



2022 Guide to Passwordless Authentication



What's the Problem with Passwords?

Computers have been around since the 1960s and since then they have evolved considerably. One thing that has remained constant since then however is **passwords**. Passwords have been around since the earliest days of computing as a line of defense for user security.

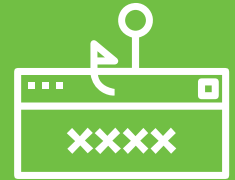
But passwords aren't actually that secure. No matter how good a password is, or how well implemented the authentication system, there's always a risk bad actors will compromise credentials. Add to that more resources in the cloud. More people working remotely on their own networks and from various devices. In that environment, ensuring the safety of corporate assets is a challenge.

The Damage

Like with anything though, technology has evolved considerably, and it is no longer optimal or even necessary for a company to have to use passwords. In fact, passwords actually end up costing an organization a considerable amount, as a single password reset can cost organizations an **average of \$70* per reset**. Over the course of time, many large companies actually end up spending over \$1 million annually** on password related support costs.

■ Did you know? ■

Stolen or poor passwords are responsible for over 80% of data breaches?



A Possible Solution

In recent years, user security has become even more complex with the introduction of MFA (Multi-Factor-Authentication). MFA can be frustrating for a user because of the time it takes and can be even more frustrating with the knowledge that it is not infallibly secure. Ideally, a user would want an authentication system that requires **no action on the part of the user** and is as close to infallibly secure as possible.

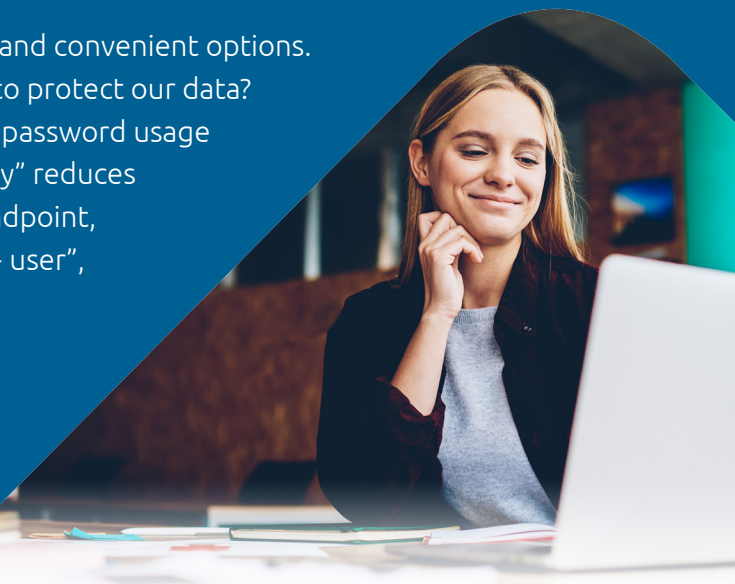
Traditional authentication systems like Push, SMS and OTP not only require user action, but are very difficult to deploy and are prone to out of bound push attacks.

Technology has come a long way and we have more secure and convenient options. So why are we still using outdated and inferior technology to protect our data? In the next few slides, we detail out the vulnerabilities with password usage and show you how a concept called Zero-Trust "always verify" reduces the burden of security from the user, and brings it to the endpoint, thereby only accepting a combined identity of the "device + user", instead of "user-only".

Source:

* <https://thehackernews.com/2021/04/cost-of-account-unlocks-and-password.html>

** <https://blog.lastpass.com/2018/05/new-forrester-report-real-cost-password-risks>



WINMAGIC[®]

MagicEndpoint Authentication

The future of passwordless is here with WinMagic's zero-factor authentication solution.



Next Generation Passwordless Authentication

WinMagic's products consist of a suite of encryption and authentication solutions which helps organizations achieve their Zero-Trust strategy. It includes next generation zero-factor authentication capability which seamlessly alleviates the user of the authentication burden. Working silently in the background MagicEndpoint performs ongoing user+device authentication as well as device health checks enabling businesses reach their Zero-Trust goals by making "always verify" possible without any burden to the end user.

Combating a Vulnerable Situation

Password Compromise



Passwords are responsible for over 80% of data breaches. Passwords can be phished, are difficult to remember and expensive to reset.

MFA



Traditional MFA still leaves enterprises vulnerable to phishing attacks which can lead to credential theft and breaches.

Ransomware Attacks



In Q1/20-Q3/21 the average downtime after a ransomware attack had increased from 15 to 22 days.

Source: [Statista 2021](#)

Fundamental Pillars

With zero-factor authentication, MagicEndpoint is the best authentication solution for an undoubtedly superior user experience, and unsurpassable security, which is all based on a zero-trust “always verify” principle. WinMagic offers customers a new authentication paradigm in cybersecurity. Made possible by making the endpoint the combined identity for “device + user” where applicable.

Undoubtedly the Best User Experience

No user action is required! With MagicEndpoint's implementation of Zero-Factor authentication the server seamlessly performs the physical, online crypto-based authentication.

This ongoing authentication simultaneously authenticates the user and the endpoint.

Unsurpassed Security

For the server, the client is not just the user but always a “user on an endpoint” with the endpoint being unmistakable. The solution's combined device+user identity confirms the endpoint is doing verification on a regular basis. Hackers would have to be in possession of your laptop, then try to unlock your laptop before gaining access your online resources.

“Always Verify” Principle

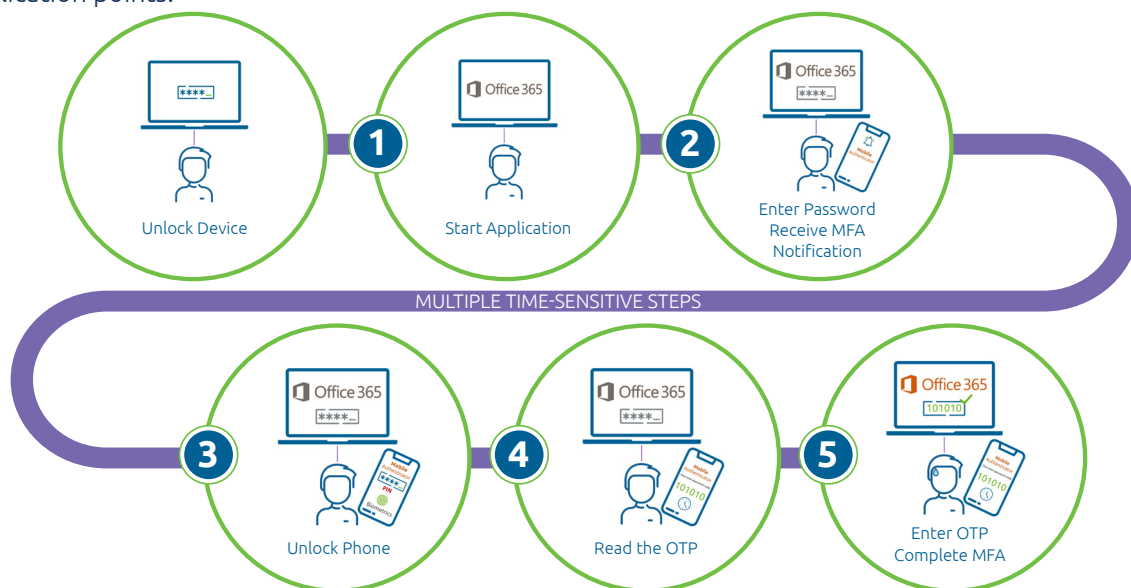
This solution goes beyond SSO and IdP identity provider capability. MagicEndpoint Authentication promotes a never trust, “**always verify**” principle. The smart endpoint performs authentication to the endpoint on an ongoing basis.

No more burden on the user. MagicEndpoint Authentication securely does it all...again and again

Dramatically Simplified Authentication with Unsurpassed Security – From 5 steps to 1

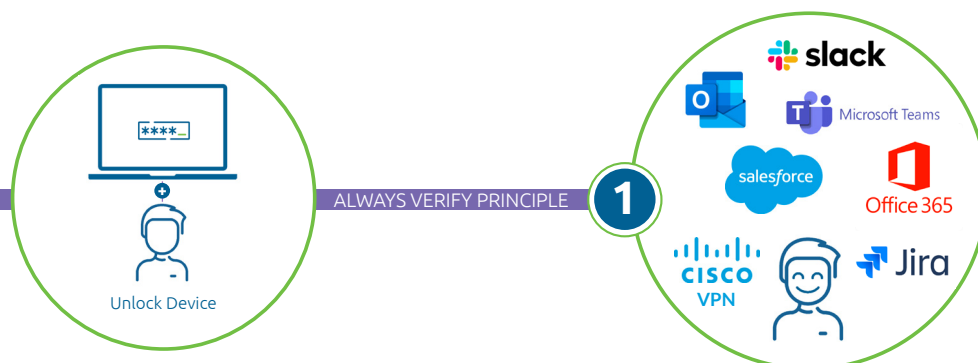
Without MagicEndpoint Authentication:

Cumbersome steps are needed to authenticate with traditional methods and the user must authenticate at multiple server & application points.



With MagicEndpoint Authentication:

No user authentication is required for secure access to servers & applications in a MagicEndpoint zero-factor environment.



The combined identity of device+user performs all remote authentications.

 WINMAGIC® Competitive Analysis	Traditional MFA (OTP, SMS, Mobile Push)	Windows Hello with Microsoft Authenticator and Azure AD	Passwordless Solutions	MagicEndpoint Authentication
User Authentication				
No user action required (Zero Factor Authentication)	✗	✗	✗	✓
Single Sign-on into the OS and applications from encryption preboot environment	✗	✗	✗	✓
Using the device, phone, or token	✓	✗	✗	✓
Enterprise Management				
Easy to deploy	✗	✗	✓	✓
Support for shared devices (kiosks)	✓	✗	✓	✓
Endpoint measured health checks (signals/conditional access)	✗	✗	✗	✓
Security				
Guard against Out-of-Band (OOB) push attacks	✗	✗	✗	✓
Guard against SolarWinds MFA bypass hack	✗	✗	✗	✓
Zero Trust Authentication				
Zero Trust Network Access (Never trust, always verify)	✗	✗	✓	✓
Device and User Trust	✗	✗	✗	✓

Why MagicEndpoint?

■ Achieve the Ideal World of No User “Action” Authentication

Does your organization ask users to use MFA such as SMS, OTP or Push? With MagicEndpoint Authentication users do not need to do anything. The solution transparently and securely takes care of the necessary authentications. Users enjoy freedom from disruptive logins!

Remote users, and users sharing the endpoint can rest assured – corporate services and applications are accessible remotely and are only accessible to the authorized device user.

■ Account Takeovers: A Thing of the Past!

Hackers would need to physically have your laptop and unlock it to access your systems.



WinMagic's Next Generation Solutions:

20-Years of Full Disk Encryption Experience

Security starts with the endpoint. With more than 20 years of continuous innovation, WinMagic takes pride in using cryptography and engineering capabilities to provide secure, feature-rich, and comprehensive solutions in both encryption and authentication.

WinMagic Full-Disk Encryption (FDE) allows enterprises to centrally manage encryption on devices across all platforms using a choice of SecureDoc FDE, FileVault2, BitLocker, dm-crypt, and Self Encrypting Drives. Providing comprehensive encryption: one solution with cross platform encryption capability.



Zero-factor authentication undoubtedly provides the best user experience one could hope for, providing secure authentication without requiring user action. We are very pleased to offer this to our customers so that breaches from account takeovers are no longer a problem."

– Thi Nguyen-Huu, WinMagic Founder and CEO

This Solution is Right For Your Organization

Security is universally valuable. For organizations that need encryption and authentication protection of their mission critical systems, MagicEndpoint is your solution.



Manufacture



Banking



Government



Healthcare

Start Your MagicEndpoint Authentication Journey Today!

Contact Your MagicEndpoint Specialist:

www.winmagic.com/magicendpoint/

WinMagic provides critical software solutions to enterprises around the world. As a trusted and recognized global IT security provider, Winmagic is focused on and dedicated to delivering intelligent solutions for Encryption and Authentication. Over 2500 customers in more than 90 countries use our encryption and authentication solutions to help them keep their day-to-day operations running smoothly. Our customers are at the center of everything we do and our singular goal is to deliver the right solutions for their industry-specific IT security needs helping to keep them at the forefront of their industries. For more information, visit www.winmagic.com.



 **WINMAGIC**[®]

US & Canada

+1 888 879 5879

EMEA

+49 69 175 370 530

Japan

+03 5403 6950

For more information, [click here](#) or contact WinMagic