Absolute Ransomeware Response

ランサムウェアへの備えと攻撃を受けた際の素早い回復を支援

ランサムウェアは、世界中の企業にとって最も重大な脅威の一つです。Cybersecurity Ventures は、2021 年には 11 秒に 1 件の割合だったランサムウェアの組織へ攻撃は、2031 年には 2 秒には 1 件の割合になると予測しています。

ランサムウェアの攻撃は、数分で組織を機能不全に陥れます。重要なデータへのアクセスが阻止され、ビジネスを継続できなくなる可能性があります。それだけではありません。近年、脅威行為者は、システムに侵入するだけでなく、重要なデータを盗み出し、それを一般に公開したり販売したりすると脅す、多面的な恐喝に移行しています。

準備と回復の必要性

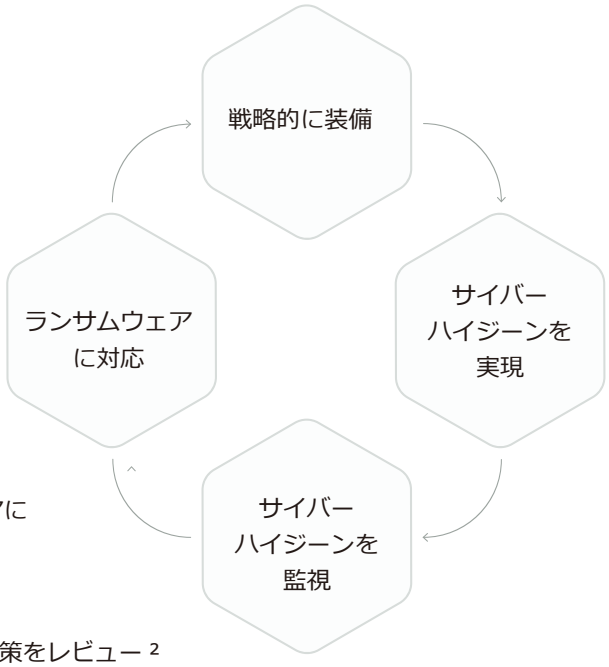
組織がランサムウェアに対応するためには、備えを強化し、修復、根絶、復旧に必要なツールを整えるのはもちろん、それらが期待通りに機能していることを確認することが重要です。特にエンドポイントの復旧は重要です。エンドポイントは、今日の「どこでも仕事ができる」ハイブリッドワーク環境において、従業員がビジネスタスクを遂行するために不可欠なツールです。ランサムウェアの攻撃を受けた場合、重要なインフラ (Active Directory、データベースサーバー、アプリケーションサーバー、メッセージサーバーなど) やビジネスアプリケーションの復旧の重要性を考慮すると、エンドポイントの復旧作業は二の次と考えられる傾向があります。リモートワークやハイブリッドワークが実施されている環境下では、従業員のデバイスの復旧に関しても迅速な対策が要求されます。

ランサムウェアの攻撃は多くの場合、エンドポイントを再感染しやすい状態にし、再イメージング／復旧がほとんど不可能な状態にします。必要なツールが機能しなくなっているからです。多くの場合、IT チームやセキュリティチームが従業員のエンドポイントを復旧にとりかかる頃には、すでにリソースを使い果たしてしまっています。

Ransomware Response でレジリエンスを強化

そこで威力を発揮するのが、Absolute® Ransomware Response です。Absolute Ransomware Response は、インシデント後のエンドポイントの対応と復旧に関する豊富な経験をベースに開発されました。また、Absolute の常時接続性、主要なセキュリティおよび管理ツール (Microsoft® Endpoint Manager、Ivanti®、Tanium™、SentinelOne®、CrowdStrike™ など) の自動復活機能、Absolute Reach スクリプトのライブラリを活用し、迅速なエンドポイントの復旧を実現します。

Absolute Ransomware Response は、ランサムウェア攻撃への備えを築き、攻撃を受けてしまった場合には迅速にエンドポイントを復旧させて、お客様のビジネスを守ります。攻撃にさらされているストレスの中で、Absolute はお客様と共に脅威に立ち向かい、IT チーム、セキュリティチームを強力に支援します。



ランサムウェアへの備えと対応

Absolute Ransomware Response の活用により、ランサムウェアに対抗する 4 つのコアコンピテンシーが強化されます。

エンドポイント全般にわたる戦略的装備 [1]

- ✓ エンドポイント全体にわたる既存の標準的なセキュリティ対策をレビュー [2]
- ✓ ランサムウェアへの暴露を最小限に抑え、迅速な復旧を保証するための必要な主要管理 (マルウェア対策など) とデバイス管理ツールを特定

エンドポイント全体におけるサイバーハイジーンの有効化 [1]

- ✓ 特定されたミッションクリティカルなセキュリティアプリケーションとデバイス管理ツールがインストールされ、意図したとおりに機能することを保証するために、アプリケーション回復ポリシーを確立
- ✓ アプリケーションの健全性を監視する方法についてのトレーニングを提供。新しいデバイスが登録された際に、これらのベースラインポリシーを適用する

エンドポイント全体にわたるサイバーハイジーンの監視

Absolute Platform を活用

- ✓ ハードウェアとソフトウェアの在庫を報告
- ✓ デバイスのセキュリティ態勢を評価
- ✓ 機密性の高いエンドポイントデータ (例：PII、PHI) を検出、リスクのあるデバイスを特定、既存のツールで適切なバックアップを確保

エンドポイント全体にわたるランサムウェア対応

Absolute Platform を活用

- ✓ デバイス上でエンドユーザーとのセキュアな通信を確保
- ✓ リスクのあるデバイスをフリーズ
- ✓ スクリプト・コマンド・ライブラリによりリカバリタスクを迅速化
- ✓ エンドポイントセキュリティまたはデバイス管理ツールを自動復活 [3]

事前に定義されたプレイブックに従い、既存の Absolute 製品の機能を活用して、インシデントに対するエンドポイントリカバリ作業を行うリモートヘルプを年間最大 2 件提供 [1]

1. Absolute プロフェッショナルサービス・コンサルタントが提供
2. Microsoft® Windows デバイスにのみ対応
3. Absolute Application Resilience カタログから、マルウェア対策アプリケーションとデバイス管理アプリケーションをひとつずつ選択

ケーススタディ

課題

ある大手リテール企業は、ランサムウェア攻撃に遭遇した後、Absolute に支援を求めました。この顧客はランサムウェア「Hard2Decrypt」に感染し、最初の 1 週間はビジネス停止に追い込まれました。攻撃者はランサムウェアを投下する前に、この企業のセキュリティおよび管理ツールを明示的に操作不能にしていました。このため、この企業は感染拡大を防ぐことも、すでに感染したマシンを復旧させることもできない状態に陥りました。

ソリューション

Absolute の Application Resilience 機能とカスタムスクリプトを組み合わせて使用することで、感染したマシンを特定して隔離し、更新されたセキュリティツールを再インストールすることで、再感染のサイクルを断ち切ることができました。

結果

復旧作業をより迅速に開始することができ、重要なセキュリティコントロールがインストールされた健全な状態を維持し、将来のランサムウェア攻撃に対するリスクエクスポージャーを最小限に抑えることができるようになりました。

導入成果

- デバイス・フリート全体におけるランサムウェアへの暴露を最小化し、迅速なリカバリ作業を保証するために必要な、主要なセキュリティ制御とデバイス管理ツールを特定
- Absolute を搭載したエンドポイント全体にサイバーハイジーンのベースラインを確立
- エンドポイントのセキュリティ状況を監視し、重要な制御を自動的に回復
- カスタム・ワークフローとタスク自動化コマンドを活用して復旧作業を迅速化
- エンドポイントの復旧作業を管理するための実行可能な推奨事項やガイダンスを提供することで、IT 管理者やセキュリティチームの負担を軽減

ランサムウェアの被害を防ぐために

Absolute Ransomware Response の採用は、最も重要なテクノロジー投資のひとつです。エンドポイントに対するランサムウェアへの備えの評価、デバイス全体にわたるエンドポイントのサイバーハイジーンの監視、エンドポイントの迅速な復旧が実現されます。

Absolute Software は、約 21,000 社のお客様から信頼いただいている、自己復活型のインテリジェント・セキュリティ・ソリューションの唯一のプロバイダです。Absolute は、6 億台以上のデバイスに搭載され、エンドポイント、アプリケーション、ネットワーク接続にインテリジェントかつダイナミックに可視化、制御、自己修復機能を実現します。ランサムウェアや悪意のある攻撃の脅威が高まる中、サイバーレジリエンスを強化するための永久デジタル接続を実現する唯一のプラットフォームです。