WinMagic Introduces The Future of Cybersecurity – The Secure Internet

MISSISSAUGA, ONTARIO, CANADA, June 26, 2025 /EINPresswire.com/ -- WinMagic Inc., a global innovation leader in authentication and endpoint security solutions, today introduced

WINMAGIC ®
Authenticate. Encrypt. Achieve.

The [Secure Internet](#), a groundbreaking innovation which redefines how users will access online services—securely and seamlessly—without requiring any user interaction.

At the core of The Secure Internet is a simple yet revolutionary advancement in secure online communication. This eliminates the theoretical - and practical - vulnerabilities of current user authentication flows, including TLS, FIDO/Passkeys, along with federated authentication mechanisms and handling of session tokens. In other words, we create the dynamic machine "user on device, in real-time" and use machine-to-machine (M2M) communication. With mutual TLS (mTLS), M2M communication is significantly more secure due to its exclusive reliance on strong cryptography and the complete elimination of user interaction.

In 2023, WinMagic discovered a fundamental flaw prevalent across most modern authentication frameworks: while authentication may verify the client correctly, the subsequent session data is often encrypted with keys that are not created and protected by that authentication.

"It's like trusting a combination lock without knowing who has the code" said Thi Nguyen-Huu, Founder and CEO of WinMagic. "We've built an Internet where authentication doesn't automatically ensure confidentiality. That changes today with The Secure Internet."

Introducing the Secure Internet
The Secure Internet establishes a safe communication channel where service providers can be confident that the authorized user is operating from an authorized endpoint in real time.

Key Features
• No User Interaction Required
Users can seamlessly access websites and online accounts without typing passwords, approving MFA prompts or engaging with authentication flows. For the user, endpoint access grants access to everything else.
• Endpoint as Authenticator

The user's device becomes the strongest and most reliable authenticator—eliminating the need for phones, tokens or one-time passcodes.

• Phishing-Resistant and AI-Secure

This architecture is inherently resistant to phishing and AI-driven attacks, as the user is completely removed from the authentication process. With no shared secrets or manual steps, there's nothing for attackers to intercept or manipulate.

• Real-Time, Continuous Verification for Enterprises

The endpoint maintains a persistent, trusted connection with the Identity Provider (IdP), updating in signals in real time about the user's and device security posture. The IdP has full visibility - before, during, after, and even unrelated to any online sessions - delivering unmatched accuracy and security.

A New Identity Paradigm: "User on Device in Real Time"

Beyond using the endpoint to establish a trusted channel to always verify the user and endpoint, our most transformative innovation is the creation of an identity: the user on the device, in real time, backed by uniquely verifiable cryptographic keys. This enables secure machine-to-machine communication on behalf of users. Understandably, this applies well for non-human accounts like "application on device", "service account on device" and for many environments beyond web applications.

WinMagic implemented this identity in its standalone, free SSH solution. We will launch the enterprise version soon and offer it for free for a limited time. This version allows you to configure which (thousands of) users can use which (thousands of) devices to access which (thousands of) servers via SSH, all using unshared cryptographic keys.

Simplifying and Strengthening the Digital Foundation

The concept of The Secure Internet uniquely fulfills Zero Trust's core principle: continuous verification of both user and device for every application and transaction. While the industry has made significant strides in online authentication—through efforts like Passkeys and IAM—there remains a critical gap in securing what comes next: the session and the transactions themselves.

The Secure Internet addresses this gap and has far-reaching implications for:

• TLS and FIDO/Passkeys
• Session token and cookie vulnerabilities
• PKI and certificate lifecycle simplification
• Federated Authentication protocols and Continuous Access Evaluation Protocol (CAEP)
• NIST's Federation Assurance Level 3 (FAL3)
• Token binding (e.g., RFC 8471 and beyond)

In essence, The Secure Internet can deliver the highest level of security using just mTLS—with no user interaction. This is not only simpler, but more secure than anything currently available.

Join the Movement
WinMagic invites technology providers, government institutions and industry leaders to collaborate in advancing The Secure Internet initiative.

"We've built a new foundation for how trust is established online—one that's simpler, stronger, and inherently secure by design," said Thi Nguyen-Huu, Founder and CEO. "Now, we call on the broader community—including IETF, FIDO, OpenID, NIST, media, and industry analysts—to help us identify potential weaknesses, integrate complementary ideas and systems, and scale this vision together."

Learn More
To see The Secure Internet in action and understand how your organization can benefit, visit: www.winmagic.com/secureinternet or contact:
marketing.team@winmagic.com
_____

About WinMagic
With over 25 years of continuous innovation, WinMagic's comprehensive full disk encryption controls user identities via MFA for endpoint access and continuously protects and monitors both endpoints and users from the moment the endpoint is powered on. For online access, embracing an identity-first approach and adhering to Zero Trust principles where the network lacks inherent trust, MagicEndpoint introduces uniquely verifiable identities, "user on device," utilizing TPM keys. MagicEndpoint IdP then provides best-in-class authentication services for all identities accessing online resources.

Thanks to the secure channel continuously monitoring the device and user, MagicEndpoint is more resilient to attacks than current approaches. Perhaps more importantly for user adoption, this solution eliminates any burden on the user beyond endpoint login.

WinMagic Media Relations: marketing.team@winmagic.com

Join us on LinkedIn: https://www.linkedin.com/company/winmagic
Subscribe to our YouTube Channel:
https://www.youtube.com/channel/UCT8BLsXOjhpwwZLyyNNrCkw
Press Release: www.winmagic.com/en/secure_internet
www.winmagic.com

Joseph Belsanti
WinMagic Corp
email us here

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.