その他サービス

インシデント調査対応サービス
Incident Response

CrowdStrikeが蓄積したノウハウをもとに、組織内で発生したインシデントを調査・分析。
攻撃者の検知、追跡から、不正アクセスの阻止などの対処までを実施し、通常業務への復旧を支援するサービスです。

侵害診断サービス
Compromise Assessment

過去から現在までで、攻撃・侵害が発生していないかを診断し、イベントを把握することで、
今後の有効なセキュリティ対策をサポートします。

対応OS・環境

Windows / macOS / Linux / iOS / Android
AWS / GCP / Azure / 仮想環境・VDI / コンテナ環境

CrowdStrike 一次代理店

マクニカネットワークス

国内の一次代理店として、2013年よりCrowdStrike製品を取り扱い、
国内における製品サポートや日本語化ツールの提供を行っています。
ユーザコミュニティ運営、Webセミナー開催など、導入企業のフォロー
アップにも注力し、企業の導入から運用までサポートします。

製品サポート
ユーザコミュニティ
豊富な情報提供

無料トライアル

マクニカネットワークスでは、CrowdStrike Falconの無料トライアルをご用意して
います。エージェントによる負荷の軽さ、スキャンの性能などを、自社の環境で検証
ください。検証後、導入を希望される場合、そのままの環境でご利用いただけます。

お申し込みはこちら
https://www.macnica.net/crowdstrike/test.html/

CROWDSTRIKE

macnica networks

マクニカネットワークス株式会社

本　　社　〒222-8562　横浜市港北区新横浜1-5-5　マクニカ第2ビル
TEL 045-476-2010　FAX 045-476-2050

西日本営業所　〒530-0005　大阪市北区中之島2-3-33　大阪三井物産ビル14階
TEL 06-6227-6916　FAX 06-6227-6917

お問合せはこちら
ＵＲＬ : https://www.macnica.net/crowdstrike/
Email : cs_sales@cs.macnica.net

2020年3月

©2020 Macnica Networks Corp.

●本書の仕様は予告なく変更する場合があります。
●本書に記載の社名及び製品名は、各社の商標または、登録商標です。

NGAV×EDR×脅威ハンティング
CrowdStrike Falcon
エンドポイント保護ソリューション

侵攻は、許さない

CROWDSTRIKE

macnica networks

従来型アンチウイルスでは サイバー攻撃を防げない

多様化する攻撃
- 標的型攻撃
- ファイルレス攻撃
- ゼロデイ攻撃

環境の変化
- テレワーク
- BYOD
- クラウドサービス利用

運用の限界
- 大量の過検知
- 対処にかかる膨大な時間
- 日々のメンテナンス負荷

これからは

NGAV×EDRで 脅威を撃破

NGAV：従来型アンチウイルスをすり抜ける未知のマルウェアやファイルレス攻撃の防御が可能

EDR：エンドポイントの操作を記録・監視し　詳細な調査・対処がリアルタイムで実施可能

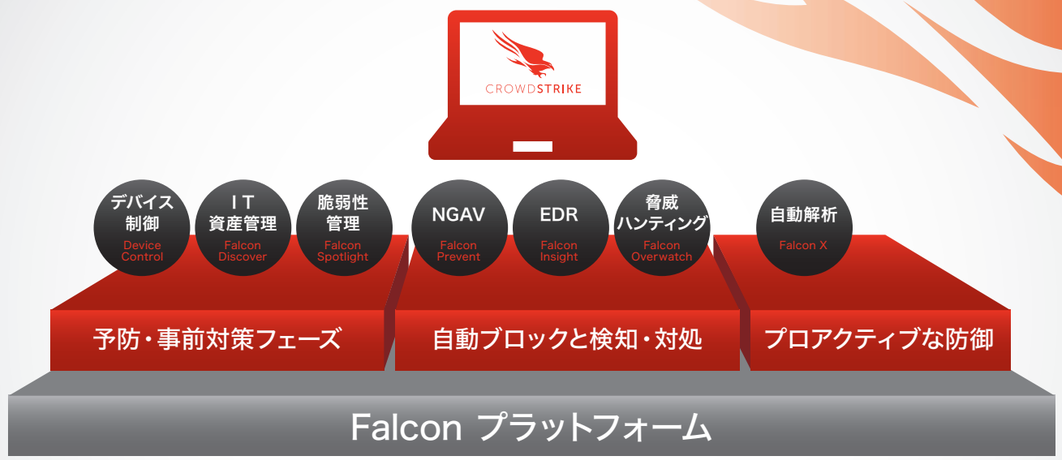
※NGAV=Next Generation AntiVirus、EDR=Endpoint Detection and Response

新たな時代のセキュリティを実現する

CrowdStrike Falcon

CrowdStrike Falconはクラウド型のエンドポイントセキュリティプラットフォームとして、
NGAV・EDRはもちろん、サイバー攻撃解析のプロ集団による脅威ハンティングサービス、
デバイス制御、資産管理までシングルエージェントで提供。
クラウドに最適化したシンプルなアーキテクチャで進化し続ける脅威への対策を実現します。

包括的なセキュリティ対策を実現する統合プラットフォーム



ホワイトハッカーが脅威をあぶり出す
世界最高クラスのサイバー攻撃解析のプロ集団が、環境に潜む高度な脅威を発見。
素早い対処を支援します。

脅威を発見し、確実に“ブロック”
EDRとNGAVの連携により、脅威の発見・通知から、ファイル隔離・プロセスキルまでシームレスに実現。

リアルタイムにログを収集・検知
エンドポイントのログをリアルタイムに収集。すべての振る舞いをリアルタイムで監視・分析し、攻撃を即座に検知します。

2019「ガートナーエンドポイント保護プラットフォームについてのマジック・クアドラント」でリーダーの評価

クラウドストライク社は、2019「ガートナーエンドポイント保護プラットフォームについてのマジック・クアドラント」でリーダーのうちの1社として、またビジョンの完全性において最上位のポジションに位置づけられました。

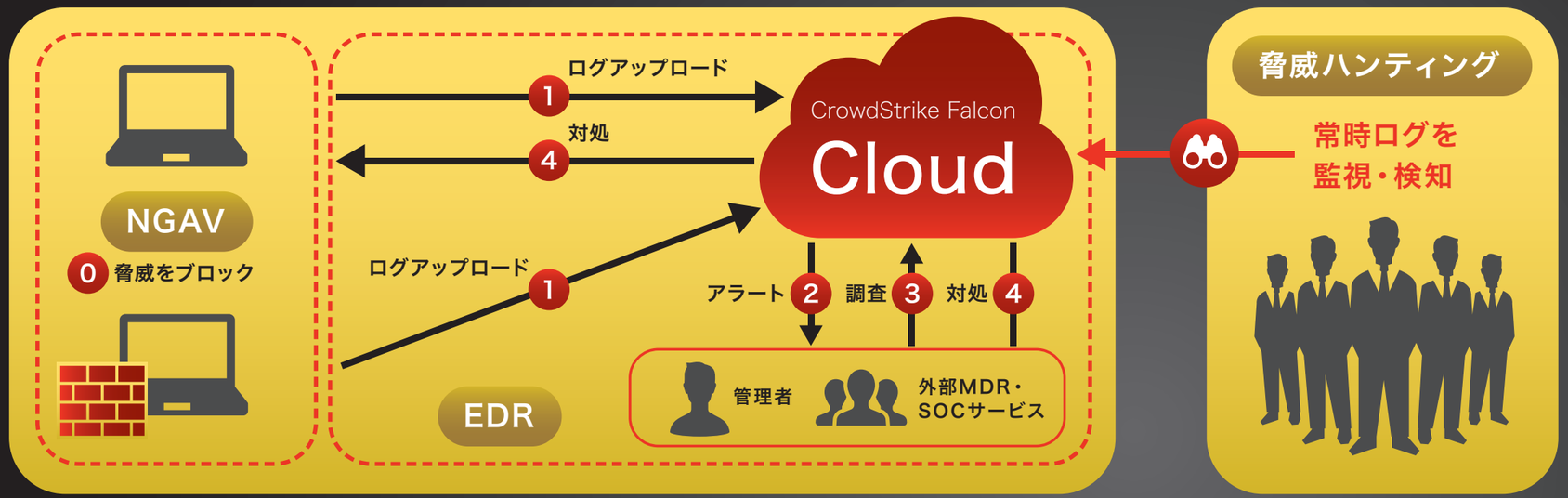
CROWDSTRIKE

※出典：Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook et al., 20 August 2019　※ガートナーは、ガートナー・リサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高のレーティング又はその他の評価を得たベンダーのみを選択するようにテクノロジーユーザーに助言するものではありません。ガートナー・リサーチの発行物は、ガートナー・リサーチの見解を表したものであり、事実を表現したものではありません。ガートナーは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の責任を負うものではありません。

Cloud × Crowd

クラウドプラットフォーム

人工知能を搭載した、クラウドネイティブな環境（Cloud）で、
世界中の攻撃・インシデント情報を集約し、”群衆”として（Crowd）脅威に立ち向かいます。



Point

詳細なログで徹底した原因調査が可能に

CrowdStrike Falconでは、詳細なログをもとに、操作・挙動をフローで確認できる画面などを提供。
「ログが不足し、原因が分からない」ことがなく、いつ・どこで・何が起きたかを迅速に究明できます。

機械学習で、未知の攻撃をブロック

Falcon Prevent **NGAV**

機械学習・AI・振る舞い検知などを組み合わせることで、従来型アンチウイルスでは見つけられない未知の攻撃も検知・ブロック。

- ファイルレス攻撃もブロック
- オフラインでも検知・ブロック
- 分かりやすいプロセスツリー

すべての振る舞いを記録し、攻撃を検知

Falcon Insight **EDR**

ログをもとに実際の挙動を監視することで、NGAVをすり抜けた攻撃を検知。ログはすべてクラウドにアップロードされるため、攻撃者によって端末内のログが削除されても、調査可能です。

- リアルタイムな生ログの可視化
- 攻撃者がログを削除できない保全性
- リモートから端末の隔離も可能

セキュリティのプロ集団

Falcon Overwatch 脅威ハンティング

すべて検知すると…
アラートが多すぎて運用負担が増加

検知をあきらめると…
脅威の侵入に気づけないリスクが増加

“人”が監視することで攻撃・脅威をピンポイントで発見

さまざまな対策をシングルエージェントで実現

Falconエージェント1つで、すべての対策が利用できます。エージェントは軽量で端末に負荷をかけず、
アンチウイルス製品のエージェントなどと併用することも可能です。

USBデバイスからの
感染・情報漏えい

抜け穴になりがちな
USBデバイスの挙動を制御する

デバイス制御
Falcon Device Control

Falconエージェントをインストールした端末に対し、USBデバイス利用状況の可視化・制御を実施。誰が・いつ・どんなデバイスを利用したかのログをリアルタイムに取得。利用禁止などのポリシーもまとめて設定できます。

- USBデバイス利用傾向を可視化
- ポリシーによる利用制御
- グループごとの管理も可能に

アプリの
無断インストール

社内IT資産の可視化を実現

IT資産管理
Falcon Discover

アプリケーション、端末、アカウントの3つの観点から、社内のIT資産状況を可視化。非管理端末やアプリケーションの利用状況、バージョン、エンドポイント環境をリアルタイムに可視化します。

- Falconの非管理端末を洗い出し
- アプリ利用状況の可視化
- 特権IDの利用状況なども明確に

脆弱性を把握
できていないリスク

脆弱性を
リアルタイムに可視化

脆弱性管理
Falcon Spotlight

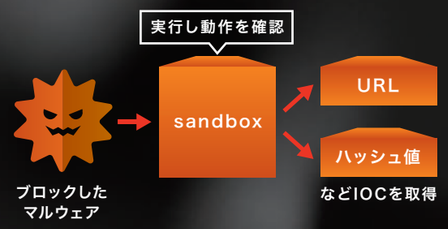
OSやサードパーティー製アプリケーションの脆弱性を収集・可視化。Falconエージェントのログを活用することで、ほぼリアルタイムの可視化を実現します。脆弱性を素早く検出し、パッチを適用することで、脆弱性を突く攻撃を防げます。

- リアルタイムに脆弱性を可視化
- パッチの配布状況を把握
- スキャン不要

インシデント発生後の
対応遅延

脅威インテリジェンスを活用し、
マルウェアの即時分析を実現する

自動解析
Falcon X



社内で発見されたマルウェアを、サンドボックスで解析することで、URLやHash値などのIOCを取得し、自社へ展開することでセキュリティの強化を実現します。

- ブロックしたマルウェアを動的解析
- 自動解析レポート
- IOCを自社環境に展開可能