Brochure

標的型攻撃を阻止

WithSecure™ Elements Endpoint Detection and Response

高度なサイバー攻撃からビジネスとデータを保護

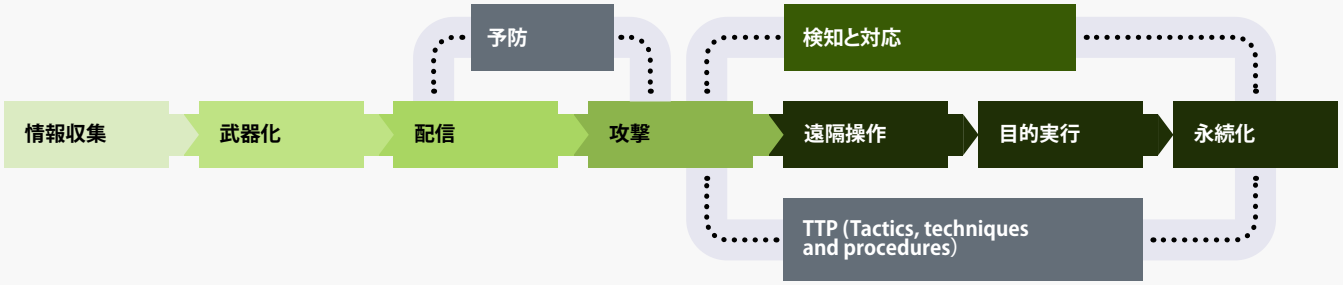
侵害される前に効果的な脅威防止策を講じておくことが、サイバーセキュリティの基本です。しかし、標的型攻撃で使われる戦術、手法、および手順（TTP：Tactics, Techniques and Procedures）からビジネスとそのデータを守るためには、防止策だけに頼るわけにはいかないのも事実です。

絶えず変化する脅威ランドスケープや、GDPRなどの規制上の要件に適切に対応するため、企業は侵害された場合にそれを即座に検知できるよう、準備を整えておかなければなりません。そうすれば、企業は高度な攻撃に対して迅速に対応できるようになります。

WithSecure™ Elements Endpoint Detection and Responseソリューションは、経験豊富な脅威ハンティングチームによってトレーニングされており、お客様社内のITチームや認定サービスプロバイダーは、これを使って高度な脅威から企業を守ることができます。

ウィズセキュアが擁する世界トップレベルのサイバーセキュリティの専門家による支援があるため、社内ITチームはインシデントに迅速かつ効果的に対応できます。

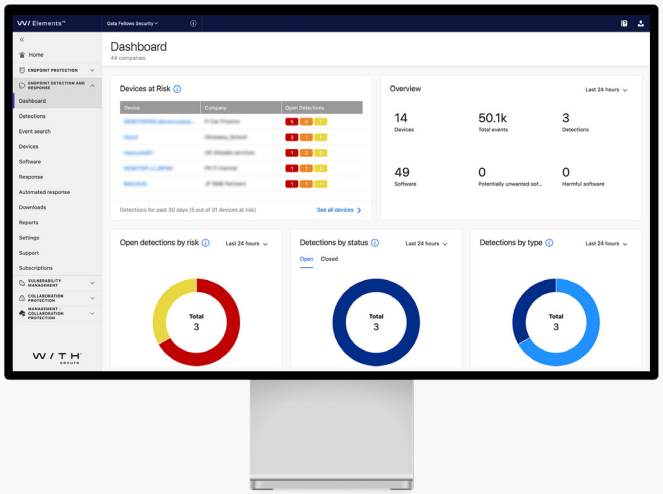
あるいは、検知と対応をサービスプロバイダーに委ねれば、社内の人材をコアビジネスに集中させることができ、攻撃を受けたときはいつでも専門家の指導を受けることができます。



概要

ガイダンスと自動化により、標的型攻撃を迅速に阻止

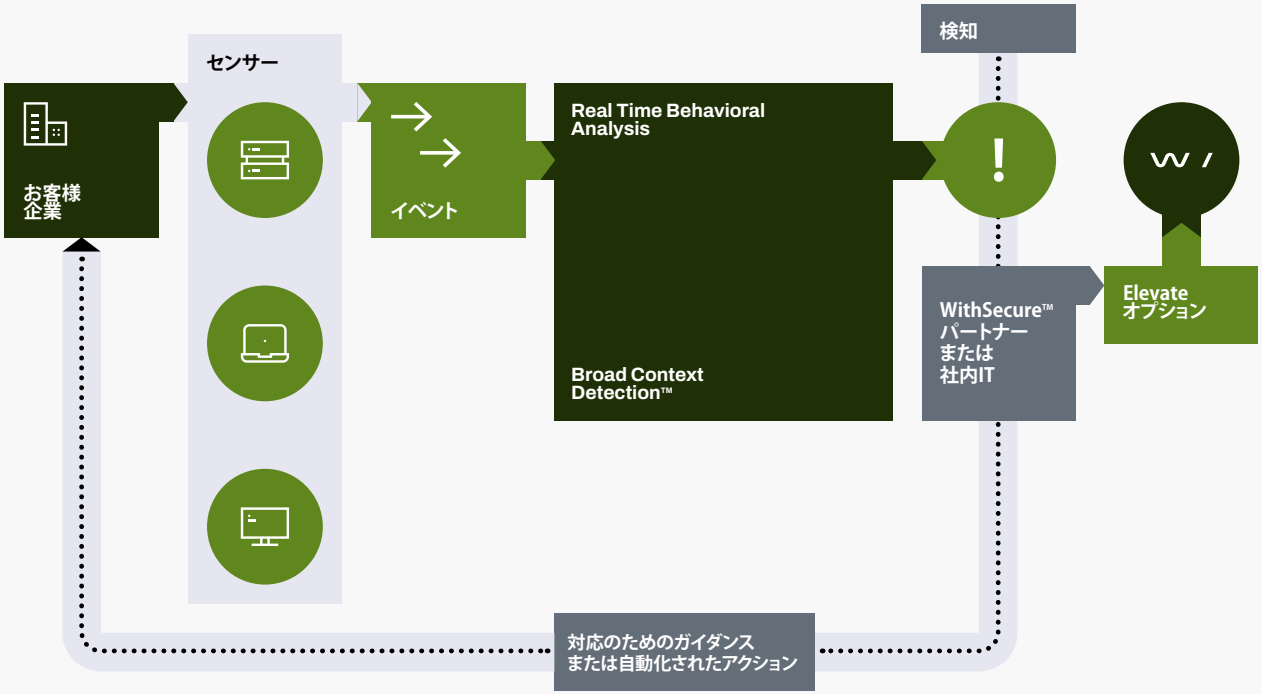
皆様は、高度な攻撃をどのように検知していますか? 最先端の分析と機械学習の技術を駆使することで、高度なサイバー脅威や侵害のリスクから企業を守ることができます



業界をリードするウィズセキュアのEndpoint Detection & Response（EDR）ソリューションを使えば、高度な脅威についてコンテキストに沿った可視性を得ることができ、自動化された対応と適切なガイダンスによって標的型攻撃を検知してそれに対応することができます。

実際に侵害が発生した場合には、単なるアラート以上のものが必要です。可能な限り最善の対応策を講じるためには、攻撃の詳細について理解する必要があるからです。ウィズセキュアのBroad Context Detection™のメカニズムには自動化の機能が組み込まれており、認定サービスプロバイダーとともに攻撃を迅速に阻止し、修復アクションのための実用的なアドバイスを提供します。

サービスの仕組み



業界をリードするテクノロジーとサイバーセキュリティの専門家がサービスをサポート

1. エンドポイントに配置された軽量なセンサーがユーザーの行動イベントを監視し、データをReal Time Behavioral AnalysisおよびBroad Context Detection™ に送り込み、悪意のある行動パターンなのか通常のユーザー行動なのかを識別します。
2. アラートには、リスクスコアと影響を受けたホストのBroad Contextを可視化した情報が含まれており、社内のITチームまたはウィズセキュアのパートナーが、検知結果を簡単に確認することができます。そして、困難なケースをウィズセキュアにエスカレーションしたり、自動化されたアクションに任せたりすることができます。
3. このソリューションは検知が確認された後に対応のためのアドバイスと推奨される対応策を提供し、攻撃を迅速に封じ込め、修復のために必要なステップをガイドします。

サービスの仕組み

干し草の山で針を探す：実際にあった例

攻撃者が引き起こす個々の小さなイベントを探して高度な脅威を検知しようとすることは、干し草の山から針を見つけようとするようなものです。

325台のノードを持つあるお客様のサイトでは、1か月間に約5億件のイベントがセンサーから収集されました。その生データをバックエンドシステムで分析したところ、疑わしいイベントの数は225,000件にまでフィルタされました。

その疑わしいイベントはBroad Context Detection™ のメカニズムによってさらに分析され、24件にまで絞り込まれました。最後にこれらの24件の検知結果が詳細にレビューされましたが、実際の脅威として確認されたのは7つだけでした。

これにより、ITチームとセキュリティチームは少数の正確な検知結果に集中できるため、現実にサイバー攻撃が発生した場合に、より迅速で効果的な対応アクションを行うことができます。

500,000,000

325個のエンドポイントから
1ヶ月の間に5億件のイベントを収集

225,000

リアルタイム行動分析の結果
225,000件までフィルタリング

24

Broad Context Detectionによって、
さらに24件まで絞り込み

7

最終的に7件を実際の脅威として確認

メリット

Visibility（可視性）

IT環境とセキュリティ状況を即座に把握するための可視性を提供します

- アプリケーションとエンドポイントのインベントリにより、IT環境とセキュリティ状況の可視性が向上します
- コモディティマルウェア以外の行動イベントを収集して関連付けすることで、不審な行動を特定します
- インシデント対応を容易にするために、幅広いコンテキスト情報と資産の重要度を示すアラートを提供します

Detection（検知）

侵害を迅速に検知し、ビジネスと機密データを保護します

- 標的型攻撃を迅速に検知して阻止し、ビジネスの中断やブランドへの悪影響を最小限に抑えます
- ソリューションのセットアップは数時間で完了し、即座に侵害に対応します
- 72時間以内の報告義務が課されているPCI、HIPAA、GDPRの規制要件を満たすことができます

Response（対応）

ガイダンスと自動化で迅速に攻撃に対応します

- 自動化機能とインテリジェンス機能により、本物の攻撃に集中できます
- アラートには適切な対応のためのガイダンスが含まれており、24時間体制で対応を自動化するオプションも用意されています
- ウィズセキュアがサポートする認定サービスプロバイダーが攻撃に対応することで、社内のスキルやリソースの不足を補います

機能

エンドポイントセンサー

あらゆるエンドポイントプロテクションのソリューションに対応する、軽量で目立たないモニタリングツール

- 企業内のすべての関連するコンピュータに軽量なセンサーを導入
- ウィズセキュアのエンドポイントセキュリティソリューションにより、単一クライアントでの管理インフラを実現
- センサーはユーザーのプライバシーを侵害することなく、Windows、Mac、Linuxデバイスから行動データを収集

Broad Context Detection™

ウィズセキュア独自の検知技術により、標的型攻撃の範囲を容易に把握

- 機械学習によるリアルタイムな行動・レピュテーション・ビッグデータ分析
- タイムライン上に可視化されたコンテキストに検知結果を自動的に配置
- リスクレベル、影響を受けたホストの重要性、一般的な脅威ランドスケープなどを提供

アプリケーションの可視性

かつてなく簡単にIT環境とセキュリティ状況を可視化

- 有害なアプリケーションや不要なアプリケーションを特定し、外部のクラウドサービスをすべて特定
- ウィズセキュアのレピュテーションデータを活用して、有害な可能性のあるアプリケーションを特定
- 情報漏えいが発生する前に、有害なアプリケーションやクラウドサービスを制限

対応のためのガイド

高度なサイバー攻撃にも社内のリソースで対応可能

- 対応のためのステップバイステップのガイダンスと攻撃を阻止するためのリモートアクションをあらかじめ組み込み
- 認定サービスプロバイダーが対応策を指導・サポート
- 脅威アナリストおよび専門家による独自のガイダンスサービスである「Elevate to WithSecure™」がお客様をバックアップ

自動化された対応

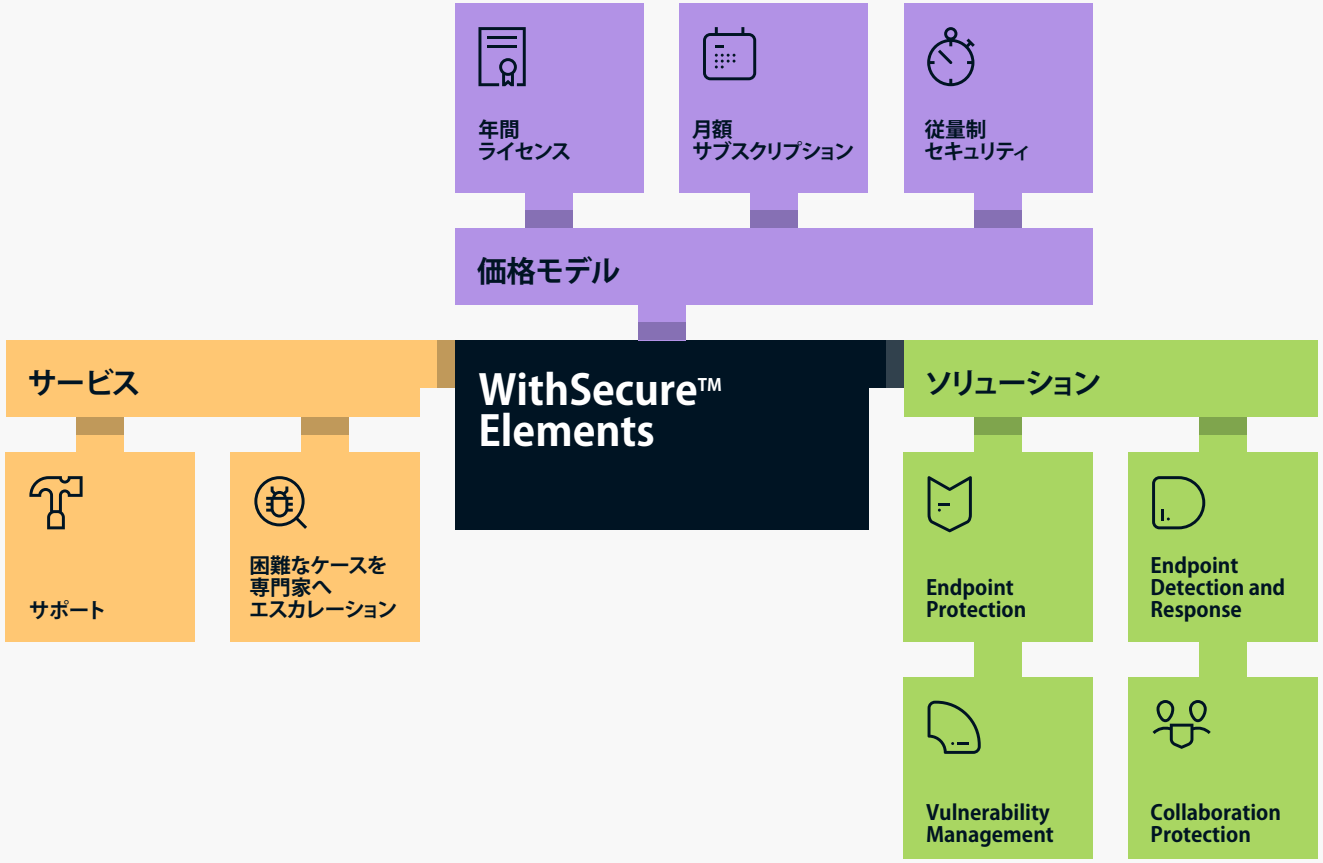
24時間体制で対応を自動化し、標的型サイバー攻撃の影響を軽減

- 重要度、リスクレベル、事前定義されたスケジュールに基づいた自動対応アクション
- ソリューションが提供する深刻度とリスクレベルにより、対応策の優先順位付けが可能
- 営業時間中しか稼働しないチームでも、攻撃を迅速に封じ込めることが可能

WithSecure™ Elements – サイバーリスク、複雑性、非効率性を低減

WithSecure™ Elements Endpoint Detection and Response はスタンドアロンとして使用することも、モジュール式のWithSecure™ Elements サイバーセキュリティプラットフォームの1つの機能として使用することもできます。

今すぐ試してみる



WithSecure™ について

WithSecure™は、ITサービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちはAIを活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は30年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988年に設立されたWithSecure™は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。

ウィズセキュア株式会社
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.withsecure.com/
2022/04

WITH secure