データシート

One Identity特権アクセス管理

特権アクセス管理によって権限管理の一元化を実現

メリット

- 管理アクセスの全社的な制御
- 効率、セキュリティ、およびコンプライアンスの改善
- すべての特権アクティビティのシンプルな追跡および監査

IDおよびアクセス管理（IAM）ソリューションのOne Identityにより、全社規模で管理アクセスを制御する権限が付与されます。特権アクセス管理のためのOne Identityソリューションは、セキュリティとコンプライアンスを強化しながら効率性を改善します。管理者には必要十分な権限だけが付与され、すべてのアクティビティが追跡、監査されます。

具体的には、One Identityソリューションでスーパーユーザ資格情報に関するきめ細かいポリシーベースの委任、セッションの監査および再生、キーストロークロギングが行われます。また管理者に対して、あるいはアプリケーション間、アプリケーション-データベース間で特権資格情報を発行するセキュアな自動ワークフローも確立されます。One Identityの特権アクセス管理ソリューションスイートには、ネットワークベースとホストベース両方のソリューションが含まれています。

ONE IDENTITY

特権アクセス管理のためのOne Identityソリューションには、スーパーユーザ資格情報に関するきめ細かいポリシーベースの委任、セッションの監査および再生、キーストロークロギング、セキュアな自動ワークフローが含まれています。

ネットワークベースのソリューション

この強力なソリューション群は、「特権保護」機能と、セキュアで強固な単一のアプライアンスによるセッションの監査と再生を可能にします。アプライアンスは最大の経済効率で容易に導入でき、システム全体が保護されます。

One Identity Safeguard for Privileged Passwords

はシステム、デバイス、およびアプリケーションの非常に多様な展開にわたって個々のアカウンタビリティを確保するために、特権パスワードのセキュアなストレージ、リリース管理、変更管理を提供します。管理者が（一般的にUNIXのルートアカウントやWindows Administratorアカウントなどの共有資格情報を通じて）昇格された特権を要求した場合は、適切な承認により、確立されたポリシーに従ってアクセスが許可されます。すべてのアクションが完全に監査および追跡され、返されたパスワードは直ちに変更されます。One Identity Safeguard for Privileged Passwordsアプリケーションのパスワード管理機能では、ハードコードされたアプリケーションとデータベースパスワードの代わりに、プログラム呼び出しによってアカウントの資格情報が動的に取得されます。

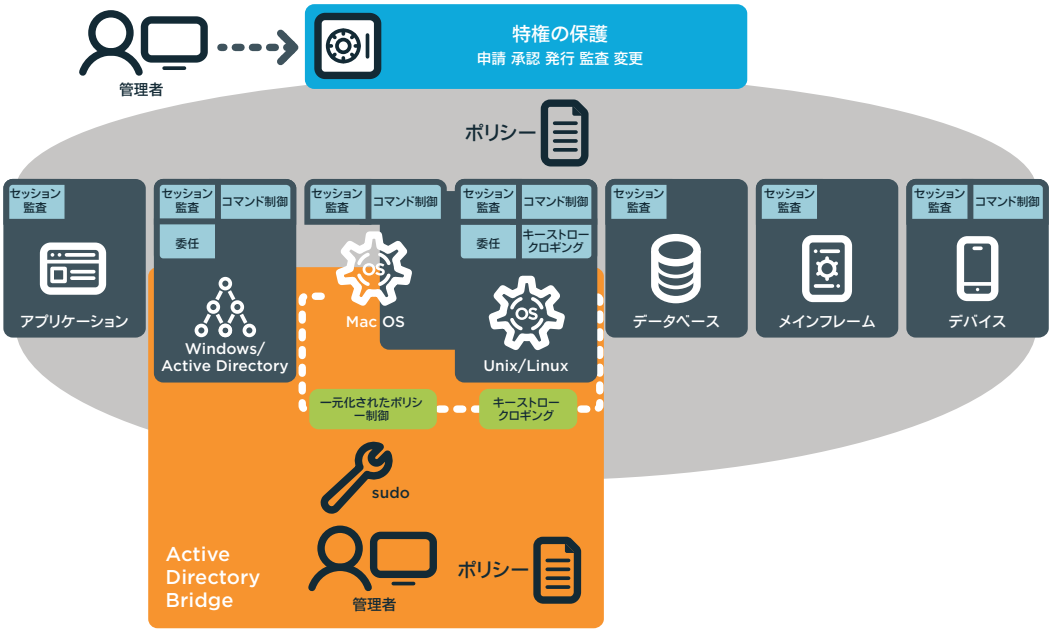
One Identity Safeguard for Privileged Sessions

は、管理者やリモートベンダーなどの高リスクのユーザのセッション制御、プロキシ、監査、記録および再生を可能にします。接続の許可、特定のリソースへのアクセスの制限、アクティブな接続の表示、すべてのアクティビティの記録、事前に設定した制限時間を超過した場合のアラート、接続の停止は、すべて一元的に管理できます。

ホストベースソリューション

これらの強力なソリューションは、ターゲットシステムに導入されたエージェントを通じて、セキュリティと制御を最大にします。最も厳しいコンプライアンスが要求されるシステムでも、One Identityのホストベースのソリューションにより、監査担当者が求める詳細できめ細かい「フォレンジック対応」の可視性が得られます。

Privilege Manager for Sudoは、UNIX/Linuxを使用している組織において、sudoによる特権アクセス管理を新たな次元へと導きます。プラグインにより、中央のポリシーサーバ、sudoおよびsudoersポリシーファイルの集中管理、sudoersのアクセス権やアクティビティに関する一元化されたレポート作成、ならびにsudoアクティビティの



One Identityソリューションにより、各種のプラットフォームとシステムで、スーパーユーザアカウントと共有管理資格情報へのアクセスに対する保護、委任、制御、監査が可能になります。

ONE IDENTITY

One Identityソリューションにより、全社規模で管理アクセスを制御する権限が付与されます。

キーストロークロギングが可能になり、Sudo 1.8.1以降のプログラムが強化されます。sudoを全社規模で簡単かつ直感的に、一貫性をもって管理できるため、 ボックス単位の管理が不要になります。Authentication Servicesは、UNIX/LinuxのIDをMicrosoft® Active Directory®に統合することで、Privilege Manager for UNIXを強化します。共通の管理インターフェイスとポリシーセットを使用してUNIXのルート権限の委任を制御できます。Authentication Servicesは、広く普及している「Active Directory Bridge」の先鞭をつけたサービスです。

> 特権アクティビティは、すべてワンクリックレポートによって監査できます。

Privilege Manager for UNIXは、ルートアクセスの全権限を誤用や悪用の可能性から保護します。Privilege Managerは、誰がどのルート機能にアクセスできるかと、それらの機能をユーザがいつどこで実行できるかを規定するセキュリティポリシーの定義を支援します。また、既存のプログラムや、一般的なシステム管理のタスクに使用される特定用途向けに設計されたユーティリティへのアクセスを制御します。さらにPrivilege Managerでは、キーストロークレベルに至るすべてのアクティビティの包括的な監査が可能です。

Active Roles Serverは、明確に定義された単一のロール、ルール、ポリシーのセットを使用して、Active Directory Administratorアカウントをきめ細かく委任し、管理アクセスを一元的に制御できます。

Privilege Managerは、ベストプラクティスに従ってユーザアカウントに必要最低限の権限を付与しながら、必要に応じて、特定のアプリケーションとActiveXコントロールの権限を昇格させます。実行権限の昇格は、選択したアプリケーション、機能、コントロールだけに設定できます。アクセス権は、特定のユーザ、ユーザグループ、組織単位、オペレーティングシステム、コンピュータグループ、オフィス、またはアプリケーションに付与します。特権アクティビティは、すべてワンクリックレポートによって監査できます。

詳細情報

特権アクセス管理の詳細については、oneidentity.com/solutions/privileged-access-management/をご覧ください。

One Identityについて

One Identityは、組織がIDおよびアクセス管理（IAM）を最適化するために役立ちます。IDガバナンス、アクセス管理、特権管理、およびIDaaS（Identity as a Service）ソリューションを含む当社のサービスの独自の組み合わせにより、組織はセキュリティに妨げられることなく、かつ、脅威に対して保護しながら、最大限の可能性を実現できます。詳細については、OneIdentity.comをご覧ください。

DataSheet-PrivilegedAccessMgmt-US-KJ-30920

ONE IDENTITY