データシート

Password Manager

ユーザに権限を与え、サポートコストを削減、セキュリティを強化

メリット

- ヘルプデスクおよびITチームによる日常的なパスワード管理を軽減
- ユーザのダウンタイムを大幅に削減
- ROIを即座に実現
- 使いやすさとシンプルな導入によって、ユーザおよびITの満足度を向上
- ネットワークセキュリティを強化
- 異種システム間におけるパスワードの同期を可能に
- セキュリティ強化のため、多要素認証のDefenderと統合

概要

ヘルプデスクのサポートを求める要求のほとんどが、パスワードのリセットに関連しています。組織はセキュリティポリシーをより強固にしようと尽力していますが、パスワード管理はますます困難になっています。より頻繁に変更する必要がある複雑なパスワードを要求すれば、ユーザがパスワードを忘れ、サポートを求めて電話を掛ける可能性は高くなります。また、組織が複数の異なるシステムやアプリケーションにパスワードを適用すれば、この不具合はさらに深刻になります。結果的に、多くの組織がセキュリティの強化とユーザサポートのコスト削減との間で板挟みになっています。

Password Managerは、エンドユーザが忘れてしまったパスワードのリセットやアカウントのアンロックを自分で行えるようにする、シンプルでセキュアなセルフサービス式のソリューションです。管理者はより強固なパスワードポリシーを実施でき、ヘルプデスクのワークロードも軽減できます。コストを削減するためにセキュリティを犠牲にする必要はもうありません。

特長

セキュリティの強化

Password Managerを使用すると、組織はMicrosoft® Active Directory®でネイティブに提供されているアクセス制御よりもセキュアなデータアクセスポリシーを採用できます。ヘルプデスクのミスを減らし、ユーザがパスワードをメモする必要性を排除して、パスワードを推測した不正アクセスをより困難にすることでセキュリティを向上します。組み込み型のデータ暗号化機能はグローバルアクセスをサポートし、データのセキュリティを維持します。

ユーザの参加によるROIの保護

Password Managerによって、ユーザは最も基本的なパスワードタスクを自ら処理できるため、IT予算を節約し、迅速な投資収益を実現できます。

賢明な投資の実施

Password Managerは、深刻さを増す不具合に対する長期的なソリューションです。ITの運用効率を向上させ、セキュリティを強化したいと考えている企業にとって、Password Managerは賢明な投資です。

- 既存のActive Directoryインフラストラクチャの使用におけるコストパフォーマンスの高さ—Password Managerでは、既存のActive Directoryインフラストラクチャをさらに活用できます。Password Managerを迅速に展開し、ROIを即座に実現することもできます。さらにPassword Managerは、Windows Serverよりもきめ細かい、グループベースのパスワードポリシーを提供します。

- ヘルプデスクのワークロードとコストの軽減、ユーザの生産性の向上—Password Managerを使用すると、ユーザはヘルプデスクまたは管理者のサポートを必要とせずに、自分のパスワードをリセットしたり、アカウントをアンロックしたりすることができます。
- オンデマンドのユーザヘルプ—Password Managerは、パスワードポリシーに関する説明をオンラインで提供します。さらに、パスワードのセットアップのルールを満たしていない場合はユーザへ自動的にフィードバックを提供し、ヘルプデスクのサポートを要することなくコンプライアンスに準拠したパスワードをユーザのために生成できます。
- Windowsログオン・ダイアログ・ボックスのためのGINA拡張—ユーザがパスワードを簡単にリセットできるようにするため、管理者はログオン前にパスワードをリセットするボタンをWindowsのログオン画面に表示することができます。これにより、パブリックキオスクや電話を利用した高コストのシステムを構成する必要がなくなります。

組織基準の施行

Password Managerは、組織のポリシーおよびデータセキュリティの基準として想定し得る最大範囲の要求に対応できます。

- 厳格なポリシーの強制—Password Managerは管理者が定義した基準を施行し、失敗した認証試行をログに記録し、必要に応じて対応するアカウントをロックします。
- 強制的な登録—Password Managerは、ユーザが必ず登録を行ってからソフトウェアを使用するためのメカニズムを複数提供することで、その有効性を保証しています。
- 信頼性の高い認証—ユーザ用のQ&A個人プロファイルには、ユーザ自身には思い出しやすく、他人にとっては推測が難しい固有の答えがある質問が含まれています。さらに、Password ManagerをDefenderと共に実装することで、Q&Aプロファイルと併せて、あるいはQ&Aプロファイルの代わりに、より安全なワンタイムパスワード（OTP）認証を要求することもできます。
- セキュリティとシンプルさ—Password ManagerはWindowsとシームレスに統合でき、信頼関係の有無に関わらず、複数のドメインのユーザに対応できます。MicrosoftのCryptoAPIや、SHA-256などの主要なセキュリティテクノロジーをサポートしているので、強力なデータ暗号化やセキュアな通信を実現できます。

システムアクティビティの監視

Password Managerでは、管理者は堅牢なログ記録機能やレポート作成機能を使用でき、システムアクティビティの監視と異常の修正を簡単に行うことができます。

ID管理イニシアチブのサポート

Password Managerには応答性の高いWebインターフェイスがあり、Microsoft Identity Integration Server（MIIS）と接続するあらゆるシステムでパスワード管理を利用できます。また、Authentication ServicesをUnixやLinuxなどMicrosoft以外のオペレーティングシステムにも拡張します。Defenderを介した2要素認証の追加機能です。

One Identity Hybrid Subscription

追加のクラウド機能とサービスを提供するOne Identity Hybrid Subscriptionにより、Password Managerの機能を拡張しましょう。無制限のStarling Two-Factor Authenticationへのアクセスを取得すると、電話検証アドオンの代わりにPassword Managerで管理者およびエンドユーザアクセスの保護を行えます。1件のサブスクリプションで、One Identityソリューションの導入環境すべてに利用できます。

One Identityについて

Quest SoftwareグループのOne Identityは、オンプレミスやクラウドサービス、あるいはハイブリッド環境であっても、組織によるIDを重視したセキュリティ戦略の実装を実現します。アカウント管理、IDのガバナンスおよび管理、特権アクセス管理などを含む当社独自の広範に統合したID管理サービスのポートフォリオにより、組織はプログラムの中心にIDを据えることでセキュリティが実現できる潜在能力を最大限に発揮し、すべてのユーザタイプ、システム、およびデータにわたって適切にアクセスできるようになります。詳細についてはこちらをご覧ください: OneIdentity.com

Datasheet_2019_PasswordManager_US_RS_55939