Tech Brief

Windows ログオンのパスワードレス認証

課題 / 状況

多くの組織は、 MS Windows ログオンをパスワードのみで保護することは、もはやセキュリティ対策として不十分だと結論付けています。 特に、 エンドポイントはランサムウェア攻撃のエントリポイントとして利用されてしまう可能性があるため、 サイバー攻撃が絶えない昨今、 エンドポイントのセキュリティをさらに強化する必要があります。 管理者権限やシステム権限を持つアカウントのエンドポイントへのログオンを、 多要素認証を利用して不正ログオンを防止することは、 急速に、 サイバーセキュリティ保険 （英語） を取得・維持するための標準的な要件となっています。

これは、 Windows のローカルログオンだけでなく、 Windows リモートデスクトップや仮想デスクトップのログインにも当てはまります。 これらの組織はさらに、 多要素認証ソリューションをサポートする IAM （ID およびアクセス管理） プロバイダを求めています。 IAM プロバイダは、 リモートデスクトップなどのリモートアプリケーション向けの SSO （シングルサインオン） ポータルを提供していますが、 エンドポイントが SSO ポータルにアクセスする際の認証リスクに対応するソリューションを同時に求めています。 特に、 複数のオペレーティングシステム （Windows、 Mac、 Linux など） を考慮する必要がある場合など、 それぞれの OS に別の認証ソリューションを導入すると、組織内で認証ソリューションの分断 （サイロ化） を生みます。

理想的には、 OS ログオン、 そしてリモートアプリケーション （リモートデスクトップなど） へのログインまでをカバーする多要素・パスワードレス認証をサポートする単一の統合ソリューションが求められています。 また、 組織の特定のニーズに十分に対応できる柔軟性、 および使用される認証方法を問わない、 かつ一貫したユーザエクスペリエンスを備えている必要があります。 認証を複数回要求して、 ユーザに負担をかけるものではいけません。 たとえば、 多要素認証でローカルデバイスへのアクセスを認証し、 次に、 多要素認証で VPN へのアクセスを認証し、 最後に、 多要素認証でリモートデスクトップへのアクセスを認証することは、 最適なユーザエクスペリエンスとは言えません。 すべてのユーザに万能な解決策はありません。 多くのソリューションは、 スマートフォンと、 既に推奨されなくなったプッシュ通知や OTP、 SMS を組み合わせて使用する必要があります。 一部のユーザはスマートフォンを全く使用できなかったり、 ハードウェアに制限がある場合など、 組織内でソリューションを展開することは非常に困難です。 たとえば、 政府組織や関連機関では、 PIV （Personal Identity Verification） カードが義務付けられていたり、 パスワードの使用を禁止されている場合もあります。 また、 スマートフォンが禁止されていたり、 スマートフォンを認証デバイスとして利用しているが、 ゼロトラスト戦略の要件を満たすためのフィッシング対策が必要な場合もあります。 組織のニーズに合った柔軟性と選択肢を備え、 あらゆる認証で一貫したユーザエクスペリエンスを提供する単一のソリューションを見つけることは、 大きな課題になっています。

解決方法

ウィンマジックは、 下記のように、 Windows 認証の幅広い選択肢を提供しており、 パスワードレス認証への移行におけるお客様のニーズに対応します。

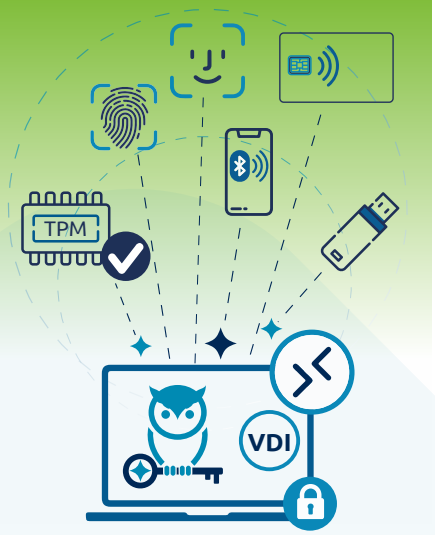
- Bluetooth 接続のスマートフォンを使用した認証
- TPM / PIN （トラステッドプラットフォームモジュール / 個人識別番号） を使用した認証
- Network / IdP （ID プロバイダ） 接続のスマートフォンを使用した認証
- PIV カードを使用した認証
- USB トークン （Yubikey など） を使用したパスワードレス認証

MagicEndpoint は、 Windows のローカルログオンを多要素認証で認証することが可能で、 その後、 SSO によりユーザの操作なしで、 VPN やリモートデスクトップへの認証を自動化することができます。

リモートデスクトップと仮想デスクトップへのログイン

リモートワークでリモートデスクトップを使用する場合、 公共のインターネット接続の安全性を確保することが大変重要です。 また、 ワークステーションとサーバを保護するためのセキュリティ対策が必要になります。 公共のインターネットに接続されたリモートデスクトップサーバは、 多くの場合、 多要素認証を実行できません。 また、 パスワードをフィッシングしたり、 総当たり （ブルートフォース） 攻撃で脆弱なパスワードや再利用パスワードを取得した攻撃者は、 ワークステーションのリモートデスクトップに簡単にアクセスできてしまいます。 このような状況を軽減するため、 多くの組織では、 リモートユーザは、 最初に、 VPN を利用して多要素認証で社内ネットワークに接続する必要があります。 これは第一歩としては適切ですが、 ゼロトラストの観点では、 “社内ネットワーク上からアクセスしたユーザ “ということだけでそのユーザを信頼することは非常に危険で、 ” 外部インターネットからアクセスしたユーザ “と同様に扱う必要があります。 「ゼロトラストアーキテクチャの鍵となる考え方では、 暗黙的に信頼済みとみなすネットワークは存在しません」 （https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf）。 また、 エンドポイントのユーザに管理者権限を与えることはサイバー保険の多要素認証に関する要件を満たしていません。

仮想デスクトップについても、 状況は Windows ログオンと同様です。



フルディスク暗号化を使用している場合、 プリブート認証も同様の方法を利用することが可能で、 一貫したユーザエクスペリエンスが得られます。 さらに良いことに、 一度ユーザがエンドポイントに認証されると、 ユーザの操作なしでシームレスに、 リモートサービスに直接ログインしたり、 認証サービスを IAM に委任することができます。

MagicEndpoint を利用した Windows 認証のデモ動画 （英語） はこちらから視聴できます。

認証し、 暗号化し、 成し遂げる。

Tech Brief

Windows ログオンのパスワードレス認証

MagicEndpoint は、導入・展開、バックアップ・リカバリを支援する一元管理ツールを備えた、Windows ログオンをパスワードレス化する統合認証ソリューションです。

ソリューションの概要を以下に紹介します ：

スマートフォンを使用したパスワードレス認証 ：

Bluetooth 接続のスマートフォンを使用したパスワードレス認証
ユーザにスマートフォンを支給している組織が、 認証にスマートフォンの SMS や OTP、 モバイルプッシュを利用しているが、 これらの認証手段はもはや耐フィッシングではなく、 ゼロトラストの要件を満たしていないため他のスマートフォン認証ソリューションを検討している場合、 MagicEndpoint の Bluetooth 接続は、 最適な選択肢です。 Bluetooth 接続は、 スマートフォンでの OOB （アウトオブバンド） 認証とは異なり、 スマートフォンが物理的にエンドポイントデバイスと Bluetooth 接続可能な距離にある必要があります。 この制限により、 認証ツール （スマートフォン） とエンドポイント間の関連性を確保することが可能になり、 フィッシング攻撃を防止します。 スマートフォン上の MagicEndpoint Authenticatior アプリは、エンドポイントに Bluetooth 接続し、 パスワードレス認証により Windows ログオンすることが可能になります。 ユーザは、エンドポイントに何も入力する必要がなく、 Windows ログオンが可能になり、 真のパスワードレス環境を実現することができます。

Network / IdP 接続のスマートフォンを使用したパスワードレス認証
ユーザにスマートフォンを支給している組織が、 認証にスマートフォンを利用したいが、 Bluetooth を使用できない場合、MagicEndpoint のモバイルプッシュ通知による Windows ログオンを利用することで、 一貫したユーザエクスペリエンスとともにパスワードレス認証を実現することができます。

TPM / PIN を使用したパスワードレス認証 ：

外部トークンや外部デバイスの管理が困難な組織の場合、 エンドポイント自体に内蔵された TPM ハードウェアが、 最適な選択肢になります。 ユーザは、 TPM とローカル PIN を組み合わせて、 Windows にログオンします。 Windows ログオンは TPM によって保護され、 さらに SSO により自動化することができます。 TPM / PIN はローカル上にあるため、 リモートから攻撃することはできません。 また、TPM はハードウェアベースのアンチハンマリング（耐総当り攻撃）保護を備えています。

スマートカード、 USB トークン、 PIV カードを使用したパスワードレス認証 ：

スマートカードや USB トークン、 PIV カードの使用を義務付けている組織の場合、 ユーザは、 ハードウェアトークンを使用して Windows にログオンすることが可能です。 Windows ログオンはハードウェアトークンによって保護され、 さらに SSO により自動化することができ、 優れたユーザエクスペリエンスを実現できます。

IAM ソリューションに対する多要素認証 ：

MagicEndpoint を利用すると、 Windows ログオンと Okta などの IAM ソリューションを統合することができます。
MagicEndpoint のプリブート認証と Okta を統合したデモ動画 （英語） はこちらから視聴できます。

Bluetooth 接続のスマートフォンを利用した MagicEndpoint のプリブート認証 （PBA） のデモ動画 （英語） はこちらから視聴できます。

ウィンマジックの MagicEndpoint は、 ユーザのためにエンドポイントを最大限に活用することに焦点を合わせ開発された、非常にセキュアなパスワードレス認証ソリューションです。 ユーザの認証操作や追加の多要素認証デバイス / USB キーが不要なため非常に安全で、 使用にあたってもシームレスで MagicEndpoint が導入されていることを意識する必要がありません。

2022 年 10 月 26 日

認証し、 暗号化し、 成し遂げる。

米国 / カナダ ： +1 888 879 5879
欧州 / 中近東 / アフリカ （EMEA） ： +49 69 175 370 530
日本 ： +03 5403 6950
詳細は、 こちらをクリックするか、 ウィンマジックまでお問い合わせください。