CROWDSTRIKE FALCON:
エンドポイントプロテクションの新たなスタンダード

シンプルかつ強力なアプローチによるエンドポイントセキュリティ

CrowdStrike Falconの軽量エージェントと強力なクラウドがシームレスに連動し、エージェントがインターネットに接続していない場合でも、**リアルタイムのプロテクションと可視性を実現します。** CrowdStrike Falconは脅威を防止する堅固な機能を提供し、先進的な攻撃検知・対策機能に人工知能や機械学習を活用して脅威情報を統合します。こうした機能は、すべて高度に直感的な管理コンソールで提供しています。

なぜCROWDSTRIKEなのか?

完全なプロテクション

オンライン環境でもオフライン環境でも、マルウェア攻撃でもマルウェアを使わない攻撃でも、すべての攻撃を即座に、かつ効果的に検知して防止します。

群を抜く可視性

エンドポイントの"DVR"となる本製品は、何ひとつ見逃しません。その時点のエンドポイントの動作状況や動作の履歴を数秒で検出し、調査することができます。

究極の使い易さ

1つのクラウドによるプラットフォームは、導入、設定、保守が簡単です。すべて単体の軽量エージェントを利用して実現しています。

十分にテストされた、実績のあるCROWDSTRIKE

既知の攻撃であれ、未知の攻撃であれ、マルウェア攻撃であれ、マルウェアを使わない攻撃であれ、CrowdStrikeを利用すれば、サイバー攻撃から組織を確実に守ることができるようになりました。これは当社が主張しているだけの話ではありません。セキュリティのエキスパートたちも、CrowdStrike Falconについて次のように語っています。

"先見の明"

– Gartner エンドポイントプロテクションプラットフォームマジッククアドラント – 2017年1月

"優良企業"

– Forrester Wave: エンドポイント セキュリティ スイート – 2016年10月

"定評あるビジネスセキュリティ製品"

AV comparatives

– AV Comparatives – 2016年12月

CROWDSTRIKE 本社

15440 Laguna Canyon Road, Suite 250, Irvine, California 92618, U.S.A | (888) 512-8906

info@crowdstrike.com | sales@crowdstrike.com | crowdstrike.com

セキュリティ侵害でお困りですか? お問い合わせはこちらへ (855) 276-9347 または services@crowdstrike.com

CROWDSTRIKE

セキュリティ侵害を防止する革新的システム

クラウドで実現するエンドポイントプロテクション

CROWDSTRIKE FALCON:
"不可能"を可能に

これまで、ユーザのパフォーマンスに影響を与えずに、たった1つの軽量エージェントで完全なエンドポイントプロテクションを実現することなど、不可能だと言われてきました。しかし、当社はこの定説を覆しました。CrowdStrike Falconは、これまでにないリアルタイムの可視性とセキュリティ侵害の防止と封じ込めを実現し、**以下のことを可能にしたのです。**

- 攻撃にマルウェアが使われているかどうかに関わらず、エンドポイントがオンラインでもオフラインでも、一般的な攻撃、巧妙な攻撃のいずれからも保護することが可能。
- 環境内のどこで稼動するアプリケーションやプロセスに対しても可視性や鑑定機能を提供し、何ひとつ見逃さず、必要な対策をすべて実施することが可能。
- 進化した脅威の挙動をより速く、より効果的に見つけ出し、事前に捕らえることが可能。
- Windows、OS X、Linuxなどのエンドポイント、データセンター・サーバ、仮想マシン、さらにはAWS、AzureやGoogleなどのクラウドプラットフォームといった、最先端のプラットフォームのエンドポイントを保護。
- 既存のアンチウィルスをリプレイスし、効果的なアンチウィルスシステムとして、独自にテストされ、認知された次世代ソリューションを導入可能。

CrowdStrike Solutions Overview

FALCON DISCOVER
ITの予防措置
Falcon Discoverは、未承認のシステムやアプリケーションが環境内のどこにいても、リアルタイムで識別し、より迅速に対処することでセキュリティの体制を向上します。

FALCON PREVENT
次世代アンチウィルス(NGAV)
Falcon Preventは、マルウェア攻撃からも、マルウェアを使わない攻撃からも、環境を保護します。第三者機関によってテストされ、認証されているため、既存のアンチウィルスのリプレイスとして利用することができます。

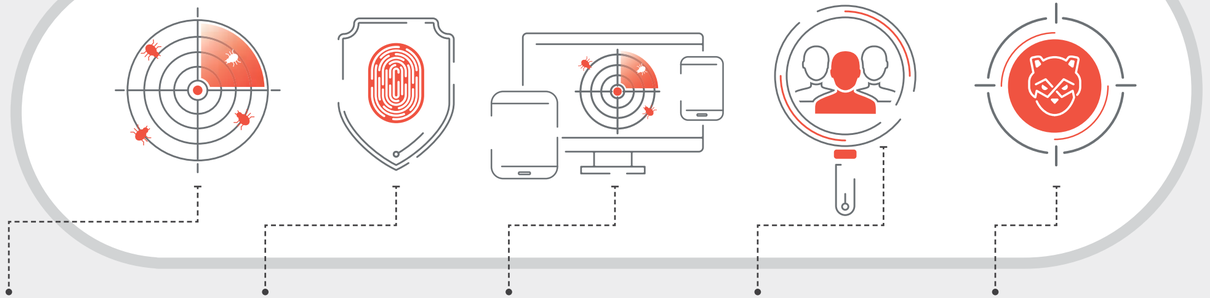
FALCON INSIGHT
エンドポイントでの検知と対応(EDR)
Falcon Insightは、検知、対応、フォレンジックを通じて、継続的で総合的なエンドポイントの可視性を提供し、何ひとつ見逃さずに、セキュリティ侵害を引き起こす恐れのある挙動を阻止します。

FALCON OVERWATCH
組織化された脅威ハンティング
24時間対応のFalcon OverWatchチームが、お客様のセキュリティ担当チームの一員として、悪質な活動をできるだけ早い段階で検出し、攻撃者の動きを阻止します。

FALCON INTELLIGENCE
脅威インテリジェンス
Falcon Intelligenceは世界中の攻撃者の活動を追跡し、全体的なセキュリティ体制を簡単に向上することのできる、カスタマイズされたアクショナブルレポートと分析結果を提供します。

クラウドで実現するエンドポイントプロテクション

FALCON PLATFORM



ITの予防措置
組織はあらゆる攻撃に備える必要があります。しかし、認識できない問題を解決することはできません。管理下にあるかどうかに関わらず、すべてのエンドポイントを認識し、環境内で稼動するアプリケーションがどこにあっても、そのすべてをリスト化し、脅威を生む可能性のある活動を即座に識別して排除するために、組織には完全なリアルタイムの可視性が必要です。

次世代アンチウィルス(NGAV)
マルウェア攻撃、マルウェアを使わない攻撃のいずれからも環境を守るために、機械学習やエクスプロイトブロッキング、攻撃のインジケータを捕らえる先進的な振る舞い分析などのさまざまな保護技術を兼ね備えた、総合的で実績のある次世代アンチウィルスが必要です。

エンドポイントでの検知と対応(EDR)
継続的で総合的な EDR には、その時点のエンドポイントの挙動とそれまでの履歴を 5 秒で検出する機能があります。この機能によって、エンドポイントで起きている事象を把握し、何ひとつ見逃さずに、攻撃者を確実に見つけ出すことができます。

組織化された脅威ハンティング
最も先進的な防御技術を導入したとしても、十分とはいえません。巧妙な攻撃者に打ち勝つためには、侵入を防ぐエキスパートの専任チームがプロアクティブに 24 時間対応で不審な挙動に目を光らせ、「クラウドの力」を活用して、台頭する新たな脅威を識別する必要があります。

脅威インテリジェンス
知らないものは守れない、ということは、リスクがあるということです。脅威インテリジェンスなら、攻撃者の動機を明らかにし、攻撃手法を予測して、効果的な対策を実施して組織への侵入を防ぐことができます。

CrowdStrike のサービス

インシデント対応サービス
CrowdStrikeは問題発生前後の総合的なインシデント対応(IR)サービスを24時間対応で提供し、セキュリティ侵害の発生前、発生中および発生後のサポートを実施しています。非常にスキルの高いサポートチームが、お客様のセキュリティインシデントを防ぎ、対策を取るためのサービスを提供して、セキュリティ侵害を予防し、対応するスピードを最適化します。

プロアクティブサービス
CrowdStrikeのサービスチームは、お客様と協同して脅威を予測し、侵入を阻止すべくネットワークを整備し、サイバー攻撃によるダメージを防ぐためにお客様がスキルを磨くお手伝いをします。プロアクティブサービスは、総合的な査定、次世代の侵入テストと机上演習に加え、IRとSOC（セキュリティオペレーションセンター）の開発プログラムを提供しています。