YOUR GUIDE TO GOING PASSWORDLESS IN 2022

WINMAGIC®

Introduction to Passwordless

Passwords are becoming a thing of the past.

Did you know the first digital password was created in the 1960s? Yep, the first password was created for the Massachusetts Institute of Technology's massive time-sharing computer called a Compatible Time-Sharing System (CTSS).

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. Perhaps that's why stolen or poor passwords are responsible for over 80% of data breaches.

The rise of remote access has also given rise to ever-more sophisticated ransomware and other cyber-attacks. To combat these attacks, a host of MFA, SSO and passwordless authentication solutions have been created. But they all miss the mark. Why? Because their focus is either on the user or third-party devices like phones, which can slow productivity and increase risk.

Introducing Magic Endpoint Passwordless Authentication

Magic Endpoint from WinMagic is the passwordless authentication solution that protects access by focusing on the endpoint, not the user. It requires no user action, and not third-party devices or keys, so it's seamless, secure and virtually invisible.

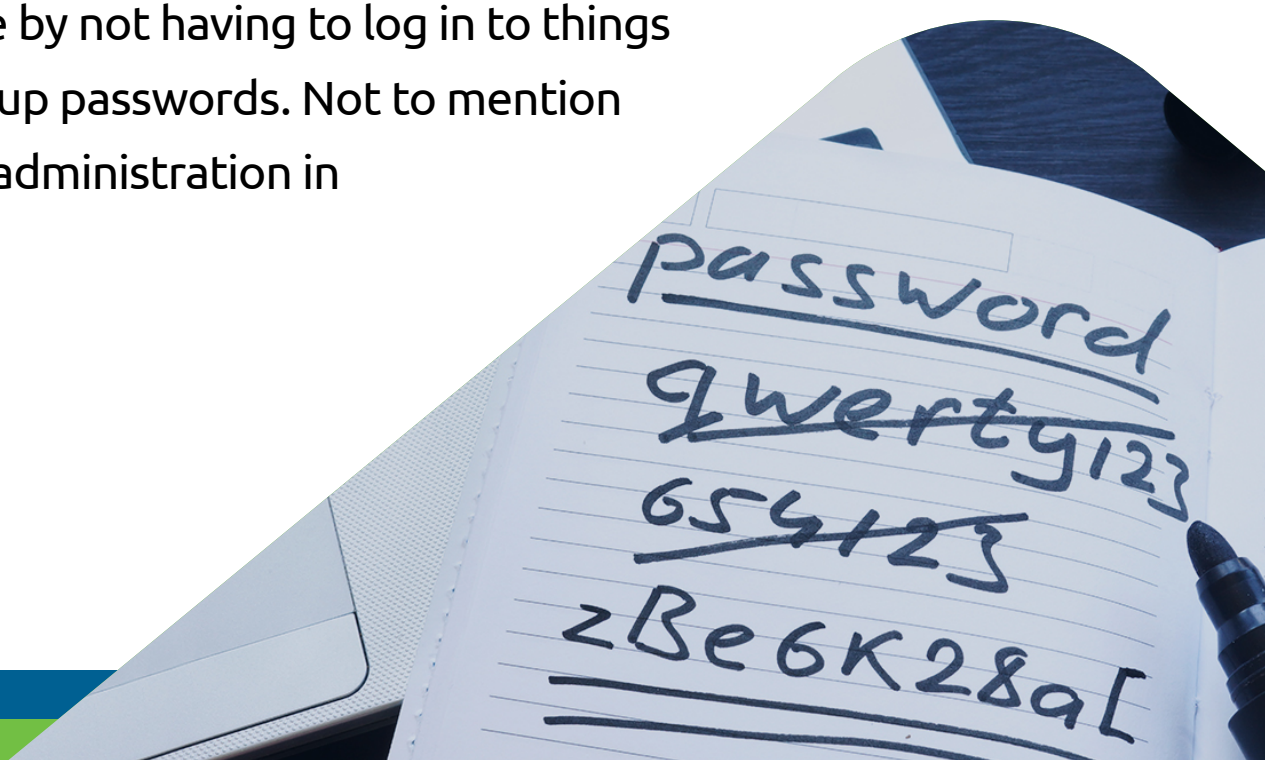
Gartner predicts that this year, 60% of large and global enterprises, and 90 percent of mid-size enterprises will implement passwordless methods in more than 50% of use cases.

Here are our top 8 reasons why passwordless is the future.

#1

Say Goodbye to Annoying Password Management

Passwords are easy to mistype or forget. And why are there so many!? To make things easier, we make up weak “MacGyver-style” passwords like p@ssw0rd. We write them down on sticky notes or keep them in a document on the computer - thus putting data at risk. With passwordless authentication, there are no passwords to maintain. Save time by not having to log in to things over and over or look up passwords. Not to mention the cost of password administration in your organization.



#2

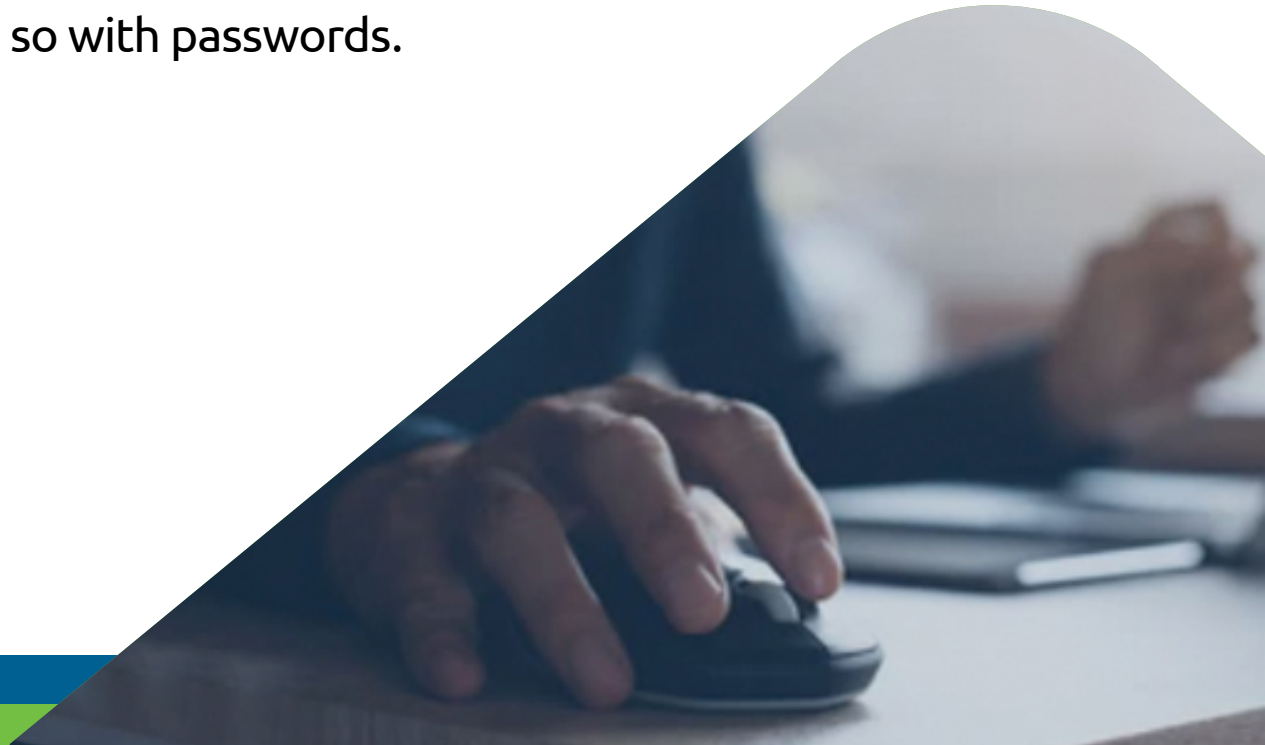
Save Money on IT Support

Forrester Research determined that large organizations spend up to $1 million per year on staffing and infrastructure to handle password resets alone. Passwordless authentication can drastically reduce help desk calls.

#3

Reduce The Risk Of Bot Attacks

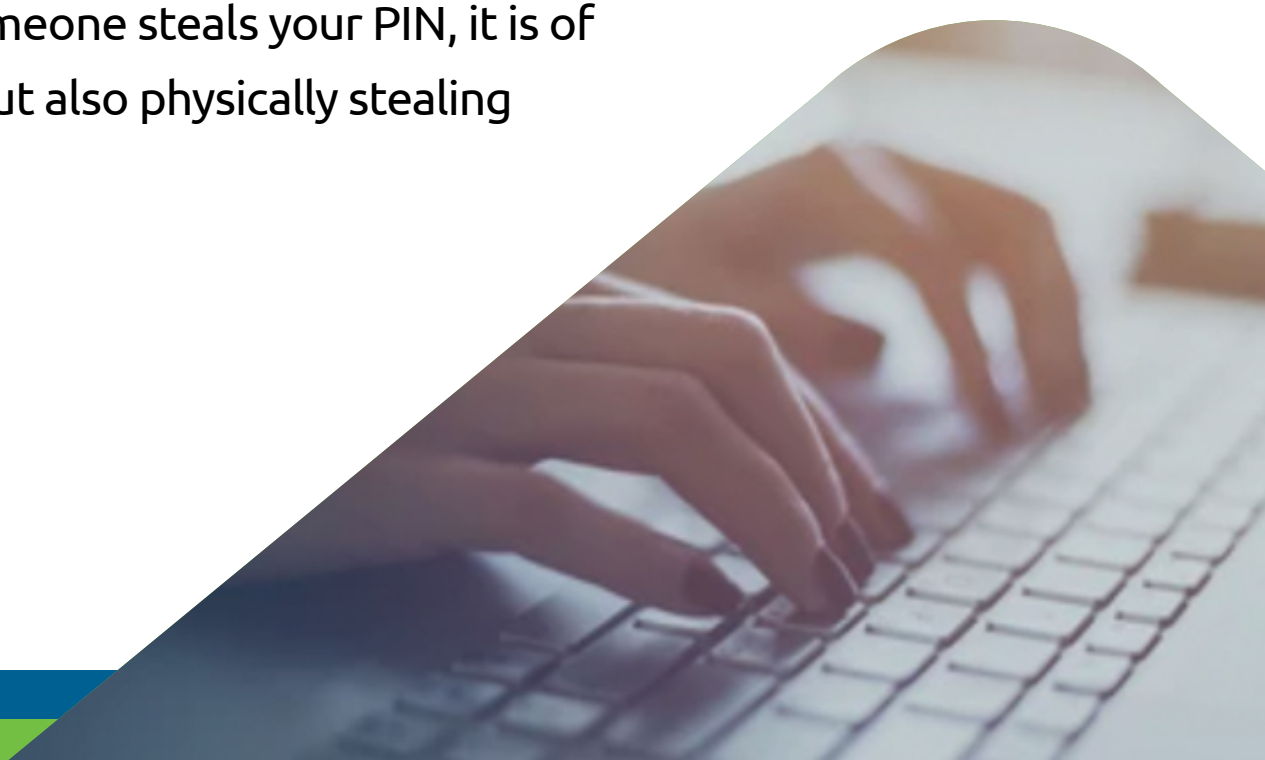
Bot attacks are an increasing cyber-threat for enterprise companies, yet few are prepared to fight them. Bot-based attacks are complex and can take many forms, and passwords are susceptible to them. Passwordless authentication mitigates that risk. By having a user actively click on their screen or enter a pin to authenticate, you can prove there is a human on the other end. Not so with passwords.



#4

Protect Your Data From Malicious Malware Attacks

Keyloggers use malware to spy on users remotely as they type login information. They literally record keystrokes as they happen, essentially stealing precious user passwords. This type of attack is very popular for grabbing bank details and hijacking business email accounts. When you go passwordless, you mitigate this attack. Even if someone steals your PIN, it is of no use to them without also physically stealing your device.



#5

Thwart Business Email Compromise Attacks

Speaking of email account hacking, Business Email Compromise (BEC) scams use phishing, spoofing, and keylogging to enable fraudulent money transfers. They use crafty emails to pose as CEOs, executives, vendors, or suppliers requesting a payment or transfer. Protect your employees from costly and embarrassing BEC scams by cutting fraudsters off at the source.

#6

Avoid SMS Attacks During 2Factor Authentication

One of the most common methods of two-factor authentication (2FA) and two-step verification is an SMS or text message. But text messages are insecure and thus vulnerable to attack. From code-cracking and phishing to spoofing and SIM swapping, there are a number of ways for hackers to intercept your SMS code and gain access to private data.

Passwordless authentication is a safer alternative to 2FA since it doesn't rely on SMS text messages.

#7

Easy to Integrate Into Your Organization & Seamless Integration With Your Existing Tech Stack

The movement is already in motion! That means passwordless authentication is now available for endpoint devices. Passwordless authentication is easy to integrate with enterprise solutions like Microsoft Office 365, Windows Logon, SaaS applications, VPN, and more.

#8

Choices Available to Fit Every Situation

One size does not fit all when it comes to authentication. Certain authentication methods may not be reliable, depending on the situation. That's why passwordless authentication offers options for what can be used as a Security Key*:

- Software-based authenticators (Eg: FIDO certified)
- Trusted Platform Module (TPM) based authenticators (Eg: FIDO certified)
- Certificate-based Passwordless Authentication (Eg: VPN)
- Smartphone-based authenticators (Eg: usingBluetooth connectivity)
- Hardware-based authenticators (Eg: USB connectors)
- Biometrics-based authenticators (Eg: fingerprint, face recognition)

* Both our Software and TPM based FIDO Security Keys are

Endpoint focused. Incredibly secure. Practically invisible. That's Magic Endpoint Passwordless Authentication.

WinMagic's Magic Endpoint includes next generation zero-factor authentication capability which seamlessly alleviates the user of the authentication burden making it a true passwordless authentication solution. Working silently in the background Magic Endpoint 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.

Contact WinMagic to get an initial consultation or a FREE demo.

Email sales@winmagic.com to begin your Passwordless journey!

WINMAGIC®

MagicEndpoint

About the FIDO Alliance

The FIDO (Fast ID Online) Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The FIDO Alliance is working to change the nature of authentication with open standards that are more secure than passwords and SMS OTPs, simpler for consumers to use, and easier for service providers to deploy and manage.

FIDO uses standard public key cryptography techniques to provide stronger authentication. It supports a full range of authentication technologies, including biometrics such as fingerprint and iris scanners, voice and facial recognition, as well as existing solutions and communications standards, such as Trusted Platform Modules (TPM), USB security tokens, embedded Secure Elements (eSE), smart cards, and near field communication (NFC).

Magic Endpoint Passwordless Authentication by WinMagic

With WinMagic, get a comprehensive multi-platform client software supporting from the easiest to the highest end encryption needs. Your computing device – mainly the laptop – protected by Magic Endpoint, offers businesses an easy entry to the passwordless era, with the fewest moving parts. Simply being logged in to a Magic Endpoint-encrypted device can serve as the one-time set of credentials that permit users access to all approved applications and sites. WinMagic is a member of FIDO Alliance since September 2020.