CROWDSTRIKE

CROWDSTRIKE FALCON INSIGHT™ ENDPOINT DETECTION AND RESPONSE (EDR)

導入しやすく、深い検知が可能で、運用もしやすい EDR 製品の決定版

FALCON INSIGHT：運用のしやすさを重視した EDR

従来のエンドポイントセキュリティツールには盲点があり、高度な脅威を検出したり、阻止したりすることができませんでした。Falcon Insight なら、組織全体に完全なエンドポイントの可視性を提供し、この問題を解決します。Insight は全てのエンドポイントのアクティビティを常時監視し、リアルタイムでデータを分析して攻撃の挙動を自動的に識別するため、高度な攻撃が発生すると即座に検出して環境を保護することができます。一方で、すべてのエンドポイントのイベント情報は CrowdStrike Falcon® プラットフォームに送られ、CrowdStrike の OverWatch 脅威ハンティング・チームのアナリストが AI を駆使しつつも人の目でそれを調査し、優先度を明示したアラートの発信を行います。

さらに AI やマシンラーニングだけでは見つからない高度な脅威も逃さずハンティングすることで、高度なセキュリティ・レベルを実現すると同時にお客様の人材不足の課題を解決し、お客様やご契約されている SOC 担当者様に負担の少ない日々の運用を可能にしています。

FALCON INSIGHT が EDR 業界をリード「振る舞い分析／企業向け脅威検知において最高のシステム」 — 2017 年 Security Magazine アワード

「完璧な検知結果」(5/5) と「申し分のないコスト性」(コスト効果) — 2017 年 Forrester Endpoint Security Wave
2017 年 の Gartner の Comparison of Endpoint Detection and Response Technologies and Solution Report（EDR 技術とソリューションの比較レポート）で、評価対象となった全ての事例において、(最高ランクの) “ Strong” を獲得

製品の主な機能

検知と対処をシンプルに

主な特長

- 高度な攻撃を自動的に検出できます
- リアルタイムフォレンジックにより素早い調査ができます
- 対処作業を確信を持って行えます
- 5 秒で全環境を検索できます
- Falcon OverWatch の脅威ハンティングサービスを使えます

- **攻撃者の挙動を自動的に検知** — Insight は IOA（Indicator of Attack）を利用して自動的に攻撃者の振る舞いを識別して、優先度を付けたアラートを Falcon 管理画面に表示させることで、時間のかかる調査作業を低減させます。
- **1つの画面で攻撃の全体像を解明** — 見やすいプロセスツリーで、攻撃活動の全貌を詳細に提供するため、調査をスピードアップできます。
- **調査ワークフローのスピードアップ** — 直観的な UI によって全環境の検索が実行できます。
- **全体像とインテリジェンスを提供** — 脅威インテリジェンスと統合することにより、攻撃元の情報を含めた攻撃の全体像の情報を見ることができます。
- **感染した可能性のあるシステムを1クリックで封じ込め** — 感染したシステムを封じ込めることによって、攻撃を即座に止めることができます。

圧倒的な深さと速さ

- **すべての動きをリアルタイムに監視** — 可視化によって、攻撃者を「肩越しにのぞき込む」かのようにその挙動を監視することができます。
- **フォレンジックに必要となる200種類以上の情報を取得** — ユーザー・モードよりもさらに深いカーネル・モードで動作するドライバーにより、実に200種類以上ものイベントを収集することで、他社にないレベルでの脅威の発見を可能にしています。
- **数秒で回答を提示** — CrowdStrike Threat Graph TM のグラフ・データベースはイベントデータを保存し、たとえ何十億のイベントがあったとしても、5秒以下でクエリーに回答します。
- **最大90日の履歴** — Falcon Insight はエンドポイントのアクティビティの完全な記録を一定期間保持します。環境内のエンドポイント数が100以下であっても、50万以上であっても変わりません。

導入の早さとエンドポイントの軽さも魅力

- **時間、労力、費用を削減** — Falcon Insight はクラウドから全て提供されるため、オンプレミスのサーバーなどは一切必要ありません。
- **数分で導入完了** — Falcon エージェントを各エンドポイントに展開するだけで導入が完了します。例えば7万台のエンドポイントに Falcon Insight を展開されたあるお客様では、1日以内で導入作業を全て完了されました。
- **短時間で稼働開始** — 導入にあたり、エンドポイントの再起動は必要ありません。複雑なチューニングやコンフィギュレーション設定もありませんので、導入初日からその効果を発揮します。
- **エンドポイントが重くならない** — Falcon の軽量エージェントはわずか20MB のサイズ。検索などの処理は全てクラウド上の Falcon Threat Graph TM データベース上で行われるため、エンドポイントやネットワークへの影響はほとんどありません。

サイレントな攻撃を見つけ、情報漏洩を防ぐ Falcon のパワー

攻撃を防御する技術は完璧ではありません。優れた攻撃者は防御システムをバイパスして侵入し、何週間、何カ月も気づかれずに環境内で活動する技術を有しています。この「サイレントな攻撃」の期間をどれだけ長く取れるかは攻撃者にとって成功の鍵であり、いずれ組織に大きな被害をもたらす脅威となるでしょう。Falcon Insight は既存の防御システムでは認識できないインシデントを即座に検知し、識別して、対策を打てるようにします。

CROWDSTRIKE

CrowdStrike は、クラウドベースの次世代エンドポイントプロテクションの業界を牽引しています。 CrowdStrike は、次世代のアンチウィルス、EDR、および24時間体制のマネージド脅威ハンティングサービスを統合し、すべてを1つの軽量エージェントで提供する、業界初、かつ唯一の企業として、革新的なエンドポイントプロテクションを提供しています。

詳細は、**crowdstrike.com** をご覧ください。