データシート

One Identity Safeguard for Privileged Passwords

共有された特権資格情報からリスクを排除する

メリット

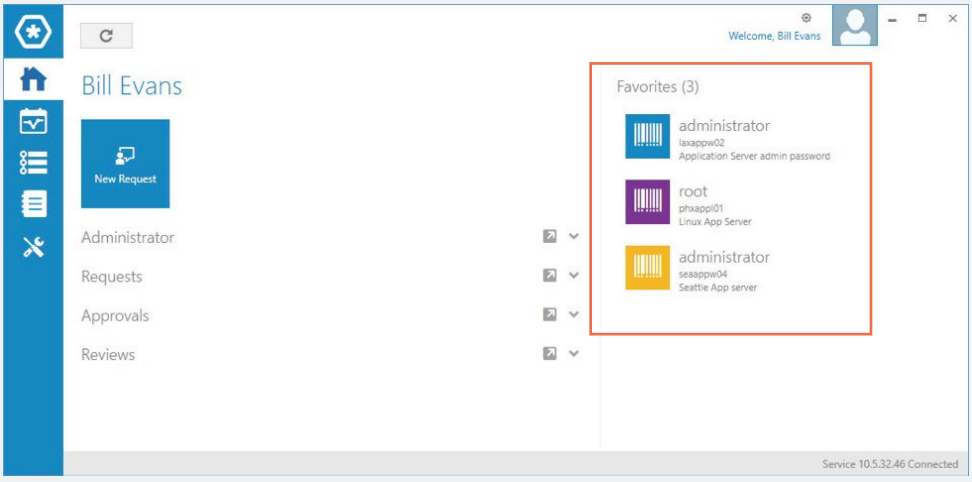
- 特権アカウントへのアクセスを制御することでセキュリティ違反による被害を緩和
- 特権アカウントのコンプライアンス要件を容易に満たすことが可能
- シンプルになった導入と進行中の管理で、より早く価値を獲得
- 短期間で習得でき、UIのデザインも洗練されているので、生産性が最大化
- シンプル化されてより早くなった監査レポートの作成

はじめに

最近のインシデントでは、システムセキュリティにおいて最も重要で、なおかつ大きな損害を与える可能性も秘めている要素は、特権アカウントのパスワードであることが幾度となく示されています。こうしたパスワードは王国への鍵となります。ハッカーは一度パスワードを入手してしまうと、システムとデータへ無制限にアクセスできてしまいます。すでにお分かりのとおり、影響を受けた組織の評判と失われた知的財産にかかるコストは計り知れません。

これまでは、特権資格情報を保護することで摩擦が生じ、日常的にも長期的な運営においても生産性が低下してしまっていました。この難題のせいで、IT管理者とセキュリティ責任者はしばしば、使いやすさとセキュリティを比較検討するという不幸な状況にありました。それもこれまでの話です。One Identity Safeguard for Privileged Passwordsなら、セキュリティと使いやすさの両方を実現できます。

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、特権資格情報を付与するプロセスが自動化、制御、保護されます。強化されたアプライアンスとして導入することができるので、ソリューション自体へのアクセスを保護することに関して懸案事項がなくなります。また、システムとIT戦略の統合を加速することにも役立ちます。さらに、ユーザ中心の設計であるため、短期間に習得でき、どこにいても、ほとんどどんなデバイスからでもパスワードを管理することができます。その結果、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。



パスワードへの迅速なアクセス

お気に入り機能により、最もよく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。

機能

リリース管理

アクセスを許可されたアカウントについて、承認されたユーザからのパスワード要求を管理できます。安全なWebブラウザ接続を通じて作業でき、モバイルデバイスもサポートしています。

ワークフローエンジン

時間制限、レビュー担当者、複数の承認者、緊急アクセス、ポリシーの有効期限をサポートするワークフローエンジンです。また、理由コードを入力したり、チケット発行システムに直接統合したりする機能もあります。パスワードリクエストを自動的に承認するよう設定することもできますし、複数レベルの承認を必須とするよう設定することもできます。

検出

ネットワーク上のあらゆる特権アカウントやシステムを、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。

どこからでも承認可能

One Identity Starlingを活用して、VPN外でどこでもリクエストを承認または拒否できます。

お気に入り

最もよく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。

常にオンライン

このソリューションは分散クラスタリング用にビルドされているので、真の高可用性を得ることができます。さらにロードバランシング機能により、アプライアンスからパスワードとセッションを要求した際のスループットが早くなり、応答時間がさらに短くなります。

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。

アクティビティセンター

クエリビルダを使用して、すべてのアクティビティを素早く簡単に表示できます。レポートをリクエストした人によって（ITオペレーション、経営幹部など）、必要な情報を取得するためにデータを追加または削除できます。また、クエリをスケジュールしたり、データをさまざまな形式で保存/エクスポートしたりできます。

2要素認証サポート

パスワードへのアクセスを他のパスワードで保護するだけでは不十分です。Safeguardに2要素認証を要求することでセキュリティを強化します。SafeguardはOne Identity Hybrid Subscriptionを使用した無制限の2要素認証など、あらゆるRADIUSベースの2要素認証ソリューションをサポートしています。

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、クラウドサービス配信型の機能とサービスへの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無制限のStarling Two-Factor Authenticationと、特権アクセス権限を認証して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。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。

スマートカードのサポート

強力な認証方法を使用して、資産へのアクセスを保護します。

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、組織がIDおよびアクセス管理（IAM）の権限を取得するのに役立ちます。IDガバナンス、アクセス管理、特権管理、IDaaSソリューションのポートフォリオなどのサービスを固有に組み合わせることで、組織はセキュリティによる制限なく、しかも脅威から保護され、潜在能力を十分に発揮できます。

詳細については、OneIdentity.comを参照してください。

Datasheet_2019-Safeguard-PrivPass_RS_41020