

Halcyonとバックアップ： 最強の組み合わせ

バックアップは不可欠。 だが、ランサムウェアレジリエンス戦略にはならない。

バックアップは、誤削除、ハードウェア障害、自然災害からの復旧を支援するために設計されています。ランサムウェアは、そのいずれにも当てはまりません。ランサムウェアは、データを流出させ、復旧手段を破壊し、身代金を要求する前に事業への被害を最大化するために作り上げられた、組織的かつ多段階にわたる攻撃活動だからです。

その結果、バックアップを導入していても企業が危険にさらされたままとなる「ランサムウェアレジリエンスギャップ」が生じます。攻撃者が防御を突破すると、バックアップツールは、そもそも解決するために設計されていない数多くの課題に直面することになります。

ランサムウェアがバックアップを打ち破る仕組み



01. 誰にも気づかれないうちにデータを盗み出す

滞留期間中、攻撃者はアラートを発生させる前の数日から数週間にわたり、価値の高いデータをひそかに流出させます。バックアップからの復元では、暗号化されたファイルは元に戻せても、盗み出されたデータを取り戻すことはできません。どれほどクリーンに復旧できたとしても、情報漏えいの通知、顧客データの流出、そして二重脅迫がもたらす影響は、依然として残り続けます。



02. 復旧手段を見つけ出し、破壊する

攻撃者は暗号化を実行する直前に、保持ポリシーの改ざん、カタログの削除、時刻同期の悪用、サービスの直接停止といった手口でバックアップインフラを無力化します。Sophosの調査によれば、ランサムウェア攻撃の94%がバックアップの侵害を試み、そのうち57%が成功しています。



03. バックアップが侵入経路ごと復元してしまう

バックアップは、ある時点の環境の状態を、その脆弱性も含めてそのまま記録します。最初の侵入経路を特定して塞がないまま復元すれば、業務が復旧しないうちから、攻撃者に再侵入の機会をそのまま差し出すことになります。最新の調査では、ランサムウェア攻撃を受けた組織の78%が、その後再び被害に遭っていることが明らかになりました。



04. 復旧のダウンタイムを武器として利用する

バックアップを無力化し、暗号化を完了させた攻撃者は、数週間にわたる過酷なダウンタイムを背景に、身代金の支払いを迫ろうとします。Gartnerによれば、平均的な組織では復旧に22日を要しており、Total Assureの調査では、エンタープライズ環境においてこの日数が38日にまで延びていることが確認されています。

バックアップとHalcyonの価値

バックアップ製品の役割は、データを復旧することです。Halcyonは、その復旧が確実に機能することを保証します。具体的には、以下を提供します。

- ・ **バックアップ改ざん防御:** Halcyonは、攻撃者がバックアップインフラを破壊する前に、それを無効化・破壊させようとする試みを監視します。
- ・ **ファイルレジリエンス:** Halcyonは、進行中の暗号化プロセスを検知し、発生と同時に巻き戻すことで、暗号化の完了を阻止します。
- ・ **暗号化ファイルの復元:** Halcyonは暗号鍵の情報を取得し、バックアップに頼ることなく被害を受けたファイルやシステムを復号します。これにより、復旧時間を数週間から数分へと短縮します。
- ・ **データ流出防御:** 二重脅迫攻撃に悪用されるデータの窃取を防止し、盗み出されたデータによってバックアップからの復旧が損なわれる事態を回避します。
- ・ **24時間365日対応のランサムウェアオペレーションズセンター (ROC):** Halcyon ROCが、検知・対応・復旧をお客様に代わって追加費用なしで運用し、復旧にかかる時間を数日から数週間単位から数分単位へと圧縮します。

Halcyon vs. バックアップのみ

機能	バックアップのみ	HALCYON とバックアップ
バックアップ保護	攻撃者は、保持ポリシーの改ざん、カタログの削除、NTPの悪用、サービスの直接停止によってバックアップを無力化します。	Halcyonは、ランサムウェアがバックアップインフラに到達する前に検知し、バックアップシステムを無効化・破損させようとする試みを監視します。
暗号化の阻止と封じ込め	アラートが発生するまで暗号化が歯止めなく拡散し、データ損失と復旧範囲が最大化します。	Halcyonは、進行中の暗号化プロセスを検知してリアルタイムで巻き戻し、暗号化を阻止すると同時に、環境を保護して拡散を抑え込みます。
フルリストア不要のファイル復元	暗号化されたファイルの復元には、数日から数週間に及ぶフルリストアのサイクルが必要です(バックアップが無事に残っていることが前提です)。	Halcyonは攻撃の最中に暗号鍵の情報を取得し、ROCが被害を受けたファイルを数分で復号できるようにします。
復旧範囲	バックアップが唯一の復旧手段である場合、組織はクリーンルームからの全社的な再構築に直面します。それは数週間に及ぶ作業であり、しかもデータの復旧は不完全なものにとどまります。	Halcyonは大規模な暗号化を阻止し、被害範囲を封じ込めることで、全社規模の再構築を、被害を受けた一部システムへの的を絞った復元へと転換します。これにより、復旧時間とデータ損失を大幅に圧縮します。
データ流出への対応範囲	バックアップが復元できるのは暗号化されたファイルのみです。暗号化の前に盗み出されたデータは、どのような復元を行っても元には戻りません。	Halcyon DXPは、データが環境の外に出る前に窃取を阻止するため、盗まれたデータによってバックアップからの復旧が損なわれることはありません。
マネージドレスポンス	インシデント対応には別途契約が必要で、多額の追加費用がかかるうえ、対応開始までに時間を要することも少なくありません。	24時間365日対応のHalcyonランサムウェアオペレーションズセンター（ROC）が、お客様に代わって調査・対応・復旧の主導を、追加費用なしで行います。

バックアップだけでは不十分。 Halcyonが、それを機能させる。

Halcyonは、ランサムウェアの攻撃者が突いてくるそのギャップを埋めます。ランサムウェアがバックアップインフラに到達する前に検知し、暗号化を発生と同時に巻き戻し、暗号鍵の情報を取得して被害を受けたファイルを数分で復元し、被害範囲を封じ込めて復元すべき対象を最小限に抑え、復旧時間を数週間から数時間あるいは数分へと短縮し、さらに専門家主導の対応を24時間365日・追加費用なしで提供します。こうしてHalcyonは、バックアップを「最後の手段」から、ランサムウェアレジリエンスを支える信頼できる要素へと変えます。

その結果、失われるデータは減り、フルリストアを必要とするシステムは少なくなり、復旧は数週間単位ではなく、数分・数時間単位で測れるものになります。

最後に

バックアップツールは、事故に備えて作られたものです。しかしランサムウェアは事故ではありません。データを盗み出し、復旧手段を破壊し、企業を人質にするために仕組まれた、組織的な攻撃です。バックアップだけでは、これを食い止めることはできません。

Halcyonは、そのギャップを埋めます。バックアップインフラを改ざんから保護し、暗号化を発生と同時に巻き戻し、暗号鍵の情報を取得してファイルを数分で復元し、データの流出を阻止し、さらに専門家主導の対応を24時間365日・追加費用なしで提供します。こうしてHalcyonは、バックアップを「最後の砦」から、真のランサムウェアレジリエンスを支える基盤へと変えます。

バックアップは不可欠。Halcyonが、それを機能させる。

詳細はこちら：www.halcyon.ai/jp