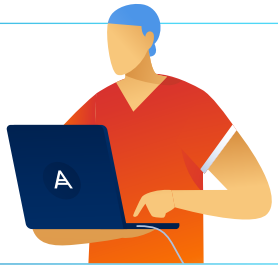
Acronis Advanced Security + EDR

Acronis Cyber Protect Cloud の拡張オプション

エンドポイントセキュリティをシンプルに

セキュリティ侵害の 60% 以上に何らかのハッキングが関連しており[1]、企業は高度なセキュリティソリューションとプロバイダーを検討し、今日の洗練された脅威状況に対処する必要に迫られています。しかし、こうした脅威に対処できる、市場をリードする EDR ソリューションのほとんどは、以下の問題を抱えています。

- **コストが高く、複雑で、低価格での提供が難しい**
- **保護機能が不完全で、ビジネス継続性のためにさらなる統合を必要とする**
- **トレーニングやオンボーディングに関する要件が厳しく、価値を発揮するまでに長期間を要する**
- **拡張性に課題があり、運用にあたって多数のセキュリティ専門家を必要とする**



残念ながら実践を開始したばかりのサービスプロバイダーの場合、自身の MDR サービスを実行するためのスキルと費用は、想定外かもしれません。専門的なセキュリティを確立しているプロバイダーの場合、市場をリードするソリューションで MDR サービスを構築しようとすれば、中流層または SMB の顧客からは相手にされず、ソリューションベンダーの MDR サービスとも競合することになりかねません。

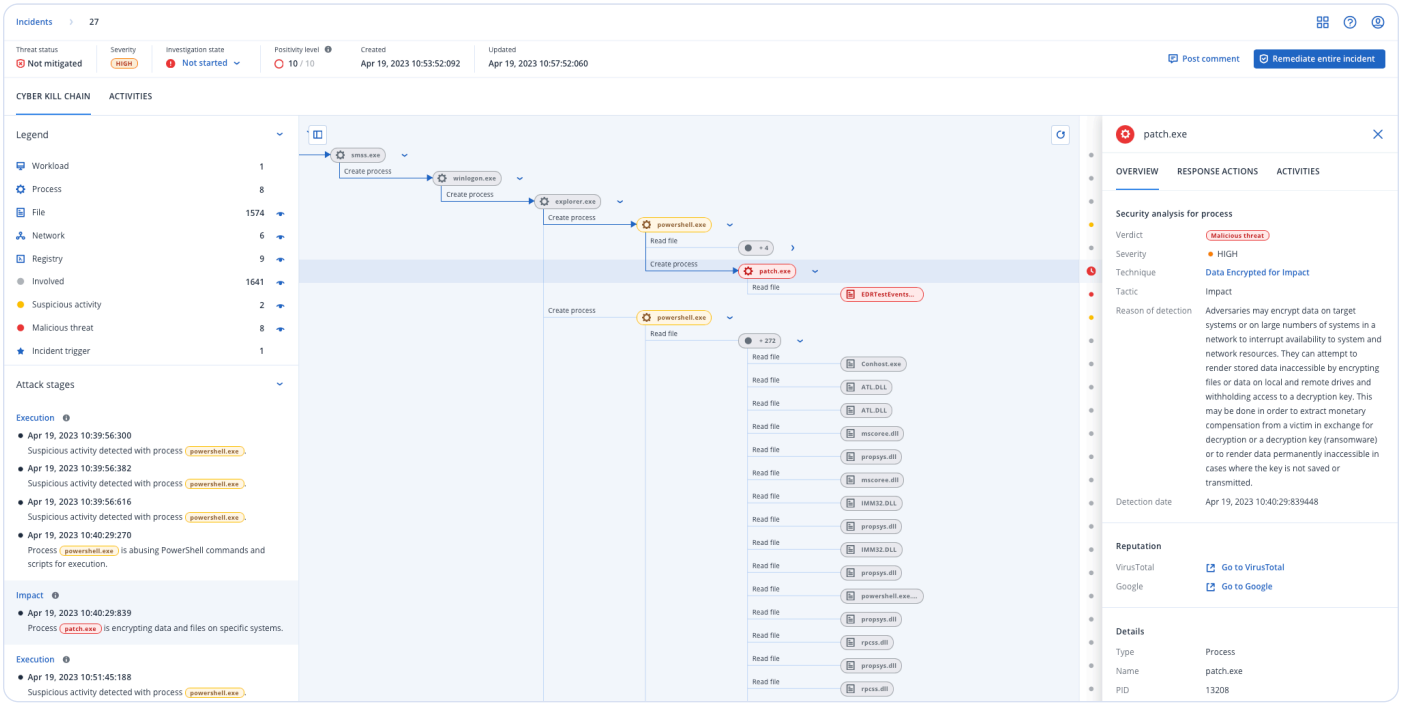
アクロニスの Advanced Security + EDR はサービスプロバイダー向けに開発されています

アクロニスは、サービスプロバイダーが効果的なサービスの提供と、顧客それぞれの異なる要件や予算への対応のバランスを取る必要があることを理解しています。

また、サービスプロバイダーが、マージンと社内スキルの適切な範囲調整が行え、マルチテナントで SaaS ベース、優れたセキュリティ成果を実現し、十分な自動化と使いやすさに重点を置き、さまざまな顧客やそれぞれ独自の環境において迅速に導入・拡大できる高度なセキュリティソリューションを必要としていることを理解しています。

サービスプロバイダー向けに設計された **アクロニスの Advanced Security + EDR** により、エンドポイント保護をシンプルで簡単に行えます。今までにないきビジネス継続性を確保しながら、高度な攻撃を迅速に検出、分析、修復できます。複数セキュリティ製品とソリューションによるコストと複雑もなく、管理と導入がシンプルな、1 つの完全なサイバープロテクションソリューションです。

アクロニスのEDRで検出と応答サービスを効率化



最適化された攻撃の優先順位付けと分析による迅速な対応	統合バックアップ&復元機能で今までにないビジネス継続性を実現	MSP 向けに開発した、単一エージェントによる完全なサイバープロテクションソリューション
• 潜在的なインシデントの優先順位付けと大量のアラートによる複雑さの軽減により調査を効率化。 • 自動相関による数時間ではなく数分の分析を広範囲で実行し、AI ベースのガイド型の攻撃解釈を提供。 • MITRE ATT&CK® における可視性を向上させ、攻撃がどのように侵入したか、どのような被害をもたらしたか、どのように広まる可能性があったかなど、攻撃の分析と影響を迅速に把握。	• セキュリティソリューションによる侵入防止が失敗した場合に、統合バックアップ&復元機能で今までにないビジネス継続性を実現。 • 簡単なクリック操作による効率的な修復と復元。 • NIST サイバーセキュリティフレームワーク全体にわたる完全な統合型保護。特定、保護、検出、対応、復元を単一のソリューションで実現。	• 単一のアクロニス エージェントとコンソールを使用して新しいサービスを迅速かつ簡単に提供開始。導入、管理、拡張も可能。 • 健全な利益率を維持し、OPEX を最小限に抑えながら、複数の顧客に簡単に拡張可能。高スキルのスタッフで構成された大規模なチームによる運用は不要。 • 組織のビジネスについて競合することなく、組織の成功とイネーブルメントにフォーカスするベンダーと協力。

受賞歴のあるエンドポイント保護によりサポート

エディターズチョイス

AV-TEST に参加して受賞

VB100 認定

ICSA Labs エンドポイントマルウェア対策認定

AV-Comparatives 認定

アクロニスで今までにないビジネスレジリエンスを実現

アクロニスは、NIST のような定評ある業界標準と連携し、包括的なエンドポイント保護とビジネス継続性のための単一のプラットフォームを提供することで、脆弱なアセットやデータの特定と積極的な保護、あらゆる脅威の検出とサービス停止、攻撃時の対応と復元を実現します。

NIST フレームワーク全体にわたるビジネス継続性

特定

保護

検出

対応

復元

Advanced Security + EDR

特定	保護	検出	対応	復元
• ハードウェアインベントリ • 保護されていないエンドポイントの検出	• 脆弱性診断 • エクスプロイト防止 • デバイス制御 • セキュリティ構成	• 新興の脅威フィード • 新興の脅威の IoC の検索 • マルウェア対策 & ランサムウェア対策 • AI および ML を基盤にした振舞い検知 • URL フィルタリング	• 迅速なインシデント分析 • ワークロードの隔離と修復 • フォレンジックバックアップ	• 攻撃に対する迅速なロールバック • ワンクリックの一斉復元 • セルフ復元

Acronis Cyber Protect Cloud

特定	保護	検出	対応	復元
• ソフトウェアインベントリ • データ分類	• パッチ管理 • DLP • バックアップ統合 • サイバースクリプティング	• E メールセキュリティ	• リモート接続による調査	• ディザスタリカバリと統合さたバックアップ

主要機能

インシデントの優先順位付け

インシデントアラートという形での、不審なイベントチェーンの優先順位付けにより、エンドポイントイベントの監視と自動関連付けを行います。

MITRE ATT&CK® にマッピングされたインシデントの自動解釈

MITRE ATT&CK® にマッピングされた AI ベースの攻撃解釈を活用して対応を効率化し、脅威への応答性を改善して以下について数分で理解できます。

- 攻撃者はどのように侵入したか
- 攻撃者が侵入経路をどのように隠したか
- 攻撃がどのような被害をどのようにもたらしたか
- 攻撃はどのように広まったか

攻撃にあった場合でも、簡単なクリック操作で、今までにないビジネス継続性を提供

セキュリティソリューションによる侵入防止が失敗した場合に効果を発揮します。サイバーセキュリティ、データ保護、エンドポイントセキュリティ構成管理における統合を最大限に活用し、簡単なクリック操作でインシデントに対応できます。

- **修復**：エンドポイントを分離し、脅威を隔離
- **さらに調査**：リモート接続やフォレンジックバックアップを使用
- **将来の攻撃を防止**：脆弱性を修復
- **ビジネス継続性を確保**：攻撃に対するロールバックならびに統合バックアップ & 復元機能

1.出典:“2022 Data Breach Investigation Report”, Verizon

Acronis

詳細は www.acronis.com をご覧ください。