DATASHEET

WATCHGUARD FULL ENCRYPTION（フル暗号化）

最前線の防御によりシンプルかつ効果的にデータを保護

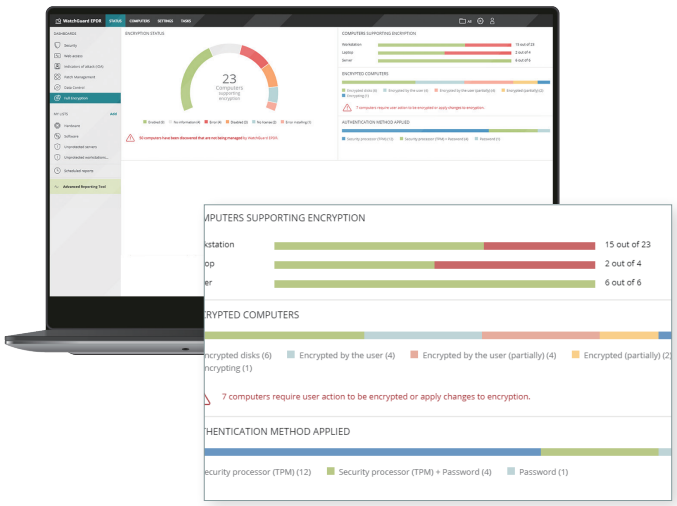
Gartner[1]によると、53秒に1台の割合でノートPCが盗難に遭っています。エンドポイントに保存されるデータ量が増大しているため、攻撃者の関心が高まり、データの紛失、窃取、不正アクセスによる情報漏えいのリスクが増えていることは明らかです。

そのため、EUのGDPR[2] や米国のCCPA[3] などの規制が強化され、データの紛失、盗難、不正アクセスの可能性が高まる中で、それがもたらす深刻な経済的影響を低減するための取り組みが進められています。

不正アクセスに対してセキュリティを集中的に強化

データの漏えいを最小限に止める最も効果的な方法の1つは、デスクトップ、ノートPC、サーバのハードドライブを自動的に暗号化することです。この方法により、データへのアクセスは、確立された認証メカニズムに準拠した安全なものとなります。暗号化ポリシーを確立することは、組織にとってセキュリティとコントロールのレイヤを増やすことになりますが、キーを紛失した場合のデータコントロールとリカバリの問題を引き起こす可能性もあります。

WatchGuard Full Encryption（フル暗号化）は、Microsoftの実績豊富な堅牢なテクノロジーを採用したBitLockerを活用し、エンドユーザーに影響を及ぼさずにディスクの暗号化と復号化を実現します。また、ウォッチガードのクラウドベースの管理プラットフォームに保管されているリカバリキーの一元的なコントロールと管理も可能にします。



WatchGuard Full Encryption（フル暗号化）ダッシュボードは、ウォッチガードのWeb管理コンソールで利用することができ、組織全体にわたるエンドポイントの暗号化ステータスに関する重要指標が表示されます。

特長

ユーザーに影響を与えることなく、データの紛失、盗難、不正アクセスを防止

- ディスクを暗号化することにより、データの盗難、偶発的な紛失、社内の不正利用者による窃取を防止することができます。データの暗号化と復号化は自動化されており、ユーザーは影響されることなく、迅速かつシームレスにデータにアクセスすることができます。
- リカバリキーはクラウドプラットフォームに保管されており、Webコンソールから安全にリカバリすることができます。

導入やインストール作業、およびサーバ類は不要で追加コストゼロ

- **WatchGuard Full Encryption（フル暗号化）**では、Windowsで広範に利用されている実績豊富なBitLockerを一元管理します。
- BitLockerはWindowsのオペレーティングシステムに搭載されており、ウォッチガードのクラウドプラットフォームのWebコンソールから全てのデバイスを集中管理することができます。
- 別途専用のエージェントの導入またはインストールは不要で、ウォッチガードの全てのエンドポイントセキュリティソリューションで採用している、共通の軽量エージェントを利用することができます。
- クラウドでリカバリキーを集中管理することにより、管理するためのサーバのインストールやメンテナンスは不要です。
- **WatchGuard Full Encryption（フル暗号化）**は、速やかに利用開始することができ、WatchGuard Cloudの操作性に優れたインターフェイスを通じて容易に管理することが可能です。

規制コンプライアンス、レポート、一元管理

- **WatchGuard Full Encryption（フル暗号化）**は、Windowsデバイス上のBitLockerのアクティベーションを監視・実行することにより、データ保護規制へのコンプライアンスをサポートし、簡素化します。
- ウォッチガードの全てのエンドポイントセキュリティソリューションでは、直感的なダッシュボード、詳細レポート、および変更監査機能を提供しています。
- さらに、ロールベースの管理により、管理者はグループやデバイスに対して異なる権限レベルや異なるポリシーを単一の一元Webコンソールから設定することができます。

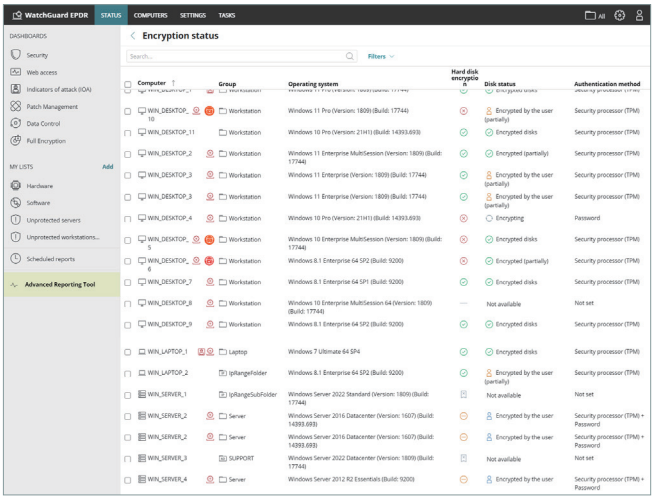
USBフラッシュドライブを保護

この1年間で、世界的にペンドライブ（USBメモリを組込んだボールペン）の使用が増えてきており、特に産業組織では30%も増加しています。この傾向に目をつけたサイバー攻撃者は、USBメモリを侵入経路として利用し、システムにアクセスし、ネットワークの全てまたは一部に感染させています。

その結果、企業はデータ漏えいや機密情報への不正アクセスに見舞われる可能性が高くなっています。Forrester[4] の調査によると、2020年に世界各地のセキュリティの責任者が報告したデータ漏えいのうち、ノートPCやUSBメモリなどのアセットの紛失や盗難が20%を占めています。

脅威のリスクを最小化するための最初のステップは、組織内でのUSBドライブの使用ガイドライン、ロールレベル、スタッフのプロファイルに基づく許可など、組織のIT部門またはMSPが提供し、確認したデバイスのみを使用する厳格なポリシーを設定することです。

しかし、増大するサイバー脅威を前に、これらのガイドラインでは十分でない可能性があります。WatchGuard Full Encryption（フル暗号化）は、全ての暗号化されたエンドポイントに対して最大のデータ保護を実現し、オペレーティングシステムがロードされる前にユーザーの身元情報を確認するプリブート認証を有効にすることで、ノートPCの紛失や盗難によるデータ漏えい、およびデータへの不正アクセスを防ぐことができます。



デバイスリストでは暗号化ステータス、所属グループ、オペレーティングシステムの種類、使用されている認証方法が表示されています。

主な機能

リモートワークやオフィス勤務など、ハイブリッドワークモデルのトレンドにより、ノートPCやUSBメモリなどのデバイスの最前線の防衛策として、フルディスクの暗号化が重要視されています。

WatchGuard Full Encryption（フル暗号化）は、ウォッチガードのエンドポイントセキュリティソリューションの追加モジュールとして利用することができ、フルディスクの暗号化を一元管理し、以下の機能を利用することができます：

ドライブのフル暗号化と復号化

WatchGuard Full Encryption（フル暗号化）は、BitLockerを活用してWindowsのノートPC、デスクトップ、サーバ、リムーバブルストレージデバイスにおけるドライブのフル暗号化を実現します。**WatchGuard Full Encryption（フル暗号化）**のダッシュボードでは、ネットワーク上のエンドポイント、暗号化ステータス、使用されている認証方法を包括的に可視化し、管理者は暗号化設定の割当てや暗号化の許可制限を行うことができます。

リカバリキーの一元管理

アクセスキーを忘れたり、ブートシーケンスに変更があったりした場合、BitLockerは対象となるシステムを起動するためにリカバリキーを要求します。必要であれば、ネットワーク管理者は管理コンソールからリカバリキーを取得し、ユーザーに送信することができます。

リスト、レポート、ポリシーの一元的な適用

コンソールのデバイスリストでは、管理者は暗号化ステータスに応じて複数のフィルタを適用することができます。これらのリストは、外部ツールでデータ分析するためにエクスポートすることができます。

コンソールから暗号化ポリシーを定義し、必要に応じて規制機関や組織に提出できる監査レポートを通じて、ポリシーの変更を確認できます。

[1] TechSpective

[2] GDPR - General Data Protection Regulation（一般データ保護規則）：組織が処理する個人情報の保護を徹底することを強制します。遵守しない場合、厳しい罰金や間接的な損害が発生する可能性があります。

[3] CCPA - 2018年カリフォルニア州消費者プライバシー法：EUのGDPRに続く米国初の法律であり、カリフォルニア州およびその他の州に拠点を置く事業者に適用されます。

[4] The State Of Privacy And Data Protection（プライバシーとデータ保護の現状）」2021年 – Forrester

WatchGuard Full Encryption（フル暗号化）の対応プラットフォームとシステム要件

WatchGuard EPDR、WatchGuard EDR、WatchGuard EPPと互換性があります。対応しているオペレーティングシステム：Windows

互換性のあるブラウザ：Google Chrome、Mozilla Firefox、Internet Explorer、Microsoft Edge 、Opera

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