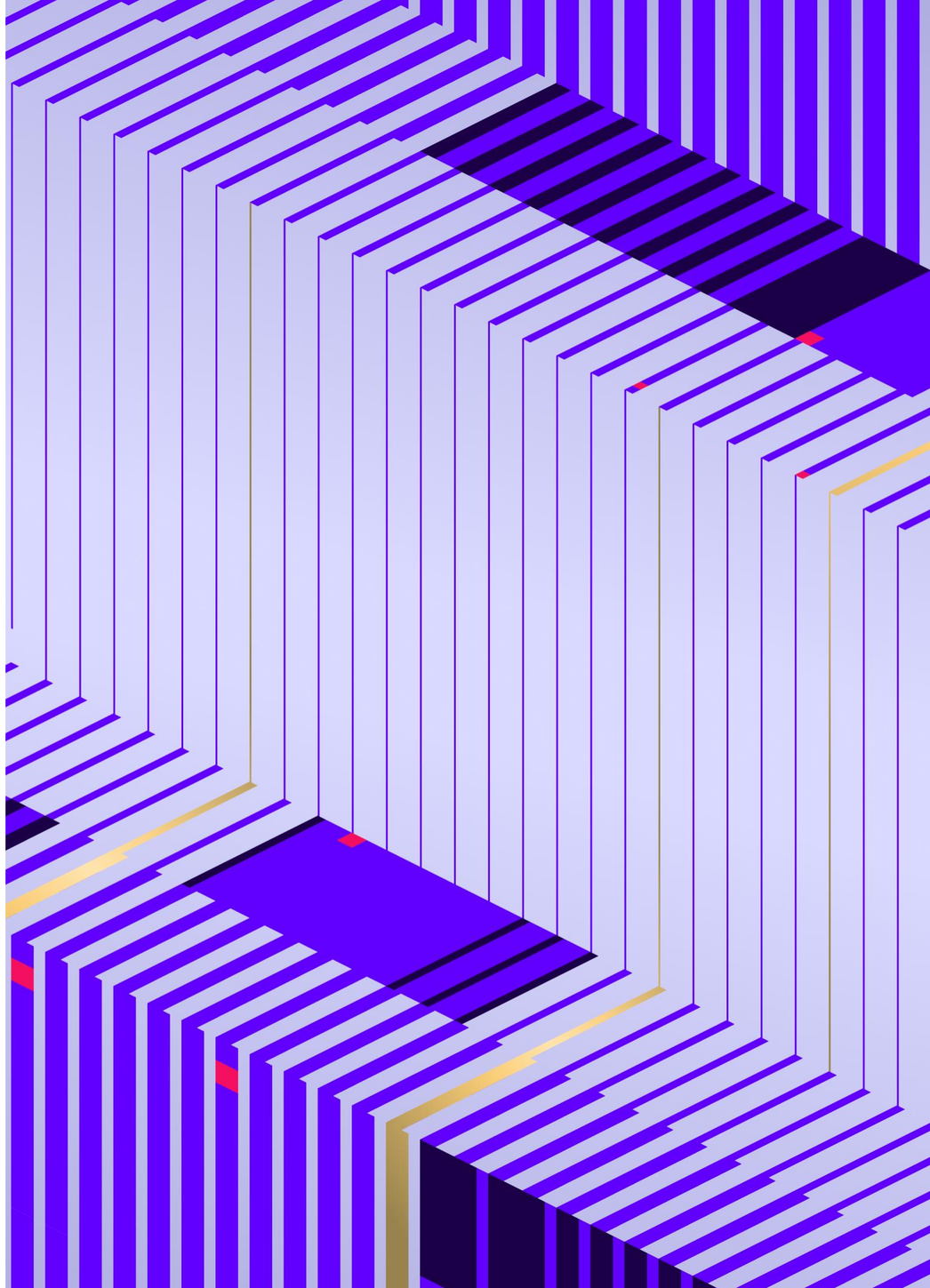
SentinelOne
Singularity Endpoint のご紹介

株式会社 アイ・アイ・エム



Singularity Platform の価値

単一のコンソールとプラットフォーム
ベンダーを統合し１つのソリューションで実現

作業効率の向上
組織全体で数日以内に完全展開および保護

TCOの削減
統合エージェントによるライセンスコストの抑制

データレイクの統一
統一されたデータプラットフォームによる効率的な運用

オープンエコシステム
導入済みセキュリティツールを有効活用

優れた保護機能の提供
MITER における高い評価（100% 防御）

連携製品による対応の自動化
SOC ワークフローの効率化

使いやすい管理コンソール
使いやすいコンソールへの統合により管理負荷を軽減

SentinelOne が選ばれる理由

SentinelOne が提供する
さまざまなセキュリティ
機能をすべて一つの
コンソールで運用管理

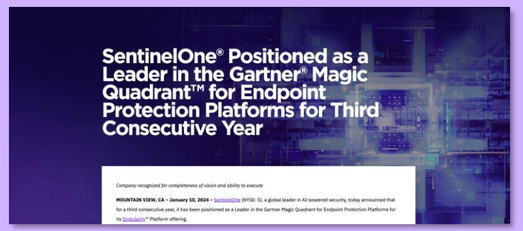
アラートの確認から
エンドポイントの隔離・修復
まで直感的でわかりやすい
インシデント対応が可能

万が一ランサムウェアに感染
した場合でも管理コンソール
から遠隔で迅速に暗号化
されたファイルを復旧

第三者機関の評価

Gartner

2021, 2022, 2023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
→ 3年連続でリーダーポジションを獲得



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

Gartner peerinsights™

EDR ソリューションマーケット部門
→ユーザーによる高い評価を獲得。
96%のお客様がSentinelOneを推奨

https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/sentinelone/product/singularity-xdr/reviews

MITRE ENGENUITY™

2020年、2022年、2023年の各ラウンド連続で
トップの検知能力を証明。

https://www.sentinelone.com/lp/mitre/

SentinelOne 製品ラインナップ

Singularity 基本ライセンス

Singularity Endpoint

Singularity Core
EPP 自律型 AI（ファイル検知・振る舞い検知）

Singularity Control
Singularity Core の機能 + デバイス制御 + アプリケーションインベントリ管理

Singularity Complete
Singularity Control の機能 + EDR/XDR

本日ご紹介の製品

Singularity 追加ライセンス

* Control が必要（サーバープラットフォームには Control 以上が必要）
** Complete が必要

Singularity Cloud
クラウドインスタンス・コンテナ* セキュリティ

Singularity Mobile
モバイルセキュリティ

Singularity Ranger
IP デバイス管理・エージェント展開

Singularity Ranger Insights
脆弱性管理

Singularity RangerAD
Active Directory アセスメント

Singularity Identity
認証情報保護（デセプション）

Hologram
おとりサーバ（デセプション）

CloudFunnel
外部クラウドストレージへの XDR データのアーカイブ **

RemoteOps
自動フォレンジック **

BinaryVault
バイナリファイルアーカイブ **

Singularity Data Lake
XDR およびサードパーティデータの長期間保存および分析

Purple ai
EPP 自律型 AI（ファイル検知・振る舞い検知）

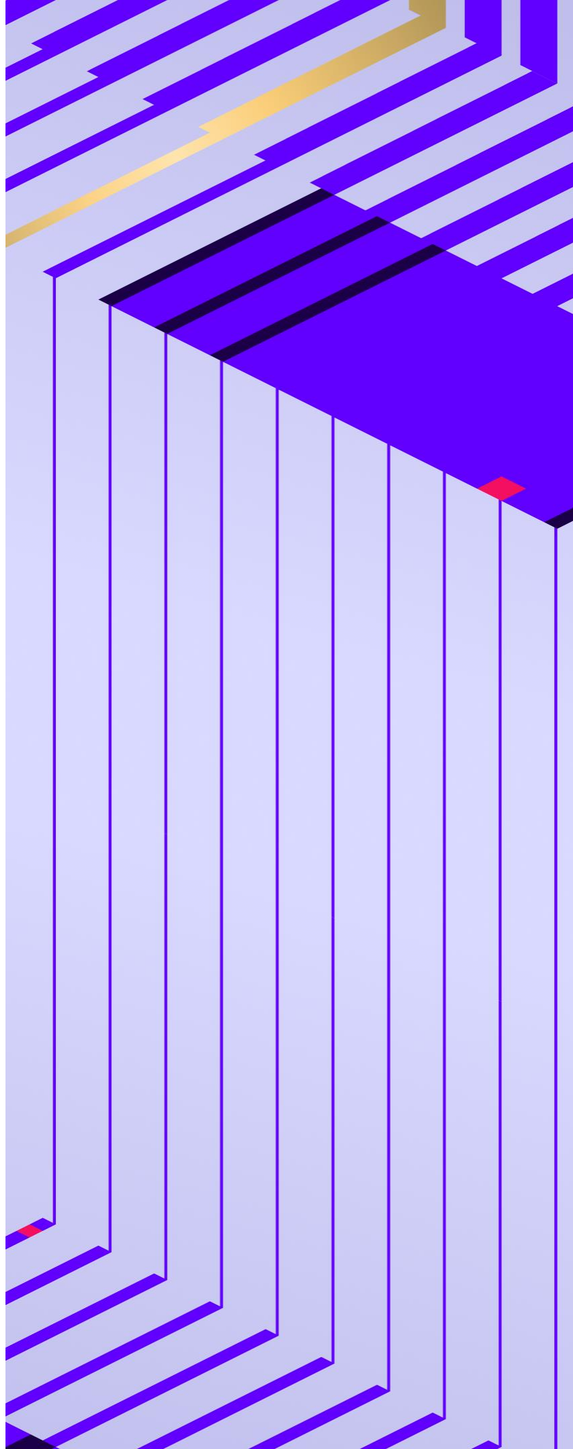
サービス（英語での提供）

VIGILANCE Respond
MDR

VIGILANCE Respond PRO
MDR + DFIR

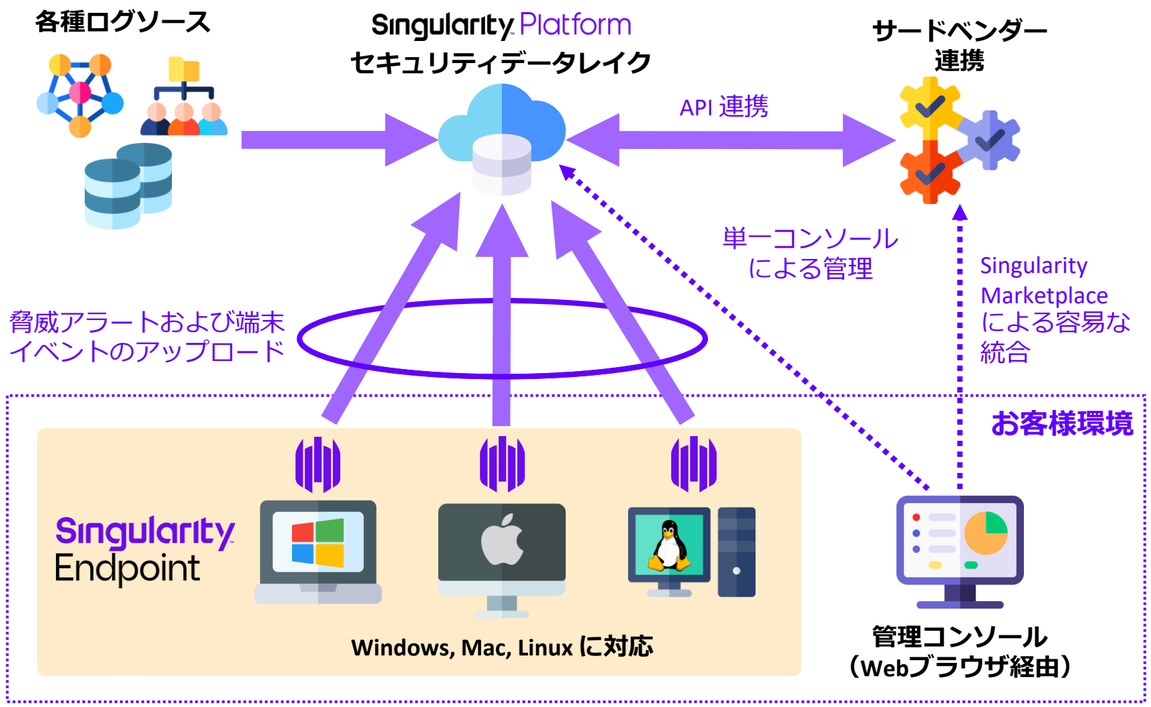
WatchTower
脅威ハンティング

Singularity Endpoint
のご紹介



Singularity Endpoint

従来型エンドポイントセキュリティ製品
から乗り換え可能な EPP の機能と侵入後の
不正なアクティビティを検知する EDR の
機能を単一コンソール・
シングルエージェントで提供



ライセンスの種類と主な機能

Singularity Complete

Singularity Control の機能 ＋

- EDR による端末イベントの収集および可視化
- STAR™ によるカスタムルールでの脅威検知

Singularity Control

Singularity Core の機能 ＋

- ホストベースFW、デバイスの制御、リモートシェル
- アプリケーションのインベントリおよび脆弱性管理

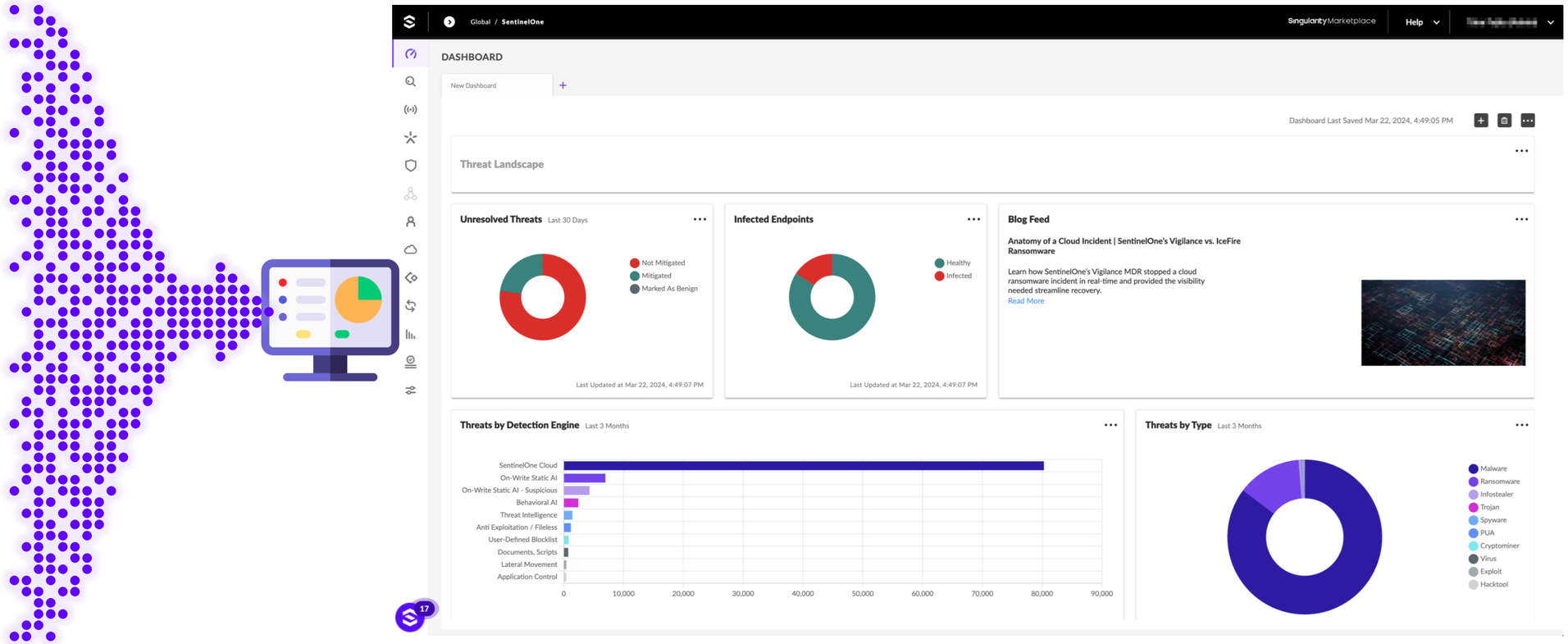
Singularity Core

- エージェント未導入デバイスの検出
- シングルプラットフォームでの運用管理
- 自律型 AI による静的ファイルおよび動的振る舞い解析
- 不正プログラム検知時の自動隔離
- Storyline™ 技術による高度な脅威検出
- 1クリックでの修復およびロールバック

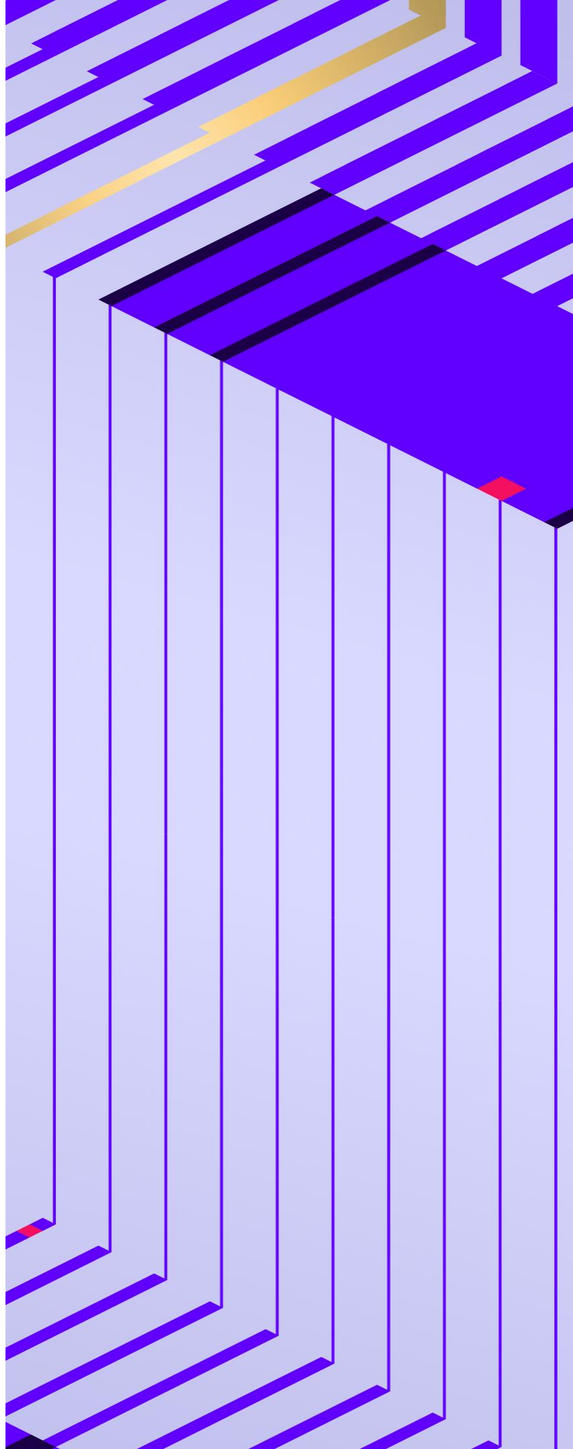
SentinelOne 製品をシングルコンソールで管理

SentinelOne 製品を統一されたインターフェースに集約することで
ナビゲーションを簡素化し、シームレスなユーザーワークフローを実現

- EPP 自律型 AI
（ファイル検知・振る舞い検知）
- デバイス制御・
アプリケーション管理
- EDR・XDR
- IP デバイス管理・
エージェント展開
- 脆弱性管理
- Active Directory
アセスメント
- 認証情報保護
（デセプション）
- クラウドインスタンス・
コンテナセキュリティ
- セキュリティデータの取込・
正規化・視覚化・長期保存



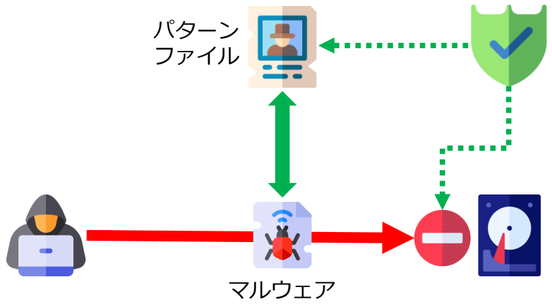
Singularity Core のご紹介



従来のセキュリティ対策との違い

IIM
Singularity Core

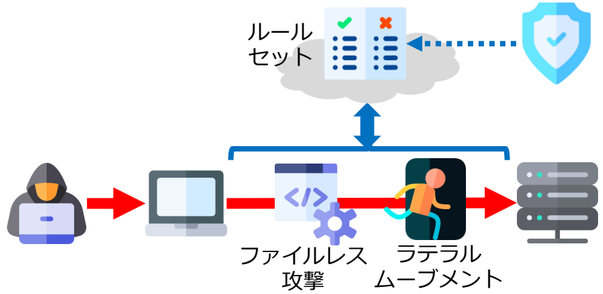
従来型ウイルス対策製品



ハードディスクに書き込まれる際に**パターンファイルやヒューリスティック**によるファイルスキャンで不正プログラムを検知

パターンファイルやヒューリスティック技術は**既知の疑わしいファイル**や**未知の実行形式ファイルであることが前提**のためOSに組み込まれている機能や公開されている市販ツールなど**信頼された機能やツールを悪用した攻撃の検知は困難**

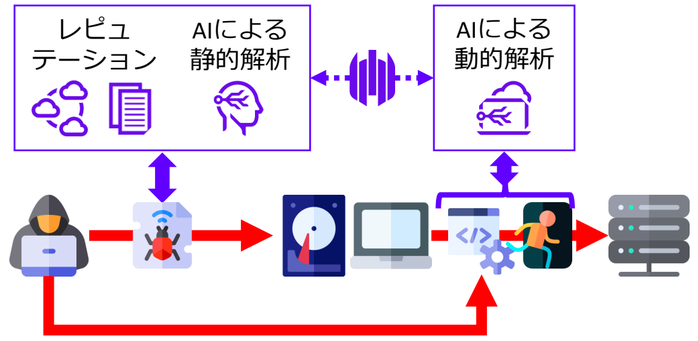
従来型 NGAV 製品



パターンファイルやヒューリスティックを利用せず、**疑わしい振る舞いを検知するためのローカルやクラウド上のルールセット**を利用することでルールセットに合致したOSに組み込まれている機能や公開ツールによる疑わしい振る舞いを検知

最新の脅威にはクラウドベースでの検知に依存するため**タイミングによって不正行為そのものが止められない場合**があり、さらに**検知時の対処がインターネットに接続されていることが前提**のため**従来型のウイルス対策製品やEDRやMDRによる分析・対処との組み合わせての利用が前提**

Singularity Endpoint



既知の不正プログラムを検知するためのレピュテーション技術に加えクラウドに依存しない**オフラインで稼働する静的・動的両方に対応した自律型AI機能**により動作前の不正プログラムおよびOSの機能や市販ツールの悪用による不正行為に対して**ローカル側で迅速に対処**

高度なセキュリティ対策をオフライン環境で実現できるため**従来型ウイルス対策製品やNGAV製品からのリプレースが可能です。**

SEIKO GROUP

Singularity Endpoint における保護機能の特徴

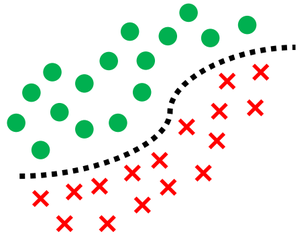
IIM

Singularity Core

EPP（エンドポイント保護プラットフォーム）

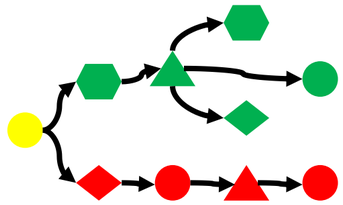
EDR（エンドポイント検知・対応）

リアルタイム ファイル分析



AI による静的
ファイル構造解析

リアルタイム 行動分析



AI による動的
プロセス振る舞い解析

自動または 1クリックでの回復

- プロセスの停止と隔離
- ネットワークの切断
- 不正行為によるシステム変更やファイル生成からの修復
- ランサムウェアによる暗号化からのロールバック

高い可視性と 迅速な対応

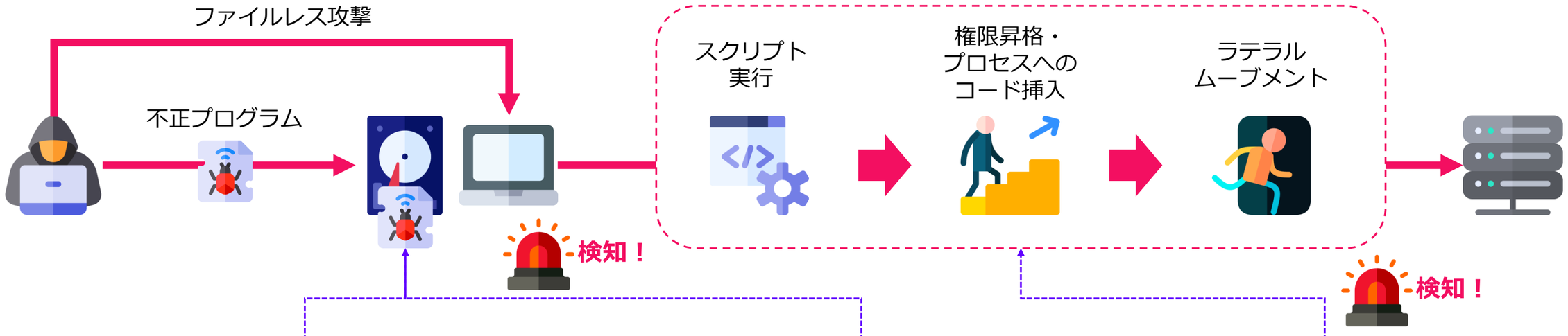
- 単一の脅威に関連するプロセスを自動的に関連付け・可視化
- MITRE ATT&CK TTPへの自動マッピング
- 管理コンソール経由でのインシデント対応
- ユーザーが作成したカスタムルールでの検知

クラウドに接続できない オフライン環境下でも動作

Singularity Platform
セキュリティデータレイク

SEIKO GROUP

オフラインで実現可能な検知テクノロジー



レピュテーション

ローカルブラックリスト
によるハッシュファイル照合

クラウドレピュテーション
によるハッシュファイル照合

- 既知の不正プログラムを効率的に検知する技術を提供
- クラウドに接続可能な場合はローカルに保持するブラックリストに加えクラウド上の最新のレピュテーション情報も活用
- クラウドで不正プログラムが検知された場合ローカルのブラックリストを更新しさらに同一環境内のエージェント全てに自動で情報共有

AI による静的解析

AI による静的ファイル
構造解析

- 数百万のファイルを分析しトレーニング・構築された機械学習エンジンによって検出した不正プログラムの脅威指標に対して **AI を活用し信頼スコアを算出**
- 算出されたスコアに基づいて不正プログラムを識別

AIによる動的解析

AIによる動的
プロセス振る舞い解析

- 監視対象のosおよびプロセスの各操作を特徴づけるイベントデータを生成
- イベントデータを使用して構築されたステートフルモデルに対して **AI を活用し分析、悪意ある行為を検出**

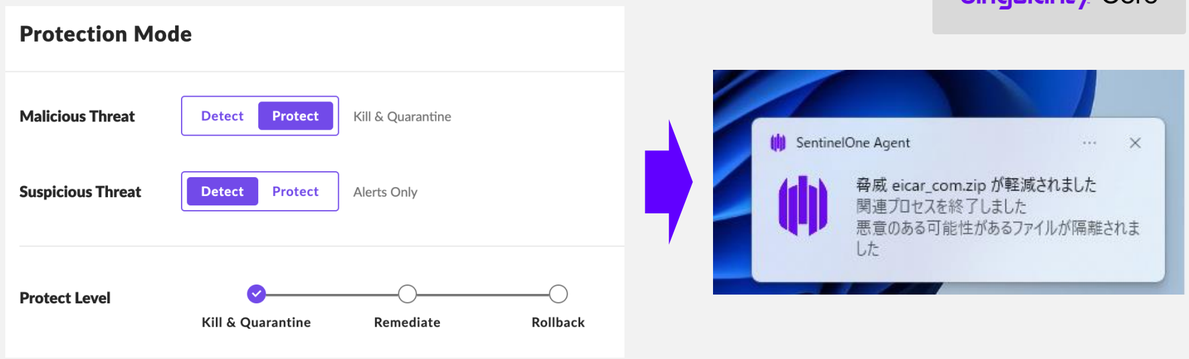
検知時の自動対応

エンドポイントにてリアルタイムで
検出した脅威に対してプロセスの停止や
ファイルの隔離、ネットワーク隔離を
エンドポイント側で自動実行

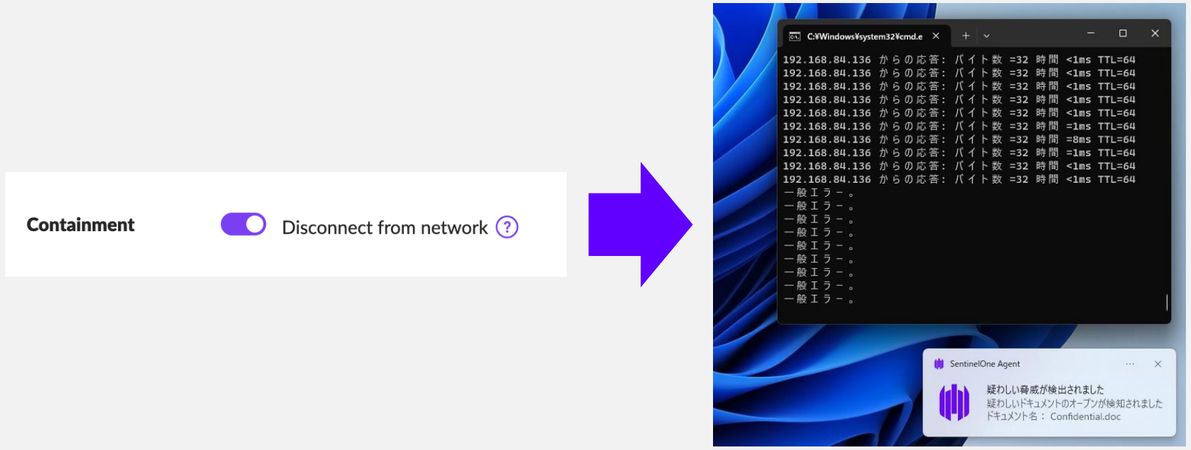
主な特徴

- 自律型で動作するため、オフライン状態でも
  自動でファイルの隔離やネットワーク隔離の
  実行が可能
- 隔離されたファイルは管理コンソール経由
  での取得、およびリモートでの復元が可能
- ネットワーク隔離のデフォルト設定では、
  管理サーバ以外の通信は全てブロック
- ネットワーク隔離の除外ルール設定により
  特定のアプリケーションや通信先の
  アドレスなど通信を許可する条件の設定が可能

Singularity Core



明らかに脅威であると判断されたファイルに対しては
プロセスの停止および脅威ファイルの隔離を自動実行



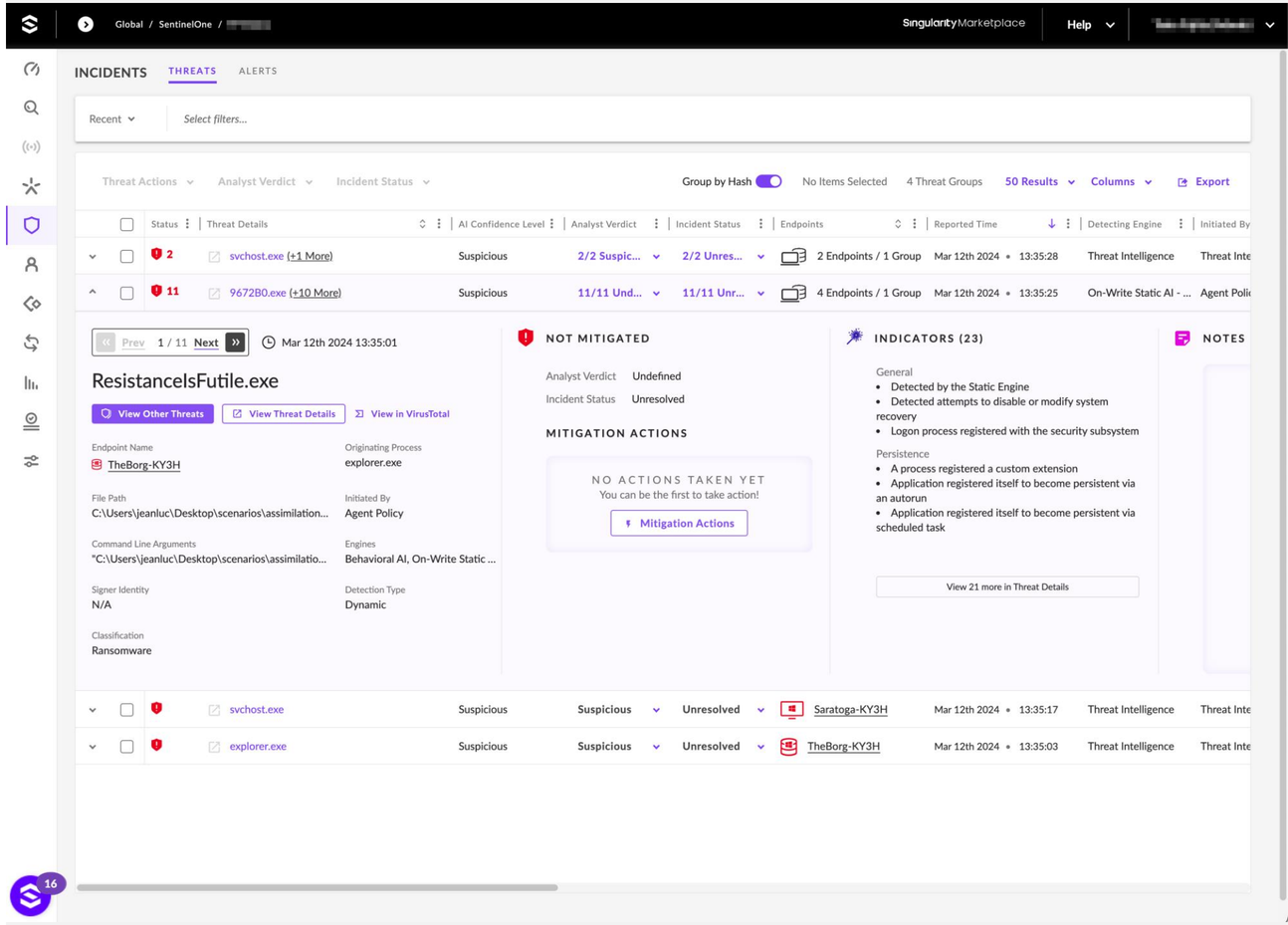
ファイル実行後の振る舞いが疑わしいと判断された場合
自動でエンドポイントの通信を強制的に切断することも可能

検知された脅威の確認

検知された脅威が確認可能な Threat ページでは、一覧表示、フィルタリング、検索および検知された脅威に対する対応アクションの実行が可能

主な特徴

- SentinelOne の自律型エージェントが検知したマルウェアまたは疑わしい行為をリスト形式で表示
- 特定の脅威や疑わしい行為を迅速に見つけるための多様なフィルタオプションや検索機能が利用可能
- [Group by Hash] 機能で同じハッシュ値を持つ脅威を一つの行にまとめることで、類似した脅威に対する一括の調査および処理が可能
- 脅威が検知されたプロセスをクリックすることで脅威の詳細の確認が可能

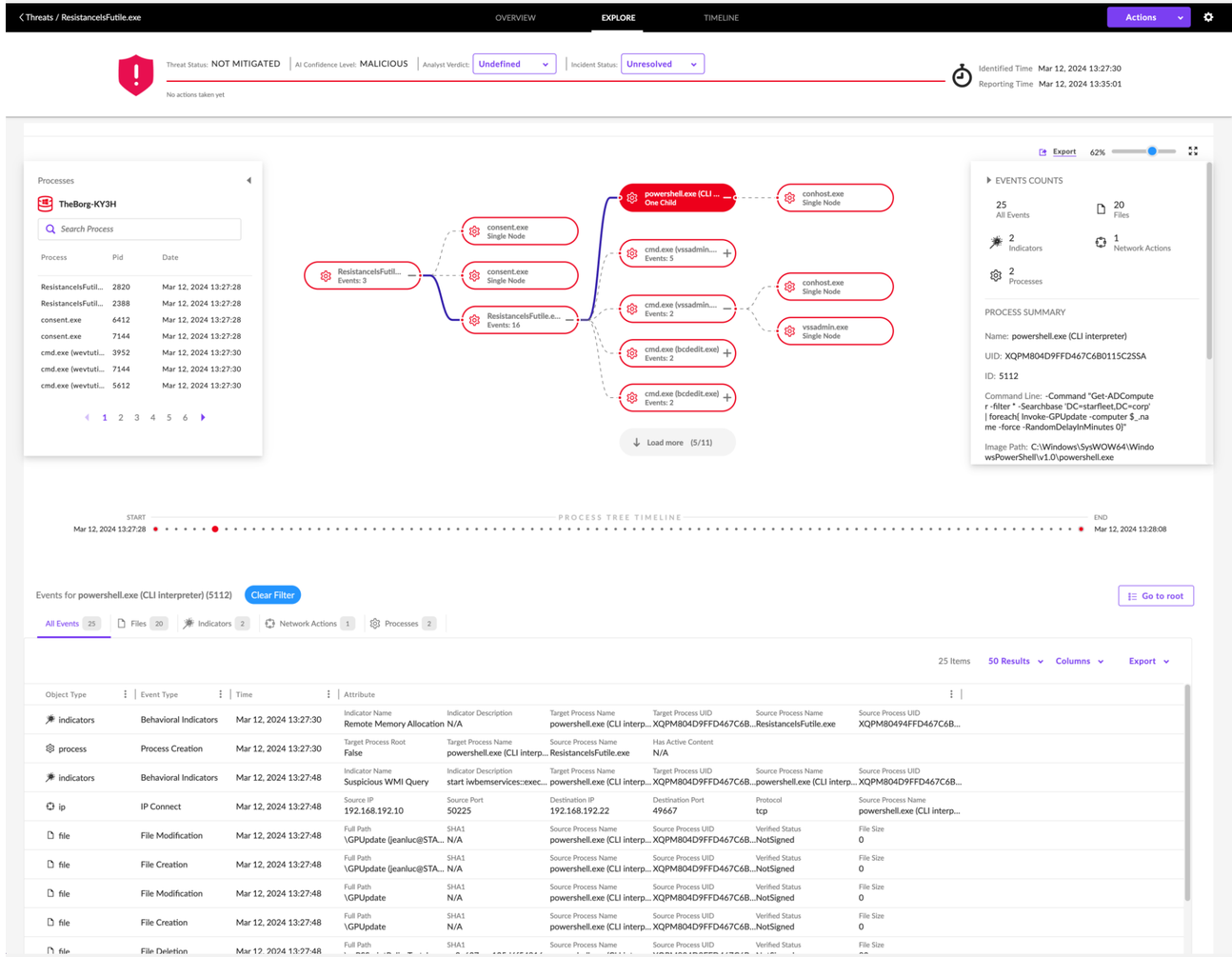


Storyline™ による脅威の可視化

エンドポイントのセキュリティイベントを
自動的に関連付け、リアルタイムで
更新される脅威のストーリーを可視化
することで迅速な分析と対応を支援

主な特徴

- SentinelOne の自律型エージェントが検知した
  単一の脅威に関連するイベントを自動的に
  グループ化し、それらを一つのアラートに結合
- 脅威情報には Storyline™ ID が含まれており
  それを使用して関連するプロセス、ファイル、
  スレッド、イベントなどを迅速に確認可能
- Storyline™ はリアルタイムで継続的に更新され
  常に最新のテレメトリデータが取り込まれる
  ことで活動の完全なストーリーを可視化
- Storyline™ を使用することで、エンドポイント上
  で何が起こったのか容易に理解することが可能

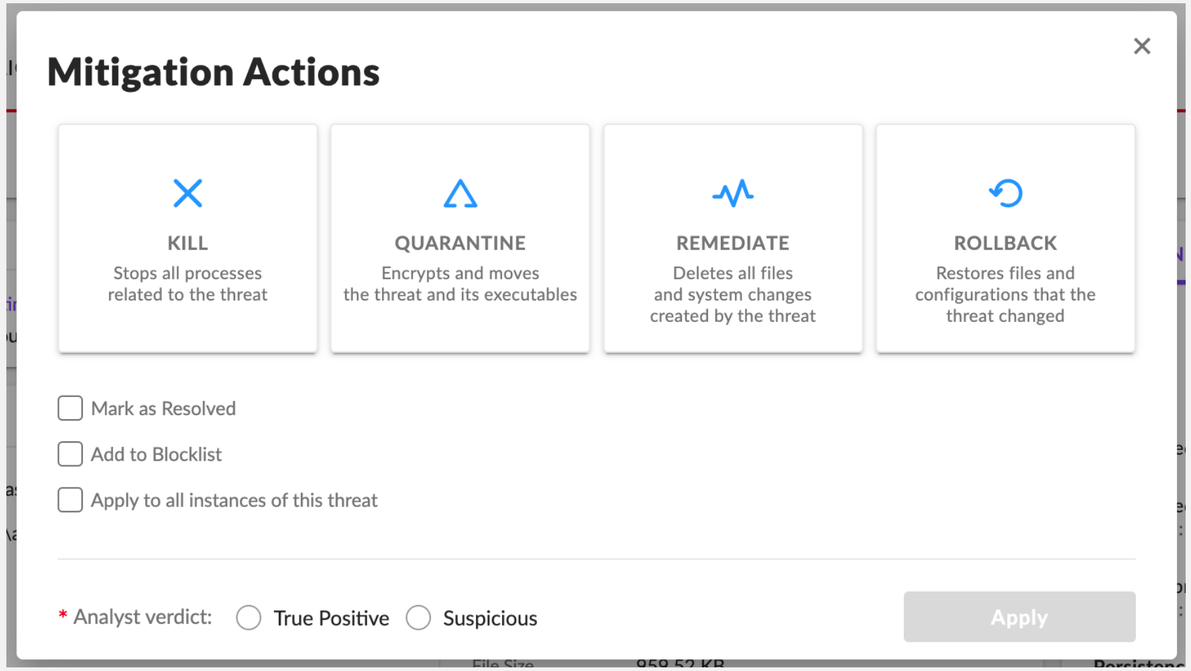


ワンクリックで修復・復旧

ランサムウェアやマルウェアなどの
不正プログラムによる攻撃で変更された
ファイルやシステム設定を攻撃前の状態へ
迅速に修復・復旧する機能を提供

主な特徴

- Windows OS の VSS（ボリュームシャドーコピーサービス）の スナップショットを利用した復元プロセスを実行
- SentinelOne のエージェントによってローカルデータベースに記録された不正プログラムの行為に基づいて、攻撃により変更されたファイル、レジストリやシステム構成のみを修復・復旧します。
- 自動での修復・復旧の設定も可能
- 攻撃検出後の即時対応によるビジネスのダウンタイム最小化を実現

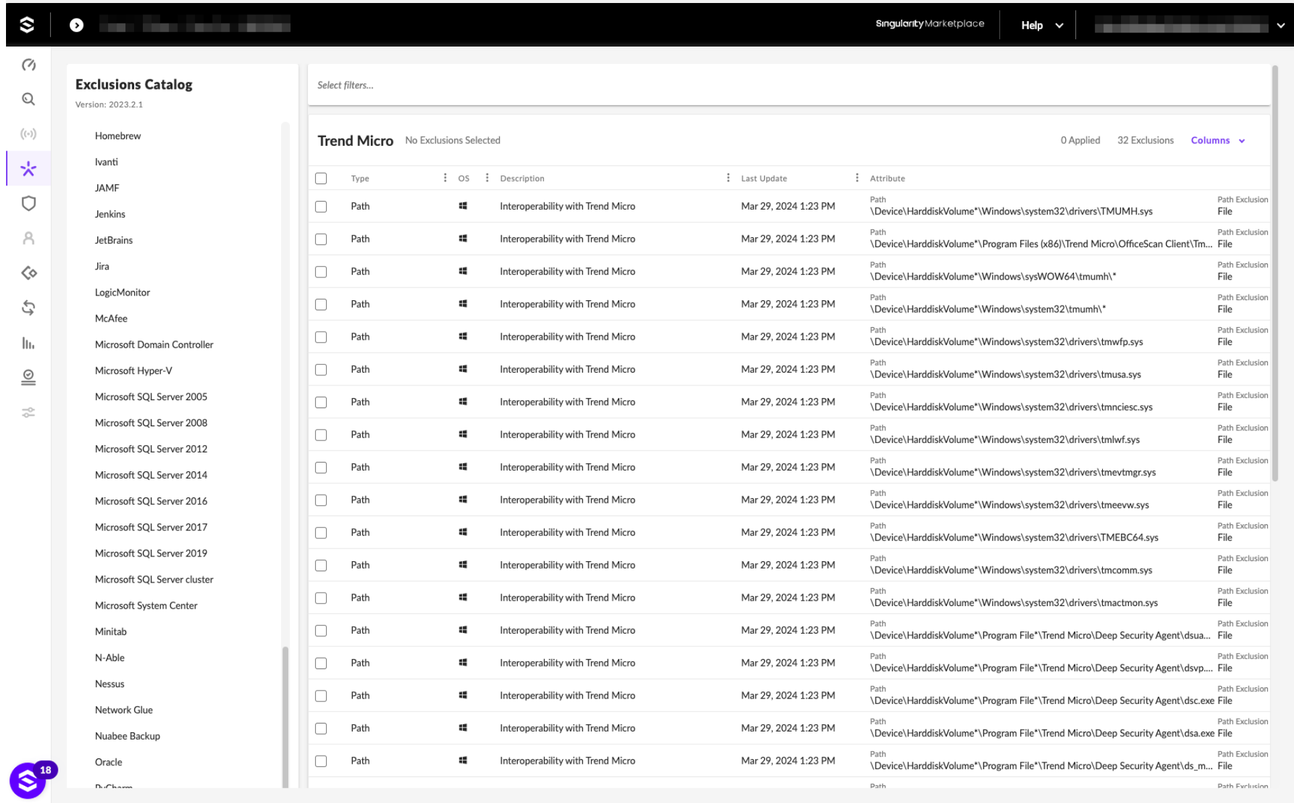


ブロックリスト・
除外リストの登録

脅威として検知したいファイルの
ブロックリストへの登録や
過検知となったファイルの除外リスト
への登録により検出精度の調整が可能

主な特徴

- 検知された脅威からワンクリックでブロックリストや除外リストへの登録が可能
- ブロックリストはハッシュ値で登録
- 除外リストはハッシュ値、ファイルパス、証明書に加えて WindowsOS ではファイルタイプやブラウザによる除外が可能
- SentinelOne が提供するアプリケーションのカタログから除外設定の選択が可能
- 登録前に、記録されているログやイベントから登録した場合の影響を確認可能



エージェント未導入端末の可視化

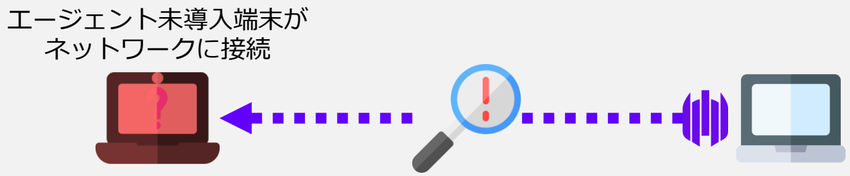
端末に導入されたエージェントが
ネットワークスキャナとして
ローカルサブネットのスキャンを実行し
まだエージェントが導入されていない
ネットワーク上の端末を可視化

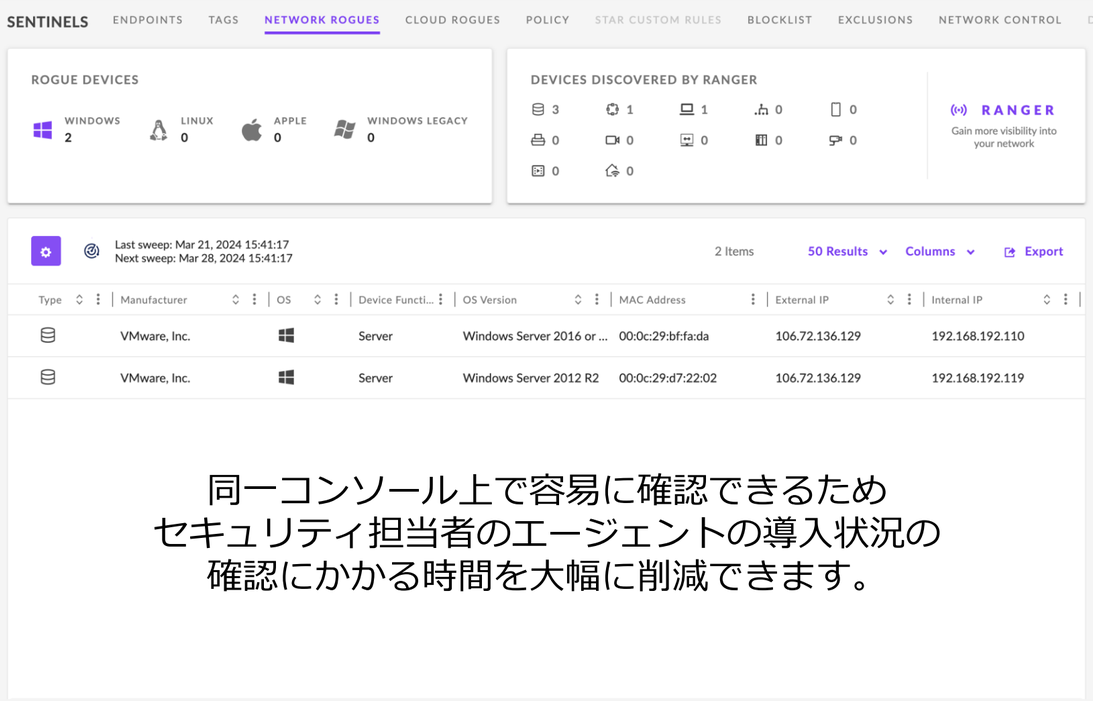
主な特徴

- 週に1回自動でスキャンを実施
- スキャンした結果、購入したライセンスの範囲内で、エージェントの導入が可能でかつ未導入の端末を一覧表示
- 一つのコンソール上でエージェントの導入状況の確認が可能

IIM

Singularity Core



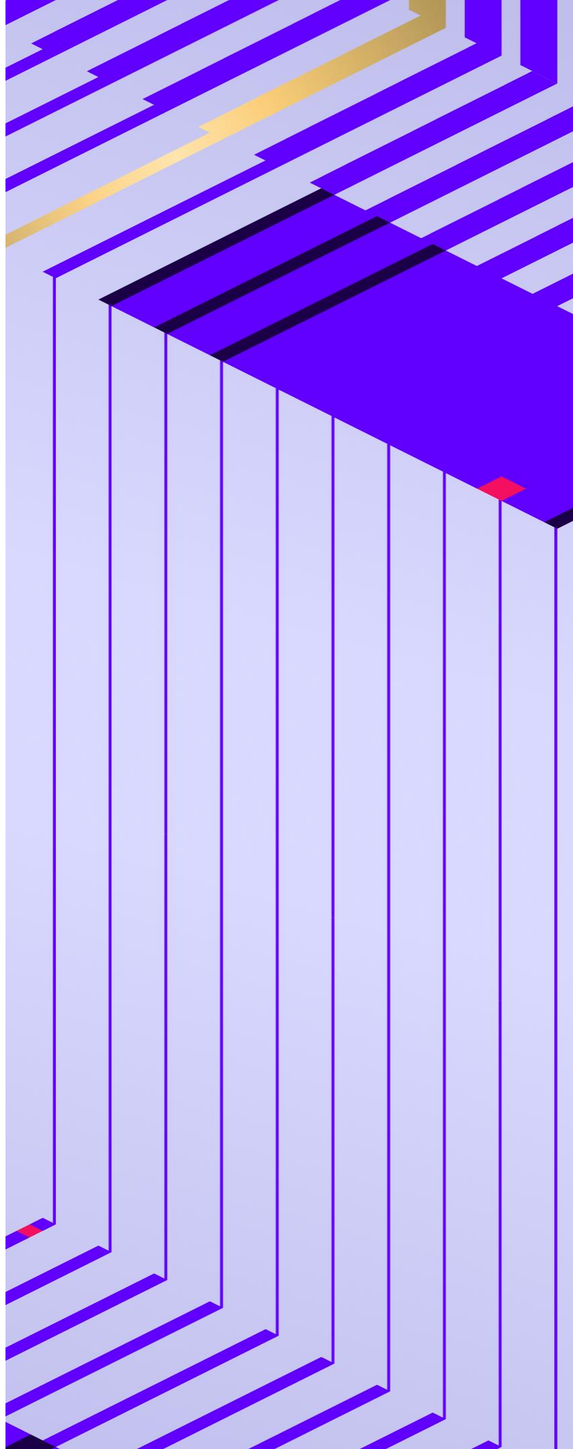


同一コンソール上で容易に確認できるため
セキュリティ担当者のエージェントの導入状況の
確認にかかる時間を大幅に削減できます。

さらにアドオン製品「Singularity Ranger」を追加することで IoTデバイスなど
ネットワーク上に接続されている全ての IP デバイスの表示や
エージェントのリモート展開等が実施できます。

SEIKO GROUP

Singularity Control のご紹介

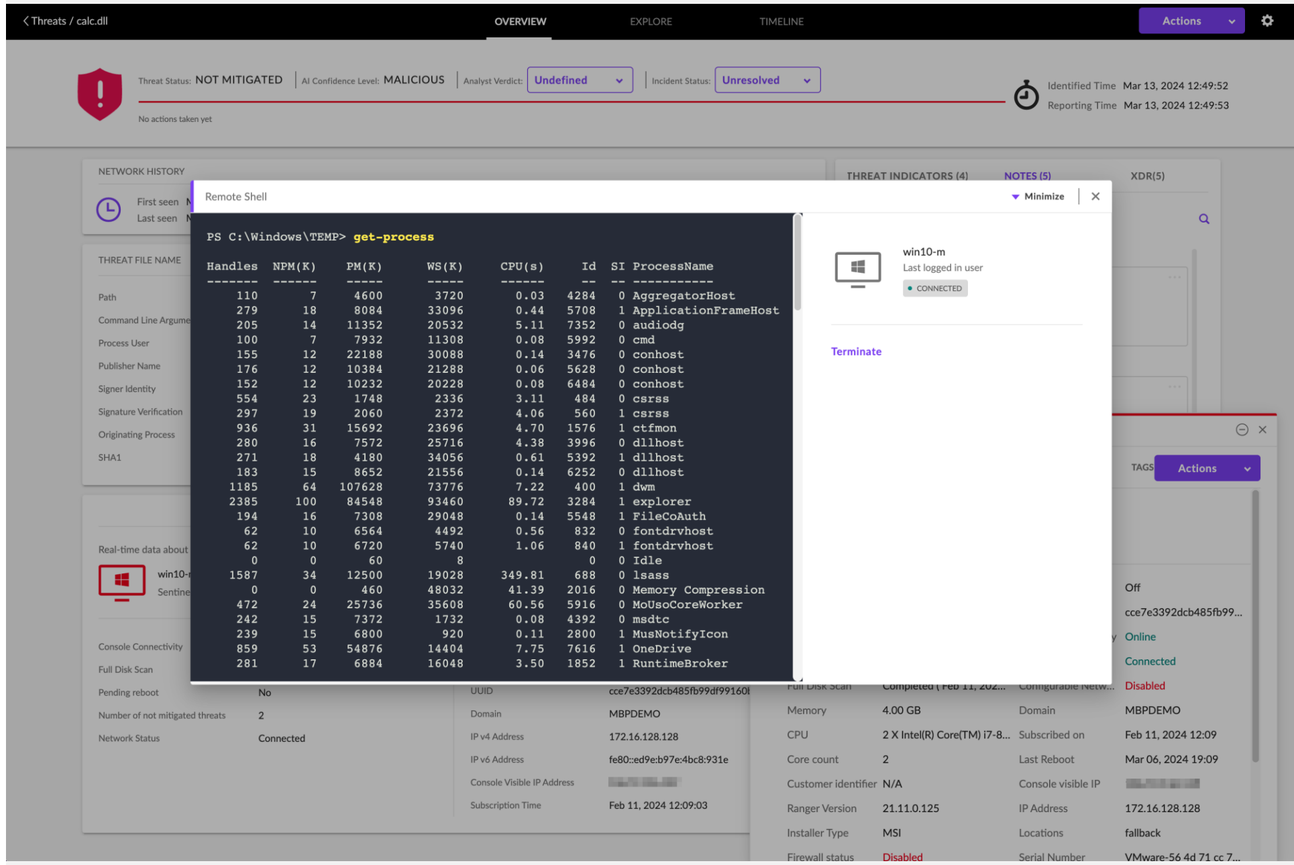


リモートシェルによるインシデント対応

管理コンソール経由でのエンドポイントへのリモートによるシェルアクセスにより迅速なセキュリティインシデントの調査や対応を実行

主な特徴

- 管理コンソール経由でのリモートからのコマンド実行
- セキュリティインシデントの迅速な調査
- エンドポイントの詳細情報の取得
- ネットワーク接続状態の確認
- ローカルユーザーアカウントの管理、など



USB・Bluetooth のデバイス制御

組織内のエンドポイントで使用する
USBのメモリやハードディスクなどの
外部デバイスや Bluetooth による
接続の制御を実現

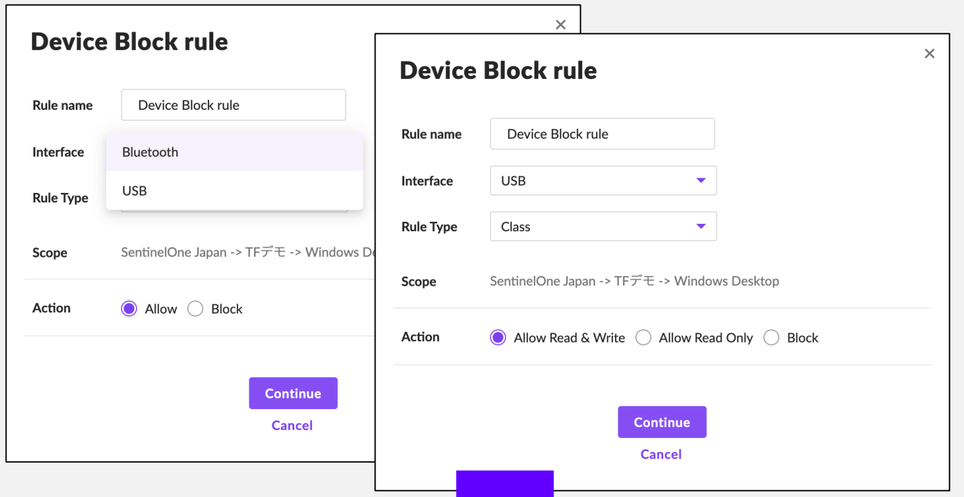
主な特徴

- エンドポイントへの不要な外部デバイスの制御により情報漏えいを防止
- 組織として認められたデバイスの接続を許可
- 端末に接続された USB マスストレージデバイス、および Bluetooth デバイスの管理が可能
- USB の場合は、読み取り専用許可の設定も可能

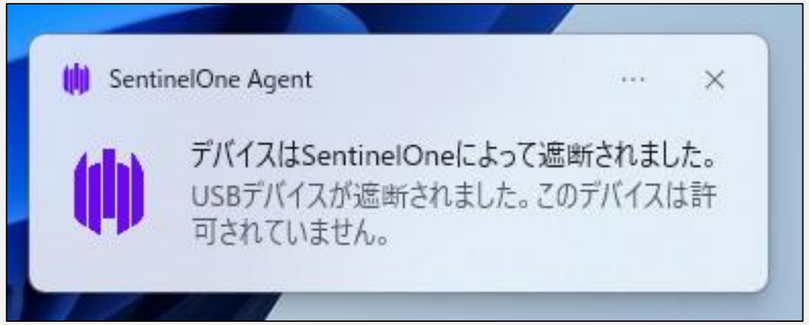
IIM

Singularity Control

USB（全て許可・読み取りのみ許可・全て禁止）
および Bluetooth デバイス（許可・禁止）
の制御ポリシーの作成が可能



組織として認められていないデバイスが接続された場合はブロック



SEIKO GROUP

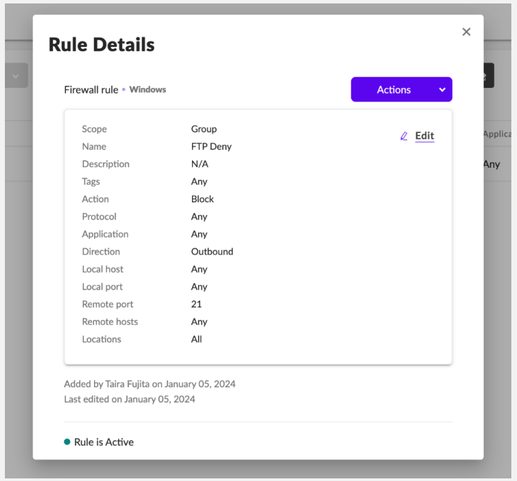
端末のファイアウォールポリシーの管理

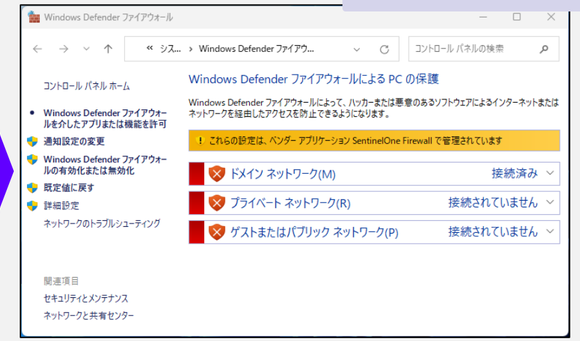
特定のアプリケーションによる接続の
許可またはブロックポリシーの設定により
組織で認められていないアプリケーション
による情報漏えいを防御

主な特徴

- OS に搭載されているファイアウォール機能を活用することで消費リソースを抑制したネットワーク制御を実現
- ポリシーに基づいた集中管理によりインバウンドおよびアウトバウンドの効果的なトラフィックコントロールを実現
- 付与された IP アドレスや定義された 名前解決可能なDNS サーバ、有線または無線ネットワークなどネットワーク状況に応じたポリシー設定が可能

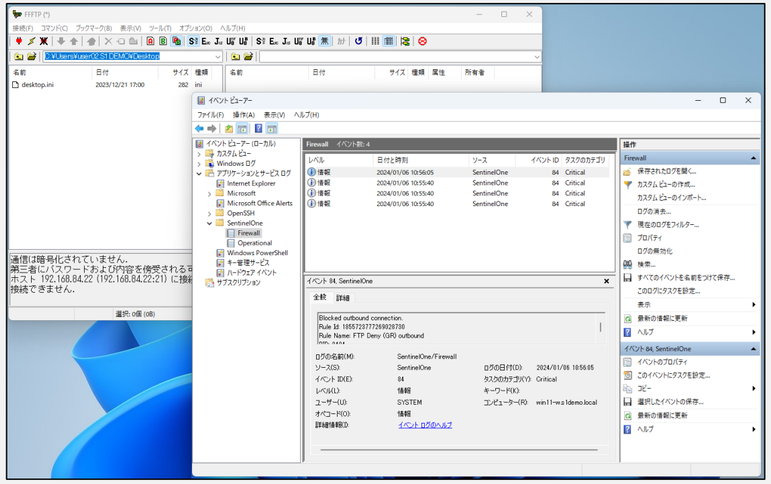
端末のファイアウォールポリシーを
SentinelOne の管理コンソールから設定





ファイアウォールポリシーにて
許可されていないアプリケーション
による通信をブロック

FTPによる
接続をブロック



外部からの不正
侵入による水平
展開や外部への
情報の不正持ち
出しから防御

アプリケーションインベントリおよび脆弱性の可視化

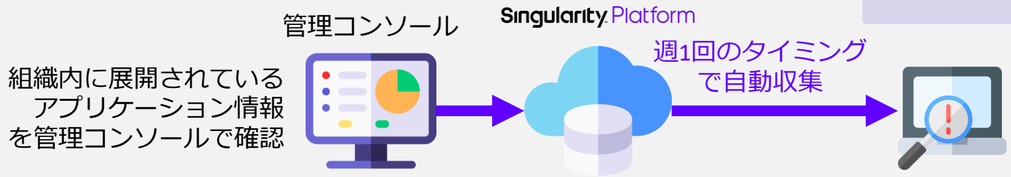
アプリケーションに関連するリスクに
関係なく、環境内のエンドポイント上で
実行されているサードパーティ
アプリケーションを検出し表示

主な特徴

- エージェントによって検出された
  エンドポイントに導入されているアプリ
  ケーションをリストアップ
- アプリケーション名、ベンダー名、
  異なるバージョンが存在する場合のその数、
  アプリケーションが導入されているエンド
  ポイントの数を集計
- グループ毎、OS毎や、アプリケーションの
  バージョン毎のフィルタリングによる表示
  が可能

IIM

Singularity Control



組織に導入されているアプリケーションの一覧を表示
アプリケーション名をクリックすることでそのアプリケーションが
導入されている端末の所属するサイトやグループ等が確認可能

APPLICATION MANAGEMENT　RISKS　INVENTORY　POLICY

Select filters...

Actions

Last Scanned　Feb 1, 2024 4:23 AM
Next Scan　Feb 8, 2024 2:30 AM

Name	Vendor	Number Of Versions	Number Of Endpoints
MSXML	Microsoft	3	1777
.NET Framework	Microsoft	6	1228
Sentinel Agent	Sentinel Labs, Inc.	39	1157
Google Chrome	Google LLC	90	1041
Microsoft Edge WebView2 Runtim	Microsoft Corporation	57	895

アプリケーションのバージョンや、アプリケーションがインストール
されている OSの種類等でフィルタリング表示も可能

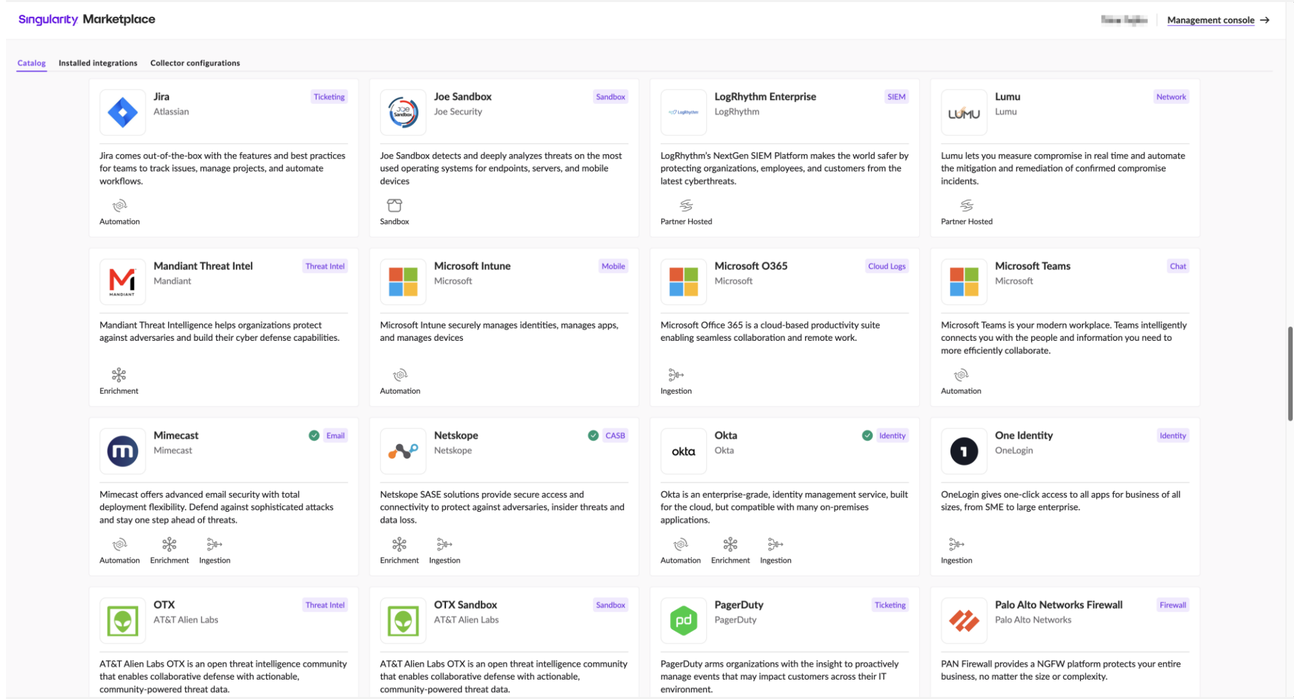
SEIKO GROUP

Singularity Marketplace
アプリケーションによる連携

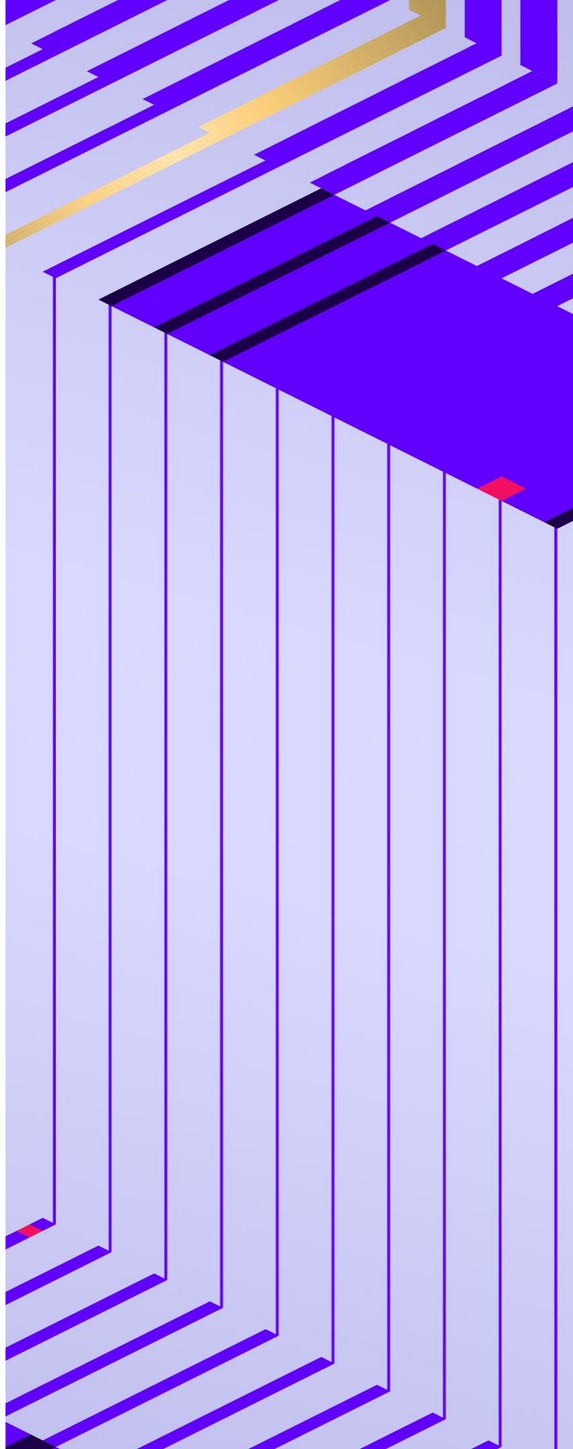
SentinelOne の統合型セキュリティ
プラットフォーム内において、簡単に
サードパーティ製品との連携が開始
できるアプリケーションを公開

主な特徴

- 複数のサードパーティセキュリティ製品の
  データソースの統合を容易に実現
- インシデント対応の自動化により soc チーム
  の作業負荷を軽減
- 脅威インテリジェンスの統合により
  迅速な検出と対応を実現
- 外部サンドボックスとの連携により
  検知されたマルウェアの動的診断を実現



Singularity Complete のご紹介



Singularity Endpoint における保護機能の特徴

IIM
Singularity Complete

EPP（エンドポイント保護プラットフォーム）

EDR（エンドポイント検知・対応）

リアルタイム ファイル分析

AI による静的
ファイル構造解析

リアルタイム 行動分析

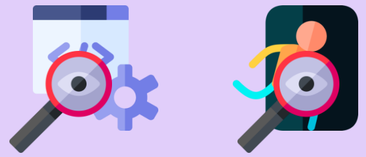
AI による動的
プロセス振る舞い解析

自動または 1クリックでの回復

- プロセスの停止と隔離
- ネットワークの切断
- 不正行為によるシステム変更やファイル生成からの修復
- ランサムウェアによる暗号化からのロールバック

高い可視性と 迅速な対応

- 単一の脅威に関連するプロセスを自動的に関連付け・可視化
- MITRE ATT&CK TTPへの自動マッピング
- 管理コンソール経由でのインシデント対応
- ユーザーが作成したカスタムルールでの検知

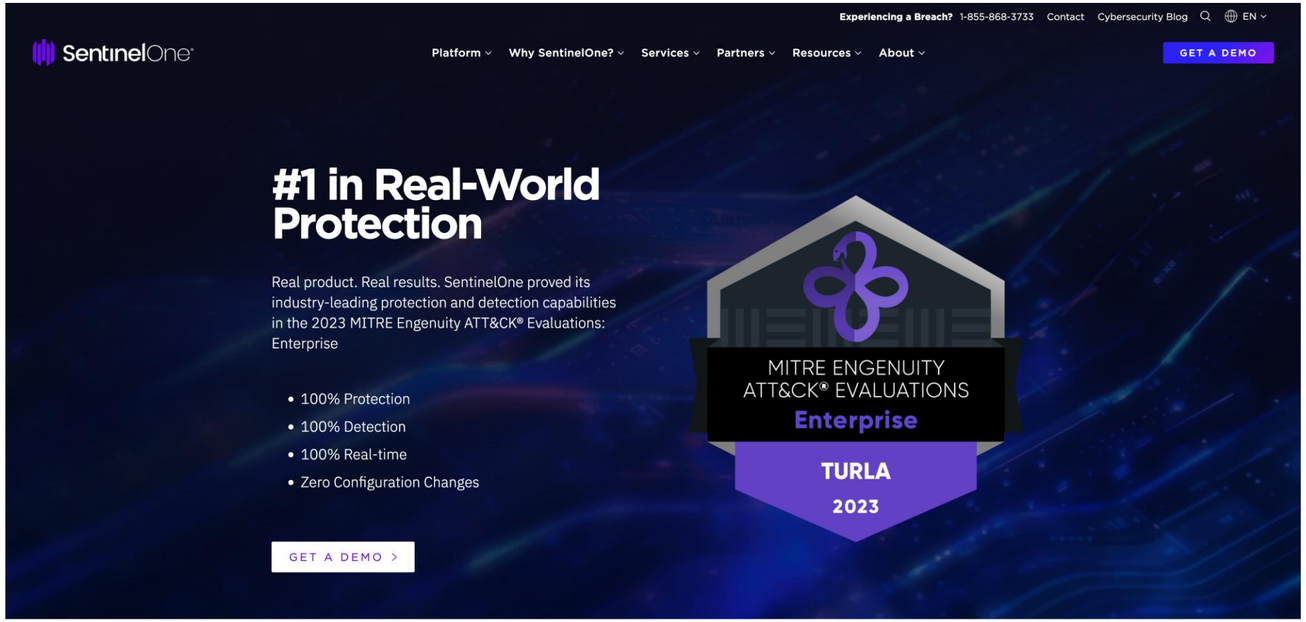


クラウド上に保存されたイベントから 過去に遡ってのインシデント対応が可能

SEIKO GROUP

2023 MITRE Engenuity ATT&CK Evaluation における評価

IIM
Singularity Complete



Webinar: Decoding the 5th Round of Results from MITRE Engenuity ATT&CK Evaluation.

Learn the details and results from the latest MITRE Engenuity ATT&CK Evaluation covering the adversary Turla. The webinar goes into the details of:

https://www.sentinelone.com/lp/mitre/

100%
保護

13件中13件の悪意ある
アクティビティを検知

100%
検出

18の攻撃ステップのうち
18すべての脅威を検知

100%
リアルタイム

包括的かつ統合されたビュー
により遅延なく脅威を検出

0回
設定変更

お客様が利用している一般的な
構成から変更なしでテスト

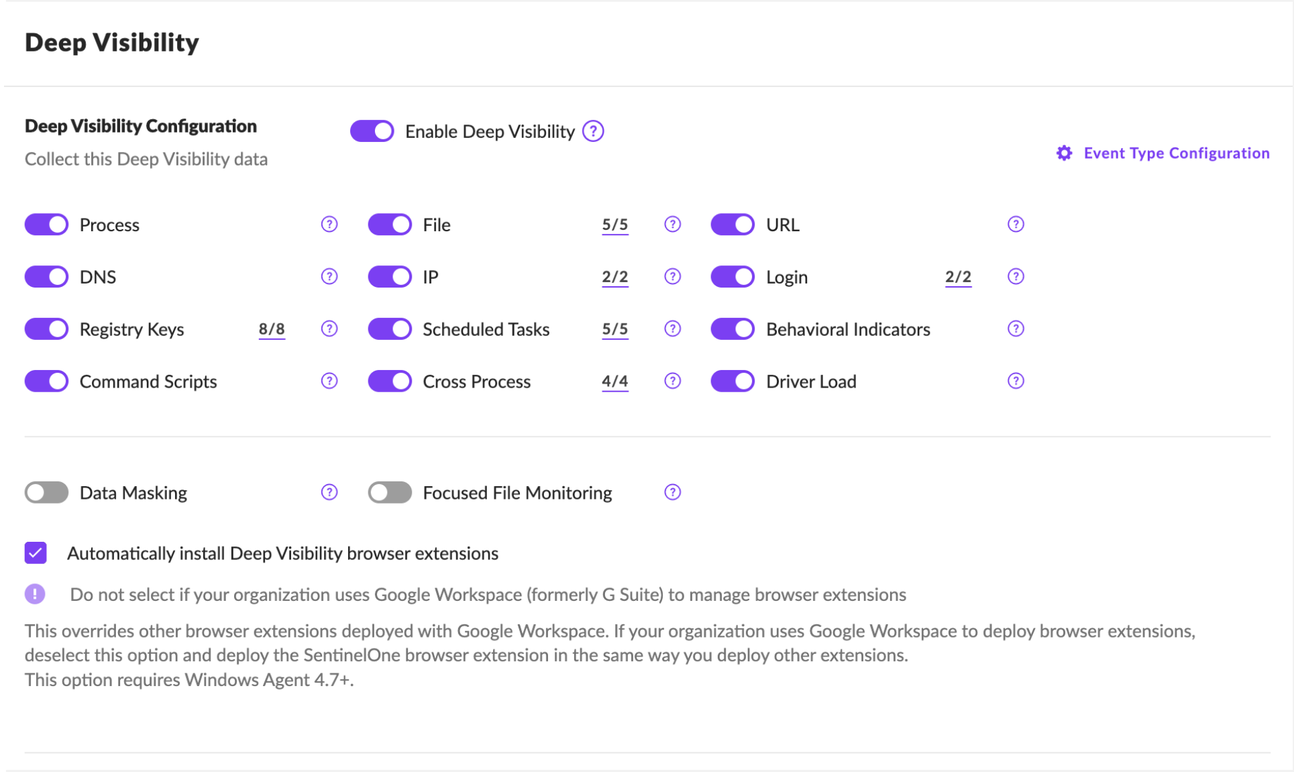
SEIKO GROUP

Deep Visibility™ による可視化

エンドポイント上のアクティビティを
カーネルレベルで監視し、脅威ハンティングや
インシデントの原因分析に必要な情報を
クラウド上に集約・可視化

主な特徴

- プロセス、ファイル関連イベント、
  ネットワーク接続などさまざまな種類の
  イベントをキャプチャしログに記録
- ユーザーのポリシー設定により特定の
  種類のデータのみ収集するよう構成可能
- Deep Visibility™ によって収集されたデータは
  Storylines™ テクノロジーによって自動的・
  継続的にイベントを関連付け
- ユーザーにて作成したクエリにより効率的
  な脅威ハンティングを実現



端末上のアクティビティ情報をリアルタイムで収集

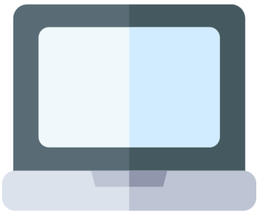
IIM
Singularity Complete

Singularity Platform
セキュリティデータレイク

データ保持期間：14日間
（オプションで最大1年
間まで保持可能）

収集されたアクティビティ情報を
1分毎にアップロード
通信量（平均）：約20MB/日(※)

Singularity
Complete



オフライン時も
一定量を保持し
再接続時にまとめて
データを送付

収集する主なアクテビティ情報

プロセス アクティビティ	ファイル操作	ユーザーアカウント アクティビティ	ネットワーク アクテビティ	レジストリ アクティビティ	スケジュールされた タスク
• プロセスの作成 • プロセスの終了 • プロセスへのアクセス • イメージ/ライブラリのロード • リモートスレッドの作成 • プロセス改ざん活動	• ファイルの作成 • ファイルがオープン • ファイルの削除 • ファイルの変更 • ファイル名の変更	• ローカルアカウントの作成 • ローカルアカウントの変更 • ローカルアカウントの削除 • アカウントのログイン • アカウントのログオフ	• TCP 接続 • UDP 接続 • URL • DNS クエリ	• キー/値の作成 • キー/値の変更 • キー/値の削除	• スケジュールされたタスクの作成 • スケジュールされたタスクの変更 • スケジュールされたタスクの削除
サービス アクティビティ	**ドライバ/モジュール アクティビティ**	**デバイス操作**	**名前付きパイプ アクティビティ**	**WMI アクティビティ**	**Powershell アクティビティ**
• サービスの作成 • サービスの変更	• ドライバのロード • ドライバのアンロード	• 仮想ディスクのマウント • USB デバイスのマウント • USB デバイスのマウント解除	• 名前付きパイプの作成 • 名前付きパイプの接続	• WMIによる各種クエリ アクティビティ	• スクリプトブロックに関する アクティビティ

(※) エージェントが導入されている端末上で動作するアプリケーションやプロセスの数や処理内容により、これ以上のデータ量になる場合があります。

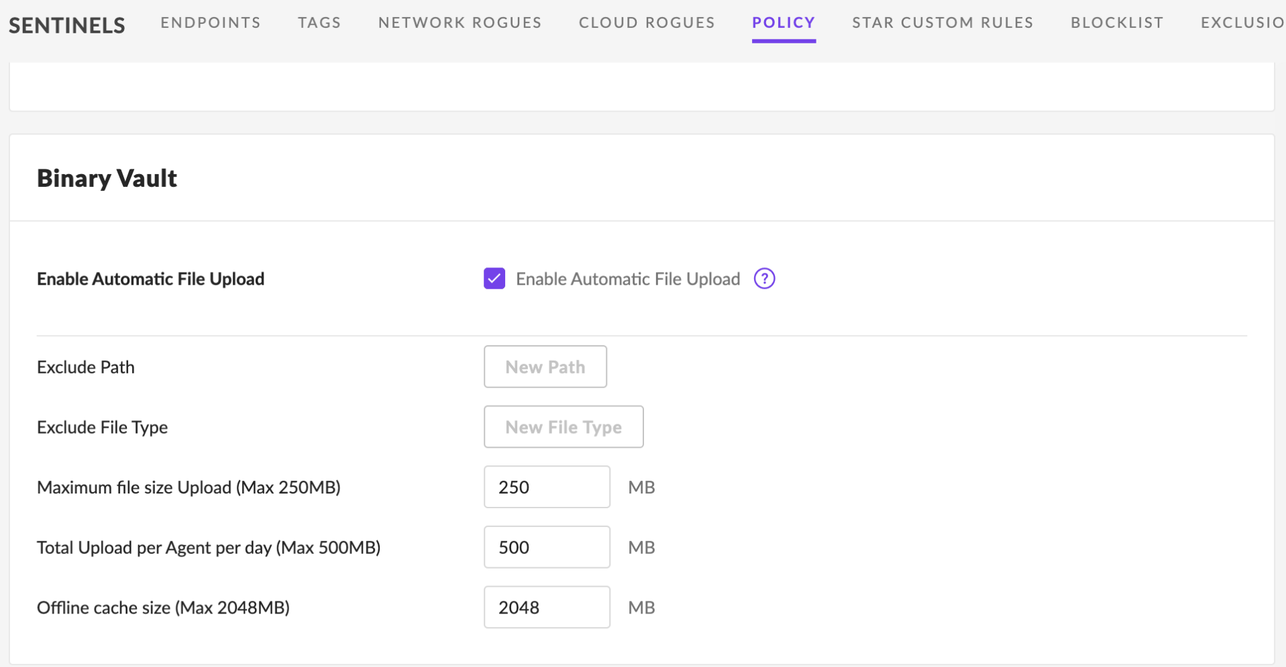
SEIKO GROUP

悪意のあるファイルの自動アップロード

実行可能ファイルを SentinelOne クラウドストレージに自動アップロード
管理コンソールからオンデマンドで
ダウンロード可能

主な特徴

- EPP で脅威として検知された実行可能ファイルを自動的にクラウドにアップロード
- 脅威として検知された実行可能ファイルは１年間保持
- 分析や検査のために管理コンソール経由でダウンロードが可能
- 特定のファイルタイプやファイルパスからのアップロードを除外するカスタマイズが可能

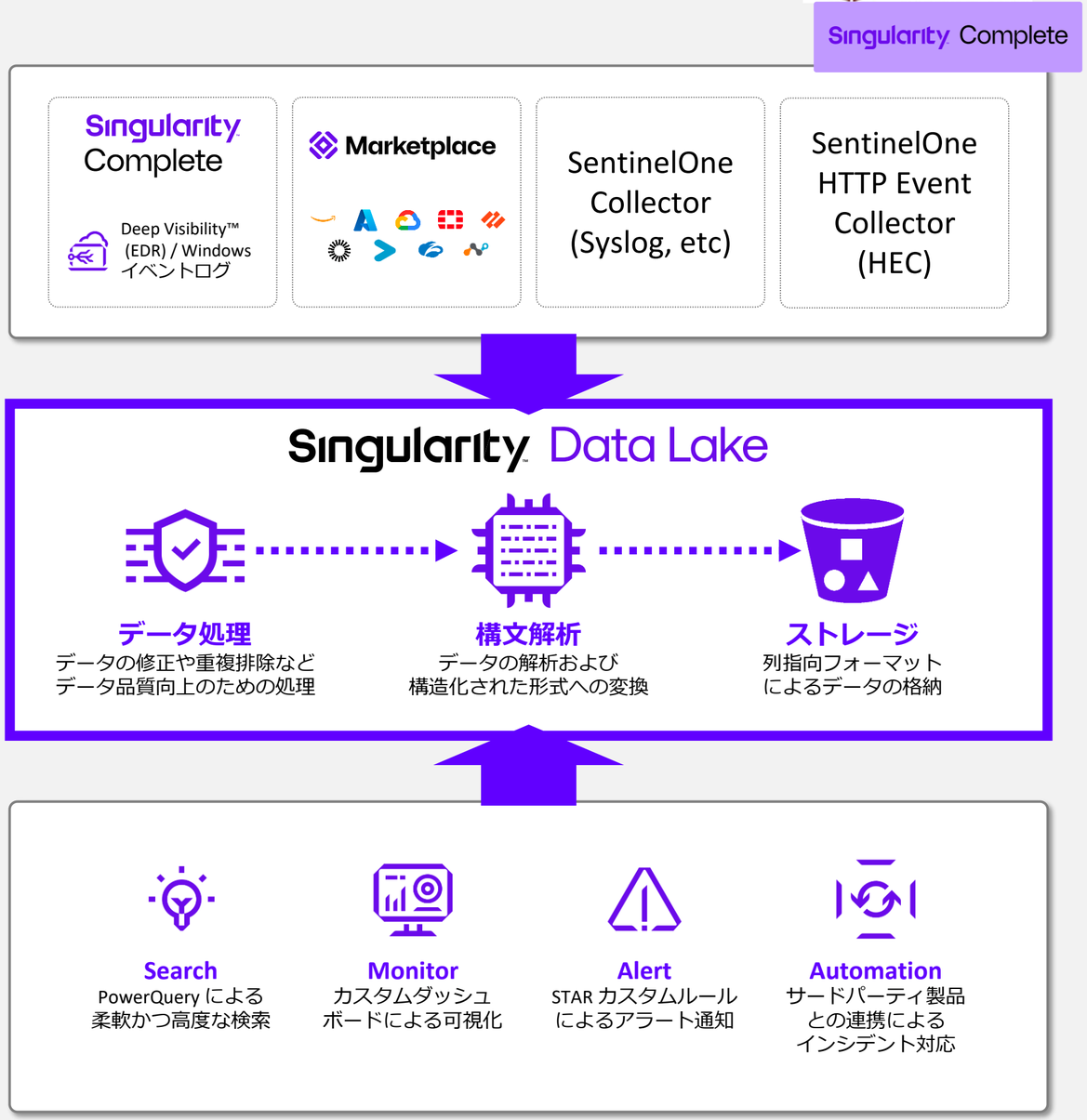


サードパーティの
イベントデータ集約

組織で記録される EDR、XDR、および
非セキュリティデータを一か所のクラウドの
データレイク上に集約し一つの
コンソールで簡単に可視化・検索・分析

主な特徴

- OCSF 対応のコネクタを Singularity Marketplace から利用することで容易にサードパーティデータの取り込みが可能
- 特許取得済みのクエリエンジンにより検出および応答時間の大幅な高速化を実現
- データレイクがクラウド上にあるため運用上のオーバーヘッドを与えることなくオンデマンドで柔軟に拡張可能
- 標準で14日間のデータを保存
（オプションで最大1年間まで保持可能）

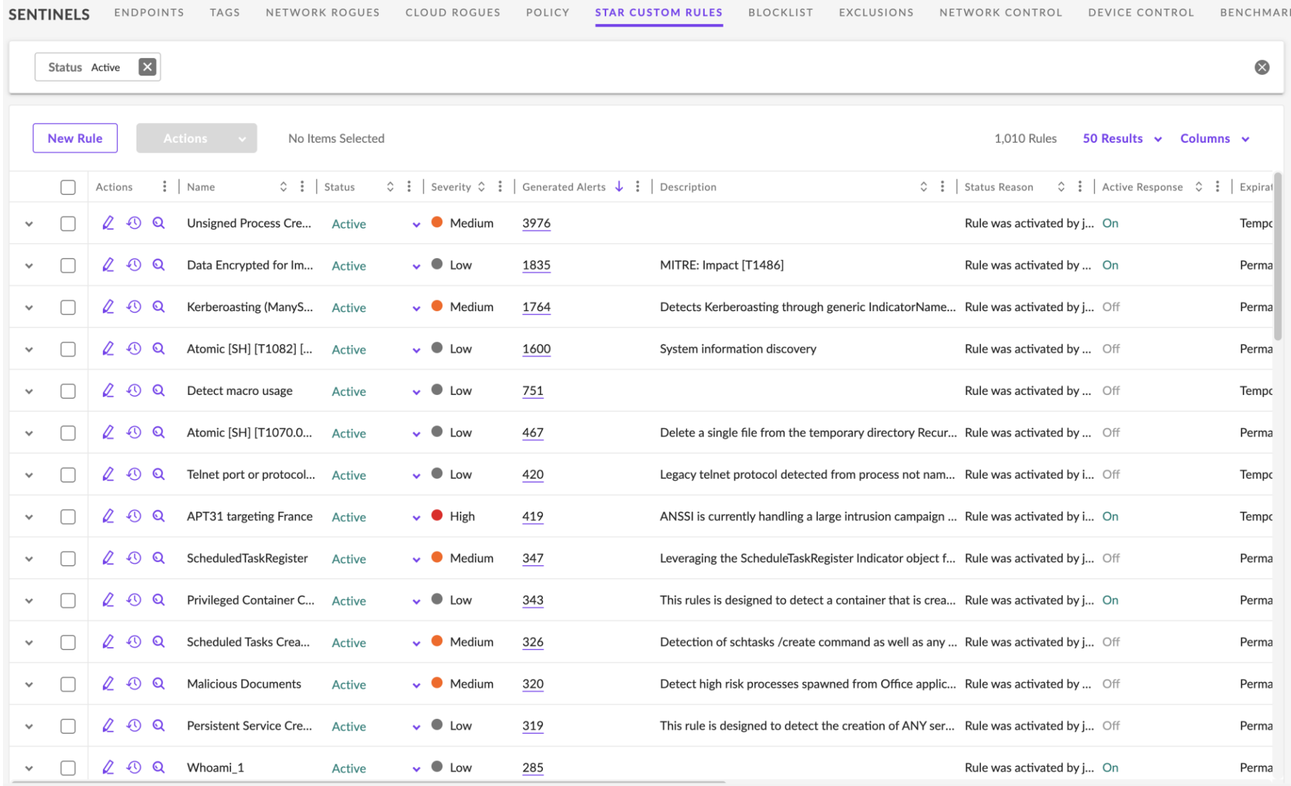


カスタムルールによる検知

Deep Visibility™ や Singularity Data Lake の
検索クエリ文を自動化された
脅威ハンティングルールに変換

主な特徴

- 変換された脅威ハンティングルールに
  マッチしたイベントが検知された場合
  アラートやネットワーク隔離などの
  自動対応を実行
- ルール毎に、アラートのみ通知するか
  または自動対応を実行するかの選択が可能
- 各アカウントで最大100のActiveな
  カスタムルールの作成が可能
  （追加のルールセットを購入することで
  数量の拡張が可能）

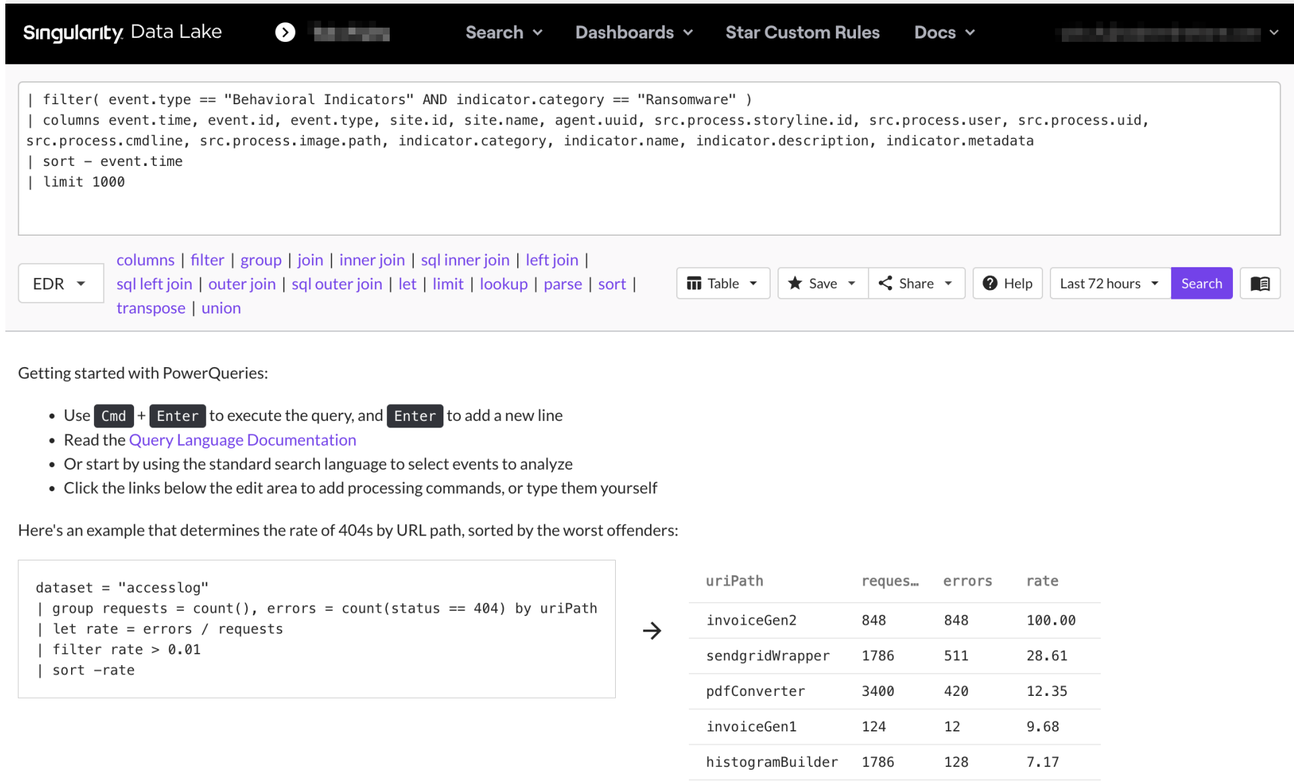


PowerQueries による高度な脅威ハンティング

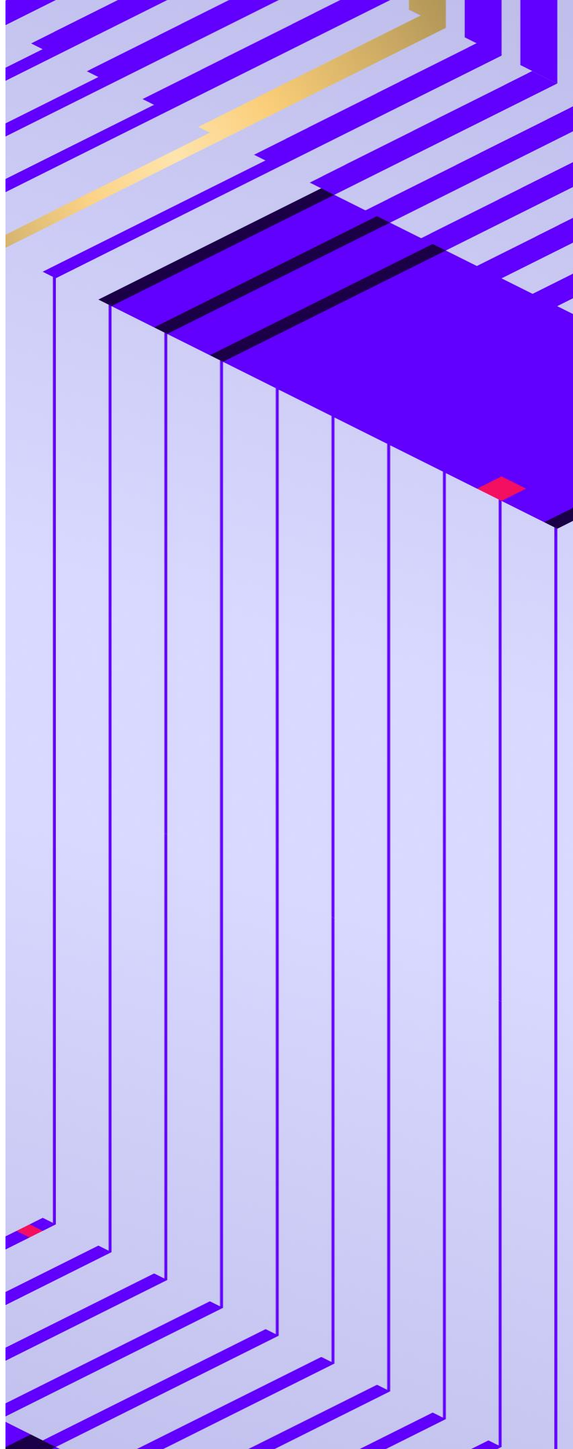
複数のコマンドやフィールド、セットを
使用してマルチラインクエリを
作成する高度なツールを提供

主な特徴

- 複雑なデータセットに対する高度なクエリ実行が可能
- 複数のコマンドを組み合わせることで柔軟なデータ抽出が可能
- PowerQueries のクエリ文を STAR カスタムルールのクエリ文として利用可能



Singularity Endpoint
ライセンスと機能の一覧



Singularity Endpoint ライセンスと機能

主な機能	Singularity Endpoint		
	Singularity Core	Singularity Control	Singularity Complete
マルチテナント対応の統合コンソール	✓	✓	✓
自律型 AI によるエンドポイント保護（EPP）	✓	✓	✓
検知時のファイル隔離・ネットワーク隔離の自動対応	✓	✓	✓
Storyline™による脅威の可視化	✓	✓	✓
自動またはワンクリックによる修復および復旧	✓	✓	✓
エージェント未導入端末の可視化	✓	✓	✓
リモートシェルによるインシデント対応		✓	✓
USB・Bluetooth のデバイス制御		✓	✓
端末のファイアウォールポリシーの管理		✓	✓
アプリケーションのインベントリおよび脆弱性の可視化		✓	✓
Singularity Marketplace アプリケーションによる連携（XDR）		✓	✓
サードパーティのイベントデータの集約（XDR） （標準データ転送量：1日あたりの平均データ転送量 10GB まで）		✓	✓
Singularity Data Lake のデータ分析インターフェースの利用（XDR）			✓
Deep Visibility™ によるエンドポイントのアクティビティの可視化（EDR） （標準保持期間 14日間 – 別途オプションにより最大 1年間まで延長可能）			✓
悪意あるファイルの自動アップロード			✓
カスタムルールによる検知			✓
PowerQueries による高度な脅威ハンティング			✓

Singularity Endpoint ライセンスと機能

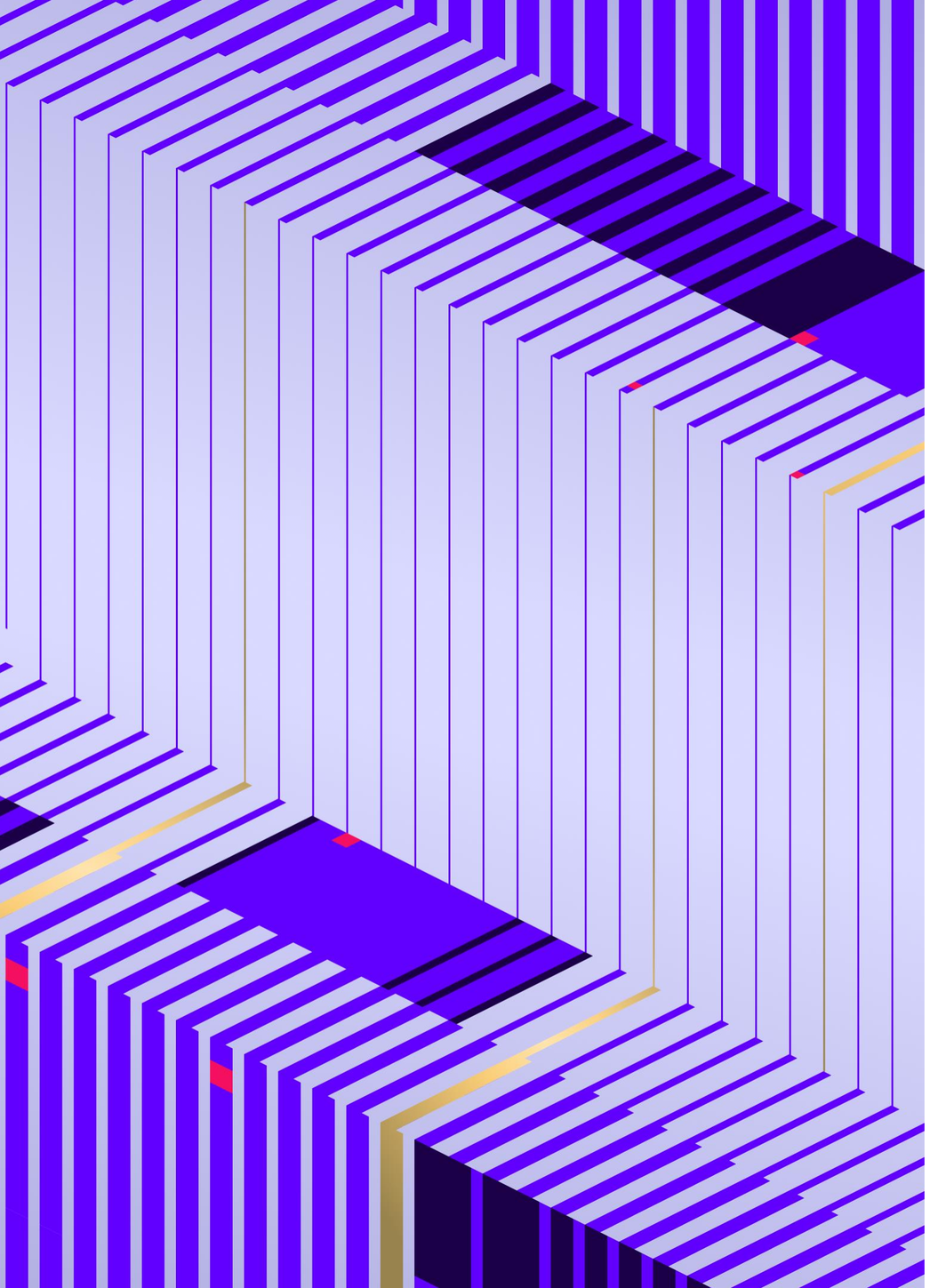
CSF 2.0 6つの主要な機能 / Singularity Endpoint ライセンス	ガバナンス	識別	保護	検知	対応	回復
Singularity Core	マルチテナント対応の統合コンソール	エージェント未導入端末の可視化	自律型 AI によるエンドポイント保護（EPP）	Storyline™による脅威の可視化	検知時のファイル隔離・ネットワーク隔離の自動対応	自動またはワンクリックによる修復および復旧
Singularity Control		アプリケーションのインベントリおよび脆弱性の可視化	USB・Bluetooth のデバイス制御 端末のファイアウォールポリシーの管理	Singularity Marketplace アプリケーションによる連携（XDR）	リモートシェルによるインシデント対応	
Singularity Complete				Deep Visibility™ によるエンドポイントのアクティビティの可視化（EDR） サードパーティのイベントデータの集約（XDR） カスタムルールによる検知	悪意あるファイルの自動アップロード Singularity Data Lake のデータ分析インターフェースの利用（XDR） PowerQueries による高度な脅威ハンティング	

Singularity Endpoint 対応 OS（2024年3月現在）

Windows OS	Windows 7 SP1 Windows 8 Windows 8.1 Windows 10 Windows 11 Windows Server 2008 R2 SP1 Windows Server/Storage Server/Server Core 2012 Windows Server/Storage Server 2012 R2 Windows Server/Storage Server/Server Core 2016 Windows Server/Server Core 2019 Windows Server/Storage Server 2022
Mac OS	Monterey 12.0 – 12.7.4 Ventura 13.0 – 13.6.5 Sonoma 14.0 – 14.4

Linux OS	CentOS 8.4 - 8.0, 7.9 - 7.0, 6.10 - 6.4 CentOS Stream v9 Red Hat Enterprise Linux (RHEL) 9.3, 9.2, 9.1, 9.0, 8.9, 8.8, 8.7- 8.0, 7.9 - 7.0, 6.10 - 6.4 Ubuntu 22.04.6, 22.04, 20.04, 18.04, 16.04, 14.04 Amazon Linux 2023.3, 2023.1, 2023 Amazon Linux 2, AMI 2018, AMI 2017 SUSE Linux Enterprise Server 15 sp5, 15.x, 12.x Debian 12.4, 12.2, 12.1, 12, 11.9, 11.8, 11.7, 11, 10.13, 10, 9, 8 Virtuozzo 7 Scientific Linux 7,6 Alma Linux 9.3, 9.2, 9.1, 9.0, 8.8, 8.7, 8.6, 8.5, 8.4 Rocky Linux 9.3, 9.2, 9.1, 9.0, 8.8, 8.7, 8.6, 8.5, 8.4 Oracle 9.3, 9.2, 9.1, 9.0, 8.8, 8.7-8.0, 7.9 - 7.0, 6.10 Fedora 39, 38, 37, 36, 35 Cloud Linux Shared v8, v6

※ 最新の対応状況および対応するディストリビューションのバージョンは、弊社 Knowledge Base に掲載しております。
ご購入前のお問い合わせにつきましては、販売パートナー様または弊社担当者までご相談ください。



株式会社 アイ・アイ・エム

Thank You