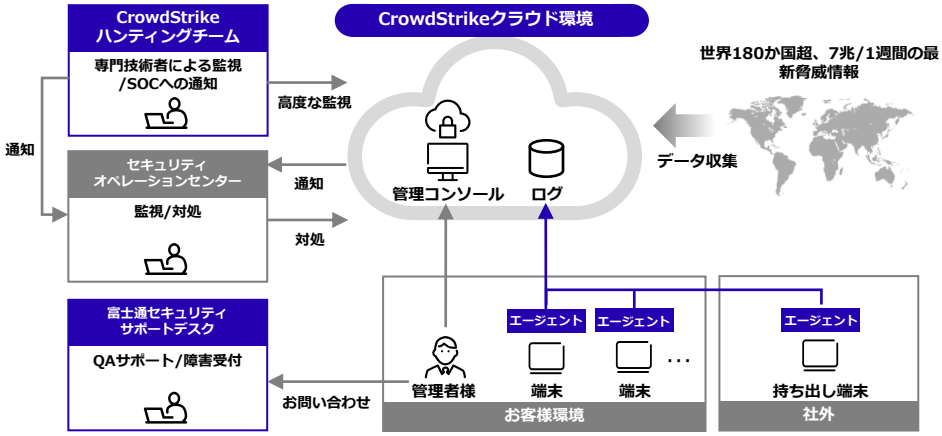
Endpoint Security

エンドポイントを中心に多彩な機能をもつAIを活用したクラウド型の統合セキュリティソリューション

本ソリューションは、CrowdStrike社の高度なセキュリティ基盤をベースに、エンドポイントから収集したログを分析・監視することで、エンドポイントへのサイバー攻撃を検知・防御するセキュリティソリューションです。本ソリューションをご利用いただくことで、日々、高度化・複雑化するマルウェアなどの脅威からお客様環境を守ります。



お客様の課題

1. **未知の脅威やランサムウェアへの対策ができていない**
   従来型のアンチウイルスソフトウェアで既知の脅威は防御できるが、未知の脅威や新しいランサムウェアを防御することができない

2. **マルウェアに侵入された場合の調査・対策ができない**
   エンドポイントの不審なアクティビティやマルウェアの兆候を検出することができないため、セキュリティインシデントが発生してもすぐに気づくことができず、被害が拡大する恐れがある

3. **セキュリティソフトウェアにより端末の動作が遅くなる**
   PCにインストールされたセキュリティソフトウェアの負荷が高くエンドユーザーからのクレームが多発している

本ソリューションが解決します

本ソリューションをご利用することで、サイバー攻撃の事前予防と事後対処を統合し、簡単かつ迅速なインシデント対応を実現することができます。

お客様は、環境に合わせてNGAV（次世代アンチウイルス）、EDR（検知と対応）、脆弱性管理、IT資産管理などの各コンポーネントを組み合わせてご利用いただけます。また、各コンポーネントは1つの共通エージェントで動作しますので、共通エージェントの導入後にコンポーネントを追加する際にインストール作業は発生しません。

© 2025 Fujitsu Limited

特長

1 新しい脅威、高度な脅威に対しても防御可能

豊富な検知ロジックでサイバー攻撃を多層的に防御

ふるまい検知、機械学習、サンドボックス分析などを組み合わせることで未知の脅威や新しいランサムウェア、ファイルレスマルウェアなど高度な脅威を防御
また機械学習により進化するサイバー攻撃にも日々対処可能。

2 リアルタイムで端末上のふるまいの可視化、対応が可能

検知・対処機能と脅威ハンティングを提供

端末上のエージェントが収集したログを管理コンソールで検索・可視化しリモートで端末からのマルウェアの除去や端末の隔離を実施可能。
機能的な検知をすり抜けた高度な脅威はエキスパートによる脅威ハンティングでアラート通知

3 軽量なシングルエージェント

軽量なシングルエージェントで多彩な機能を提供

端末にインストールするエージェントソフトウェアは軽量であり、NGAV機能、EDR機能のほか、資産管理機能や脆弱性管理機能を利用する場合も端末への追加インストール不要でユーザー業務に与える影響は軽微

基本サービス

NGAV（次世代アンチウイルス）サービス

脅威が既知、未知に関わらず、悪性な攻撃を多層的に防御します。ディスクに痕跡を残さないファイルレスマルウェアへの対応も可能です。

EDRサービス

PC端末/サーバー上でのエージェントが収集する端末上のふるまいを様々な観点から調査可能な検索機能を提供します。マルウェアが端末をまたがって感染を広げるラテラルムーブメントの可視化や、リモートでの端末調査、端末隔離、端末に対する命令の実行を行うことも可能です。

EDRサービス for Mobile サービス

モバイル端末向けのEDRサービスであり、iOS/Android の両OSに対応し、軽量で電池消費量も考慮したエージェントによって、モバイル端末上の振る舞いの記録及び検知が可能です。

脅威インテリジェンスサービス

セキュリティ脅威を理解し、対策を立てるための情報を提供いたします。世界中のエンドポイントから得られたリアルタイムの分析結果からなる脅威のデータや、特定の脅威アクターやキャンペーンについての調査レポートを提供します。また、お客様のニーズに合わせてカスタムした情報の提供も可能です。

アイデンティティ脅威検知／防御サービス

アカウントのセキュリティを強化するための機能です。異常な行動や不審な認証パターンを検出し、リアルタイムで警告を通知します。これにより不正アクセスや内部からの脅威を早期に検出し、迅速に対応できます。また、検知した特定の脅威に対して、ID認証のブロックやMFA認証の強制等の自動的な防御を行い、セキュリティインシデントの発生を防止することも可能です。

アタックサーフェス管理サービス

CrowdStrike社の知見・ノウハウによる独自技術により自組織のインターネット上に公開された資産の可視化や脆弱性・設定ミスを自動的かつ継続的に検出します。また自動化された優先順位付けの提供やガイド付きの修復ステップで、対応の効率化と効果的な対処を実現します。

NGBA／EDR／資産管理／脅威ハンティング／簡易通報パック

NGAVサービスとEDRサービス、資産管理オプション、脅威ハンティングオプションとMDRがパックになったサービスです。

© 2025 Fujitsu Limited

オプションサービス

脅威ハンティングオプション

CrowdStrike社のハンティングチームによる24時間365日体制での脅威ハンティングを提供します。機能的検知をすり抜けた高度な行為をプロアクティブに見つけ出し、通知します。

脆弱性管理オプション

エージェントがインストールされた端末のOSやアプリケーションの脆弱性を可視化します。また、セキュリティパッチの適用状況を可視化すると共に、未適用パッチの適用指示を出すことも可能です。

デバイス制御オプション

エンドポイントに接続されたデバイスを一元管理、またエンドポイントのデバイスへのアクセスポリシーを適用することで、不正なデバイスへのアクセスを防止します。エンドポイントのデバイスアクティビティのリアルタイム監視も行い、異常な動きや不正なアクティビティをすぐに検出できます。

XDRオプション

エンドポイントに加えて、ネットワークやクラウドなどのログを統合し、組織のIT環境全体に検知と対応機能を拡張します。攻撃対象領域全体の疑わしいアクティビティを自動的に相関させ、リスクを軽減し、企業全体で脅威の可視性と検知を改善することが可能です。

生ログ関連オプション

端末から収集したイベントデータ（生ログ）をJSON形式で外部へ出力することや、長期保存することが可能です。

資産管理オプション

エージェントがインストールされた端末のアプリケーション、端末ハードウェア情報、ユーザアカウント情報を可視化します。また、エージェントがインストールされていない非管理端末を検出し可視化することが可能です。

ファイアーウォール管理オプション

エンドポイントのファイアーウォール設定やポリシーの適用を一元管理・自動化することができます。さらにリアルタイムでネットワークトラフィックを監視して異常な活動を検知することで、ネットワークのセキュリティを強化し、不正なネットワークアクティビティを防止します。

ファイル整合性監視オプション

エンドポイントのファイルをAIと機械学習を利用して詳細に調査、分析することで、ファイルの改ざんや不正な変更を検知・ブロックし、データやシステムを保護します。

エクスポージャー管理オプション

資産管理オプション、脆弱性管理オプション、アタックサーフェス管理オプションを統合し、内部・外部を問わず資産と脆弱性の管理およびリスクの深堀が可能です。また、エクスポージャー管理独自のダッシュボードの提供や機能があり、より環境内の端末のセキュリティ管理が可能です。

事例

本ソリューション導入に至った背景から導入後の効果までをご紹介しております。導入検討いただく際に是非ご覧ください。

事例一覧

関連リンク

- ✓ グローバル環境の監視にも対応セキュリティ運用監視サービス
- ✓ ゼロトラストセキュリティ導入から運用までをトータルにサポート
- ✓ セキュリティ ホワイトペーパー・記事

お問い合わせ先

富士通株式会社

富士通コンタクトライン（総合窓口）0120-933-200
受付時間 : 9:00～12:00および13:00～17:30（土・日・祝日・当社指定の休業日を除く）
お問い合わせフォーム

© 2025 Fujitsu Limited