rf IDEAS

# 2024 State of Passwordless Security

# Foreword

There's a reason several prominent tech companies such as Apple, Google, and Microsoft are investing in the adoption of passwordless authentication. Hybrid workplaces and mass digitization have created a demand for dependable data security and improved user interfaces. Without them, corporations are vulnerable to data breaches, leaks, and severe losses. Although password-protected endpoints deliver an adequate level of protection, they are also vulnerable to security issues such as phishing and stolen identities. Moreover, users often struggle to remember several different passwords, further compromising security as the same password is used to access multiple business systems and endpoints.

On the other hand, passwordless systems such as biometrics, smartcards, multi-factor authentication, and FIDO security key technology maximize data protection while creating a seamless user experience. Nevertheless, not all passwordless authentication systems are the same. A thorough understanding of their differences, benefits, and limitations helps decision-makers evaluate and systematically deploy passwordless solutions for at-risk workflows. For example, industries facing more cyberattacks such as healthcare and finance demonstrate a higher need for seamless passwordless authentication.

In our mission to safeguard enterprise workflows, rf IDEAS dives into the intricacies surrounding passwordless authentication and its place in modern operations. By understanding the foundational principles of passwordless authentication, we hope to empower organizations in developing efficient access control systems with adaptable technologies.

**- Raul Cepeda Jr.**
**Vice President, Global Marketing and Product Management - rf IDEAS**
Raul Cepeda Jr. is the Vice President of Marketing and Product Management at rf IDEAS, a global leader enabling logical access solutions across healthcare, manufacturing, financial, education, enterprise, and government markets for nearly 30 years.

# Table of Contents

## Driving Factors Behind Passwordless Authentication Adoption

New technologies can be daunting at first. However, emerging challenges and persistent obstacles have generated a need for uniform authentication systems. While individual businesses may have unique factors fueling change, most corporations cite the following issues driving new implementations.

- Security
- Workforce Efficiency
- Regulatory Compliance

# 1 Current Multi-Factor Authentication (MFA) Systems Are Unable to Ward Off Threat Actors

Serving a step above traditional password access, MFA systems would require users to essentially “double-check” their identity before permitting access. **An estimated 59% of large corporations use some form of MFA**, requiring users to verify accounts via an SMS text or mobile app.[1] Nevertheless, some MFAs are proving to be inadequate when fighting:

*Push Notification Attacks* : These incidents often spam a user with countless push notifications to verify identity. The user then mistakenly verifies a stolen identity, giving threat actors full access to the account.

2022 saw a **33%** increase in push notification attacks.[2]

*Credential Stuffing Attacks:* When threat actors get a hold of one access credential, they can test passwords on multiple accounts, conducting a credential stuffing attack.

Of the 194 billion credential stuffing attacks reported last year, **3.4 billion targeted financial businesses alone**.[3]

*Reused/Poorly Updated Password:* While hackers are notoriously behind most cybersecurity damages, employees are not completely exempt. Poorly updated passwords and the reusing of passwords ultimately enable attacks.

The average person will reuse a password at least **14 times**.[4]

## 2 Remote Employees Need a Faster, More Secure Way to Access Data to Remain Productive

Work-from-home (WFH) and hybrid schedule models have become a normal part of life in many industries. Empowering employees to balance work and home life, remote positions are expected to remain popular, with some studies predicting a **417% increase in remote workers by 2025 compared to pre-pandemic statistics.**[6] While MFA can provide an extra layer of security for remote workers, they still lack:

### Immediate access to data

If verification credentials are not readily available, remote teams need to wait for access codes provided by an in-person worker.

### Device authentication

Since remote workers may use a mix of personal and business devices, a proper security system should verify all endpoints.

### A seamless access system

Constant MFA popups and page refreshes can frustrate workers. Moreover, as mentioned before, hackers leverage MFA fatigue to gain access through remote devices.

**Users spend 3min 46 sec on average resetting one password.**[5]

3

# Current Systems Are Not Meeting Regulatory Compliance Consistently

Whether HIPAA, GDPR, or SOX, regulatory compliance standards are often sustained by zero-trust policies. However, as more users and devices enter a network, enforcing zero-trust practices becomes more complex, compromising compliance standards. As a result, **32% of breached companies have incurred regulatory fines on top of financial losses.** Implementing passwordless authentication can support regulatory compliance by:

**Verifying a person's identity before sharing confidential information**

**Restricting users from sharing logins**

**Managing privileges for individuals who seek access to networks or information**

When developed alongside trusted IT professionals, passwordless authentication has been found to exceed NIST 800-63 compliance, meeting the criteria for Authentication Assurance Level 3 (AAL3) due to its unphishable factors.

## Bracing Against Cyberattacks and Data Breaches

Surpassing every driving factor, cyberattacks and data breaches are the top driver demanding reliable security parameters. It is estimated that a cyberattack happens every 39 seconds, costing businesses millions of dollars yearly. As businesses expand their digital footprint, it is important to understand the main reasons behind growing cyberattacks as well as the current systems employed to prevent them. With an understanding of these factors, businesses can target which areas may benefit from passwordless authentication and support new systems with peripheral solutions, lowering costs while heightening security.

# It's All Connected: How the Internet of Things Creates the Perfect Environment for Attacks

**By 2030, researchers suggest the globe will hold approximately 29 billion Internet of Things (IoT) devices.[7]** From A/C units to mobile computers, virtually everything -and everyone- is connected to the internet. In terms of cyber security, this means threat actors now have a variety of entry points to choose from to access systems.

| | |
|---|---|
| 112 Million | Number of IoT cyber attacks worldwide in 2022[8] |
| 54% | Average number of organizations that suffer from attempted cyberattacks targeting IoT devices each week[9] |
| $8.94 Million | Average cost of a successful endpoint attack[10] |

As companies integrate more devices into their workflows, security measures must be implemented alongside them to protect data. Unique industries such as finance and healthcare may require specialized plans; however, the following initiatives have proven useful to a variety of companies seeking to minimize data risks within their IoT systems:

Designate a cybersecurity team

Implement credential checking

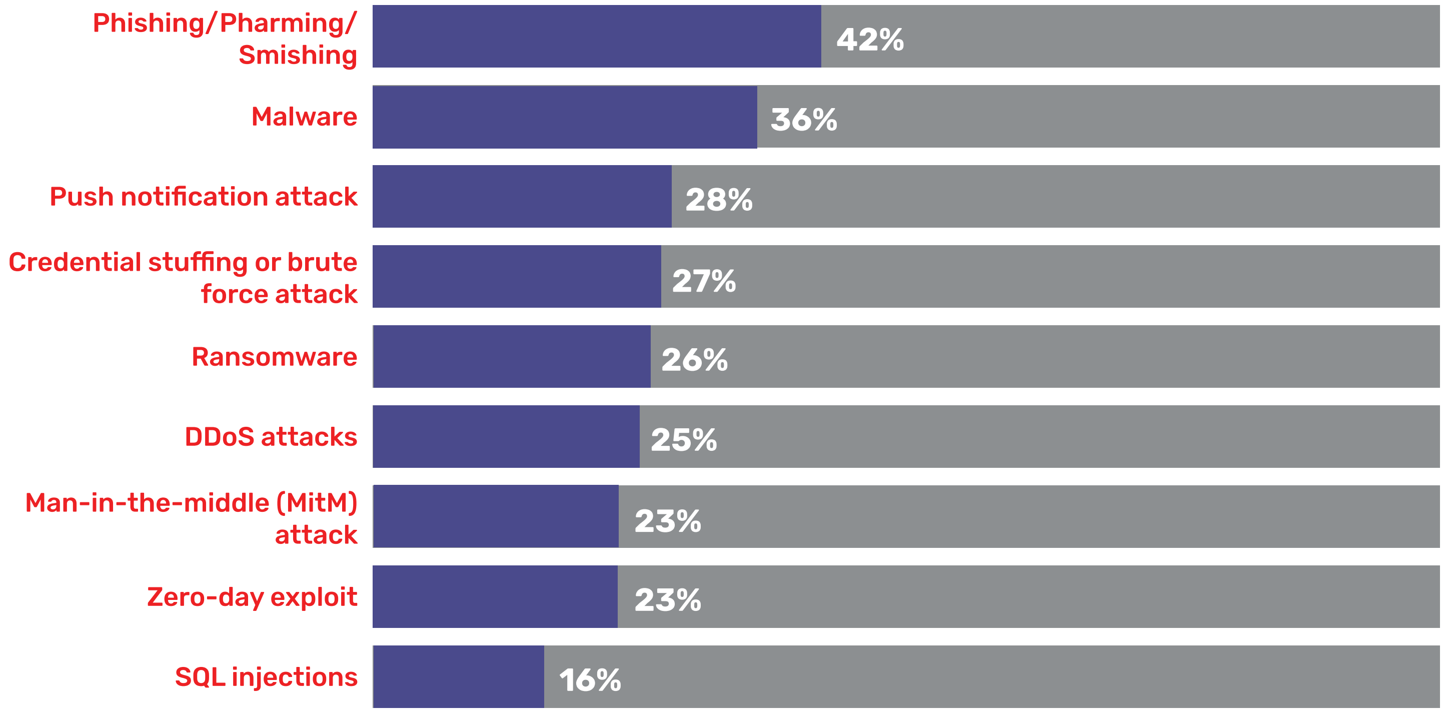
Establish training and awareness seminars for employees

Segment data access in a tiered level

Update privileged access and governance

# Sharing isn’t Always Caring: Understanding the Impact of New Connectivity Systems in Cybersecurity

2020 marked many changes worldwide. Amidst unprecedented times, 5G took center stage in the digital world, promising faster speeds, decreased latency, and higher network capacity. These benefits are set to empower businesses seeking to expand their IoT network and onboard more remote employees. Along with 5G, other connectivity systems became more mainstream such as WiFi 6E. While these systems offer new benefits, they also come with new unforeseen risks. Organizations have faced the following types of cyberattacks in the last 12 months:



*Percentage Chart*[2]

To support cybersecurity parameters, CISA and leading cybersecurity developers recommend pairing automated systems with:

Individualized Network Slicing Management

Protected System Monitoring & Anomaly Detection

Zero Trust Architectures for All Systems

High-Level Data Encryption Between Endpoints

# Where Passwordless Authentication Fits

Regardless of which connectivity network is deployed or how many connected devices exist within an infrastructure, automated authentication systems empower businesses with real-time visibility into user activity, data sharing, and communication between access tiers. Set within the discussed challenges, passwordless authentication can help:

**Save up to $2.95M[11]**

typically lost to an authentication-related breach

**Create a safe space**

for remote teams without compromising in-house employees

**Authenticate users**

to interact within a network

**Segment access**

within your IoT network

## The Methods & Benefits of Authentication

Authentication systems are constantly evolving. Therefore, when evaluating the need for passwordless authentication, many decision-makers may also consider other common authentication systems such as SMS Authentication and MFA.

# Methods of Passwordless Authentication

Depending on an organization's needs, passwordless authentication may take different forms. While there are many systems currently on the market, the most common methods are:

1. One-time password via SMS or Push – An additional endpoint such as a smartphone or an application can be used to verify account activity, providing immediate notice and access controlled by the user.

2. One-time Authentication link sent to email – Similar to hardware tokens, a magic link can be accessed through a cleared email address, granting access to the user without a password. Reliable security should be in place for issued emails to protect magic links

3. Biometrics – One of the most common types of passwordless authentication, biometric systems leverage fingerprints, retina scans, and other physical traits to verify the user's identity. Because these traits are unique to the user, biometrics offers one of the most secure avenues for authentication.

While some organizations are adopting these common methods, not all methods are created equal. Check out the chart below to see how these passwordless authentication methods stack up against one another in terms of security, encryption, and accessibility.

| | Provides Additional Layer of Security | Quick Access | Protects Against Phishing |
|---|---|---|---|
| **Username/Password** | No | No | No |
| **Password Manager** | Yes | No | No |
| **SMS Authentication** | Yes | No | No |
| **Passkeys and Security Keys** | Yes | Yes | Yes |
| **MFA Systems** | Yes | No | No |
| **Tap-and-Go/Passwordless** | Yes | Yes | Yes |

**81% of data breaches are caused by lost or stolen passwords.**[12]

# Benefits of Passwordless Authentication

When working alongside a reliable solution provider, businesses have witnessed...

Increased User Productivity

Reduced Breach Risks

Increased Employee Satisfaction

Improved Supply Chain Resilience

2.6X **Faster Sign-in Time**

25% **Fewer Password Request Inquiries from Users**

Established Zero Trust Models

Simplified IAM Infrastructures

$9.4 Million **Saved Per Year (Average Cost Per Breach)**[13]

*Results are based on unique implementation use cases and may vary under different environments.*

## Who Needs Passwordless Authentication the Most?

As cybercriminals continue to fine-tune their attacks, the following industries are more vulnerable than others, and therefore, should highly consider implementing a passwordless authentication solution:

- Healthcare
- Financial
- Manufacturing
- Enterprise

# Industry Risks at a Glance

### Healthcare

**Over $10 million[14]**

Average Cost of a Cyberattack in the Healthcare Industry

### Financial

**Over $6 million[15]**

Average Cost of a Cyberattack in the Financial Industry

### Manufacturing

**Over $4.35 million[17]**

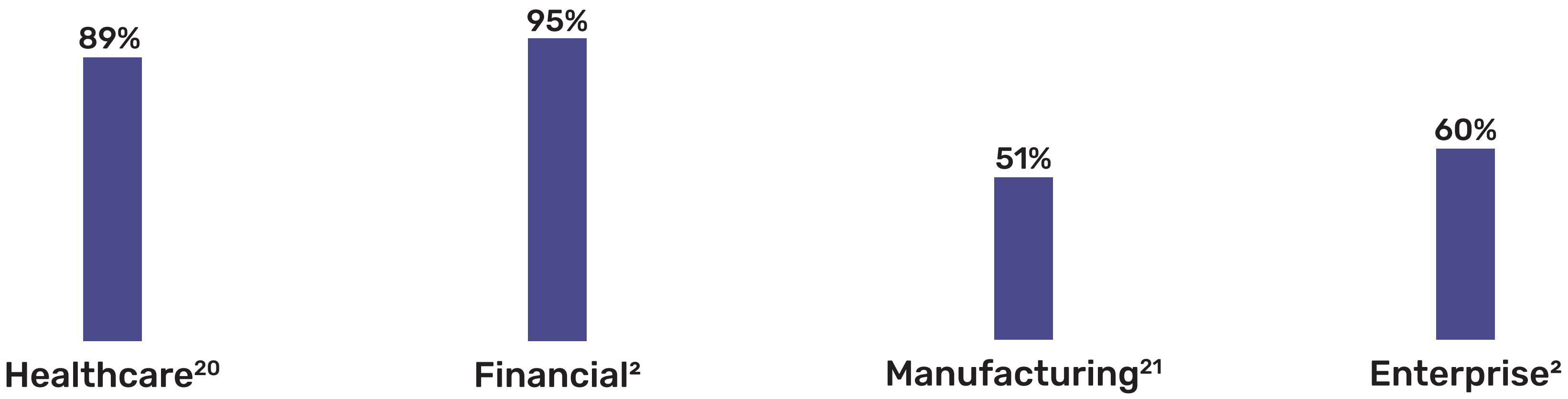
Average Cost of a Cyberattack in the Manufacturing Industry

### Enterprise

**Over $4.35 million[19]**

Average Cost of a Cyberattack in the Enterprise Industry

**Percent of organizations within each industry that have experienced a cyberattack in the past year:**



## Maintaining FIDO Standards with Passwordless Authentication

Without a clear pathway for implementation, even the most advanced systems can compromise security. As a result, 36% of IT professionals report concerns about how to integrate passwordless authentication.[11] For the sake of transparent implementation and dependable security, a viable passwordless authentication system should adhere to the Fast Identity Online (FIDO) standards.

# Maintaining FIDO Standards with Passwordless Authentication

[ 90% ]

**of IT professionals are considering FIDO standards when implementing passwordless authentication.**

Major Tech Players Committed to FIDO

**Google**

**Apple**

**Microsoft**

By leveraging cryptography for verification, FIDO standards enable a seamless authentication system across websites and applications in both mobile and desktop endpoints. Unlike other methodologies, FIDO Authentication empowers businesses with:

Consistent Security –
Cryptographic credentials don't need to be stored on a server or mobile device, reducing chances of phishing and password theft.

Convenient Data Access –
By eliminating passwords and multi-factor access codes, security keys reduce wait times to access data.

Scalable Growth –
FIDO provides a growth pathway to expand passwordless authentication solutions involving multiple devices.

## Geographical Impacts

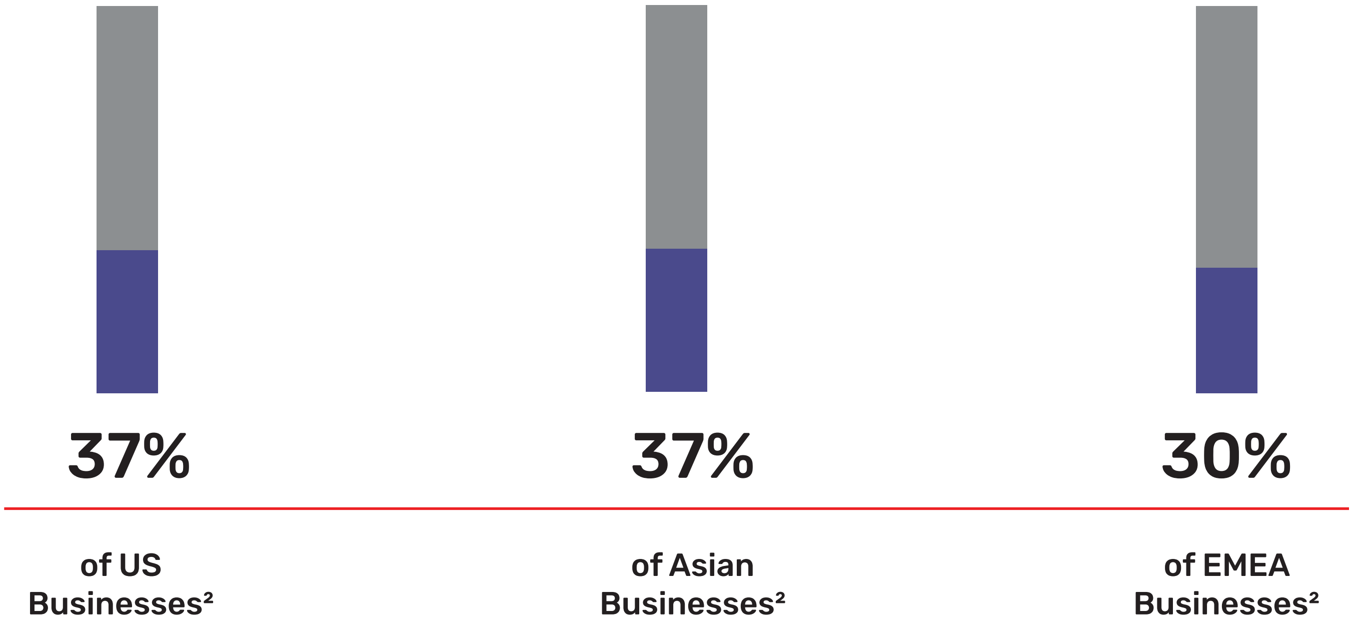
Depending on geographical location, businesses may have a higher need for passwordless authentication to meet national policies and guard against attacks stemming from international tensions. Unique reporting systems also impact the rate at which attacks are reported and how they are resolved. After surveying over 700 global breaches, researchers at Vanson Bourne uncovered the following trends:

- 62% of companies in the Americas have experienced a data breach within the last year[22]
- 81.4% of organizations in the UK experienced a successful cyberattack within the last year[23]
- 59% of companies in the Asia-Pacific region reported being the victim of a cyber attack in 2022[24]

# Responding to Authentication Weaknesses at a Geographical Level

North American and Asian countries tend to have the highest inclination to adopt passwordless authentication to withstand ongoing threats. As a result, surveys demonstrate ongoing plans to adopt passwordless authentication within the next 3 years.

**Geographical Locations Expecting to Adopt Passwordless Authentication within 3 Years**



## Concluding Remarks & Next Steps

While it is not likely traditional password systems will disappear overnight, a careful evaluation of their performance illuminates one sure conclusion: Modern-day businesses need more than a password to secure data. Increasing cyberthreats and evolving compliance standards have created a demand for reliable data protection that preserves unbroken productivity for both in-office and remote teams.

This study aims at creating a space for conversations surrounding passwordless authentication while providing insights into driving forces, methodologies, and adoption rates around the world within high-risk industries. As organizations become more familiar with the limitations of their current systems and persistent security threats, passwordless authentication becomes less of a mystery and more applicable to our current digital climate.

## About this Study

As a leader in innovation, rf IDEAS gathered surveys conducted by leading researchers within the data security industry to contrast findings and evaluate the demand for passwordless authentication. Studies cover multiple continents and industry sectors to provide a broad yet in-depth scope of the subject matter.

*This study was not funded by outside 3rd parties.*

# Next Steps: Developing a Passwordless Authentication System with a Solution Provider

As previously mentioned, a successful passwordless system should implement FIDO standards, adapt to growing employee pools, and integrate secured technologies that are still compatible with deployed systems. At rf IDEAS, our teams leverage over 30 years of authentication experience to tailor solutions that grow alongside labor pools and challenges. Built to establish trust and ease, rf IDEAS partners with several leading technology developers to expand data security.

**Our Partners:**

imprivata

Rockwell Automation

Microsoft

Google

Cerner

GE HealthCare

hp

RICOH imagine. change.

ForgeRock

authX

NTware

SOLOINSIGHT

For more information about this study or to see how you can develop a passwordless authentication system in your space, contact rf IDEAS.

rf IDEAS

rfideas.com
(866) 439-4884

# Works Cited

[1] Whitney, Lance. “More companies use multi-factor authentication, but security still weak from poor password habits”. TechRepublic. Oct 8, 2019.
[2] "The State of Passwordless Security". Cybersecurity Insiders. HYPR. 2022.
[3] Arampatziz, Anastasios. “Understanding the Economic Impact of Credential Stuffing Attacks”. The Security Ledger. May 17, 2022.
[4] “The Issue of Password Reuse”. Enzonic.
[5] “Survey: How much time do you waste resetting your passwords?”. ExpressVPN. Dec 20, 2022.
[6] Ryan, Robin. “Here’s What’s Happening to Remote Work in 2023”. Forbes. Jan 10, 2023.
[7] "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030". Statistica. Jul 22, 2023.
[8] "Annual number of Internet of Things (IoT) malware attacks worldwide from 2018 to 2022". Statistica. Mar 2023.
[9] "The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally". Check Point Research. Apr 11, 2023.
[10] Jones, Caitlin. "50 Endpoint Security Stats You Should Know In 2023". Expert Insights. Feb 20, 2023.
[11] "The State of Passwordless Security". VansonBourne. 2023.
[12] “3 Common Mistakes That Lead to a Security Breach”. Okta. Feb 14, 2023.
[13] “Eliminate Passwords and Deliver Great Experiences”. ForgeRock. 2023.
[14] “Cybersecurity Nightmares: The Cost of Healthcare Cyberattacks in 2023”. Intraprise Health. Apr 6, 2023.
[15] Petrosyan, Ani. “Cyber crime and the financial industry in the United States - Statistics & Facts”. Statistica. Apr 20, 2023.
[16] Vasquez, Christian. “Ransomware Attacks Surge Against US Manufacturing Plants”. Cyberscoop. Feb 14, 2023.
[17] “The Cost of Cyber Attacks on Supply Chains”. Fortress. Feb 3, 2023.
[18] Graham, Taylor. “Enterprise Sector Suffers Cyberattacks at Higher Rates than Smaller Organizations”. Security IT News. May 23, 2023.
[19] “Average cost of a data breach in the United States from 2006 to 2022”. Statistica. 2022.
[20] Mensik, Hailey. "Healthcare cyberattacks led to worse patient care, increased mortality, study finds". HealthcareDive. Sep 8, 2022.
[21] Robert, Peter. "Manufacturing Cybersecurity Statistics: Recent Cyber Security Attacks, Risks & Threats to Manufacturing Industry". Expert ComputerSolutions.
[22] “A triple threat across the Americas: KPMG 2022 Fraud Outlook”. KPMG. Jan 2022.
[23] O’Driscoll, Aimee. “UK cyber security and cyber crime statistics (2023)”. CompariTech. Feb 10, 2023.
[24] Powell, Olivia. “The top 9 hacks, data breaches and cyber security threats in APAC”. Cyber Security Hub. Feb 28, 2023