opentext™ | Cybersecurity

データシート

NetIQ Advanced Authentication

NetIQ Advanced Authentication は、セキュリティとユーザーエクスペリエンスを必要な認証レベルに合わせて柔軟に調整することを可能にします。大量の ID とパスワード、アクセスバッジの構築、秘密の質問、PIN など、お客様の組織ではすでにセキュリティのためのさまざまな手法が使われていることと思われますが、どれも基本的なアクセスニーズに応えるものです。NetIQ Advanced Authentication のフレームワークを利用すれば、規制や業界やクライアントの要件に対応するために必要な、強力な認証 (MFA または 2 要素認証) を加えることができます。

主なメリット

NetIQ Advanced Authentication by OpenText は、認証を単一のフレームワークに集約し、単一のポリシーコンソールで管理できるようにすることで、コストの削減とセキュリティの向上を実現します。幅広い統合機能と最新の認証方式およびデバイスを提供しているため、環境全体にわたって、適切なシナリオで適切なセキュリティを自由に使用できます。オープンスタンダードをベースとした当社のソリューションにより、セキュリティ侵害から保護すると同時に、ベンダーロックインのリスクからも保護することができます。ニーズに合わせて最適なオプションを選択できます。

認証の柔軟性は、どの方式がサポートされているかということ以上に重要であり、同様にどのプラットフォームがサポートされているかという点も重要です。NetIQ Advanced Authentication は、Windows、OS X、Linux、iOS、Windows Mobile、Android など、非常に幅広いプラットフォームに対応しています。

つまり OpenText™ は、NetIQ Advanced Authentication をお客様の環境に合わせられるようにすることに注力しています。NetIQ Advanced Authentication は、大規模な組織では大規模で複雑な環境に対応できる拡張性を高く評価されており、小規模な組織ではそのシンプルさを高く評価されています。

主な特長

マルチサイトサポート
地理的に分散された、複数の拠点に対応する必要のある組織をサポートします。

マルチテナントサポート
要件が大きく異なる複数の部門や事業部がある場合に、そのような個別の構成をサポートします。

高可用性：冗長性と負荷分散
内部に負荷分散とレプリケーションを含む高可用性設計により、信頼性とパフォーマンスを保証します。

Active Directory Federation Services (ADFS) 向けの NetIQ Advanced Authentication
IT セキュリティチームは、NetIQ Advanced Authentication の ADFS プラグインを使用して、より多くの方式やアプリケーション統合にアクセスを拡張することができます。

FIPS 140-2 採用
National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 規格に準拠した暗号化機能を搭載しているため、安心して導入することができます。

アプライアンス要件

最小構成
- 4 コア
- 8 GB RAM
- 60 GB の空きディスク容量

推奨構成
- 8 コア
- 12 GB RAM
- 100 GB の空きディスク容量

ジオフェンシング
IP ベースの位置情報についてご存知でしょうか。当社は、GPS テクノロジーを使ってこれを新たなレベルに引き上げました。当社のジオフェンシング機能では、ユーザーの特定の場所 (建物やキャンパスなど) に基づいた認証ポリシーを使用できます。

第 2 要素のスキップ
アクセス速度とセキュリティニーズの間でのバランス調整が必要になる場合もあります。認証を行った後に一定の猶予期間を設定し、その間は次の認証を行ったときに第 2 要素が要求されないようにすることができます。ただし、ユーザーは最初の認証のときに完全に認証要件を満たす必要があります。それとは別に、NetIQ Access Manager by OpenText™ のリスクベースの認証エンジンを使用して、2 要素認証が要求されるタイミングを定義することもできます。

モバイル環境のサポート：
オフラインでのログイン
移動中であっても、いつでも必要なときに 2 要素認証を行って個人情報にアクセスできるようになりました。つまり、ユーザーはネットワークに接続しなくても作業を行うことができます。

幅広いプラットフォームのサポート
当社は、さまざまなプラットフォーム (Windows、OS X、Linux、モバイル) でセキュリティを提供することに精通しています。認証についても、iOS、Android、Windows Mobile ベースの方式や、RADIUS、カード、生体認証など、さまざまな方式を使用できます。

標準ベースのアプリケーション統合
当社のソリューションはさまざまな標準規格 (HSPD11、PKI12、OAuth、FIDO、OATH、RADIUS、FIPS 140、NFC ISO/IEC など) に準拠しています。一部の商用ソリューションもサポートしていますが、当社は常に最高の柔軟性を提供することを基本に構築を行っています。

ヘルプデスクモジュール
ヘルプデスクモジュールで利用可能なさまざまな機能により、優れたエンドツーエンドのカスタマーエクスペリエンス (登録、再登録、トークン割り当て緊急パスワードなど) を確保できます。

緊急パスワード
ユーザーが登録した認証方式を利用できないときには、どうしたらよいでしょうか。バックアップとして、ヘルプデスクが緊急パスワードを生成することができます。

外部プロキシ
HTTP プロキシにより、インターネットと認証サーバー間で柔軟なルーティングが提供されます。

非ドメインクライアントのサポート
個人所有デバイス (BYOD) を使用していて、企業ドメインに属していないユーザーもサポートされます。当社では、多要素認証の利用対象は、ドメインメンバーシップが必要な企業デバイスだけに制限されてはいません。

オンプレミス、クラウド、または SaaS
認証フレームワークがポータブルな Docker コンテナとして提供されるため、お客様のニーズに最適な形で環境全体に柔軟に組み込むことができます。Docker 形式のため、クラウド、オンプレミス、または OpenText が提供する SaaS のいずれかを選択できます。どれを選択しても、ご利用のクラウド環境やハイブリッド環境に応じて適切に機能します。Docker プラットフォームはまた、高機能で完成度の高い管理ツールセットを活用できるため、構成やメンテナンスのニーズに最適なプラットフォームともなります。当社の認証フレームワークは as-a-Service としても提供されており、お客様の環境全体に高速かつ強力にパスワードレス認証を組み込むことができます。

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-JA0008-007 | O | 04/24 |