DATASHEET

AUTHPOINT

強力な多要素認証（MFA）を容易に導入

パスワードだけでは不十分

毎日のようにサイバー犯罪者は盗んだパスワードを使用して、システムへ不正にアクセスしたり、システムを感染させたり、企業情報を盗んだりしています。これらに対抗するための最も効果的な方法は、認証時にユーザー名とパスワードに加え、他のさらなる本人確認を求めることです。これは、企業規模にかかわらず、すべての企業で確実な認証を展開する必要があります。

MFAにより、なりすましを阻止

WatchGuard AuthPoint™はこうした時代に合ったソリューションであり、使いやすいクラウドプラットフォームでの多要素認証によって、セキュリティ上の脆弱性に対処します。AuthPointモバイルアプリは、ログインが試みられるたびにシンプルなプッシュ通知で表示するので、ユーザはすぐにスマートフォンからアクセスを承認したりブロックしたりすることが可能です。WatchGuard独自のアプローチとして、「モバイルデバイスDNA」が識別要素として追加されます。これにより、適切な人物にのみ機密ネットワークやクラウドアプリケーションへのアクセスを承認するという運用をより厳格にできます。

直感的なクラウド管理

これまでMFAは、多くの企業では、導入が難しいものでした。統合が複雑で、オンプレミス管理に手間がかかるため、大勢のIT管理者と多額の初期費用がないと実装できないからです。一方、WatchGuardのAuthPointソリューションはクラウドサービスであるため、高価なハードウェアを必要とせずに、WatchGuard Cloudの直感的なインターフェースを使ってどこからでも管理できます。また、WatchGuardのエコシステムでは、多数のサードパーティアプリケーションとの統合が可能です。機密性の高いクラウドアプリケーション、Webサービス、VPN、ネットワークへのアクセスにMFA保護を幅広く確実に適用できます。AuthPointユーザーは1度のサインインだけで複数のアプリケーションにアクセスでき、FacebookやGoogle Authenticatorなどのサードパーティの認証システムを容易にモバイルアプリに追加することも可能です。

> *安全でないパスワードは世界中のサイバー攻撃の81%で悪用されており、全体の61%の攻撃は従業員が1000人以下の企業を標的としたものです。*
>
> *ベライゾン2017年版データ漏洩/侵害調査報告書*

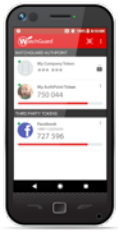
アプリを使った3つの認証方法

プッシュベースの認証

ワンタッチでセキュアな認証を完了します。認証しようとしているユーザーと場所を確認して、リソースへの不正なアクセスをブロックできます。

QRコードベースの認証

アプリでしか読み取ることのできないチャレンジ（鍵）が含まれた暗号化されたQRコードを、カメラを使って読み取ります。レスポンスが入力されると、認証が完了します。



時間ベースのワンタイムパスワード（OTP）

表示される動的な時間ベースのワンタイムパスワードを取得して、それをログイン時に入力します。

機能とメリット

- オンライン（プッシュ）およびオフライン（QRコードとOTP）認証
- 総保有コストの低いクラウドサービス
- 強力な本人確認を実現するモバイルデバイスDNAチェック
- 軽量で全機能を備えたモバイルアプリ（11の言語で利用可能）
- VPN、クラウド、PCログインすべてに対応
- Webシングルサインオン（SSO）ポータル
- 統合ガイドを使って、VPN、クラウドアプリ、Webサービスを簡単に保護

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

WatchGuard Technologies, Inc.

DATASHEET

AuthPointモバイルアプリ

認証機能

- プッシュベースの認証（オンライン）
- QRコードベースの認証（オフライン）
- 時間ベースのワンタイムパスワード（オフライン）

セキュリティ機能

- モバイルデバイスDNA
- 動的なキー生成によるオンラインアクティベーション
- PIN、指紋、顔認証（iPhone X）による認証システムへのアクセス
- 別のデバイスへのセルフサービスかつセキュアな認証システムの移行
- ジェイルブレイクとルート検出

便利な機能

- マルチトークンサポート
- サードパーティのソーシャルメディアトークンのサポート
- カスタムトークンの名前と画像

対応するプラットフォーム

- Android v4.4以上
- iOS v9.0以上

対応する言語

- 英語、スペイン語、ポルトガル語、ドイツ語、オランダ語、フランス語、イタリア語、日本語、中国語（簡体字および繁体字）、韓国語、タイ語

標準規格

- OATH Time-Based One-Time Password Algorithm (TOTP) – RFC 6238
- OATH Challenge-Response Algorithms (OCRA) – RFC 6287
- OATH Dynamic Symmetric Key Provisioning Protocol (DSKPP) – RFC 6063

AuthPointサービス

対応する用途

- Web SSOによるクラウドベース認証
- リモートアクセスおよびVPN認証
- Windowsログオン保護（オンライン/オフライン）
- MacOSログオン保護（オンライン/オフライン）
- Linuxログオン保護

管理機能

- WatchGuardクラウドプラットフォーム
- Active DirectoryおよびLDAPユーザーの同期と認証
- 監視およびレポート作成のウィジェットを含むダッシュボード
- ユーザーのグループごとのアクセスポリシー
- 構成可能な認証リソース
- 統合ガイドを使った簡単な展開
- ログとレポート

AUTHPOINTゲートウェイ

- ネットワークからWatchGuard Cloudへのセキュアな接続
- MS-ADおよびLDAPの同期
- RADIUSサーバー

AUTHPOINTエージェント

- Windowsログオン
- MacOSログオン
- ADFS

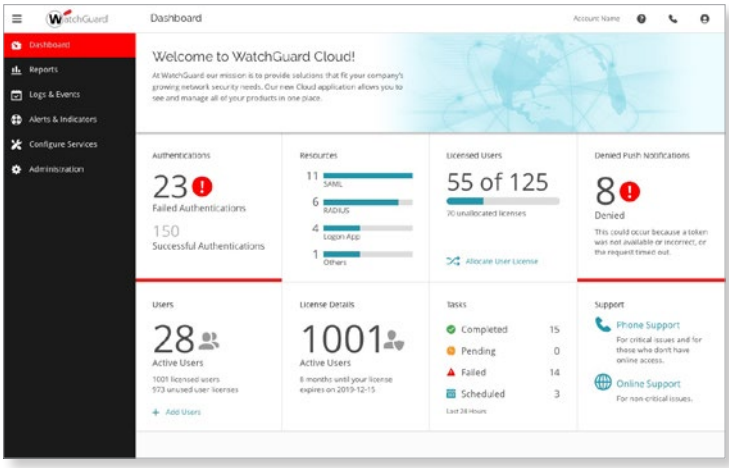
標準規格

- RADIUS
- SAML 2.0 IdP

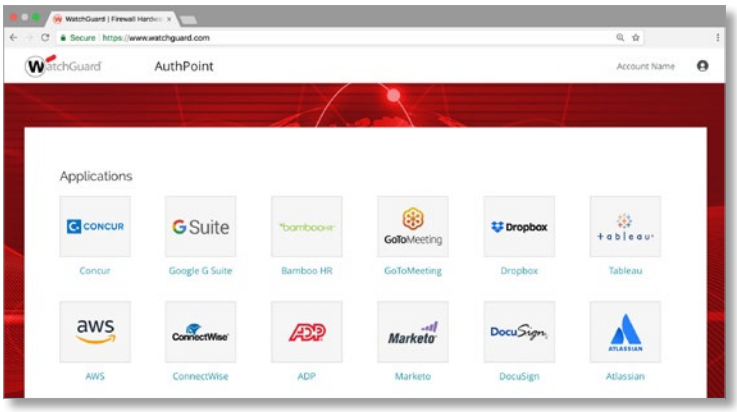
統合（完全な一覧についてはWATCHGUARDのウェブサイトを参照）

- Microsoft Office 365、G-Suite、WatchGuard Firebox、Dropbox、Go-to-Meeting、Open VPN

AuthPointモバイルアプリ



WatchGuard Cloud管理



統合とSSO

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

Secure Wi-Fi

多要素認証

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、**www.watchguard.co.jp**をご覧ください。

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