for its susceptibility to spoofing.

While MFA has helped organizations improve their organizational security posture and lower the risk of password-based attacks, it does not fix today's password problem. That is why passwordless authentication is needed now.

A Passwordless Future

The requirements for stronger authentication are changing rapidly. Patients, members, and consumers demand a frictionless, retail-like experience. And fully remote or hybrid workforces are the new normal. Security-conscious organizations are increasingly considering re-architecting their networks and access around Zero Trust principles. Passwords are increasingly being talked about as antiquated technology that must evolve toward obsolescence.

Evolutionary standards and enterprise maturity

If enterprise identity and authentication were looked at as layers, the foundational layer would be the identity-as-a-service (IDaaS) single sign-on (SSO) solutions that most enterprises have deployed as a result of cloud adoption.

Standards, such as SAML and OIDC, are well developed in this ecosystem. Newer standards, such as the Fast Identity Online (FIDO2) WebAuthn and passkeys, are being accepted by major hardware manufacturers (Apple, Google, Microsoft) and leading browsers (Google, Microsoft), and have the potential to transform enterprise computing environments.

Modern architectures

Passwordless solutions are built on modern architectures that leverage decentralized architectures, private-key cryptography, and biometrics. These solutions continue to be MFA in nature, but they are designed to be mobile-first to capitalize on smartphone-based chips and biometrics. Android and iOS devices have highly developed security enclaves to store key information, such as private keys defined by the FIDO standard. Smartphone biometrics are also harder to spoof than MFA is to hack. In combination, these innovations enable an authentication solution that dramatically reduces the risk of a centralized data breach.

A great user experience

Passwordless authentication solutions don't generally eliminate the need for mobile phone involvement, but they do substantially cut down on friction by eliminating the need to type codes or passwords, as most MFA solutions require. FIDO-based solutions generally send a cloud notification to a mobile device that is easily acknowledged. This action often ties in with a quick biometric that follows the notification and provides enhanced security over most MFA. MFA fatigue can be reduced with passwordless, since the need for typing is eliminated, unless smartphone biometrics are unavailable, in which case a PIN may be required.

Lower operational costs

Enterprise passwordless solutions with wide support for both consumer and workforce use cases can help lower the costs related to authentication. Help desk password resets, and, potentially, the cost of password management systems can often be eliminated. Many large North American organizations allocate over a million dollars per year for help desk password reset costs, so the savings from passwordless have the potential to be significant.

The ForgeRock Approach to Passwordless

With ForgeRock, you can move to passwordless at your own pace without it being an all-or-nothing experience. The important thing is to progress from authentication that relies on traditional usernames and passwords to processes that introduce passwordless.

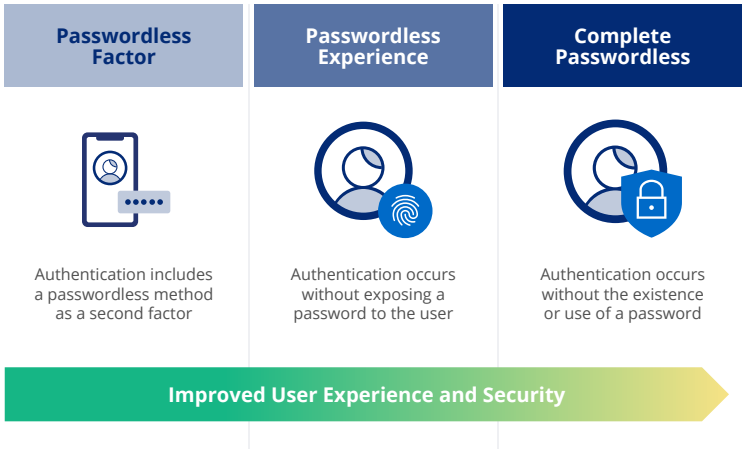
Accelerating your passwordless journey

ForgeRock offers three methods to approach to passwordless authentication. First, you can easily include a passwordless method as a second factor (passwordless as a factor). Moving further, you can deliver a passwordless service experience in which users never have to interact with their passwords (passwordless experience). Ultimately, you'll can leverage a passwordless implementation where passwords are fully eliminated (complete passwordless). Authentication methods, access orchestration, and application integrations can help you to accelerate your passwordless journey with a full spectrum of options for your passwordless deployment.

Passwordless Factor
Use a passwordless method, such as a push notification or an emailed magic link, as an additional authentication factor beyond a password.

Passwordless Experience
Remove the password from the user experience and perform any password-based authentication securely in the background.

Complete Passwordless
Eliminate creation and use of passwords completely and perform authentication with biometrics or private-key cryptography.



The ForgeRock platform provides multiple passwordless authentication methods, no-code orchestration, and extensive application integrations to help implement a successful passwordless program.

Authentication methods

Embrace passwordless with an expansive set of authentication methods, such as FIDO2 WebAuthn, passkeys, OATH, push, OTP, biometrics, and others, to easily enable passwordless across mobile authenticators, smart cards, biometric devices, digital certificates, browsers, and applications.

Access orchestration

Configure and deploy drag-and-drop passwordless authentication workflows, including security signal analysis and third-party integrations, based on the unique security and user experience needs of your business. Orchestration capabilities allow for easy creation of no-code, out-of-the-box passwordless user authentication journeys to help improve login experiences for every type of user (consumers and workforces).

Application integrations for your enterprise

Purpose-built for workforces, ForgeRock Enterprise Connect Passwordless provides support for an extensive list of enterprise applications and infrastructure, including legacy applications, Windows and Mac workstations and servers, RADIUS-based authentication, Remote Desktop (virtual and Windows), desktop SSO, VPNs, databases, mainframes, LDAP, REST, Unix/Linux servers, and many more.

Passwordless Capabilities

Authentication Methods

- WebAuthn/ Passkeys
- OTP (OATH)
- Push
- Biometrics
- QR Code
- Trust Network

Access Orchestration

- General Signals
- Device Signals
- Intelligent Signals
- Intelligent Access

Application Integrations

- SAML/OIDC
- Gateway
- Agents
- SDKs
- Workstations
- Remote Desktop
- RADIUS
- Desktop SSO

Why the Business of Healthcare Runs Better with ForgeRock

ForgeRock passwordless authentication allows you to mitigate one of the biggest security risks your organization faces: passwords. Passwords are insecure, inconvenient, and costly. By removing a user's interaction with passwords, your business can strengthen security and lower operational costs while delivering great user experiences.

Strengthen security

Eliminating the exchange of passwords reduces the risk of compromise due to password-based attacks, such as phishing, credential stuffing, and brute-force attacks. When user interaction with passwords is eliminated, you can also strengthen security with password encryption and rotation for legacy systems. And by deploying ForgeRock Enterprise Connect Passwordless for your workforces, you remove the exchange of passwords between users and enterprise applications and infrastructure, including legacy applications, servers, workstations, VPNs, and more.

Lower costs

Eliminating account lockouts, escalated login failures, and password-related trouble tickets lowers operational costs from help desk interactions. With Enterprise Connect Passwordless, you can also reduce deployment costs by eliminating the need to rewrite legacy enterprise applications to implement passwordless authentication.

Enhance the user experience

Eliminating the cumbersome login process for all scenarios, including diverse enterprise applications and infrastructure, enhances the user experience and provides users with faster, more secure, and more flexible access to resources.

Why ForgeRock?

ForgeRock provides a number of unique differentiators including:

Passwordless at Your Own Pace

Move your users from password dependency to a passwordless experience or to complete passwordless authentication without having to rewrite your business applications and resources. Advance passwordless at your own pace without it being an all-or-nothing experience.

Broad Passwordless Coverage

Simplify and secure your enterprise infrastructure by eliminating your users' interactions with passwords. At the same time, you can enable stronger security to web and mobile-based applications and resources with passwordless authentication methods, such as FIDO2, WebAuthn, and passkeys.

No-Code Authentication Orchestration

Effortlessly define and administer no-code authentication orchestration within ForgeRock Intelligent Access. You'll improve your users login experiences and accelerate their access to resources and your business.

Start Your Passwordless Journey Today

Today's enterprises have reached a critical juncture. The continuous growth of password-based cyberattacks has created an extraordinarily risky healthcare business environment. Security and risk professionals are overwhelmed as they try to defend against the increasing volume and velocity of these attacks.

Now is the time to start your passwordless journey.

Learn how security and risk professionals use ForgeRock to strengthen security, deliver great user experiences, and increase workforce productivity.

Contact us to learn how ForgeRock can help you.

[1] Verizon 2022 Data Breach Investigations Report (DBIR)

[2] 2020 State of Password and Authentication Security Behaviors Report

[3] Verzion 2022 Data Breach Investigations Report

[4] Are Password Resets Costing Your Company? Bioconnect, December 2021

[5] TechTarget: Resetting Passwords in the Enterprise Without The Helpdesk

[6] https://www.healthcareitnews.com/news/half-ransomware-attacks-have-disrupted-healthcare-delivery-jama-report-finds#:~:text=In%20June%202022%2C%20Sophos%20found,more%20than%205%2C000%20IT%20professionals

[7] NCC Threat Pulse Report, August 2022

[8] https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

[9] Mary Meeker Internet Trends Report, June 2019

[10] State of Workforce Authentication, Ponemon-Sullivan Privacy Report, December 2021

About ForgeRock

ForgeRock® (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit: www.forgerock.com.

Follow Us

ForgeRock