サイバー攻撃からの防御・被害の最小化をシンプルな運用で実現

「エンドポイントセキュリティ プラスEDR」

WITH secure

ランサムウェアを筆頭としたサイバー攻撃の自動化/ビジネス化（RaaS）が進んだ結果、
企業規模や業種に関係なく攻撃の対象となっており、企業のセキュリティ対策は喫緊の課題になっています。

「EPPによる感染前の検知」と「EDRによる被害の拡大防止」を
適切に運用することが重要です。

シグネチャ / NGAV × **EDR**

適切な運用

■ 本サービスのおすすめポイント！

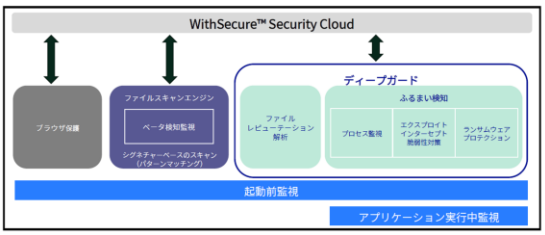
総合セキュリティサービスとして従来型のエンドポイント機能とEDR機能をワンストップで提供します。
また、EDRはセキュリティ専任者のいない企業での運用を前提に「被害が広がる前に危険端末は隔離」し
「インシデントログ全体を生成AIで要約」するなど少数の担当者でハンドリングできるサービスです。

- **法人で求められる機能を1つのサービスで網羅**
- **EPPとEDR 統合ポータルで効率よく管理**
- **インシデント通知から端末の隔離までを自動化**
- **専門家によるアラート解析 MSSサービス**

■ 多層防御によるウイルス対策

世界的なセキュリティソフトウェア評価機関である
AV-TESTが発表する「Best Protection Award」を
最多受賞している **WithSecure Elements** のエンジンを採用。

AIを活用した高性能の振る舞い検知機能を
標準で搭載し、多層防御による**”感染させない”対策**と
EDRによる**”被害を拡大させない”対策**をご提供します。



■ インシデントログの可視化（EDR）

EDRがインシデントを検知した場合、
管理者にアラートを通知し、ポータル上では
インシデントのログをツリー形式で可視化します。

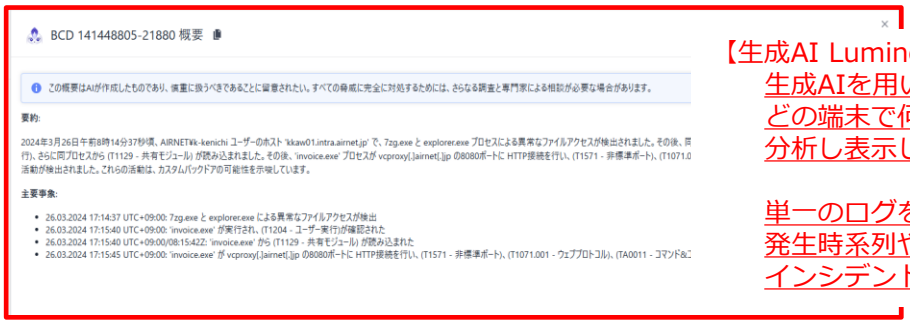
ログからは、発生日時・検出箇所・検出理由などを
確認することが可能です。

■ インシデント発生端末の自動隔離

EDRではインシデントのリスク度合いをポイント付けし、
一定のリスク度（中/高/深刻）を超過した場合は、
発生端末を自動でネットワークから隔離できます。

■ 生成AIによるアラート解析（EDR）

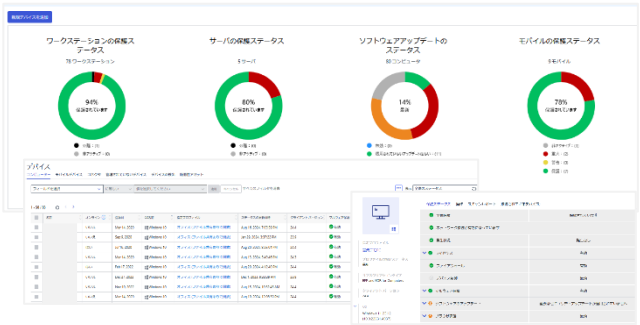
インシデントの解析には専門知識が必要なケースもあり、全てのログの詳細を追うことは困難です。
生成AIによりログの全体像を把握し検出理由を整理することで、アラート検証の負荷が大きく軽減されます。



【生成AI Luminen での解析】
生成AIを用いて該当アラート全体を解析し
どの端末で何が原因で発生したアラートなのかを
分析し表示してくれます。

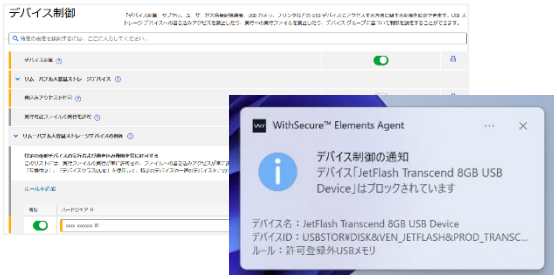
単一のログを確認する従来の機能に比べ
発生時系列やログ同士の関連性が分かりやすく
インシデント調査が効率的行えます。

■ 管理ポータルでの一元管理



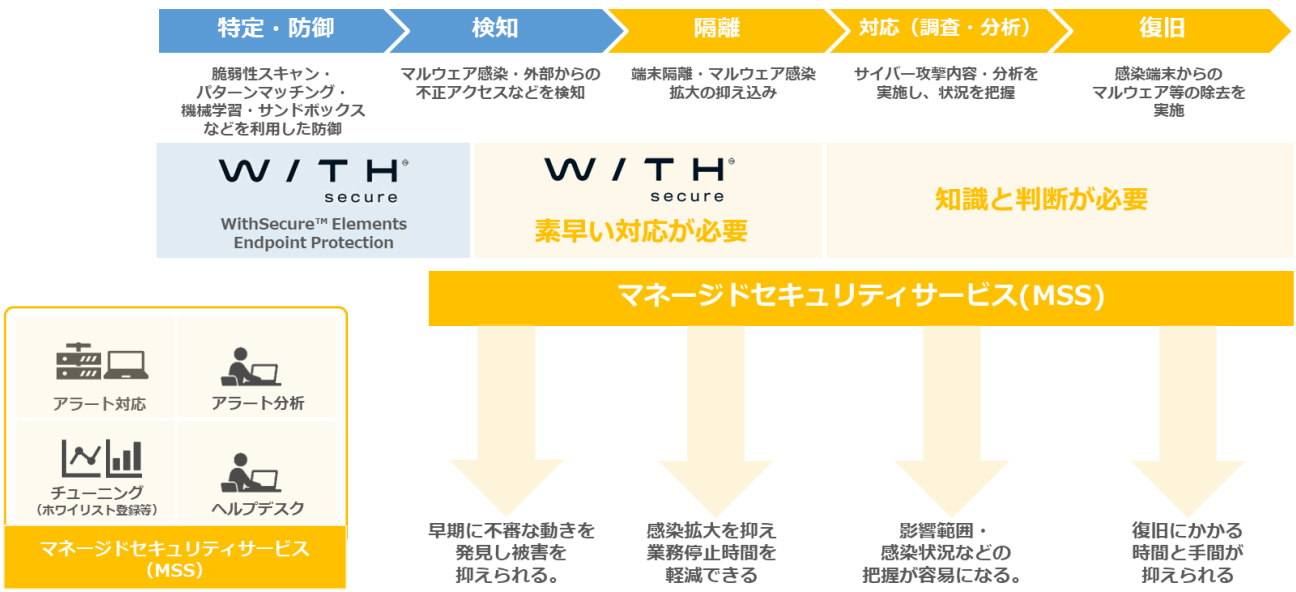
■ USBデバイスの利用制限

USBデバイスを制限し情報漏洩対策も可能です。



■ MSS（セキュアイノベーション社 運用支援サービス）

自社での運用に不安のあるお客様は、運用支援サービス（MSS）をご契約いただくことで
専門チームでのアラート監視及びインシデント対応の支援を受けることができます。



お客様へは<u>インシデント発生時の対応報告</u>と<u>毎月発行の運用レポート</u>をご提出します。

サービスの詳細、ご提供条件等に関しましては、弊社営業担当までお気軽にお問い合わせください。
無料トライアルのご用意もございます。

AIR Internet Service
株式会社エアネット 営業グループ
https://www.airnet.jp/contact/service/
〒140-0001　東京都品川区北品川1-10-4　Y.B.ビル4F
03-6717-5856
sales@air.ad.jp