CROWDSTRIKE

クラウドストライク製品
データシート

Falcon Complete for Service Providers

シームレスで強力な保護を実現するマネージド型のセキュリティサービス

課題

組織のセキュリティを保護することは、特に巧妙な攻撃による脅威が増えている今日において非常に重要です。企業の規模にかかわらず、重要な攻撃対象領域に対する包括的な検知と対応の仕組みの必要性が認識されており、あらゆる企業が環境を管理し、必要な保護を提供してくれるパートナーを求めています。

これまでに観測されている最短のサイバー犯罪（eCrime）のブレイクアウトタイムはわずか7分と短く、1秒たりとも無駄にできません。このように非常に短時間かつ巧妙な手口で攻撃が試みられるようになっているため、サービスプロバイダーは最新の戦術、手法、手順（TTP）を把握し、顧客環境を保護するという難しい課題への対応を迫られています。

サービスプロバイダーがプロアクティブな体制を整え、ビジネスのレジリエンスを高めるためには、運用を合理化し、可視性を高め、そしてこれが最も重要なポイントですが、セキュリティ侵害を阻止できるよう、強力なテクノロジーとマネージド型のセキュリティサービスによりセキュリティ機能を強化する必要があります。

ソリューション（解決策）

マネージド検知と対応（MDR）サービスであるCrowdStrike Falcon® Completeを使用すると、広い範囲で脅威に対抗し、サイバー保護を強化できます。サービスプロバイダーは、Falcon Complete for Service Providersを使用することにより、クラウドストライクの業界をリードするMDRサービスを基盤として、あらゆるエンドポイント、アイデンティティ、クラウドワークロードにわたり24時間365日体制の包括的かつ専門性の高い脅威検知、脅威ハンティング、統合型インテリジェンス、およびフルサイクルの対応を提供する顧客向けのカスタムサービスを構築することができます。

Falcon Completeの精鋭のエキスパートチームがCrowdStrike Falcon®プラットフォームを積極的に監視し、平均わずか数分でインシデントをリモートから修復します。そのためサービスプロバイダーは、単一ベンダーによるシームレスなサービスとして優れた保護を提供するという新しい価値を顧客に届けつつ、収益を拡大させることができます。

主な利点

- 24時間365日体制のエキスパートによる保護、MDRのリーダーでありパイオニアによる専門性の高いセキュリティに関する知見
- プロアクティブな脅威ハンティング、ネイティブな脅威インテリジェンス、外科的修復による高度な保護
- 巧妙な攻撃に対する迅速な対応
- 単一ベンダーによるフリクションレスなサービスとしてあらゆる規模の企業の顧客に保護を提供

主なサービス機能

切れ目のない保護

Falcon Completeが提供する24時間365日体制の保護と可視化機能により、サービスプロバイダーは管理する環境全体にわたる脅威の状況を包括的に把握することができます。検知された脅威は、エキスパートチームによるトリアージ、調査を経て迅速に解決されるため、顧客環境内で問題が生じる前に先手を打って脅威に対応することができます。

層の厚い専門家集団

Falcon Completeは、信頼できるパートナーとして検知と対応、脅威ハンティング、統合型の脅威インテリジェンスといった幅広い機能を提供します。そのため、顧客環境内のリスクにプロアクティブに対処するために必要なインサイトを獲得することができます。セキュリティの保護は背後で動作するFalcon Completeに任せることができるため、顧客環境の最適な運用に専念できます。

- **CrowdStrike Falconプラットフォームのエキスパート:** Falcon Completeチームは、CrowdStrike Certified Falcon Responder (CCFR) およびCrowdStrike Certified Falcon Administrator (CCFA) の資格を保持しています。
- **精鋭による脅威ハンティングとインテリジェンス:** CrowdStrike® Falcon OverWatch™のチームが脅威ハンティングを実施するほか、クラウドストライクのAIを活用したインテリジェンスがFalconプラットフォームに組み込まれているため、これらのインサイトを統合的に活用して、防御を強化し、攻撃が仕掛けられてもセキュリティ侵害に発展する前に阻止することができます。

包括的な保護

Falcon Complete for Service Providersは、エンドポイントに対する包括的なMDRだけでなく、クラウドワークロード、コンテナ、Kubernetesの高度な保護や、フリクションレスでリアルタイムのアイデンティティ脅威に対する保護も提供します。

Falcon Complete MDRサービスには、以下が含まれています。

24時間365日体制のエキスパートによる対応:

- 世界中のセキュリティエキスパートが集結したFalcon Completeアナリストチーム
- Falcon OverWatch脅威ハンティングチーム

マネージド型Falconプラットフォームのモジュール:

- CrowdStrike Falcon® Preventの次世代アンチウイルス機能
- CrowdStrike Falcon® Insightによるエンドポイントに留まらないXDR検知と対応
- CrowdStrike Falcon® Discover ITハイジーン
  - アドオン:
    - CrowdStrike Falcon® Identity Threat Protection
    - CrowdStrike Falcon® Cloud Security－クラウドワークロード保護

透明性があり安全なコミュニケーション

フリクションレスで透過的、かつ安全なコミュニケーション方法が用意されています。サービスプロバイダーは、Falconメッセージセンター、Eメール、またはAPIを通して、Falcon Completeチームといつでもコミュニケーションをとることができます。

外科的修復

Falcon Completeのアナリストは、Falconのネイティブな機能を使用して脅威の影響を受けたシステムにリモートからアクセスし、脅威を外科的に取り除いて、システムを運用状態へと復元できます。具体的には、プロセスの終了、サービスの停止、永続化メカニズムの除去、ホストのネットワーク隔離、その他潜伏しているあらゆるアーティファクトの消去を行うことができます。そのため、システムを再イメージングする手間を省けるだけでなく、エンドユーザーへのサービス提供が中断されることもありません。

インシデントが修復された後、サービスプロバイダーは、Falcon Completeチームが実施したすべてのアクションおよび補足データを含む詳細なレポートを受け取ることができるため、顧客と共有し、事後分析に役立てることができます。

お客様のビジネスをサポートする仕組み

保護: CrowdStrike Falconプラットフォームを利用すると、24時間365日体制の強力な監視、検知、対応の機能と、人間の手による脅威ハンティングにより、プロアクティブで確実なセキュリティ保護を提供できます。

パートナーシップ: Falcon Completeとの共同ブランドにより、強力で専門性の高いマネージドセキュリティサービスを提供できます。

利益: 自身が負担するコストは削減しつつ、ライセンスや顧客向けの価格を自由に管理して、顧客との関係を思いのままに築き、最大限の利益を手にすることができます。

信頼できるパートナーシップによりシームレスにセキュリティを提供

Falcon Complete for Service Providers — MDR

あらゆるエンドポイント、クラウドワークロード、アイデンティティにわたる優れたマネージド型の保護により、リアルタイムで攻撃を阻止します。

役割と責任	クラウドストライク	パートナー
オンボーディングとプランニング		
顧客のオンボーディング		√
顧客との関係の管理		√
センサーのインストール		√
競合するサービスの削除		√
カスタマーIDの作成とセットアップ	√	√
ポリシーの作成と更新	√	
Falcon Completeによる監視の有効化	√	
監視と修復		
Falcon Completeへのエスカレーションとコミュニケーションの対応		√
必要なレポートの提供		√
センサーのトラブルシューティングの実施		√
追加のFalconモジュールの管理（Falcon Complete管理対象外のモジュール）		√
顧客とのコミュニケーション		√
Falcon OverWatchアラートへの対応	√	
Falconプラットフォームの検知への対応	√	
許可リストの管理	√	

Falcon Complete for Service Providers — Identity Threat Protection

アドオンとして提供されるFalcon Identity Threat Protectionを使用すると、マネージド型のエンドポイント保護サービスである中核的なCrowdStrike Falcon Completeの機能を強化して、アイデンティティおよびアイデンティティストアに対する業界最先端のセキュリティを提供できます。

役割と責任	クラウドストライク	パートナー
オンボーディングとプランニング		
ATIポリシーの作成と適用		√
MFAコネクターおよびIDaaSコネクターの設定		√
ポリシールールの実装、調整、設定		√
監視と修復		
サポート対象のアイデンティティベースの検知のトリアージ	√	
サポート対象のアイデンティティベースの検知への対応	√	
Falcon Completeの定義に基づく対応策の実行	√	
エスカレーション／修復チケットに従った推奨復旧措置の実施		√

CrowdStrikeについて

CrowdStrike (Nasdaq：CRWD)は、サイバーセキュリティのグローバルリーダーであり、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、データを含む企業におけるリスクを考える上で重要な領域を保護する世界最先端のクラウドネイティブのプラットフォームにより、現代のセキュリティを再定義しています。

CrowdStrike Falcon®プラットフォームは、CrowdStrike Security CloudおよびワールドクラスのAIを搭載し、リアルタイムな攻撃の痕跡、脅威インテリジェンス、進化する攻撃者の戦術、企業全体からの充実したテレメトリーを活用して、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、優先付けられた脆弱性の可観測性を提供します。

Falconプラットフォームは、軽量なシングルエージェント・アーキテクチャを備え、クラウド上に構築されており、迅速かつスケーラブルな展開、優れた保護とパフォーマンスを提供し、複雑さを低減し即座に価値を実現します。

CrowdStrike: **We stop breaches**

ソーシャルメディア：ブログ | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

デモをスケジュール

詳細については、**www.crowdstrike.jp**をご覧ください。