DATASHEET

WatchGuard Zero Trust Bundle

境界のないセキュリティ

場所やデバイスを問わず、常時ユーザーを保護

今日のビジネスパーソンは、自宅、オフィス、空港、公共Wi-Fiが利用できるエリアなど、あらゆる場所からネットに接続しています。毎回接続が確立されるたびに、攻撃者が脆弱な認証情報、感染デバイス、またはセキュリティ上欠陥があるアプリケーションを悪用する機会が生まれます。WatchGuard Zero Trust Bundleは、ユーザーがどこで働いていても、デバイスとともに保護します。

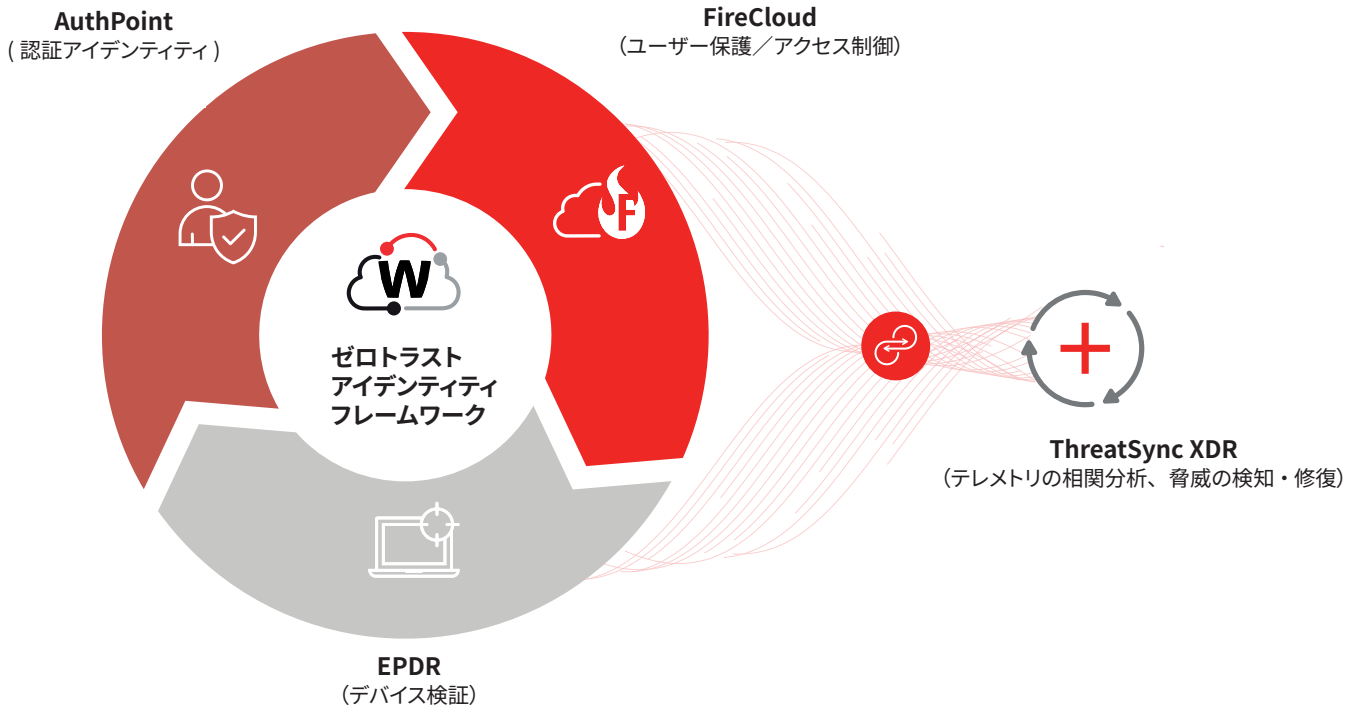
WatchGuard Zero Trust Bundleでできること:

1. **信頼性を確保**するために、新規セッションごとにアクセス権を付与する前に、すべてのユーザーとデバイスを確認
2. ユーザーがどこから接続しても、**インターネット上の脅威から保護**し、ユーザーの活動やリスクを可視化
3. ゼロトラストネットワークアクセス（ZTNA）を活用し、オンプレミスのアプリケーションやデータに対する**攻撃や水平方向の移動を防止**

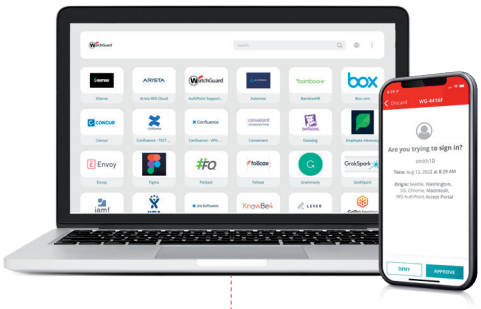
クラウド上で管理・導入

WatchGuard Zero Trust Bundle は、100% クラウド管理型であるため、ソフトウェアのメンテナンスやハードウェアの導入は不要です。管理者は、WatchGuard Cloud の統一コンソールから、ゼロトラストポリシーの定義、エンドポイントエージェントの導入、認証トークンの管理をすべて行えます。主要なツールやマルチテナント管理機能が組込まれており、組織やマネージドサービスプロバイダーは迅速に運用を開始し、容易に拡張することができます。

> アイデンティティ、デバイス、ネットワークにわたる継続的な検証

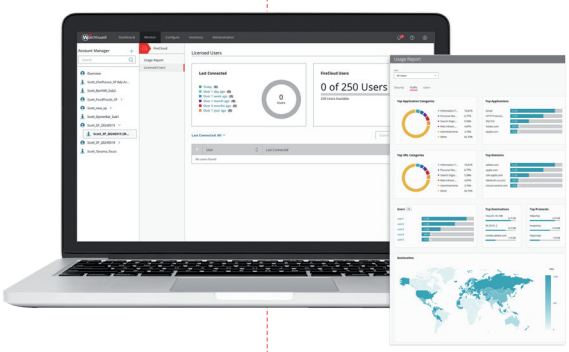


WatchGuard Zero Trust Bundle に含まれるもの



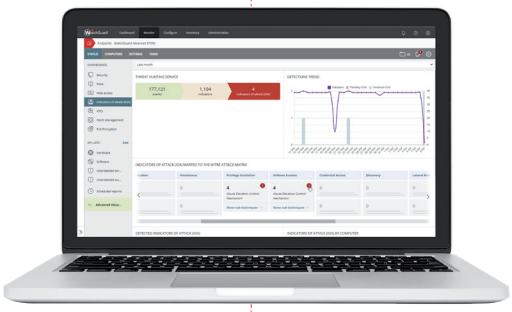
> ダークウェブ上の認証情報モニタリング機能を備えた多要素認証

認証情報の盗難やアカウントの不正利用が増加する中、本人確認はゼロトラストの基盤となります。AuthPoint は、多要素認証、シングルサインオン、およびコンテキストに基づいてすべてのユーザーを検証するリスクベースのポリシーを提供します。統合されたダークウェブ認証情報モニタリング機能により、攻撃者が悪用する前に、流出している認証情報を事前に検知します。AuthPoint は、適切な人物が、適切な認証要素を用いて、適切なタイミングでアクセスできるようにします。



> ハイブリッド型ネットワークセキュリティとゼロトラストネットワークアクセス

FireCloud Total Access は、安全なインターネットアクセスとゼロトラストネットワークアクセスを 1 つのクラウドサービスに統合しています。SaaS やプライベートアプリへの接続において、VPN に代わってセッション単位のアイデンティティベースの接続を提供します。Firewall as a Service（FaaS）と Secure Web Gateway は、あらゆるネットワーク上でフィッシングやマルウェアをブロックします。ゼロトラストポリシーにより、アクセス許可を与える前にユーザーとデバイスの認証が行われます。グローバル PoP は、セッションを高速かつ暗号化された状態で維持し、攻撃者からは検知されません。



> 高度なエンドポイントセキュリティ

ウォッチガードのエンドポイントセキュリティの AI エンジンは、すべてのプロセスを監視・分類し、未知または悪意のある活動を自動的にブロックします。ゼロトラストアプリケーションサービスは、ゼロデイ攻撃やインメモリ攻撃を防止します。継続的なセキュリティチェックにより、各デバイスがセキュリティポリシーを満たしていることを確認した上でアクセスを許可します。信頼され、ポリシーに準拠したエンドポイントのみが接続可能になります。

WatchGuard Cloud

AuthPointモバイルアプリ

認証機能

プッシュ通知による認証（オンライン）

QRコードによる認証（オンラインおよびオフライン）

時間制限によるワンタイムパスワード（オンラインおよびオフライン）

セキュリティ機能

デバイスDNA署名

動的鍵生成によるオンラインアクティベーション

各種の認証方法に対応
- PIN
- 指紋認証（Samsung/Apple）
- 顔認証（Apple）

別のデバイスへのセルフサービスによる安全な認証方法への移行

ジェイルブレイクおよびルート化検知

利便性機能

マルチトークン対応

サードパーティ製ソーシャルメディアトークン対応

カスタマイズ可能なトークン名と画像

標準仕様

OATH時間制限によるワンタイムパスワードアルゴリズム（TOTP）– RFC 6238

OATHチャレンジレスポンスアルゴリズム（OCRA）– RFC 6287

OATHダイナミック対称鍵プロビジョニングプロトコル（DSKPP）– RFC 6063

エンドポイント検知／レスポンス

対応OS

Windows：ワークステーション - XP、Vista、7、8、8.1、10。サーバー - 2003 SP2以降、2008、2008 R2、SBS 2011、2012、2012 R2、2016、2019、Server Core 2008、2008 R2、2016、2019

Linux：Red Hat Enterprise 6.0以降、Debian Squeeze、Ubuntu 12以降、OpenSUSE 12以降、SUSE Enterprise Server 11 SP2以降、CentOS 6.x以降

macOS：10.6 Snow Leopard、10.7 Lion、10.8 Mountain Lion、10.9 Mavericks、10.10 Yosemite、10.11 El Capitan、Sierra

検知手法

汎用シグネチャおよびヒューリスティック

Collective Intelligenceへのクラウドベースの照会

IoA検知

ファイアウォール、IDS/IPS

改ざん防止

デバイス制御

エンドポイントのアクティビティ監視およびEDR機能の例：

コンテキストに応じた行動検知

インメモリ型不正対策

ダークウェブ上の認証情報モニタリング

検知手法

継続的な認証情報監視

ユーザーアカウントごとの侵害された認証情報の相関分析

検知された各侵害イベントをコンテキストと共に記録

FireCloud

対応OS

Windows 7、8、10

ゲートウェイ：Hyper-V（Windows Server 2022/2025）、VMware ESXi 7.0/8.0、Proxmox 8.4/9.0

検知手法

フィッシング攻撃のブロック

C2接続の防止

コンテンツフィルタリング

即時のセキュリティ意識向上トレーニングの実施

認証対応

AuthPoint
SAML：サードパーティIDP、Entra ID、Okta、FIDO

WatchGuard Cloud Directory：Active Directory、Entri ID、Cloud Directory

セッションレベルのアイデンティティ検証：Unified Zero Trust

管理・導入

管理：設定、ポリシーテンプレート、マルチテナントサービスプロバイダー機能向けのWatchGuard Cloud一元コンソール

PoP：5大陸にまたがるグローバルネットワーク

> 仕組み

認証 > 検証 > 適用

- **AuthPoint**：新しいセッションごとにユーザーの身元を確認し、リスクを評価します。
- **エンドポイントセキュリティ**：デバイスの状態とコンプライアンスをリアルタイムでチェックします。
- **FireCloud**：ゼロトラストポリシーを適用し、Web、SaaS、プライベートアプリへのアクセスを管理します。
- **ゼロトラストアイデンティティフレームワーク**：ID、デバイス、アクセス検証を 1 つの連続したプロセスに統合します。
- **ThreatSync XDR**：すべてのアクティビティを相関分析し、継続可視化、検知、自動レスポンスを実現します。
- **WatchGuard Cloud**：すべてのサービスを統合管理し、単一のマルチテナントコンソールを通じて、ポリシーの作成、導入、レポート作成を簡素化します。

WatchGuard Zero Trust Bundleについて

詳細は、ウォッチガードの認定販売代理店にお問い合わせいただくか、
www.watchguard.co.jpをご覧ください。

ウォッチガードについて

WatchGuard® Technologies は、主にマネージドサービスプロバイダー向けに設計された統合型サイバーセキュリティ分野におけるグローバルリーダーです。Unified Security Platform® を通じて「現実世界のための真のセキュリティ」を提供します。ネットワーク、エンドポイント、アイデンティティを AI およびゼロトラスト技術と統合し、拡張性に優れた強力なプロテクションを実現します。25 万社以上の企業を保護する 1 万 7,000 社以上の販売代理店やマネージドサービスプロバイダーに利用されており、パートナーがベンダーやコンソールの追加、および複雑さを増すことなく、急成長、運用負担の解消、堅実な成果を上げられるよう支援しています。ワシントン州シアトルに本社を置き、世界中にオフィスを展開しています。詳細は https://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 1-11-9 BPR プレイス神谷町 5 階
TEL：03-5797-7205　Email：jpnsales@watchguard.com　www.watchguard.co.jp

　作成日：2026 年 3 月