DATASHEET

WATCHGUARD ADVANCED REPORTING TOOL（高機能レポーティングツール）

実用的なIT／セキュリティインテリジェンス

セキュリティ体制を積極的に強化

組織が扱うセキュリティに関するデータは増加しており、IT部門は知っておくべき重要情報の選別に苦慮しているのが現状です。こうした重要情報は、外部要因や社内の人間に起因するセキュリティの課題や情報漏えいの検知に役立てることができます。

セキュリティの責任者は膨大なデータ量に辟易しています。取り扱う情報の過多や、次世代型のマルウェアの出現は、本当に必要な情報を見過ごしたり、対策されないケースを生み出したりする場合があり、結果的にシステム全体のセキュリティに悪影響を及ぼしてしまいます。

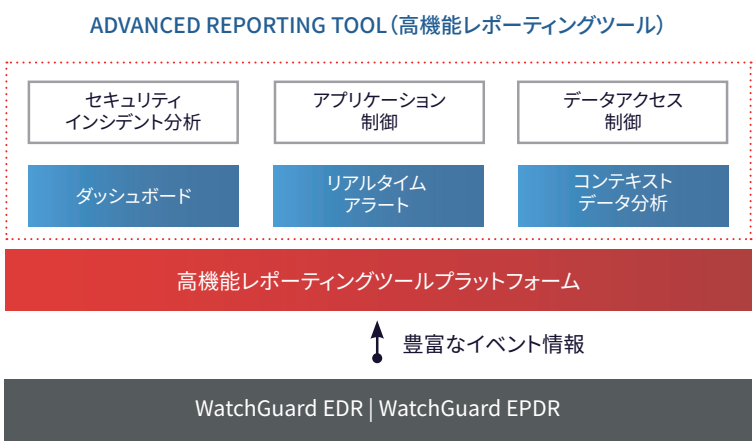
WATCHGUARD ADVANCED REPORTING TOOL（高機能レポーティングツール）

Advanced Reporting Tool（APT）（高機能レポーティングツール）プラットフォームは、新たなインフラや設備、あるいは保守を不要とし、WatchGuard EPDRやWatchGuard EDRを活用してエンドポイントから抽出された、プロセスの実行やコンテキストより生成された情報の保存と相関分析を自動化します。

生成された情報を元に、**Advanced Reporting Tool（高機能レポーティングツール）**は、自動的にセキュリティインテリジェンスを生成し、組織は発生元を問わず攻撃や異常な振舞いをピンポイントで特定し、企業ネットワークやシステムの社内における誤使用も検知することができます。

Advanced Reporting Tool（高機能レポーティングツール）は、以下のように、データを検索、探求、分析し、ITやセキュリティに関する知見を提供します：

- セキュリティインシデントの発生元を判断し、セキュリティ対策を施すことで将来的な攻撃を防止します。
- 特に重要な業務情報に対するアクセスポリシーを、さらに厳格化します。
- 業務や従業員のパフォーマンスに影響を与えるような、企業リソースの誤用を監視・制御します。
- 企業の利用ポリシーを遵守していない従業員の振舞いを是正します。



主な特長

機密情報へのアクセス

- あらゆるデバイスに関する全ての情報を最大限に可視化し、IT部門の効率性と生産性を向上させます。
- 過去のデータにアクセスし、企業リソースのセキュリティと利用状況の指標を分析します。
- きめ細かな情報を取得し、ITインフラのセキュリティリスクや社内の誤用を特定します。

ネットワークの問題を解明

- リソースの使用状況やユーザーの振舞いパターンの情報を抽出し、ユーザーの教育やコストを節約するポリシーの導入に役立てます。
- ネットワークにつながっているPCやアプリケーションを可視化し、企業アセットのセキュリティと制御を改善します。

アラートの発信

- 異常値を検知し、リアルタイムでアラートを発信したりレポートを作成したりします。
- セキュリティの異常値や従業員によるITリソースの誤用にフラグを立て、安心して業務を遂行できるようにします。

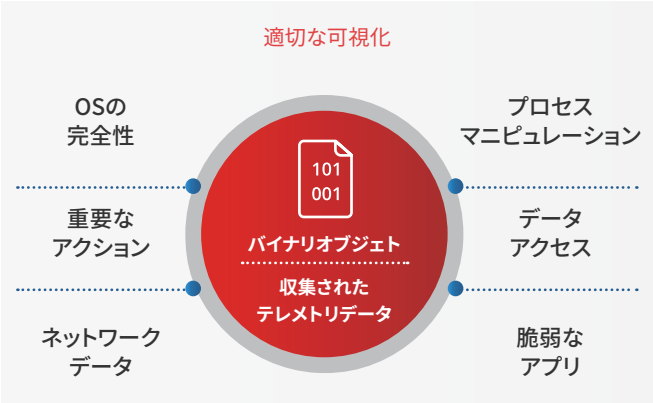
セキュリティインシデントに対する準備

- カスタマイズが可能なレポートを生成し、企業のセキュリティ体制を特定の手法により分析するとともに、企業アセットの誤用を特定して異常な振舞いを検知します。
- 主要なセキュリティ指標のステータスを表示し、是正措置の結果における経時的な変化を追跡することができます。

ニーズに適応した柔軟な分析

Advanced Reporting Tool（高機能レポーティングツール）は、主要な指標、検索オプション、そして以下の3つの領域におけるアラートをデフォルトで表示するダッシュボードを備えています：

- セキュリティインシデントに関するアラート
- 機密情報へのアクセスに関するアラート
- アプリケーションおよびネットワークリソースの利用状況に関するアラート
- 検索や重要情報のアラートは、ビジネスニーズに合わせて適応させることができます



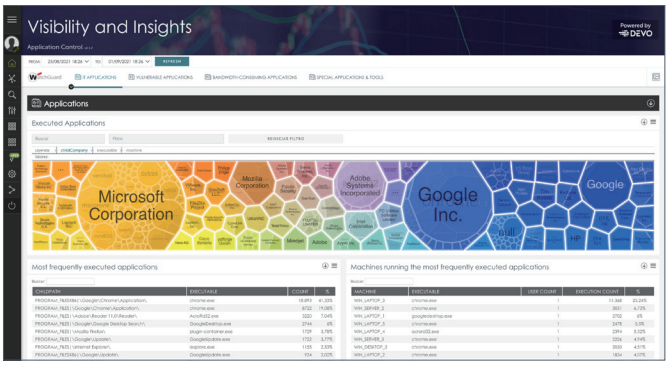
セキュリティインシデント情報

セキュリティインテリジェンスを生成し、侵入行為の最中に発生したイベントの対処と相関分析を実施します：

- 過去1年間に検知されたマルウェア、PUP（不審なプログラム）、不正行為のカレンダー表を作成
- 最も感染の影響を受けたPCリストや検知されたマルウェアの標本を作成
- 脆弱なアプリケーションが搭載されているPCを特定
- マルウェア、PUP（不審なプログラム）、悪用行為の実行ステータス

シャドーITの検出

- 最も頻繁に実行されたアプリケーションと最も実行されていないアプリケーション
- 実行されたスクリプトアプリケーション（PowerShell、Linux shell、Windows cmdなど）
- 実行されたリモートアクセスアプリケーション（TeamViewer、VNCなど）
- 実行された不要なフリーウェアアプリケーション（Emule、torrentなど）



ネットワークリソースの利用パターン

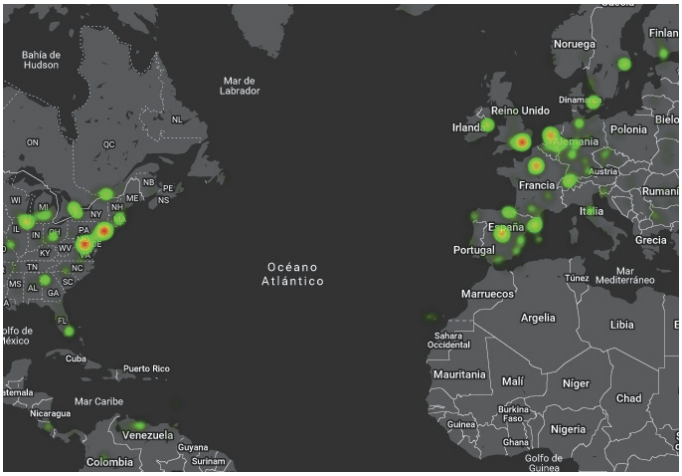
ITリソースの利用パターンを見つけ出し、セキュリティポリシーを定義・実行：

- ネットワーク上の企業アプリケーションと非企業アプリケーション
- 感染、もしくは業務パフォーマンスに影響を及ぼす可能性があるネットワーク上の脆弱なアプリケーション
- MS Officeのライセンス制御（利用中のライセンスと企業で購入したライセンスを比較）
- 帯域幅消費の高いアプリケーション

業務データへのアクセスを制御

ネットワーク上の機密データファイルへのアクセスを表示：

- ネットワークユーザーが高頻度でアクセスし、利用しているファイル
- 過去1年間に送信されたデータ（カレンダー表やマップに表示）
- ユーザーごとのネットワーク上のPCアクセス状況
- 各国のネットワーク接続状況



リアルタイムアラート

イベントに基づくアラートを設定することで、セキュリティ侵害や企業のデータ管理ポリシー違反を把握：

- リスク状況を示すデフォルトのアラート
- ユーザーが作成したクエリに基づくカスタムアラートを定義
- 7つのアラート方法に対応（画面上またはメール経由、JSON、Service Desk、Jira、Pushovery、PagerDuty）

WatchGuard Advanced Reporting Tool（高機能レポーティングツール）の対応プラットフォームとシステム要件

WatchGuard EPDR、WatchGuard EDRと互換性があります

互換性のあるブラウザ：
Google Chrome、Mozilla Firefoxなど

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　FAX：03-5797-7207　https://www.watchguard.co.jp　Email: jpnsales@watchguard.com