

# PASSWORDLESS

The future of identity and access security

Passwords are no longer the most secure and effective method to protect access to our systems

**U\$155.000**

losses, on average, a medium-sized company incurs for each password attack.

(Kaspersky).

**U\$2.9 MILLION**

cybercrime costs the global economy suffers every minute, with 80% of those attacks directed at passwords. (World Economic Forum).

**100 PASSWORDS**

are used by an average person across different sites (NordPass), and just 31.3% of users create new passwords "once or twice a year". (Digital Guardian).

**+40 MM USERS**

use 100.000 of the most common passwords that a cybercriminal could obtain in just one second. (NCSB).

**84%**

of organizations have adopted new authentication methods in the last 2 years. (MobileIron).

Passwords generate vulnerabilities and enable attacks

## Passwords are not enough

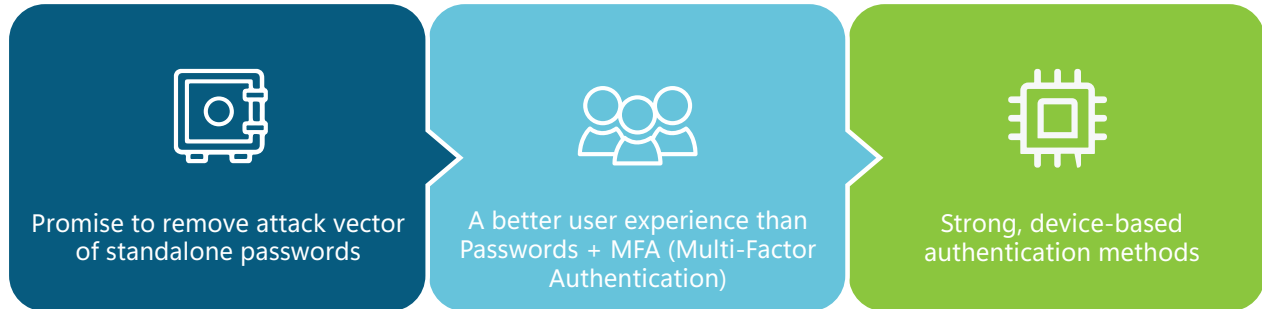
Passwords are becoming a relic of the past. The use of passwords leaves us increasingly vulnerable as we become more predictable in generating them. Trying to combat this with requirements for stronger complexity and frequent updates makes it harder to be productive, drives up already-high costs in password maintenance and support, and still isn't enough to keep up with current cybersecurity threats. (Microsoft)

## Attacks and security gaps

- ? Guessing
- 👊 Brute force
- 🔄 Replay
- \*\*\* Password spraying
- 📧 Phishing
- 🧠 Social engineering
- 👤 Man-In-the-middle
- 🔑 Key-logger

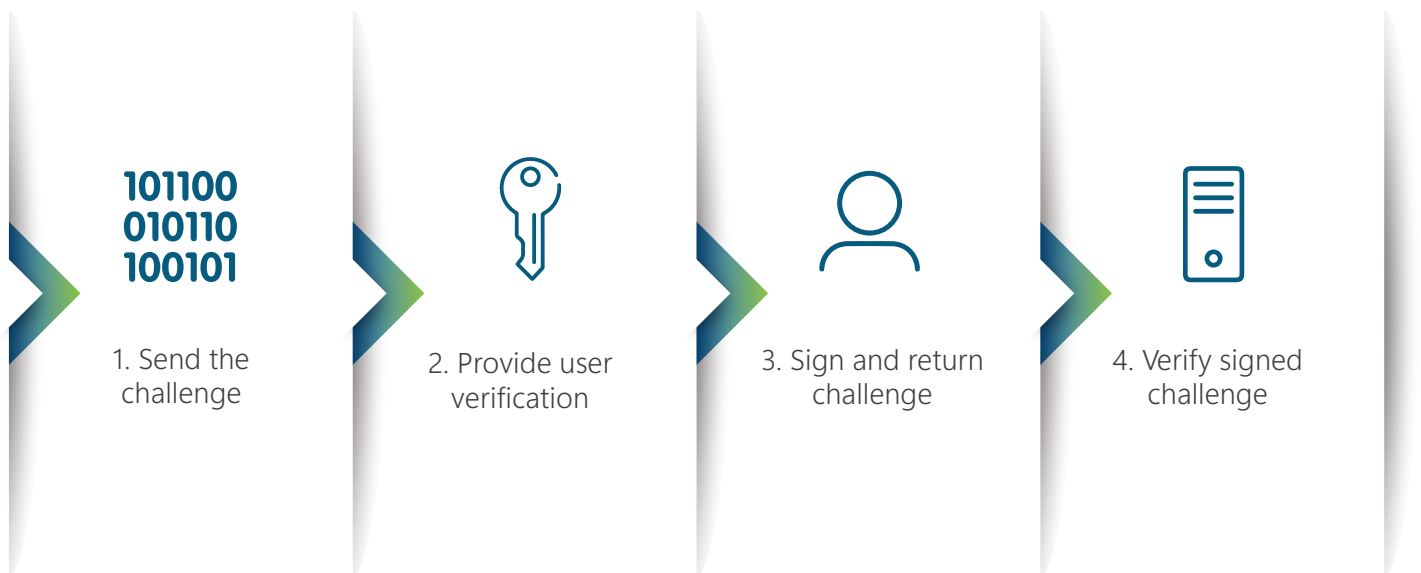
## The solution: Passwordless

Passwordless is a multi-factor authentication method in which a user can log in to a computer system, service, or application without entering (and having to remember) a password or any other knowledge-based secret.

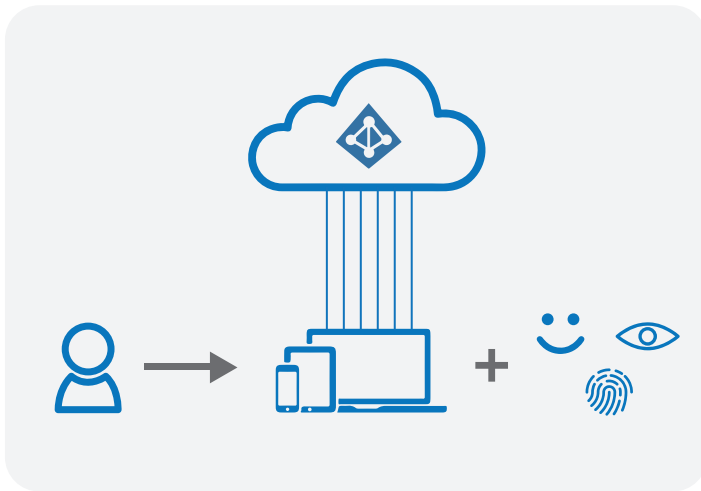


## How passwordless authentication works

Each technology uses the same established cryptographic authentication pattern, with credentials based on the certificate or asymmetrical key pair



## Passwordless secure authentication components



- Something you have [Windows 10 Device, Phone, Security Key] + Something you are [Biometric] or know [PIN]
- Authentication based on Public/Private Keys pair
- Private keys are securely stored on the Device [PCs, Mobile Application, FIDO2 Key]
- Private keys are tied to a device and are never shared
- Requires the use of local gesture [PIN, Biometrics] to unlock the private key

## Advanced, modern, and secure methods

### WINDOWS HELLO FOR BUSINESS

#### User friendly and privacy protecting

- Passwordless: biometrics or a PIN
- SSO with Windows apps
- Biometrics never leave the device
- Private key is never shared

#### Enterprise-grade

- Strong two-factor authentication
- Asymmetric keys pair auth model
- Can be deployed in cloud, hybrid, or on-premises environments
- Key or certificate-based options





## FIDO2 SECURE KEYS



### Enterprise grade

- Authentication based on hardware [Portable]
- Security devices that are Microsoft compatible
- Sign in using FIDO2 [biometrics, PIN, and NFC]
- Recommended for shared PCs scenarios or when a mobile device is not a viable option [Examples: help desk personnel, public kiosk, hospital team, bank teller]
- Recommended for Privileged and Critical Identities
  - Azure AD Global Administrator, Security Administrators, CEO, CISO, others
- Cross platform if using as Smart Card [on-premises services required]

## MICROSOFT AUTHENTICATOR



### Overview

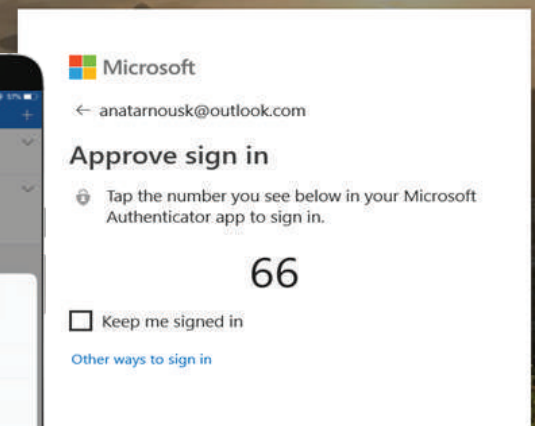
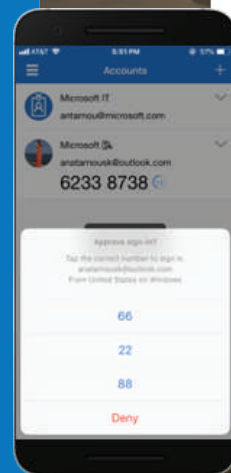
- Authentication based on software
- Standards-based MFA
- Supports TOTP, Push Approvals, Biometrics + Number Match

### Windows 10

- Passwordless authentication, such as device registration in OOBE, Windows Hello provisioning

### Mobile

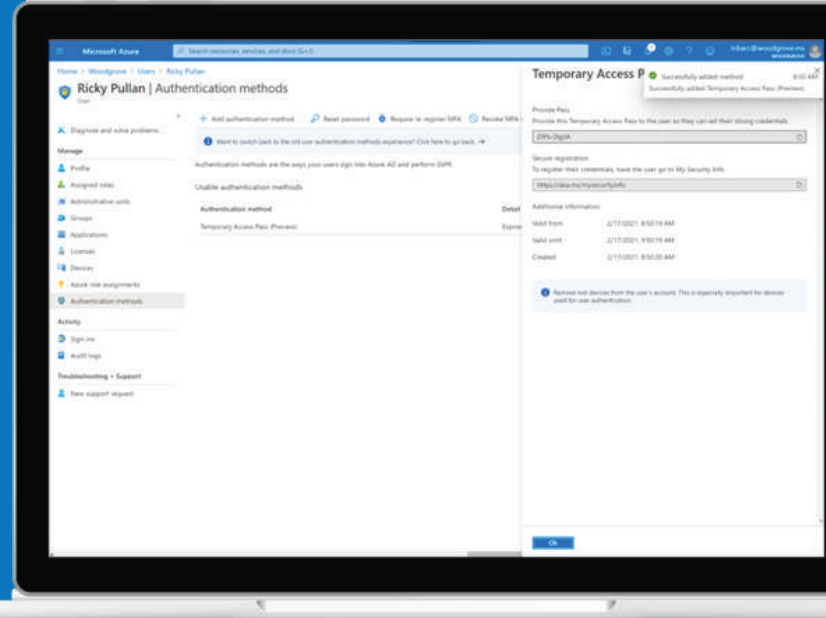
- SSO to native mobile apps



## TEMPORARY ACCESS PASS | TAP

### Enterprise-grade

- Time-limited code for passwordless credentials set up and account recovery
- Enables end-to-end passwordless user journeys and remote onboarding/recovery scenarios
- User can receive a temporary passcode to login and register their account, and then register a passwordless credential



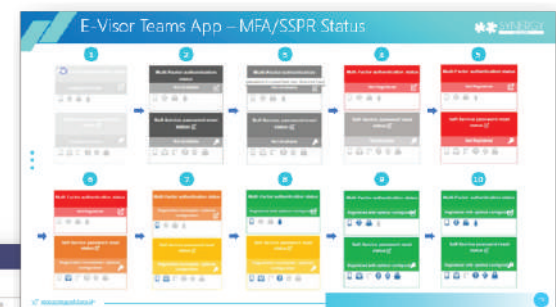
## Extended identity capabilities with E-Visor Teams App

E-Visor Teams App is a reporting and analytics app that helps end users boost their security and productivity, directly from within Microsoft Teams. E-Visor Teams App complements the passwordless strategy by presenting to end users, managers, and IT department the MFA configuration status, sign-in information filtered by risk events, failed logins, location, devices, identity and much more, as well as self-protect actions.

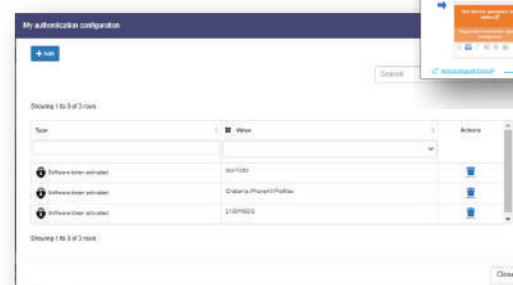
## Simplified end user Multi-factor Authentication and Self-Service Password Request (SSPR) management

- Reduce complexity to access Microsoft 365 information spread along with multiple sites, reducing costs.
- Reduce user education as Microsoft portal adds/removes information/capabilities and changes URLs.
- Simplified user experience providing multiple technologies/workloads view with the same look and feel.

### Optimized Configuration

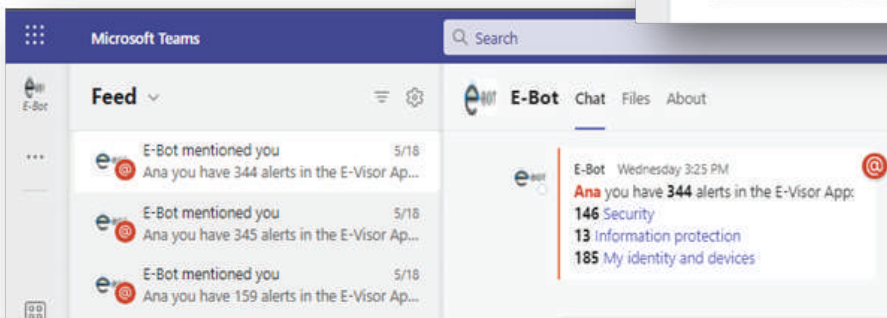
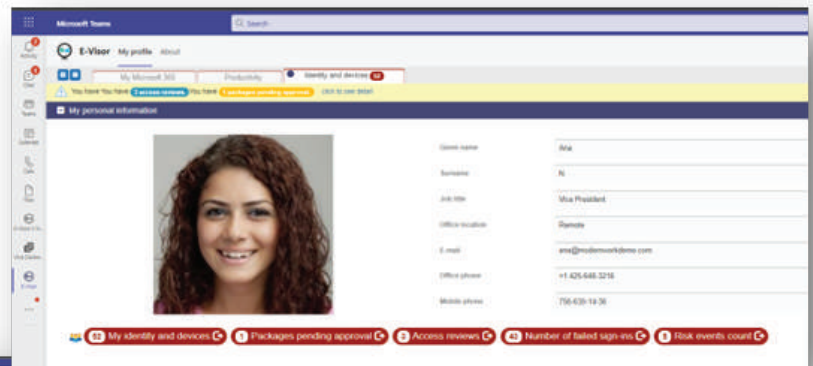


### MFA/SSPR self – service



## Alerts and notifications

- Reduce time and create awareness
- Mitigate phishing attacks
- Reduce troubleshooting and support time
- Self-service
- Reduce organization cost
- Empower end users to strengthen their security posture



## Other features



### Sign-in insights

- Suspicious actions
- Conditional Access details



### Optimized identity and device view

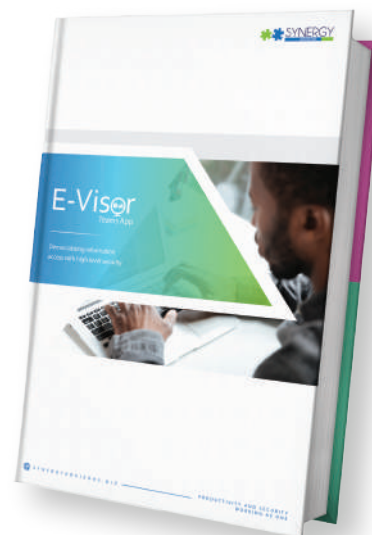
- Device focused identity and access status



### Simplified access/approval to apps

- My apps Packages
- My request status
- Approvals
- Validate access

## Learn more about E-Visor Teams App.

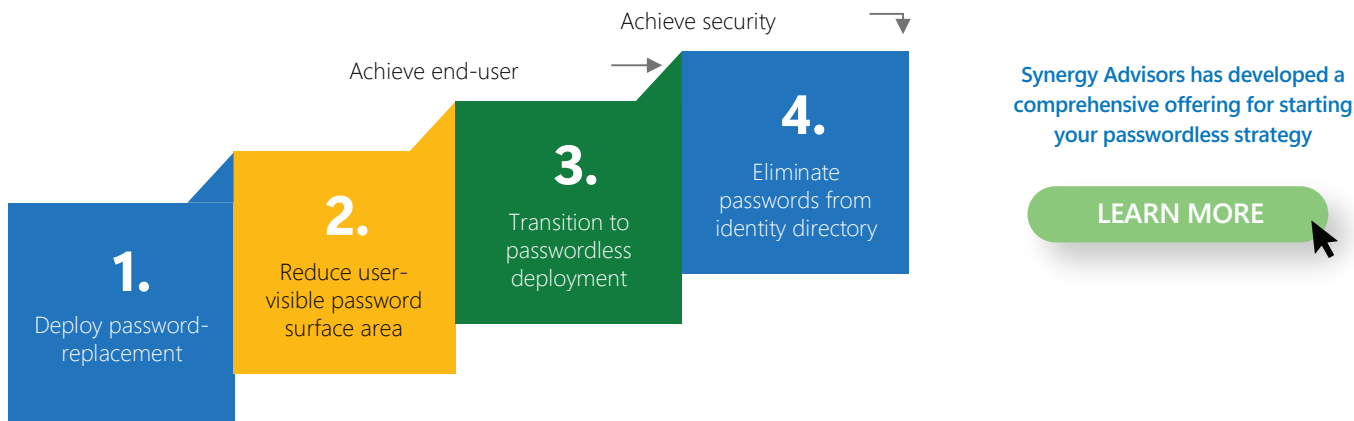


[DOWNLOAD THE E-BOOK](#)



## The journey towards effective passwordless implementation

Synergy Advisors is ready to support your organization in its journey to effectively establish a passwordless strategy, and make a smooth transition, while boosting productivity and cybersecurity in your organization.



## About us

Synergy Advisors is a premier Microsoft Certified Partner that specializes in Microsoft 365, Identity, Azure B2C and B2B Collaboration, Security, Management, and Cloud technologies. We help you digitally transform and implement a more secure collaborative infrastructure, reduce your IT costs, and meet your regulatory requirements through our comprehensive portfolio and experience in consulting and managed services.



### Secure E-mail

- Users
- Apps
- Services
- Hygiene
- Threats
- Data Leak Mitigation



### Secure Collaboration

- Users (internal / external)
- Apps
- Services
- Hygiene
- Threats
- Data Leak Mitigation



### Device Protection

- Applications security
- O.S. security
- Security base line
- Threats
- Data Leak Mitigation



### Information Protection

- Data in use
- Data at rest
- Data in transit
- Application integration
- Data Leak Mitigation
- Structured and unstructured data protection



### Platform Protection

- Monitoring / Services analysis/ Alerts and notifications
- Security base line

Contact us and get a free demo of passwordless solutions, [HERE](#)

E-mail us and get a free consulting session:  
[ww-marketing@synergyadvisors.biz](mailto:ww-marketing@synergyadvisors.biz)

