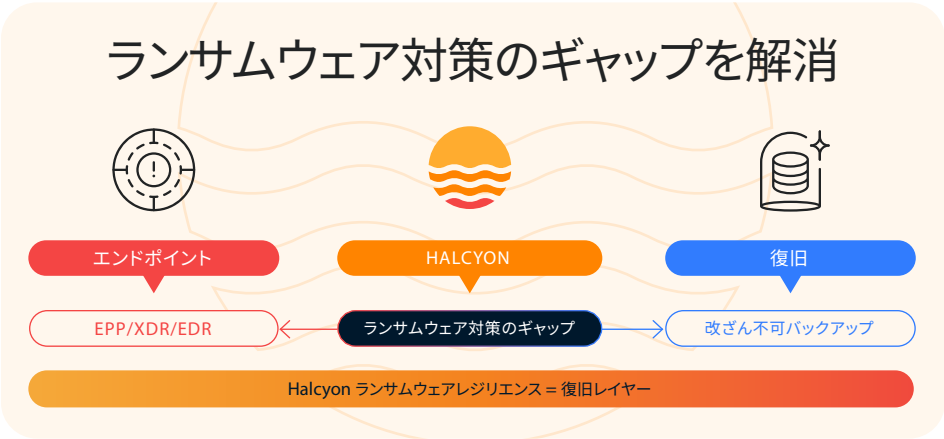
データシート

Halcyon(ハルシオン)
ランサムウェア対策プラットフォーム

ランサムウェア対策に特化した、唯一の専用ソリューション

あらゆるセキュリティ対策を講じていても、ランサムウェアの被害は後を絶ちません。エンドポイントセキュリティやバックアップに投資していても、攻撃者は防御の隙を巧みに突いてきます。EDRを回避し、セキュリティツールを無効化し、バックアップすら破壊します。既存のセキュリティ製品は、汎用的な脅威を想定して作られているからです。

Halcyonのアプローチはまったく異なります。ランサムウェアの封じ込めとデータ恐喝の阻止だけを目的に、ゼロから設計された専用ソリューションです。攻撃ライフサイクルのあらゆる段階で脅威を先回りして遮断するエンドツーエンドの防御に加え、24時間365日体制の専門チームが対応にあたることで、身代金の支払いゼロ・業務停止ゼロを実現します。



Halcyonの優位性

エンドツーエンドの保護

ランサムウェアは、よくあるマルウェアの一種ではありません。最大限の被害を与えることを目的とした、複数段階にわたる人間主導の攻撃キャンペーンです。Halcyonが攻撃の一段階だけでなく、実行前の侵入からデータの窃取、暗号化まで、攻撃ライフサイクル全体をカバーしているのはそのためです。ランサムウェアがどこに潜んでも、Halcyonは見逃しません。

ランサムウェアだけに特化しているからこそ、高精度のAIと行動分析モデルにより、攻撃チェーンの早い段階で脅威を検知できます。EDR改ざん検知と権限昇格検知が、既存のエンドポイントセキュリティを無効化・回避しようとする動きをい

主なメリット

- ランサムウェアによる事業リスクを根本から排除
- 既存のエンドポイント対策をすり抜ける攻撃も確実に阻止
- 24時間365日のランサムウェア専門対応力
- データの窃取・恐喝から組織を守る
- 迅速な検知と復旧で事業継続性を確保

ランサムウェアの実態

104%
過去2年間でランサムウェア攻撃の成功件数が104%増加

22 Days
ランサムウェア攻撃からの平均復旧期間は22日間

69%
被害を受けた組織の69%が「十分な備えがある」と考えていた

ち早く捉えます。さらに、データ持ち出し防止機能（DXP）が、暗号化される前のデータ窃取の兆候を特定。万が一ファイルが暗号化された場合でも、Halcyonは攻撃中に暗号鍵を傍受するため、バックアップに頼ることなく迅速に復号・復旧が可能です。

24時間365日のマネージド運用

セキュリティチームの負荷はすでに限界に近づいています。これ以上業務を増やしたり、大量の誤検知に振り回されるようなツールは必要ありません。Halcyonでは、ランサムウェア対策プラットフォームの標準機能として、24時間365日対応のランサムウェアオペレーションセンター（ROC）を提供しています。

すべてのHalcyon導入環境に、専門チームによる24時間365日のマネージドランサムウェア保護が含まれています。アラートの調査、脅威への対応、復旧作業の主導まで、煩雑な作業はすべてお任せください。追加の人員を雇うことなく、常時ランサムウェアから守られている安心感を手に入れることができます。

日本市場向けサポート体制

Halcyonは、日本のお客様に安心してご利用いただけるよう、日本拠点に専任チームを設置しています。ランサムウェア対策の豊富な知見を持つ専門家が、日本語で手厚くサポートしています。

Halcyon(ハルシオン)について

Halcyonは、ランサムウェア対策に特化したソリューションプロバイダーです。侵入の初期段階からデータの窃取、暗号化に至るまで、攻撃のあらゆる局面で脅威を先回りして封じ込めます。24時間365日対応の専門チームで、身代金の支払いをなくし、事業の継続性を守り、データ恐喝の被害を防ぎます。詳細はhalcyon.aiをご覧ください。

また、お見積もりや導入のご相談については、Halcyon Japan株式会社までお気軽にご連絡ください。

電話：03-6825-0915 / Email:japan-sales@halcyon.ai

Halcyon ランサムウェア対策プラットフォーム

身代金の要求から企業を守り、事業の継続性を確保し、データの流出を未然に防ぐ。