DATASHEET

WatchGuard CloudDR（クラウド検知／レスポンス）

インシデントが発生する前にクラウドのリスクを事前に把握

セキュリティ侵害は、ハッカーによる侵入だけではありません。例えば、存在すら知らなかった環境、意図せずに開放されたままになっていた設定、あるいは盗まれたり悪用されたりした信頼できるアカウントなどにも原因があります。Microsoft 365、Google Workspace、Salesforce、およびその他のAIやSaaSなど多様なアプリケーションは、現在、認証情報の盗難、設定ミスやシャドーITの悪用における主な標的となっています。従来のエンドポイントおよびネットワークセキュリティツールでは、アクセスが許可された後にこれらの環境内で何が起きているのかを見通すことができません。

WatchGuard CloudDR™ により、隠れたクラウドアプリを継続的に検知し、リスクの高い設定を制限し、IDの不正利用を阻止することで、攻撃者が最も容易に攻撃を仕掛けられる経路を断ち切ることができます。SaaSおよびクラウド環境全体にわたって継続的な可視化、検知、自動レスポンスを実現するAIネイティブかつエージェントレスのプラットフォームとして、お客様とエンドユーザーを保護します。

保護対象

IDの悪用

認証情報の盗難、セッショントークンの悪用、多要素認証（MFA）の迂回、および休眠状態の特権アカウントの放置など、正当なアクセス手段がセキュリティ侵害へとつながります。

設定ミス

デフォルト設定、過度に緩い共有設定、および構成ドリフトは、攻撃者が高度なハッキング技術を必要とせずに悪用できる容易な侵入経路を生み出します。

シャドーITとAI

従業員が許可されていないアプリやAIツールに接続することで、IT部門が把握できないデータの漏洩やサプライチェーン上のリスクが生じます。

仕組み

1つの統合プラットフォームで可視化 + 検知 + レスポンスを実現

WatchGuard CloudDRは、エージェントレスの強固なAPI接続を活用し、SaaSプラットフォームと直接連携します。ソフトウェアのインストールやエージェントの実装は不要であり、エンドユーザーのデバイスのパフォーマンスに影響を与えることもありません。接続が完了すると、設定を継続的に評価し、アクティビティを監視するとともに、セキュリティのベストプラクティスを自動的に適用します。

シャドーITの発見

組織全体にわたるすべてのクラウドアプリケーションおよびOAuth接続の連携（AIツールを含む）を発見します。リスクを伴うアプリを特定し、アプリケーションの利用ポリシーを適用します。

アイデンティティ脅威検知／レスポンス（ITDR）

SaaSプラットフォーム全体におけるユーザーおよびアカウントの行動を監視します。侵害されたアカウント、多要素認証（MFA）の迂回、不自然な移動経路、不審な活動を検知します。リアルタイムで自動的にアクセス権を無効化したり、制御措置を適用します。

SaaSポスチャー管理

セキュリティのベストプラクティスに照らして、クラウドアプリケーションの設定を継続的に監視します。リスクの高い設定、権限の過剰な共有、構成ドリフトを検知し、自動的に是正します。

コンプライアンスの可視化

CIS Controls、NIST CSF、SOC 2に準拠した、あらかじめ設定済みの多くのポリシーが用意されています。組み込みのレポート機能により、手作業による集計を必要とせずに、監査対応のエビデンスを提供します。

標準搭載の自動修正機能

すべての環境にわたる一括修正により、手動による確認作業が不要になります。数週間後の定期監査で問題が発見されるのではなく継続的に修正されます。

マルチテナントMSPコンソール

すべての顧客環境を単一の画面で一元管理できます。拡張性を考慮して設計されており、1つのプラットフォームから、各クライアントに対してポリシーの標準化、リスクの監視、およびセキュリティ機能を提供することができます。

DATASHEET

WatchGuard CloudDRの特長

01 包括的に保護

他のソリューションは、問題の一部にしか対処できません。WatchGuard CloudDRは、シャドーIT、設定ミス、アイデンティティの脅威を包括的にカバーし、ツールの乱立、情報の分散、運用上の複雑さを解消します。

02 設計段階から実用性を重視

単なるアラートにとどまらず、WatchGuard CloudDRは何が問題なのか、なぜそれが重要なのか、そしてどのように解決すべきかといった、明確で実用的な知見を提供します。さらに、一括修復および自動化機能が標準で搭載されています。

03 最先端のアーキテクチャ

ワークフローはエンタープライズ向け製品から流用されたものではなく、すぐに使える仕様となっています。ウォッチガードの他のセキュリティサービスと組み合わせて容易に管理でき、包括的かつ手頃な価格のソリューションを実現しています。

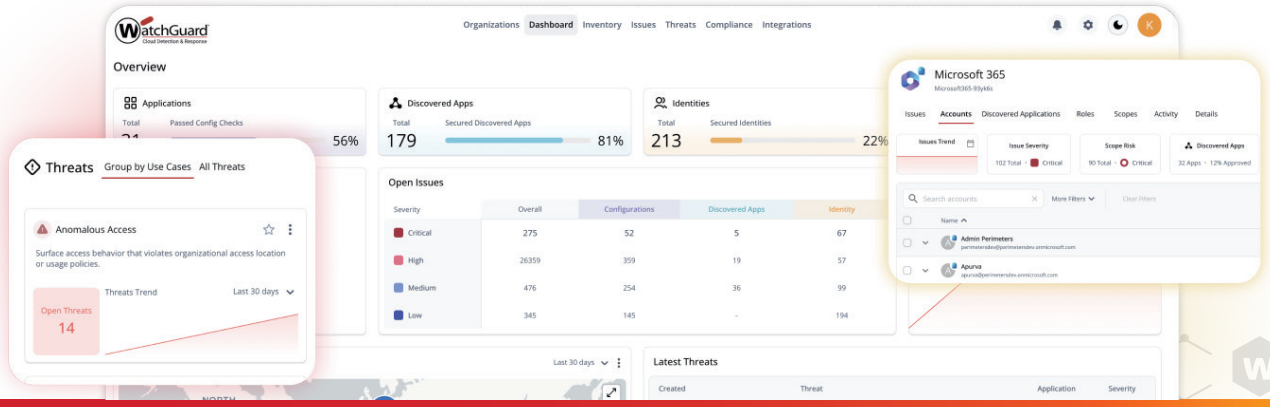
04 エージェントレスで導入

ソフトウェアのインストールは不要であり、パフォーマンスへの影響もありません。WatchGuard CloudDRはSaaS APIに直接接続され、通常、顧客のシステム環境全体への導入は数分で完了し、即座に効果を実感することができます。

サポートしているクラウドアプリケーション

WatchGuard CloudDRは40以上のアプリケーションをサポートしており、進化し続けるクラウドアプリ環境に対応するため、新たな連携機能が継続的に追加されています。対応アプリケーションには以下が含まれます：

- Atlassian Guard
- Atlassian Jira
- BambooHR
- Bitbucket
- Box
- Confluence
- Datadog
- Docusign
- Dropbox
- Duo
- Email
- EntraID
- Github
- Gitlab
- Google Workspace
- HiBob (Coming Soon)
- Hubspot
- Jamf
- Jumpcloud
- Microsoft 365
- Microsoft Intune
- Monday.com
- MongoDB
- Okta
- OneLogin
- OpenAI
- Salesforce
- Sentry
- Service Now
- SharePoint
- Slack
- Teams
- Trello
- Webhook
- Zendesk
- Zoom



シンプルかつ低コストでクラウド環境を包括的に保護します。

ウォッチガードについて

WatchGuard　Technologiesは、統合型サイバーセキュリティ分野における世界的なリーダーです。30年以上にわたり、包括的なセキュリティ対策の実現方法を確立し、脅威情勢のあらゆる大きな変化に先んじるべく、絶えず革新を続けてきました。AIを活用したUnified Security Platform®（統合型セキュリティプラットフォーム）は、ゼロトラストに準拠したネットワーク、エンドポイント、アイデンティティの保護機能を単一の統合プラットフォーム上で提供しています。運用の複雑さを軽減するとともに、セキュリティ効果を向上させ、ビジネスの効率的な成長を支援しており、世界中で150万社以上の顧客に利用されています。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6月