Evidian

Authentication Manager ビジネス指向・容易な展開

組織全体を対象としたビジネス指向の多要素認証管理

どのような状況でもPCとサーバーへのアクセスを保護できます。ユーザーが1台または複数の PCにアクセスする場合でも、複数のユーザーが1台のPCを共有する場合でも、すべての 認証シナリオに対応できます。

パスワードは、多くの認証ポリシーの弱点なります。共有または安易なWindowsパスワードは侵入のリスクがあり、Windowsアカウントの使用状況を正確に監査することはほぼ不可能です。

パスワードをデバイスまたは生体認証などの強力な多要素認証に置き換えることでこれらの問題は解決されます。

しかし、強力な認証は利用者に運用上の制約をもたらす場合があります。何千人ものユーザーを配置し管理するには、すべてのユースケースをカバーする必要があります。そうしないと、従業員の日常業務に支障をきたすリスクがあります。

専用のビジネス機能

Evidian Authentication Managerを使用すると、共有PCを利用する従業員はWindowsにログオンしたりログオフしたりすることなく、数秒で自分のWindows環境にアクセスできます。

医師が回診のために病院の敷地内を移動しても自身のWindowsセッションを維持できます。フロントデスクのトレーダーやコントロールルームの技術者は、1台のPCから、多要素認証を使用して複数台のPCのWindowsセッションのオープン、ロック、ロック解除、またはクローズを1度に行うことができます。

また、一人の従業員は、1台または複数台のPCに対して、ロックされたセッションへのアクセスを永続的または一時的に (オプションで読み取り専用画面を使用して) 委任できます。

多要素認証の導入を簡単に

Evidian Authentication Managerは、強力な認証の導入と日常的な管理を簡単にします。

- アクセスポリシーの集中管理
- グループベースの認証プロファイル
- 統合カード管理 (発行、在庫、ブラックリストなど)
- PCへのすべてのアクセス試行を一元的に監査

Evidian Authentication Managerを採用すると、一つのテクノロジーに拘束されません。適切な認証を適切な場所に導入できます。貴社の認証ポリシーは、すべての方式に対して中央ポイントから適用されます。

使用コストの削減

Evidian Authentication Managerを使用すると、ヘルプ・デスクのスタッフは1つのコンソールから多種の認証手段 (パスワード、スマートカード、RFID、生体認証、ワンタイムパスワード (OTP) など) のロックを即座に解除したり、アクセスを削除したりできます。

さらに、ユーザーはSelf-Service Password Request (SSPR) を使用してWindowsアクセスのロックを解除できます。これにより、「ロックを解除してください」のようなサポートコールがなくなります。

既存のインフラストラクチャを活用

Evidian Authentication Managerは、セキュリティデータが暗号化されて保存されるLDAPまたはActive Directoryに対応できますので、ユーザーが重複することはなく、アプライアンスも必要ありません。

Microsoftスマートカードログオン

Evidian Authentication Managerは、スマート・カードによるログオンと完全に互換性があり、効率的な緊急アクセス手順を提供します。

IGELシンクライアント統合

Evidian Authentication ManagerとIGELを使用すると、シン・クライアントでの認証がより容易、迅速、安全になります。ユーザーは、RFIDまたはスマートカードを介してLinuxベースのシンクライアントにアクセスできます。

既に認証済みの従業員は、RFIDバッジを提示するかスマートカードを挿入するだけで、その日のうちにシンクライアント上で迅速かつ安全にセッション (Citrix XenAppとMicrosoft RDS) にアクセスできます。

容易な導入

Evidian Authentication Managerでは、1つの部門から開始し、後から数千、数万人のユーザーに拡張することができます。またEvidian Authentication Managerは、Microsoft Windows、Citrix XenApp、Window Terminal Server環境で動作します。

Atos

ビジネス指向・容易な展開

サポートされているさまざまな認証方式

Evidian Authentication Managerは、次の主要な認証テクノロジーをサポートしています。

- 証明書の有無にかかわらず、スマートカードとセキュリティトークン
- 指紋および静脈バイオメトリクス
- RFID無線タグ
- ワンタイムパスワード（OTP）
- 質問と回答の順序
- ログイン・パスワード

認証ライフサイクルの管理

Evidian Authentication Managerには、デバイスのライフサイクルを一元的に管理できるカード管理機能が含まれています。データと証明書が保存されたカードを従業員に発行または貸与できます。カードを一時停止またはブラックリストに登録することもできます。

ユーザーによる委任

ユーザーが不在の場合、Evidian Authentication Managerにより、セキュリティ・ポリシーの管理下でPCへのアクセスを委任できます。

共有アカウント管理

ユーザーは一般的なWindowsアカウントを安全に使用できます。監査イベントには、その認証情報が含まれますのでパスワードを知る必要すらありません。

ActiveSync統合

Evidian Web Access Managerは、モバイルデバイスでWindowsパスワードを要求せずにActiveSyncプロトコルを使用して、電子メールシステムへのモバイルアクセスを制御できます。この場合、Evidian Web Access Managerは

Evidian Authentication Managerが持っているメール・サーバで認証するためのWindowsパスワードを使用します。Evidian Authentication ManagerとWeb Access Managerを組み合わせると、Windowsパスワードを危険にさらすことなくメール・サーバへのアクセスをユーザーに許可できます。

QRコードによる強力な認証

Evidian QRentryでは、ユーザーはモバイルデバイスでQRコードをスキャンするだけでWindowsにログオンできます。このアクセスは、企業ネットワークに接続していなくても使用できます。

Windowsログオン画面からの緊急アクセス

Evidian Self Service Password Request (SSPR) 機能を使用すると、ユーザーは自分でパスワードをリセットすることも、ヘルプデスクから提供されるプロンプトを使用してパスワードをリセットすることもできるため、使用コストを削減できます。この機能を有効にすると、ユーザーは個人的な質問に回答します。アクセス手段を忘れた場合は、パスワードをリセットするか、Windowsセッションにアクセスするための質問に回答します。

ユーザーがSSPRを使用してリセットするパスワードは以下の種類があります。

- 定義された期間のみ使用可能な一時パスワード
- リセットが要求されたPCでのみ有効なパスワード
- ユーザーの最終的なパスワード

そしてオフラインでも!

モバイルユーザーは、企業ネットワークに接続していない場合でも、PCからアクセスをリセットできます。

Q&Aの代替ソリューションとして、QRentryを緊急アクセスとして使用することもできます

Webポータルからの緊急アクセス

ワークステーションからの場合と同様に、ユーザーはAuthentication Manager Webポータルに接続して質問に回答したり、緊急アクセスを有効にしたりできます。

Webポータルを使用して、次の点の組み合わせでパスワードをリセットすることもできます。

- メールまたはSMSでユーザーに送信される確認コード
- 認証手段としてのQRentry

CAPTCHAを使用すると、緊急アクセス手順のセキュリティを強化できます。

情報システムが法律や規制に準拠していることを確認

アクセスおよび管理アクションに関連する署名付き監査証跡は、中央データベースに格納されます。

Authentication Managerは、Sarbanes-Oxley (米国企業改革法)、医療機密に関する法令、PCI DSS、財務の完全性に関する法律などの法的要件や規制要件への準拠を支援します。

従業員のPCへのアクセス試行を監視できます。監査イベントには、ユーザーIDが含まれます。これにより、アクセスポリシーが監視され、その目的を満たしていることを示すことができます。

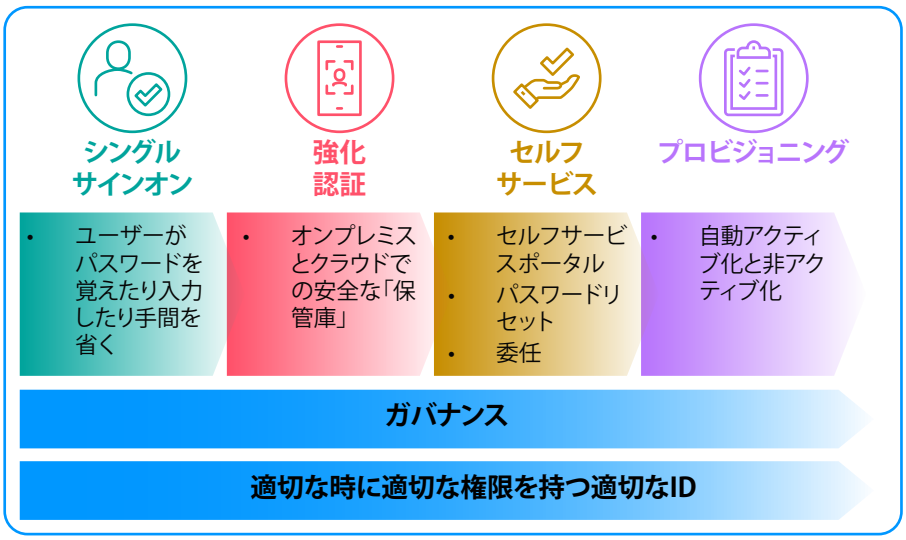
高度なレポートモジュール

Evidian Authentication Managerにはレポート作成モジュールが組み込まれており、アクティビティ、スナップショット、リスク、監視、KPIなどの主要な指標に関するダッシュボードを生成できます。レポートは、権限のあるユーザーがダウンロードできます。

Evidian IAMソリューションへの統合

Evidian Authentication Managerは、Evidianのアイデンティティおよびアクセス管理ソリューションの一部です。以下のソリューションとの組み合わせにより、認証とIDのライフサイクルの収束が保証されます。

- Evidian Enterprise SSOを使用すると、パスワードを追加せずに複数のアプリケーションを起動できます。
- Evidian Web Access Managerを使用すると、各アプリケーションに対する再認証を行うことなく、どのブラウザからでも安全にWebアプリケーションにアクセスできます。
- Evidian Identity Governance and Administrationを使用すると、承認ワークフローと組み合わせたセキュリティポリシーによって、承認ガバナンスと、IDおよびサービスへのアクセスの完全なライフサイクル管理を実現できます。



詳しくはこちら evidian.com/ja/