Tech Brief

Passwordless Authentication for Windows Login

The Challenge

Many organizations find password-only protection for Microsoft Windows login insufficient. Persistent attacks drive the need for increased endpoint defenses, as endpoints can serve as entry points for ransomware attacks.

Endpoint Security Needs: MFA for admin and system accounts is now a standard cybersecurity insurance requirement.
Application Scope: This requirement applies to local Windows logins, Windows remote desktop (RDP) and virtual desktop (VDI) logins.

IAM Limitations: Many IAM solutions provide SSO for remote apps but lack integrated endpoint protection, leading to siloed authentication across different operating systems (Windows, Mac, Linux).

Ideal Solution: Organizations need an integrated solution that offers passwordless MFA from OS login to remote applications, including RDP, which

- Accommodates specific organizational needs.
- Ensures a consistent user experience without multiple authentication prompts.
- Supports diverse methods, including Push, OTP, SMS, PIV cards, and phones, with a focus on phishing resistance.

Finding a flexible, comprehensive solution to meet these needs and provide a seamless user experience can be challenging.

The Solution

WinMagic has the broadest set of choices for Windows authentication to match your organization's passwordless needs:

- Phone Authenticator via Bluetooth Low Energy (BLE)
- Trusted Platform Module/ Personal Identification Number (TPM/PIN)
- Phone Authenticator via Network /IdP
- Smartcard/Personal Identity Verification (PIV) Cards
- USB Token (e.g. Yubikey)

With MagicEndpoint, the user can authenticate with MFA for local Windows login, and then MagicEndpoint takes care of SSO into the VPN and RDP with no user action required.

Once the user is authenticated to the endpoint, MagicEndpoint can provide seamless "no user action" authentication to remote services.

Check out the simplicity of MagicEndpoint Windows Authentication.

RDP and VDI Log In

Securing RDP for remote work involves addressing its inherent insecurity over the public internet. Key points include

Insecurity of RDP:
- Requires additional security measures.
- Many servers with public RDP access lack MFA.
- Vulnerable to phishing, weak passwords, and brute force attacks.

Mitigation Strategies:
- Avoid exposing RDP to the internet.
- Use VPN with MFA for remote users.

Zero Trust Perspective:
- Internal network access shouldn't be implicitly trusted more than internet access.
- "No network is implicitly considered trusted" (source: White House).
- VPN with MFA alone doesn't meet cybersecurity insurance requirements for MFA on admin-privileged endpoints.

VDI faces similar security challenges and requires comparable measures to secure access.

Tech Brief

Passwordless Authentication for Windows Login

Passwordless Phone Use Cases:

Passwordless phone authenticator via BLE
For organizations issuing phones to employees and seeking phishing-resistant authentication, a BLE mobile phone authenticator is an ideal choice. Unlike out-of-band (OOB) authenticators, the BLE authenticator communicates locally with the endpoint, requiring proximity to work and providing a strong phishing-resistant link. MagicEndpoint's phone-based authenticator uses Bluetooth for high-assurance, cryptographically enforced, MFA passwordless login, allowing users to log in without entering any information on the endpoint.

Passwordless phone authenticator with network/IdP
For organizations that issue phones to employees and prefer this device for authentication but can't use Bluetooth, MagicEndpoint supports mobile push at Windows Login for a consistent user experience.

TPM/PIN Use Case:

The TPM hardware on the device is ideal for organizations struggling to manage external tokens. Users log into Windows with a local TPM PIN, ensuring Windows Login is secured by TPM and can be configured for SSO. The local TPM PIN is safe from remote attacks and benefits from hardware-based anti-hammering protection.

Smart Cards, USB Tokens and PIV Card Use Case:

For organizations mandated to use Smart Cards, USB Tokens and PIV Cards for access control, users access Windows using their hardware tokens. Windows login is protected by the hardware token and can be configured for SSO for the best user experience.

MFA for IAM Solutions Use Case:

MagicEndpoint offers IAM solutions integration for Windows login such as Okta.

Click here to watch MagicEndpoint PBA with Okta.

CHECK OUT THE SIMPLICITY OF MAGICENDPOINT PBA WITH PHONE BLE

MagicEndpoint from WinMagic is the passwordless authentication solution that protects access by focusing on the endpoint, for the user. It requires no user action, and no third-party devices or keys, so it's seamless, secure and virtually invisible.

Authenticate. Encrypt. Achieve.

US & Canada +1 888 879 5879 | EMEA +49 69 175 370 530 | Japan +03 5403 6950
For more information, click here or contact WinMagic