cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Transparent Encryption Ransomware Protection ランサムウェア プロテクション

課題:ランサムウェアによるビジネスクリティカルなデータへのアクセス妨害を防ぐ

2020年以降、ランサムウェアは増加の一途をたどっており、全データ侵害の25%を占めています[1]。ランサムウェア攻撃は、身代金が支払われるまで重要なデータへのアクセスを妨害することにより、ビジネス運営を急停止させることができます。2031年までに、ランサムウェアは2秒に1回の割合で企業や個人を攻撃するようになると予想されています[2]。

次世代ファイアウォール、セキュアメール/Webゲートウェイなどの境界制御を使用し、脆弱性のギャップを埋めることだけに重点を置いた基本的なセキュリティプラクティスでは、ランサムウェア攻撃を防ぐには不十分です。フォーチュン500社が直面する主な課題は、ビジネスクリティカルなデータを安全に保護し、エンドポイントやサーバー上の不正なプロセスやユーザーによる暗号化を防ぐことです。

ソリューション:CipherTrust Transparent Encryption Ransomware Protection (ランサムウェアプロテクション)

CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP) は、ランサムウェア攻撃からファイルやフォルダを保護する非侵入型の方法を提供します。CTE-RWPは、ビジネスクリティカルなデータをホストしているファイルでの異常なI/Oアクティビティをプロセスごとに監視します。これにより管理者は、ランサムウェアがエンドポイント/サーバーに感染する前に、疑わしいアクティビティを警告またはブロックできます。

主なメリット

- **透過的なデータ保護。**CTE-RWPは、エンドポイント/サーバー上のアプリケーションに変更を加えることなく最小限の設定で、ボリュームごとにランサムウェア保護を常時適用します。継続的な監視によりランサムウェアに感染したプロセスから異常なファイルアクティビティが検出された場合、警告またはブロックを行います。
- **容易な展開。**CTE-RWPでは、管理者はCTEライセンスで提供されるファイル/フォルダ単位での制限的なアクセス制御や暗号化ポリシーを設定することなく、ランサムウェア保護のみで開始できます。

1 https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/

2 https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031/#:~:text=Cybersecurity%20Ventures%20predicts%20that%20by,than%20ever%20protecting%20against%20ransomware

- **高度なランサムウェア検出。**CTE-RWPは、プロセスベースの機械学習モデルを使用して、疑わしいファイルI/Oアクティビティを動的に検出します。また、エンドポイント/サーバー上のランサムウェアを特定し、警告またはブロックします。承認されたプロセスは、信頼済みリストに追加することで監視対象から外せます。

ライセンス

CTE-RWPは単体でライセンスされます。CTE-RWPは、各エンドポイント/サーバーのファイル/フォルダレベルで詳細なアクセス制御ポリシーを設定することなく、十分なレベルのランサムウェア検出機能を提供します。CTEライセンスと組み合わせることで、管理者はさらにきめ細かなアクセス制御や暗号化を適用できます。CTE-RWPは、単体またはCTEと組み合わせてライセンスを取得できます。

CipherTrust Transparent Encryptionでランサムウェアに対するデータ保護を強化

CipherTrust Transparent Encryption（CTE）のライセンスを追加することで、ランサムウェアに対するエンドポイント/サーバーの保護を最大限に向上させ、CTE-RWPでは提供されない次のメリットを得ることができます。

きめ細かなアクセス制御

- ビジネスクリティカルなデータの暗号化/復号化/読み取り/書き込みや、ディレクトリをリストする権限を持つ人（ユーザー/グループ）を定義します。
- バックアップを暗号化してデータの流出を防ぐなど、バックアッププロセスに関する厳格なアクセス制御ポリシーを設定します。
- 信頼されたアプリケーション上でのシグネチャチェックを含め、保護されたフォルダへのアクセスと暗号化/復号化が承認されているファイル（バイナリ）のGuardPointレベルの信頼済みリストにより、整合性を確保します。

保存データの暗号化

- ビジネスクリティカルなデータがオンプレミスやクラウドのどこに保存されていようと暗号化します。
- 重要なデータを無価値化することにより、侵入者が暗号化されたデータを公開すると脅して収益化できないようにします。
- 信頼されたアプリケーション上でのシグネチャチェックを含め、保護されたフォルダへのアクセスと暗号化/復号化が承認されているファイル（バイナリ）のGuardPointレベルの信頼済みリストにより、整合性を確保します。

MFA for CipherTrust Encryptionの使用

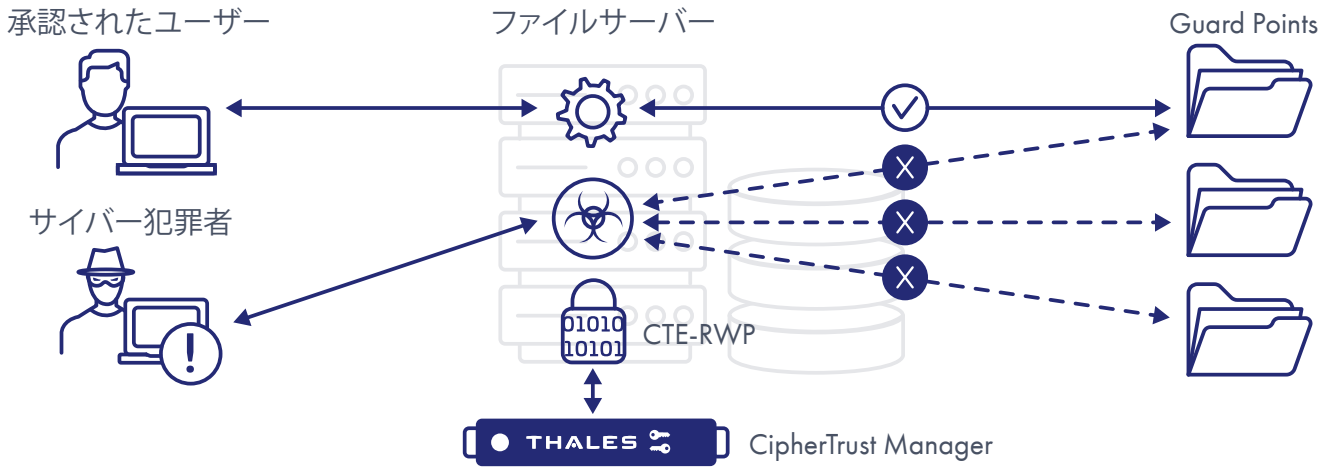
MFA（多要素認証）for CipherTrust Encryption（CTE）を追加して、フォルダ/ファイルレベルでさらなる保護層を加えることができます。MFA for CTEは、GuardPointの背後にある機密データにアクセスしようとするシステム管理者や特権ユーザーに対し、パスワードのほかに追加の認証要素を要求します。

MFA for CTEは、Windowsプラットフォームで利用可能です。タレスのSafeNet Trusted Access、Okta、Keycloakなど、複数の認証プロバイダーとの統合をサポートしています。

About Thalesタレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。



CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

> cpl.thalesgroup.com <

お問い合わせ先 – cpl.jpsales@thalesgroup.com すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。