NGAV×EDR×脅威ハンティング

進化し続ける脅威への Best Answer

CROWDSTRIKE FALCON

止められないシステムに 安心を。

Thelemaassist

なぜ従来型アンチウイルス製品のままではいけないのか？

環境の変化

- リモートワークの増加
- 海外拠点数の増加
- 暗号化通信の主流

攻撃者の変化

- 標的型攻撃
- ビジネスメール詐欺
- ランサムウェア

従来型アンチウイルスでは
阻止できない脅威が増えている！！

NGAV×EDR× 脅威ハンディングで脅威から守る

攻撃者もセキュリティ製品の抜け道を研究しています。
日々新しく生み出される脅威の対策として
Falcon Prevent（次世代型アンチウイルス）、
Falcon Insight（EDR）、Falcon Overwatch（脅威ハンティング）を
導入することにより、運用負荷を最小限にエンドポイントの
セキュリティを強化が可能です。

CROWDSTRIKE FALCON

CrowdStrike Falcon は侵害防止に焦点を絞って設計されたCrowdStrikeプラットフォームです。１つのプラットフォームで、PC 端末、サーバやモバイル、様々な環境をカバーすることができます。複数の管理コンソールは必要ありません。

FALCON PLATFORM

1つのプラットフォームですべての環境をカバー

セキュリティを守るのに複数のエージェント、複数の管理コンソールはもう必要ありません。

CrowdStrikeの特徴

容易な導入・運用

管理サーバーはクラウドサービスとして提供されるため、構築は不要で、自動的にアップグレードされ、再起動は不要です。

エンドポイントセキュリティプラットフォーム

USB 制御、脆弱性管理、IT資産管理や自動解析などエンドポイントセキュリティにかかわる様々な機能をシングルエージェントで実現。

軽量と負荷

様々な機能は 1 つのエージェントで実現可能です。また、ディスクに書き込むデータは数十 MBと軽量であり、稼働時の CPU 使用率は1% 未満と端末やネットワーク環境の負荷も高めません。

従来型アンチウイルス製品の課題点

①検知・防御が不可能な攻撃の台頭
②不明瞭で特定困難な侵入経路
③感染時に立ちはだかる対処・復旧の壁
④業務に支障をきたす運用と端末負荷

次世代型アンチウイルス製品 (NGAV) で課題を解決！！

①多様な検出方法による検知・ブロック能力
②インシデント状況とマルウェア挙動の可視化
③軽量なエージェントとメンテナンス不要のクラウド環境

NGAV
Falcon Prevent

シグネチャを利用しない機能学習により既知・未知のマルウェアを検知。

◆オフラインでも検知・ブロック
◆ファイルレス攻撃を防御
◆軽量エージェント

EDR
Falcon Insight

EDR が振る舞いを見て、自動的に怪しいと判断したものを検知。

◆リモートから端末の隔離可能
◆完全なリアルタイムの可視性
◆攻撃者が痕跡を消した場合も行動を全て把握可能

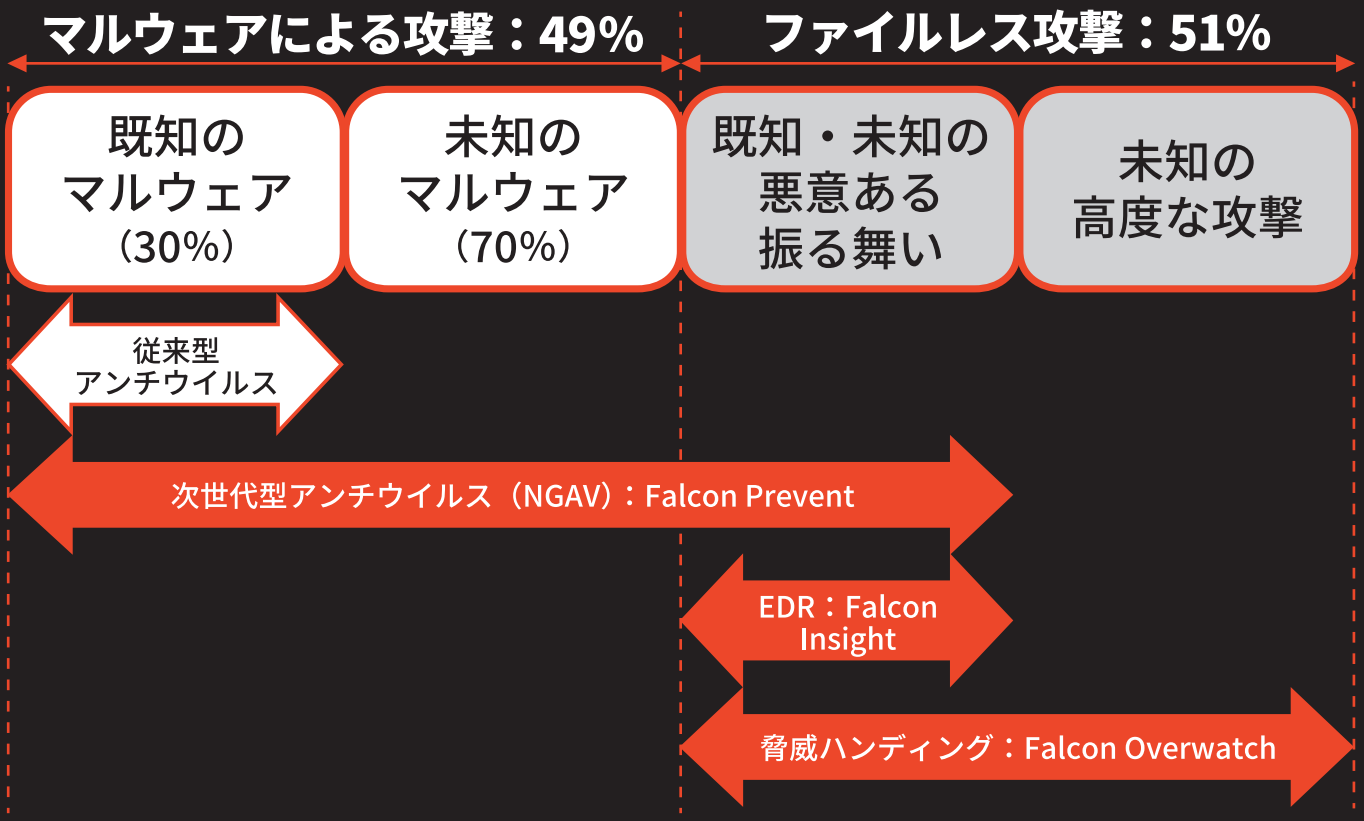
脅威ハンディング
Falcon Overwatch

プロフェッショナルが、24 時間 365 日振る舞いを監視し、EDR で検知できないような高度な攻撃を検知。

従来型アンチウイルスで守ることができるのは全体の攻撃の半分以下！

従来型アンチウイルス

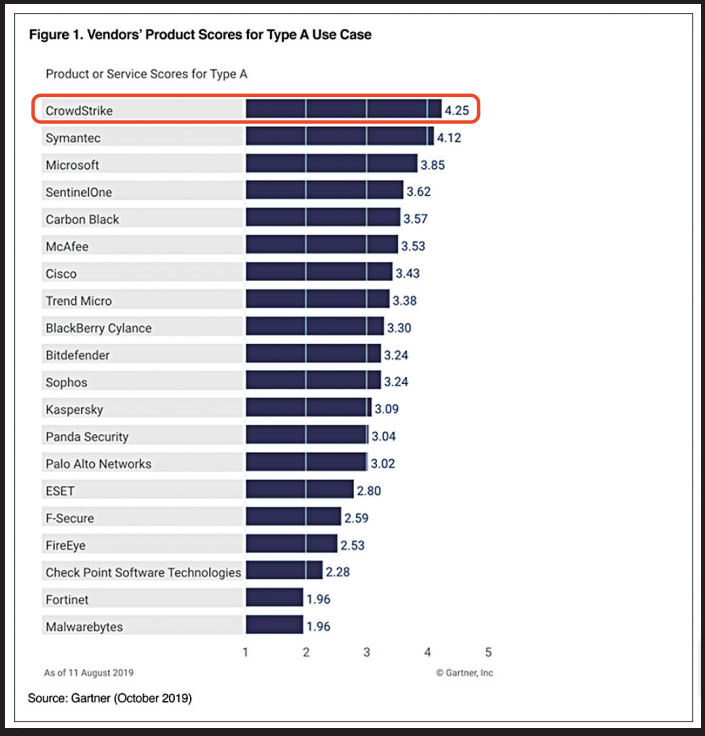
CrowdStrike Falcon



※割合は、2020 CrowdStrike グローバル脅威レポートより抜粋。Crowdstrike.jp/gtr よりダウンロード可能。

CrowdStrikeは高く評価されています！！

CrowdStrikeおよびATPについて Gartner 社の第三者評価においても高い評価を得た実績のある製品となっています。



出典：https://www.crowdstrike.com/blog/crowdstrike-scores-highest-overall-gartner-critical-capabilities-epp-2019/

■EDR 製品比較

項目	観点	CrowdStrike	M社	T社	A社	C社	R社
機能要件	・価格最新の攻撃を検知できるか ・端末を隔離できるか ・AV 機能が包含されているか, など	◎	○ MAC、Linux 対応が弱	—	—	—	—
展開負荷	・Agent の配布・展開が容易か ・既存 APとの相性など	○	◎ 国内有効化のみ / ○ 海外	○	○	○	○
運用負荷	・一部拠点での導入実績があるか	◎ 既存一元運用窓口の拡張が可能 一部拠点導入済	◎	△ IT 運用が必要	○	○	○
コスト	・ライセンスの有効活用が可能か ・ボリュームディスカウントなど	○	◎ 国内ライセンス保有 / △ 海外必要	△ 要サーバ構築運用	○	○	○

製品比較の観点から、**CrowdStrikeが最適**と考えます。

セレマアシストができること

ライセンス販売

・公式販売パートナーとしてのライセンス販売可能

導入支援

・お客様の環境に合わせた設計、構築、展開が可能

運用支援サービス

・弊社の運用センターの中でサポート
・専門的なセキュリティ知識を持つ技術者の提供
・標準的な運用資料の提供

セレマアシストによるCrowdStrike Falcon導入事例

	A社	B社	C社
ライセンス販売	×	○	×
導入支援	○	○	○
運用支援	○	○	×
導入台数	8,000台	100台	5,000台
期間	150日	90日	120日

HIGH QUALITY SYSTEM OPERATION AND MANAGEMENT

お問い合わせはこちら

https://thelemaassist.com/contact/

Thelemaassist

株式会社セレマアシスト

本　社　〒553-0003　大阪府大阪市福島区福島 1-4-40 JBSL 梅田ビル 9F

TEL.06-4797-6464　　FAX.06-4797-6465

東京事業所　〒101-0041 東京都千代田区神田須田町 2-25-16
日宝秋葉原ビル 11F

TEL.03-6285-2930

06-4797-6464 受付（平日 9:00 ～ 18:00）

URL : https://thelemaassist.com/