WINMAGIC®

The Future of Cybersecurity
A Guide to Passwordless Authentication

Authenticate. Encrypt. Achieve.

WINMAGIC®

Introduction

Passwordless authentication solutions shouldn't jeopardize the user experience or productivity

With the increasing sophistication of cyberattacks, passwords are now considered one of the weakest links in cybersecurity. Today, IT and Security experts are turning toward passwordless solutions, which use advanced technology for user verification. Prominent authorities, including The World Wide Web Consortium (W3C) or FIDO, have set new standards for resilient passwordless authentication.

While security should be any enterprise's number one concern regarding user authentication, the industry has reached a pivotal stage where we can evolve the authentication experience into something seamless. Many passwordless authentication companies are relying on technology like one-time passcodes (OTPs), in-app push notifications or biometrics for two-step verification. But, more advanced companies offer solutions that don't jeopardize the user experience or productivity.

"Organizations try to balance strong security with convenience but often fail to achieve either."
– Forbes.[1]

In this guide, we'll introduce you to the latest up-and-coming innovations in passwordless authentication. Discover how the best passwordless solutions not only deliver unbelievable security but also

- A superior user experience that optimizes productivity
- Groundbreaking, continual "user + device" verification to support zero-trust frameworks
- Cost savings with seamless authentication and no password resets

74% of all breaches include a human element — like passwords.

Verizon 2023 Data Breach Investigations Report [2]

WINMAGIC®

Traditional MFA Doesn't Measure Up

Traditional Multi-Factor Authentication (MFA) has been widely adopted to enhance the security of online accounts by requiring users to provide additional verification beyond their password. This verification typically involves using a second factor such as an SMS code, one-time password (OTP) or push notification sent to a mobile device. While these methods do add an extra layer of protection, they're not phishing-resistant.

The Resilience of Phishing Attacks

Phishing attacks are a common tactic used by cybercriminals to steal login credentials and sensitive information. In a phishing attack, a hacker creates a fake login page that looks identical to the legitimate one and tricks the user into entering their credentials. With legacy MFA, even if a hacker obtains a user's password through a phishing attack, they would still need to provide the additional verification factor to access the account. However, hackers have found ways to bypass MFA and obtain the second factor as well. For example, they may use social engineering tactics to trick users into providing their second factor or use SIM swapping to intercept the verification code sent to a user's mobile device.

It's time to evolve beyond legacy MFA. Because hackers already have.

The one constant in cybersecurity is change. Today's best practices can become tomorrow's vulnerabilities — things can move that quickly.

For example, when the United States released its Zero Trust Maturity Model in support of Executive Order 14028, it recommended government employees and contractors — and, by extension, any organization — to stop using legacy MFA solutions based on SMS text, OTP and push notification because they can be subverted by phishing attacks.

WINMAGIC®

What is Passwordless Authentication?

“By 2025 more than 50% of the workforce and more than 20% of customer authentication transactions will be passwordless, up from less than 10% today.”
Gartner ® [3]

Passwordless authentication is a new approach to online security that aims to eliminate the use of passwords altogether. Instead of relying on users to create and remember complex passwords, typical passwordless authentication uses other forms of user verification, such as biometric data or hardware tokens. This approach seeks to address the weaknesses of traditional password-based authentication, such as the risk of weak passwords, phishing attacks and password reuse. By removing the reliance on passwords, passwordless authentication provides a more secure and seamless user experience.

Looking ahead, while they do enhance security, hardware tokens and even biometrics for user verification aren’t necessary. In fact, your modern computer comes with security measures far more advanced than any human action or credential.

Should users have to reauthenticate themselves every time they access online apps?

Founded in 2013, the FIDO Alliance established that high-level security should use public-key cryptography to verify the end device, not just the user. By following FIDO2 protocols, authentication solutions can deliver robust security that verifies the user’s endpoint device every time the user logs into an online application or service.

Still, should users have to reauthenticate themselves to each online application and service every time they access them? Once the user has logged into the endpoint, they’ve already unbreakably proven that the authentic user is using the authentic device.

WinMagic realized this redundancy and suboptimal user experience. In 2022, we released MagicEndpoint — a passwordless solution that securely **authenticates the user to online applications without any user action after the user has logged into the endpoint**.

Your computer comes with security measures far more advanced than any human action.

Achieving Continuous Zero-Trust Security in Real-Time

79% of organizations breached didn't deploy zero-trust architecture.
IMB Security [4]

In 2022, the U.S. government released Memorandum M-22-09: Federal Zero Trust Strategy. This strategy is designed to combat the increasingly sophisticated and persistent nature of cyberattacks.

The foundation of zero-trust security is the concept of "never trust — always verify." This perspective presses that no actor, system, network or service outside or within the security perimeter will be trusted.

When it comes to user authentication, M-22-09 outlines these key requirements:

- User identity verification
- Device verification
- Continual verification of user and device

Since the memorandum was released, some passwordless authentication solutions now offer "zero-trust architecture" yet overlook one key element: continual verification.

WinMagic bridges this gap with an innovative approach to zero-trust authentication. Our solutions verify the "user + device" entity at preboot log-in and Windows sign-on through MFA using a phone (over Bluetooth or the network), smartcard, USB tokens, TPM-protected PIN, password, biometrics, pre-boot networking and backup methods.

Because MagicEndpoint is the only solution that doesn't require any user action for online authentication, it can verify the user and device as often as needed. The software offers continual, event-driven verification of the device, the user's actions and even the user's intent in real-time. Based on groundbreaking principles, MagicEndpoint provides the authentication elements of zero-trust architecture to support enterprises on their zero-trust journey.

Secure FIDO public key authentication

The TPM Root of Trust (RoT) is used to verify the "user + device" entity, proving unbreakably that the authentic user is using the authentic endpoint in real-time.

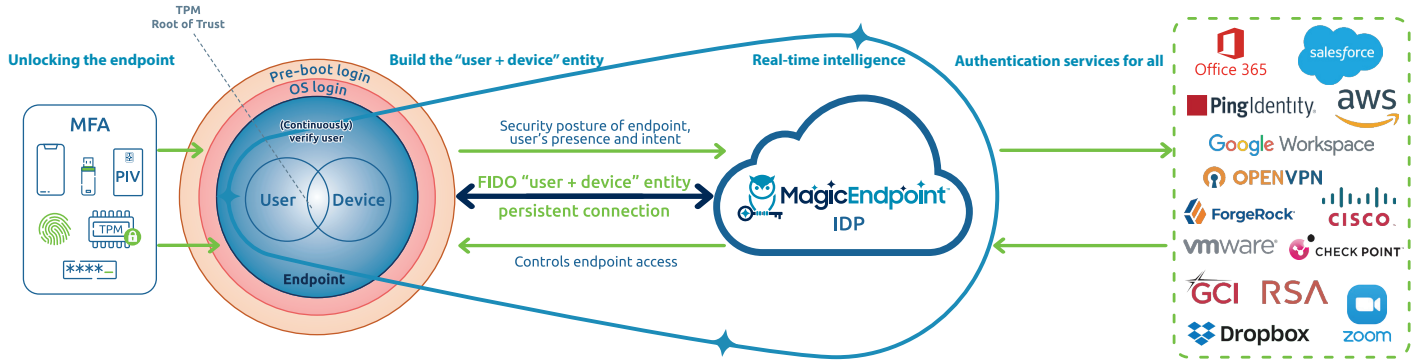
Zero trust "always verify"

Event-driven, continuous "user + device" verification with the trusted, authentic endpoint, independently from applications.

Federated authentication

With trusted detailed real-time "user + device" intelligence, MagicEndpoint can provide federated authentication services without further verification upon application requests.

MagicEndpoint Center



MagicEndpoint provides the authentication elements of zero-trust architecture to support enterprises on their zero-trust journey.

WINMAGIC®

Choosing a Passwordless Solution

With leading cybersecurity authorities supporting passwordless as a more secure option for user authentication, the market is becoming inundated with passwordless solutions. So, how do you pick the right one? Here are some tips for choosing a product that'll deliver a great ROI.

Security	The most important factor to consider is the security of the authentication solution. Make sure the solution you choose is phishing-resistant, delivers continuous verification and meets the highest security standards.
✓	Founded on cutting-edge security, MagicEndpoint follows FIDO protocols and zero-trust frameworks, meeting today's most sophisticated cybersecurity standards.
User experience	Passwordless authentication shouldn't get in the way of productivity. Look for a solution that's easy to use and doesn't require users to jump through too many hoops to access their accounts.
✓	MagicEndpoint doesn't sacrifice the user experience to achieve maximum security. Log into online applications and services without any user action!
Integration	Ensure that the passwordless authentication solution integrates with your existing systems and applications. This benefit will help avoid disruptions and minimize the need for additional training and support.
✓	MagicEndpoint is compatible with Windows environments and will support MacOS and Linux in the future. The software grants passwordless authentication to applications and services supporting federation protocols SAML, OIDC, Radius, LDAP and more.
Compliance	If you're subject to regulatory requirements, make sure the passwordless authentication solution you choose meets those requirements.
✓	MagicEndpoint aligns with the US government's 2021 Executive Order 14028 recommendations regarding zero trust and can be customized to support all cyber insurance requirements.
Cost	Consider the cost of the passwordless authentication solution, including any hardware or software licenses, maintenance fees and ongoing support costs.
✓	MagicEndpoint doesn't require any external hardware keys and therefore reduces costs by using technologies employees already have on hand. Going passwordless also saves on service desk calls by eliminating password reset tickets.
Scalability	As your company grows, your authentication needs may change. Choose a solution that can scale with your company and adapt to changing security requirements.
✓	MagicEndpoint offers features and customization for complex environments and changing requirements. Each product update enhances scalability for your enterprise, keeping up with changing security requirements.

By considering these factors, you can choose a passwordless authentication solution that provides a secure and convenient way for users to access their accounts without the need for passwords.

The typical cost of a single password reset is $70.

Forbes [5]

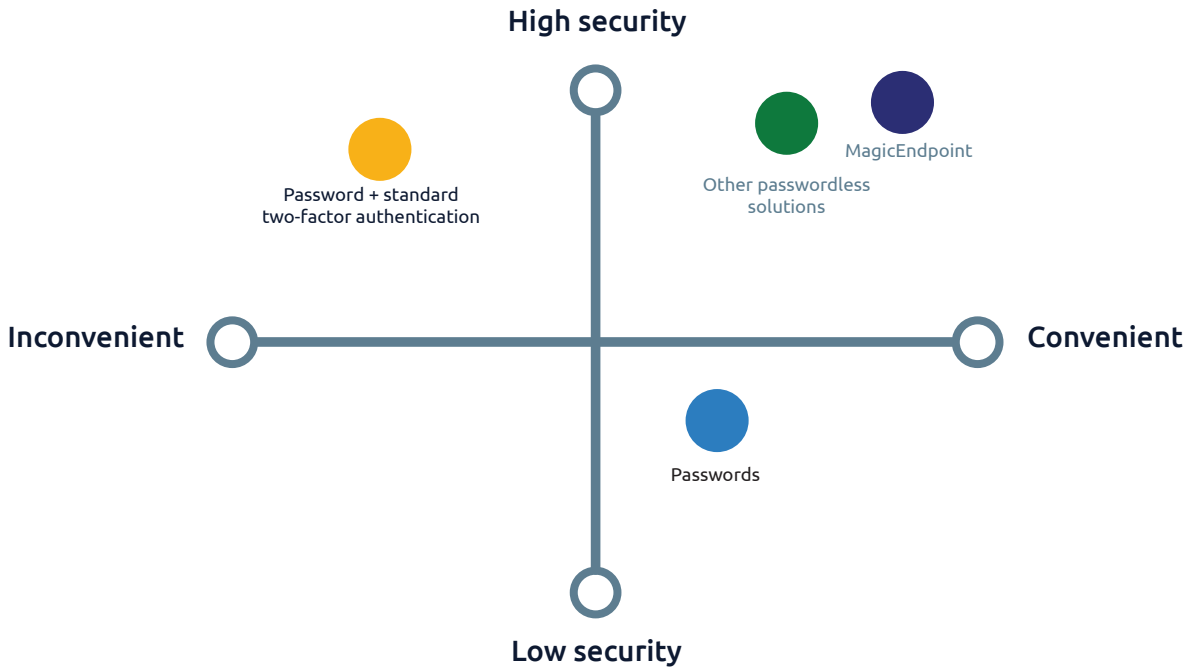
WINMAGIC®

MagicEndpoint Transforms User Authentication

No user action.
No passwords.
No friction.

Just secure remote access.

Most endpoints today have built-in, device-bound security keys. By using the capable endpoint correctly, customers can secure enterprises with device-bound security keys and the best possible user experience: no user action required. MagicEndpoint frees users from all online authentication steps while performing secure "device + user" authentication, at times continuously. It's seamless, phishing-resistant and virtually invisible to the user.



WINMAGIC®

Passwordless Authentication Use Cases

Finance

Sean is a branch manager at a bank. Because he handles sensitive client and employee information, Sean is required to lock his computer every time he's away from his desk. When he returns to his computer, he has to go through a lengthy two-factor authentication process of typing in his password, opening his authenticator app and approving a Push notification to finally gain access to his computer.

MagicEndpoint offers a passwordless experience that gets Sean into his computer faster without sacrificing security. As Sean walks into his office, he opens the MagicEndpoint app and wakes up his computer. The app then connects to his computer using localized BLE. Not only does the software authenticate Sean, securely verifying both the user and device, but also provides seamless, no-user-action access to online apps and services.

Enterprise

Rene is a remote employee and works entirely from her home office. Whenever she unlocks her computer, she has to enter in her password, open her phone authenticator app and type in an OTP to be authenticated. Furthermore, to access online apps or services, she must pull out her phone, open an authenticator app, get a new OTP and type it in, wasting time and slicing her productivity.

With MagicEndpoint, the endpoint handles authentication on the user's behalf. With a tap in the MagicEndpoint authenticator app, the software delivers passwordless pre-boot sign-on and Windows log-in. Once Rene has been authenticated, she enjoys seamless access to her online apps and services — no user action required! This no-user-action approach helps eliminate time spent on passwords, OTPs and other time-consuming authentication steps.

Healthcare

Kate is a nurse in a city hospital. It's her job to deliver direct care to patients, monitor them and reassess, within her scope. During every shift, she signs into multiple computers throughout the ward to update patient records. Every time she logs in, she loses valuable time remembering and entering a highly-complex password instead of moving on to the next patient.

MagicEndpoint supports multiple users per device. So, to access any of the five computers in her ward, all Kate has to do is securely log into her phone and open her WinMagic authenticator app, then tap "Authenticate" to seamlessly log into any of her usual computers. The process is passwordless, saving Kate from having to remember a complex password that changes every three months, and saving the Help Desk from password reset tickets.

WINMAGIC®

Common Questions

Is passwordless authentication difficult to integrate?

Generally, passwordless authentication solutions are more difficult to integrate than passwords, but easier to implement and maintain than technology like legacy MFA, hardware keys and more.

Can a phone offer secure multi-factor authentication (MFA)?

MagicEndpoint natively uses Bluetooth Low Energy (BLE) MFA with preboot login and Windows sign-on compared to legacy MFA methods that rely on the network. For online services, WinMagic has advanced past MFA and supports passwordless, federated authentication.

Note: MagicEndpoint may be configured to support MFA using a phone (over Bluetooth or the network), smartcard, USB tokens, TPM-protected PIN, password, biometrics, pre-boot networking and backup methods.

Will there be a surge in support desk tickets?

Quite the opposite. By removing passwords from the equation, going passwordless decreases the number of service desk tickets by eliminating password reset requests.

Does going passwordless mean my passwords will stop working?

For the most part with online apps, passwords won't be in the equation at all once federation is commonplace.

For endpoint access, your password won't work for the devices that are configured to be passwordless. However, if the same Windows account is used to access other endpoints or services that have not yet been configured with passwordless authentication, your password will continue to work for those.

Do all my online apps and services support passwordless?

All apps that offer federated authentication through one of the supported authentication protocols can be passwordless. WinMagic offers the largest set of compatible authentication protocols including SAML, OIDC, Radius, LDAP and even some of the lesser-known ones such as WS-Fed and WS-Trust.

Why is zero-trust security important to my company?

Zero-trust security is considered the paradigm for keeping your data out of the hands of hackers. With this level of cybersecurity, companies can feel safe and potentially save millions by preventing cyber attacks.

References

[1] Forbes “Embracing the End Of The Password Here And Now”

[2] Verizon 2023 Data Breach Investigations Report

[3] Gartner® Research, Take 3 Steps Toward Passwordless Authentication, 22 February 2023

[4] IBM Cost of a Data Breach Report 2022

[5] Forrester Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers

Garry McCracken, CISSP at Winmagic, has more than 30 years of experience in data communications and information security. He’s contributed to developing WinMagic’s full-disk encryption and passwordless authentication solutions for desktops, laptops and other mobile devices. For over 10 years, Garry has been writing for WinMagic from a position of technical expertise, making him the company’s longest-running writer.

About WinMagic
With over 25 years of continuous innovation, WinMagic is a leading authority in endpoint encryption and authentication solutions.

WinMagic’s passwordless authentication solution, MagicEndpoint, uses MFA to authorize endpoint access via a smartcard, USB token, phone, TPM, PIN, password or combinations for Windows and preboot sign-on. Users are then granted secure, passwordless authentication to online applications and services without requiring any user action. The solution supports zero-trust security frameworks by continuously verifying the endpoint’s security posture plus the user’s presence and intent.

Founded on public-key-based FIDO standards, MagicEndpoint offers the most secure online authentication while delivering the best user experience with no user action.

Learn more
Learn more about WinMagic’s groundbreaking approach to passwordless authentication.

- Passwordless Authentication
- Pre-boot Authentication
- Secure Authentication for Federal Government
- Demos and More

US & Canada +1 888 879 5879 | EMEA +49 69 175 370 530 | Japan +03 5403 6950

For more information, click here or contact WinMagic

Authenticate. Encrypt. Achieve.