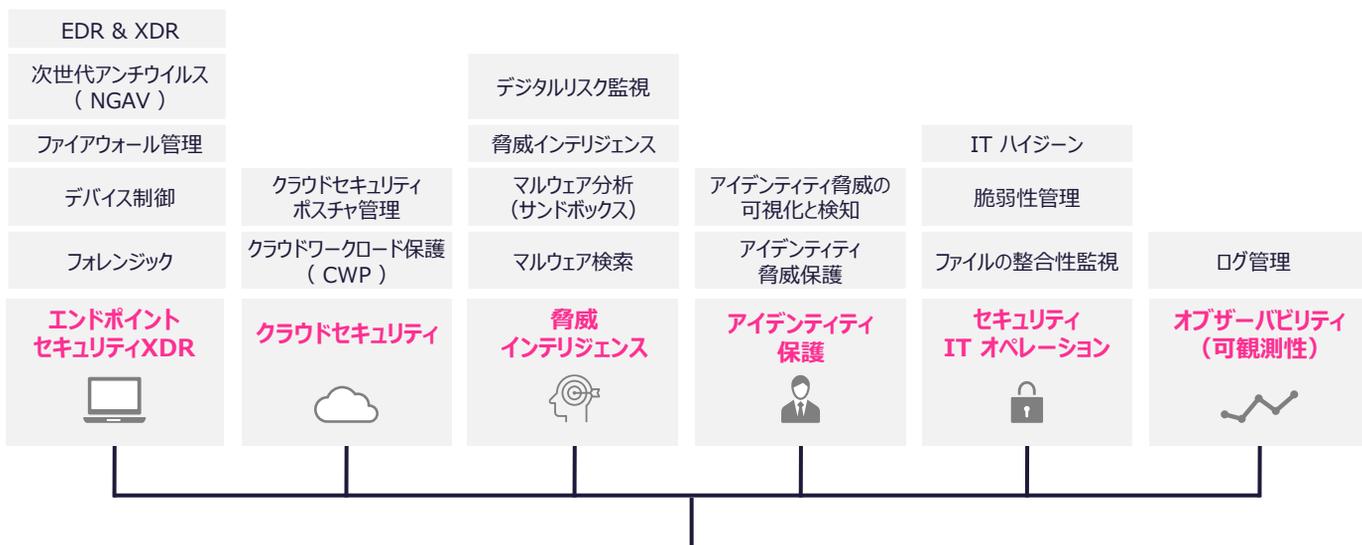


CROWDSTRIKE

リモートワークやクラウドサービスの利用拡大が進んでいる中で、昨今エンドポイントを狙うサイバー攻撃が高度化そして巧妙化していますクラウドストライクは、次世代アンチウイルス（NGAV）とエンドポイントでの検知と対応（EDR）、デバイス制御、脆弱性評価、IT 衛生管理が一体化された、クラウドで提供されるソリューションです。新しい攻撃手法対策として、セキュリティ侵害を効果的に検知・防御します。

1つのプラットフォームで様々なセキュリティの課題を解決します



Falcon Platform のサービスでまとめて解決！

脅威ハンティング

MDR

インシデント対応

アドバイザリーサービス

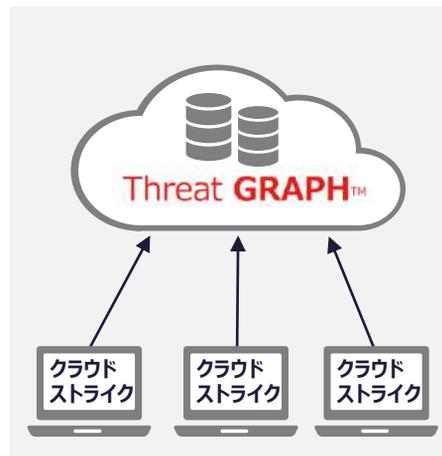
従来型と次世代型のアンチウイルスの機能の違い

	従来型アンチウイルス	次世代型アンチウイルス
新しい攻撃への対処能力向上 (ファイルレス攻撃・正規のアプリケーションを悪用)	×	○ 定義ファイルで検出できない脅威への対応
リアルタイムな振る舞い分析による脅威の検出	×	○
検知時の詳細状況把握	×	○ 侵入経路の特定、振る舞いの状況
定義ファイルの更新	必要 定期的な更新が必要	不要 定義ファイルなし
定期的なスキャン	必要 最新の定義ファイルによるスキャン	不要
端末の負荷	高負荷	低負荷
端末の対処機能	抜線等必要 ユーザーの負担あり	即時隔離可能 管理者側から可能

クラウドストライク を選ぶ理由

1 クラウドネイティブ：常に最新の脅威情報で防御

高度化、巧妙化する脅威に素早く対処するためには、最新の脅威情報をいち早く共有するためのプラットフォームが必要不可欠です。クラウドストライクはプラットフォームをクラウド化することで、全世界176 개국以上のユーザーからの膨大なログ(1日10億以上)をリアルタイムに収集・解析しています。これにより、最新の脅威からの素早い保護を実現しています。セキュリティ業界最大のクラウド分析プラットフォームである Threat Graph を利用することで、過検知・誤検知の少ない高精度な防御を実現することが可能となっています。



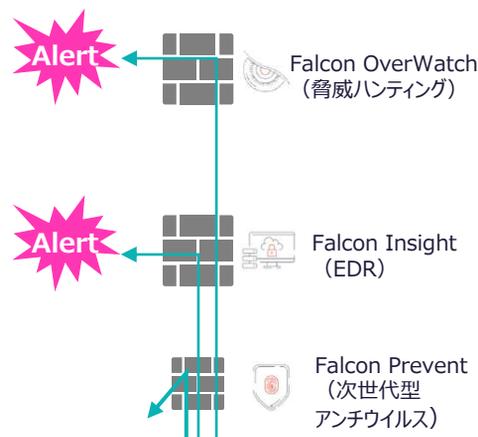
2 シングルエージェント：管理者と PC への負荷を大幅に軽減

次世代型アンチウイルス / EDR ほか様々なモジュールが、1つのエージェントとして機能し、エンドポイントがオフラインの時にも保護を提供します。軽量なエージェントであるので、エンドポイントの本来のパフォーマンスを妨げることなく監視を行い、然るべきタイミングで防御を実現します。単一の機能を持つセキュリティ製品を複数導入する場合(マルチコンソール)と比べ、ブラウザのシングルコンソール上で管理が完結するため、管理者にとって運用、管理、機能拡張が簡単です。



3 脅威ハンティング：セキュリティの専門家・プロによる 24 時間 365 日監視

次世代型アンチウイルス / EDR でも防御しきれない、さらに高度な侵入に対しては、いかに早く攻撃を検知するかが重要になります。元 FBI やホワイトハッカーなど、セキュリティの専門家・プロが 24 時間 365 日体制で監視を行い、Threat Graph から解析された最新の脅威情報を基に高度な攻撃の検知、影響範囲の調査、対処法のアドバイスを行います。10 年以上の実績がありますが、脅威ハンティング由来の過検知、誤検知は今までで一回もありません。



アイビーシー株式会社

本社

〒104-0033
東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780 fax.03-5117-2781

西日本
事業所

〒532-0003
大阪府大阪市淀川区宮原4-1-14 住友生命新大阪北ビル3F
tel.06-7653-1014 fax.06-7177-0542