はじめに

対象者
- オンプレミス製品を利用中の既存ユーザ様、パートナー様が対象になります
- 尚、完全クローズド環境やスタンドアロン運用のお客様におかれまして、本移行フローにてご対応ができない可能性がある点についてはあらかじめご了承くださいませ。

Webinar 内容（約2時間）
- Elements製品の概要と既存ユーザ様向けの移行優遇措置について（30分）
- オンプレミス製品からElements製品への移行について（1時間20分）
  - 移行前の動作要件/環境の確認について
  - 現在の運用構成から移行後の運用構成について
  - 移行フロー概要
  - 移行フローの詳細説明（別紙 ①～⑪手順）

・質疑応答（10分）

注意点
- 本Webinar中はマイク等はオフとなるため、ご質問がある場合は適宜「QA」ボタンにて、テキストにてご質問をお願いいたします。挙手ボタンはございますが、ご利用なさらないようにお願いいたします。
- 後日、本ウェビナーへのご参加頂いたお客様、パートナー様向けに当日のウェビナー動画と質疑応答後のQA表をお送りする予定でございます。
- ご不明点やお問い合わせがある場合は、弊社代表アドレス＜japan@withsecure.com＞宛、件名「8月27日開催ウェビナーについて」にてご連絡をお願い申し上げます。

CLIENT CONFIDENTIAL

WithSecure EPP/EDR 製品紹介

CLIENT CONFIDENTIAL

EPP (Endpoint Protection Platform) とEDR (Endpoint Detection and Response) 役割の違い

マルウェア(Malware)

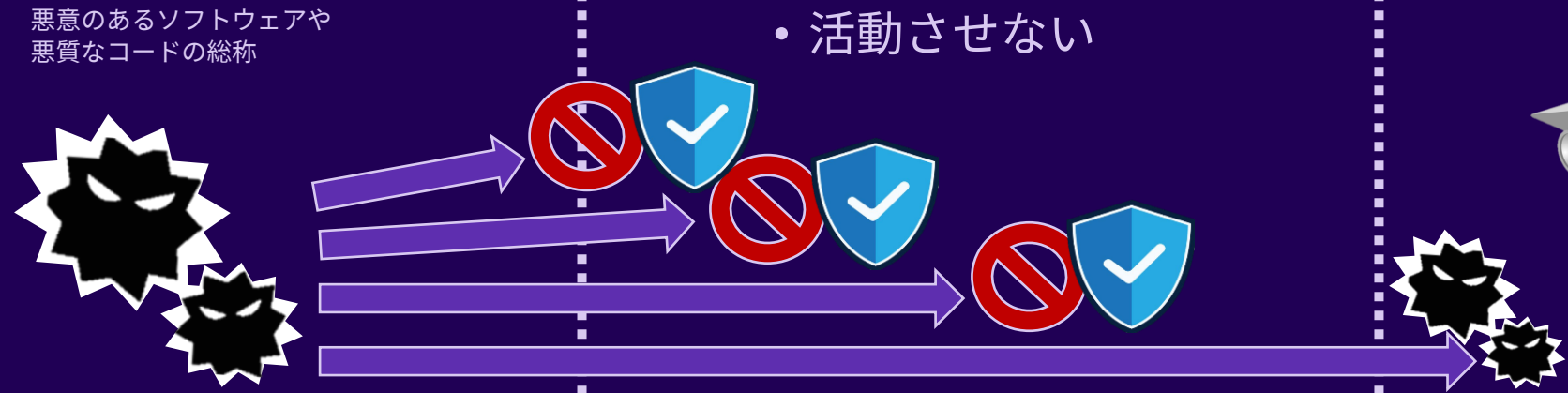
悪意のあるソフトウェアや
悪質なコードの総称

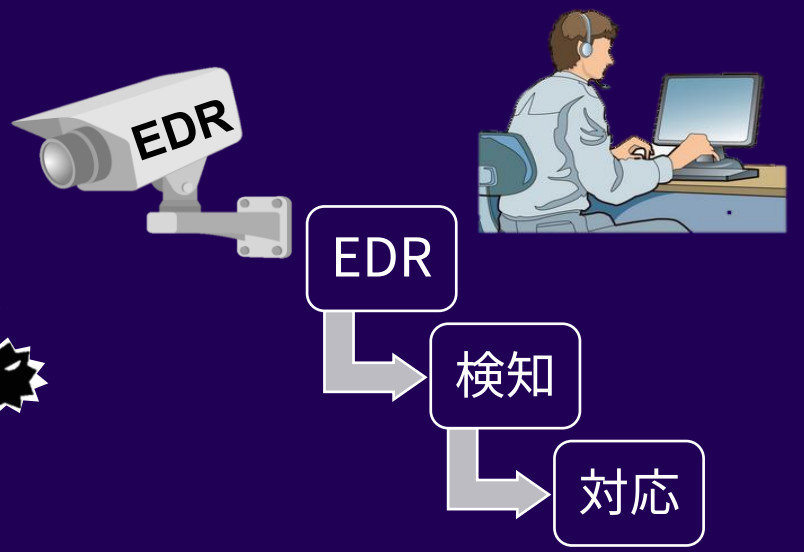
EPP

- 侵入/感染を防ぐ
- 感染を防ぐ
- 活動させない

EDR

- 侵入後の検知
- インシデント対応





今も昔もエンドポイントセキュリティは最後の砦

いまの時代は企業規模を問わずEPP＋EDRは絶対に必要

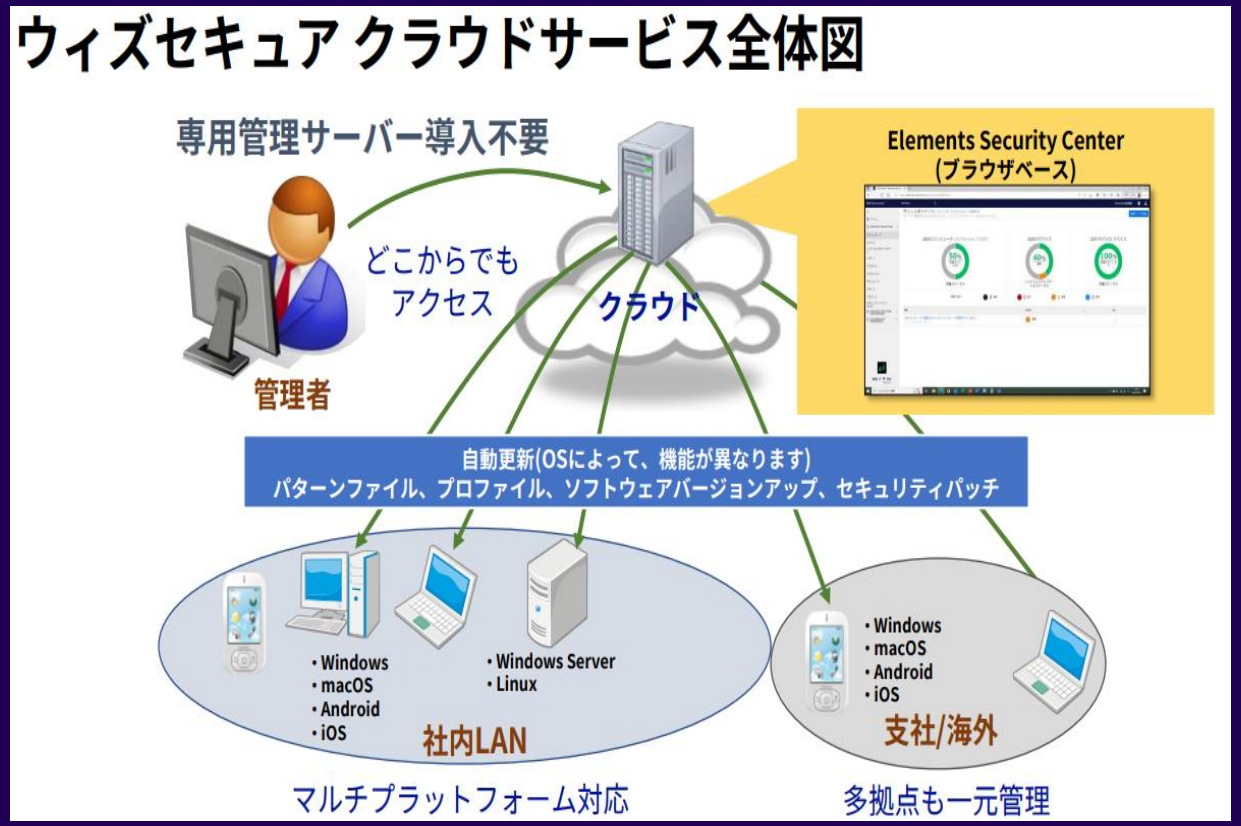
CLIENT CONFIDENTIAL

Elements EPP（クラウド）の特長

Elements EPPのメリット

- 物理サーバ不要（コストカット）
- どこからでもアクセス可能
- マルチプラットフォーム対応
- 1Lから購入可能

- WithSecure Elementsは
  - 1つのエージェント (追加の作業不要)
  - 1つのポータル (一元管理)
  - 資産管理やパッチ管理の機能も搭載



CLIENT CONFIDENTIAL

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/
ロールバック
(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

静的解析
パターンファイル検査
クラウド上で検査
＋ AI解析

パスしたファイルは
振る舞い検知へ

動的解析
リアルタイム挙動解析
ファイルが開き切る前に
挙動を見てブロック

振舞い検知
実行中のプロセスも
継続監視
危険な挙動を察知し
即座にブロック

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

ランサムウェア対策：
データガード(プレミアム版)/ロールバック

～データガード～

F-Secure

あらかじめ登録されている
業務で使用するアプリの操作

普段どおりの
ファイルの保存や加工が可能

～　ロールバック機能とは　～
「ランサムウェアのような悪意のある攻撃を検知し、侵害前の状態に戻す機能」

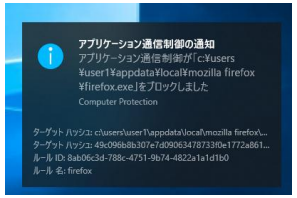
Webサイトのカテゴリフィルタリング

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	

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。

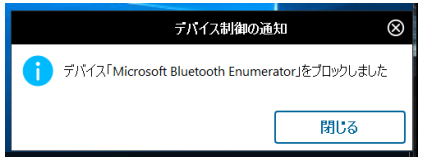


パッチ管理：脆弱性対策

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

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



CLIENT CONFIDENTIAL

オンプレミス製品との機能差分

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		●		● ランサムウェア対策に
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		●		● EMOTET対策に
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。

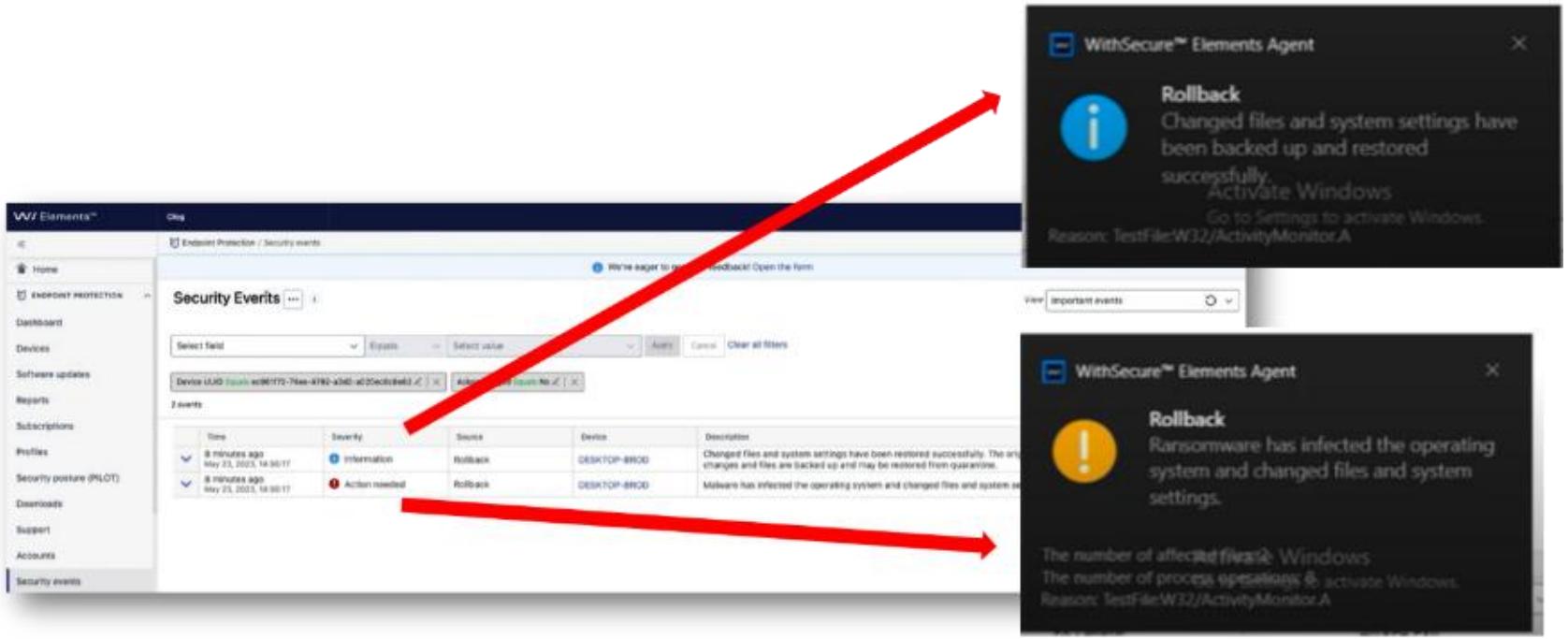
※非インターネット環境でのElementsシリーズの利用については、今後リリース予定のElements Connectorを併用することで運用可能となります。
Elements Connectorを導入した端末がインターネットに接続されていれば、配下の端末をクラウド管理できるようになります。
ただしElements Connector導入端末だけはインターネット接続が必要となるので、完全クローズ環境ではご利用いただけません。

CLIENT CONFIDENTIAL

ランサムウェア対策に特化した機能が充実①

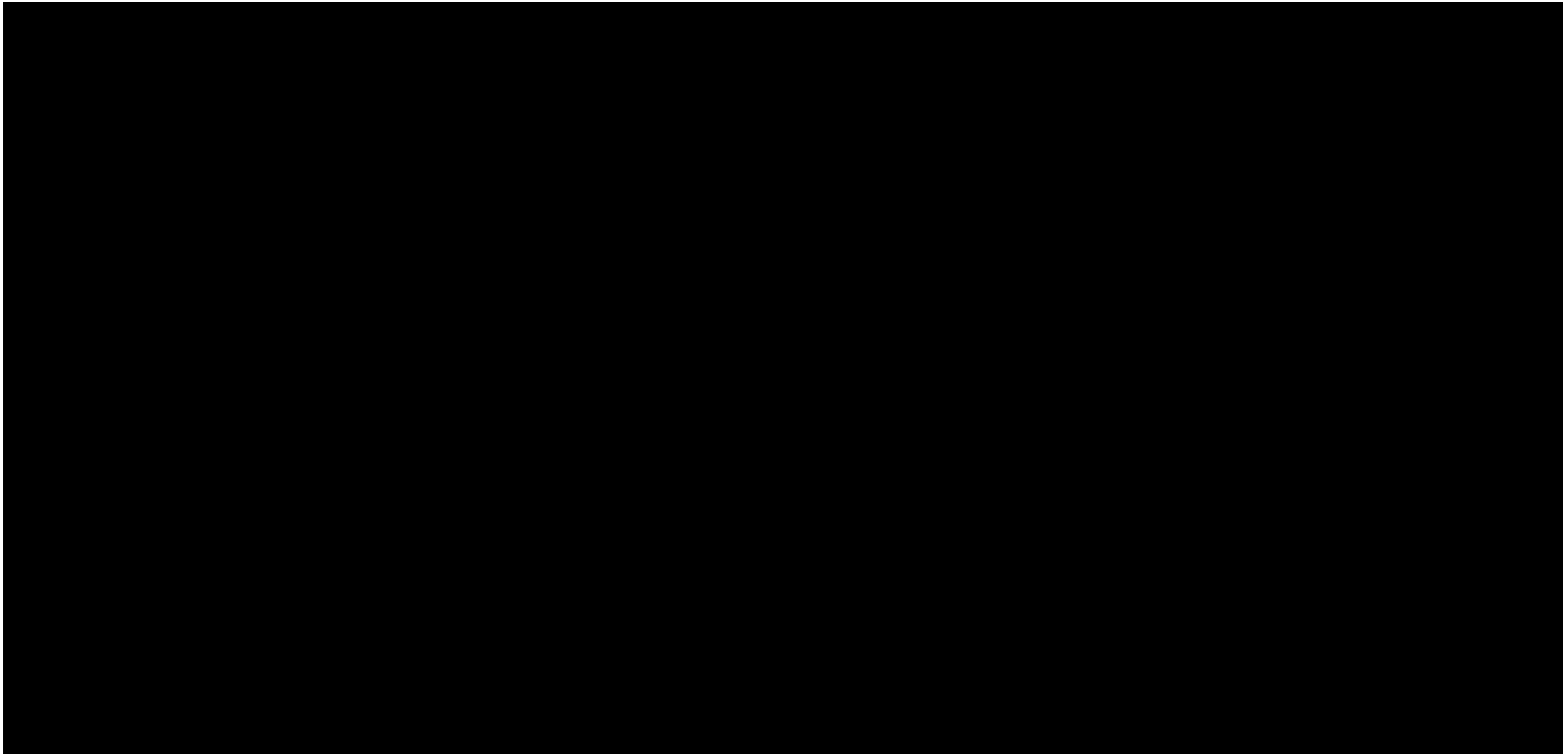
➢ロールバック機能

- ➢ ランサムウェアのような悪意のある攻撃を検知し、侵害前の状態に戻す機能



CLIENT CONFIDENTIAL

ロールバック　デモ動画



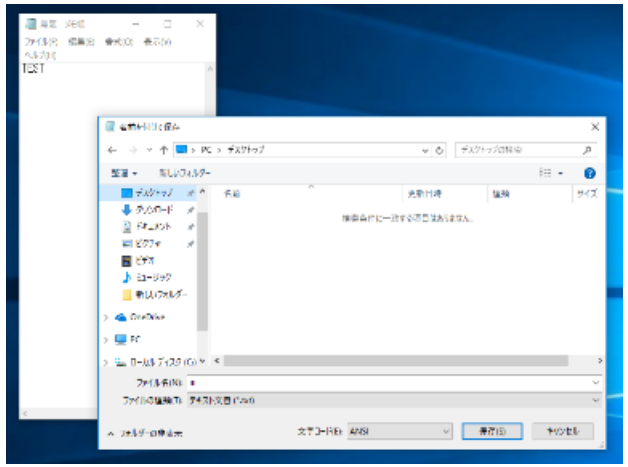
CLIENT CONFIDENTIAL

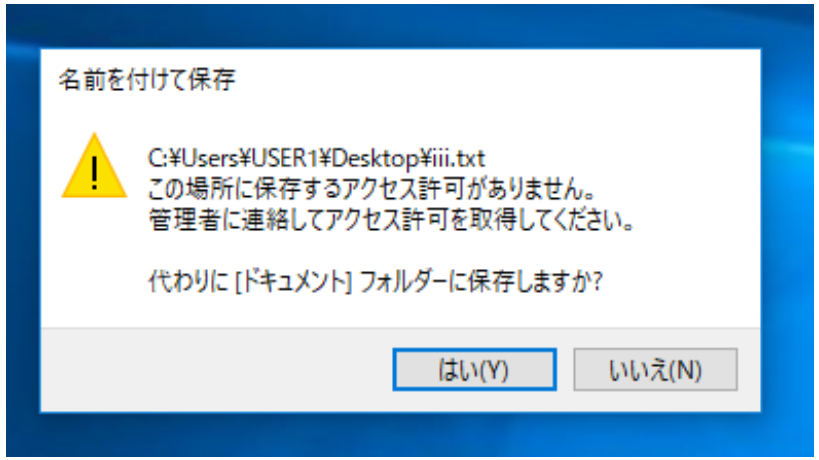
動画URL：https://youtu.be/HodNNLcileI?si=jHr2mCL_Yb5Ik9Qs

ランサムウェア対策に特化した機能が充実②

➢データガード機能（*プレミアム）

- ➢ 信頼できるアプリケーションのみ監視対象のフォルダにアクセスを許可する機能。





CLIENT CONFIDENTIAL

ランサムウェア対策に特化した機能が充実③

➢ サーバー共有保護の設定および動作概要

Windowsサーバー用プロファイルで
ON/OFFおよびオプションを設定

1. サーバー共有に対して新しいユーザーがファイル変更を行うと、特定のプロセスIDとともに変更したユーザーのSIDが記録される
2. ロールバック機能と同様に、ファイル変更手順を記録しながらバックアップを作成
3. ファイル変更が不正なものと判断された場合、該当ユーザーは一定期間接続が解除される
4. ロールバック機能と同様に、自動的にバックアップファイルからオリジナルファイルを復旧

CLIENT CONFIDENTIAL

脆弱性対策：パッチ管理

パッチ管理機能により最新のソフトウェアにアップデートが可能。
デフォルトで常時最新適用もしくは都度パッチ適用として対応が可能

CLIENT CONFIDENTIAL

デバイスのセキュリティポスチャ

CLIENT CONFIDENTIAL

Elements管理ポータル：簡易版IT資産管理

EPPの情報だけではなく、インストールしている端末の
インベントリ情報の取得が可能。

簡易版IT資産管理ツールとしても活用ができる。

例：OSバージョン、BIOSメーカー、システムドライブ空き容量等

CLIENT CONFIDENTIAL

Elements管理ポータル：アクションボタン

CLIENT CONFIDENTIAL

WithSecure Elements EPP おすすめポイント

✓ウィズセキュア独自のディープガードやAIによる多層防御（他社EPPとの差別化）

✓ランサムウェア対策に最適なロールバックとデータガード機能を搭載

✓簡易版IT資産管理機能として活用可能（OS情報の可視化、システムドライブの容量等）

✓パッチ管理による脆弱性対策

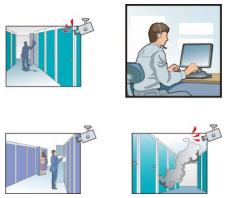
CLIENT CONFIDENTIAL

EDRとは？

EDRでは、
・アプリケーションの実行
・ファイルアクセス
・ネットワーク接続等
を記録して、クラウド上で解析し、侵入や侵害を特定

侵入を検知できるのは
EDR

監視センター



監視カメラ

人感センサー

オフィス空間や店舗では

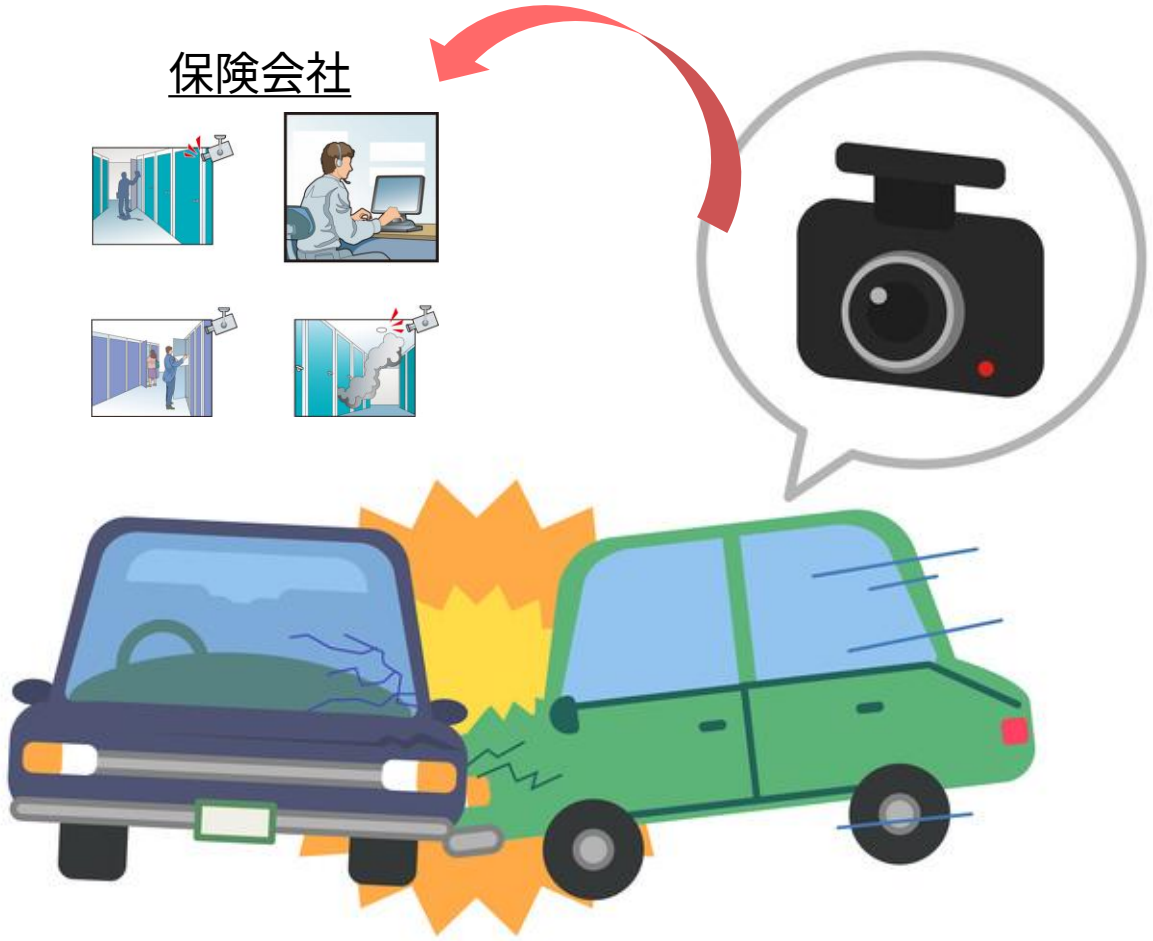
監視サービス

サイバー空間では

CLIENT CONFIDENTIAL

WITH secure

EDRを車に例えると



ドライブレコーダーで

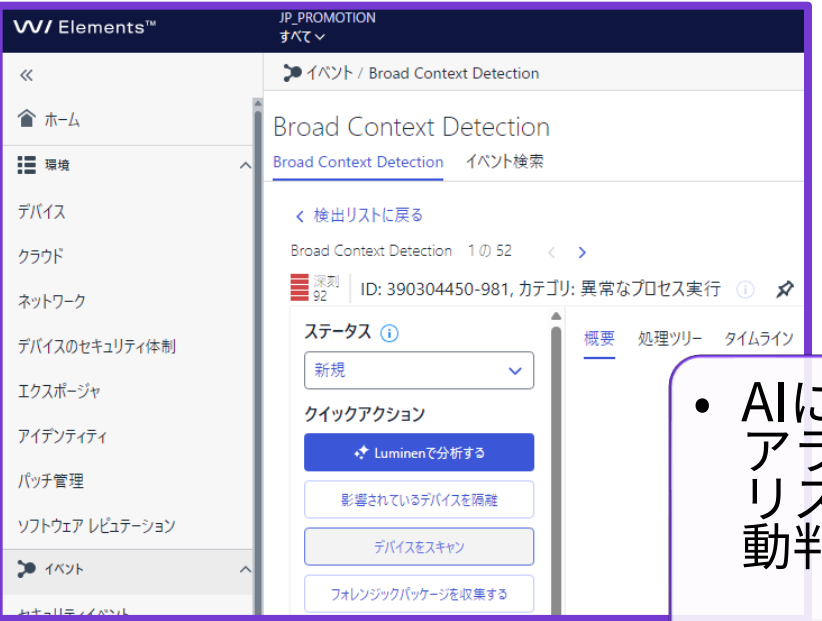
運転中の前方を録画

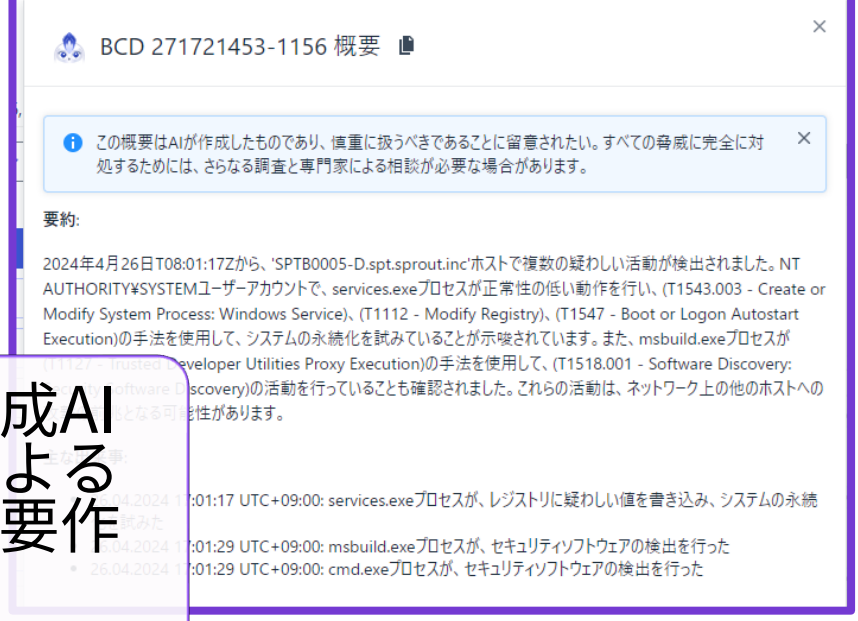
することで事故当時の状況を確認することができます。

EDRではPC内のインシデント発生時の状況を確認できます。

CLIENT CONFIDENTIAL

Elements EDR の特長





- AIによるアラートリスク自動判別

- 生成AIによる概要作成

検知

可視化

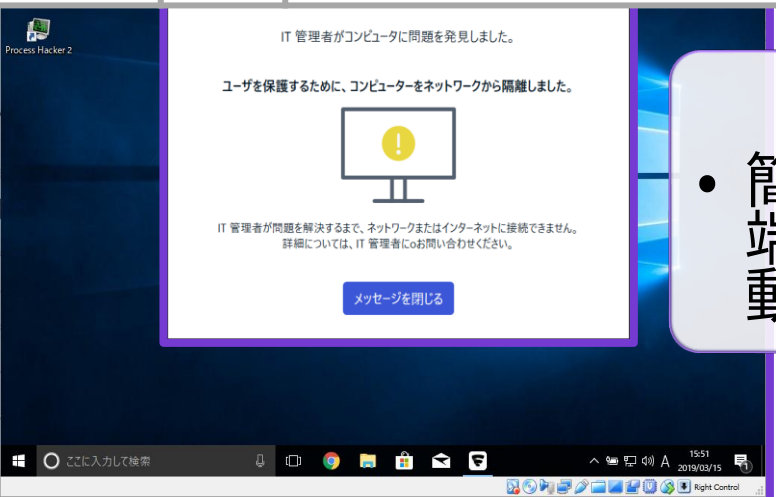
封じ込め

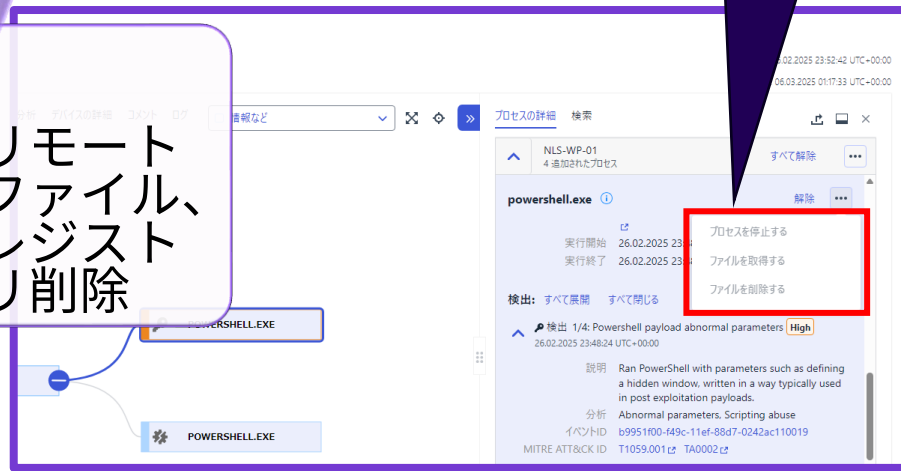
復旧

- 簡単な端末自動隔離

- リモートファイル、レジストリ削除

スコア	重大度	異常なサイバー活動の可能性
0		可能性があるがリスクとしては判断できていない
36 ～ 65		可能性はあるがリスクとしては低い
66 ～ 75		可能性はあるが大きな影響はない
76 ～ 90		可能性は高く、深刻な被害をもたらすと考えられる
91 ～ 100		可能性は高く、重要なホストが危険にさらされていると考えられる

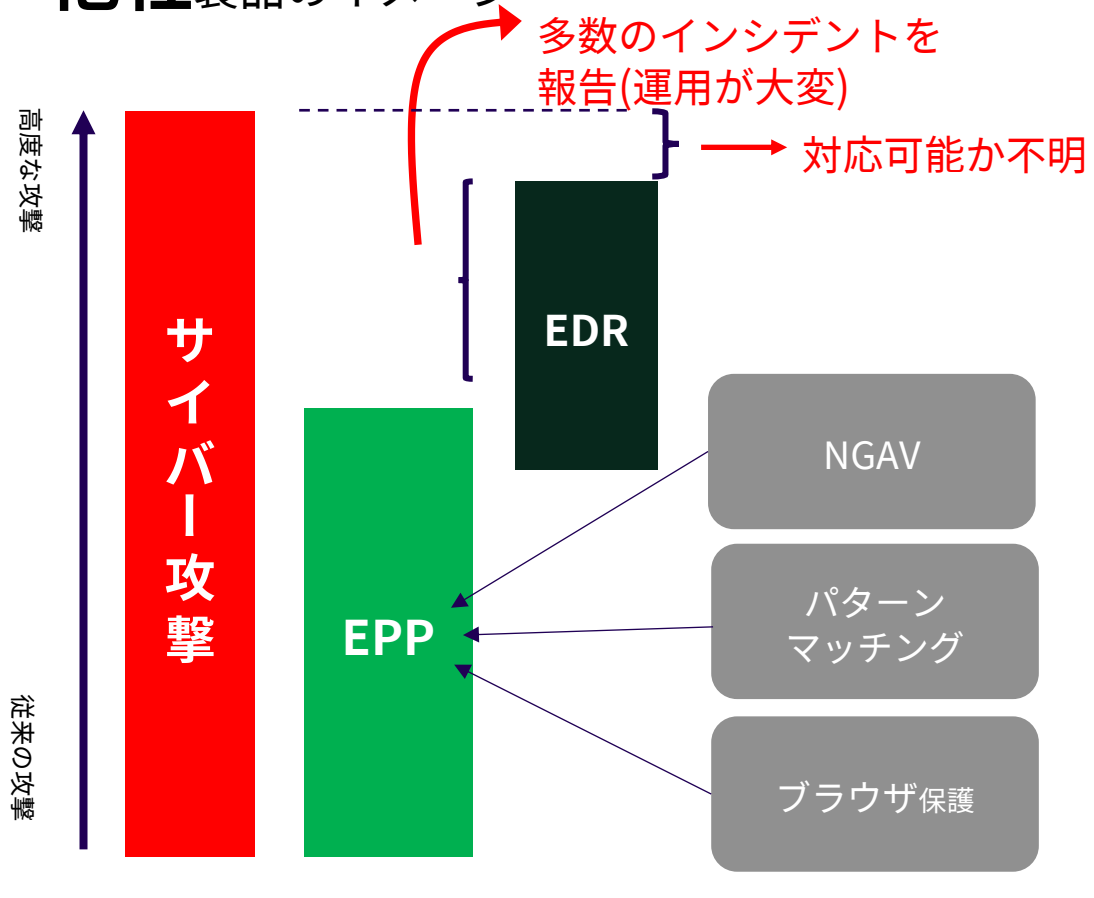




WithSecure Elements EDR

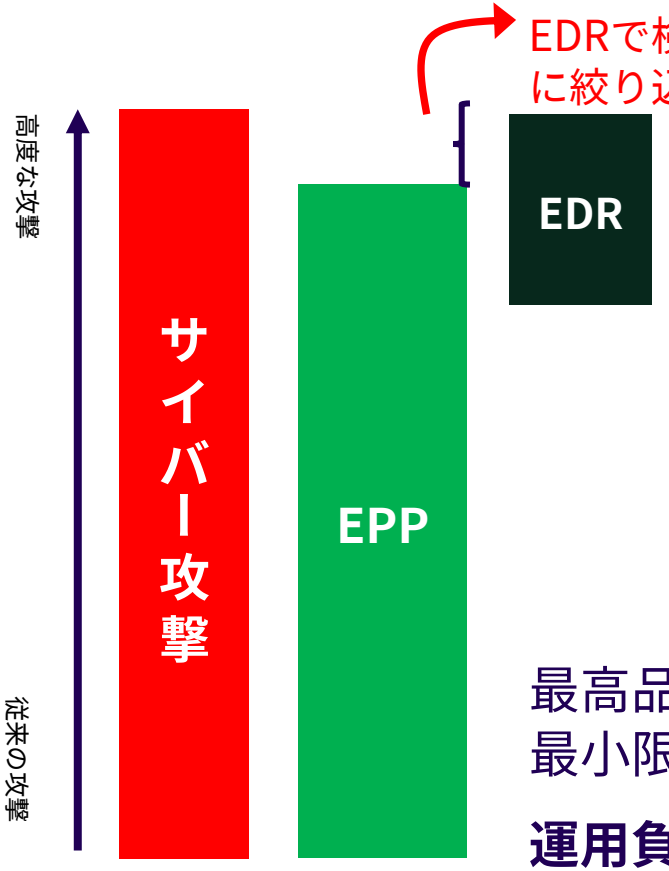
最高性能のEPPと組み合わせることで運用負荷を最小限に抑える！

他社製品のイメージ



EPPでカバー出来る範囲が少ない

WithSecure のイメージ



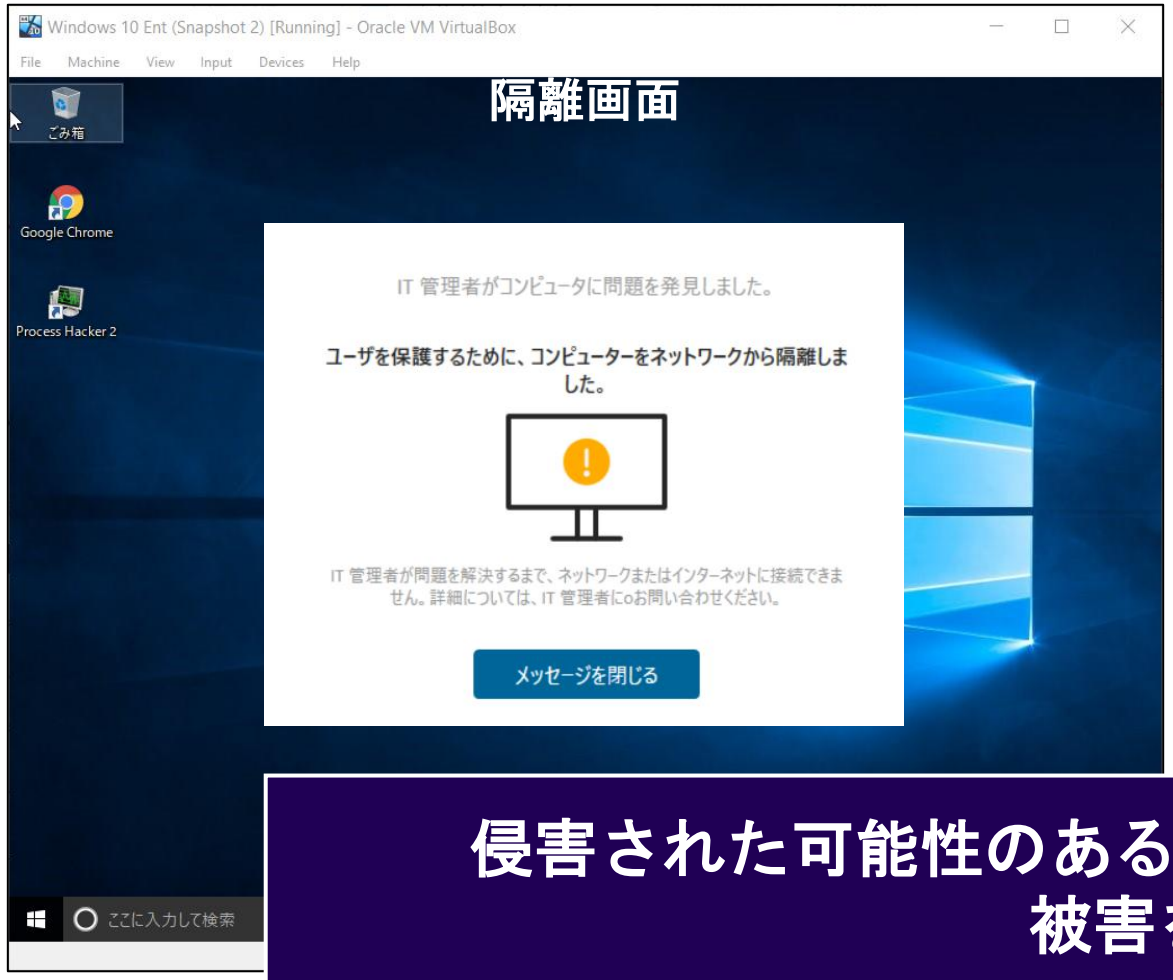
最高品質のEPPでインシデントを
最小限に絞り込み。

運用負担と被害リスクの両方を少なくできる！

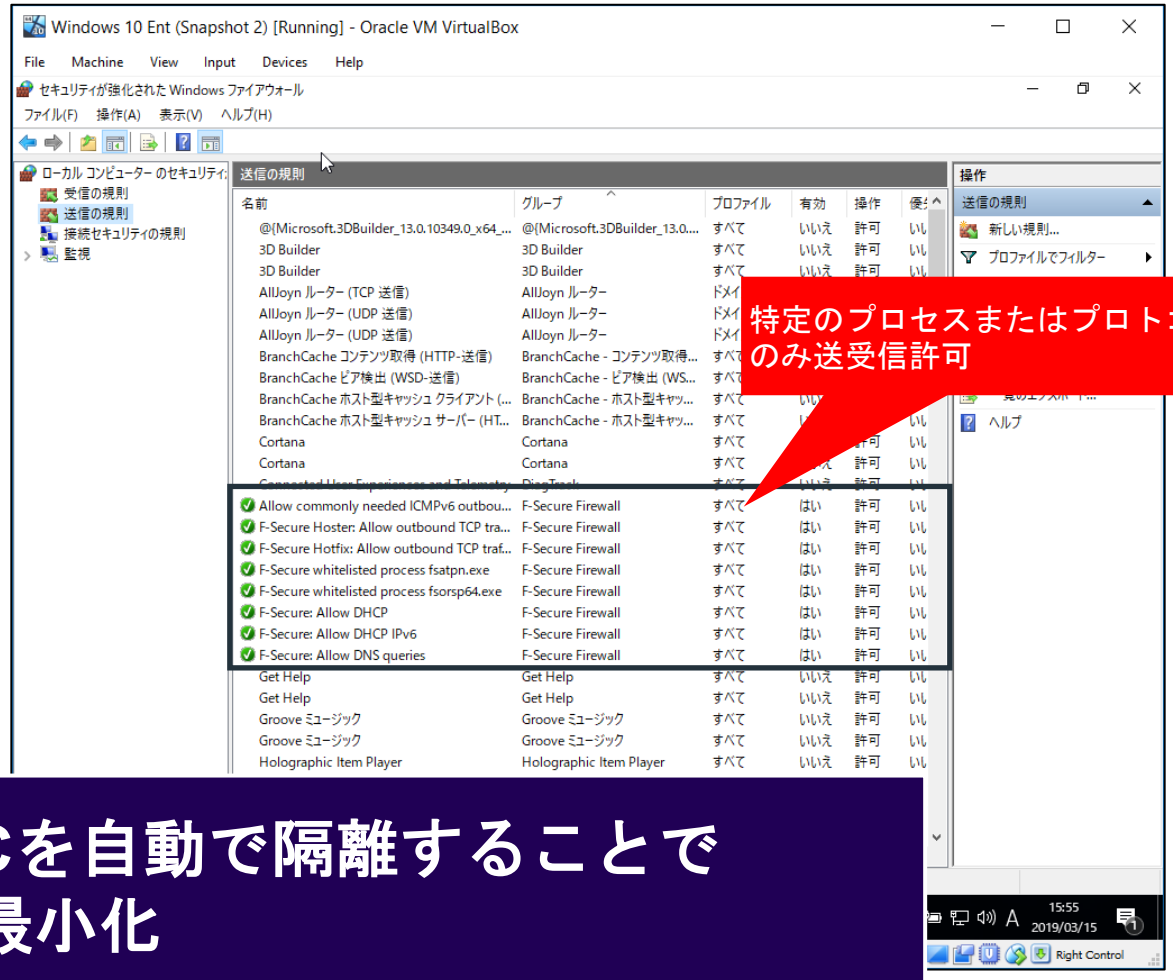
CLIENT CONFIDENTIAL

WithSecure Elements 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

CLIENT CONFIDENTIAL

WithSecure Elements EPP + EDR おすすめポイント

✓ウィズセキュア独自のEPPで高度な検知が前提なため **運用負担が少ない**

✓危険を検知したら、設定した危険度に応じて **自動隔離**し 被害拡大防止

✓EDRへライセンス変更したら **ワンクリック** でEDR機能がONにできる

CLIENT CONFIDENTIAL

EPP移行に伴う優遇措置について（既存ユーザ様向け）

ビジネススイート製品は 2027 年 12 月 31 日に製品の提供・サポートの終了予定となるため、以下の通り移行優遇措置をいたします。

✓**Elements 製品でのご契約後から 最大1 年間はビジネススイート製品の併用を許諾いたします**

（ビジネススイート製品の証書発行はされない為、従来使用頂いているキーコードをご流用ください）

✓**2025 年中※1にビジネススイート製品から Elements 製品に移行頂けるお客様におかれましては、従来の据え置き価格にてご提供いたしますので、１年以内の移行完了をお願いいたします**

※1：2025年12月22日ご注文到着分まで

※2：特価対応分などは除く

（参考）ビジネススイート製品の価格改定ならびに EOL に関するお知らせ

https://www.withsecure.com/content/dam/with-secure/ja/resources/2025-04-01_Important_Notice-BS_Price_Change_and_EOL_Notification.pdf

CLIENT CONFIDENTIAL

CLIENT CONFIDENTIAL

Appendix

CLIENT CONFIDENTIAL

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。

1ライセンスから購入可能
コスパ最強、クラウド管理型エンドポイントセキュリティ

WithSecure™ Elements Endpoint Protection (EPP)

クラウド管理型製品は専用の管理サーバーの導入が不要で、マルチプラットフォームに対応しています。
（対応OS：Windows | Mac | Linux | Android | iOS）

WithSecure™ Elements EPPの特長

- **1ライセンス**から購入が可能
- ウィズセキュア独自のディープガードやAIによる**多層防御**
- **ランサムウェア対策**に最適なロールバックとデータガード機能を搭載
- バンキングサイト接続保護機能により、**安全に銀行のサイト**へアクセス可能
- 3階層に対応した**マルチテナント**により、販売店様による管理を実現

ランサムウェア対策に特化した機能（Windows版のみ）

- **Dataguard(データガード)**
  - ランサムウェアに感染時に指定したファイルを**暗号化ブロック**
- **Rollback （ロールバック） 機能**
  - ランサムウェアのような悪意のある攻撃を検知し、侵害前（暗号化前）の状態に戻すことが可能

多様な機能を搭載！

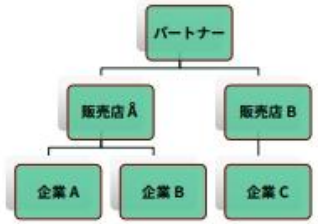
* Windows版に搭載されている機能です。

❖ Dataguard 及びアプリケーション制御はプレミアム版に搭載されている機能です。

販売店様の管理に最適な最大3階層マルチテナント

販売店様が販売したユーザー様については、**3階層**までElementsのクラウド管理ポータル上で保有ライセンスの状態が確認可能！

❖ 2階層以上管理希望の場合は諸条件ありのため、メーカーまで要問合せ。



WithSecure™ Elements EPPシリーズ

WithSecure™ Elements Security Center
サーバレスで各セキュリティ対策ポイントを安心・簡単に一括管理

WithSecure™ Elements EPP for Computers
WindowsとMacのエンドポイントに対する最新のセキュリティ対策

WithSecure™ Elements Mobile Protection
モバイルデバイスのマルウェア対策、VPNを含むiOSとAndroidデバイスに対するセキュリティ対策

WithSecure™ Elements EPP for Servers
Windows、Linux、およびCitrixサーバに対するセキュリティ対策

Windows/Mac向け:	WithSecure™ Elements EPP for Computers（スタンダード or プレミアム）
Windowsサーバー向け:	WithSecure™ Elements EPP for Servers（スタンダード or プレミアム）
Linuxサーバー向け:	WithSecure™ Elements EPP for Linux
iOS/Android向け:	WithSecure™ Elements EPP for Mobiles

ウィズセキュア株式会社パートナー営業本部
- 〒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@withsecure.com | https://www.withsecure.com/

2024.11

CLIENT CONFID

中小企業に最適！1ライセンスから購入可能
クラウド管理型EDRソリューション

WithSecure™ Elements EDR＆EPP

侵害時の被害を最小化しビジネスを止めない運用を実現

WithSecure™ Elements EDR＆EPPは
企業のIT環境とセキュリティ状況を単一の統合管理コンソール上に可視化し、サイバー攻撃を迅速に検知・表示し、ガイダンスに沿った侵害の対応が可能
(対応OS : Windows/Mac/Linux)

自動車保険に例えると…

自賠責保険	Mac・Windows標準搭載のセキュリティ
任意保険	有償版セキュリティソフト
安全装置（ドラレコ・エアバック）	EDR（感染した後の対応）

ドラレコやエアバッグを装着する感覚でEDR導入がおすすめ
安全装置があると万が一の時に安心！

ドラレコ搭載していると、事故発生時の運転状況を可視化
エアバッグを装着していると、事故発生時の被害を最小化

EDRを導入すると

感染時の感染経路が確認でき、
自動隔離で被害拡大を阻止し、被害を最小限にできます。

WithSecure™ Elements EDR＆EPP のポイント

- **1ライセンス**から購入が可能
- W/Elements EPPは高度な検知機能を備えており、**運用負担を大幅に減らせます**
- 危険を検知したら、設定した危険度に応じて **自動隔離し** 被害拡大を阻止
- Elements Security Center（管理ポータル）上から **ワンクリック** でEDR機能をONにできる

入れておくだけで安心できる

- インシデントのリスクレベルに応じて、端末の**自動隔離**が可能
- 調査する場合に**追跡のためのデータ**を遠隔操作でも簡単に取得可能

自動隔離ができるのは
ウィズセキュアだけ
他社は手動隔離のみ

SOCサービスによるセキュリティ体制の堅牢化

- W/ Elements EDRはSOCサービスなしでも効果的です。
- より堅牢なセキュリティ体制構築のため、EDR導入後に弊社パートナー様のSOCサービスを導入できます。

生成AIアシスタント W/ Luminen が検知した脅威を要約

- 標準搭載の生成AIアシスタント **W/ Luminen** が、感染時の感染経路の分析の要約など、セキュリティイベントの概略を要約。
- **W/ Luminen**は、ワンクリックで社内やお客様への報告ツールとして活用できるため、EDRの運用工数の削減にお役立ていただけます。

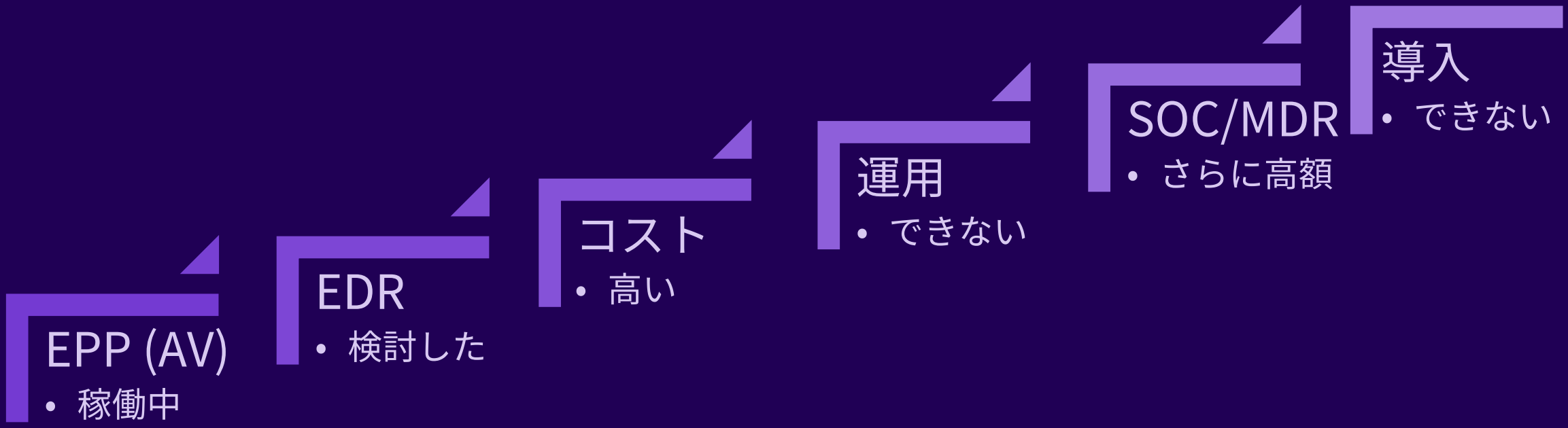
お問い合わせ先

ウィズセキュア株式会社 パートナー営業本部
- 〒105-0004 東京都港区新橋2 丁目2 番9 号 KDX 新橋ビル 2 階
- E-mail : japan@withsecure.com | https://www.withsecure.com/

WS-EDR-2502

CLIENT CONFI

EDRあるある (ハードルが高い？)



- EDRは導入コストもかかるうえ、その後の運用も難しいイメージ
  - EPPだけでは防げない脅威がある （ゼロデイ攻撃・ゼロトラスト等）
- いまの時代の企業としての責任
  - EPP＋EDRは説明責任を果たすためにも最低限必要なものに
- 難しくて高いイメージのEDRをどう訴求・説得・導入したらいいのか…

CLIENT CONFIDENTIAL

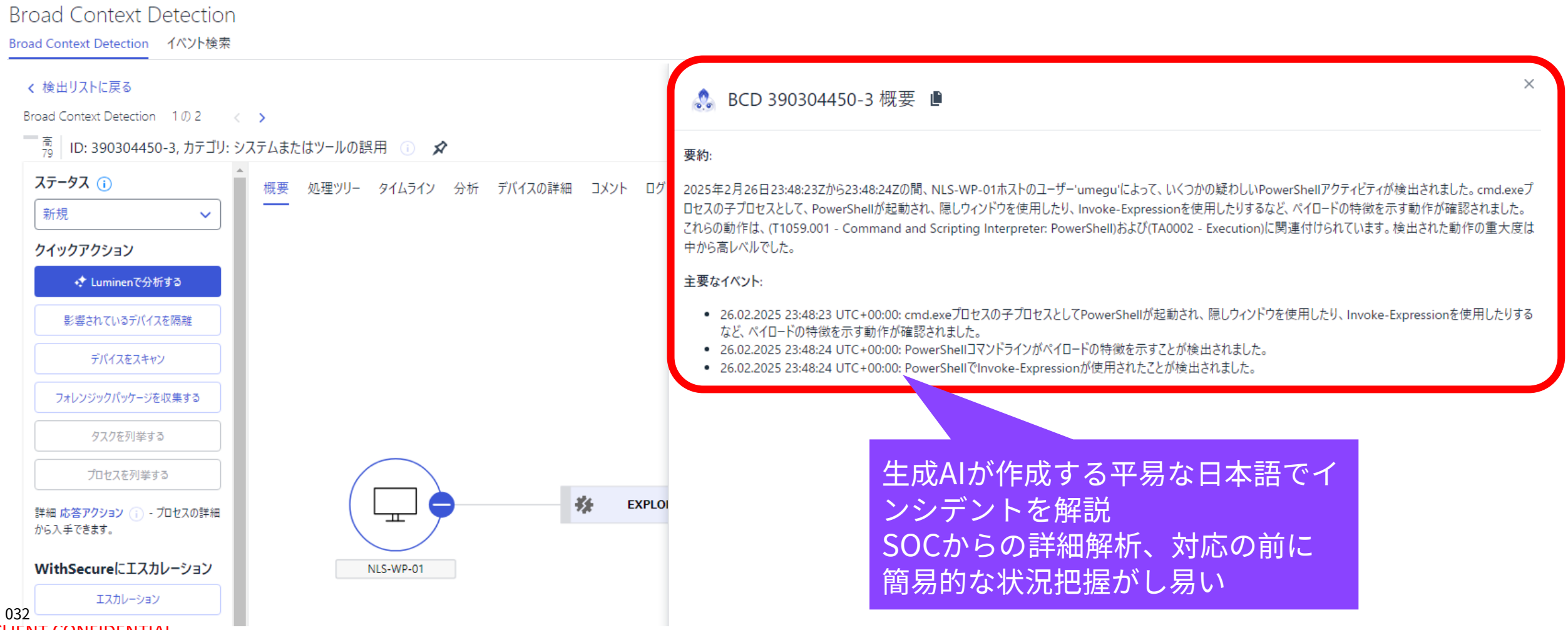
✓ 必須項目：EDRはEPPを含めて比較する

WithSecure EPP+EDR		他社(例:EDR発祥ベンダー)
非常に強い	EPPの防御力	あまり強くない
高くない	EDRの運用負荷	高い
1年	ログ保存期間	30日
あとから解析可	解析	消失前に対処要
ニーズに応じて	監視体制	常時監視必要
よかった!!	その結果？	**後悔？**

CLIENT CONFIDENTIAL

WithSecure Elements EDR:生成AI“Luminen”

生成AI「Luminen」活用によるインシデントの要約が可能



生成AIが作成する平易な日本語でインシデントを解説
SOCからの詳細解析、対応の前に簡易的な状況把握がし易い

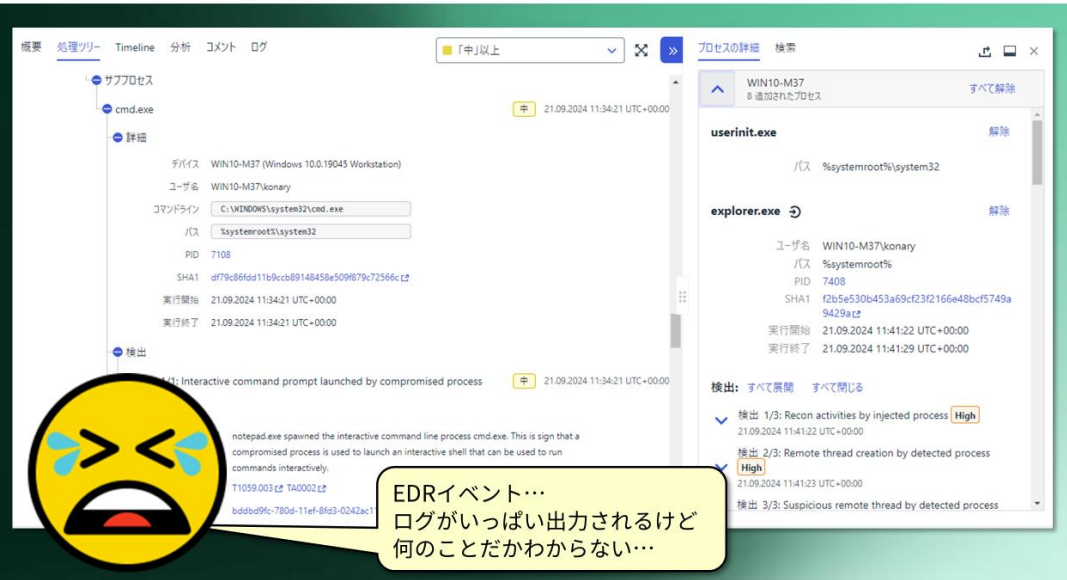
CLIENT CONFIDENTIAL

WithSecureの生成AI:Luminen

- **W/Luminenは、多忙で人員不足のサイバー防御担当者向けに、複雑なサイバーセキュリティタスクを簡単で理解しやすく、効率的に行うための、状況に応じた実行可能なガイダンスを提供します。**
- WithSecureは、AIアルゴリズムを責任を持って使用することで、高品質と厳格なプライバシー基準を維持し、エネルギー消費量と環境への影響を最小限に抑えています
- Luminenのビジョンは、より深い分析でテクノロジーと連携し、アクションを自動化し、より豊富なコンテキストを提供し、データと柔軟に会話することです。

CLIENT CONFIDENTIAL

“Luminen” 新搭載！
生成AIでEDRの運用をラクにしませんか？



EDRイベント…
ログがいっぱい出力されるけど
何のことだかわからない…

こんにちは！Luminenです。
ボタンひとつでEDRイベントを要約して分かりやすく表示しますよ。

すごい!!
これなら何が
起きたかわかる!!

Luminen使用時　「概要」サンプル

BCD 1586476-18985 概要

この概要はAIが作成したものであり、慎重に扱うべきであることに留意されたい。すべての脅威に完全に対処するためには、さらなる調査と専門家による相談が必要な場合があります。

要約:

2024年9月21日11時34分07秒に、WIN10-M37ホストのユーザー konary によって新しいプロセス process_ghosting.exe が実行されました(T1204 - ユーザー実行)。その後、プロセスの即時注入(T1055 - プロセスの注入)や、notepad.exe から cmd.exe への異常なプロセス実行(T1059.003 - コマンドとスクリプト インタープリター: Windows コマンド シェル、T1059.001 - コマンドとスクリプト インタープリター: PowerShell、T1002 - 実行)が検出されました。さらに、ホスト上で複数の情報収集活動(T1016 - システム ネットワーク構成の検出、T1033 - システム所有者/ユーザーの検出、T1049 - システム ネットワーク接続の検出、T1057 - プロセスの検出、T1082 - システム情報の検出)が行われました。

主要な出来事:

- 21.09.2024 11:34:07 UTC+00:00: ユーザー konary が新しいプロセス process_ghosting.exe を実行
- 21.09.2024 11:34:09 UTC+00:00/21.09.2024 11:41:22 UTC+00:00: プロセスの注入、異常なプロセス実行、情報収集活動が検出
- 21.09.2024 11:41:22 UTC+00:00: explorer.exe プロセスが注入された可能性があり、さらに情報収集活動が行われた

CLIENT CONFIDENTIAL

WITH secure