

ランサムウェアレジリエンス

ランサムウェア攻撃は、必ず来る。確かな備えを、Halcyonで。
攻撃を受けても、事業は止まらない。Halcyonは事業継続そのものを守ります。

ランサムウェアは、数ある脅威の一つではありません。AIを武器にした、人間主導の「作戦」です。

ランサムウェアは、スキャンして駆除すれば終わり、というマルウェアではありません。その正体は、人間が指揮を執る「作戦」です。攻撃者はいまやAIを使い、偵察を自動化し、思わず開いてしまうフィッシングメールを作り込み、シグネチャベースの防御をすり抜ける新種の暗号化プログラムまで生み出しています。そうして環境に入り込み、データを窃取し、バックアップを破壊し、事業そのものを止めにかかります。その被害は、数字にはっきり表れていません。復旧までに平均22日、平均コストは508万米ドル(約8億円)※。しかも、これは身代金を除いた金額です。Halcyon(ハルシオン)は、この現実を変えるために生まれた、ランサムウェアレジリエンス専用のプラットフォームです。 ※1米ドル=153円換算(2026年9月時点)

既存のツールでは止めきれない攻撃を、初期侵入から暗号化までのすべての段階で阻止します。それでも突破された場合は、数週間ではなく数分で復旧。さらに、ランサムウェアオペレーションセンター(ROC)の専門家が24時間365日、対処を引き受けます。お客様のチームは、本来の業務に集中したままでいられます。事業の存続を左右しかねなかった事態を、何事もなかった一日に変える。それがHalcyonの目指すゴールです。

攻撃の段階	HALCYONの対応
初期アクセス	AI・振る舞い検知
データの窃取	二重脅迫防止(DXP)
バックアップの破壊	暗号鍵素材の捕捉／Halcyon ROC
暗号化と業務停止	ファイルレジリエンス

事業の存続を左右する事態を、何事もない一日に。 攻撃を受けても、ビジネスは止まりません。

Halcyonは既存の防御の上にレジリエンスレイヤーを重ね、被害を最小限に抑え、攻撃者を環境から締め出し、数週間ではなく数分で業務を元に戻します。ファイルレジリエンスは、ファイルの読み書きが行われるその瞬間に暗号化の動きを捉え、悪意ある暗号化を事実上成立させません。万データが暗号化されても、暗号鍵素材の捕捉と復号がそのインシデント固有の鍵を再構成し、被害を受けたデータを元どおりにします。身代金を支払う必要も、バックアップに頼る必要もありません。

主要な特徴

- ・ **AI・振る舞い検知エンジン:** 実際のランサムウェアの戦術・技術・手順(TTP)、検体、そして現場のインシデント対応で得た知見をもとに学習させた2層モデルが、実行される前の脅威と、一般的な検知をすり抜ける不審な挙動の両方を捉えます。
- ・ **ファイルレジリエンス:** これまでに一度も観測されていない暗号化プログラムであっても、暗号化の動きをその場で捕捉し、ディスクに書き込まれる前に止めます。
- ・ **BYOVD・EDR改ざん検知:** 署名は正規でも脆弱性を抱えたドライバを攻撃者が持ち込む手口(BYOVD)を阻止し、EDR(エンドポイント検知・対応)ツールが改ざんされていないかを常時監視します。
- ・ **二重脅迫防止(DXP):** 大容量の通信や既知の不正な宛先への接続を監視し、データの持ち出しを検知します。複雑なルールを組む必要はありません。
- ・ **暗号鍵素材の捕捉と復号:** 攻撃の進行中に暗号鍵素材を押さえ、身代金を支払うことも、バックアップに頼ることもなく、数時間でデータを取り戻します。
- ・ **ランサムウェアオペレーションセンター(ROC):** ランサムウェア専門のチームが、お客様の環境を24時間365日監視します。アラートの調査から脅威への対応、復旧の主導まで担い、追加費用は一切かかりません。

攻撃者にとって、Halcyonを迂回する道はありません。

暗号化される前に止める。データが持ち出される前に止める。「侵害」と呼ばれる事態になる前に止める。AIが攻撃を加速させるいま、攻撃者はかつてない速さで、しかも以前ほどの手間をかけずに動きます。汎用的なセキュリティツールは、この速さについていくようには作られていません。Halcyonが加えるのは、ランサムウェアだけを想定した防御レイヤーです。実行前の準備段階から、データの持ち出し、そして暗号化まで、攻撃者がたどるすべての段階で検知し、動きを妨げ、進行を断ち切ります。汎用ツールはランサムウェアのために作られたわけではありません。Halcyonは、そのためだけに作られました。

ランサムウェアは休みません。Halcyonも同じです。

ランサムウェア専門としては世界初のオペレーションセンター(ROC)が、専門家の目で守ります。このROCがお客様の環境を24時間体制で見張り、調査から対応、復旧までを担います。お客様のチームが、ランサムウェアと単独で向き合うことはありません。最初のアラートから完全な復旧まで、専任のランサムウェ

アスペシャリストが引き受けます。追加費用はかかりません。

ROCのアナリストは、大量のアラートの中から本当に危険なものを見極め、すべてに目を通します。お客様のチームがアラート対応に忙殺されることも、重大な予兆を見落とすこともありません。インシデントが起きたときは、封じ込め、修復、攻撃者の排除、復旧までをROCが一貫して指揮します。緊迫した状況の中で、お客様のチームが手探りで判断を迫られることはありません。

Halcyonについて

ランサムウェアの脅威は、業種や規模を問わず、あらゆる企業に及びます。Halcyonは、ランサムウェアレジリエンスに特化した専用プラットフォームです。既存のツールでは止めきれない攻撃を阻止し、万一突破された場合でも数分で復旧します。本来なら事業の存続を左右しかねない事態を、通常業務を止めずに乗り切れる出来事に変えます。詳しくは halcyon.ai/jp をご覧ください。

詳細については[資料請求](#)や[お問い合わせ](#)からご連絡ください。

