opentext™ | Cybersecurity

ソリューションハンドアウト

Workday と NetIQ Identity Governance and Administration の統合

ID ライフサイクルの変更を検出する Workday コネクタを使用して、ビジネスの加速、リソースへのアクセス管理、リスクへの適応を実現します。

Workday と NetIQ Identity Governance and Administration 統合の概要

生産性の強化

ビジネスプロセスの自動化により、リソースへのタイムリーなアクセスを実現。

リアルタイムでの変更検出

Workday で ID ライフサイクルの変更が発生したときにそれを検出して対応。

継続的なコンプライアンス

ガバナンスポリシーとアクセスレビューを通じてリスクを特定し、修正。

リアルタイム同期の重要性

人事情報の主要な情報ソースであるクラウドベースの Workday システムには、組織全体のプロビジョニングとガバナンスのプロセスをサポートする重要な情報が含まれています。しかし、企業全体でこの情報を効果的に共有して同期させることは困難です。

Workday やその他のシステムが ID 情報をサイロ化して管理すると、効率性とセキュリティに影響を及ぼします。IT チームは、つながりのないシステムを定期的な調整と手動プロセスによって管理する作業に多大な時間を取られます。ユーザーは、アプリケーションやデータへのアクセスに時間がかかりすぎるため、生産性が低下します。そして承認者は、正確なレビューによって意思決定を行うための適切なデータを得られず、不適切な承認も行われ、本来の適切なアクセスよりもはるかに多くのアクセスが承認されることになります。

効果的な ID ガバナンスおよび管理 (IGA) を実現するためには、新しいアプローチが必要です。

適応型の ID ガバナンスおよび管理

組織に必要なのは、Workday で変更が発生したときにその変更を検出する機能です。特定の時点で行われる定期的な照合作業をただ待つのではなく、ほぼリアルタイムの現状に基づいてポリシーを評価する必要があります。そうすれば、リソースへのアクセスを自動化し、人の介入が必要となるのは例外に対してのみとすることができます。ビジネスユーザーはリスクの高いアイテムに集中し、何度もアクセスしなければならない原因であるシステム間の差異をなくすことができます。

Workday Connector for NetIQ Identity Governance and Administration by OpenText により、Workday での ID ライフサイクルの変更が他のシステムのアクセスにどのような影響を与えるかを、ほぼリアルタイムで確認できます。Workday で変更が行われると、接続されたシステムでワークフローを開始して、リソースを保護しながらアクセスを効率化できます。また、リスクに影響を与える変更を特定してこれに対応し、セキュリティ制御を適応させるための措置を即座に講じることもできます。

Workday と NetIQ Identity Governance and Administration の統合により、組織は接続された複数のシステム全体にわたって、以下のようなユースケースに対応できるようになります。

- Workday での退職処理後に、Active Directory から特権ユーザーの管理アクセス権を削除する。
- ある管理者が離職した後に、その管理者が持っていた経費承認の責任を再割り当てする。
- 職務の移行期間中にあり、移行前 / 移行後のどちらの職務にも適合しない外れ値のアクセス権を持っているユーザーに対して、マイクロ承認処理を付与する。

仕組み

NetIQ Identity Governance and Administration は、オンプレミスおよびクラウドベースのアプリケーション、ディレクトリ、データベースなど、さまざまなシステムに対応するコネクタを備えています。リアルタイムかつイベントドリブンのセキュリティアーキテクチャにより、エコシステム全体での双方向の自動変更が可能なため、定期的な調整が不要になり、システム間の差異がなくなるためアクセスを頻繁に繰り返す必要もなくなります。

お問い合わせ
www.opentext.com

Workday と NetIQ Identity Governance and Administration を統合することで、以下のことが可能になります。

- **Workday の変更をリアルタイムで検出**：組織環境全体の ID とアクセスの最新状況を統合された形で確認できます。
- **継続的なコンプライアンスの実現**：リソースへのアクセスの自動調整、マネージャーへのアラートの送信、ITSM システムへのアクセス変更の送信などの機能によって実現されます。
- **IT リソースを解放**：極めて複雑な ID プロセスであってもプロビジョニングとフルフィルメントを実施する自動ワークフローに変換できます。
- **ガバナンスの制御を実現**：過剰なアクセス、孤立したアカウント、職務分離違反などを修復します。

包括的な ID ガバナンスおよび管理プログラムの一環として、Workday と NetIQ by OpenText™ の統合を行うと、組織はビジネスを加速し、リソースへのアクセスを管理し、リスクへの適応を行うことができます。柔軟性と拡張性に優れたこの強力な基盤によって、エンタープライズ環境全体で ID を管理し、アクセスを制御できるようになります。

詳細はこちら：
www.microfocus.com/ja-jp/cyberres/identity-access-management/identity-governance-administration

NetIQ by OpenText について

このたび、OpenText による、CyberRes を含む Micro Focus の買収が完了しました。両社の専門知識の融合によって、セキュリティ製品 / サービスの提供が拡張され、権限とアクセスの制御の自動化を通じて、アプリケーション、データ、リソースへの適切なアクセスを確保することにより、お客様の機密情報の保護を支援します。NetIQ Identity and Access Management は OpenText Cybersecurity の一部であり、あらゆる規模の企業やパートナーに包括的なセキュリティソリューションを提供します。

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。

761-JA0024-004 | O | 05/24 | © 2024 Open Text