AuthPoint

驚異的に使いやすい多要素認証

ハッカーが最もよく使用する手法は、証明書情報を盗み、それを使用してネットワークリソースに不正アクセスするというものです。*シンプルなパスワードよりもセキュリティレベルの高い認証を追加で要求する多要素認証は、企業のビジネスを守るための最も重要なセーフガードとなります。

WatchGuard独自の多要素認証(MFA)ソリューションは、証明書情報が脆弱であったり盗難されたりすることで発生するネットワークからの遮断やデータへの不正アクセスを減らすだけでなく、この重要な機能をクラウドから提供する事で簡単にセットアップおよび管理を行うことができます。さらに、AuthPointでは、モバイルデバイスDNAなど、従来の二要素認証(2FA)を上回る革新的な方法でユーザを識別します。サードパーティとの統合により大規模なエコシステムが構築されています。これは、ネットワーク、VPN、クラウドアプリケーションなど、必要であればどこにでも強力な保護を一貫して展開できるということを意味しています。使い勝手のAuthPointモバイルアプリは、技術的な知識のないユーザであっても簡単に利用できます。総括すると、WatchGuard AuthPointは、サイバー攻撃を阻止するための正しいタイミングで多要素認証を実現するソリューションです。

モバイルデバイスDNAによる効果的なMFA保護

多要素認証では、特定の個人に関連付けられる要素だけでなく、その人が把握している情報(ユーザ名とパスワード)や、所持品に関する情報を提供する必要があります。AuthPointは、プッシュメッセージ、QRコード、またはワンタイムパスワード(OTP)を使用して、安全性の高いMFA製品を提供します。システムおよびアプリケーションへのアクセスを許可する際には、モバイルデバイスDNAが、認証済みユーザのスマートフォンとのマッチングを行います。そのため、攻撃者がユーザのデバイスを複製してシステムにアクセスしようとしても、デバイスDNAが異なるため、アクセスはブロックされます。

使いやすいAuthPointモバイルアプリ

WatchGuardのAuthPointアプリでは、ユーザは自分のスマートフォンから認証を受けることができます。キーフォブやサムドライブを持ち運ぶ必要はありません。その代わりに、スマートフォン上でAuthPointアプリをインストールしてアクティブ化します。この操作はわずか数秒で行えます。次に、アプリを使用して認証します。こうして、スピーディなプッシュベースの認証と、携帯電話のカメラでQRコードを使用したオフライン認証が可能になります。このアプリは11か国語で利用でき、AppStoreとGoogle Playから無料でダウンロードできます。

Web SSOによる広範なカバレッジ

WatchGuardのエコシステムでは、数多くのサードパーティがAuthPointと統合されています。これによって、企業は機密性の高いクラウドアプリケーション、VPN、および企業ネットワークにアクセスする前にユーザに認証を要求することができます。AuthPointはSAML標準をサポートしており、ユーザが一度ログインすれば、あらゆる種類のアプリケーションやサービスへのアクセスが可能となります。さらに、安全なログイン機能により、AuthPointアプリケーションを使用したWindowsおよびMacマシンへのオンラインおよびオフライン認証が可能です。

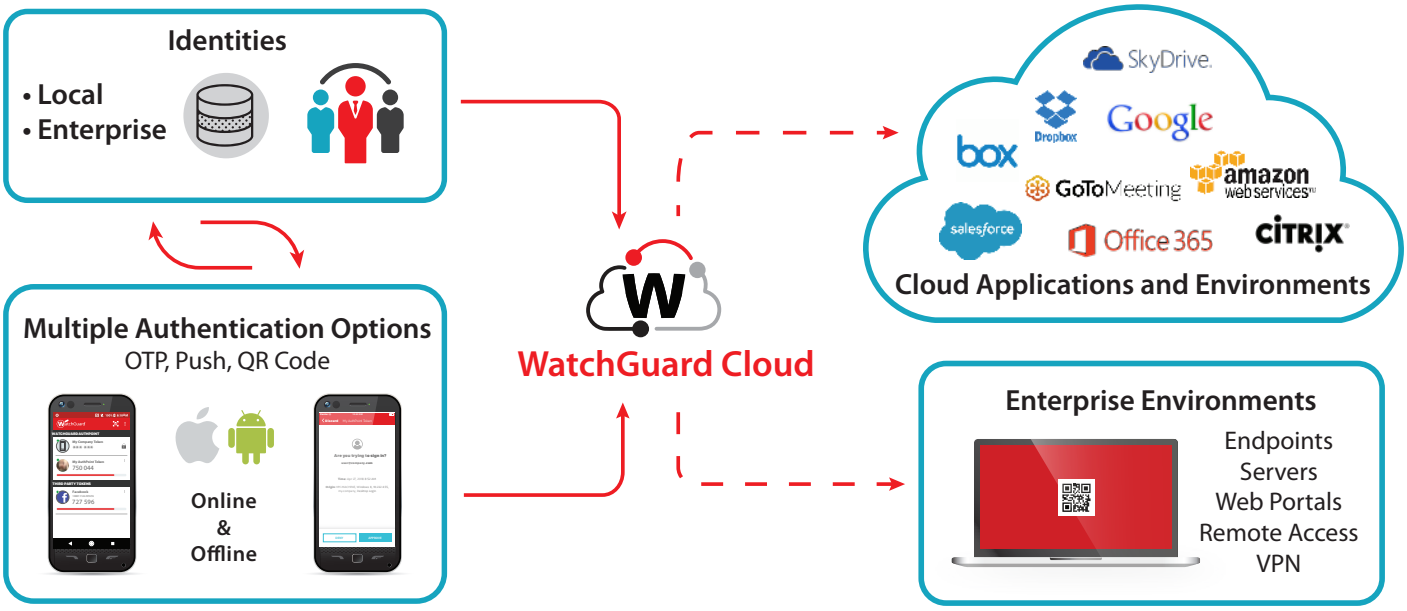
管理負荷を軽減したクラウドベースサービス

IT管理者とセキュリティ担当者などのリソースが限られている企業にとってMFA保護は、クラウドから簡単に導入・展開および管理ができるというメリットがあります。AuthPointはWatchGuardクラウドプラットフォーム上で動作し、どこからでも利用可能です。ソフトウェアをインストールしたり、アップグレードをスケジュールしたり、パッチの管理は不要です。さらに、プラットフォームは単一のグローバルアカウントビューや、多くの独立したアカウントにも簡単に対応できるため、分散した企業やマネージドサービスプロバイダは、役割に応じて、必要な情報だけを表示する事が可能です。

**Verizon Data Breach Investigations Report 2018*

ウォッチガード・テクノロジージャパン株式会社: TEL: 03.5797.7205 FAX: 03.5797.7207 ウェブ: www.watchguard.co.jp 〒106-0041 東京都港区麻布台 1-11-9BPR プレイス神谷町 5 階

ネットワーク、VPN、クラウドリソース、その他多くのものを不正アクセスから守ります



WatchGuard Cloudプラットフォーム

- 100%クラウドベース管理
- 認証アプリの割り振りとアクティベーション
- グループとリソースに基づいた認証ポリシー
- ログとレポート
- ロールベースのアクセス
- 直観的で魅力的なユーザインターフェース

AuthPointモバイルアプリ

- 3つの認証方式が1つに:
  1.プッシュメッセージ
  2.ワンタイムパスワード
  3.オフライン時のQRコード
- モバイル認証 – 追加のハードウェアは不要
- 11か国語対応
- マルチトークンサポート
- iOSおよびAndroidに対応 – 無料ダウンロード
- PIN/生体認証保護(一部のデバイス)
- モバイルデバイスDNA – 新たな認証要素
- 新しいデバイスへのセルフサービスでのモバイルトークンの移行

AuthPointゲートウェイ

- 企業ネットワークゲートウェイ
- ADおよびLDAPユーザ認証および同期
- RADIUSプロキシ

AuthPointエージェント

- ネイティブMFAサポートを必要としないサードパーティアプリケーションとの統合
- WindowsとmacOSでのコンピュータログイン保護

AuthPointエコシステム

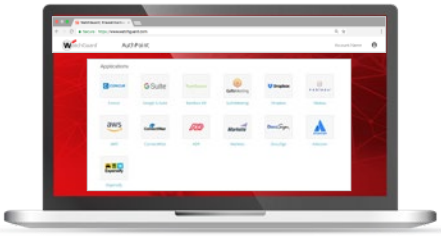
- クラウドリソース、アプリケーション、データベース、およびWebリソースへのMFAの追加
- SAMLおよびRADIUS標準のサポート
- 多くの一般的なサードパーティソリューションの包括的な統合ガイド

推奨されるユースケース

VPN/リモートアクセス

ユーザエクスペリエンスはユーザ名+パスワードと同じですが、安全性がより高く、ワンクリックで確認できます。

1. ユーザ名とパスワードで接続を要求
2. VPN接続の確認(AuthPointアプリから要求)



クラウドアプリケーション – Web SSO

1. IDポータル(IdP)にアクセス
2. OTP、プッシュまたはQRコードを使用して認証
3. 権利を持つすべてのアプリにアクセス
   (再認証は不要)

PCログイン – オンライン認証

1. [Send push (プッシュの送信)]をクリック
2. AuthPointアプリからPCログイン要求を確認
3. ログインが実行

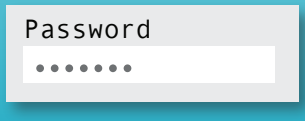
PCログイン – オフライン認証

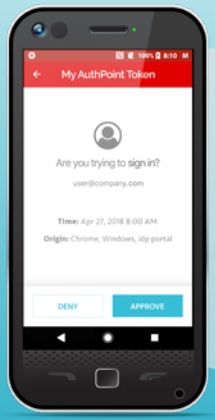
1. [QR code (QRコード)]を選択して認証
2. AuthPointアプリを使用してQRコードをスキャン
3. この例では、応答717960を入力

多要素認証(MFA)とは?

以下より2つ以上の認証要素を使用:

- **ユーザが把握している情報**
  (パスワード、PIN)
- **ユーザが所持するデバイス**
  (トークン、携帯電話)
- **ユーザの生体認証**
  (指紋、顔)





AuthPoint要素:

1.パスワード

2. モバイル認証
   アプリでの承認
3. 正しいモバイルデバイスDNA
4. アクセスのための指紋認証
   (一部のデバイス)

AuthPointは、従業員やIT管理者の使いやすさを損なうことなく、貧弱なパスワードに起因するビジネスリスクを軽減するMFAを実現します。

すべてがクラウドサービスから提供されるため、ハードウェアのインストールやソフトウェアのメンテナンスは不要。多要素認証(MFA)は重要な中心的保護手段と見なされており、WatchGuardによって簡単に導入できます。

Tom Ruffolo
eSecurity Solutions CEO

MFAを推奨する理由

データへの不正アクセスに関連した直接的および間接的な出費により、セキュリティコストが増える可能性があります。たとえば、企業内で不正アクセスが発見されると、規制による罰金や訴訟の費用などの支払いが生じる可能性があります。それに加え、専門家による不正アクセスの原因調査や、障害に対処するための新たなセキュリティ対策が必要となることもあります。そうした対策を講じたとしても、従業員の生産性が低下したり、現在および将来の顧客を失うことにより、それより大きな間接的コストが生じるかもしれません。Ponemon Instituteの調査[1]では、機密データを含む**データレコードあたりのデータへの不正アクセスの平均コストを約1万5千円**として計算し、数字を算出しました。平均データ不正アクセス数を9,350レコードとすると、コストは1億4千万円となります。

弱いパスワードまたは共有パスワードによって不正アクセスを経験する可能性はどのくらいあるでしょうか?調査結果によると、100人中3人[2]が弱いパスワード"123456"を使用しており、**100人中6人がすべてのオンラインアカウントで同じパスワードを使用しています。**そこで、パスワードの管理に問題がある従業員が社内に1人以上いる可能性について検討してみる必要があります。Payment Card Industry Data Security Standard (PCI-DSS) v 3.2への追加など、準拠企業のユーザの少なくとも一部に対して二要素認証(2FA)または多要素認証(MFA)を求めている規制機関が増えているのは、このような理由なのかもしれません。

そこで、リーズナブルな費用で実現可能なクラウドベースの多要素認証により、こうしたリスクを軽減することが可能です。追加のインフラストラクチャ、ハードウェアトークン、ソフトウェアのサポートやメンテナンスのための費用は一切かかりません。**1ユーザ1か月あたり約190円(参考価格)**で、不正アクセスによって生じる可能性のある上述の1億4千万円の出費を回避することができます。

1 2017 Ponemon Institute Cost of Data Breach Studyおよび2017 Ponemon State of SMB Cybersecurity Report

2 http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

3 https://www.statista.com/statistics/763091/us-use-of-same-online-passwords

WATCHGUARDセキュリティポートフォリオ

ネットワークセキュリティ

エンタープライズグレードのセキュリティを提供するだけでなく、WatchGuardのプラットフォームは、容易な導入と運用、継続的な管理に焦点を当てて設計されているので、WatchGuardは世界中の中堅・中小企業、および分散型エンタープライズにとって理想的なソリューションです。

Secure Wi-Fi

煩わしい管理をなくし、大幅にコストを削減し、Wi-Fi環境に安全で保護された空間を提供するように設計されたWatchGuardのSecure Wi-Fiソリューションは、今日の無線LAN市場に真の変革をもたらします。広範なエンゲージメントツールとビジネスアナリティクスの可視性により、ビジネスの成功に必要な競争優位性を実現します。

多要素認証

WatchGuard AuthPoint™は、使いやすいクラウドプラットフォーム上で多要素認証を提供し、セキュリティを強化する最適なソリューションです。WatchGuardの独自のアプローチにより「モバイルデバイスDNA」による識別が付加されています。これは、正しく認識された人だけが機密ネットワークとクラウドアプリケーションにアクセスできるようにする識別要素です。

詳細

詳細については、お近くのWatchGuard販売代理店までお問い合わせになるか、**https://www.watchguard.co.jp**をご確認ください。

WatchGuardについて

WatchGuard® Technologies, Inc.は、ネットワークセキュリティ、セキュアなWi-Fi、ネットワークインテリジェンス製品やサービスを世界各国の80,000以上のお客様に提供している業界のグローバルリーダーです。当社のミッションは、WatchGuardのシンプルかつ理想的なソリューションを分散型企業や中堅・中小企業に提供し、あらゆる業種と規模の企業でエンタープライズグレードのセキュリティ対策を可能にすることです。WatchGuardは米国ワシントン州シアトルに本社を置き、北米、ヨーロッパ、アジア太平洋、南米に支社を展開しています。詳細については、**WatchGuard.co.jp**をご覧ください。