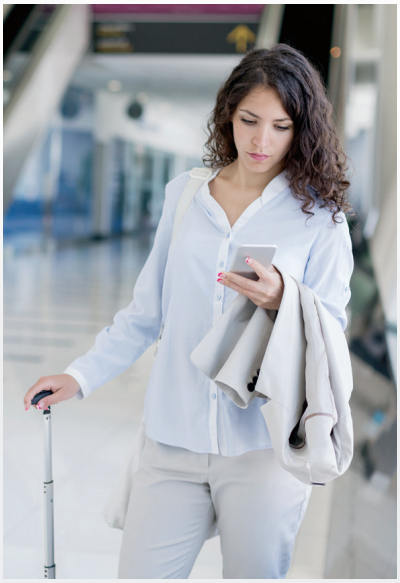
opentext™ | Cybersecurity

製品ハンドアウト

Web シングルサインオンをすべてのユーザーに

顧客がさらにデジタル化していく中で、ビジネスがこのシフトする深化に対応できているかどうかを問うことは重要です。なぜなら、顧客およびパートナーとの関係を今後も維持するためには、一般的なインフラストラクチャよりも優れたアクセスとセキュリティインフラストラクチャが必要になるからです。自社のアクセス管理は、ビジネスにおけるデジタル領域の保護と提供を行ううえで十分な堅牢性を備えているでしょうか？

NetIQ Access Managerの概要
フェデレーションによるシングルサインオンを提供する場合でも、複雑な環境にNetIQ Access Manager by OpenTextの堅牢なゲートウェイが必要な場合でも、組織のアプリケーションやサービスへのアクセスを便利で安全に提供することができます。



強力なアクセス管理が必要な場合とは

NetIQ Access Manager は、顧客、従業員向けのモバイルおよび Web シングルサインオンソリューションです。単なるフェデレーション機能だけでは不十分なマルチプラットフォーム環境に特に適しています。一般的に、セキュリティを強化してオーバーヘッドコストを削減する場合、アクセスを一元的にコントロールすることがセキュリティの向上とオーバーヘッドコストの削減につながりますが、それに加えて、NetIQ Access Manager は市場の他の製品よりも、特定のユーザーエクスペリエンスを提供するうえで適していることにお気づきになるかもしれません。NetIQ Access Manager は、異なるアプリケーションを単一のユーザーエクスペリエンスに統合したり、複数のバックエンドプロセスを単一のモバイルエクスペリエンスに統合したりする必要がある場合に、その力を発揮します。

企業のインフラストラクチャは時を経て新旧のテクノロジーが混在したものとなるため、一連のアプリケーションとサービスとして単一のユーザーエクスペリエンスにまとめることは、往々にして複雑で、制限的でさえあります。組織が NetIQ Access Manager よりも堅牢性と成熟度が劣るアクセス管理ソリューションを選択した場合、複数のソリューションを管理しなければならず、追加のハードウェアコストやオーバーヘッドコストが発生する可能性があります。そして最終的に、最高のエクスペリエンスをユーザーに提供することも、必要なセキュリティを確保することもできなくなる可能性があります。このような環境では、個々のアプリケーションとサービスを、スムーズで途切れることのないシームレスなユーザーエクスペリエンスに統合する、優れたアクセスゲートウェイが必要となります。

認証と権限管理を単一のソリューションにまとめると、単一のポリシーとプロセスでアクセスを保護し、制御できるため、コストを削減することができます。このアプローチは特に、モバイルユーザーに当てはまります。サイロ化されたモバイルアプリは本質的にセキュリティが低いという事実に加え、モバイルアプリのセキュリティや使用するシステムではなく、モバイルアプリ自体にセキュリティを集中する必要があります。開発者からすると、そうしたアプリは余計な仕事を増やす原因でもあります。デスクトップおよびラップトップユーザーの場合と同様に、ID管理とアクセス管理のフレームワークを1つにすれば、不要な資格情報管理とアクセス制御の作業をなくすことができます。

調査対象者の 78% が、モバイルプラットフォームへのマイグレーションが自社のアクセス管理のアプローチに多大な影響を与えたと回答しています *。NetIQ Access Manager は、クラウド、モバイルおよび企業全体にわたる Web リソースの安全を確保します。

お問い合わせ
www.opentext.com

NetIQ Access Manager を選択する理由

他のベンダーからも類似のテクノロジーが提供されていますが、NetIQ Access Manager では柔軟でコンパクトなアプローチにより構成が簡素化されており、大規模な環境や分散環境に必要な優れたパフォーマンスが提供されます。必要なボックスの数が少なく、管理コストも抑えられます。アクセス管理はその特性上、多くの動的パーツを含む構成に拡大しやすいため、このことは重要です。主な特長は以下のとおりです。

- **モバイルシングルサインオン：**NetIQ Access Manager はネイティブでモバイル SDK をサポートしているため、シングルサインオンの負担を軽減できます。ネイティブのモバイルアプリでサービスを提供する場合も、NetIQ Access Manager なら、iOS 用の SDK、OpenID Connect、あるいは OAuth 認証が含まれています。顧客向けか社内向けかを問わず、NetIQ Access Manager はこれらのアプリケーションに適した認証とアクセス制御を行います。
- **Web アプリケーションの SSO をモバイルユーザーに拡張：**NetIQ Access Manager は、動的な Web ベースのアプリケーションをモバイルユーザーに拡張することができます。NetIQ Access Manager は、Web アプリケーションをセキュアに維持したままアクセスをシンプルにする MobileAccess アプリ (Apple App Store または Google Play) に対応しています。このアプリ内で、企業のミニポータルがユーザーに表示され、アイコンを 1 回タッチするだけで SSO のエクスペリエンスが提供されます。何より重要な点として、管理者は半日でこれらのアプリケーションをポーティングすることができます。
- **簡素化されたポータル：**NetIQ Access Manager のポータルは、各種デバイス (ノートパソコン、タブレット、スマートフォン) からアプリケーションやサービスへのアクセスを容易にすると同時に、管理者による設定も容易にします。またポータル画面は、各種デバイスに応じて表示内容が最適化されます。なお、ポータル画面はカスタマイズが可能で、独自の外観とすることも可能です。
- **顧客のオンボーディング：**NetIQ Access Manager では、ソーシャルメディアの認証情報 (Facebook、Google、Twitter、LinkedIn など) を使用して顧客自身のサインアップとアカウント設定が可能です。また、セルフサービスのオンボーディングとアカウントのメンテナンスプロセスを自動化することもできます。
- **パートナーに対する完全なアクセス管理：**パートナーとのやり取りはデジタル化が進んでいるため、より高度なアクセス管理が必要となります。NetIQ Access Manager の堅牢なフェデレーションは、IdP または SP としてのサービスなど、現在使用されている最新のフェデレーション標準をすべてサポートしているため、パートナーの ID プロバイダーを信頼することができます。モバイルデバイスを使用しているパートナー企業の担当者に安全なアクセスを提供して、ネイティブアプリを使用できるようにすることも、既存の Web ベースアプリケーションを拡張することもできます。

*Decision Analyst, Inc. による調査。2017 年に公開

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-JA0009-003 | O | 05/24 |