



# 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11月22日 デジタル×テクノロジー2023

# 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

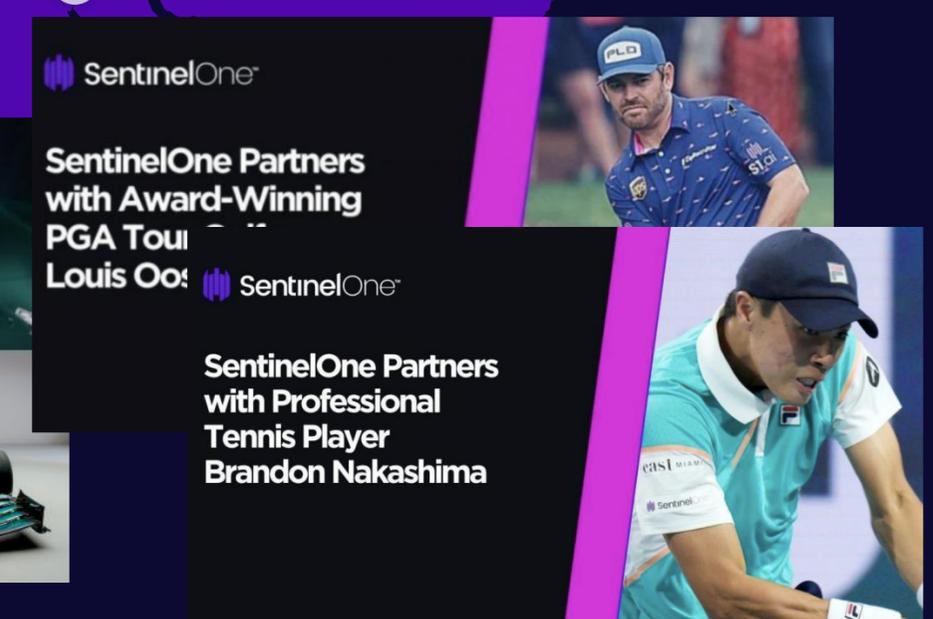
AWS GovCloud 高可用性

## 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 契約交渉中

ATPツアー ブランドン ナカシマ



# 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

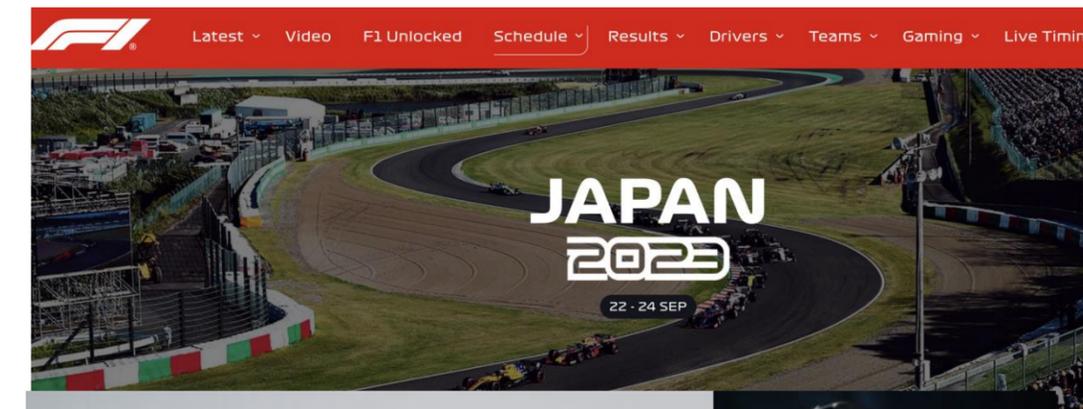
6/9(土)、6/10(日) 19:00台-20:00台  
@TOKYO MX、エムキャストにて放映  
\* 日本法人代表 青山やパートナー企業、エンドユーザー様が出演

## 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



# 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/>



EDRソリューション市場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>



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

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (December 2022)

### 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

技術に前のめりな組織

**Highest Score**

#### TYPE B USE CASE

総合的に判断する組織

**Highest Score**

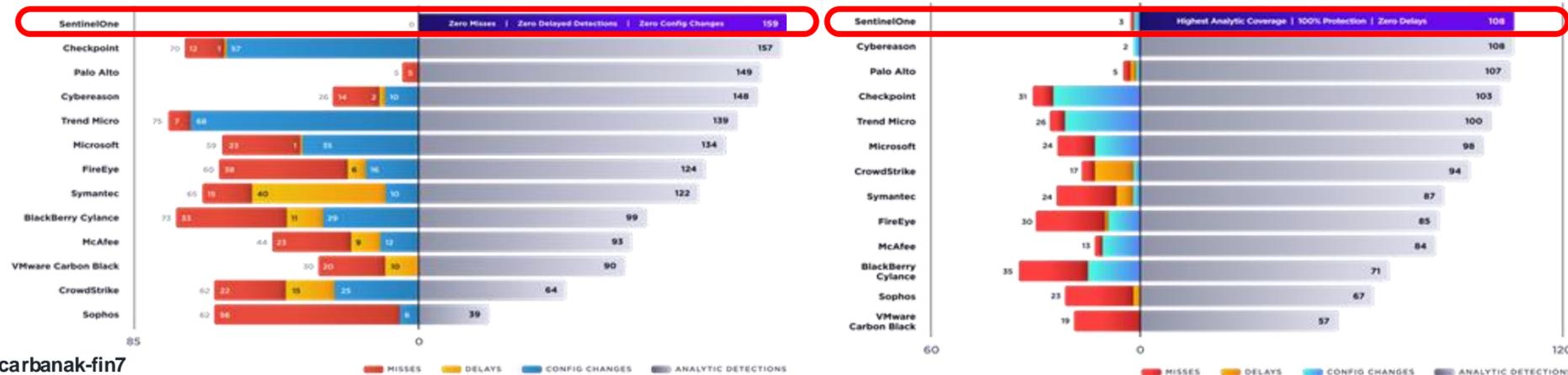
#### TYPE C USE CASE

予防重視の組織

**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

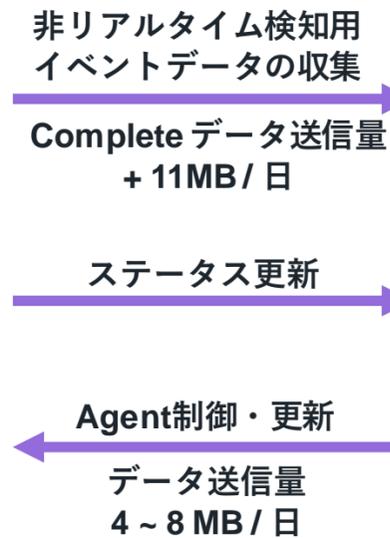
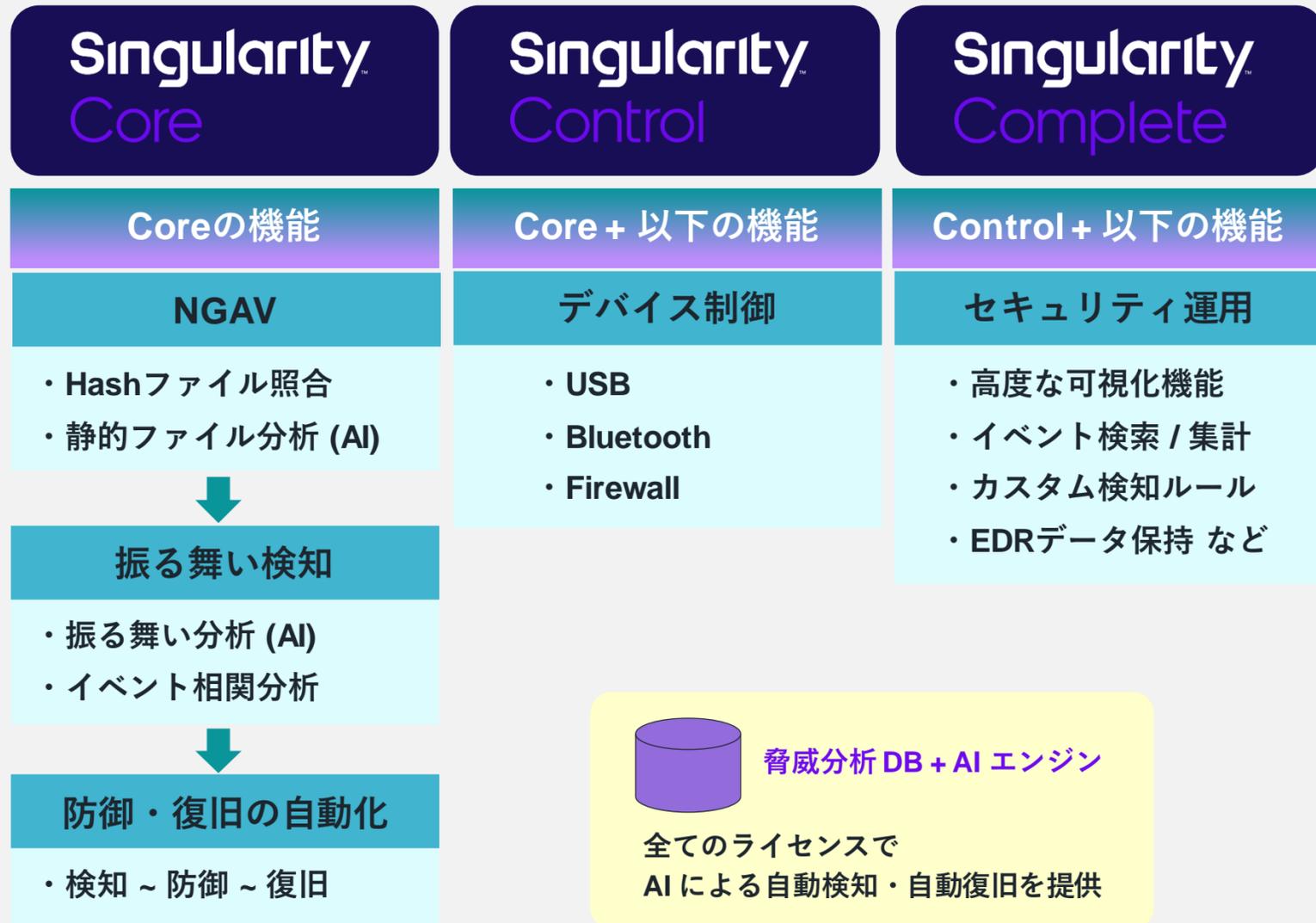
✓ ゼロ設定変更

✓ ゼロ検出遅延

# SentinelOne EDR

## 自律型 AI + クラウド型の EDR

 3種類の基本ライセンスを提供・エンドポイントへAgentを導入



# 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

## アドオン機能

搭載機能	Complete	Control	Core
グローバルSaaSプラットフォーム	●	●	●
<b>基本的なエンドポイント保護機能</b>			
自律型SentinelエージェントStoryline™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	●	●	●
<b>IT OPS/セキュリティハイジーン&amp;スイート機能</b>			
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	●	●	●
<b>セキュリティ運用のEDR機能</b>			
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	●	●	

搭載機能	Complete	Control	Core
<b>Singularity RANGER</b>			
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	○		
<b>Singularity Cloud</b>			
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

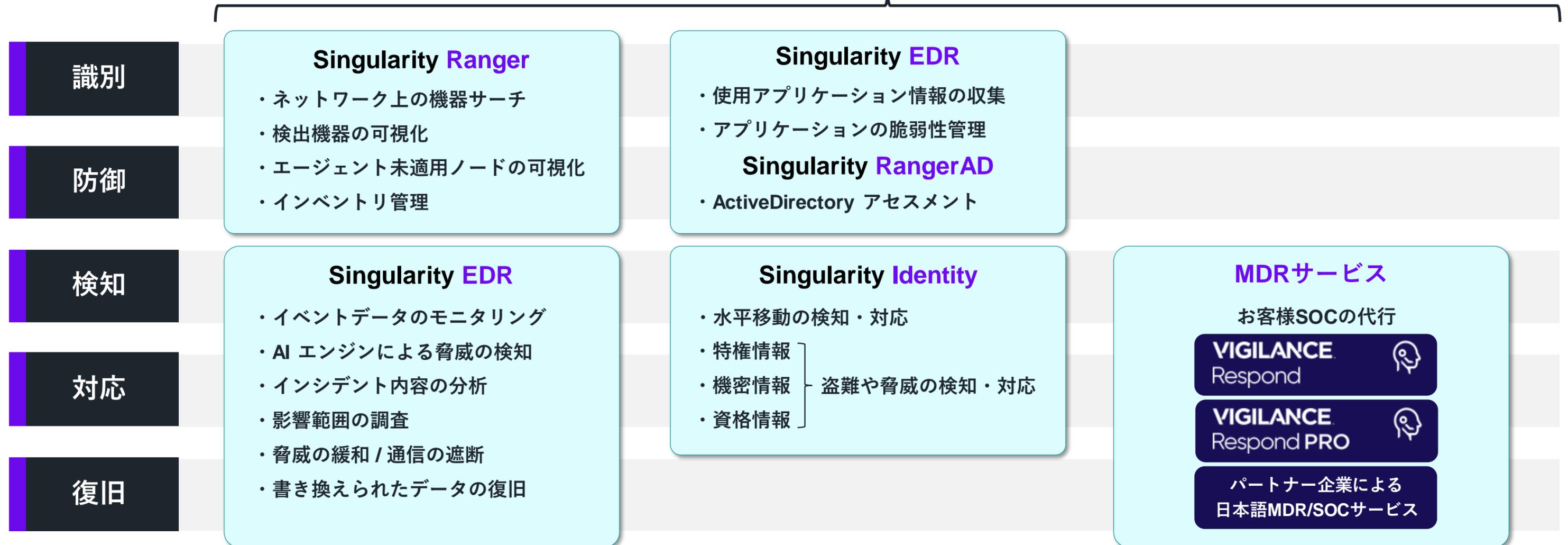
復旧計画の作成・改善・コミュニケーションの3つのカテゴリーで構成され、セキュリティインシデント発生時の具体的な復旧方法や関係者への伝達といった面についてもまとめている。

# 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

### Singularity XDR



# 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

Name	Vendor	Number Of Versions	Number Of Endpoints
VMware Tools	VMware, Inc.	1	2
Sentinel Agent	Sentinel Labs, Inc.	1	2
Microsoft Visual C++ 2015-2019 Redistributable -	Microsoft Corporation	1	2
OpenHashTab バージョン	...	...	...
Mozilla Thunderbird	...	...	...
Mozilla Maintenance Service	...	...	...
Mozilla Firefox	...	...	...
Microsoft Update Health Tools	Microsoft Corporation	1	1
Microsoft OneDrive	Microsoft Corporation	1	1
Microsoft Office Professional Plus 2013	Microsoft Corporation	1	1

Endpoint Name	Endpoint Type	OS	OS Version
win10-41	Desktop	Windows	Windows 10 Pro 19045
win2019-111	Server	Windows	Windows Server 2019 Standard 177...

### 検出したアプリケーションの脆弱性の一覧

CVE ID	Endpoint Name	Application Name	Vendor	Severity	NVD Base Score	Days From
CVE-2021-4140	win10-41	Mozilla Thunderbird 60.6.1	Mozilla	Critical	10 (CVSS v3.1)	6 Days
CVE-2021-38503	win10-41	Mozilla Thunderbird 60.6.1	Mozilla	Critical	10 (CVSS v3.1)	6 Days
CVE-2019-11708	win10-41	Mozilla Thunderbird 60.6.1	Mozilla	Critical	10 (CVSS v3.0)	6 Days
CVE-2019-9800	win10-41	Mozilla Thunderbird 60.6.1	Mozilla	Critical	9.8 (CVSS v3.0)	6 Days
CVE-2019-9819	win10-41	Mozilla Thunderbird 60.6.1	Mozilla	Critical	9.8 (CVSS v3.0)	6 Days

**CVE Details**

Mozilla Thunderbird 60.6.1 by Mozilla

**9.8 CVE-2019-9819**

Published Jul 23, 2019

Detected Feb 2, 2023 (6 days ago)

Description

A vulnerability was found in Mozilla Firefox, Thunderbird and Firefox ESR (Web Browser) (affected version unknown). It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Fetch API. Upgrading eliminates this vulnerability.

[View On MITRE](#) [View On NVD](#)

**Endpoint Details**

Endpoint Name

**win10-41**

Scope

SentinelOne Japan / 01 / Group-01

Domain

LAB

[cve.orgで詳細確認](#) [NISTで詳細確認](#)

- ・ 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

The screenshot displays the SentinelOne console interface for device control. The top navigation bar includes 'SENTINELS', 'エンドポイント', 'タグ', 'ポリシー', 'ブラックリスト', '除外設定', 'ネットワーク制御', 'デバイス制御', 'アップグレードポリシー', and 'グループ情報'. The 'デバイス制御' tab is active, showing a 'Block-USB' rule configuration. The rule name is 'Block-USB', the interface is 'USB', and the rule type is 'ベンダーID'. A dropdown menu for 'ベンダーID' shows options: 'ベンダーID', 'クラス', 'シリアルID', and 'プロダクトID'. Below this, there are two Windows File Explorer windows. The left window shows the 'USB ドライブ (E:)' selected. The right window shows a message '使用不可' (Not available) with a red 'X' over the USB drive icon. At the bottom, there are two 'Block-Bluetooth' rule configuration panels. The first panel shows 'Rule name: Block-Bluetooth', 'Interface: Bluetooth', 'Rule Type: ハードウェア識別子', and 'Action: Block'. The second panel shows 'ベンダーID: Any', 'プロダクトID: Any', 'クラス: Any', and 'マイナークラス: Any'.

### Firewallの設定

The screenshot displays the SentinelOne console interface for firewall settings. The top navigation bar is the same as the previous screenshot. The 'ネットワーク制御' tab is active, showing a 'Create New Rule' configuration. The rule name is 'ICMP-Drop-192.168.2.254', the OS type is 'Windows', and the action is 'Block'. A 'Rule Values' panel on the right shows various settings like 'OS Type: Windows', 'Action: Block', 'Scope: SentinelOne Japan -> Tokyo -> Sales-01', and 'Rule parameters'. Below the console, there are two Windows Firewall configuration windows. The top window shows 'Firewall Control is on' and a table of rules. The bottom window shows the Windows Defender Firewall settings, with a yellow warning box stating 'これらの設定は、ベンダー アプリケーション SentinelOne Firewall で管理されています'. A command prompt window at the bottom right shows the command 'C:\Users\User1041>ping 192.168.2.254' and the output: '192.168.2.254 に ping を送信しています 32 バイトのデータ: 一般エラー。 一般エラー。 一般エラー。 一般エラー。 192.168.2.254 の ping 統計: パケット数: 送信 = 4、受信 = 0、損失 = 4 (100% の損失)'.

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

**SECURED STATE**

50%	Secured
25%	Unsupported
25%	Unsecured

**DEVICE REVIEW**

62.5%	Allowed
37.5%	Not Reviewed

**DEVICES (TOTAL: 8)**

ワークステーション	4	サーバ	2
ネットワーク	2	不明	0
サーバーインフラ	0	モバイル	0
プリンター	0	ビデオ	0
IP電話	0	ストレージ	0

**OS TYPE**

Windows 6	Linux 2	アンドロイド 0
Apple 0	Unix 0	不明 0
レガシー Windows 0	シスコ 0	ワイズ WYSE 0

Scanning Network... Latest scan finished at Feb 8, 2023 09:32

タイプ	IPアドレス	OS	デバイス機能	OSバージョン	保護状態	ホスト名	Macアドレス	ドメイン	デバイスレビュー	TCPポート	UDPポート	発見方法	初回検知	最終更新日時
ワークステーション	192.168.99.71	Windows	Workstation	Windows 10 Pro	Secured	win10-41	00:50:56:a6:55:f6	LAB	Allowed	3389 135 445	53	agent	Dec 15, 2022 16:12:00:120	Feb 8, 2023 09:32:56:3256
ワークステーション	192.168.4.41	Windows	Workstation	Windows 10 Pro	Secured	win10-41	00:50:56:a6:09:23	LAB	Allowed	445 3389 135	53	agent	Dec 15, 2022 16:12:00:120	Feb 8, 2023 09:32:56:3256
サーバ	192.168.1.111	Windows	Server	Windows Server 2019 Sta...	Secured	win2019-111	00:50:56:a6:07:35	LAB	Allowed	なし	なし	agent	Jan 10, 2023 14:25:56:25...	Feb 8, 2023 09:32:56:3256
サーバ	192.168.1.1	Windows	Server	Windows Server 2019 Sta...	Unsecured	_ldap	00:50:56:a6:6a:a2	なし	Not reviewed	なし	なし	neighbor	Jan 10, 2023 21:24:03:243	Feb 8, 2023 08:37:14:3714
Router		Generic	Router	Generic	Unsupported	なし	00:0c:29:8c:2c:6e	なし	Not reviewed	なし	なし	neighbor	Jan 10, 2023 21:24:03:243	Feb 8, 2023 08:37:14:3714

**Legend:**

- Secured (Green checkmark)
- Unsecured (Red X)
- Unsupported (Blue minus)

**Legend Text:**

- エージェント適用済 (Agent Applied)
- エージェント未適用 (Agent Not Applied)
- エージェント適用外(通信機器など) (Agent Not Applied (Communication devices, etc.))

**Action Menu:**

- エージェントの展開
- タグデバイス
- デバイスのフィンガープリントを更...
- デバイスレビューを適用する
- ネットワークから隔離

**Callout:** エージェント未適用のノードに対して遠隔インストールを行うこともできます

- ・ 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

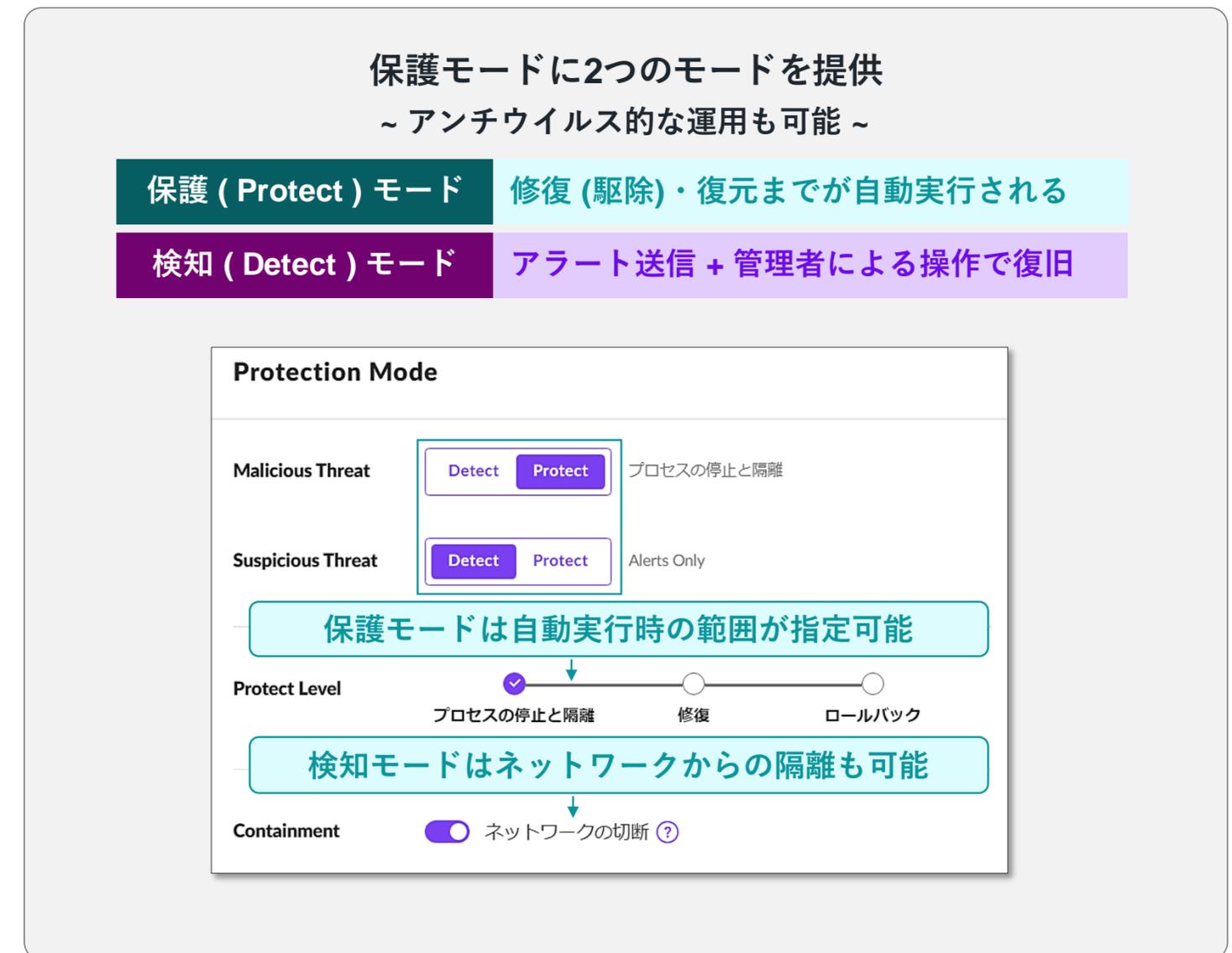
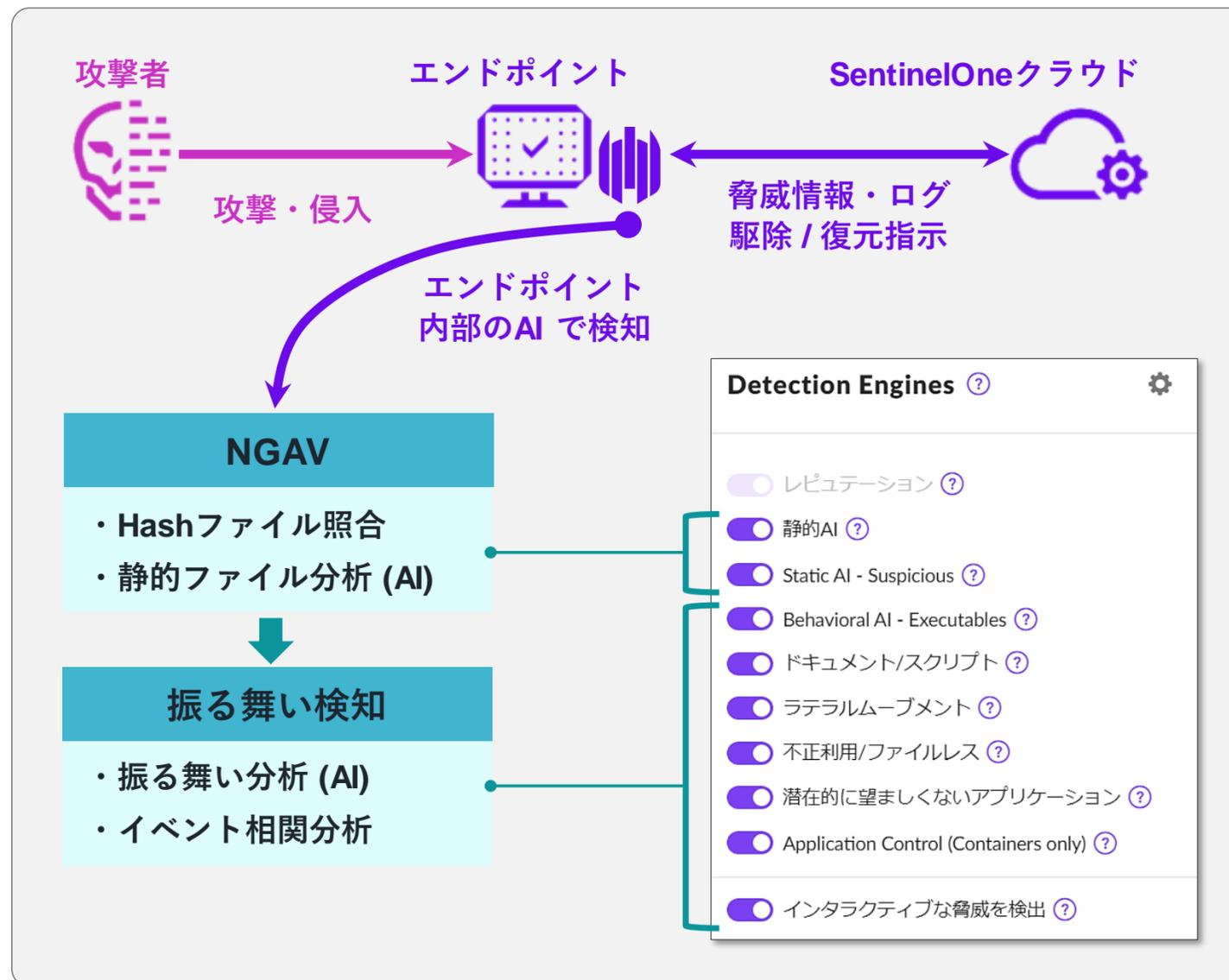
対応

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



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

#### エンドポイント

(感染)



人・ツール・所要時間

#### ■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

#### エンドポイント

(復旧)



### SentinelOneでの復旧方法

#### エンドポイント

(感染)



ワンクリック・短時間・確実

#### ■復旧の仕組み

- ・ VSSを定期的を取得 ( 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

#### エンドポイント

(復旧)



※ 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。

# Purple AI - 生成 AI を利用したインシデント対応（2024年春リリース予定）

The screenshot displays the SentinelOne Purple AI interface. The top navigation bar includes 'Singularity XDR', 'SentinelOne', 'Purple AI', 'Logs', 'Search', 'Dashboards', 'Star Custom Rules', 'Alerts', and 'Docs'. The main interface is divided into several sections:

- SOURCES:** All (2)
- FIELDS:** Filter fields (8, 28, 15, 119, 3, 14, 14, 14, 2, 1, 12, 3, 2, 13, 26, 1, 6, 17, 9, 76, 3, 53, 32, 25, 56, 250, 121)
- Event Details:** Search event, Event Actions
- Purple AI:** Beta button, analysis text (see below)
- Event Summary:** 68,449 matching events, 10 seconds / bar, Expand Graph
- Event Table:** Agent UUID, Object Type, Event type, Event
- Endpoint Details:** IP Connect, Agent UUID, Source Process Unique ID, Source IP, Source Port, Destination IP, Destination Port

**Purple AI Analysis Text:**

イベント中、「プロセスハンドルの重複」イベントが342件発生し、潜在的な不審なアクティビティが示されました。「firefox.exe」として識別されるソースプロセスは、表示名「Firefox」とコマンド引数「C:\Program Files\Mozilla Firefox\firefox.exe」を持つプロセスによって作成されました。ソースプロセスは「Program Files」ディレクトリにあります。ソースプロセスは署名されていないため、その信頼性と完全性について懸念が生じます。さらに、ソースプロセスには28,424件のファイル変更イベントと8,800件のファイル作成イベントという多数のイベントがあり、潜在的な悪意のあるアクティビティを示唆しています。ソースプロセスには、検出を回避しようとする試みを示す、回避手法に関連する16,287個の多数のインジケータも含まれています。ソースプロセスは、HTTPSプロトコルを使用して、ポート443上のIPアドレス157.240.3.29への送信ネットワーク接続を作成しました。イベントは2回同時に発生しました。オペレーティングシステムに関しては、エンドポイントはWindows上で実行されます。ソースプロセスはWin32サブシステムで実行されており、整合性レベルは中程度です。処理はユーザー名「GUNTER-PC\GUNTER」で実行されました。ソースプロセスを作成した親プロセスも「firefox.exe」であり、「MOZILLA CORPORATION」によって署名されています。親プロセスの整合性レベルは中程度で、「Program Files」ディレクトリにあります。親プロセスはソースプロセスと同じユーザー名で実行されました。ソースプロセスはネイティブ64ビットではなく、stdoutリダイレクトがありません。イベントデータは、ソースプロセスから宛先IPアドレスへのネットワーク接続の成功を示します。ソースプロセスには、一般的な動作に関連する25,687個の多数のインジケータがあり、潜在的な悪意のあるアクティビティを示唆しています。全体として、イベントデータはソースプロセス「firefox.exe」に関連する不審なアクティビティを強調しており、その整合性と潜在的な悪意についての懸念を引き起こしています。

Agent UUID	Object Type	Event type	Event
GUNTER-PC 986477c8887342b8b9741341e0c802f2	ip	IP Connect	Oct 7 7:24
GUNTER-PC 986477c8887342b8b9741341e0c802f2	ip	IP Connect	Oct 7 7:24
GUNTER-PC 986477c8887342b8b9741341e0c802f2	dns	DNS Resolved	Oct 7 7:24
GUNTER-PC 986477c8887342b8b9741341e0c802f2	ip	IP Connect	Oct 7 7:24
GUNTER-PC 986477c8887342b8b9741341e0c802f2	dns	DNS Resolved	Oct 7 7:24
GUNTER-PC 986477c8887342b8b9741341e0c802f2	dns	DNS Resolved	Oct 7 7:24
GUNTER-PC 986477c8887342b8b9741341e0c802f2	indicators	Behavioral Indicators	Oct 7 7:24
GUNTER-PC 986477c8887342b8b9741341e0c802f2	dns	DNS Resolved	Oct 7 7:24
GUNTER-PC 986477c8887342b8b9741341e0c802f2	ip	IP Connect	Oct 7 7:23
GUNTER-PC 986477c8887342b8b9741341e0c802f2	dns	DNS Resolved	Oct 7 ---

Agent UUID	Endpoint Actions
GUNTER-PC 986477c8887342b8b9741341e0c802f2	Endpoint Actions

Endpoint Details:

- IP Connect
- Agent UUID: GUNTER-PC (986477c8887342b8b9741341e0c802f2)
- Source Process Unique ID: firefox.exe (0A1A71A18D152AFC)
- Source IP: 192.168.1.5
- Source Port: 64734
- Destination IP: 157.240.3.29
- Destination Port: 443

# お客様事例



# 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**

# 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、アンチウイ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

- アンチウイ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**

# 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

# 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**

# 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