Tech Brief

Passwordless Pre-Boot Authentication

Challenge/ Situation

Many organizations are concluding that protecting their MS Windows logon or Pre-Boot logon, if employing FDE (Full Disk Encryption), with just a password is no longer sufficient. Persistent attacks are driving organizations to increase their defenses on the endpoint which can be used as an entry point for ransomware attacks, amongst other things. In fact, protecting the endpoint login with MFA (Multi-Factor Authentication) for accounts that have administrator or system privileges is fast becoming a standard requirement in order to obtain or maintain cyber security insurance.

Some organizations look to their Identity & Access Management (IAM) providers for an MFA or Pre-boot authentication solution. Although these solutions provide a convenient single sign-on (SSO) portal for remote applications, they still need an integrated solution to protect the endpoint. Adding another authentication solution to the mix to address endpoint authentication risks the creation of authentication silos, especially when multiple operating systems (i.e., Windows, Mac, and Linux) must be considered.

Ideally, organizations need one integrated solution that provides Passwordless MFA from Pre-boot to OS login to the user's remote applications. The solution needs to be flexible enough to accommodate the organization's particular needs and provide a consistent user experience regardless of the method used for authentication. Not one size fits all for users. Many solutions require phones with Push, OTP, or SMS (which most will be depreciated). Some users might not be able to use phones at all (or have other hardware limitations), so the solution cannot easily be deployed within their organization. For example, governments and other agencies may require PIV cards, or others have the mandate to eliminate passwords. Some avoid phones, while others embrace them as the authentication device but require phishing resistance as part of their zero-trust strategy. It is a big challenge to find one solution with the flexibility and options to match the organization's needs and provide users with a consistent user experience for all authentications.

Solution

WinMagic has the broadest set of choices for your Pre-Boot authentication to match your organization's needs for moving to Passwordless:

- Passwordless Phone Authenticator via Bluetooth Low Energy (BLE)
- Passwordless Phone Authentication via Network/IdP
- Trusted Platform Module/ Personal Identification Number (TPM/PIN)
- Smartcard/Personal Identity Verification Cards (PIV)
- Yubikey

These same methods can also be employed for Windows login, providing a consistent user experience. Better yet, once the user is authenticated to the endpoint, MagicEndpoint can seamlessly provide "no user action" authentication to remote services, either directly or by acting as a delegated authentication service to your IAM.

Check out the simplicity of MagicEndpoint Pre-Boot Authentication.

Tech Brief

Passwordless Pre-Boot Authentication

MagicEndpoint allows organizations to enable pre-boot authentication and Windows logon by providing the tools to easily deploy and use authentication that best suits their users – including recovery and backup options for each.

Solutions summary:

Passwordless Phone Use Cases:

Bluetooth Low Energy (BLE) connection
For organizations that issue phones to employees and prefer this device for authentication, but are phasing out SMS, OTP, and Mobile Push because they are not phishing resistant, a BLE (Bluetooth Low Energy) connected mobile phone authenticator is a good choice. Unlike Out of Band (OOB) mobile authenticators, the BLE mobile authenticator is locally connected to the endpoint device and requires proximity to work. This proximity provides a strong association between the authenticator and endpoint to resist phishing. Users log into pre-boot using our Passwordless authentication option available with the phone app. MagicEndpoint phone-based authenticator connects to the laptop via Bluetooth to provide the high-assurance, cryptographically enforced, MFA Passwordless login to the endpoint. Users don't have to enter anything on the endpoint for a truly passwordless experience. And the BLE-connected phone app also works the same way for Windows login.

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 PBA and at Windows Login for a consistent user experience.

TPM/PIN Use Case:

The TPM hardware on the device itself is a good option for organizations that find external tokens and devices hard to manage. Users log into pre-boot using the TPM with a local PIN, and Windows Login is protected by TPM and can be configured for SSO. The TPM PIN is local and cannot be attacked remotely, and TPM also provides hardware-based anti-hammering protection.

PIV Card Use Case:

For organizations mandated to use PIV Cards for access control, users access pre-boot using their PIV card. Windows Login is protected by the PIV card and can be configured for SSO for the best user experience.

MFA for IAM Solutions Use Case:

MagicEndpoint offers IAM solutions, like Okta, integration at SecureDoc's Pre-Boot.
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