opentext™ | Cybersecurity

データシート

NetIQ Privileged Account Manager

NetIQ Privileged Account Manager を使用すると、データベース、アプリケーション、クラウドの全体にわたって特権ユーザーアクセスを制御および監視できます。

製品の概要

専門家の推計によると、セキュリティ侵害の半分は組織内部から発生しています。内部脅威は、必要以上に高度なアクセス権限を持つ従業員が関連している場合には、特に深刻です。権限の不正使用が従業員の手によるものであれ、内部ユーザーのアクセス資格情報を利用して IT ネットワークにアクセスしたサイバー犯罪者の仕業であれ、スーパーユーザーやデータベース管理者などの特権ユーザーが何にアクセスし何を行っているかを厳密に制御および監視できれば、こうしたリスクを適切に管理できます。

NetIQ Privileged Account Manager by OpenText を使用すると、管理スタッフ全員に root アカウントの資格情報を配布する必要がなくなります。一元化されたポリシーによって管理者権限でのアクセスが委任されます。ユーザー名、入力コマンド、ホスト名、時刻を特定する包括的な「誰が、何を、どこで、いつ」モデルに基づいて、ユーザーアクティビティを許可または拒否するよう、これらのポリシーを設定します。このようにして権限を管理することで、ユーザーが何のコマンドをいつどこから実行する権限を持つかを制御できます。

NetIQ Privileged Account Manager には、システム、アプリケーション、データベースのパスワードを安全に保管する Enterprise Credential Vault (暗号化されたパスワードの「保管庫」) という機能が備わっています。Enterprise Credential Vault は、組織の特権アカウントを一元的に管理できます。また、特権ユーザーは直感的なインターフェイスでパスワードをチェックアウトおよび返却することができます。アプリケーション (SAP System など)、データベース (Oracle DBMS など)、クラウドサービス (Azure、AWS、Salesforce.com など) を対象とした、より広範な特権アカウントのサポートも可能になります。

NetIQ Privileged Account Manager は、業界唯一の GUI ベースのドラッグアンドドロップインターフェイスを採用しているため、ルールを簡単に作成でき、複雑な手作業でのスクリプト作成が実質的に不要となります。統合されたテストスイートツールを使用すると、新しいルールの組み合わせを本番環境に導入する前にモデル化してテストできます。

NetIQ Privileged Account Manager は独自のリスク分析エンジンを用いて、入力された各コマンドを分析し、実行されたコマンド、実行したユーザー、実行した場所に応じて、それぞれに 0 ～ 9 のリスクレベルを割り当てます。リスクの高いコマンドは赤色、リスクの低いコマンドは緑色で示され、リスクの度合いに応じて色調が変わっていくため、セキュリティリスクを招く可能性のあるイベントを即座に識別できます。加えて、再生機能を備えた直感的なインターフェースを通じて、記録されたすべてのキー操作を表示することができます。イベントを詳細に分析する必要がある場合は、ワークフロープロセスによって、そのイベントを適切な管理者にエスカレーションし、管理者は即座に対応することができます。

NetIQ Privileged Account Manager では、リスクベースのアクティビティ制御が拡張されており、特権ユーザーのセッション中に自動的にポリシーが適用されます。制限されたデータへのアクセスやサービスの停止などの高リスクのアクティビティをユーザーが実行したときには、セッションを自動的に切断したり、特権アカウントへのアクセスを無効化するなどの設定が可能です。

システム要件

NetIQ Privileged Account Manager の対応プラットフォーム一覧およびインストール要件の詳細については、こちらのインストールガイドを参照してください。

主なメリット

異機種混在環境全体にわたり、未承認・未監視の特権ユーザーのアクセスを制御および監視できます。

- セキュリティポリシーを単一の画面で一元管理できます。
- 社内のポリシーや外部規制に対するコンプライアンスを継続的にサポートできます。
- 複雑な手動スクリプト作成を行う必要が実質的になくなります。
- 一元的な管理によって環境全体に一貫したポリシーを適用できます。
- プライバシーに関する法律や規制に準拠するための、アクセスの強制、分析、レポート作成が可能です。
- ArcSight Intelligence by OpenText™ との連携により、ID 権限の昇格時にアクティビティに関連するリスクを考慮するリスク認識型サービスを利用できます。
- 特権セッションをリアルタイムに監視できます。

主な特長

特権アカウント管理ソリューションを設計、構成、テストし、1 か所から環境全体に導入できます。

- 暗号化されたパスワードの「保管庫」である Enterprise Credential Vault
- ユーザー、ツール、アプリケーションを対象とするデータベース特権アカウントの監視
- セッションの自動終了やアクセス権無効化を可能にするリスクベースのセッション制御
- オペレーティングシステムに対するリモートでのセッションの確立と制御
- リスクの高いユーザーを迅速に特定するリスクプロファイリング
- 潜在的な脅威分析に基づくスマートリスク評価
- Windows と Linux をエージェントベースとエージェントレスの両方でサポートする柔軟な導入

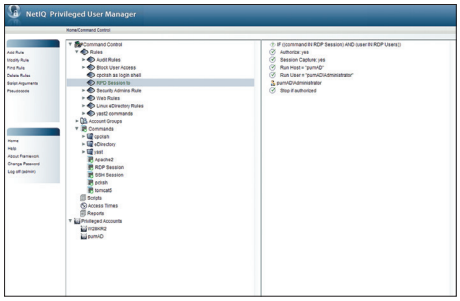

図 1. ［Command Control］コンソールで管理者はユーザーコマンドを保護および制御できます。

主な差別化要因

極めて包括的な監査証跡を構築できます。NetIQ Privileged Account Manager は、SAP System などのアプリケーション、Oracle DBMS などのデータベース、Azure、AWS、Salesforce.com などのクラウドサービスを含む、すべての資格情報ベースの環境を対象に、100% のキーストロークロギングとビデオキャプチャを使用してすべてのユーザーアクティビティの監査を実施することを可能にします。

特定のアクセスイベントに対し、監査担当者はイベント全体をキーストロークレベルで、色分けされた形で行単位で詳細がわかるように再生することができ、また、各イベントに「許可済み」または「未許可」のステータスを適用することができます。

NetIQ Privileged Account Manager の詳細については、こちらをご覧ください。

お問い合わせ

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。

760-JA0001-004 | O | 06/24 |