Accelerating the Journey to Passwordless Authentication

Leveraging Results from the EMA Research Report, "Passwordless Authentication—Bridging the Gap Between Low-Friction and High-Security Identity Management"

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM
By Steve Brasen
July 2019

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

UNDERSTANDING PASSWORDLESS AUTHENTICATION

The primary purpose of enterprise IT security is to ensure the right people have the right access to the right IT resources under the right conditions. As such, the application of security policies is broadly dependent on correctly identifying the users requesting access, rendering identity management the first line of defense in enterprise security. However, traditional password-based authentication solutions are commonly considered to be "high-friction"—that is, they are challenging and time-consuming for users. Enterprises are now widely considering passwordless approaches to authentication that can improve user productivity while responsibly achieving security assurance.

Passwordless authentication technologies typically fall into one of three categories: biometrics, which identifies users by a physical characteristic (such as a fingerprint, face scan, voice print, or unique behaviors), encrypted tokens (including hardware and software keys), and device authentication (which enables user access from authorized devices). It is important to recognize that no single form of authentication will be optimally secure and user-friendly in all cases, and most organizations will adopt multiple approaches. In this way, transitioning from traditional password controls to low-friction solutions is more frequently a protracted journey than an overnight deployment. Passwordless authentication and identity management solutions (including single sign-on and password vaulting) should be strategically introduced to systematically reduce the reliance on passwords while simultaneously delivering low-friction experiences to end users.

The results from the research provide clear indications of methods for simplifying the onboarding of passwordless authentication technologies while improving security effectiveness and reducing management efforts and related costs.

Unfortunately, finding the optimal path to enabling passwordless authentication while achieving security assurance is often a confusing and time-consuming endeavor for IT and security managers. To help bring clarity to this decision-making process, Enterprise Management Associates (EMA) conducted primary, survey-based research into the requirements, challenges, and most effective approaches to authentication.[1] The results from the research provide clear indications of methods for simplifying the onboarding of passwordless authentication technologies while improving security effectiveness and reducing management efforts and related costs.

1 Passwordless Authentication: Bridging the Gap Between Low-Friction and High-Security Identity Management

EMA Research Study at a Glance...

Research Methodology

EMA conducted primary, survey-based research of IT professionals knowledgeable about the administration and use of identity and access management services in their organization. All respondents were carefully vetted to ensure credibility, and statistical results were calculated to be within a 5% margin of error.

Survey Demographics

- 200 respondents total
- 56.4% of respondents hold executive-level positions within their organizations
- Respondents were from a diverse range of business verticals, with 81% representing the following industries: high technology, manufacturing, professional services, healthcare, finance, retail, education
- Respondents were from a diverse range of business sizes
  - ► 37.5% from small businesses with less than 1,000 employees
  - ► 39.5% from medium businesses with between 1,000 and 7,500 employees
  - ► 23% from large business with greater than 7,500 employees
- 96.5% of respondents were physically located within North America

Key Findings

- Low-friction authentication solutions increase security effectiveness
- Low-friction authentication solutions substantially reduce administration efforts and related costs
- Passwordless authentication technologies are most frequently recognized as providing the lowest-friction user experiences
- Deployment challenges were indicated to be the greatest barrier to adoption of passwordless authentication technologies
- Deployment challenges are substantially reduced with the use of identity standards (such as FIDO and SAML) and integration with advanced identity management technologies

THE UNSUSTAINABILITY OF PASSWORD-BASED CONTROLS

Before determining the best approaches for adopting low-friction authentication solutions, it is important to recognize the greatest challenges to relying on traditional password controls and why they are no longer viable in today's dynamic business environments. EMA's survey results indicate that **64% of organizations continue to rely on passwords as a primary method of user identification.** Paradoxically, however, passwords do not actually identify users, but rather grant access to anyone who happens to know a particular string of characters, whether they are authorized to access business IT resources or not. This opens up a whole host of opportunities for nefarious characters to employ dubious methods to acquire passwords in order to gain access, including brute-force attacks, keystroke logging, and phishing schemes. Respondents also stated that reliance on passwords is creating significant security problems. **Overall, more than 90% of EMA survey respondents noted that their organization experienced a significant password policy violation by users in the preceding 12 months.** Most frequently reported were identical passwords being used to support multiple accounts (Figure 1).

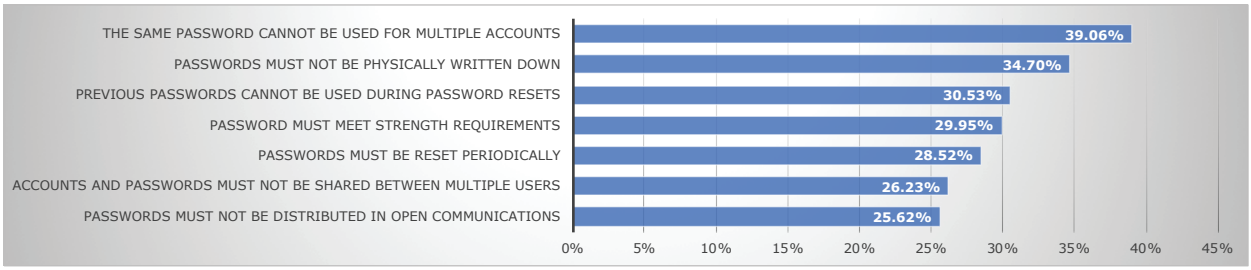


Figure 1: Percentage of survey respondents indicating a password policy violation that occurred in their organization within the last year

The high frequency of password-related policy violations is contributing to significant, real-world consequences for businesses and users. In total, 71% of survey responders were able to directly correlate access policy violations to specific penalties, including employee terminations, malware infections, compromised data, an inability to meet regulatory compliance objectives, loss of customers, and direct impacts to revenue generation (Figure 2). Additionally, an overreliance on passwords reduces administrator effectiveness and increases operational costs. EMA determined that increases in end-user friction results in a proportional increase in the number of user-reported problems that require administrator attention. On average, administrators spend roughly 27 hours each year resolving user access problems for every 100 users. To put this in perspective, an organization supporting 7,500 users must hire the equivalent of a full-time employee dedicated to continuously solving mundane user access problems.

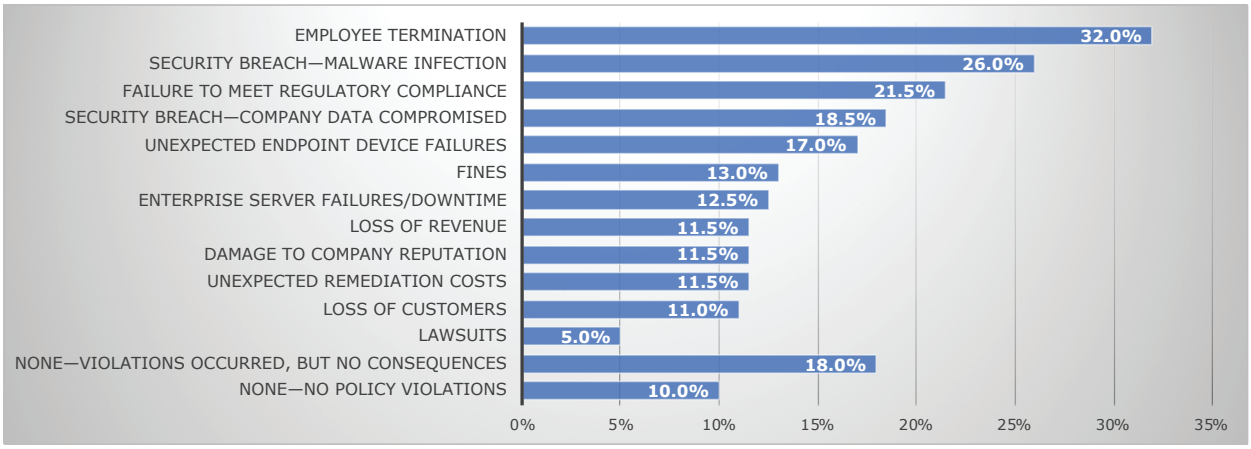


Figure 2: Percentage of respondents indicating consequences that occurred in their organization due to a violation of access management policies

KEY BENEFITS OF PASSWORDLESS AUTHENTICATION

According to EMA's research results, IT and security professionals recognize the advantages to utilizing passwordless authentication, and the majority of them recognize passwordless approaches to authentication as inherently more secure than passwords (Figure 3).

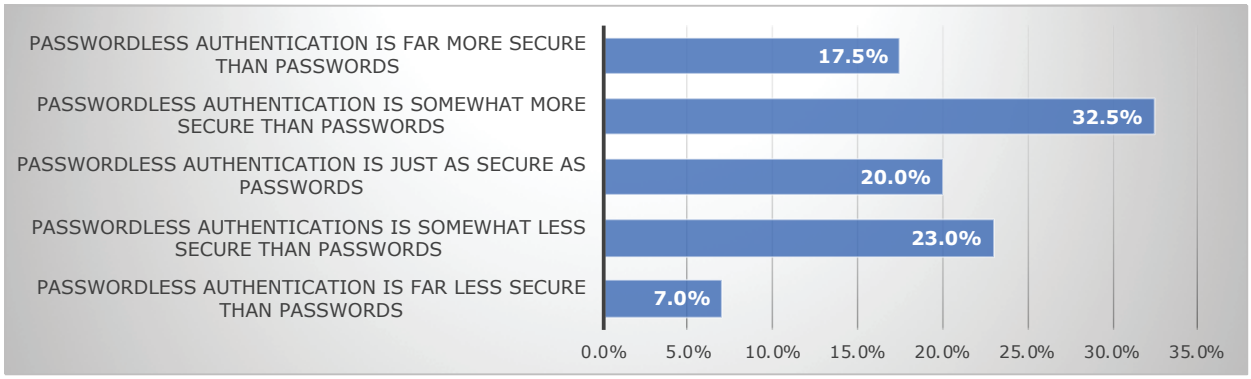


Figure 3: Percentage of respondents indicating their perceptions of the level of security offered by passwordless approaches to authentication

Of course, the most easily quantifiable value to passwordless authentication solutions is that they improve user experiences. Reducing user efforts results in increased workforce productivity, accelerated business agility, and improved user satisfaction, which in turn helps retain valued employees. Similarly, the adoption of passwordless authentication can have a profound effect on reducing administrator efforts and related costs. Overall, respondents to EMA's survey reported that biometric authentications and hardware tokens offer the greatest boost to end-user productivity. These technologies were also noted to provide the highest level of security, indicating a direct correlation between the amount of friction presented by the approach and the achieved level of security effectiveness.

Reducing user efforts results in increased workforce productivity, accelerated business agility, and improved user satisfaction, which in turn helps retain valued employees.

Authentication Type	Description	User Productivity Improvement	Security Effectiveness
Facial Recognition	A biometric technology that identifies users by their unique facial textures and shape	Very High	Very High
Fingerprint	A biometric technology that identifies users by reading the friction ridges of the user's thumb or other finger	High	Very High
Retinal Scan	A biometric technology that identifies users by scanning the unique patterns of a person's retina blood vessels	High	Very High
Behavioral Biometrics	Identifies users by monitoring their uniquely applied actions and mannerisms	Very High	High
Hardware Tokens	A physical device (such as a key fob, USB key, or smartcard) that provides an automatically-generated encrypted key that substitutes traditional passwords	Medium	High
Device Authentication	Allows users that have been positively identified on a personal device (such as a PC or mobile device) to gain access to approved IT services without the need to reauthenticate	Low (*)	Medium (*)
Voice Print	A biometric technology that identifies users by analyzing their unique acoustic patterns when speaking a predetermined word or phrase	Low	Medium
One-Time Passwords	Confirms users by delivering to a verified user's device or email address a password that is only valid for a single login session	Low	Medium
Personal Identification Number (PIN)	A short sequence of numbers (typically four to six characters) users memorize and enter when prompted to enable access	Low	Low
Password	A memorized string of characters consisting of letters, numbers, and/or symbols that is entered when prompted to enable access	Very Low	Low

** Note: The level of user productivity improvement and security effectiveness for device authentication are dependent on the types of solutions used to initially authenticate the user on their personal device. Represented here are averaged results from survey respondents.*

NAVIGATING THE JOURNEY TO PASSWORDLESS AUTHENTICATION

While there is an increased awareness of the value provided by low-friction authentication, the chief inhibitors to the adoption of passwordless approaches are concerns about the complexity of the deployment of the solutions. In other words, many organizations are reluctant to introduce passwordless authentication if they believe it will be challenging to deploy or disruptive to business operations. The most effective solutions include features supporting the "Four Is" of passwordless authentication:

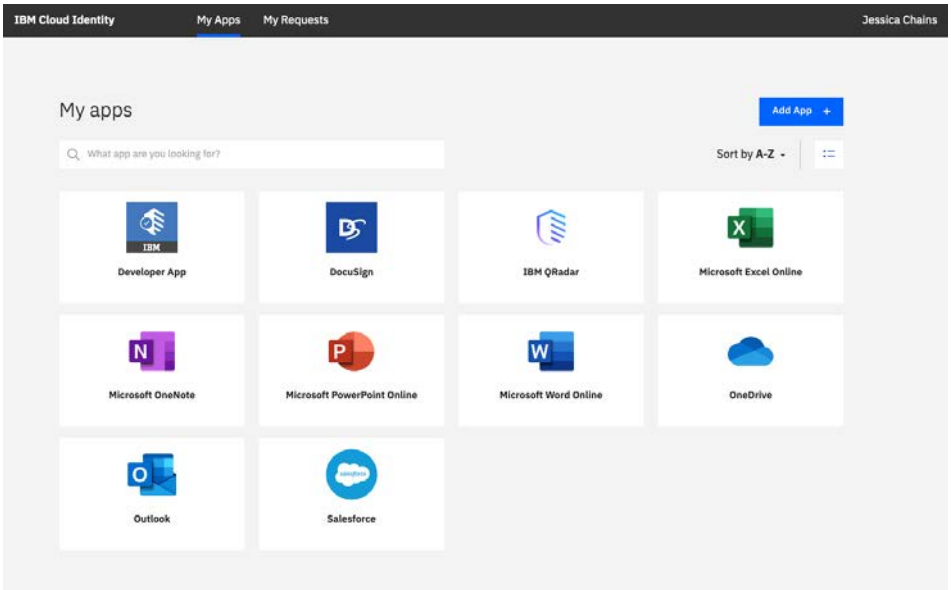
- **Intuitive** – Solutions should be easy to onboard, require little or no end-user training to use, and be simple to manage, requiring little administrator time to support.

- **Informative** – Holistic visibility should enable across the entire identity ecosystem to collect contextual data on users, devices, networks, and hosted services. Information reports should be easily digestible to simplify the identification of potential risks or challenges to user experiences.

- **Intelligent** – Intelligence technologies (such as analytics, machine learning, and language processing) should leverage collected identity data to determine the level of risk associated with enabling access. The number of authentication factors presented to the user should be dynamically determined based on the identified level of risk.

- **Integrated** – Solutions should leverage industry standards (such as FIDO, SAML, and Open ID Connect) to enable integrations between authentication technologies and hosted service. Direct integration with service, system, and security management platforms will further simplify administrative tasks and help consolidate access policy management.

A prime example of a solution designed to simplify the onboarding of low-friction passwordless authentication technologies is the IBM Cloud Identity platform. Designed to leverage existing on-premises identity and access management investments, IBM Cloud Identity enables centralized management of access between all endpoint devices and all hosted IT services. The solution works with key identity standards, including FIDO and SAML, to easily unify access controls for IT services hosted both on-premises and in the cloud. With thousands of prebuilt connectors included with the platform, organizations can quickly and easily enable access to the most popular SaaS applications using the most effective authentication methods. The solution is also designed to directly integrate with the unified endpoint management platform, IBM MaaS360, to establish seamless digital workspace experiences to end users. The simplicity and breadth of support offered by IBM Cloud Identity makes it easy for organizations to responsibly introduce passwordless authentication technologies that will boost user productivity while enhancing security effectiveness.



IBM Cloud Identity Dashboard

EMA PERSPECTIVE

Many IT and security professionals regard requirements for security and user access as diametrically opposed forces. The belief is that the more security is increased, the more user access is limited, and vice versa. However, there is no reason these two requirements need to be in conflict. EMA research results indicate that reduction in the amount of friction imposed on authentication processes proportionally increases the level of security. Additionally, by reducing the number of authentication steps, organizations proportionally reduce the amount of effort administrators must perform. In this way, low-friction passwordless authentication approaches effectively align user and business requirements.

Unfortunately, many organizations envision the need for complex technology introductions as necessary to deploying and maintaining low-friction authentication approaches. Indeed, organizations should not have to rip and replace existing identity technology investments, but instead should be able to enhance the resources they already have in place. The most effective solutions to responsibly introducing passwordless authentication are designed to systematically reduce the number of authentication steps by right-sizing the number and severity of challenges appropriate to the amount of risk associated with the access request. EMA recommends organizations adopt identity management solutions, such as IBM Cloud Identity, that enable the easy onboarding of passwordless authentication technologies that enhance security, boost user productivity, and reduce management efforts.

ABOUT IBM SECURITY

IBM offers an advanced and integrated portfolio of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter, or visit the IBM Security Intelligence blog. Additional information about IBM Cloud Identity can be found at https://ibm.co/2XOLQsx.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3868.07222019