WithSecure™ Elements
- Endpoint Protection (EPP)
- Endpoint Detection and Response (EDR)

2023年4月

ウイズセキュア株式会社

ウィズセキュア クラウドサービス全体図

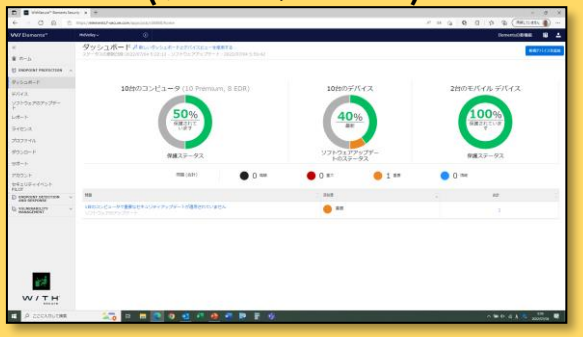
専用管理サーバー導入不要

どこからでも
アクセス

管理者

クラウド

Elements Security Center
(ブラウザベース)



自動更新(OSによって、機能が異なります)
パターンファイル、プロファイル、ソフトウェアバージョンアップ、セキュリティパッチ

- Windows
- macOS
- Android
- iOS

- Windows Server
- Linux

社内LAN

- Windows
- macOS
- Android
- iOS

支社/海外

マルチプラットフォーム対応

多拠点も一元管理

WithSecure™ Elements Endpoint Protection – 主要機能

ディープガード
(振る舞い検知)

データガード
(ランサムウェア対策)

Web保護 &
カテゴリフィルタリング

アプリケーション制御

ソフトウエアアップデータ
(アップデートパッチ管理)

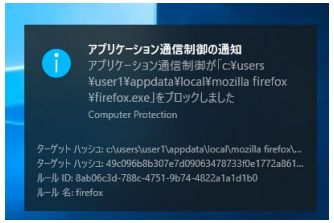
デバイス制御

ディープガードによる多層防御

ウイルス対策はどれか一つあれば大丈夫ではなく多層防御が必要

アプリケーション制御 (プレミアム版)

アプリケーションを実行する条件を設定し、制御します。
例: cmd.exeはWordファイルのマクロからの実行は不可、他は可。



データガード(ランサムウェア対策)
(プレミアム版)

普段どおりの
ファイルの保存や加工が可能

ソフトウェアアップデータ

アップデートパッチを最新にバージョンアップすることで、脆弱性を利用したマルウェアの攻撃を回避することができます

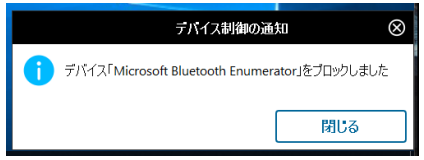
Webサイトのカテゴリフィルタリング

管理ポータルでWebサイトのカテゴリフィルタリングを一元管理
32のカテゴリーをグループ毎に設定可能

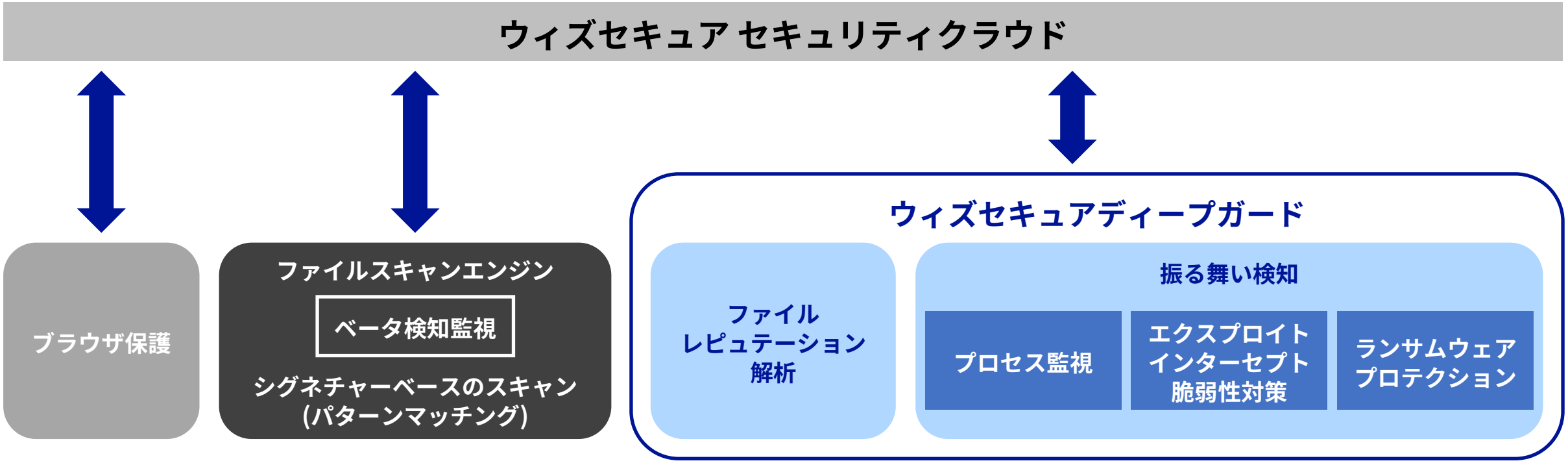
中絶	ハッキング
広告の提供	憎悪表現
アダルト	就活
アルコールとタバコ	

デバイス制御

大容量記憶装置、USB カメラ、プリンタなどの USB デバイスへのアクセス制限を設定



マルチレイヤプロテクション (階層型防御)



- サンドボックスでは検知出来ないマルウェアが益々増加しています。
- サンドボックスを擦り抜けるマルウェアの対策として
- ディープガードは機械学習にて振る舞い検知機能を随時強化しています。

WITH secure

WithSecure™ Elements Endpoint Protection - メリット

■ウィズセキュアクラウドの管理ポータルによる一元管理

- オンプレミスのような管理サーバの準備が不要
- Windows PC・サーバ、Mac、Linuxサーバ、iOS、Androidをサポート
- PC・サーバのWindowsセキュリティパッチを管理ポータルにて管理可能（脆弱性対策に有効）
- 管理ポータルからの操作で、PC・サーバへWindowsアップデートパッチを適用可能
- 不具合時も管理ポータルを利用する事でスムーズに対応可能

■クライアントエージェントの自動バージョンアップ

- パターンファイル、スキャンエンジンに加え、クライアントエージェントを再起動無しで自動的にバージョンアップ
- ソフトウェアのバージョンアップの工数削減
  （オンプレミス製品のような手動バージョンアップ作業が不要）

■ソフトウェアの不正利用への対策

- PCのユーザーインターフェースで、ソフトウェアのキーコードが確認出来ない仕様
- MSIインストーラにキーコードを埋め込むことができるため、インストール時にもキーコードの確認ができない仕様

■シングルエージェント

- EPPに加え、EDR、脆弱性診断も対応可能なシングルエージェント
  （それぞれのライセンスは別途必要）
- ソフトウェアのキーコードの属性変更で、EDR、脆弱性診断機能が利用可能
  （ソフトウェアの再インストール、キーコードの再登録は不要のため、今後EDR検討時の作業負担の簡素化）

WITH secure

補足情報

■オンプレミス製品群のEOLについて

- 2022年10月、既存ユーザ様ならびに販売店ご担当様にはご案内の通り、オンプレミス製品群のEOL予定（～2027/12/31）を発表させて頂きました。そのため、サポートならびに販売期間につきましても、2027年末までのご提供となります旨、　ご了承頂きたく存じます。

■ライセンス課金対象（Elements EPP）

- 現契約の「ビジネススイート」では、サーバとクライアントを含めたすべての台数＝ライセンス数（サーバは20%が上限）、いわゆるスイート製品となりますが、Elementsシリーズの場合は各クライアントOS毎に製品が異なります。
- *インストール台数=ライセンス数となります。仮想環境の場合は、ゲスト OS 数＝ライセンス数となります

例）

- クライアントPC向け ＝ WithSecure™ Elements EPP for Computers（スタンダード or プレミアム）
- Windowsサーバ向け ＝ WithSecure™ Elements EPP for Servers（スタンダード or プレミアム）
- Linuxサーバ向け ＝ WithSecure™ Elements EPP for Linux

Appendix（BS vs EPP）

WITH secure

製品比較表 - クライアントセキュリティ(Windows) vs. Elements EPP for Computers

機 能	機能の概要	クライアントセキュリティ	クライアントセキュリティ プレミアム	Elements EPP for Computers	Elements EPP for Computers Premium
マルウェア・スパイウェア防御	パターンファイルによる既知のマルウェア、スパイウェア防御	●	●	●	●
ディープガード	機械学習を用いた振る舞い検知による未知のマルウェア・スパイウェアの対策	●	●	●	●
ファイアウォール	Windowsファイアウォールを使用したネットワークアクセスの制御	●	●	●	●
デバイス制御	ハードウェアデバイスの制御	●	●	●	●
Webトラフィックスキャン	Webトラフィック(HTTP)に含まれる怪しいファイルの対策	●	●	●	●
ブラウザ保護	怪しいWebサイトへの接続の対策	●	●	●	●
Webコンテンツ制御	コンテンツに基づいて、Webサイトへの接続の制御		●	●	●
接続制御	金融サイト接続時の情報漏洩対策として、他のネットワーク通信の制御		●	●	●
ソフトウェアアップデータ	Windowsやサードパーティ製品のセキュティパッチの適用・管理		●	●	●
データガード	フォルダ、ファイルにアクセス出来る実行ファイルの制御		●		●
アプリケーション制御	アプリケーションの起動、動作の制御		●		●
製品自体の自動更新	自動的に製品のバージョンアップやモジュールの自動更新			●	●
非インターネット環境	非インターネット環境での利用について	●	●	Elements Connector (無償ソフト）を併用し対応を予定	Elements Connector (無償ソフト）を併用し対応を予定
集中管理	製品の集中管理ソフト（無償）	ポリシーマネージャ	ポリシーマネージャ	Elements Security Center	Elements Security Center

- Elementsシリーズは製品の自動バージョンアップ機能があるため、オンプレミス製品のような手動バージョンアップ作業が不要となります。
- Elementsシリーズは弊社クラウド上のElements Security Centerで管理するため、各端末にインターネット接続環境が必要となります。
- ポリシーマネージャで集中管理された各端末にElementsシリーズをポリシーベースでインストールできるため、短時間で移行が可能です。

※非インターネット環境でのElementsシリーズの利用については、Elements Connectorを併用することで運用可能となります。
Elements Connectorを導入した端末がインターネットに接続されていれば、配下の端末をクラウド管理できるようになります。
ただしElements Connector導入端末だけはインターネット接続が必要となるので、完全クローズ環境ではご利用いただけません。

WITH secure

製品比較表 - Windowsサーバセキュリティ vs. Elements EPP for Servers

機能	機能の概要	Windowsサーバ セキュリティ	Windowsサーバ セキュリティプレミアム	Elements EPP for Servers	Elements EPP for Servers Premium
マルウェア・スパイウェア防御	パターンファイルによる既知のマルウェア、スパイウェア防御	●	●	●	●
ディープガード	機械学習を用いた振る舞い検知による未知のマルウェア・スパイウェアの対策	●	●	●	●
ファイアウォール	Windowsファイアウォールを使用したネットワークアクセスの制御	●	●	●	●
デバイス制御	ハードウェアデバイスの制御	●	●	●	●
Webトラフィックスキャン	Webトラフィック(HTTP)に含まれる怪しいファイルの対策	●	●	●	●
ブラウザ保護	怪しいWebサイトへの接続の対策	●	●	●	●
Webコンテンツ制御	コンテンツに基づいて、Webサイトへの接続の制御		●	●	●
ソフトウェアアップデータ	Windowsやサードパーティ製品のセキュティパッチの適用・管理		●	●	●
データガード	フォルダ、ファイルにアクセス出来る実行ファイルの制御		●		●
アプリケーション制御	アプリケーションの起動、動作の制御		●		●
製品自体の自動更新	自動的に製品のバージョンアップやモジュールの自動更新			●	●
非インターネット環境	非インターネット環境での利用について	●	●	Elements Connector (無償ソフト) を併用し対応を予定	Elements Connector (無償ソフト) を併用し対応を予定
集中管理	製品の集中管理ソフト（無償）	ポリシーマネージャ	ポリシーマネージャ	Elements Security Center	Elements Security Center

- Elementsシリーズは製品の自動バージョンアップ機能があるため、オンプレミス製品のような手動バージョンアップ作業が不要となります。
- Elementsシリーズは弊社クラウド上のElements Security Centerで管理するため、各端末にインターネット接続環境が必要となります。
- ポリシーマネージャで集中管理された各端末にElementsシリーズをポリシーベースでインストールできるため、短時間で移行が可能です。

※非インターネット環境でのElementsシリーズの利用については、Elements Connectorを併用することで運用可能となります。
Elements Connectorを導入した端末がインターネットに接続されていれば、配下の端末をクラウド管理できるようになります。
ただしElements Connector導入端末だけはインターネット接続が必要となるので、完全クローズ環境ではご利用いただけません。

WITH secure

製品比較表 - Linux Security 64 vs. Elements EPP for Linux

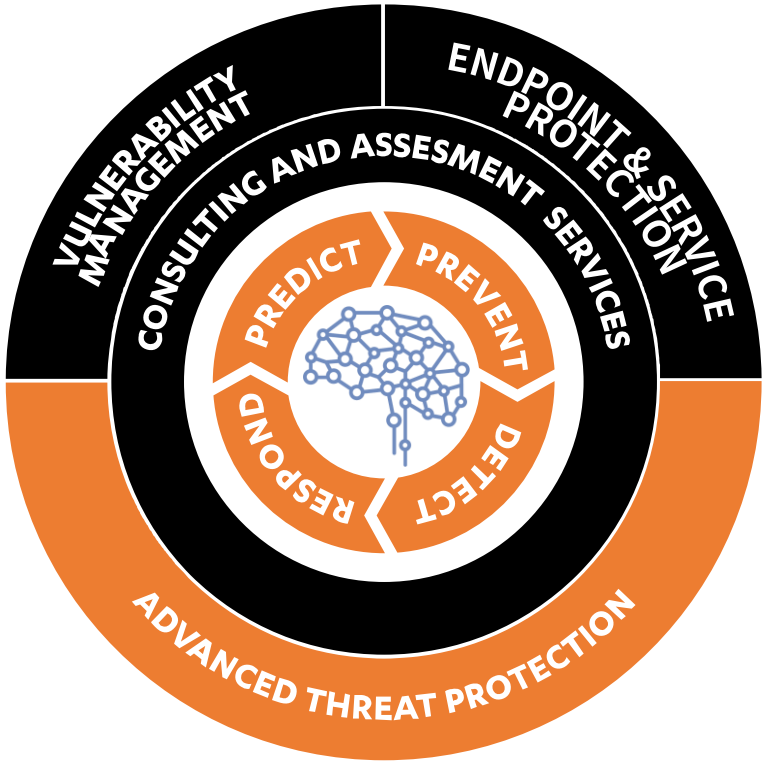
機能	機能の概要	Linux Security 64	Elements EPP for Linux
マルウェア・スパイウェア防御	パターンファイルによる既知のマルウェア、スパイウェア防御	●	●
マニュアルスキャン	コマンドによるスキャンの実行	●	●
スケジュールスキャン	スケジュールによる定期スキャン	●	●
完全性検査	登録したファイルに対してファイルの改竄を検出	●	●
スタンドアロン対応	集中管理せずスタンドアロンでの運用	●	
製品自体の自動更新	自動的に製品のバージョンアップやモジュールの自動更新	●	●
製品バージョンの固定化	自動バージョンアップせずバージョンを固定（特定バージョンのみ）	●	
非インターネット環境	非インターネット環境での利用について	●	Elements Connector (無償 ソフト）を併用し対応予定
集中管理	製品の集中管理ソフト（無償）	ポリシーマネージャ	Elements Security Center

- Elementsシリーズは弊社クラウド上のElements Security Centerで管理するため、各端末にインターネット接続環境が必要となります。

※非インターネット環境でのElementsシリーズの利用については、今後リリース予定のElements Connector（Linux版）を併用することで運用可能となります。
Elements Connectorを導入した端末がインターネットに接続されていれば、配下の端末をクラウド管理できるようになります。
ただしElements Connector導入端末だけはインターネット接続が必要となるので、完全クローズ環境ではご利用いただけません。

WithSecure™ Elements Endpoint Detection & Response (EDR)

EPPとEDRの役割



EPP WithSecure™ Elements Endpoint Protection

EDR WithSecure™ Elements Endpoint Detection and Response

EPPの役割

- マルウェアの感染、侵入を止める。
- マルウェアの活動を止める。

『止める！』

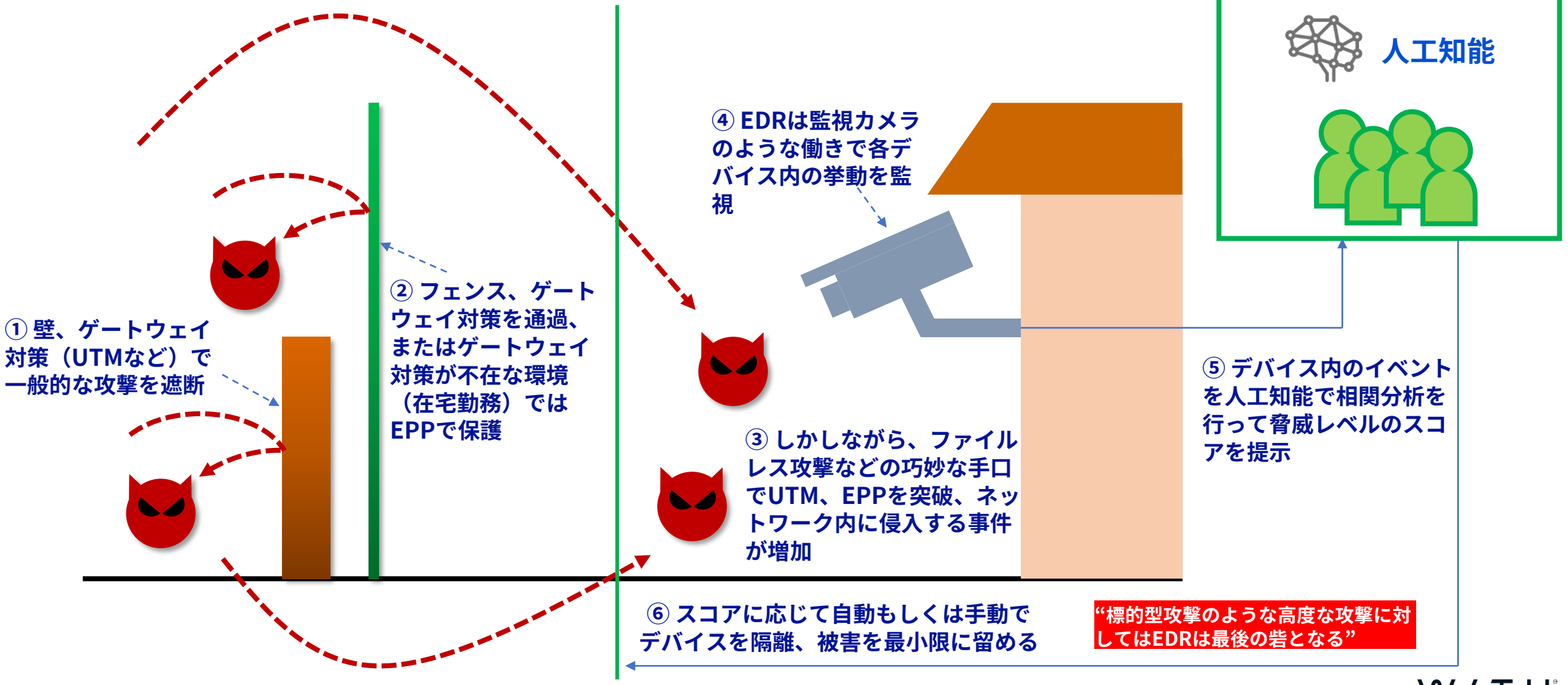
EDRの役割

- EPPでの対策が難しいマルウェアの感染、侵入を検知する。
- エンドポイントの潜在的な脅威と問題を明らかにする。
- インシデントに対応する。

『検知！』と『対応！』

WITH secure

侵害を前提とした対策（EDR）



EDRが必要な理由

	EPP		EDR	備考
機能	**マルウェアスキャン**	**振る舞い検知**	**振る舞い検知**	
検査のトリガー	下記の条件で、ファイルのウイルススキャンを行います • Webサイトからダウンロードしたファイル • 開封したメールの添付ファイル • 外部デバイスからコピーしたファイル	下記の条件で、プロセスの振る舞いを監視します • ファイルをアクセスした際、起動したプロセス	下記の条件で、**全てのプロセスの振る舞い**を監視します • EDRエージェントの起動	
自動化機能	• マルウェアが含まれたファイルの削除・隔離 • ファイルからマルウェアを駆除	• 怪しいプロセスの動作をブロック	• マルウェアが感染した可能性があるPCを自動的にネットワーク隔離 **• ウイズセキュアは自動隔離をサポート(他社の場合、自動隔離が未サポートのEDRがある)**	
課 題	**• ファイルレスマルウェアのようなファイルの有無・ファイルアクセスの有無に関係無く侵入するマルウェアの対策 • 正常な挙動に隠れたマルウェアの対策**			• 現在、猛威を振るっているファイルレスマルウェアの事例 • ファイルレスマルウェアは発見が難しいため、被害が大きくなり易い **• EDRでファイルレスマルウェアを発見しても、対処に時間・工数を要する場合が多い為、感染したPCの自動隔離が非常に有効**

ファイルレスマルウェアを使用した標的型攻撃を対策する場合、EDRが非常に有効です

WITH secure

ウイルス対策ソフトウェア(EPP)とEDR ①

	EPP	EDR	備考
コスト	安価	やや高価	
検査のトリガー	ファイルアクセス	プロセス・サービスの起動	
運用管理	普段の管理工数は少ない	管理工数が多い	
	普段の運用管理はシンプル	運用管理が複雑	
誤検知	少ない	やや多い	
製品の完成度	枯れた製品	発展途中	
	自動化機能が多い	自動化機能を追加中*	隔離、ブロックなど
投資効果	高い	高い*	SOCサービスなど要検討
導入の必要性	必要	必要	

- EDRはEPPを補完出来ますが、EDRでの対策範囲を増やした場合、誤検知、コスト、管理工数が増大します
- EDRを導入する場合、EPPの再検討が必要です
- EPPのメリットを増やし、EDRのデメリットを減らす事が重要です

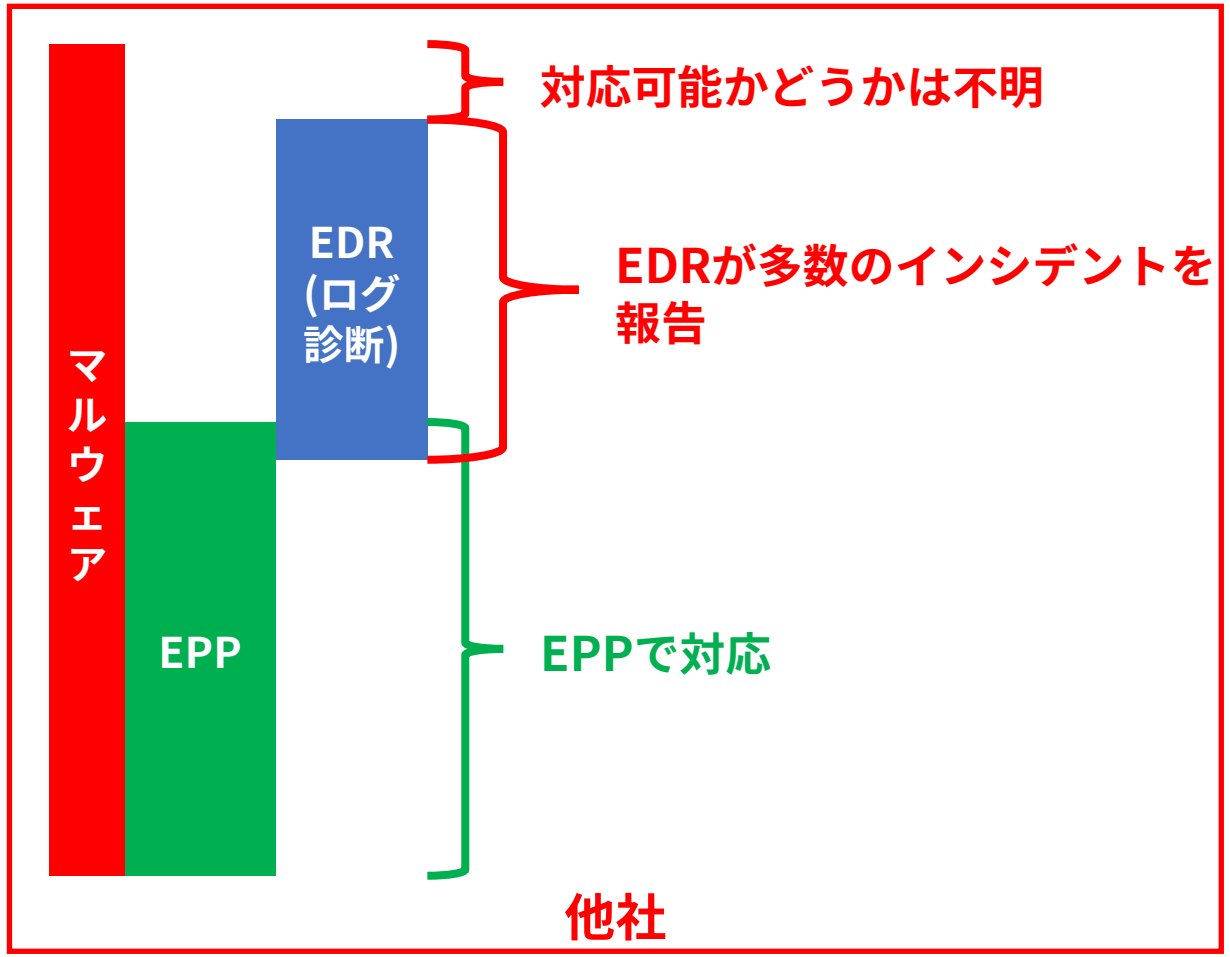
ウイルス対策ソフトウェア(EPP)とEDR ②

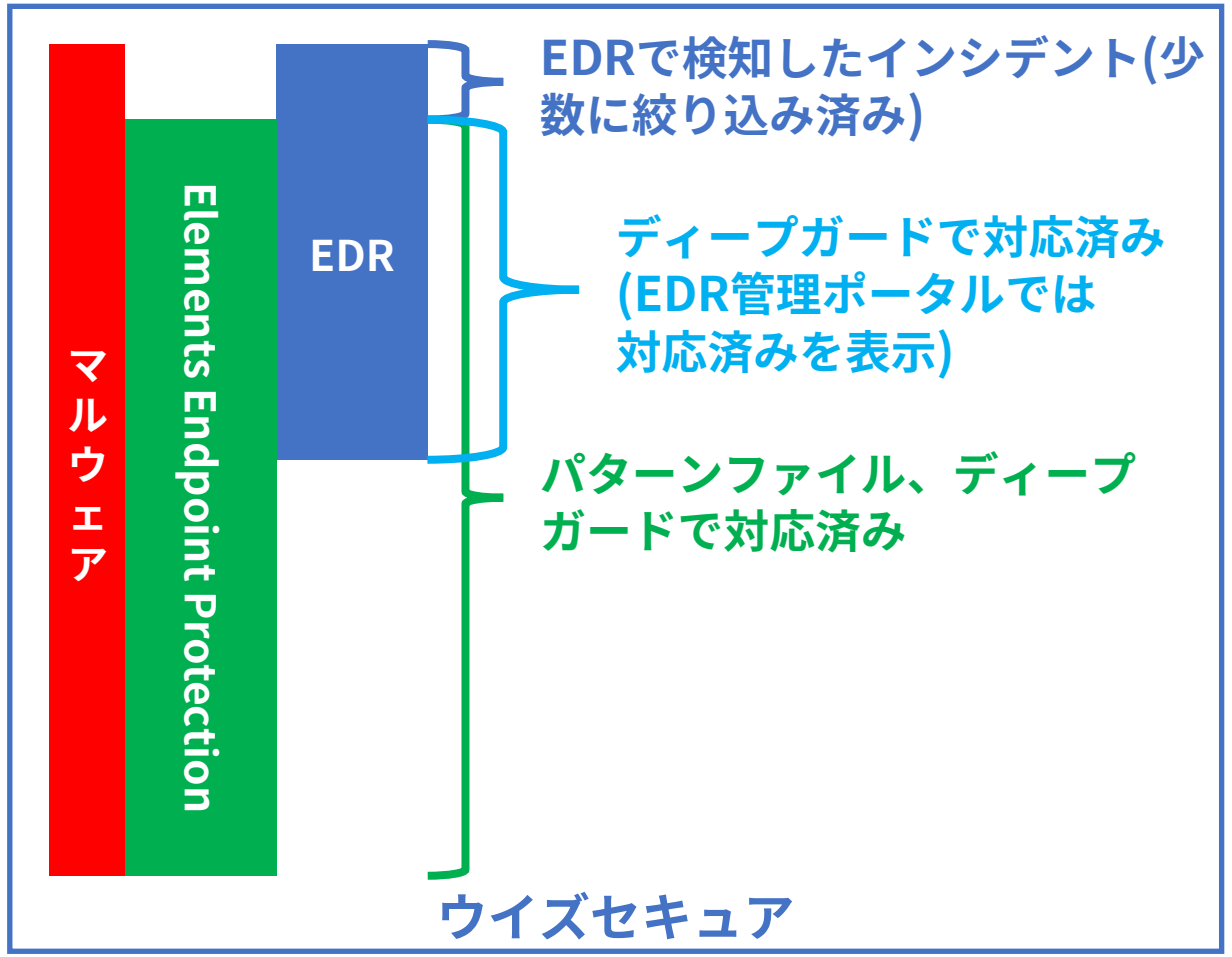
<table>
<tr><th>種類</th><th>分類</th><th>監視方法</th><th>対応方法</th><th>他社①</th><th>他社②</th><th>他社③</th><th>ウイズセキュア</th><th>備考</th></tr>
<tr><td rowspan="3">怪しい挙動の
マルウェア</td><td rowspan="2">既知</td><td rowspan="2">ファイル
スキャン</td><td>パターン
マッチング</td><td>対応</td><td>対応</td><td>対応</td><td>対応</td><td></td></tr>
<tr><td>レピュテーション</td><td>対応</td><td>対応</td><td>対応</td><td>対応</td><td></td></tr>
<tr><td rowspan="2">未知</td><td rowspan="2">振る舞い
検知</td><td>振る舞い検知</td><td rowspan="2">EDRで対応
(ログ診断)</td><td>対応</td><td>対応</td><td rowspan="2">対応
(ディープガードで
広範囲を対応)</td><td rowspan="2">• EPPの振る舞い検知で対策が可能な場合、EPPはEDRよりも運用管理が簡易。
• ファイルレスマルウェアを使用した標的型攻撃を対策する場合、EDRが必須。
• ログに記録されない標的型攻撃が多数あり、イベント情報を用いたEDRでの対策が必要。</td></tr>
<tr><td>正常な挙動に
隠れたマルウェア
(ファイルレスマル
ウェア)</td><td>Endpoint
Detection
Response
(EDR)</td><td>EDR</td><td>EDRで対応
(ログ診断)</td><td>EDRで対応
(イベント診断)</td><td>EDRで対応
(イベント診断)</td></tr>
<tr><td>SOCサービス</td><td></td><td></td><td></td><td>イベント診断の範囲が
不十分</td><td>イベント診断の範囲が
不十分</td><td>ベンダー、パートナー
のSOCサービスで
対応</td><td>ベンダー、パートナー
のSOCサービスで
対応</td><td>パートナーの
SOCサービスで
対応</td><td>• EDRは専門知識が必要なため、SOCサービスが有効。</td></tr>
</table>

EPP

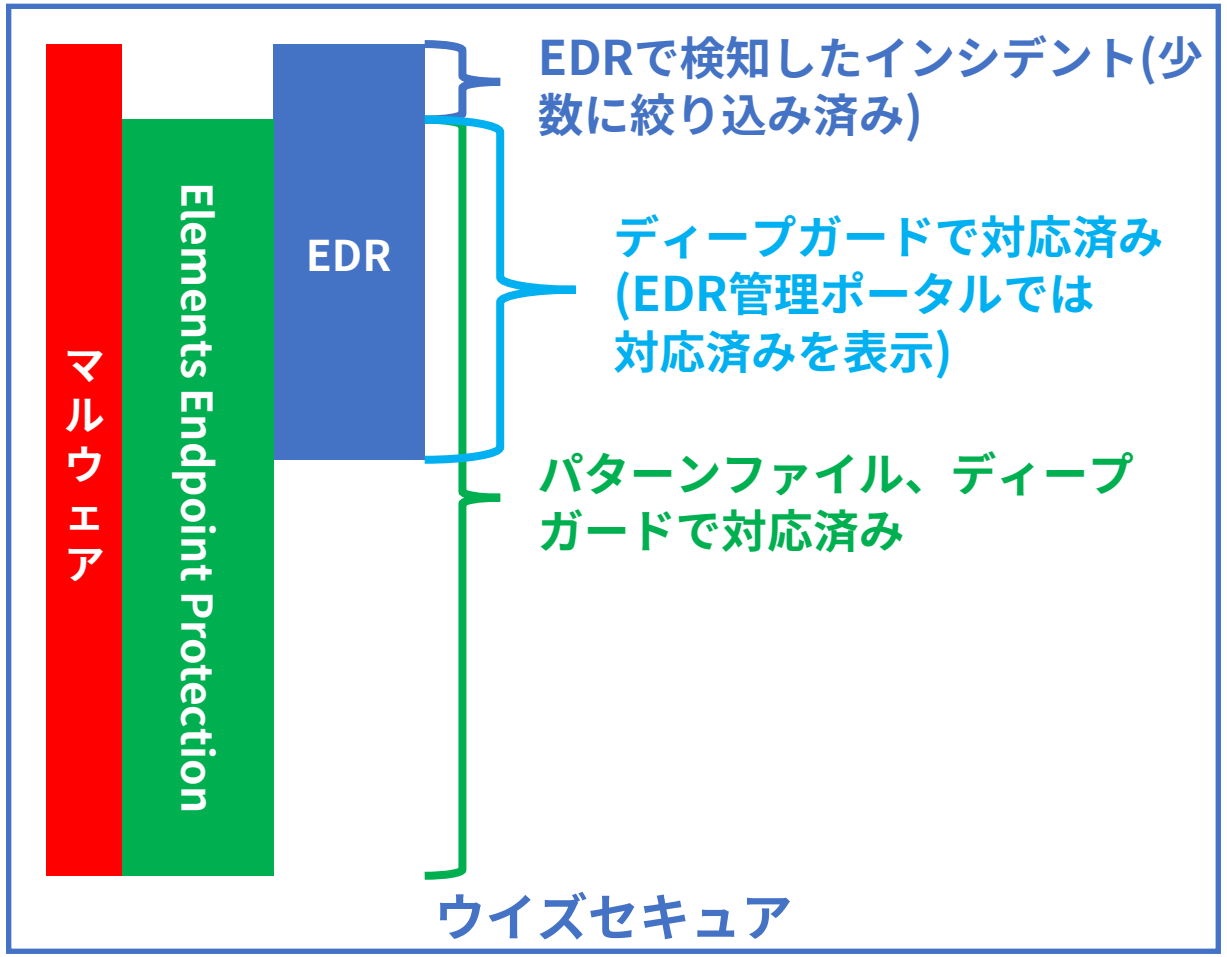
EDR

ウィズセキュア ディープガードの優位性 ①





ウィズセキュア ディープガードの優位性 ②



- EDRで検知したインシデント
  - EPPのパターンファイル・ディープガードで対策出来ない標的型攻撃に非常に有効
  - 標的型攻撃の対処は、時間・工数を要する場合が多い為、EPPとEDRの総合的な機能による絞り込みが重要
  - EDRでのPCの自動隔離機能は有効
- パターンファイル、ディープガードで対応済み
  - 既知・未知・新種を含め、広域で膨大な攻撃への対応として、非常に有効
  - 自動的にマルウェアを削除・隔離・駆除、怪しいプロセスをブロック

WITH secure

WithSecure™ EPPとEDRを組み合わせた複合的な対策のご提案

■ WithSecure™ Elements Endpoint Protection

- ファイルスキャン、振る舞い検知で、広範囲のマルウェアを対策
- 怪しいファイルの隔離・駆除、怪しいアプリケーションのブロックの自動化
- 未知のマルウェア対策に関して、誤検知と管理工数が少ない

■ WithSecure™ Endpoint Detection & Response

- WithSecure™ EPPでは対策が難しいファイルレスマルウェア、標的型攻撃にフォーカス
- Broad Context Detection™ にて、ログベースのEDRでは判定出来ないマルウェアを対策
- WithSecure™ EPPのディープガードの振る舞い検知と平行稼働する事で、誤検知、管理工数を減らす
  - ディープガード: 既知・未知・新種を含め、広域で膨大な攻撃への対応として、非常に有効
  - EDR: 対処に時間・工数を要する場合が多いファイルレスマルウェア、標的型攻撃への対応として、非常に有効
  - 正常な挙動に隠れたマルウェア(ファイルレスマルウェア)が猛威を振るっており、被害が大きいため、迅速なPCの自動隔離が重要

https://www.WithSecure™.com/jp-ja/solutions/software-and-services/elements-endpoint-detection-and-response

補足情報

■ライセンス課金対象（Elements EDR and EPP）

Elements EPPと同様に、各クライアントOS毎にご提供製品が異なり、EDR単体販売ではなく、
EDR+EPPのセット*でのご提供となります。 *デバイス課金となります

例）

・クライアントPC向け ＝ WithSecure™ Elements EDR and EPP for Computers（スタンダード or プレミアム）
・Windowsサーバ向け ＝ WithSecure™ Elements EDR and EPP for Servers（スタンダード or プレミアム）

■WithSecure™ EPPにコンポーネントが含まれており、管理ポータル上でEDRのライセンスキーコードを適応する事で、すぐに機能が有効となります（導入作業の簡素化）

WITH secure

＜参考＞
ファイルレスマルウェアを使用した標的型攻撃

標的型攻撃 - 起こり得る事件

普通の出来事

- シナリオ①
  1. 友人へ結婚祝いを計画
  2. 昼休みに金融サイトへログイン
  3. 自分の口座から結婚祝いを送金

従来の攻撃

- シナリオ②
  1. メールを受信、添付ファイルを開封
  2. **マルウェアが侵入**
  3. **マルウェアが起動**し、金融サイトへログイン
  4. 被害者の口座から送金

昨今の標的型攻撃

- シナリオ③
  1. メールを受信、添付ファイルは無し
  2. **ファイルレスマルウェアが侵入**
  3. **ファイルレスマルウェアがOSを乗っ取り**、金融サイトへログイン
  4. 被害者の口座から送金

表面的行動な行動は『口座からの送金』

事件ではない

事件・インシデント

ウイルス対策ソフトウェアのファイルスキャン、振る舞い検知で対策可能

ウイルス対策ソフトウェアのファイルスキャン、振る舞い検知では対策が難しく、EDRが必要

WITH secure

ファイルレスマルウェア - 概要

- ファイルレスマルウェアとは
  - ファイル型マルウェアを利用しない
  - マルウェアのサンプルが入手出来ない
  - ウイルス対策ソフトウェアでの対策が難しい

- ファイルレスマルウェアの侵入パターン
  - Officeの文書ファイル (マクロなどの機能や脆弱性の利用)
  - PowerShellスクリプトやシェルコードとの連携
  - 画像ファイルに不正コードを格納 (ステガノグラフィ)
  - 遠隔操作の通信を一般のWeb通信に紛れ込ませる
  - 遠隔操作の通信サーバとしてクラウドストレージなどの正規クラウドサービスを利用

昨今の標的型攻撃

- シナリオ③
  1. メールを受信、添付ファイルは無し
  2. **ファイルレスマルウェアが侵入**
  3. **ファイルレスマルウェアがOSを乗っ取り**、金融サイトへログイン
  4. 被害者の口座から送金

『口座からの送金』

事件・インシデント

ウイルス対策ソフトウェアの
ファイルスキャン、振る舞い検知
では対策が難しく、EDRが必要

WITH secure

ファイルレスマルウェア - 特 長

- ファイルレスマルウェアと思われるイベント
  - 標準プログラムの異常動作
  - 非標準の実行可能ファイルから実行中のプロセスの呼び出し
  - 予期しないスクリプトの実行
  - 標準プロセスから予期しないシステムツールの実行

- ファイルレスマルウェアの判定に必要となる情報
  - ファイルへのアクセス
  - プロセスの作成
  - ネットワーク接続
  - レジストリの書き込み
  - セキュリティ侵害の検出に関連するシステムログのエントリ
  - プログラム実行時に派生したスクリプト抽出

EDRは上記の情報を活用して、ファイルレスマルウェアなどの標的型攻撃を対策するソリューションです

昨今の標的型攻撃

- シナリオ③
  1. メールを受信、添付ファイルは無し
  2. **ファイルレスマルウェアが侵入**
  3. **ファイルレスマルウェアがOSを乗っ取り**、金融サイトへログイン
  4. 被害者の口座から送金

『口座からの送金』

事件・インシデント

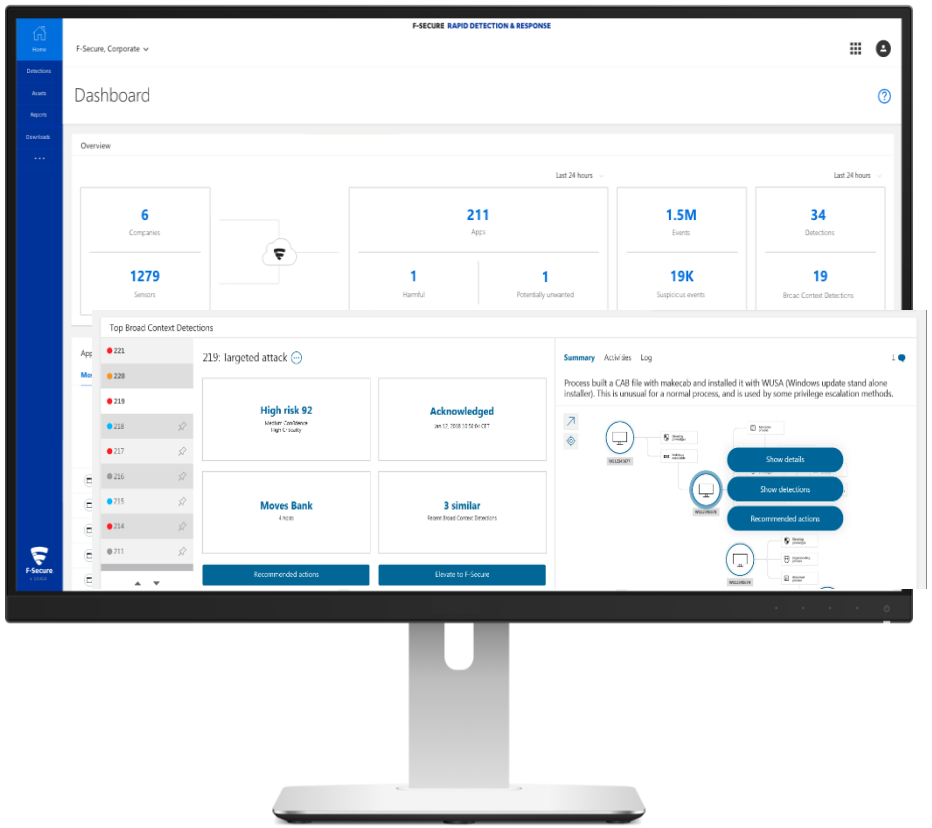
ウイルス対策ソフトウェアのファイルスキャン、振る舞い検知では対策が難しく、EDRが必要

WITH secure

Appendix（EDR）

WITH secure

WithSecure™ Endpoint Detection & Response 機能一覧



振舞い分析

BROAD CONTEXT DETECTION

WINDOWS センサー

アプリケーション インベントリ

インシデント マネジメント

集中管理

専門家の ガイダンス

MAC センサー

スレット インテリジェンス

ホスト隔離

自動対応

API

管理統合*

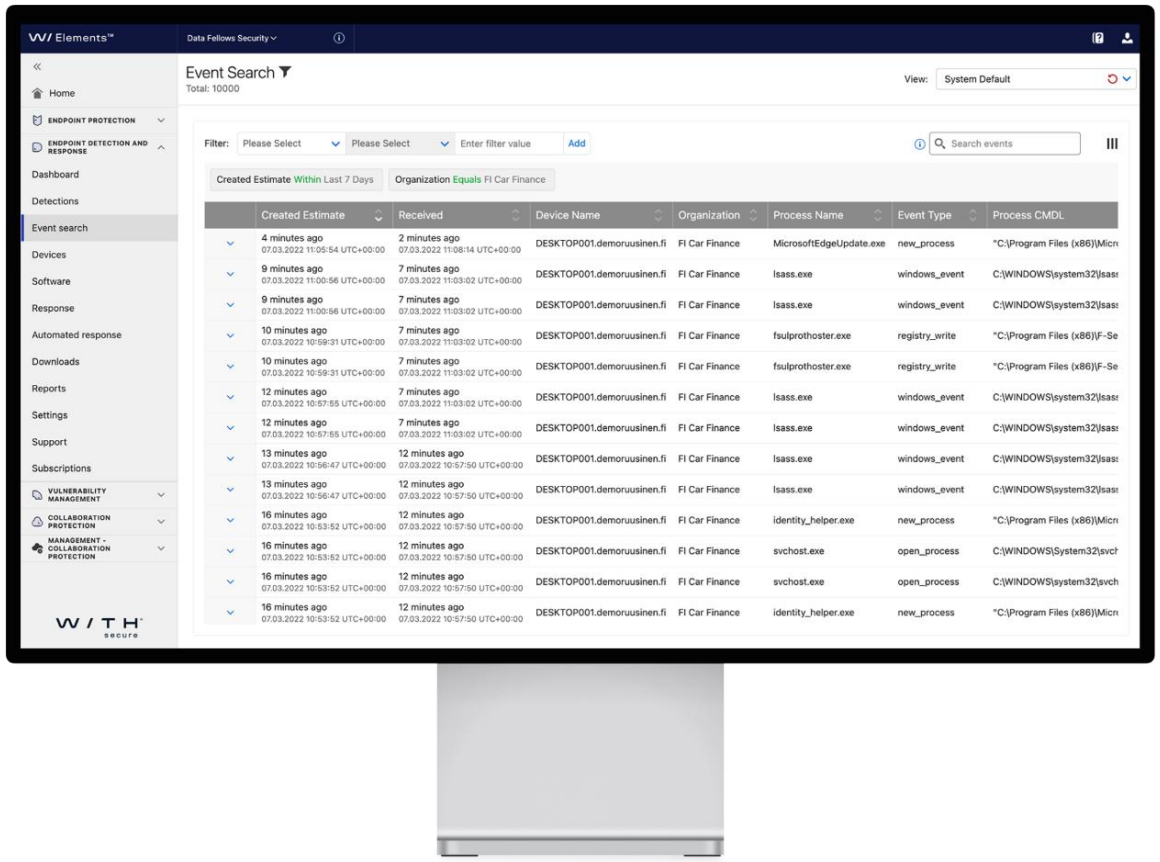
*コアリリース後に順次提供予定

WITH secure

検出タイプ

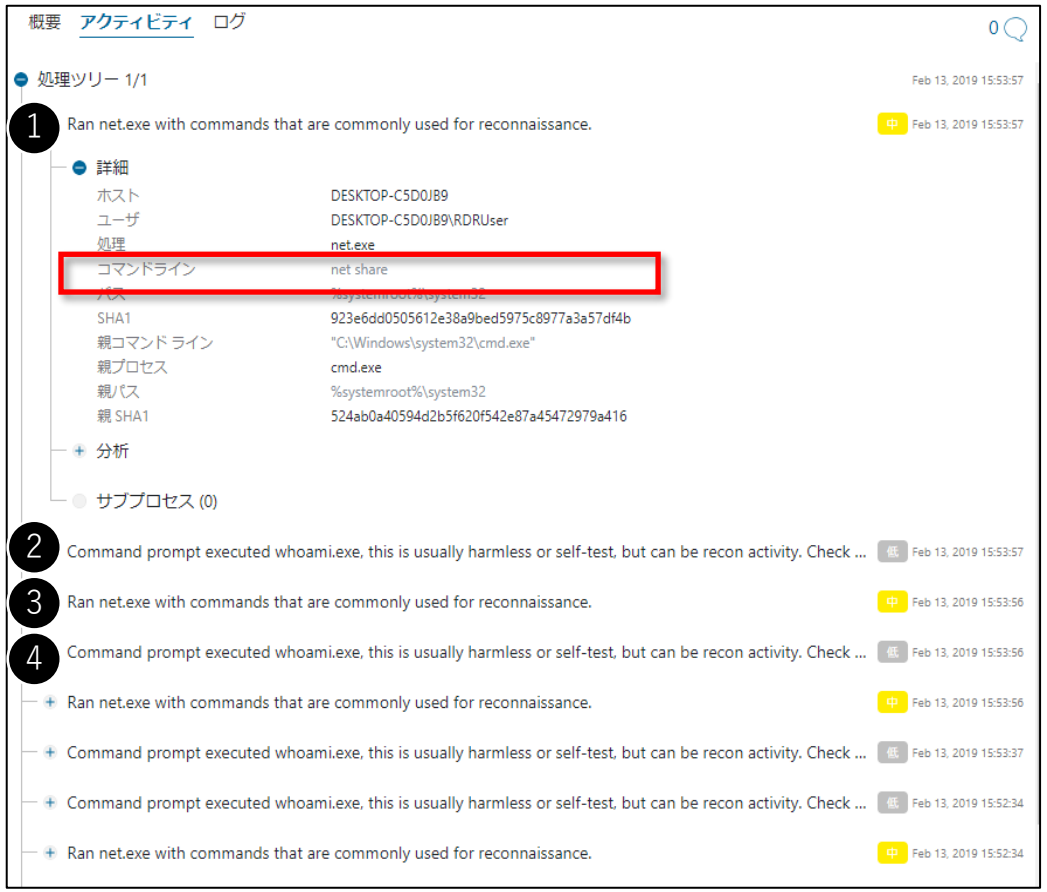
タイプ	説 明
異常	意味がない珍しいアクティビティや行動
異常なプロセス	プロセス自体が異常（実行されるべきものなど）
スクリプティングの濫用	Bash, Python, Powershell, cscriptなどスクリプト可能なコンポーネントの悪用。
異常なプロセス関係	例：outlook.exe, cmd.exe, powershellの実行など
異常なネットワーク接続	特定のプロセスに対するネットワークアクセスが異常（ネットワークポートへのバインディング、Twitterへの接続、ダウンロードなど）
永続性	持続性を獲得しようとしているプロセス（ログイン／ログアウトフック、crontab、ルートキット）
マルウェア	コンピュータ、サーバ、クライアント、またはコンピュータネットワークに損害を与えることを意図的に設計されたソフトウェア。
Cc ネットワーク接続	コマンドとコントロールへのネットワーク接続が開かれました。
ユーザ情報の変更	ユーザ情報を変更しているプロセス（ユーザの追加）
システムまたはツールの誤用	例：taskkill, net, psexec, procdumpなどスクリプトでないツールで攻撃に使用されているもの。
資格情報の盗難	mimikatzやkeyloggerまたは資格情報を盗むことができる他の方法の実行。
異常なライブラリまたはモジュール	異常なライブラリ／モジュール、不明なモジュール、不良なORSPモジュールをUSBから使用しているプロセス

センサーが収集するデータ



- ファイルへのアクセス
- プロセスの作成
- ネットワーク接続
- レジストリの書き込み
- セキュリティ侵害の検出に関連するシステムログエントリ
- プログラム実行時に派生したスクリプト抽出

WithSecure™ EDR - Windows標準コマンドによる偵察活動の検知



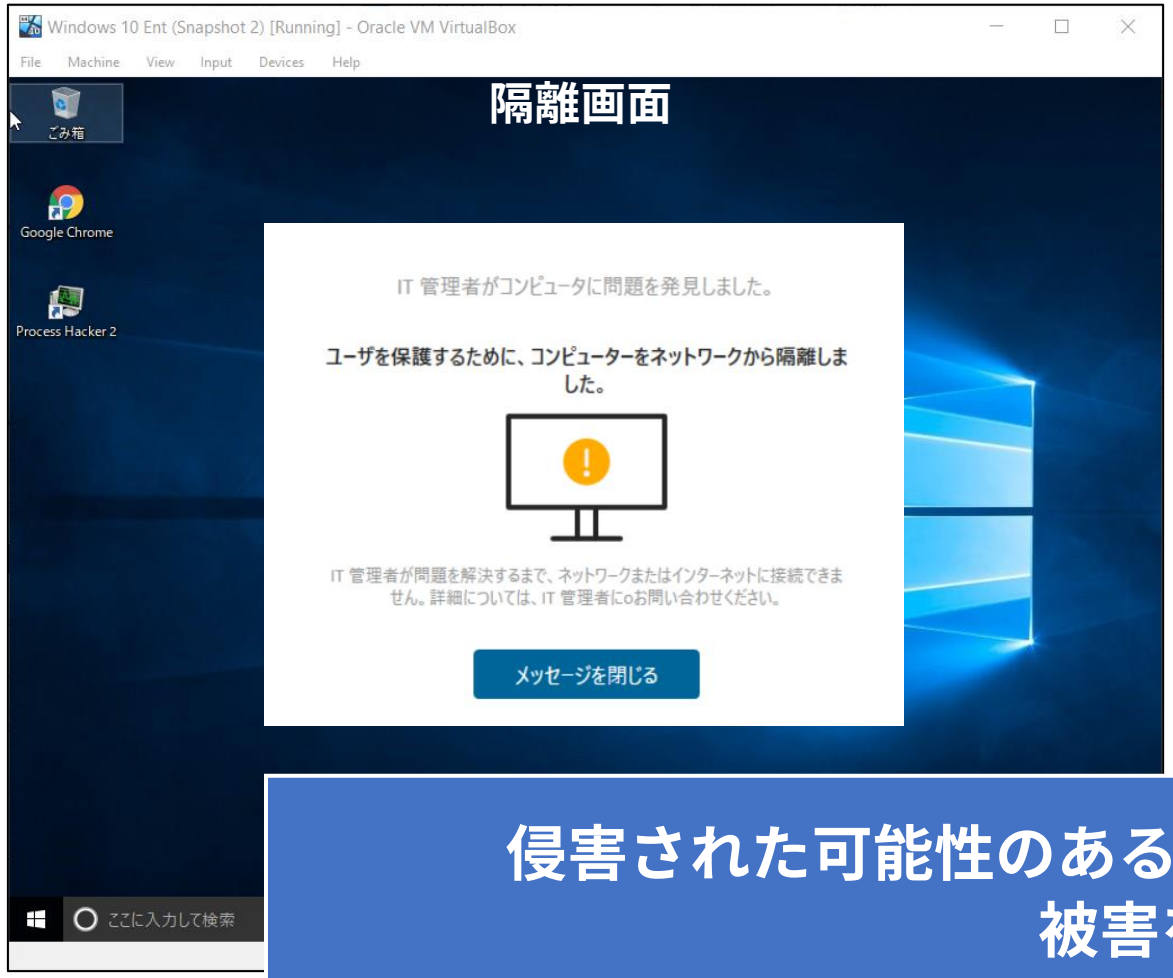

```
C:¥>net share
C:¥>whoami
C:¥>net view
C:¥>whoami /domain
C:¥>_
```

- 攻撃者はリモートからWindows標準コマンドを使用して偵察活動をしている可能性あり
- Windows標準コマンドを使用しているため、**ウイルス対策製品では検知できない**

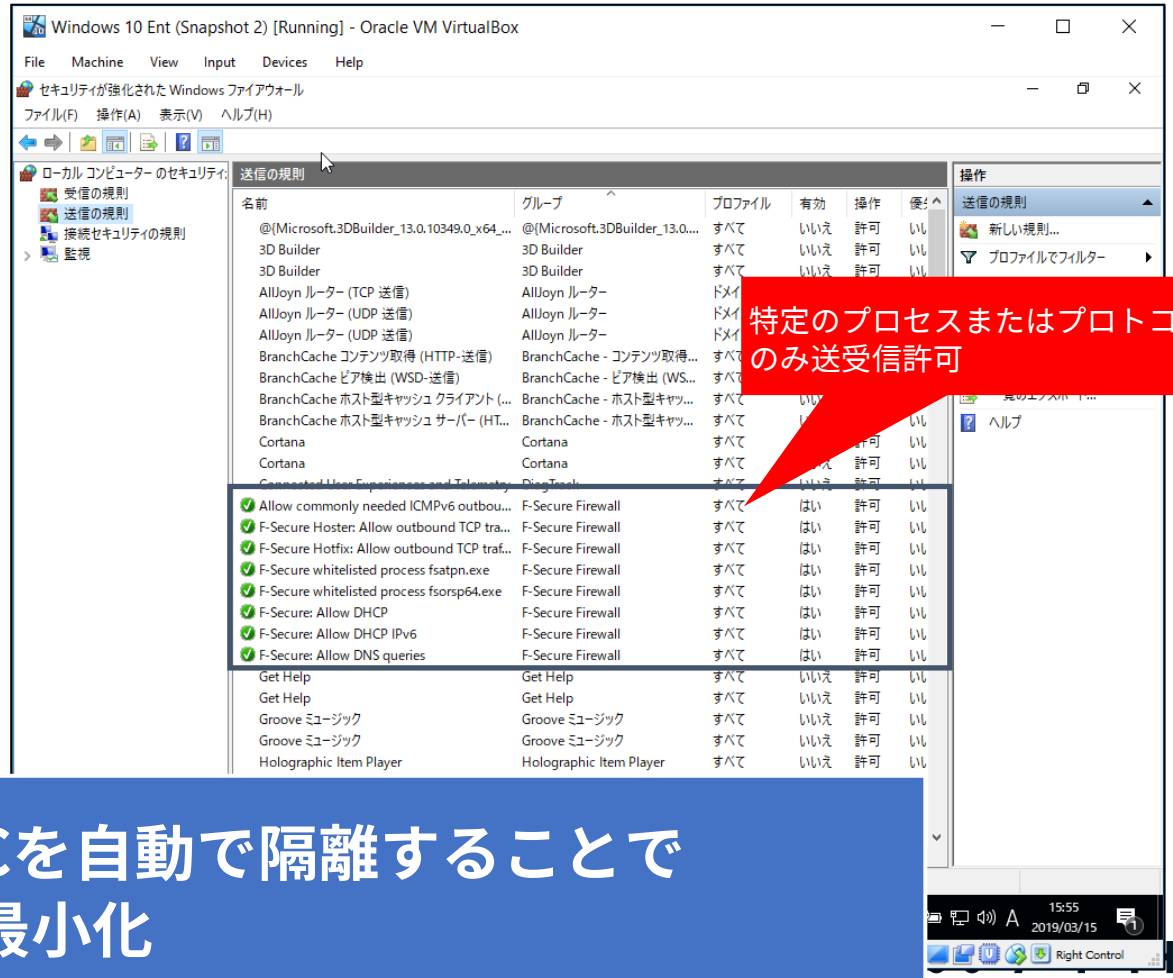
WITH secure

WithSecure™ EDR – ホストを隔離

リスクレベルの設定により自動隔離可能



隔離後のWindows Firewallの設定



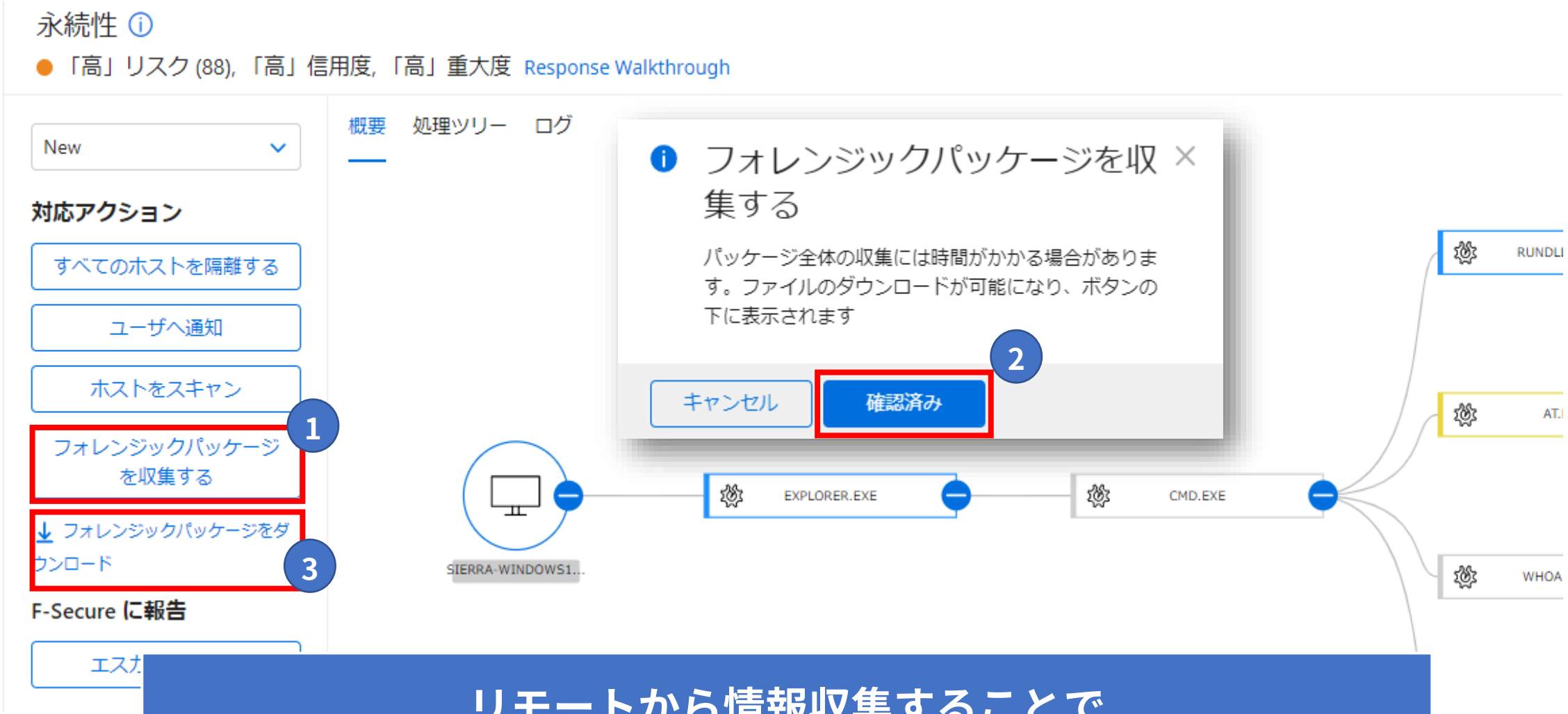
侵害された可能性のあるPCを自動で隔離することで被害を最小化

フォレンジックパッケージの収集

フォレンジックパッケージを使用すると、影響を受けるホストからより多くの情報を収集して、インシデントをより徹底的に調査できます。

フォレンジックパッケージには、デバイス（メモリとディスクの使用）、ファイアウォール構成、グループポリシー設定、ネットワーク設定とアクティビティ、Windowsプロパティ（プロセスリスト、スケジュールタスクなど）、Windowsイベントログ、およびレジストリ設定に関する情報が含まれます。

WithSecure™ EDR - フォレンジックパッケージを収集する



リモートから情報収集することで
テレワーク中のPCであっても侵害調査が可能

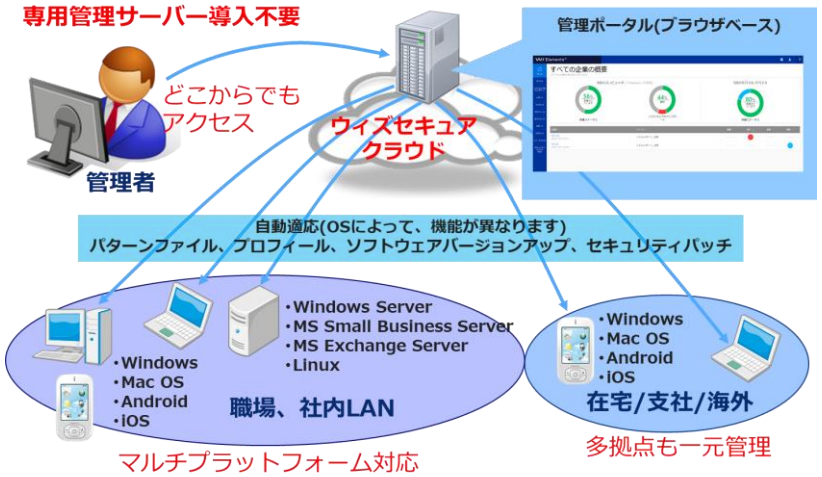
WITH secure

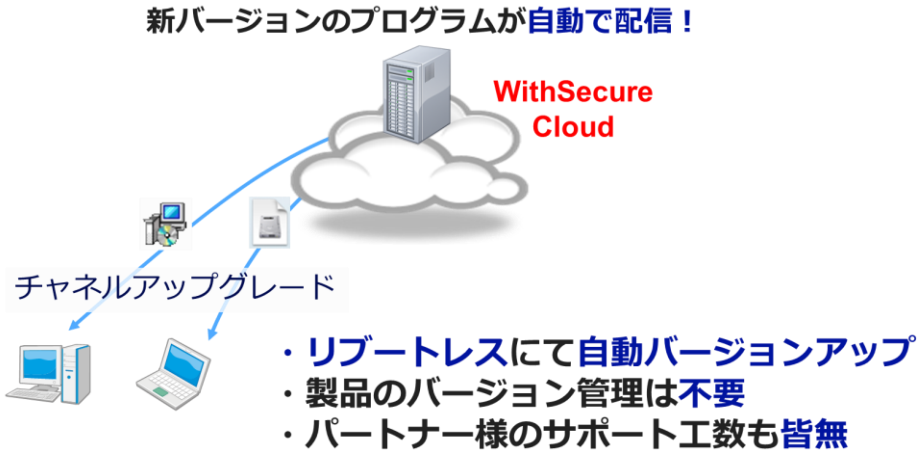
WithSecure™ Elevate

中小向けでも実績のあるクラウドサービス: EDRも自社運用が可能な時代

導入が手軽 ▶▶▶ 管理サーバーを立てる必要がなく、低コストで導入可能

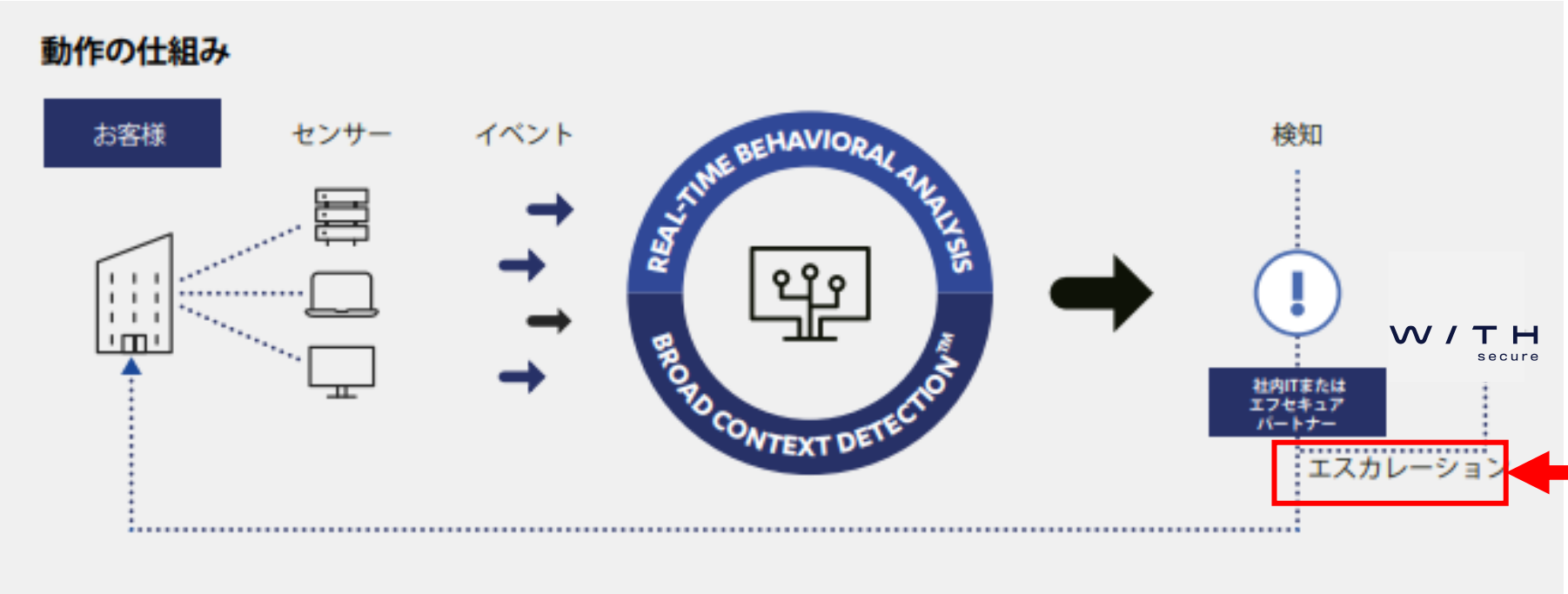
容易な管理 ▶▶▶ パターンファイル・製品のバージョンアップはリブートレスにて自動更新





- 台数も少量からご購入可能
- WithSecure™ Elevate の活用で内部運用も可能

WithSecure™ Elevate



インシデント調査を
WithSecure にエスカレート

WithSecure™ Elevate

ウィズセキュアのサイバーセキュリティ専門家に
調査を依頼することが可能

WithSecure™ Elevate

MSSまたは社内IT部門での利用が可能なチケットパッケージを提供

種類	内容	チケットパッケージ			
		個別	2枚	3枚	10枚
脅威の検証 Threat validation	「脅威の検証」フェーズでは、 ■ WithSecure™ のアナリストは、Broad Context Detection™ が脅威、誤検知、または疑わしいものかどうかを判断します。 ■ 完全な調査ではなく、迅速な検証のみを目的としています。 インシデントが既知の脅威である場合、脅威への対応方法に関するガイダンスが表示されます。検出が疑わしい場合、インシデントを個別に管理するか、調査リクエストを作成できます。	1枚	1枚	2枚	8枚
脅威の調査 Threat investigation	「脅威の調査」フェーズでは、 ■ WithSecure のアナリストがBroad Context Detection™ を分析し、対応方法をご提案します。		1枚	1枚	2枚

（対応は全て英語）

WITH secure™