MagicEndpoint™ by WinMagic

Always On Verification

NO USER ACTION **NO PASSWORDS** **ZERO TRUST**

The world's only authentication where your users do nothing and your security is always on. One architecture for humans, machines, and AI agents, with no way in for attackers.

The Challenge

Traditional MFA relies on point-in-time credential checks that attackers routinely bypass. Passwords are phished, push notifications are fatigue-bombed, and session tokens are hijacked minutes after login.

The result: organizations invest heavily in authentication yet remain vulnerable to the threats MFA was supposed to prevent.

The Solution

MagicEndpoint eliminates these risks by replacing point-in-time checks with continuous verification.
A TPM-bound Live Key binds user identity to the device.
A Trusted Channel monitors signals continuously.
Access is only granted when strict, real-time policies are met – all without interrupting the user. After the user provides strong MFA at OS login, the endpoint takes over authentication tasks.
No passwords, no OTPs, no push approvals for the user.
The endpoint does all the work.

How It Works

1. **Authenticate at the endpoint**

   User logs in via strong MFA (phone biometrics, YubiKey, PIV, etc) at pre-boot logon and/or Windows login.

2. **Live Key binds identity to device**

   A TPM-bound Live Key is generated at OS login. This key never leaves the endpoint, creating an unbreakable user-on-device identity.

3. **Trusted Channel established**

   A secure connection is established between the endpoint and MagicEndpoint IdP for continuous verification of user + device + conditions.

4. **No User Action access to all apps**

   User navigates to any configured application. The IdP verifies the Trusted Channel and policies. Login is automatic – the endpoint does all the work.

✓ **Policies enforced continuously**

Shortest session tokens, silently auto-renewed. Disk encryption and screen lock checked before, during, and after every authentication.

Capability	Password-Based Solutions
Supported Platforms	Windows & Linux (Pre-Boot) ; Windows (OS Login) ; Windows & macOS (Online)
Federated Web Apps	SAML 2.0, OIDC, WS-FED – any standard-compliant web app
Network & Remote	RADIUS, LDAP, SSH, RDP – existing infrastructure
Legacy Apps	Built-in Password Manager auto-injects credentials
Deployment	SaaS, hybrid, or fully on-premises
Management	Centrally managed through MagicEndpoint console

Ready to eliminate MFA friction and minimize session hijacking?

Contact us to learn how MagicEndpoint delivers continuous verification and passwordless access for every endpoint in your organization.

MagicEndpoint™ by WinMagic