SentinelOne EDR のご紹介

ランサムウェア復旧機能も備えた自律型AI セキュリティプラットフォーム

SentinelOne Japan株式会社
2023年8月8日　DTCウェビナー

SentinelOne 企業概要

2,500+
従業員数

10,000+
顧客数

2021年6月IPO
潤沢な投資資金

グローバルサポート
24時間365日

VIGILANCE MDR
24時間365日

本社所在地
カリフォルニア州 マウンテンビュー

グローバル技術拠点
イスラエル、カリフォルニア、ボストン、フランス、チェコ

グローバルデータセンター
北米、ヨーロッパ、アジア
AWS GovCloud　高可用性

プロスポーツへのスポンサーシップ
アストンマーティン　**Cognizant Formula One™ Team**
USPGAツアーゴルファー　ルイス ウースト ハウゼン
ATPツアー　ブランドン ナカシマ

SentinelOne™

日本における主なブランディング活動

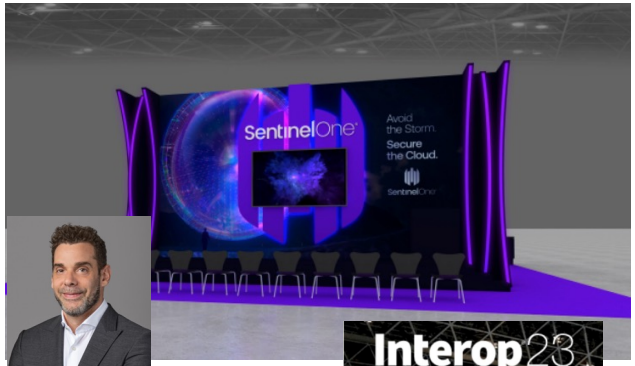
TOKYO MX 企業魂に出演

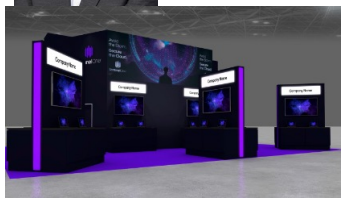
6/9(土)、6/10(日)　19:00台-20:00台
@TOKYO MX、エムキャスにて放映
＊日本法人代表 青山やパートナー企業、エンドユーザー様が出演

SentinelOne

Interop 23 Tokyo

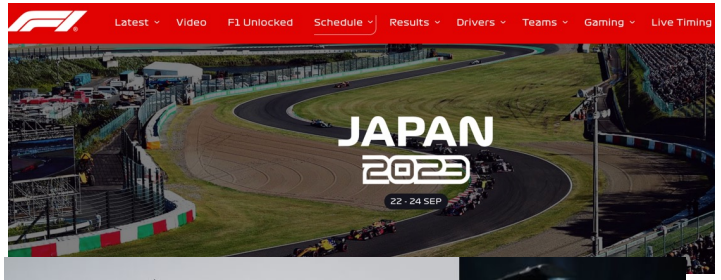
6/14-6/16@幕張メッセ
＊CEO Tomer Weingartenによる基調講演（初日）
＊展示ブース（12小間、含むプレゼンテーションステージ、パートナーブース）

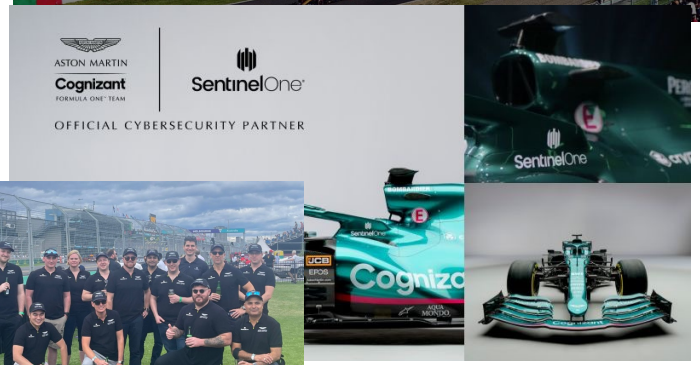




Formula 1 Japan 2023

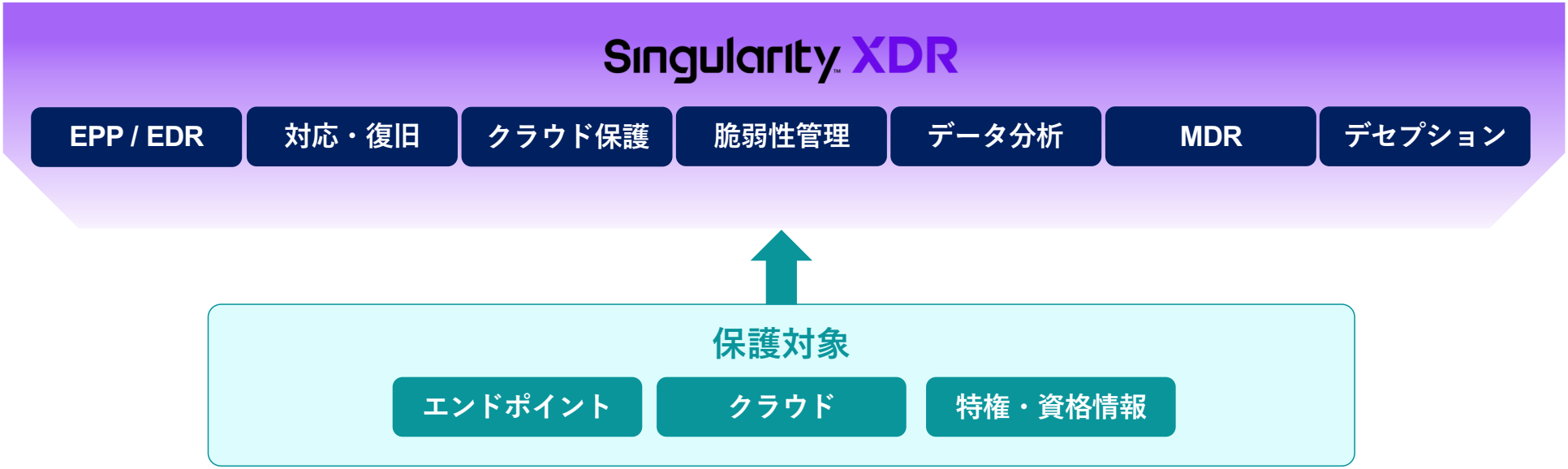
9/22-24/@鈴鹿サーキット
＊アストンマーティン　Cognizant
Formula One™ チームスポンサー企業として、お客様、パートナー様をご招待してのレース観戦ツアーを計画





SentinelOne EDR

EDRを超えた幅広い機能を提供



AI 検出　：脅威に対する高い検出率・柔軟な対応

可視化　：STORYLINE™ による脅威行動の流れを可視化

自動化　：検出・駆除に加えデータの復元が可能なロールバック機能

SentinelOne EDR

技術が人を支援

旧来の方式

McAfee　Symantec

シグネチャーベース

- 人力依存
- 対応規模やスケールに問題
- まれに高度な攻撃は検知する

人に依存した技術

Microsoft　Carbon Black.　CROWDSTRIKE

クラウドベースのモニタリング

- 人力依存（製品の技術的な補助は有り）
- 脅威の分離や修正が手動
- ビジネス停止時間の長期化
- 復元作業が困難

アンチウイルスの進化版

deepinstinct

深層学習（ディープラーニング）ベース

- 防御にフォーカス
- すり抜けた際の対策機能が無い
- 破壊されたデータの復元ができない

技術が人を支援

SentinelOne

自律型AI + Cloud

- 高い検知率
- テクノロジーによる負荷の削減
- 専門家の作業を自動化
- 各エンドポイントで稼働する自律型 AI
- 自動化による対応 ~ 復旧時間の短縮化
- ITDR による侵入後の検知と対応
- XDR 連携による対応力の拡張
- 深層学習が対応するスクリプトやファイルへも対応 + 書き込み時にも検知可能
- 感染時の不正なデータや破壊データは簡単に復旧可能

SentinelOne EDR

Gartner・MITRE での高い評価

Gartner

2022年度 マジック・クアドラント

エンドポイントプロテクションプラットフォーム部門: リーダー

同、クリティカル・ケイパビリティ: 高スコア

https://jp.sentinelone.com/lp/gartnermq/

Gartner peerinsights™

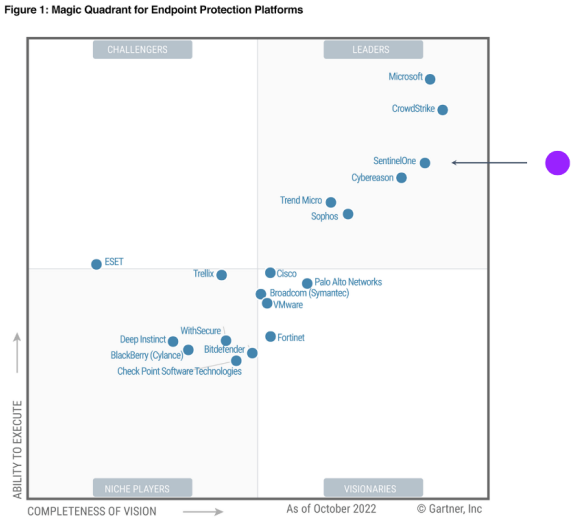
EDRソリューションマーケット部門でユーザーによる高評価を獲得

https://www.gartner.com/reviews/market/endpointdetection-and-response-solutions

MITRE ENGENUITY™

2020年ラウンド3、2021年ラウンド4で2年連続トップの検知能力

https://attackevals.mitre-engenuity.org/enterprise/participants/?adversaries=wizard-spider-sandworm%2Ccarbanak-fin7



SentinelOne の優位性

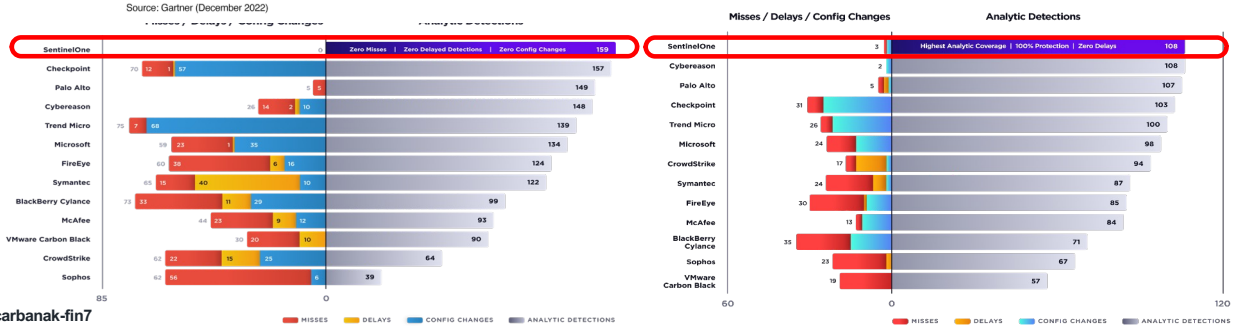
- 顧客価値の高さ
- IDセキュリティの網羅
- MITRE ATT&CKの継続的好結果
- 幅広いOSの対応
- 高度なMDRサービス提供
- グローバルでのプレゼンス

Gartner Critical Capabilities:

TYPE A USE CASE	TYPE B USE CASE	TYPE C USE CASE
技術に前のめりな組織	総合的に判断する組織	予防重視の組織
Highest Score	Highest Score	Highest Score

全てのUse Caseにおいてトップスコア！

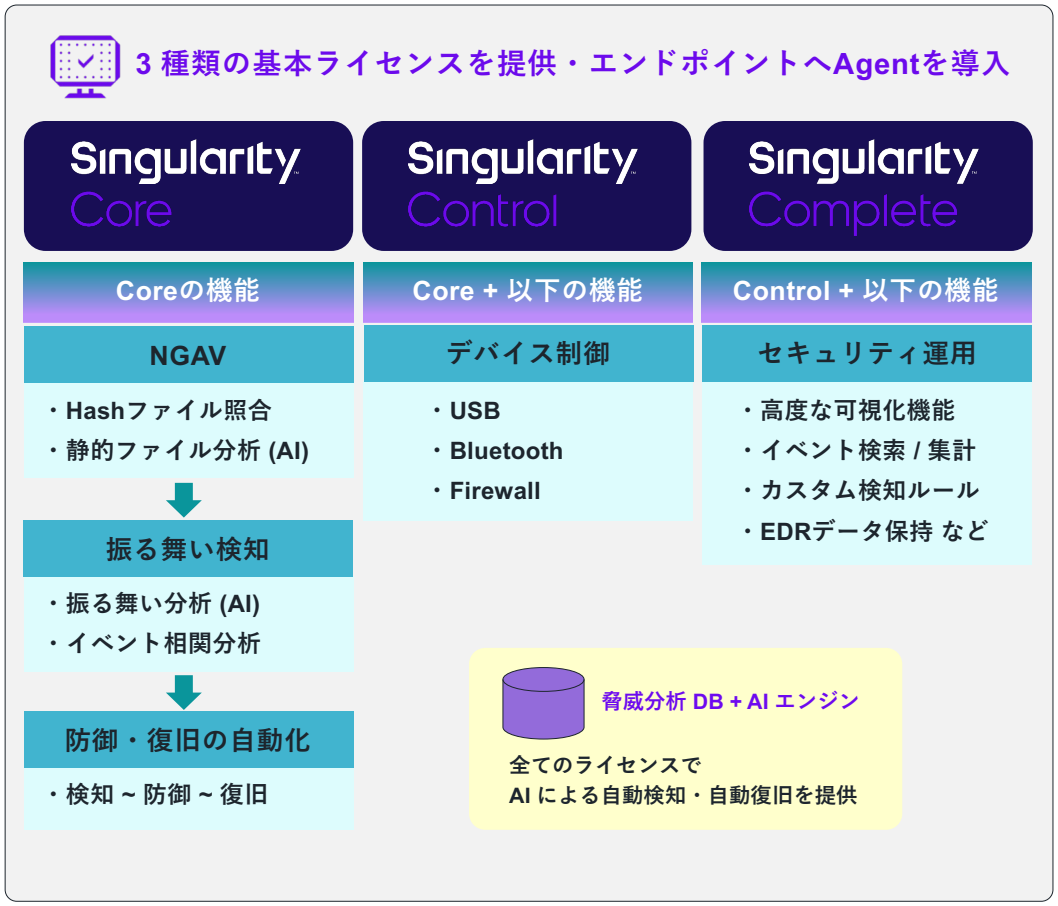
SentinelOneはGartnerの2022年エンドポイント保護プラットフォーム向けのCritical Capabilityレポートにおいてタイプ A, B, CのUse Caseでトップスコアを獲得しました。SentinelOneはそれぞれのタイムのお客様に適合したオプションを兼ね備えています。

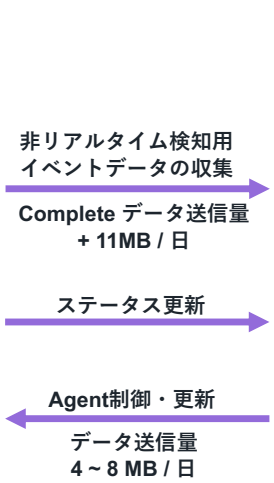


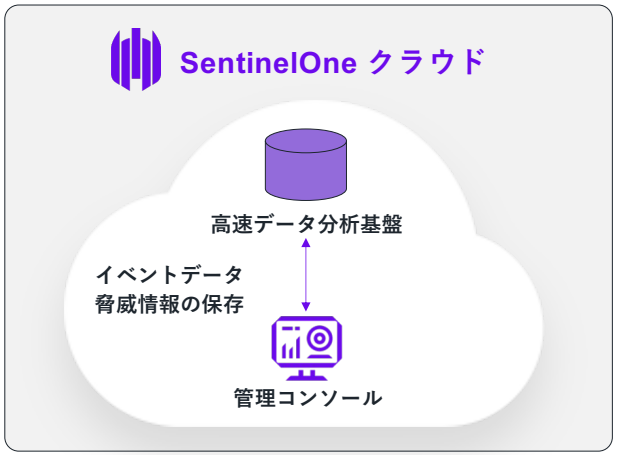
- ゼロ誤検出
- ゼロ設定変更
- ゼロ検出遅延

SentinelOne EDR

自律型 AI + クラウド型の EDR







MDR サービス

VIGILANCE Respond	VIGILANCE Respond PRO
お客様SOCの代行	Respondの内容に加えて
・お客様SOCの代行 ・Q&A ・過検知・誤検知の調査 ・除外・復旧作業 ・脅威インテリジェンス配信	・攻撃の兆候調査 ・攻撃の影響範囲調査 ・ディープフォレンジック ・マルウェア解析 ・環境保全　など

SentinelOne EDR

ライセンス・アドオン・サービス

基本ライセンス

コンポーネント名称	機能
Singularity Complete	EPP / EDR / XDR
Singularity Control	EPP + デバイス制御機能
Singularity Core	EPP

アドオン機能

コンポーネント名称	機能
Singularity Cloud Workload	サーバー・コンテナセキュリティ
Singularity Ranger	アセット管理 + エージェント展開
Singularity Identity ※	ITDR + デセプション
Singularity RangerAD/Protect	AD アセスメント, 保護
Singularity Mobile	モバイル脅威対策
Singularity RemoteOPS	リモートスクリプト起動
Singularity CloudFunnel	XDR データ保管（AWS S3）
Singularity BinaryVault	バイナリファイルデータ保管
Singularity Ranger Insight	脆弱性管理

セキュリティサービス

サービス名称	内容
VIGILANCE Respond	MDR
VIGILANCE Respond PRO	DFIR
WATCHTOWER	脅威ハンティング
WATCHTOWER PRO	侵害アセスメント（年2回）

マーケットプレイス

サービス名称	内容
Singularity MarketPlace	NDR,SASE,SIEM 等の連携、XDR化

SentinelOne EDR

基本ライセンスの機能

● 標準搭載　○ オプション

搭載機能	Complete	Control	Core
グローバルSaaSプラットフォーム	●	●	●
基本的なエンドポイント保護機能			
自律型SentinelエージェントStorylineTMエンジン	●	●	●
静的AIとSentinelOne Cloud Intelligenceによるファイルベース攻撃の阻止	●	●	●
振る舞いAIによるファイルレス攻撃の検知	●	●	●
自律型脅威対応/強制終了、隔離 (Win、Mac、Linux)	●	●	●
自律型修復対応/ワンクリック、スクリプト記述不要 (Win、Mac)	●	●	●
自律型ロールバック対応/ワンクリック、スクリプト記述不要 (Win)	●	●	●
ネットワークからのデバイスの隔離	●	●	●
インシデント分析 (MITRE ATT&CK®、タイムライン、エクスプローラ、チームの注釈)	●	●	●
エージェント改ざん対策	●	●	●
アプリケーションインベントリ	●	●	●
IT OPS/セキュリティハイジーン&スイート機能			
ロケーション認識付きOSファイアウォール制御 (Win、Mac、Linux)※	●	●	
USBデバイス制御（Win、Mac）	●	●	
Bluetooth®/Bluetooth Low Energy®の制御 (Win、Mac)	●	●	
アプリケーションの脆弱性 (Win、Mac、Linux)	●	●	
不正なデバイスの検知	●	●	●
セキュリティ運用のEDR機能			
Deep VisibilityとActiveEDR®、Storyline™コンテキスト	●		
MITRE Engenuity ATT&CK®の統合	●		
Storyline Active Response (STAR™) のカスタム検知ルール	●		
Storyline Active Response (STAR™) Proのカスタム検知ルール	○		
Binary Vaultライブマルウェア アップロードリポジトリ	○		
14日間EDRハンティングデータ保持	●		
拡張EDRハンティングデータ保持 (最大3年)	○		
Cloud Funnel™ データレイクストリーミング	○		
安全なリモートシェル	●	●	

アドオン機能

搭載機能	Complete	Control	Core
Singularity RANGER			
ライブグローバル資産インベントリ	○	○	○
高度なMLデバイス フィンガープリンティング	○	○	○
疑わしいデバイスや悪質なデバイスの分離	○	○	
Storyline Active Response (STAR™) による、疑わしいデバイスの振る舞いの監視と対応	○		
疑わしいデバイスの振る舞いの監視と対応	○		
デバイスベースの脅威ハンティング	○		
Singularity Cloud			
KubernetesとVM用Cloud Workload Security	○	○	
クラウドプロバイダのメタデータ統合	○	○	
Kubernetes用自動アプリケーション制御	○	○	
Linux VM用自動アプリケーション制御	○	○	

※ 管理コンソール内で指定するロケーション名を意味しており、GeoIPロケーションを識別する機能ではありません。

SentinelOne EDR のアドバンテージ

① シンプルな構成	EPP・EDR・ITDR の機能を単一のエージェントで提供
② 復元性能の高さ	検知・対応・復旧までの全てをスピーディーに自動実行できる脅威の性能
③ オフラインでの稼働	エージェントはオフライン状態でも導入・稼働させることが可能
④ マルチテナント	標準でマルチテナント機能を搭載し、セキュリティ担当者の運用負荷を軽減可能
⑤ 裏付けされた高い製品力	Gartner・MITRE ATT&CK などの評価結果に裏付けされた高い製品力
⑥ カバー範囲の広さ	各種OS・クラウド・AD保護・おとり技術※による検知 / 対応など広範囲にカバー

SentinelOne EDR の機能

SentinelOne EDRの機能

NISTサイバーセキュリティフレームワーク

NISTサイバーセキュリティフレームワークとは

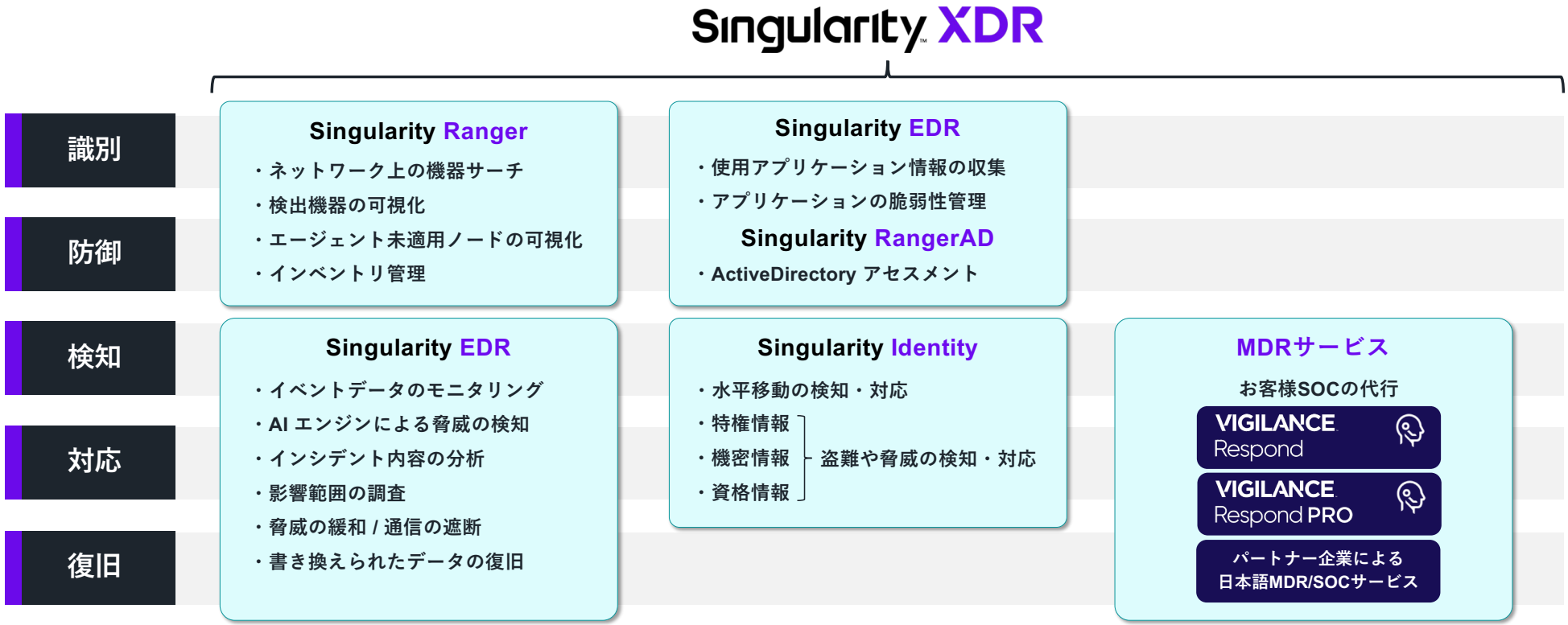
- ✓ 2014年2月に米国オバマ政権における大統領令に基づき重要インフラのサイバーセキュリティ強化を目的として制定。
- ✓ 日本においても経済産業省の「サイバーセキュリティ経営ガイドライン」や内閣官房の「重要インフラ行動計画」において同フレームワークが参照されています。
- ✓ 識別・防御・検知・対応・復旧 の5つのステップに分けて提示され、Coreと呼ばれる対策一覧が記載されています。

識別	資産管理・ビジネス環境・ガバナンス・リスクアセスメント・リスクマネジメント戦略・サプライチェーンリスクマネジメントの6つのカテゴリーで構成され、リソース管理やリスクマネジメントの方法などをまとめている。
防御	アイデンティティ管理とアクセス制御・意識向上およびトレーニング・データセキュリティ・情報を保護するためのプロセスおよび手順・保守・保護技術の6つのカテゴリーで構成され、サイバー攻撃へのシステム対策や組織的な対策や保守などをまとめている。
検知	異常とイベント・セキュリティの継続的なモニタリング・検知プロセスの3つのカテゴリーで構成されている。
対応	対応計画の作成・コミュニケーション・分析・低減・改善の5つのカテゴリーで構成され、サイバー攻撃による被害を前提に組織的な対応策についてまとめている。
復旧	復旧計画の作成・改善・コミュニケーションの3つのカテゴリーで構成され、セキュリティインシデント発生時の具体的な復旧方法や関係者への伝達といった面についてもまとめている。

SentinelOne EDRの機能

NISTサイバーセキュリティフレームワークとSentinelOne EDR

従来のEDR製品とは異なり、SentinelOne EDR はNISTサイバーセキュリティフレームワークの5つのコアへのアプローチが可能



SentinelOne EDR の機能

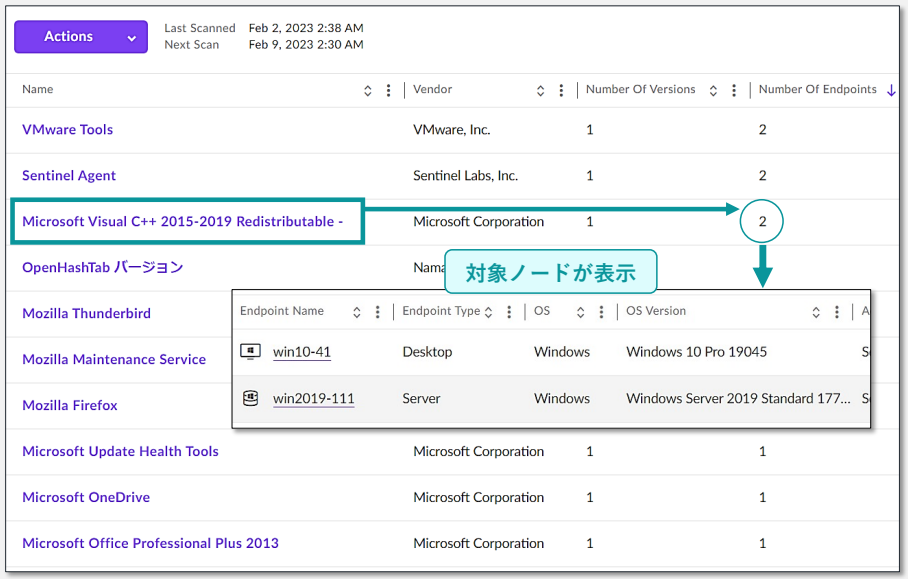
- 識別
- 防御
- 検知
- 対応
- 復旧

SentinelOne EDRの機能

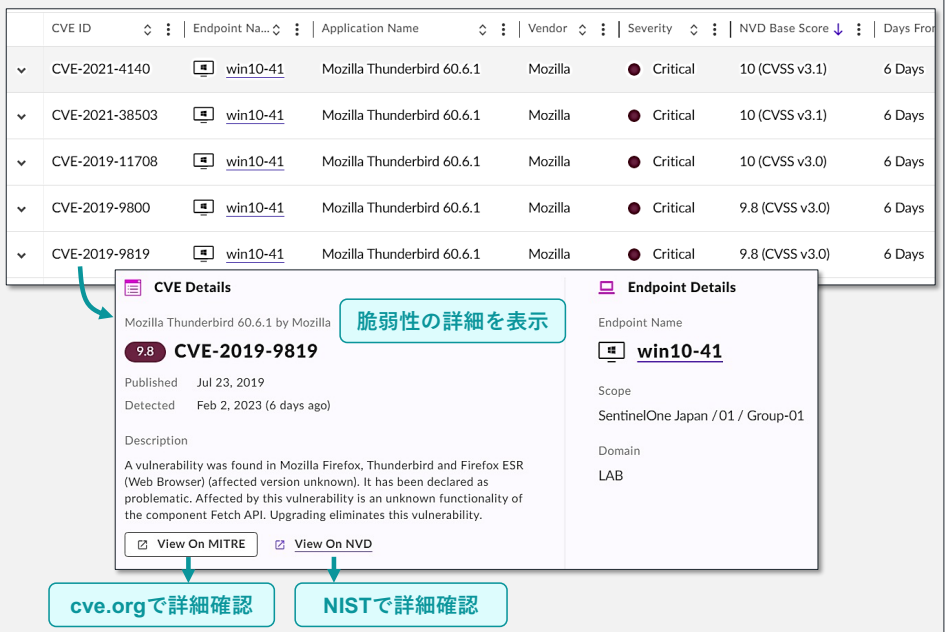
識別・防御

使用アプリケーション情報の管理・脆弱性の管理 : Singularity Complete・Control

検出したアプリケーションの一覧



検出したアプリケーションの脆弱性の一覧



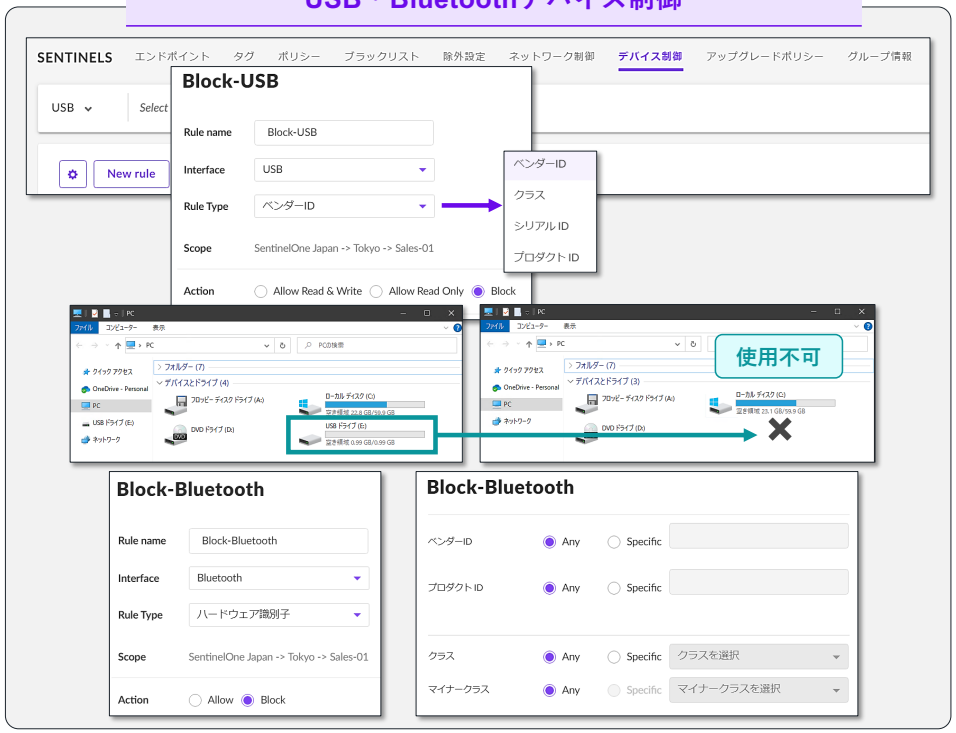
・エンドポイントに導入されているアプリケーション情報を定期的に収集・リスト化することができます。
・脆弱性が検出された場合はCVE IDと共に対象アプリケーション・対象エンドポイントが表示されます。

SentinelOne EDRの機能

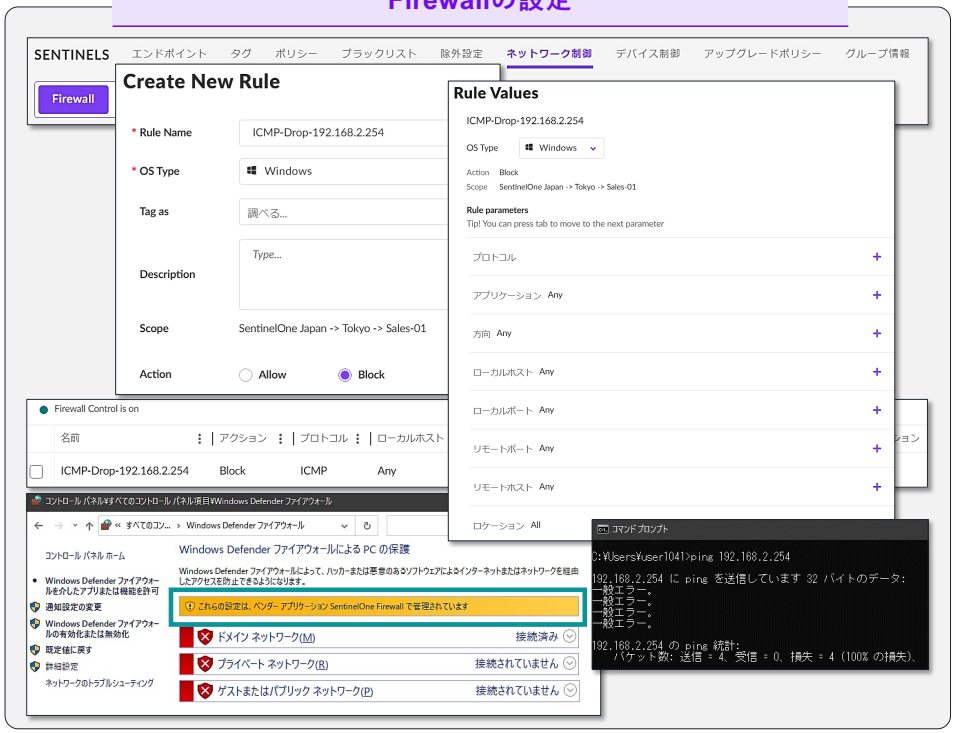
識別・防御

デバイスを制御し脅威の侵入を防止: Singularity Complete・Control

USB・Bluetoothデバイス制御



Firewallの設定



FirewallはOS側で使用しているFirewallを使用することもできます

SentinelOne EDRの機能

識別・防御

ネットワーク上の機器の識別とインベントリ管理 : Singularity Ranger（アドオン）

検出した機器の一覧

・エンドポイントに導入したエージェントより、指定した間隔・ポート・サブネットに対して定期的にスキャンが実行されます。
・エージェント未適用デバイスの検出や、解放されているポート情報を確認することができます。
・本機能を有効化するエンドポイントは個別に指定することができます。

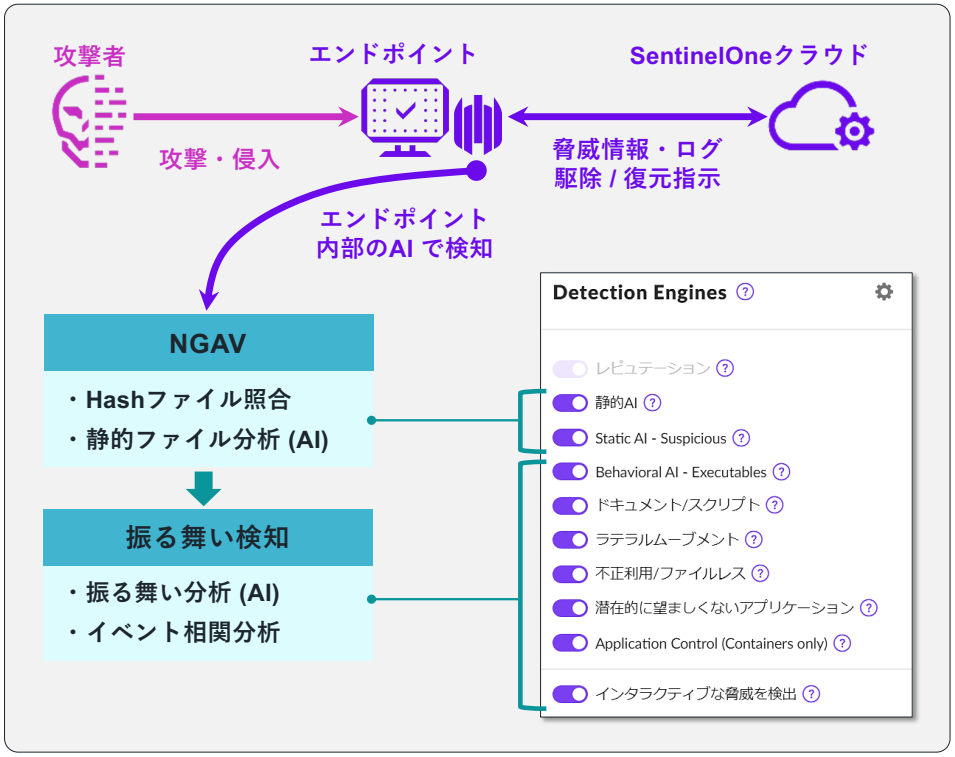
SentinelOne EDR の機能

- 識別
- 防御
- 検知
- 対応
- 復旧

SentinelOne EDRの機能

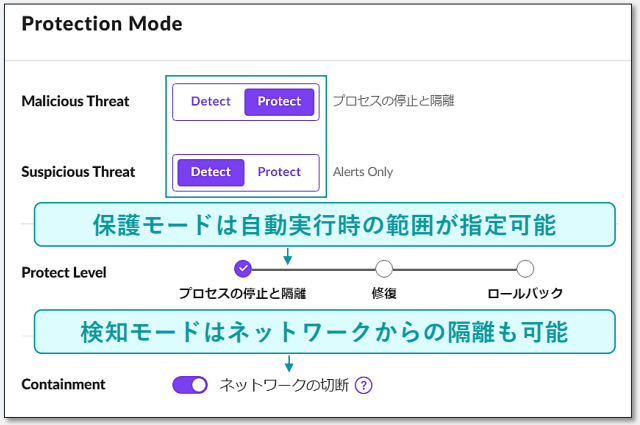
検知

AI による自律した脅威の検知 : Singularity Complete・Control・Core



保護モードに2つのモードを提供
~ アンチウイルス的な運用も可能 ~

保護 (Protect) モード	修復 (駆除)・復元までが自動実行される
検知 (Detect) モード	アラート送信 + 管理者による操作で復旧



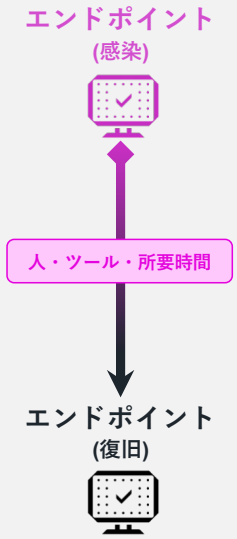
エンドポイントのAI が自律して検知・処理を行うため高速 + クラウドとの通信がオフラインでも稼働します。

SentinelOne EDRの機能

対応・復旧

データの復旧方式： Singularity Complete・Control・Core

従来・他社の復旧方法



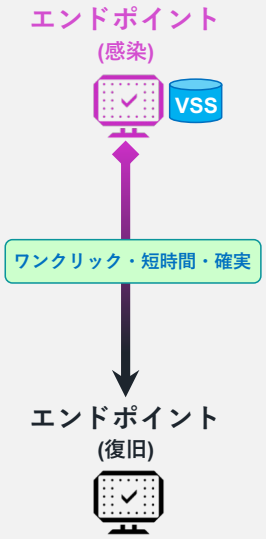
■復旧方法

・管理者がバックアップツールでリストア
・社員がバックアップツールでリストア
・社員がクラウド (OneDrive等) より復元
・イメージバックアップよりOSごとリストア
・初期化 + OS / アプリケーションの再インストール + データは別途バックアップからリストア

■問題点

・感染前のデータを特定するのに時間を要する
・社員任せのリストアは再感染のリスク
・リストアできるのはドキュメント類 (レジストリや不正なサービス・自動タスクは？)
・イメージリストアや初期化による復元は、感染端末数に比例して膨大な時間を要する

SentinelOneでの復旧方法



■復旧の仕組み

・VSSを定期的に取得 (取得間隔は指定可能)
・VSSはエージェントが保護しており、VSSへ攻撃が発生した際は検知され攻撃は遮断されます
・VSSの取得時刻と「感染+データの破壊時刻」は紐づいているため、破壊前のデータを確実に特定し復旧させることができます

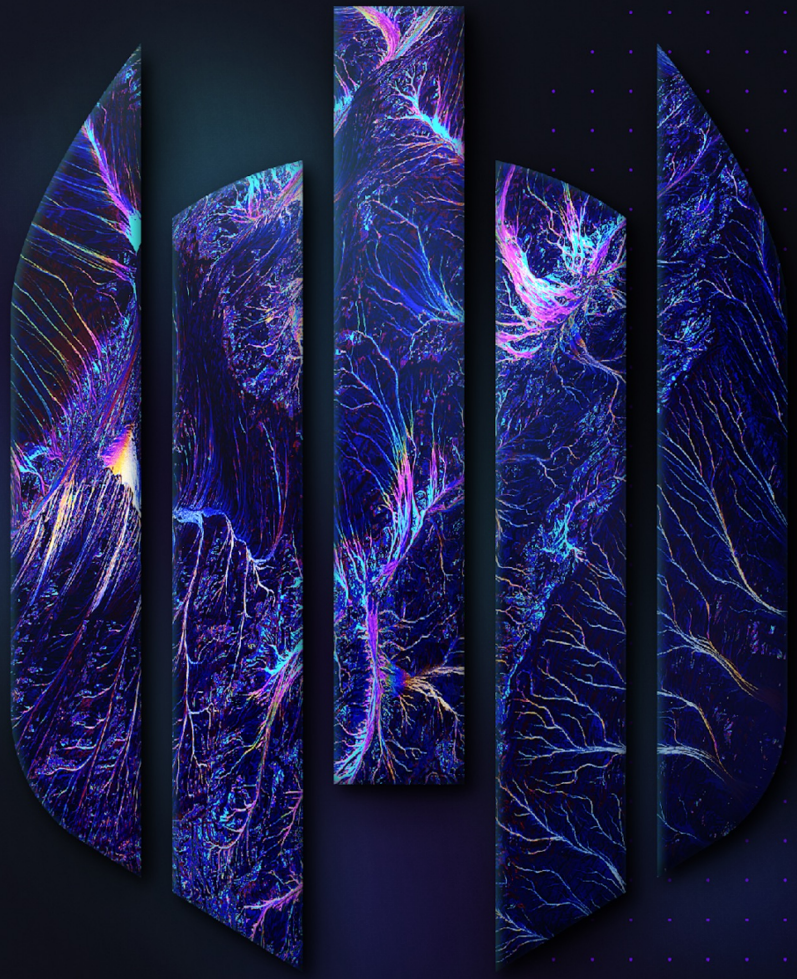
※ VSS RollBack機能はWindowsのみ対応しています。

■メリット

・管理者による操作のみで復旧することが可能
・復元対象ファイルの特定作業が不要
・社員の操作が不要
・ファイル単位で復元できるだけでなく、不正に登録されたレジストリやサービス・自動タスク類も元の状態へ復元可能

※ 保護モードの場合は脅威検知の時点で駆除されるため復旧操作は不要です。上記は検知モードの場合です。
※ 停止したプロセスや復元したデータはCSV形式でダウンロードすることができます。

他社EDR製品に対する
アドバンテージ



他社比較

各社の主要機能比較

No	機能	SentinelOne	CrowdStrike	Cybereason	DeepInstict	Microsoft E5 ATP	TrendMicro
1	自律的な保護と対応	○	△ 限定的	✖ Legacy AV(OEM) + クラウド依存	○	○	✖ Legacyシグネチャ + クラウド
2	高速修復	○ 自動	✖ 手動	✖ 手動	✖ 限定的	✖ 限定的	✖ 限定的 要MDR/XDR
3	少ないアラートと定義の多さ	自動・相関	監視に大きく依存	機械学習 (アラート多)	アラート多	インシデントベース	アラート多
4	統合されたAgent	○	○	○	○	○	✖ コンポーネント別
5	API対応	REST API	限定的	○	✖	○	?
6	静的 AI	○	○	✖ (OEM AV + 限定的なAI)	○	○	○
7	ふるまい AI	○	○	✖ 限定的 (ふるまいルール)	○	○	✖ 限定的
8	Exploits・疑わしいスクリプト	○ (AI+Full Context)	○	✖ 限定的 (ふるまいルール)	✖ 限定的	○	✖ 限定的 (クラウド依存)
9	水平移動	○ (AI+Full Context)	○	✖ 限定的 (ふるまいルール)	✖ 限定的	○	✖ 限定的 (クラウド依存)
10	対応 (Remediation)	○ 自動	✖ 手動・限定的	✖ 手動・限定的	✖ 限定的	○	✖ 手動 (要MDR/XDR)
11	復旧 (Roll Back)	○ 自動	✖	✖	✖	✖	✖
12	脅威ハンティング	自動・相関分析	○	自動	✖	○	✖ 手動 (要MDR/XDR)
13	リモートシェル	○	○ 限定的なコマンド	○	✖	○	○ 限定的なコマンド
14	統合脅威情報	○	○	○	✖ 限定的	○	○
15	デバイス制御	○	✖ USBのみ	✖ Windows + USBのみ	✖	✖ 限定的	○
16	Firewall 制御	○	○	○	✖	✖ 限定的	○
17	Bluetooth 制御	○	✖	✖	✖	✖ 限定的	○
18	マルチテナント対応	○	✖	○	○	✖	○
19	ユーザーインターフェイス	直観的・シンプル	複雑・直観的ではない	複雑・直観的ではない	複雑・直観的ではない	複雑・直観的ではない	複雑・直観的ではない
20	ロールベースアクセス制御	○	○	○	○	○	○
21	Agent 自立保護 / アンチタンパー	○	○	○	○	○	✖

他社比較

SentinelOneの優位点 - 1

■CrowdStrikeにはオンデマンドスキャン機能が搭載されていません

CrowdStrikeには

ファイルやフォルダのオンデマンドスキャン、ディスク全体のスキャン、USBデバイスのスキャン機能が搭載されていません。

■SentinelOne

SentinelOneでは

ファイル・フォルダ・ディスク全体・USBデバイスのスキャン機能が搭載されており、社員の操作で簡単に脅威のスキャンを行うことができます。

他社比較

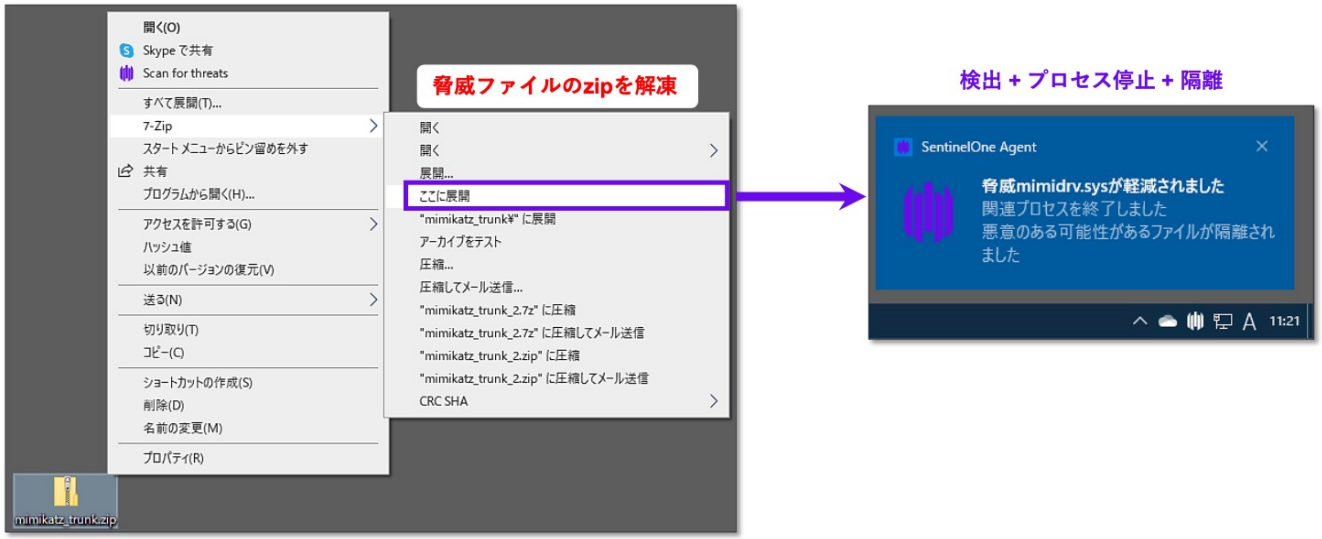
SentinelOneの優位点 - 2

■CrowdStrikeはファイルを実行しないと脅威を検出することができません

CrowdStrikeには

ファイルの書き込み時 (保存時)の脅威検出やプロテクト機能が搭載されていません。脅威の検出のためにはファイルを実行する必要があります。

■SentinelOne



SentinelOneでは

ファイルの書き込み時 (保存時) にも脅威を検出し、プロセスの終了 + 隔離が自動で行われるため、ファイルの実行前に脅威を排除することができます。

他社比較

SentinelOneの優位点 - 3

この事例ではSentinelOneを検出モードで稼働させています。
保護モードでは「ランサムウェアファイルの保存時に」検出+駆除が可能です。

■CrowdStrikeは感染後のロールバック機能がありません

CrowdStrikeには

ファイルのロールバック機能が無いため、マルウェア駆除後は手動での復旧操作またはエンドポイントの初期化が必要になります。

■SentinelOne

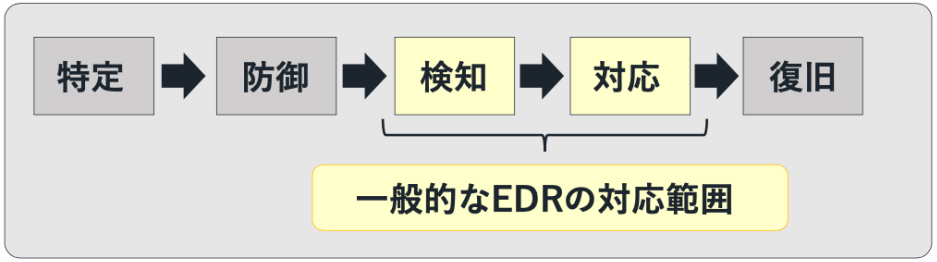
SentinelOneでは

駆除・隔離だけでなく、ロールバック機能により暗号化されたファイルや変更されたレジストリデータも簡単にロールバックすることができます。

他社比較

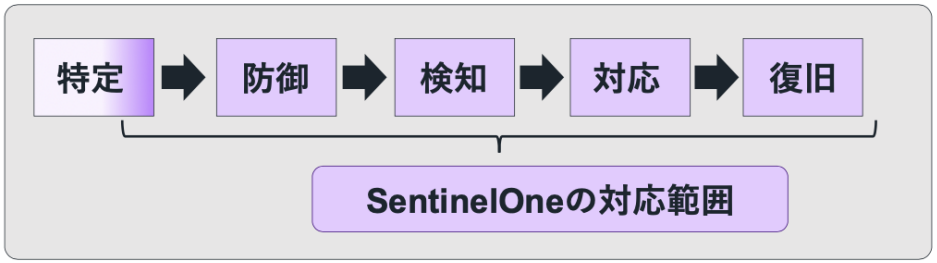
NIST セキュリティフレームワーク

■一般的なEDR製品とSentinelOne製品の違い



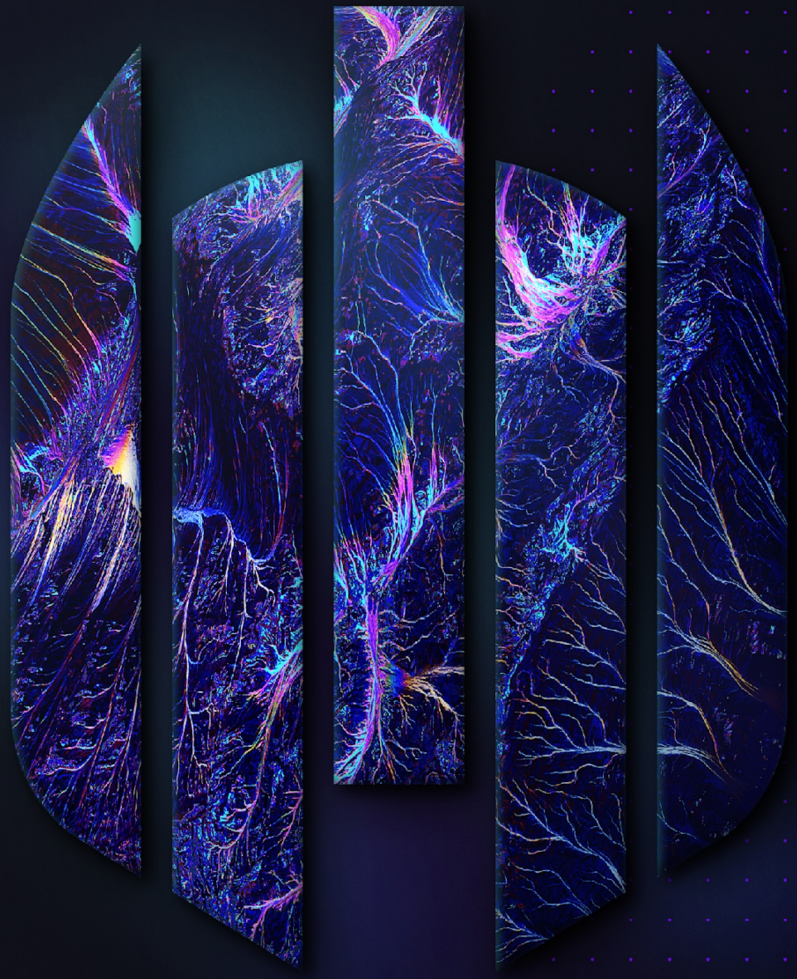
・アンチウイルス + バックアップ製品での補完が必要
・脅威に対する対応は人による判断やSOCへの依存が大きい

SentinelOne



・優れたAIエンジンによる防御/検知機能 (EPP)
・脅威ファイルの侵入時 (書き込み時) への対応
・不正ツールの停止 + 隔離
・ロールバック機能によるエンドポイント環境の復元
・使用アプリケーションの脆弱性管理

お客様事例



お客様事例 1）

人事・バックオフィス業務代行A社

人事・バックオフィス系業務の代行業務を展開する成長スタートアップ。テレワークを中心としているため、在宅勤務でも安全を確保するためのセキュリティ対策としてSentinelOneを導入。

自動ロールバック機能を活用することで、在宅勤務時に感染が発覚しても即時復旧して業務を継続できることに着目。

導入当初は50名規模の会社だったこともあり、自動運用機能が圧倒的に進んでいるSentinelOneを選択。

Company Overview

従業員：約180名
事業　：人事・バックオフィス業務の代行
本社　：北海道

導入理由

- **テレワークにおけるセキュリティ強化**
- **在宅でも自動復旧で業務継続可能**

検討競合製品

- **Sophos EDR**

お客様事例 2)

医療業界B社

医療業界に関わっていること、企業の規模などから、アンチウィルスソフトでは不足と考えEDR導入を検討。限られた予算の中で運用支援まで対応可能なSentinelOneを導入。

セキュリティ対策の予算が限られている中で、他EDR製品の高額なSOCサービスは予算オーバー。自社運用するにもIT担当のリソース不足で心配。

SentinelOneならAIによる自動の運用監視を活用しながら必要な時だけ運用サポートを受けることで運用内製化を実現。

Company Overview

従業員：約300名
事業　：医療・介護機器の製造・販売
　　福祉施設事業など
本社　：神奈川

導入理由

- **アンチウィルスソフトでは不足と考え強化**
- **AI運用監視×運用サポートで予算を抑えて導入**

検討競合製品

- **WizSecure**

お客様事例 3)

人材紹介会社C社

人材紹介事業を展開しており、求職者の個人情報も多く抱えており、2022年4月から施工された改正個人情報保護法に対応するためSentinelOneを導入。

EDRにより、情報漏洩のリスク減らすだけでなく、万が一の場合もログ情報を使って個人情報保護委員会へ速報・確報を行える体制を整備。

その中でも、コスト・リソース面で運用負担が少ないSentinelOneを導入。

Company Overview

従業員：約100名
事業　：人材紹介・求人広告代理店
本社　：愛知

導入理由

- **改正個人情報保護法への対応**
- **自動運用でコスト・リソース負担が少ない**

検討競合製品

- **ESET EDR**

お客様事例 4)

物流アウトソーシング業D社

顧客から取引時のセキュリティ要件として提示されEDR導入を検討。自社運用しやすそうなSentinelOneを導入。

社内にIT担当のリソースが確保できていたため、内製運用でEDR導入を検討。その中でも、**AIに任せることでインシデントを常時監視する必要がないSentinelOneを導入**。

常時監視はAIに任せ、IT担当は対応ログを定期的に確認して必要な設定変更だけすれば内製運用できるため負担が少ない。グループ全体への展開も予定。

Company Overview

従業員：約300名
事業　：物流業
本社　：東京

導入理由

- **顧客企業からのセキュリティ要件への対応**
- **自動運用でコスト・リソース負担が少ない**

検討競合製品

- **CrowdStrikeEDR**

お客様事例 5）

製造業E社

アンチウィルスソフトだけではセキュリティとして不十分と感じEDR導入を検討。その中でも、XDRの概念で進んでいるSentinelOneを導入。

セキュリティ対策の見直しを進める中で、今後、ネットワークセキュリティや、ID管理など、様々なセキュリティに運用監視が必要になると感じていた。

そんななか、**様々なセキュリティ製品の情報を収集して統合管理するXDRの概念を持ち、すでにネットワーク製品などとの連携が可能なSentinelOneを導入。**

将来的に、各種セキュリティ製品もSentinelOneと連携させていくことを検討している。

Company Overview

従業員：約450名
事業　：製造業
本社　：大阪

導入理由

- **アンチウィルスソフトからの強化**
- **XDRのための整備**

検討競合製品

- **CybereasonEDR**

まとめ

SentinelOne EDRは従来のEDRとは異なる次世代型のEDR製品

① 高い検知能力	AI 機能を用いた高い検知能力でアンチウイルスのリプレースとしても導入可能
② 数ステップの操作でデータを復元	EDR製品が不得意としているデータの復元も数ステップの操作で実行可能
③ レスポンス性能	検出した脅威はクラウドの管理コンソールへ即時反映
④ 解析性能	解析時間を短縮するStoryLine™を搭載 + 拡張EDR機能による高い分析性能を提供
⑤ 裏付けされた高い製品力	Gartner・MITRE ATT&CK などの評価結果に裏付けされた高い製品力


SentinelOne®
ありがとうございました