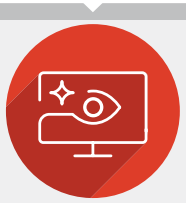
CROWDSTRIKE

FALCON DISCOVER
CROWDSTRIKE IT HYGIENE (ハイジーン) ソリューション

ネットワーク上につながる全てのエンドポイントをリアルタイムに可視化。どんなシステムが存在し、どのようなアプリケーションが使われているのか、どのユーザーアカウントが使われたのか、などの全体像を即座に把握できます。



FALCON DISCOVER：
リアルタイムでシステムやアプリケーションを可視化

セキュリティ担当者は、まずはネットワークにつながるコンピューターやアプリケーションを把握していなければなりません。Falcon Discover™は、そういった方々のための CrowdStrike™の IT Hygiene ソリューションです。Falcon Discover はシステム、アプリケーションの利用状況やユーザーアカウントの利用状況をリアルタイムに可視化し、インベントリーを作成します。

誰がネットワークにアクセスしているのかを常時監視 ― リアルタイムのシステムインベントリーは、環境内にある全ての管理されているデバイスだけでなく、管理されていないデバイスも シンプルなダッシュボードにまとめて表示することができます。それぞれにドリル・ダウンのメニューがあり、さらに詳細情報も表示できます。

ユーザーが利用しているアプリケーションを全て把握 ― リアルタイムのアプリケーションインベントリーによって、「今、この瞬間に」どこでどんなアプリケーションが走っているのかを知ることができます。また、そのデータからアプリケーションの使用率を可視化することで、無駄なアプリケーション・ライセンスの削減提案もできるようになります。

ユーザーのアカウントがどこで、どのように使われたかを確認 ― アカウントモニタリング機能によって、Admin の権限がどこで使われたのか、パスワードはいつ変更されたのか、などを監視できます。は企業内の管理者のクレデンシャルやパスワードのリセットを可視化します。Falcon Discover によって得られるデータにより、クレデンシャルが使われた場所などのログオンの傾向（アクティビティ／期間）に関する詳細情報や、パスワードの更新の状況が明らかになります。

主な特長

- システムやアプリケーションの状況を、リアルタイムおよび過去に遡って可視性できます
- 脅威からシステムを守るためのより良い準備を可能にします
- 無許可のコンピューターを即座に発見します
- 保護されていないシステムを検出できます
- ユーザーがどんな アプリケーションを使用しているかを知ることができます
- 特権アカウントのアクセスがいつどこで起きているかを知ることができます

製品の主な機能

まずは守る対象を知ることで脅威に向き合う準備を

- **まずは守る対象の確認から** — Falcon Discover を使って、今何が実際に利用されているかを可視化しましょう。 Falcon Discover のレポート機能によって環境内にある無許可のシステムやアプリケーションを報告できるため、攻撃を受ける前に効果的な対策を打つことができます。
- **不適切なアプリケーションや脆弱なアプリケーションを検出** — パッチを当てていないアプリケーションや脆弱なアプリケーションが使われていれば、それらを検出して、攻撃者に利用される前にパッチを当てることができます。
- **管理されていないシステムや無許可のシステムの発見** — システムインベントリーにより、未管理のシステムを救済し、保護されていない BYOD のシステムやサードパーティのシステムなど、ネットワークのリスクとなりかねないシステムにも対処することができます。
- **特権アカウントの悪用を防止** — Admin 権限の利用を常時監視し、もし不適切な使用やおかしな動きがあれば、それらを検出します。

セキュリティを超えて

- **アプリケーション・ライセンスのコストを削減** — リアルタイムのアプリケーションインベントリーにより、ユーザーがアプリケーションを使う頻度や期間が確認でき、実際のニーズに合わせてライセンスコストを調整することができます。
- **コンプライアンスの要件を満たす** — Falcon Discover は、いくつかのコンプライアンス要件に適合するよう、可視化とインベントリーを完全に自動化することにより、お客様がコンプライアンスの義務を果たし、それを維持して、証明するための支援を行います。

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 Discover 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。
- **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™ 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。

予防的セキュリティ、そしてその先へ

セキュリティの第一歩は、保護されていない環境を検出することから始まります。そうすることで不足している点を補い、脅威に対抗するための準備をすることができます。Falcon Discover は可視性を実現し、今日の巧妙な攻撃から環境を包括的に防御するための情報をセキュリティチームや IT チームに提供します。

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。