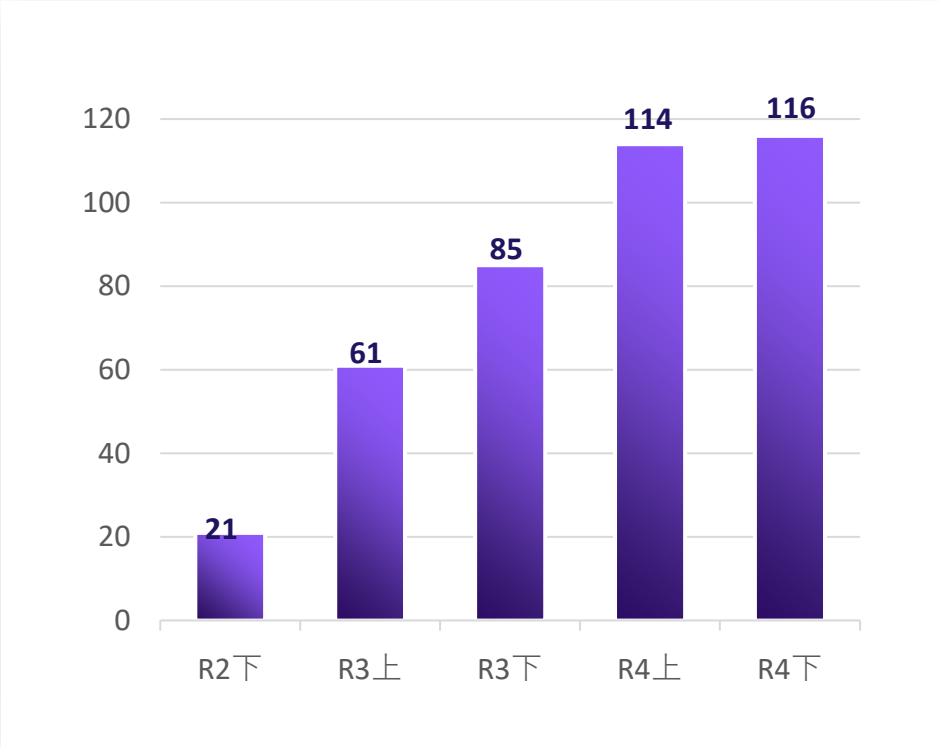
Ver. 1.2

SentinelOne™

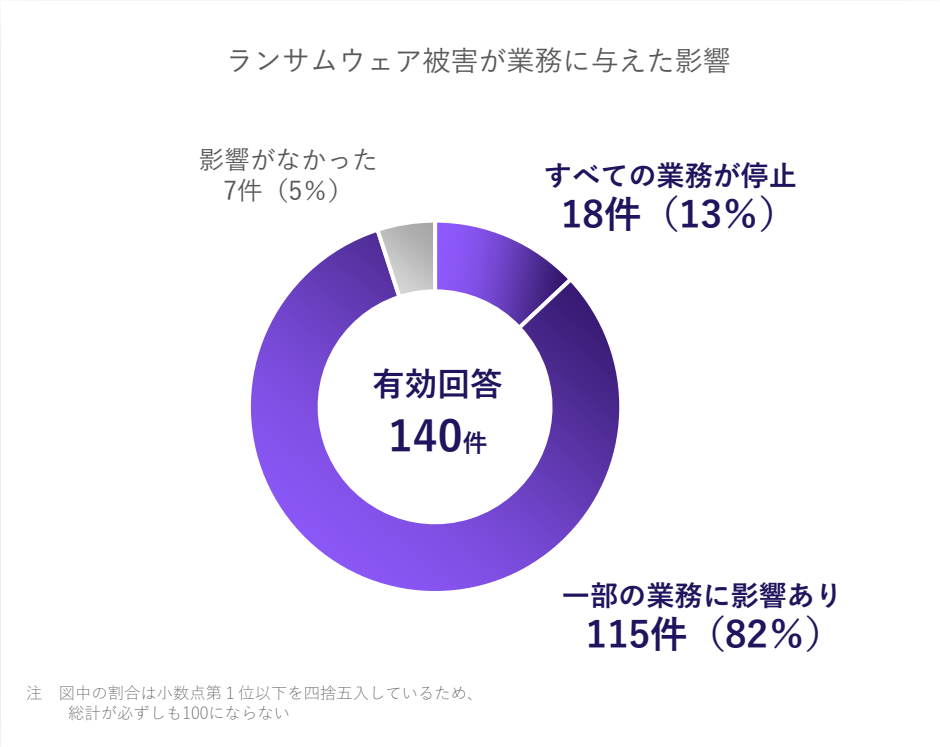
自律型EDR
SentinelOne

ランサムウェアの動向

ランサムウェア被害は２年で５倍に



95%の組織で業務に影響

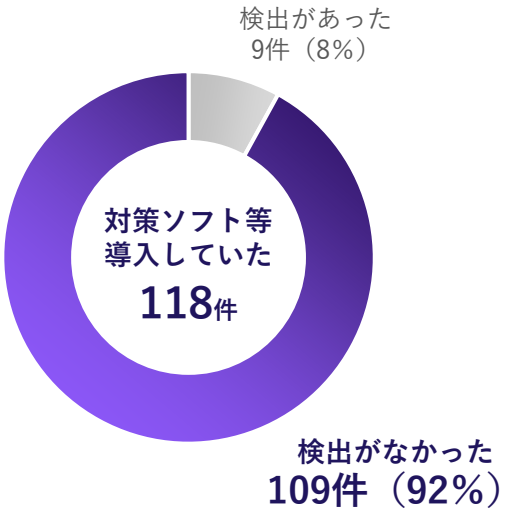


※出典 警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」

ウイルス対策ソフトでは阻止できない攻撃が増加

ランサムウェア被害組織の92%が ウイルス対策ソフトで検出がなかった

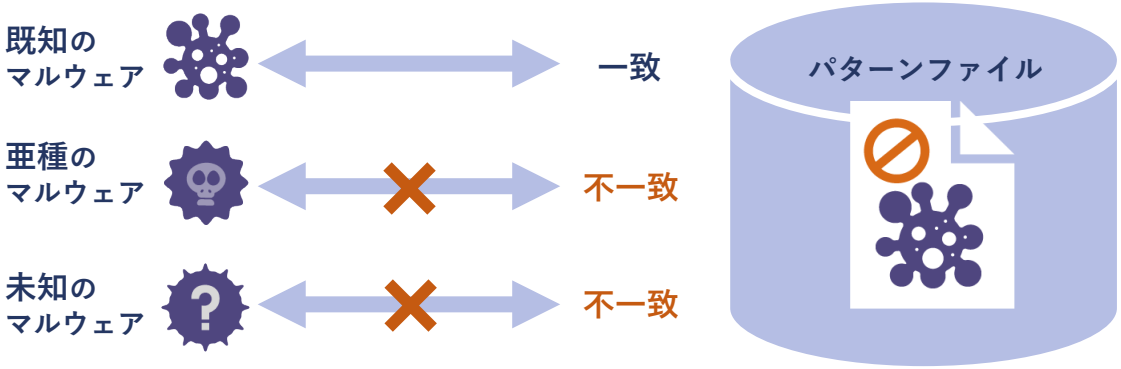
検出の有無



※出典 警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」

EPPの挙動と検出できない理由

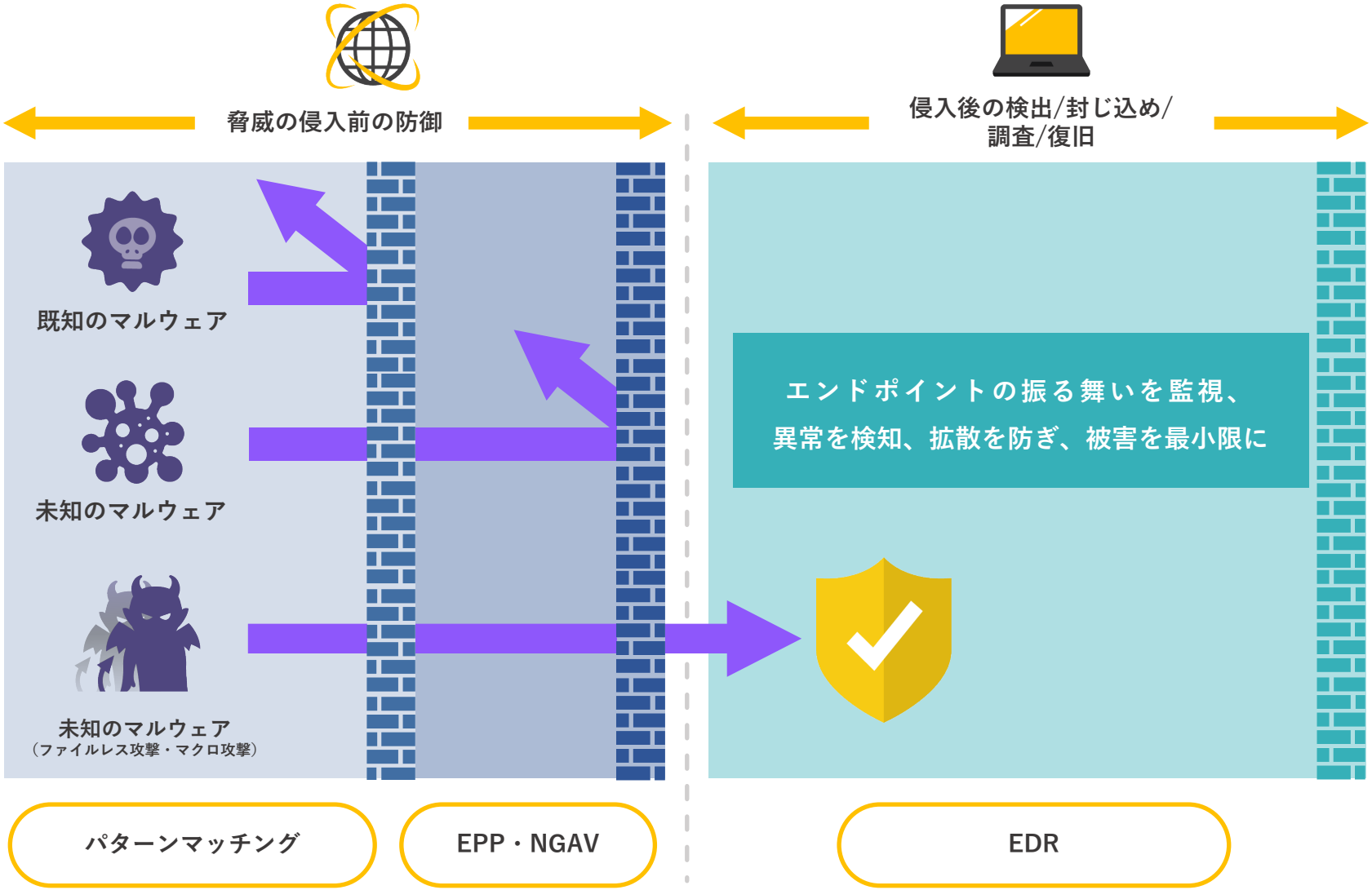
EPP（Endpoint Protection Platform）　侵入時に、実行ファイルにてパターンマッチングを行い検知



マルウェア（新種・亜種）は1日に100万個作成される
ランサムウェア（亜種）は、半年で1万個作成される

▶ パターンマッチングの仕組みでは追従できない

これからは、EDRの時代
従来のAVでは、感染拡大/Responseに対応できない



SentinelOne 企業概要

2,000 従業員数	8,000+ 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**	VIGLANCE 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
- **グローバルデータセンター**
  アメリカ、ドイツ、APAC、AWS GovCloud 高可用性
- **アジアパシフィック日本拠点**
  日本、韓国、シンガポール、オーストラリア、インド
- **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　Sam Burns

©2021 SentinelOne, All Rights Reserved.

主な導入実績

導入実績

McKESSON flex
jetBlue ASTON MARTIN
POLITICO NS NORFOLK SOUTHERN
AUTODESK
ESTĒE LAUDER
norwegian
havas FIMBANK

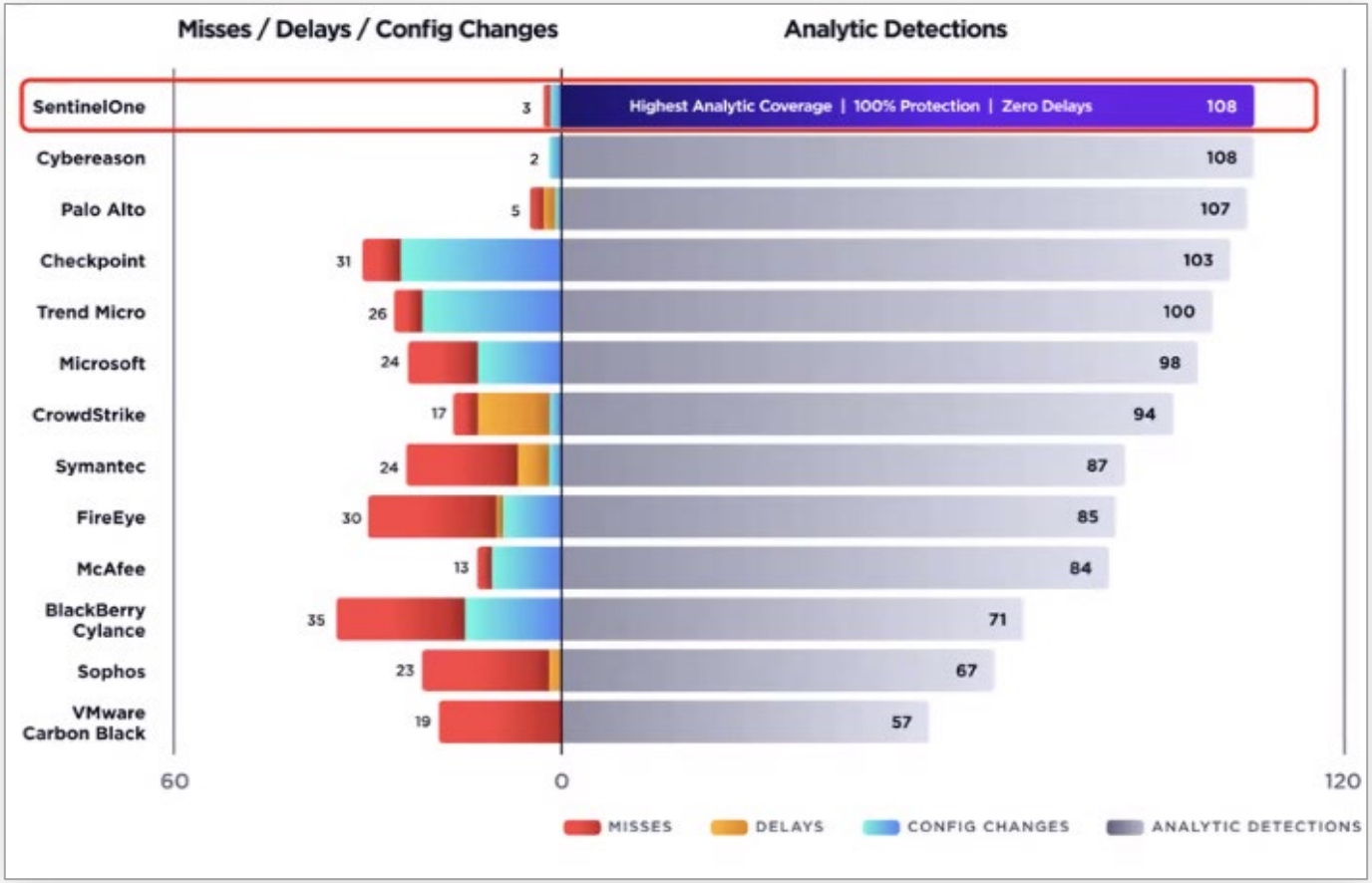
公開導入事例	業界	
SBSホールディングス	運輸	https://assets.sentinelone.com/c/sentinelone_sbs_fina_jp?x=u6040P
アンドパッド	IT	https://assets.sentinelone.com/c/sentinelone_andpad_jp?x=u6040P
駒沢大学	文教	https://www.ctc-g.co.jp/report/case-study/komazawa-u2/
オンデーズ	メガネ	https://cn.teldevice.co.jp/case/owndays/
株式会社ショクブン	食品	https://www.lenovojp.com/business/cmsimages/case/165/case_165.pdf
ビーグローバル	人材	https://www.sentinelone.to-tm.com/example/
株式会社R4	人材	
メディケアー	医療	

- その他国内1000社程度

Fortune誌 格付け上位10中3社で採用 製造 / 金融 / エネルギー

SentinelOneがLeaderに選出される（2023 Gartner Magic Quadrant）

2年連続で高い分析能力を証明（MITRE Engenuity ATT & CK® 評価結果）



100%の保護を達成

9種類のMITRE ATT＆CKテストのうち9種類

100%の検知を達成

19段階の攻撃ステップのうち19段階

100%リアルタイムの検知を達成

検知の遅延時間ゼロ

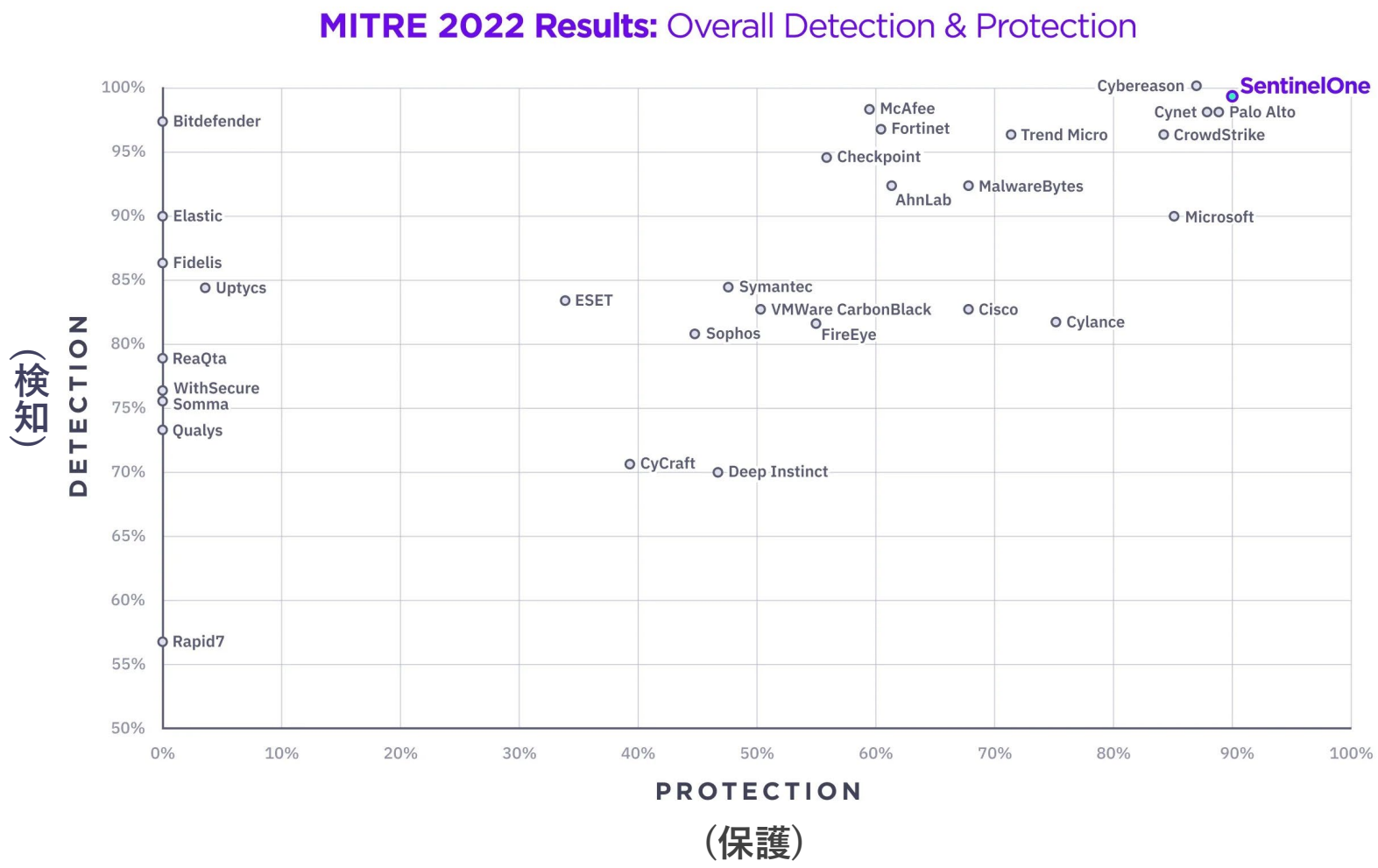
99%の可視性を達成

109段階の攻撃サブステップのうち108段階

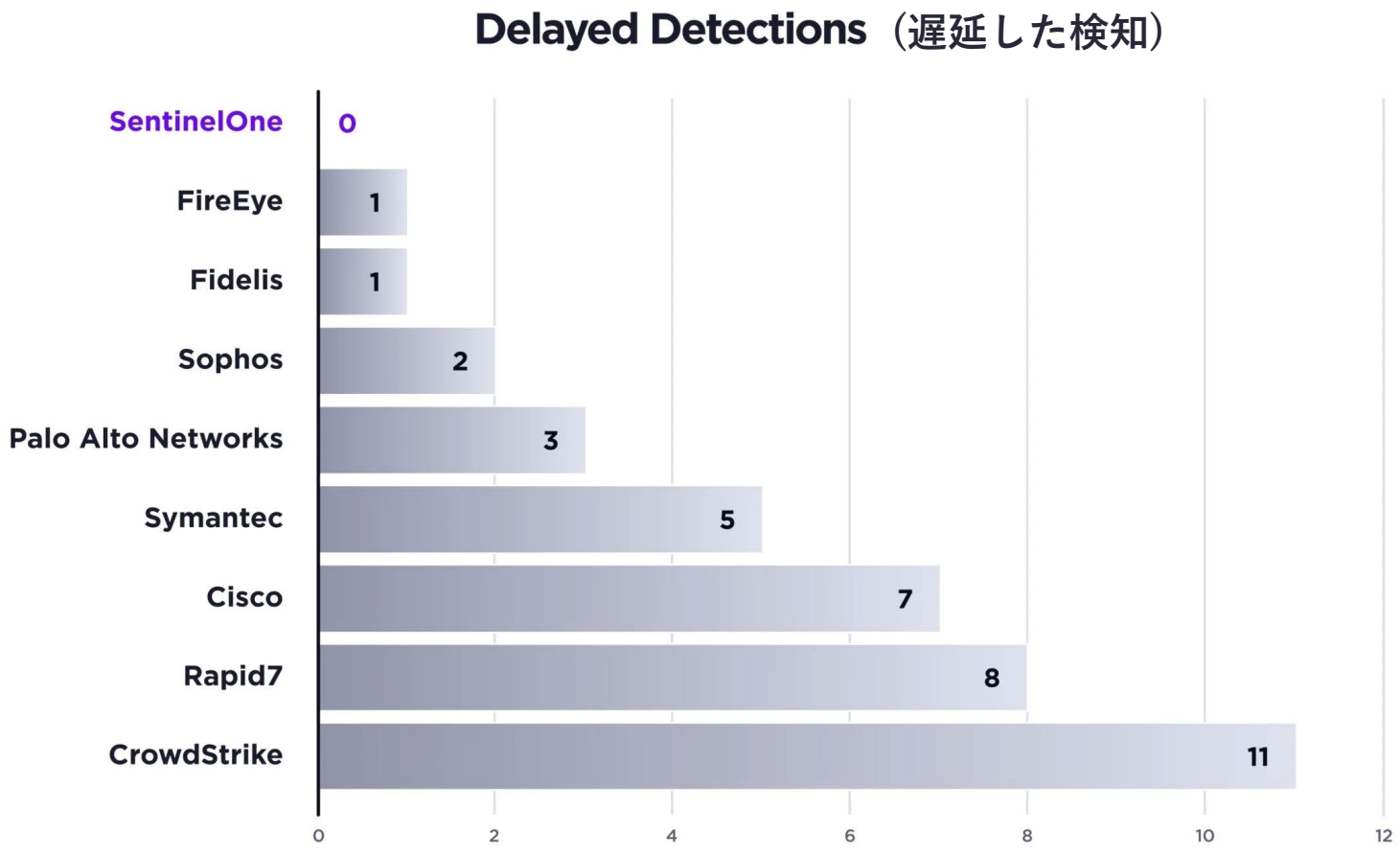
99%のアナリティックカバレッジを達成

109種類の検知のうち108種類

最高峰の保護・検知能力（MITRE Engenuity ATT & CK® 評価結果）



検知で遅延時間がゼロ（MITRE Engenuity ATT & CK® 評価結果）



エンドポイント製品の世代の移り変わり

運用自動化への潮流

アンチウィルス

レガシー/従来型

McAfee　Symantec

シグネチャ型 (定義ファイル)

- 運用や監視という概念がない
- 一度突破されたら終わり
- 標的型や高度な攻撃を検知できない

従来型EDR

EDRを使って**専門家が監視**

cybereason　Carbon Black

CORTEX　CROWDSTRIKE

有人監視型EDR

人力監視型; EDRが人をアシスト

- 大量のログデータをクラウドに保存して分析する
- インシデント対応に時間がかかる(ダウンタイム発生)
- 修復作業が複雑で困難

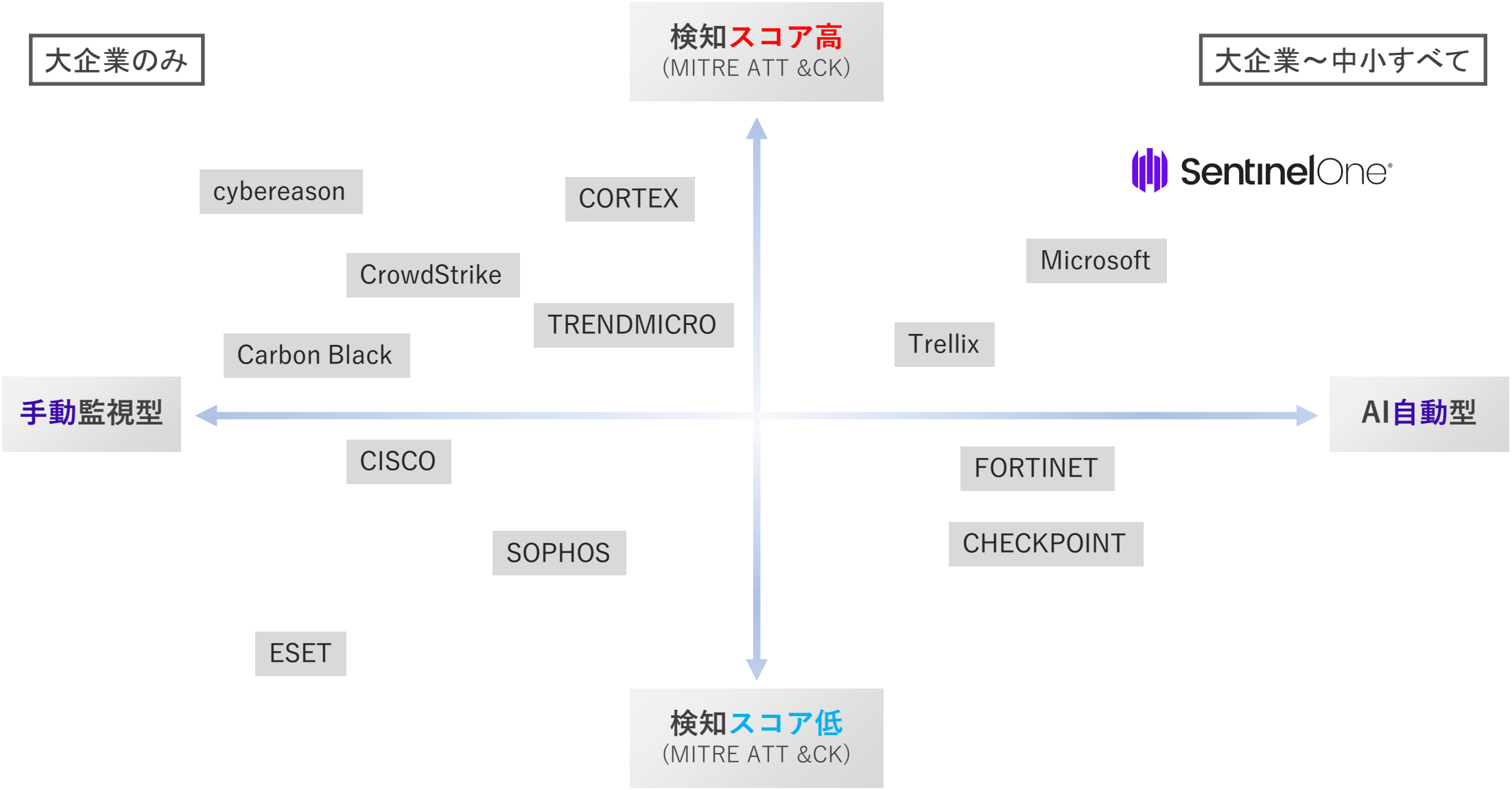
自動化されたEDR

AI監視を人が補助する

SentinelOne

端末ベースの自律AIとクラウド

- EDRの自動監視を人がサポート
- 端末内のAIでクラウドに依存しない
- 統合されたデータレイク
- 自動対応により瞬時に一次対応する事で0ダウンタイム
- 自動的に修復を行い、リスク状態から回復

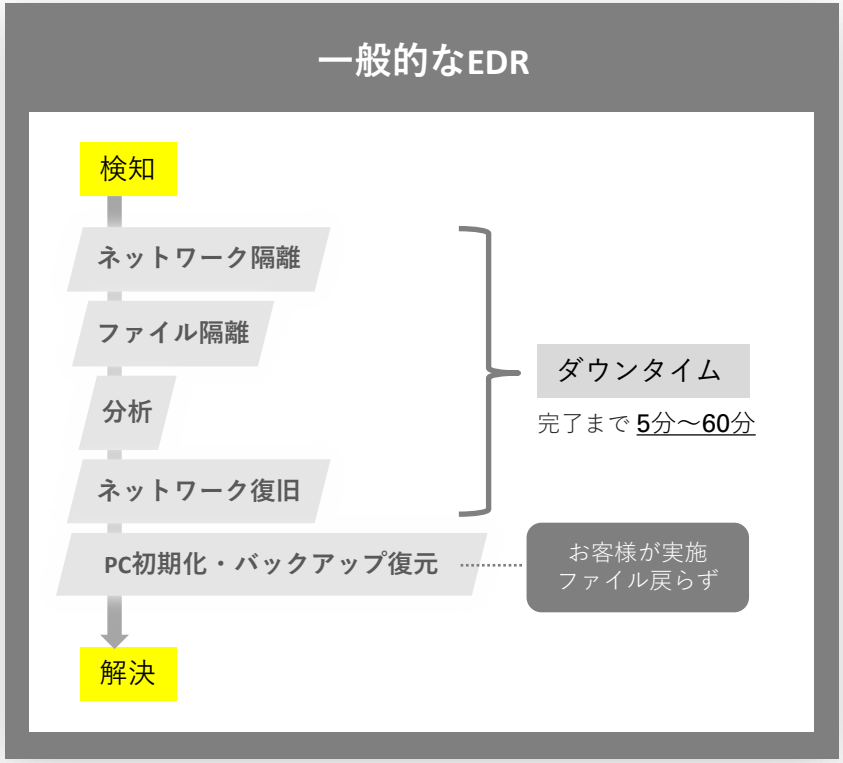


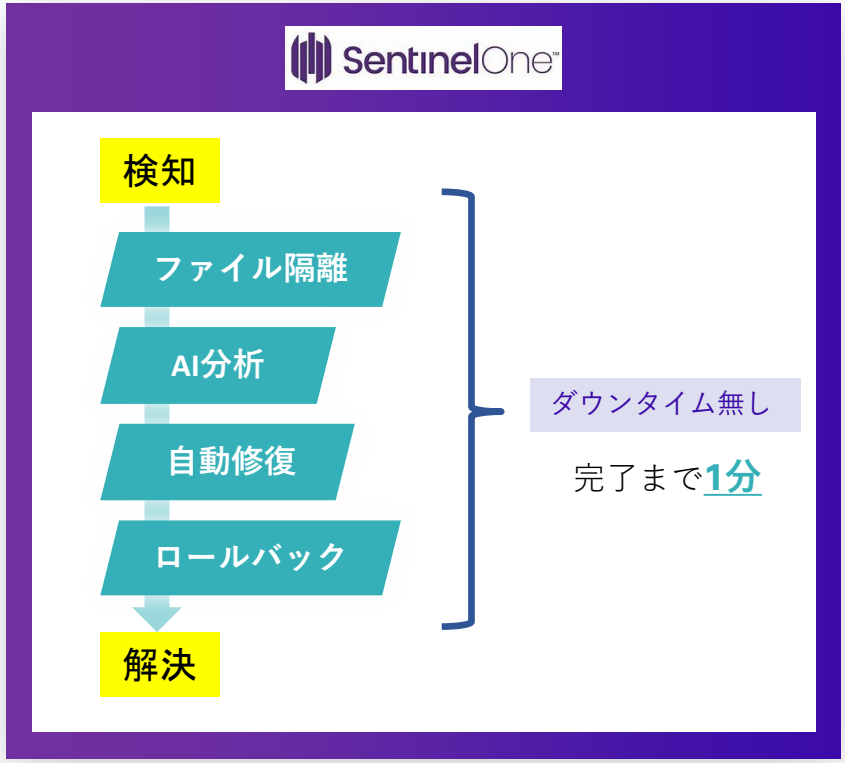
サイバーセキュリティ総研調べ(2022)

ネットワーク隔離のダウンタイム

手動対応型のEDR製品では、脅威の検知から解決までの間、ネットワーク隔離されPCの利用者にダウンタイムが発生します。SentinelOneは自動対応により即時修復まで完了するため、インシデント対応中のダウンタイムを最小限にします。

ネットワーク隔離
⇒調査するための時間稼ぎ
検知後すぐに修復が始まれば、
時間稼ぎは不要。

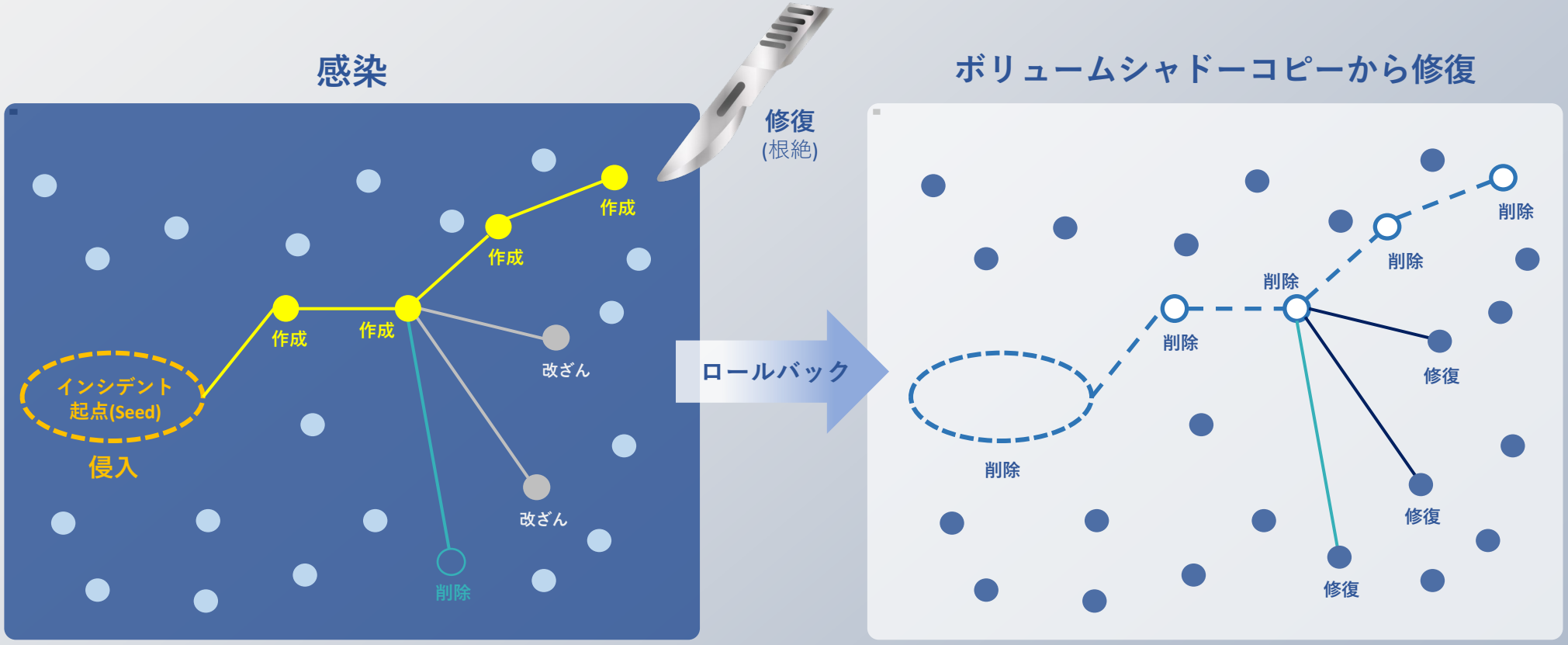




修復(根絶)＆ロールバック機能の仕組み

米国特許技術

ボリュームシャドーコピーとTrue Contextを照合し、必要最小限を部分移植する。
検知されてから0.1秒以内に修復作業を開始する



※Windows OSのみ対応

Sentinelone 自動監視の優位性

自動化領域

- ファイル レピュテーション — 既知のマルウェアをブロック
- AIコード解析 実行前 静的AI — 未知のマルウェアをブロック
- ふるまい検知 動的AIエンジン — 侵入を検知 攻撃の全体像を把握
- 自動対応 修復エンジン — 端末を自動隔離 感染部分を除去
- ファイル復元 即時ロールバック — 自動修復 ファイル復元

手動領域

- 高度なEDR Deep Visibility 脅威ハンティング — 内部感染の有無を確認

アンチウィルス → AI分析 → アンチエクスプロイト → レスポンス → ロールバック → 事後調査

予防・未然に防ぐ	早期発見	一次対応 (Kill+隔離)	二次対応 (根絶・修復)	三次対応 (分析・CSIRT)

1. マルウェアを実行前に排除
2. すり抜けても被害を最小化
3. 高速システム修復 1分以内 米国特許No.10,102,374
4. フォレンジック 再発防止策 ホワイトリスト

パターン別の運用イメージ

1. 費用/工数最小型（フルオート、費用/工数は”最小”、誤検知の課題が”中”）

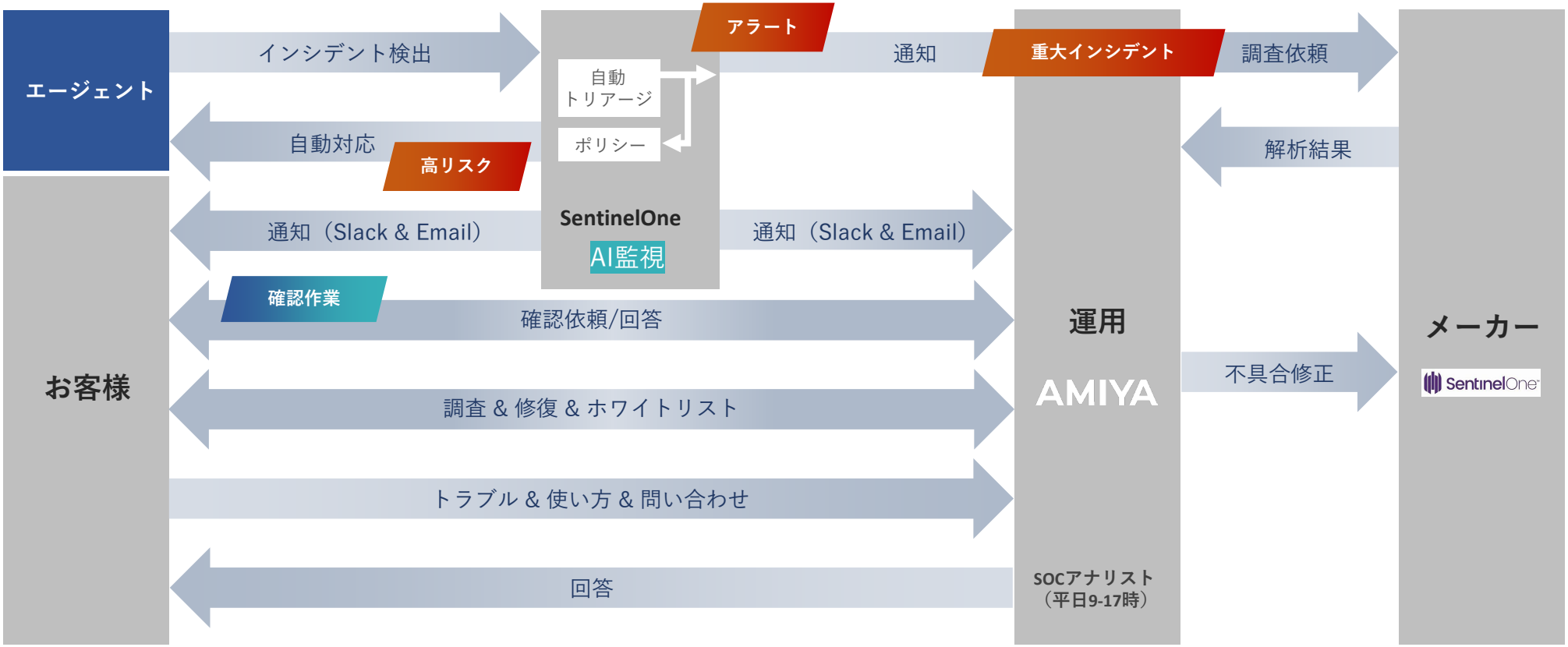
検知	隔離	調査・復旧	調整（誤検知）
オート	オート	オート	内製運用

2. バランス型（セミオート、費用は他社に比べて”小”、誤検知の課題も”小”）

検知	隔離	調査・復旧	調整（誤検知）
オート	オート （ファイル隔離 or NW隔離）	外部運用	外部運用

SentinelOne EDR運用サービス

（SOC運用監視=AI監視＋運用）



SentinelOne EDR運用サービス

サービス内容

サービス項目	詳細	ライセンスのみ	ライセンス＋ 運用サービス
AI自動インシデント対応	AIによる24時間365日の監視及び分析、復旧※オートモード時のみ	○	○
QA対応	製品の仕様/操作に関するご質問	○	○
コミュニケーション方法	各種問い合わせ時に利用するコミュニケーション手段	Email、電話	Email、電話
アナリスト詳細分析と対応	SentinelOneエージェントで検知したインシデントの確認及び誤検知判断、復旧対応	×	○
設定チューニング	ポリシーの設定やホワイトリスト登録	×	○
バージョンアップ代行	SentinelOneエージェントのバージョンアップ作業	×	○
フォレンジック調査	重大インシデント発生時にフォレンジック調査を実行	要見積	○
現地訪問/インストール作業	エージェントのインストールはお客様作業を想定	×	×

SentinelOne EDR運用サービス

アナリスト詳細分析サンプル

管理コンソールでのインシデント解析情報の更新

THREAT INDICATORS　NOTES (1)　XDR

Add new

[redacted] • Aug 28, 2023 15:14:54

本インシデントについて解析したところ以下の結果を確認しました。

AI判定　　：悪意ある脅威
検知エンジン：On-Write Static AI
検知タイプ　：スタティック
脅威の分類　：マルウエア

ハッシュ値をVirus Totalに照合したところ、本日から拡散している新型のマルウエアと合致しました。スタティック検知により即時削除されていますので実際にマルウェアが実行されたわけではありませんが念のため社内への注意喚起をお願い致します。

メールによる通知

送信(S)
宛先(T)
C C(C)　mdr-support@amiya.co.jp
件名(U)　2023/9/1 13:00発生のインシデントについて

ご担当者様
お世話になっております、網屋 SentinelOne サポートです。

2023/9/1 13:00 に検知されたインシデントについて解析したところ以下の結果を確認しました。

AI 判定　　：悪意ある脅威
検知エンジン：On-Write Static AI
検知タイプ　：スタティック
脅威の分類　：マルウエア

ハッシュ値を Virus Total に照合したところ、本日から拡散している新型のマルウエアと合致しました。スタティック検知により即時削除されていますので実際にマルウエアが実行されたわけマルウエアせんが念のため社内への注意喚起をお願い致します。

以上となりますがよろしくお願いいたします。

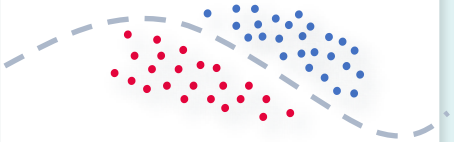
サブスクリプション機能比較

機能			CORE（オススメ）	CONTROL	COMPLETE
検知・防御	静的ファイル解析/動的挙動解析		○	○	○
	ドキュメント・スクリプト・バイナリなどのマルウェア		○	○	○
	ファイルレスマルウエア		○	○	○
	ランサムウエア		○	○	○
	エクスプロイト		○	○	○
	ラテラルムーブメント		○	○	○
レスポンス	修復・復旧		○	○	○
	ネットワーク隔離		○	○	○
	フルリモートshell		-	○	○
セキュリティスイート	デバイス制御	USBメモリ、Bluetooth制御	-	○	○
	アクセス制御（Firewall）	パーソナルFirewall	-	○	○
	脆弱性管理	アプリケーションのパッチバージョン	-	○	○
EDR 脅威検知	ActiveEDR		ベーシック	ベーシック	アドバンスト
	ストーリーライン		ベーシック	ベーシック	アドバンスト
	脅威ハンティング・Deep Visibility		-	-	○

EDR機能の違い

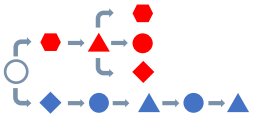
Core/Control/Complete共通 ベーシックEDR

リアルタイム脅威分析



ML for PEs & Docs

振る舞い検知エンジン



AI検知モデル

自動対応・修復

- 自動Kill &Quarantine
- ネットワーク自動隔離
- ストーリラインに基づく修復
- フルロールバック
- オフラインでも自動対応

Complete アドバンスドEDR

Deep Visibility & Response

- 脅威ハンティング
- STAR ウォッチリスト
- 高速なクエリ検索
- フルアタックストーリーライン
- 侵入経路の特定
- MITRE ATT & CK™ 脅威ハンティング
- フルリモートシェル

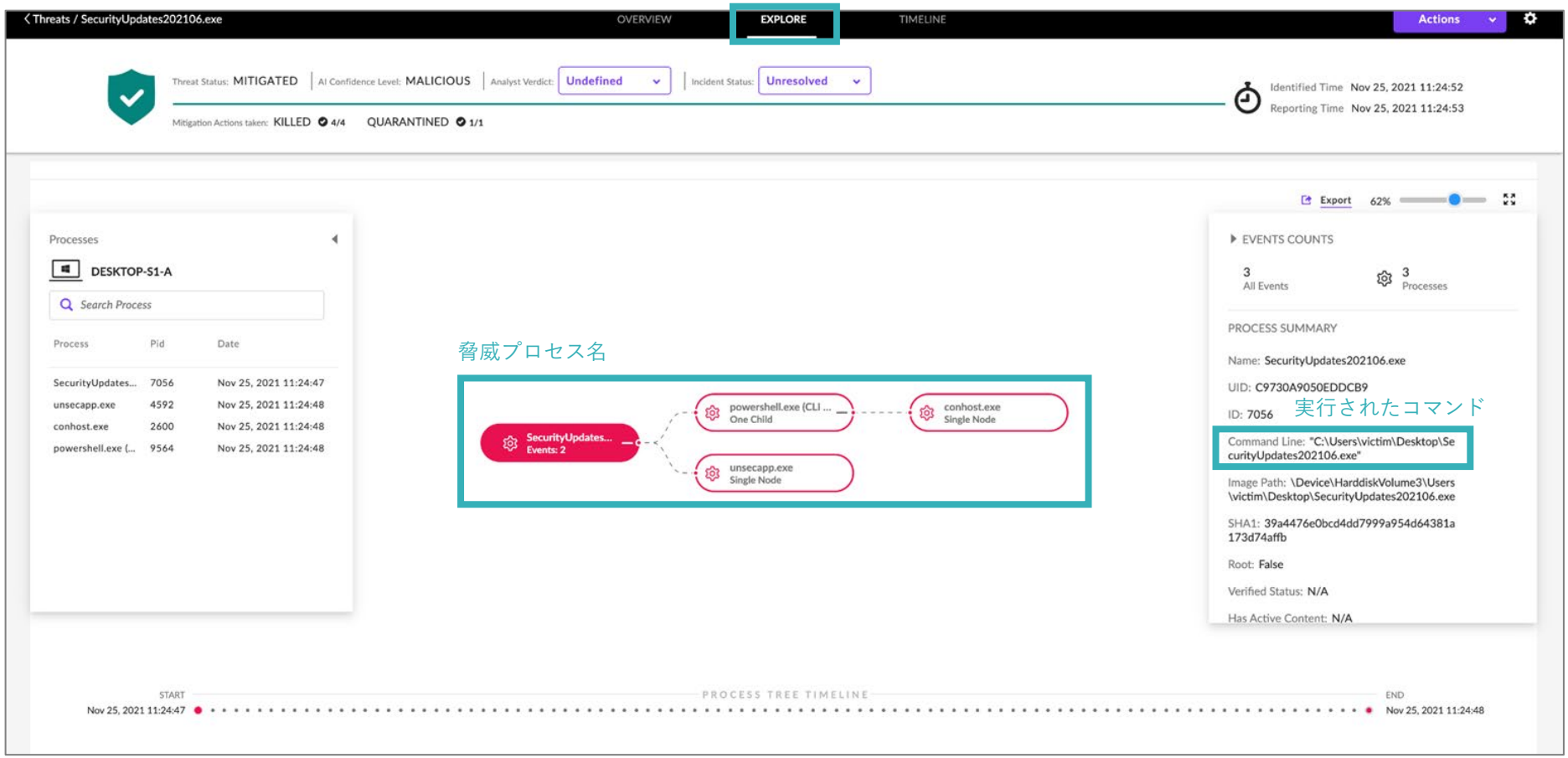
自律型のリアルタイム検知＆保護　+　修復&ロールバック

詳細な脅威対応

対応時間 = 秒単位
統合された軽量エージェント
自律型のエージェント対応 + クラウドインテリジェンス
Windows, Mac, Linux, VDI, Cloud, Kubernetes/Docker

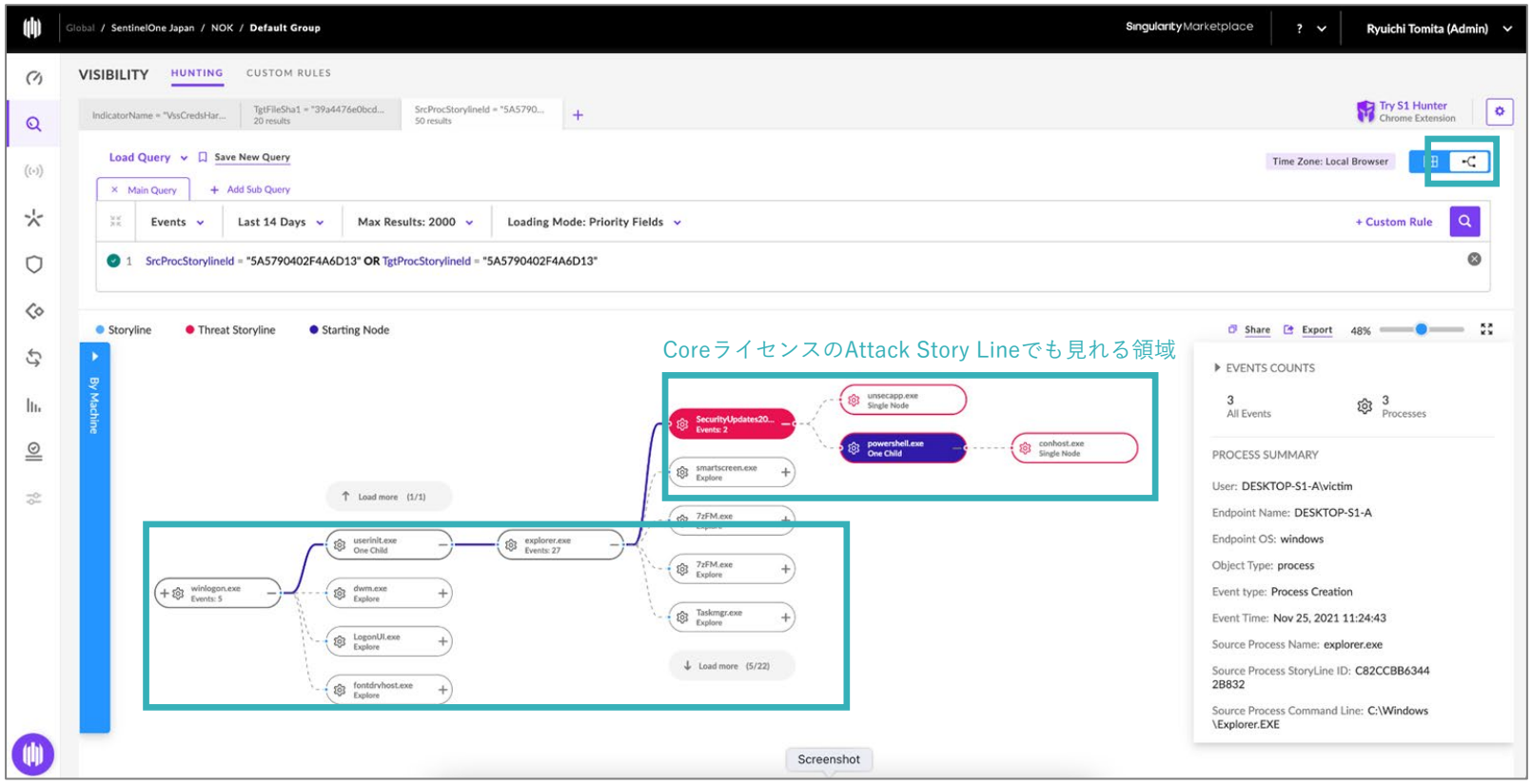
ログ保存期間
14 days(標準) - 1 year(オプション)
Full context and correlation
Integrated response workflow

Coreライセンスにおける脅威分析画面(Attack Story Line)



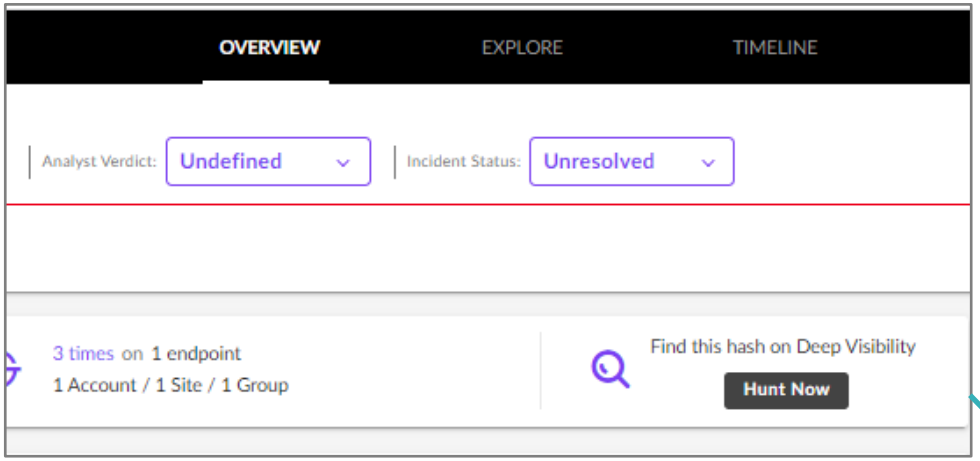
CompleteライセンスにおけるDeepVisibility StoryLine

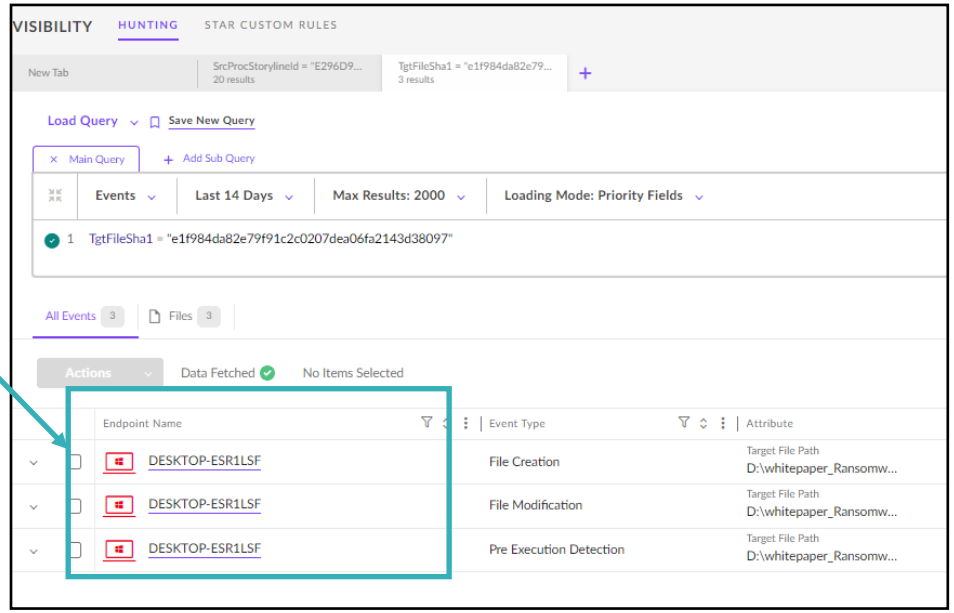
Coreには検知の起点となるプロセスよりも前の段階のログが残されていないため、さかのぼった相関分析ができない。
Compeleteではすべての挙動ログを１４日間保存しているため、
検知した時点からさかのぼってプロセスを解析する事で、侵入経路の特定などを行う。



標準的な脅威ハンティング（Complete）

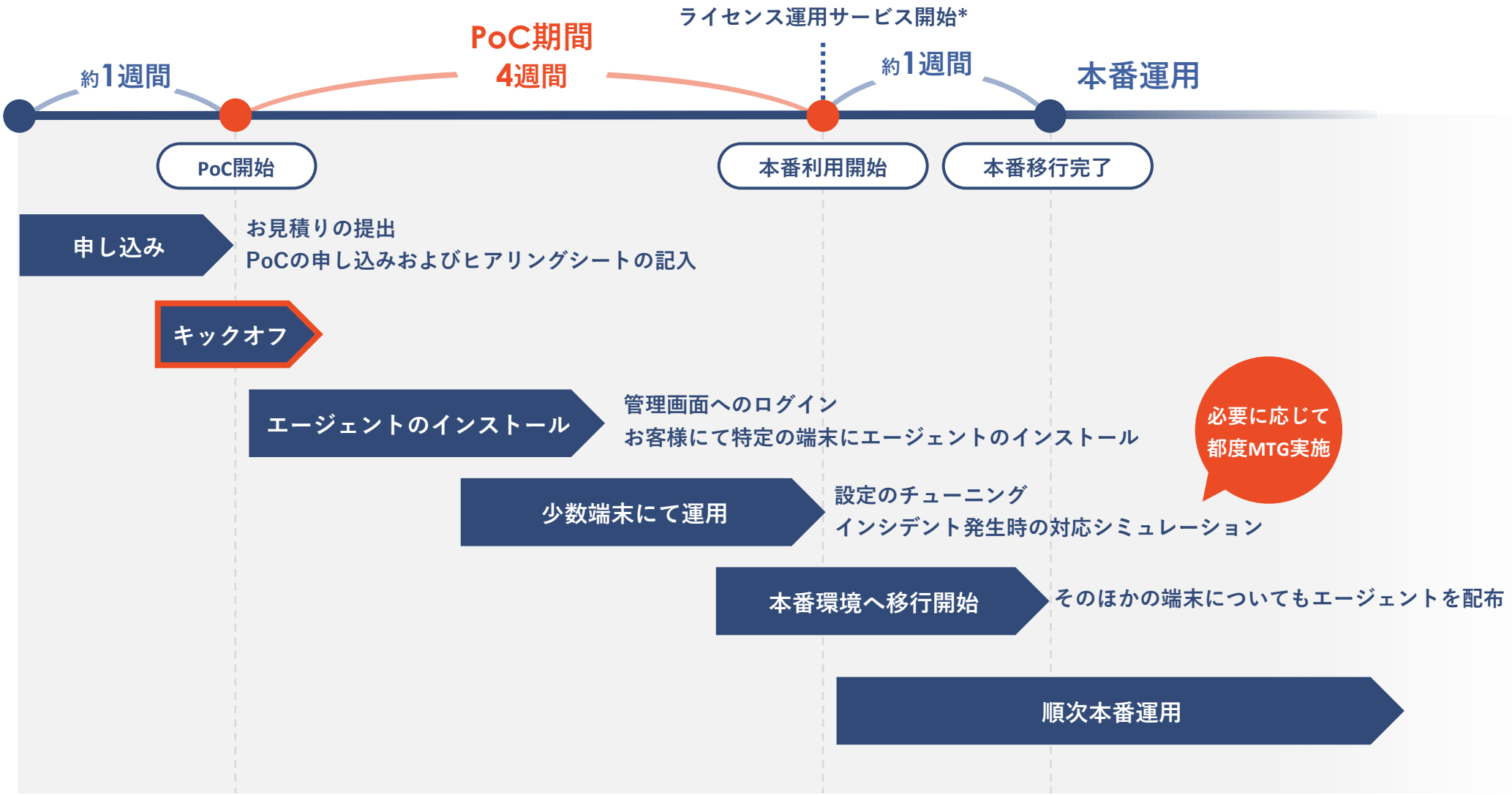
振る舞い検知で見つかった脅威は、ファイルが実行されるまで検知されない。
同様の脅威が社内の他の端末に未実行の状態で潜伏しているかどうかをハッシュ値で一斉検索する。
インシデント発生後の対応として、従来のアンチウィルスソフトにおける、「定義ファイルが更新されたのでフルスキャンをかてみる」というアクションを、リアルタイムかつ意味のある形で実施する事ができる。





発見した脅威が他のデバイスに
潜伏していないかを調査

SentinelOne 導入スケジュール



*開始タイミングは毎月1日

ライセンス価格

PC用ライセンス	型番	定価（1年間・1台）	提供価格（1年間・1台）
SentinelOne Coreライセンス	S1-CORE-PC	**￥12,000**	**￥6,000**
SentinelOne Controlライセンス	S1-CONT-PC	**￥14,400**	**￥7,800**
SentinelOne Completeライセンス	S1-COMP-PC	**￥48,000**	**￥12,000**

サーバー用ライセンス	型番	定価（1年間・1台）	提供価格（1年間・1台）
SentinelOne Coreライセンス for Server	S1-CORE-SV	**￥18,000**	**￥10,300**
SentinelOne Controlライセンス for Server	S1-CONT-SV	**￥18,000**	要相談
SentinelOne Completeライセンス for Server	S1-COMP-SV	**￥48,000**	要相談

オプションサービス価格

サービス名	型番	定価 （1年間・1台）	提供価格
EDR運用サービス	S1-MDR-OPT	**￥3,600**	**￥2,000**

サービス名	型番	数量	提供価格
EDR構築支援	S1-CS-1000	～1000台	**￥400,000**
	S1-CS-5000	1001台～5000台	**￥850,000**
	S1-CS-9999	5001台～	要相談

初年度費用
Coreライセンス100台
運用サービス込みの場合

Coreライセンス費用
：年額6,000円×100台

EDR運用サービス
：年額2,000円×100台

Total
：年額80万円

※導入社は1社を想定しております。関連会社を含む場合は要相談となります。

エージェント要件

対応OS

Windows OS（エンドポイント）	Windows OS（サーバー）
Windows 11（21H2含む）	Windows Server 2022
Windows10	Windows Server 2019
Windows8/8.1	Windows Server 2016
Windows7	Windows Server 2012/R2
	Windows Server 2008 R2 SP1
	Windows Storage Server 2016,2012 R2

レガシーエージェント（機能制限あり）	
Windows XP SP3（機能制限）	Windows Server 2003（機能制限）

サポート対象外	
WindowsMobile / Windows 10 IOT Core	
64bit/32bit対応	ARM CPU非対応

その他 K8 コンテナ関連・モバイル	
Docker	Amazon Elastic Kubernetes Service（EKS）
ContanerD（starting K8s Agent 4.5）	Azure Kubernetes Service（AKS）
CRI-O（starting K8s Agent 4.6）	iOS
Kubernetes version 1.13 or later	Android
Open Shift version 4.4 – 4.11	Chrome OS
Google Kubernetes Engine（GKE）	Net App

mac OS
mac OS latest Beta（13）
mac OS Monterey（12）
mac OS Big Sur（11）
mac OS Catalina（10.15）
mac OS Mojave（10.14）
mac OS High Sierra（10.13）
mac OS Sierra（10.12）

Linux OS
CentOS 6.4+,7,8
Red Hat Enterprise Linux 6.4+,7,8,9
Ubuntu 22.04,20.04,19.10,19.04,18.04,16.04,14.04
Amazon Linux 2,AMI 2018,AMI 2017
SUSE Linux Enterprise Server 15.x,12.x
Virtuozzo7,Scientific Linux7,6, AlmaLinux 8.4-9.0,RockyLinux 8.4–9.0
Oracle 6.9–9.0
Fedora 25-30,31（5.5.x）,32-36

2023年3月時点
※最新情報はお問い合わせください

必要となるライセンス種別

- **エンドポイントライセンス**
  Windows11/10/7/XP
  MacOS系
- **サーバーライセンス**
  Windows　Server
  LinuxOS系
- **K18ライセンス**
  コンテナ系

ハードウェア最低要件

Windows 端末		macOS 端末		Linux 端末	
CPU	1GHz Dual-core	CPU	1GHz dual core	CPU	2GHz dual core
Memory	2GB以上	Memory	2GB	Memory	4GB
HDD容量	3GB以上10%以上の空き	HDD容量	2GB以上の空き	HDD容量	2GB以上の空き
AFMチップ非対応		Intel/Apple チップ対応		SSE4a非対応	

以下のマイクロアーキテクチャには対応していません。
ppc84,x86_32,ARM,RISC,MIPS

Windowsエージェントのシステム負荷（参考値）

この数値は一般的な環境における実測値をもとにした参考値であり、環境や利用状況、設定によって大きく変動します。

項目	詳細
CPU	**平均1%未満**（0.2-0.6実測値） 併用するIT資産管理やSQLなどを正しく除外設定した場合。
Memory	**180-350MB**程度（実測値）メモリの空き状況により変動します。
HDD	**Program Files¥SentinelOne(200MB)** **ProgramData¥Sentinel(1GB)** ※ログ設定により制御
VSS上限値	**推奨は10%**（インストール時に設定値が**存在しない**場合、10%を設定します）。 ランサムウェア検知時は一時的に上限を超えてVSSを取得する場合があります。 デフォルトで4時間ごとにVSSバックアップを取得します。
ネットワーク	通信量 1日で**4-8MB**（Completeの場合追加で11MB）程度
プロセス	Sentinel Service Host External Engines Sentinel Service Host Sentinel Static Engine Scanner SentinelOne Agent