データシート

One Identity Safeguard

特権アクセスを安全に保存、管理、記録、分析

メリット

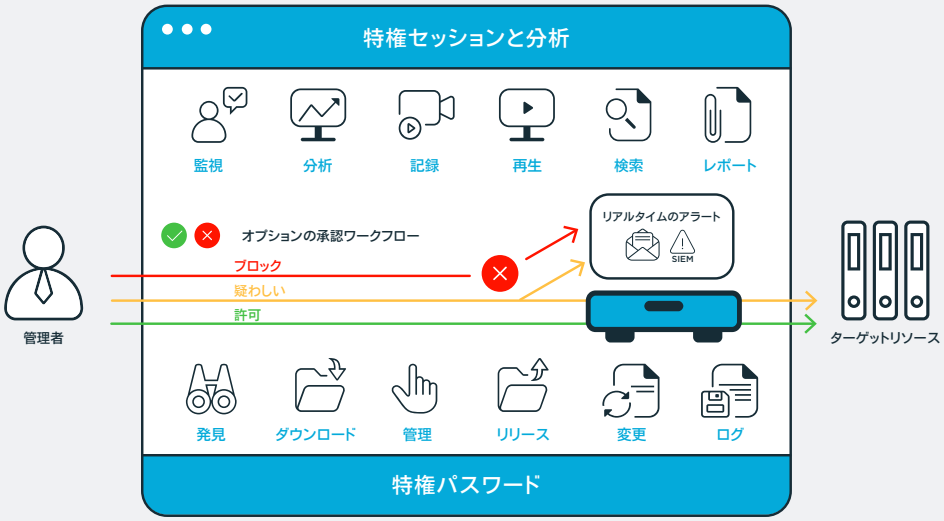
- セキュリティ侵害による損害の可能性を軽減
- コンプライアンス要件への対応
- シンプルな導入と管理で迅速なROIを実現
- 効率的な監査レポート作成
- リスクのある行動および通常でないイベントを識別して阻止
- 特権アカウント管理を簡素化

はじめに

ハッカーはシステムやデータへのアクセスを得るために、絶えずその手法を進化させています。彼らの最終目的は、特権アカウントにたどり着くことです。最近のハイプロファイルな違反のほぼすべてが、特権アカウントへの不正アクセスによって重要なシステムとデータへのアクセスを得たというものです。しかしこういった違反による損害は、安全かつ効率的に、準拠した方法で特権アカウントにアクセスできるソリューションを導入することで制限できます。

ITマネージャにとって、こうしたすべてにアクセスするアカウントの管理は課題です。これには、膨大な数の特権アカウント、およびこれらのアカウントへのアクセスを必要とする多数のユーザ数など、数多くの理由があります。その上、従来の特権アクセス管理（PAM）ソリューションには、複雑なアーキテクチャ、時間を要する導入時間、労力のかかる管理要件が伴います。

PAMは大きな課題になり得えますが、必ずしもそうである必要はありません。One Identity Safeguardは統合ソリューションで、セキュアで堅牢なパスワード保存機能と、脅威検出/分析機能を備えたセッション管理/モニタリングソリューションを組み合わせています。One Identity Safeguardでは、特権アクセスの安全な保存、記録、分析が可能です。



妥協することなく特権アクセスを安全に保護

特権アクセスを安全に保存、管理、記録、分析でき、管理者と監査担当者が満足できるOne Identity Safeguardを利用して、特権アカウント保護についてのストレスをなくしましょう。

Safeguard for Privileged Passwords

One Identity Safeguard for Privileged Passwordsでは、ロールベースのアクセス管理と自動化ワークフローによって、特権資格付与のプロセスが自動化、制御、保護されます。設計もユーザを重視したデザインのため、短期間で習得できます。さらにこのソリューションでは、どこからでもほぼすべてのデバイスからパスワードを管理できます。Safeguard for Privileged Passwordsを使うことで、企業が安全に保護され、特権アクセスを持つユーザに新しいレベルの自由と機能がもたらされます。

Safeguard for Privileged Sessions

One Identity Safeguard for Privileged Sessionsでは、管理者、リモートベンダー、およびその他のハイリスクユーザの特権セッションを、コントロール、モニタ、記録することができます。記録されたセッションコンテンツはインデックス付けされるため、後からセッションイベントを簡単に見つけることができます。また、レポート作成の簡素化と自動化にも役立つため、監査およびコンプライアンス要件への対応が容易になります。さらに、Safeguard for Privileged Sessionsは、プロキシとして機能してアプリケーションレベルでプロトコルトラフィックを検査し、プロトコル違反のトラフィックをリジェクトすることが可能です。そのため攻撃に対する効果的な保護となります。

Safeguard for Privileged Analytics

One Identity Safeguard for Privileged Analyticsではユーザ行動分析を利用できます。これにより、未知の内外脅威を検出し、疑わしいアクティビティを発見して阻止することができます。また、データ漏洩を防ぐだけでなく、可能性のある脅威のリスクレベルを順位付けるため優先順位がわかり、最も急を要する脅威への迅速な対応が可能になります。

特長

ポリシーベースのリリース管理

モバイルデバイスに対応するセキュアなWebブラウザを使用し、アクセスを要求して特権パスワードとセッションの承認を行うことができます。これらの要求は、組織のポリシーに基づいて、自動的に承認したり、承認の多重化を義務付けたりすることが可能です。要求者のIDとアクセスレベル、要求の送信日時、要求対象のリソース（特定のリソースだけか全部か）など、ポリシーで検討すべき独自のニーズに合わせて、One Identity Safeguardを設定できます。さらに、理由コードの入力や、チケットシステムとの統合も可能です。

全セッションを監査、記録、再生

全セッションのアクティビティ（キーストローク、マウスの動き、表示ウィンドウなども含む）がキャプチャ、インデックス付けされ、改ざん防止の監査証跡に保存されます。ここでは動画再生や、データベースのような検索が可能です。セキュリティチームは、全セッションから特定のイベントを検索し、検索条件に一致したポイントから記録を再生することができます。監査証跡は、フォレンジックとコンプライアンス目的で暗号化されてタイムスタンプが押され、暗号署名が行われます。

変更管理

時間に基づく変更、前回の使用に基づく変更、手作業による変更、強制的な変更など、設定できる細かい共有資格情報の変更管理をサポートします。

ユーザ行動のバイオメトリック

各ユーザは行動について特有のパターンを持っています。これは、キーボード入力やマウスの動きなどの同じようなアクションについても同様です。Safeguard for Privileged Analyticsに組み込まれたアルゴリズムでは、これらの（Safeguard for Privileged Sessionsによってキャプチャされた）行動特性を検査します。キーストロークダイナミクスとマウス動作の分析は、違反の識別に役立ち、途切れることのないバイオメトリック認証の機能も果たします。

どこからでも承認可能

One Identity Starling Two-Factor Authenticationを利用することで、どこからでもほぼすべてのデバイスで、要求を承認またはリジェクトすることができます。VPN上である必要もありません。

お気に入り

頻繁に使用するパスワードに、ログイン画面から素早くアクセスできます。複数のパスワード要求を1つのお気に入りにグループ化すれば、1回のクリックで必要なアカウントすべてにアクセス可能になります。

検出

ネットワーク上の特権アカウントまたはシステムを、ホスト/ディレクトリ/ネットワーク検出オプションを使用して迅速に検出します。

リアルタイムのアラート機能とブロック機能

Safeguard for Privileged Sessionsによって、トラフィックがリアルタイムでモニタされ、特定のパターンがコマンドラインまたは画面上に表示されると、さまざまなアクションが実行されます。事前定義のパターンには、テキスト志向のプロトコル内でリスクを伴うコマンドまたはテキスト、あるいはグラフィカル接続での疑わしいウィンドウタイトルなどがあります。ユーザによる疑わしいアクションが検知されると、Safeguardによってイベントの記録とアラートの送信が行われ、直ちにそのセッションは終了されます。

コマンドとアプリケーションコントロール

Safeguard for Privileged Sessionsは、コマンドとWindowsタイトルのブラックリストとホワイトリストの両方に対応しています。

インスタントに起動

Safeguard for Privileged Sessionsは、ユーザワークフローへの変更を必要としない、トランスパレントモードでの導入が可能です。プロキシゲートウェイとして機能するSafeguardは、ネットワーク内のルーターのように、ユーザおよびサーバから見えない状態で作動することができます。管理者は、使い慣れたクライアントアプリケーションの使用を続けられ、日々の作業を中断することなくターゲットのサーバおよびシステムにアクセスできます。

広範なプロトコルサポート

SSH、Telnet、RDP、HTTP、ICA、VNCの各プロトコルに完全対応しています。さらに、セキュリティチームは、管理者用に有効/無効にしたいプロトコル内のネットワークサービス（例: ファイル転送、シェルアクセスなど）を決定することができます。

フルテキスト検索

Optical Character Recognition（OCR）エンジンでは、セッションコンテンツでユーザが閲覧したコマンドおよびテキストの両方について、監査担当者によるフルテキスト検索が可能です。また、ファイル操作をリストし、レビュー用に転送ファイルを抽出することもできます。セッションコンテンツとメタデータを検索できる機能によって、フォレンジックとITトラブルシューティングが迅速化され簡素化されます。

簡単な導入

迅速なアプライアンスベースの導入およびシンプルなトラフィック再ルーティングを利用するため、One Identity Safeguardでは、ユーザが作業を中断することなく、数日でセッションを記録できるようになります。

RESTful API

Safeguardは、他のアプリケーションおよびシステムとの接続にREST準拠の刷新されたAPIを使用します。各機能はAPIを介してアクセス可能となり、目的やアプリケーションの使用言語を問わず、迅速かつ簡単な統合が可能です。

One Identity Hybrid Subscription

Safeguardの機能はOne Identity Hybrid Subscriptionによって拡張可能です。One Identity Hybrid Subscriptionは、クラウド配信型の機能とサービスへ迅速なアクセスを提供します。Subscriptionには、Safeguardのアクセスを保護するStarling Two-Factor Authentication、および特権アクセス権限を認証し、コンプライアンスを確実にするStarling Access Certification for Safeguardが含まれます。

One Identity製品による特権アクセス管理

One Identityのポートフォリオには、業界で最も包括的な一連の特権アクセス管理ソリューションが含まれます。また、UNIXのルートアカウントとActive Directoryの管理者アカウント、オープンソースのsudoをエンタープライズ対応にするアドオン、UNIXのルートアクティビティ用のキーストロークロギングなどの、きめ細かい権限委任を可能にするソリューションを使用して、One Identity Safeguardの機能を拡張できます。これらはいずれも、業界をリードするActive Directory連携ソリューションと緊密に統合されています。

One Identityについて

One Identityは、組織のID管理およびアクセス管理のお役に立ちます。当社独自の機能およびサービスの組み合わせ（IDガバナンスのポートフォリオ、アクセス管理、特権管理、IDaaSソリューションを含む）を利用することで、組織は、脅威に対する保護を確保しながらもセキュリティによる制限のない環境で、最大の可能性を実現することができます。詳細はOneIdentity.comをご覧ください