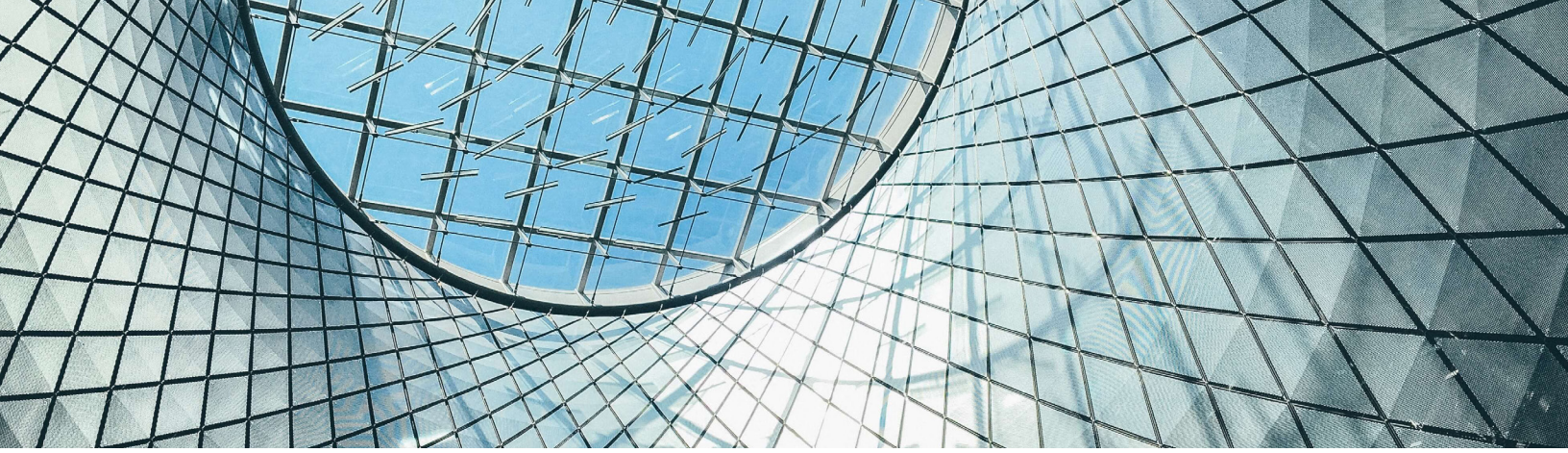


Market Insight Report Reprint

# WinMagic branches out from full-disk-encryption roots with passwordless authentication offering

May 17 2022

by Garrett Bekker

Passwords are hard to remember, annoying to type in and generally easy to defeat. WinMagic has developed its own “passwordless” offering called MagicEndpoint, which leverages the company’s DNA in full-disk encryption. It aims to deliver what it refers to as “zero factor” authentication that completely eliminates passwords.

451 Research

S&P Global
Market Intelligence

## Introduction

One of the primary ways to provide remote access securely is authentication, but as we have noted in past reports, authentication can be challenging, whether standard passwords or stronger forms of authentication such as multifactor authentication (MFA). Passwords are hard to remember, annoying to type in and generally easy to defeat.

Not surprisingly, "passwordless" authentication methods have gotten a lot of attention recently, in part thanks to the growing popularity of the Fast Identity Online (FIDO) alliance, and new standards such as FIDO2. However, there are various ways to achieve passwordless authentication, and not all are equal. WinMagic has developed its own passwordless offering, MagicEndpoint, that leverages its DNA in full-disk encryption and authentication on the endpoint, to deliver what it refers to as "zero factor" authentication that completely eliminates passwords.

## THE TAKE

Passwordless authentication based on public key cryptography is a logical extension for an encryption and authentication vendor. The move into passwordless should also provide an opportunity to tap into new growth markets compared with its core laptop and file encryption markets, which are fairly mature. However, encryption likely still accounts for the vast majority of WinMagic's revenue. Thus, its primary challenge will be to overcome market perception of the company as primarily a full-disk encryption (FDE) vendor, in order to compete with an increasingly crowded field of both legacy and emerging passwordless authentication contenders.

## Context

Toronto-based WinMagic was founded by CEO Thi Nguyen-Huu in 1997. The company initially specialized in FDE for laptops before branching out into passwordless authentication. WinMagic currently has about 80 full-time employees and is privately held and financed, with no recent fundraising activities. Roughly one-third of its customers are large enterprises (defined as over 1,000 endpoints), another third are midsized (100-1,000) and the rest are SMBs (<100 endpoints).

It is logical for an endpoint-focused encryption vendor to leverage that expertise with an endpoint-focused authentication offering. One of MagicEndpoint's main value propositions is the ability to offer no user interaction (for Windows devices), which in turn allows for continuous verification of the endpoint client, and is a step toward delivering a zero-trust architecture – along with the ability to establish device trust by combining user authentication with device health checks.

The endpoint (typically a Windows laptop or PC, but also a mobile phone app) essentially functions as an authentication proxy that connects to back-end resources on behalf of the user. While such an architecture can provide both a high degree of security and a positive user experience, it may mostly appeal to existing customers that have already installed WinMagic software on their employees' endpoints – although WinMagic claims to be targeting non-FDE customers with MagicEndpoint.

## Products

MagicEndpoint was conceived three years ago, and was launched in March after two years of development. The fundamental idea behind the technology is that users only have to authenticate to the endpoint device (by using a local gesture like TouchID on an iPhone or iPad, a biometric on the phone, Windows Hello, a USB security key, or a local PIN code) on the local device to verify they are in possession of the device.

The endpoint device, in turn, essentially serves as a middleman or proxy to authenticate the user to whatever resources they are trying to access. Since MagicEndpoint remains authenticated on behalf of the user, they do not need to reauthenticate to other websites, devices or data accessed through the PC endpoint, acting effectively like single sign-on (SSO). MagicEndpoint can also provide additional intervention if needed; if, for example, the endpoint notes suspicious behavior that indicates the user is not present on the endpoint.

Architecturally, MagicEndpoint is based on public key cryptography-based authentication rather than 'shared secrets' like passwords or OTP tokens. It leverages the trusted performance module (TPM) section on the processor of most PCs and mobile devices to store digital certificates and private encryption keys. On the client side, users need to install the MagicEndpoint agent, which also creates a private key for each user, and a corresponding public key for each service or application the user will need to authenticate to.

The private key sits encrypted in the TPM on the endpoint device, and since the private keys (each TPM can store keys for multiple users on each endpoint) never leave the TPM, the service is resistant to phishing attempts. Organizations also have the option to use a variety of authenticators to log in to the endpoint, such as USB tokens or smart cards. Users that don't have an endpoint with MagicEndpoint installed have the option of installing the WinMagic mobile app that uses the secure element or Trusted Execution Environment on most modern smartphones to store the private keys, with local gestures used to unlock the device.

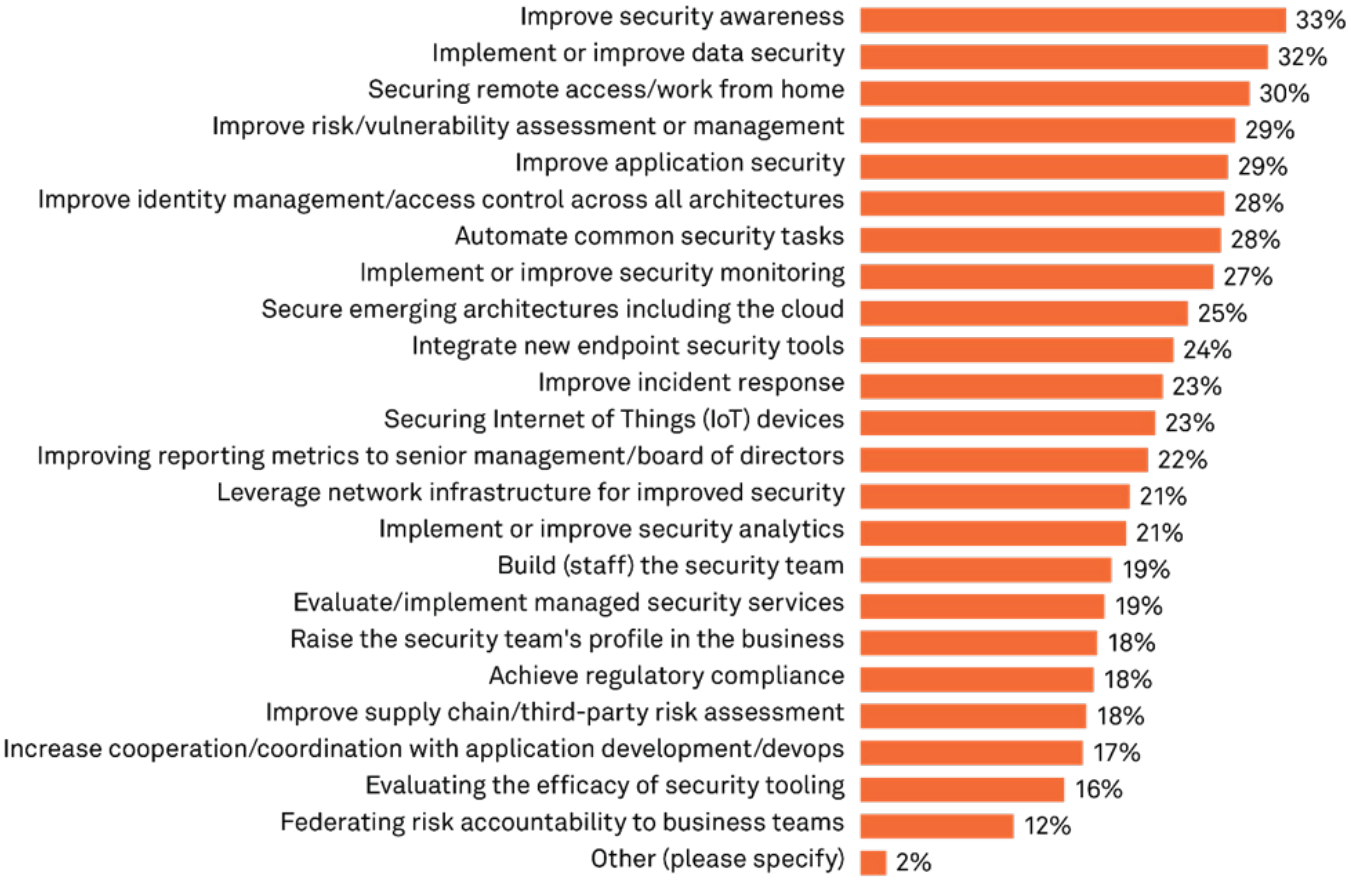
Both Android and Windows are FIDO certified platforms – so any Android 7 or later handset, or Windows 10 or later PC with Hello, can use the native biometrics on the device, or local PIN on the device without a password, although MagicEndpoint's "no user interaction" capability is available on Windows only for the time being.

On the server side, customers can elect to install WinMagic's own identity provider (IdP), and can also connect to their existing IdPs such as Active Directory or Okta. Smaller businesses or consumers that don't have an IdP have the option to use the FIDO2 protocols, CTAP and WebAuthN for authentication. The MagicEndpoint agent also performs encryption, offering a single console for managing both encryption and authentication, with an option to provide SSO functionality as well.

## Strategy

MagicEndpoint is currently sold as a separate, additional offering that is independent of WinMagic's data-at-rest encryption offerings. Pricing is currently $3 per user per month, while WinMagic FDE is typically priced per device. At the moment, MagicEndpoint is only available on Windows platforms, although there is an optional mobile phone-based authenticator that supports push notifications for non-Windows systems.

**Securing Remote Access Is a Top Information Security Strategic Objective**




Q. What are your top strategic security objectives for 2021? Please select all that apply.

Base: All respondents (n = 354)

Source: 451 Research 's Voice of the Enterprise: Information Security, Budgets & Outlook 2021

## Competition

The authentication market is one of the most crowded sectors of the security market, and leading authentication-focused vendors include Cisco Systems Inc. (Duo Security), RSA Security, Entrust, Thales (Gemalto) and OneSpan Inc. Many IDaaS vendors such as Okta Inc., One Identity (OneLogin), Ping Identity, Microsoft Corp. and SecureAuth also have their own MFA offerings. Newer vendors addressing behavioral analytics include BioCatch, BehavioSec and Plurilock.

In terms of passwordless authentication specifically, MagicEndpoint will compete directly with other passwordless authentication providers like 1Kosmos, Axiad, Cisco, HYPR, Microsoft, Beyond Identity, Secret Double Octopus, Nok Nok Labs, StrongKey, Trusona, TruU and Yubico.

## SWOT Analysis

### STRENGTHS

Its true passwordless offering authenticates both the user and the device, which is important for remote access scenarios. "No user action" helps deliver both strong security and a positive user experience. It works with legacy applications that use RADIUS and LDAP, as well as SAML or OIDC.

### WEAKNESSES

Encryption still accounts for the vast majority of revenue, and the primary challenge will be to overcome market perception of WinMagic as primarily an FDE vendor.

### OPPORTUNITIES

Securing remote access has been identified by 451 Research as a top strategic objective, which could help WinMagic tap into its existing laptop and file encryption installed base.

### THREATS

The biggest challenge will be to stand out in an increasingly crowded field of both legacy IAM platform providers, and emerging contenders with new takes on passwordless technologies.

**CONTACTS**

**The Americas**
+1 877 863 1306
market.intelligence@spglobal.com

**Europe, Middle East & Africa**
+44 20 7176 1234
market.intelligence@spglobal.com

**Asia-Pacific**
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence