
CROWDSTRIKE
侵害はここで阻止
エンドポイント、
クラウドワークロード、
アイデンティティとデータ
全てをクラウドで保護

CrowdStrike Falcon

重要なリスク領域を保護：エンドポイント、クラウド、アイデンティティおよびデータ

ユーザーパフォーマンスに影響を与えずに単一の軽量エージェントを使用し、
完全なクラウドネイティブでの保護を提供することは不可能であると言われていました。
しかし、クラウドストライクはそれが誤りだということを証明しました。
クラウドネイティブの**CrowdStrike Falcon**プラットフォームはテクノロジー、インテリジェンス、
専門知識を独自に組み合わせ、エンドポイント、クラウドワークロード、アイデンティティ、データといった企業リスク
の重要な領域にわたって、包括的なエンドツーエンドのセキュリティを実現します。
CrowdStrike Security Cloudと一度収集したデータを何度も利用する軽量のFalconエージェントを活用し、
Falconプラットフォームはセキュリティ上のあらゆる課題に対応すると同時に、コストと複雑さを排除します。
Falconプラットフォームは成長を続け、業界をリードする保護を提供しています：

- エンドポイントセキュリティ、および拡張された検知と対応 (XDR)
- クラウドセキュリティ
- マネージドサービス
- 脅威インテリジェンス
- アイデンティティ保護
- セキュリティとITオペレーション
- 次世代SIEMとログ管理
- データ保護

Falconプラットフォームなら、迅速でスケーラブルな展開、優れた保護とパフォーマンス、複雑さの軽減、
そして即時の価値実現を達成できます。

包括的な保護でお客様にパワーを

脅威を自動的に予測し、リアルタイムで防御

単一の軽量エージェントアーキテクチャによってクラウド上に構築された**CrowdStrike Falcon®**プラットフォームは、
エンドポイントとクラウドワークロード、アイデンティティとデータなど、エンタープライズリスクの
最も重要な領域を保護します。**CrowdStrike Security Cloudを基盤とする**Falcon® プラットフォームは、
リアルタイムの攻撃の痕跡、脅威インテリジェンス、進化する攻撃者の手口、企業全体からの豊富なテレメトリを活用して、
超高精度の検知、自動化された保護と修復、精鋭による脅威ハンティング、優先付けされた脆弱性のオブザーバビリティ
（可観測性）を提供します。

クラウドストライクの特徴

Charlotte AI

Falconプラットフォーム全体のクラウドストライクの生成AI機能のポートフォリオを強化し、セキュリティ専門家によってさらに強化されたクラウドストライクのペタバイト規模の自動インテリジェンスを活用して、アナリストのワークフローを加速します。

単一の軽量エージェント

フリクションレスでスケーラブルな展開を可能にし、エージェントの肥大化とスケジュールされたスキャンを排除しながら、あらゆるタイプの攻撃を阻止します。

クラウドネイティブプラットフォーム

クラウドに収集されたセキュリティデータのネットワーク効果を活用し、煩雑なオンプレミスソリューションの管理負担を解消します。

CrowdStrike Asset Graph

今日の最も複雑なお客様の問題の1つを解決します。クラウド、オンプレミス、モバイル、IoTなど、すべてのシステムのアセット、アイデンティティ、構成を正確に識別し、それらをグラフ形式で接続します。

Falcon Foundry

お客様とパートナーは、Falconプラットフォームのデータ、自動化、クラウド規模のインフラストラクチャを活用して、最も困難なサイバーセキュリティの課題を解決するカスタムのノーコードアプリケーションを簡単に構築できます。

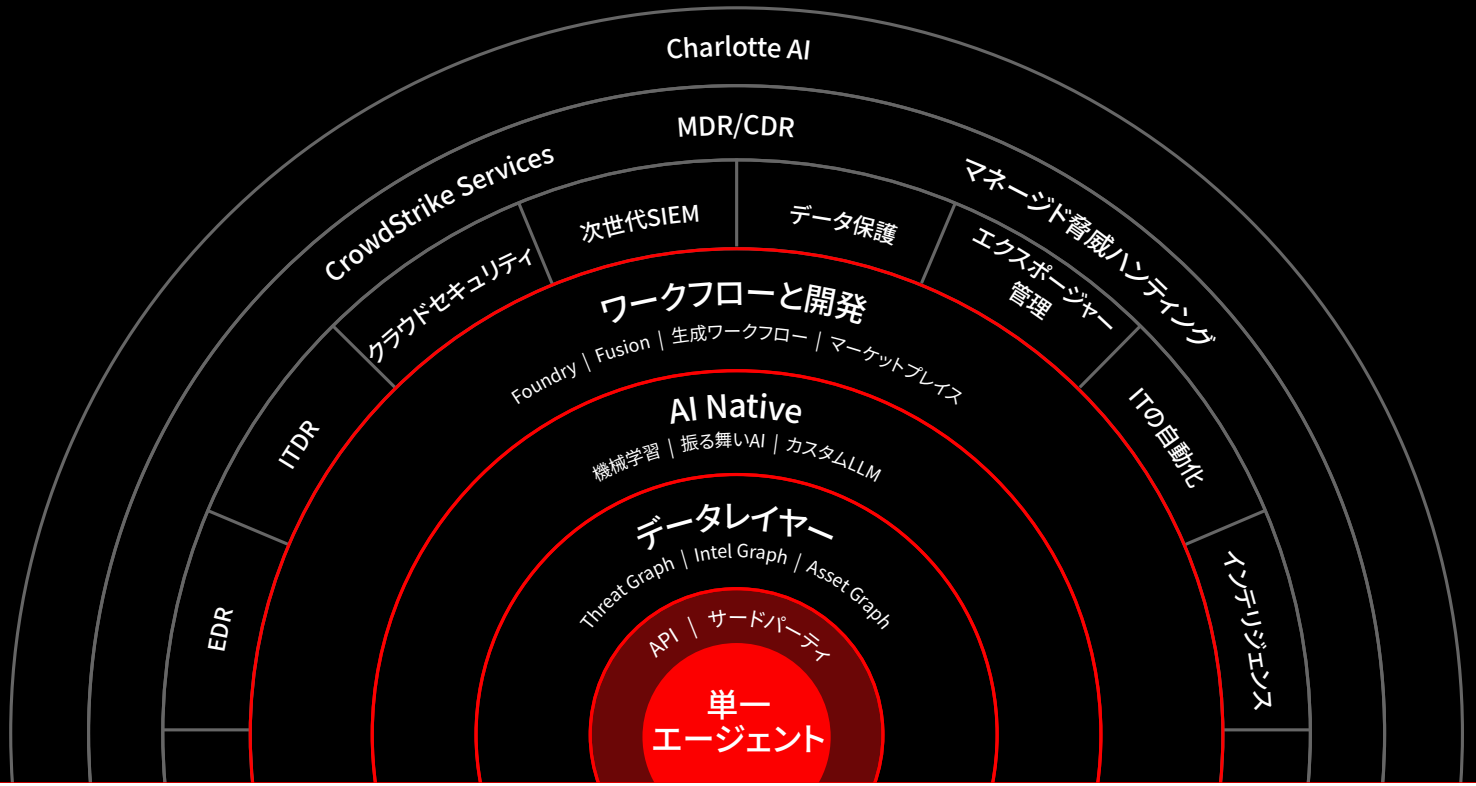
CrowdStrike Threat Graph

クラウドスケールの人工知能 (AI) を使用して、複数のテレメトリソースから得られる何兆ものデータポイントを相関付けし、攻撃者の戦術の変化を特定します。さらに、CrowdStrikeThreat Graph®**で攻撃戦術のマッピングを行い**、クラウドストライクの世界中のお客様の環境においてリアルタイムで脅威を自動的に予測して防御します。

Falcon Fusion

Falconプラットフォーム内で統合されたSOAR（セキュリティのオーケストレーション、自動化と対応）を提供し、コンテキストに富む強化されたデータを収集し、セキュリティ運用、脅威インテリジェンス、インシデント対応をすべて単一のプラットフォームで同じコンソールから自動化して、サイバー脅威と脆弱性を軽減できるようにします。

CrowdStrike Falconプラットフォーム



CROWDSTRIKE MARKETPLACE

クラウドスケールのオープンエコシステム

テクノロジーパートナーのエンタープライズマーケットプレイスを提供し、エージェントを追加したり、複雑さを増大させることなく、CrowdStrike Falconプラットフォームを拡張する信頼できるCrowdStrikeおよびパートナーアプリケーションを検出、試用、購入、展開できます。

CROWDSTRIKE UNIVERSITY

トレーニングと認定

CrowdStrike Falconプラットフォームの実装、管理、開発、使用に重点を置いたオンラインおよびインストラクター主導のトレーニングコースと認定資格を提供します。

クラウドストライクのゼロトラスト

デバイス、アイデンティティ、データの3つの重要なレイヤーでゼロトラスト保護をネイティブに適用し、リアルタイムの脅威防御とITポリシーの適用により、アイデンティティ、振る舞い、リスク分析を使用してエンドポイント、ワークロード、アイデンティティの侵害を阻止するフリクションレスのゼロトラストセキュリティを提供します。

単一のプラットフォームで完全な保護を提供

エンドポイントセキュリティ

FALCON PREVENT | 次世代アンチウイルス
マルウェアやランサムウェアから高度な攻撃まで、あらゆる種類の脅威から企業を防御。わずか数分で展開でき、即座にエンドポイント保護を実現します。

FALCON INSIGHT XDR | エンドポイントに留まらない検知と対応
業界をリードする統合型エンドポイントの検知と対応 (EDR) と拡張された検知と対応 (XDR) を提供し、企業全体を可視化し、エンドポイントとすべての主要な攻撃対象領域で攻撃者のアクティビティを自動的に検知し、対応します。

FALCON COMPLETE XDR | マネージド型の拡張された検知と対応 (MXDR)
Falcon CompleteのMDRサービスを、クロスドメインのXDR保護によって拡張したものです。クラウドストライクのグローバルエキスパートチーム、プロアクティブな脅威ハンティング、およびネイティブ脅威インテリジェンスによって強化されており、24時間365日のマネージド型保護を実現します。

FALCON FIREWALL MANAGEMENT | ホストファイアウォール
シンプルかつ一元化されたホスト型のファイアウォール管理機能で、ホスト型ファイアウォールポリシーの管理と適用を簡素化します。

FALCON DEVICE CONTROL | USBセキュリティ
組織全体でUSBデバイスを安全に使用するうえで必要となる可視性と精密な制御を実現します。

FALCON FOR MOBILE | エンドポイントでの検知と対応
iOSとAndroidデバイスを脅威から保護し、XDR/EDR機能をモバイルデバイスに拡張し、高度な脅威保護とアプリとネットワークアクティビティのリアルタイムの可視性を実現します。

脅威インテリジェンス

FALCON INTELLIGENCE | 自動脅威インテリジェンス
CrowdStrike Falconプラットフォームによって検知されたイベントとインシデントを活用して、インテリジェンスを自動化し、セキュリティ運用チームがより適切で迅速な意思決定を行えるようにします。

FALCON INTELLIGENCE PREMIUM | サイバー脅威インテリジェンス
ワールドクラスのインテリジェンスレポート、テクニカル分析、マルウェア分析、脅威ハンティングのための能力を提供し、組織がサイバーレジリエンスを築き、国家主導、eCrime (サイバー犯罪)、ハクティビストなどの攻撃者グループからより効果的に防御できるようにします。

FALCON INTELLIGENCE ELITE | 担当のインテリジェンスアナリストの配置
貴社を狙う攻撃に対する防御を使命とする、クラウドストライクの脅威インテリジェンスアナリストへのアクセスを提供し、Falcon® Intelligence Premiumへの投資を最大限にご活用いただけます。

FALCON INTELLIGENCE RECON | デジタル脅威監視
オープンウェブ、ディープウェブ、ダークウェブのすべてで悪意のある活動を監視し、ブランド、従業員、機密データの保護を一層強化します。

FALCON INTELLIGENCE RECON+ | マネージド脅威監視
クラウドストライクの専門家が、犯罪アンダーグラウンド全体の脅威の監視、トリアージ、評価、軽減を管理します。

FALCON SANDBOX | マルウェア分析
すべてのファイル、ネットワーク、メモリ、プロセスアクティビティに関する詳細なインサイトにより、マルウェア攻撃のライフサイクル全体を明らかにし、わかりやすいレポート、実用的なIOC、シームレスな統合を提供します。

マネージドセキュリティ

FALCON COMPLETE | マネージド検知と対応 (MDR)
専門家による管理、監視、外科的修復、プロアクティブな脅威ハンティングおよび統合脅威インテリジェンスを24時間365日体制で提供し、脅威をわずか数分で阻止し、根絶します。

FALCON OVERWATCH™ | マネージド脅威ハンティング
サイバーセキュリティの専門家チームと提携して、Falconプラットフォーム内でハンティングを実施。攻撃のささいな痕跡をも探し出して、攻撃者の逃げ場を奪います。

FALCON OVERWATCHTM ELITE | 担当のマネージド脅威ハンティングアナリスト
クラウドストライクの脅威ハンティングアナリストがチームを拡張し、専任の専門知識、脅威の状況に関する戦術的な日々のインサイトや戦略的なアドバイザリーを提供して、継続的な改善を推進します。

COUNTER ADVERSARY OPERATIONS ELITE | 専任の脅威ハンティングアナリスト
インテリジェンスを搭載した高度な調査および脅威ハンティングツールを使用して、IT環境内外の敵対者を特定して遮断する専任のアナリストを提供します。

クラウドセキュリティ

FALCON CLOUD SECURITY
AWS、AZURE、GCP全体で脅威インテリジェンス、検知と対応、ワークロードランタイム保護、クラウドセキュリティポスチャ管理などの侵害に対抗する保護を提供します。

FALCON CLOUD SECURITY FOR CONTAINERS
クラウドとコンテナのセキュリティと侵害保護を提供します。クラウドセキュリティポスチャ管理、オンプレミス、ハイブリッド、マルチクラウド環境における脅威の検知と対応、コンテナセキュリティとKubernetes保護を含むクラウドワークロード保護を実現します。

FALCON CLOUD SECURITY FOR MANAGED CONTAINERS
脅威インテリジェンス、検知と対応、コンテナイメージセキュリティ、Kubernetes保護など、クラウドとコンテナのセキュリティを提供します。

FALCON OVERWATCH™ クラウド脅威ハンティング | マネージドサービス
複雑なクラウドIOAや設定ミスの痕跡 (IOM) を伴う独自のクラウド攻撃経路から、AWS、Azure、Google Cloud Platformなどの重要なクラウドインフラストラクチャにおける巧妙に隠蔽された攻撃者の活動まで、クラウドの脅威を明らかにします。

FALCON COMPLETE CLOUD SECURITY | クラウドワークロード用MDR
クラウドワークロード向けに24時間365日体制の専門家によるセキュリティ管理、脅威ハンティング、監視と対応を提供する完全にマネージドなクラウドワークロード保護サービスを提供します。

セキュリティとIT運用

FALCON DISCOVER | ITハイジーン
環境内の各所に潜む不正なアカウントやシステム、アプリケーションをリアルタイムで特定し、即座に可視化できるようにして組織全体のセキュリティポスチャを改善します。

FALCON SPOTLIGHT | 脆弱性管理
自動化された包括的な脆弱性管理ソリューションをセキュリティチームに提供し、膨大なリソースを要するスキャンなしで、迅速な優先順位付けと統合化された修復ワークフローを可能にします。

FALCON EXPOSURE MANAGEMENT | エクスポージャー管理
セキュリティチームは、最大の影響を及ぼすエクスポージャーの優先順位を上げて、攻撃者の侵害やラテラルムーブメントの機会をプロアクティブに減少させることができます。

FALCON SURFACE | 外部攻撃対象領域管理
インターネットに接続するすべてのアセットを継続的に検出してマッピングし、ガイド付きのリスク軽減計画を使用して潜在的なエクスポージャーを排除することで、攻撃対象領域を削減します。

FALCON DATA PROTECTION | 統合データ保護
機密データで何が起きているかをリアルタイムで詳細に可視化し、ファイルではなくコンテンツを自動的に追跡するポリシーの適用により、データの盗難を阻止します。

FALCON FILEVANTAGE | ファイル整合性監視
包括的かつ一元化された可視性をリアルタイムで提供し、コンプライアンスを強化し、関連するコンテキストデータを提供します。

FALCON FORENSICS | フォレンジックサイバーセキュリティ
サイバーセキュリティインシデントの強力な分析のために、特定の時点および過去のフォレンジックトリアージデータの収集を自動化します。

FALCON FOR IT | 自動化ワークフロー
Falconプラットフォームを拡張し、エンドツーエンドの可視性からアクションまでのライフサイクルでITおよびセキュリティワークフローを自動化します。

アイデンティティ保護

FALCON IDENTITY THREAT DETECTION
AIと振る舞い分析を活用して、ランサムウェアなどの最新の攻撃を阻止するための深い実用的なインサイトを提供し、アイデンティティベースの脅威をリアルタイムで超高精度に検知できるようにします。

FALCON IDENTITY THREAT PROTECTION
高度なAI、振舞い分析、柔軟なポリシーエンジンを組み合わせてリスクベースの条件付きアクセスを適用することで、超高精度の脅威の検知とアイデンティティベースの攻撃のリアルタイム阻止を可能にします。

FALCON COMPLETE IDENTITY THREAT PROTECTION
フルマネージドのアイデンティティ保護ソリューションを提供し、クラウドストライクのエキスパートチームにより24時間365日体制でアイデンティティ脅威阻止、ITポリシーの適用、監視、および修復をフリクションレスかつリアルタイムで提供します。

次世代SIEM

FALCON LOGSCALE |SIEMとログ管理 業界をリードする検知、ワールドクラスのインテリジェンス、超高速検索、AI主導の調査を1つのクラウド配信プラットフォームに統合することで、攻撃者を迅速にシャットダウンし、SOCコストを削減できます。

CROWDSTRIKE SERVICES

インシデント対応 (IR) サービスを24時間365日体制で提供し、侵害の発生前、発生中、発生後にわたってサポートします。
熟練したチームがセキュリティインシデントからの保護と対応、侵害の防御、および修復速度の向上を支援します。

準備：アドバイザリーサービス

現実をシミュレーションした演習により、
高度な脅威アクターに対する防御の準備を支援します。

- 机上演習
- 攻撃者エミュレーション演習
- レッドチーム / ブルーチーム
- ペネトレーションテスト

対応：侵害サービス

侵害を阻止し、インシデントを調査し、
迅速かつ外科的精度で攻撃からの回復を支援します。

- インシデント対応 (DFIR)
- エンドポイント復旧
- 侵害調査
- 対攻撃者エクスポージャー評価
- ネットワークセキュリティ監視

強化：アドバイザリーサービス

防御を強化するための実用的な推奨事項により、
サイバーセキュリティポスチャの強化を支援します。

- サイバーセキュリティ成熟度評価
- クラウドセキュリティ評価
- テクニカルリスク評価
- SOC評価
- ADセキュリティ評価
- サイバーセキュリティ改善プログラム
- セキュリティプログラム詳細評価

クラウドセキュリティサービス

クラウドデータ侵害からの復旧とクラウドプラットフォーム構成の保護を支援

- クラウドのインシデント対応
- クラウドセキュリティ評価
- クラウド侵害調査
- レッドチーム / ブルーチームクラウド演習
- クラウドセキュリティ向けのFALCON運用サポートサービス

テクノロジーサービス

組織の保護強化を支援

- エンドポイントセキュリティサービス
- アイデンティティ保護サービス
- ネットワーク監視サービス
- ログ管理サービス
- FALCON運用サポートサービス
- FALCONゴールドスタンダード

クラウドストライクの業界における評価

クラウドストライクを導入することで、マルウェアの有無や、既知・未知を問わず、
サイバー攻撃から組織を完全に保護することができると確信しています。
業界アナリストによるクラウドストライクの評価をお聞きください。

- 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms（EPP）でリーダーおよびビジョンの完全性で最高位のセキュリティベンダーに選出されました。
- 2023 Frost & Sullivan Radar™ for CNAPPでリーダーに選出
- 2023 Frost & Sullivan Radar™ for CWPPでリーダーに選出
- 「The Forrester Wave™: Endpoint Security, Q4 2023」でリーダーに選出
- 「The Forrester Wave™: External Threat Intelligence Service Providers, Q3 2023」でリーダーに選出
- 「The Forrester Wave™: Endpoint Detection and Response Providers, Q2 2022」でリーダーに選出
- 「The Forrester Wave™: Cybersecurity Incident Response Services (CIRS), Q1 2022」でリーダーに選出
- 「The Forrester Wave™: Cloud Workload Security, Q1 2022」でストロングパフォーマーに選出
- IDC MarketScape™: Worldwide Modern Endpoint Security for Enterprise 2022 Vendor Assessmentでリーダーに選出

CROWDSTRIKE