WINMAGIC®

MagicEndpoint™

+ Okta

Unparalleled Authentication Solutions For Today's Standards

Overview

With the move to work from anywhere, cloud-based applications, and an increasingly hostile threat environment, organizations are reexamining their IT security strategies because the traditional perimeter security model is becoming less and less effective.

Many, including the US government, are transitioning to a "zero trust" approach to security to provide a defensible architecture for this new environment. The Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access.

This zero-trust – always verify strategy - requires Multi-Factor-Authentication, but not just any MFA:

"Agencies must require their users to use a phishing-resistant method to access agency-hosted accounts. For routine self-service access by agency staff, contractors, and partners, agency systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications."

https://zerotrust.cyber.gov/federal-zero-trust-strategy/

Next Generation Passwordless Authentication

Today, many organizations use phone-based MFA methods for their multi-factor authentication, but these authentication methods, including SMS, OTP and Push Notifications, fail to resist phishing. This phasing out of traditional MFA factors has raised the bar on security, making current phone-based passwordless authenticator Apps that use OTP or Push no longer acceptable, even ones that utilize public key cryptography.

What does this mean? Phone-based authenticator apps like MS Authenticator, when configured to use OTP or Push (i.e. with just an "Approve" or "Deny" button) are no longer good enough.

And considering the requirement for "continual verification," even some phishing resistant methods today will be too much of a burden for users.

Together, MagicEndpoint & Okta Help Organizations Solve These Problems

WinMagic's MagicEndpoint brings a new way of thinking to endpoint authentication. With MagicEndpoint, the device itself becomes the authenticator. MagicEndpoint utilizes public key cryptography and the Trusted Platform Module (TPM) that is found in all business class machines to perform all the remote authentications while supporting local PIN, biometrics, external tokens and mobile phones (as a token) for authentication to the endpoint. This new way of thinking distinguishes remote access from endpoint access so that there is MFA to access the endpoint and the endpoint verifies the user, continuously if needed; even the user's intent supporting the Zero Trust "always verify" principle.

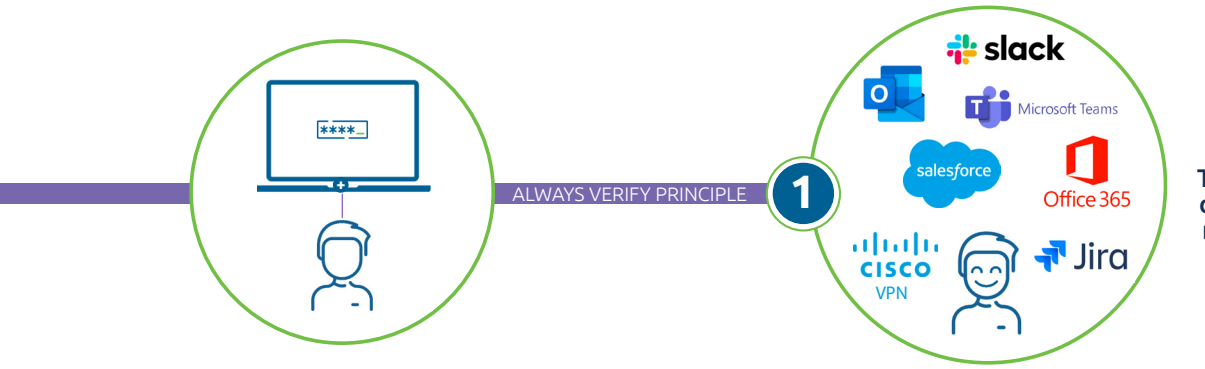
MagicEndpoint not only delivers the phishing resistance requirement that is phasing out the most popular OOB solution today, but it offers the best user experience any application can wish for – no user action required. And with that, it in turn helps the future aspired Zero-Trust principle of continual verification without user's burden. It's our new way of thinking! It's Innovation!

Implement Secure Device Trust Strategies

WinMagic's 20-plus years of experience on the endpoint with authentication and encryption provides a new security posture for your organization by supporting data signals to your IAM conditional access. Whether your user devices have been put into a compromising state, e.g. Secure Boot disabled, or encryption has been removed from files, MagicEndpoint and Okta can ensure the right measures are put into place to protect your users and organization from attacks.

How MagicEndpoint Works

When users request access to their applications, the application delegates to Okta and Okta subsequently delegates authentication responsibilities to MagicEndpoint:



The combined identity of device+user performs all remote authentications.

1 Step process:

The user only needs to authenticate to their device perhaps with a local gesture or biometrics. Once authenticated successfully, the user is no longer needed to perform any remote authentication to access their applications.

The user is logged into the system and has access to all remote authentications. With no additional burden on the user.

That's all — it's secure and simplified, all at once.

WINMAGIC®

US & Canada +1 888 879 5879 | EMEA +49 69 175 370 530 | Japan +03 5403 6950

For more information, click here or contact WinMagic