SentinelOne™ ご紹介資料

SentinelOneセールスパートナー
株式会社サンソウシステムズ

SentinelOne紹介資料
Last updated August 2023

目次

EDR導入の必要性

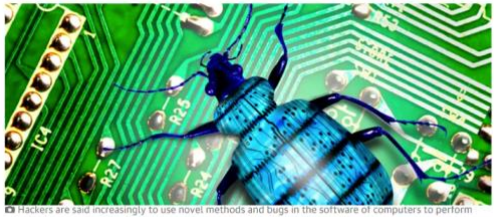
1. 現代のセキュリティ問題
2. EDRとは
3. アンチウィルスソフトでは防げない脅威
4. アンチウィルスソフト(ED)とEDRの違い
5. 御社のセキュリティ導入レベルは？

SentinelOne™

現代のセキュリティ問題

Antivirus software is dead, says security expert at Symantec

Information chief at Norton developer says software in general misses 55% of attacks and its future lies in responding to hacks



Hackers are said increasingly to use novel methods and bugs in the software of computers to perform attacks. Photograph: Dale O'Dell/Alamy Photograph: Dale O'Dell / Alamy/Alamy

Samuel Gibbs

Tue 6 May 2014 14.08 BST

210

Antivirus software only catches 45% of malware attacks and is "dead", according to a senior manager at Symantec.

Remarks by Brian Dye, senior vice-president for information security at the company, which invented commercial antivirus software in the 1980s and now develops and sells Norton Antivirus, suggest that such software leaves users vulnerable.

Dye told the Wall Street Journal that hackers increasingly use novel methods and bugs in the software of computers to perform attacks, resulting in about 55% cyberattacks going unnoticed by commercial antivirus software.

Malware has become increasingly complex in a post-Stuxnet world. Computer viruses range from relatively simple criminal attacks, where credit card information is targeted, to espionage programs that spy on users and data but can easily be upgraded into cyberweapons at the touch of a button, according to security expert Eugene Kaspersky, founder of Kaspersky Lab, which also sells antivirus software.

From protect to 'detect and respond'

That failure to detect issues is forcing Symantec, which has a turnover of about $1.6bn (£590m) and an 8% global antivirus marketshare - according to data from the enterprise software company Opswat - to diversify its products, moving into the "detect and respond" sector rather than the simple "protect" segment.

2014年 セキュリティソフト大手シマンテックの副社長が
「アンチウィルスソフトは死んだ」と発言

https://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec

ウィルス対策ソフトで阻止できる脅威は

約45%

阻止できない **55%** は？

- Emotet
- 暴露ランサム
- ハッキング

いまEDRの導入が必要

EDRとは

Endpoint Detection and Response

エンドポイントの検知と対応

従来のアンチウィルスソフトは、検知はするが、対応がない。
つまりEndpoint Detectionのみ。
EDRでは、脅威がアンチウィルスをすり抜ける事を前提とし、
早期発見、被害を封じ込めに重点をおいた製品となっており、
企業にとっての致命傷を避ける事ができる。

アンチウィルスソフトでは防げない脅威

55%の脅威は侵入=「侵入される前提の対策」が必要

脅威 → ①入り口 → ②侵入 → ③活動 → ④破壊

Detection(検知)：②侵入まで　Response(対応)：③活動以降

	①入り口	②侵入	③活動	④破壊
第１世代 アンチウィルス (E+Dの半分)	ファイル検査	該当機能なし	該当機能なし	該当機能なし
第２世代 次世代アンチウィルス (E+D)	ファイル検査 AI	ふるまい検知 AI	該当機能なし	該当機能なし
第３世代 EDR統合型 (E+D+R)	ファイル検査 AI	ふるまい検知 AI	緩和処置 AI	システム修復 AI

アンチウィルスソフト(ED)とEDRの違い

	検知フェーズ	機能	アンチウィルス	EDR(SentinelOne)
Detection (検知)	1.侵入前	ハッシュ値解析	○ 定義ファイル	○ レピュテーション
		コード解析	○ パターンマッチング	○ スタティック AI
	2.感染の瞬間	ヒューリスティック	△ サンドボックス	○ ふるまい検知AI
	3.感染中	早期発見	✖	○ ふるまい検知AI
		社内感染の検知 (ラテラルムーブメント)	✖	○ ラテラルムーブメント
Response (対応)	4.事後処理	インシデントの調査	✖	○ アタックストーリーライン
		個人情報保護法の対応	✖	○
		感染被害の復旧	✖	○ 修復＋ロールバック

御社のエンドポイントセキュリティの導入レベルは？

SentinelOneについて

1. SentinelOne企業概要
2. 導入実績
3. SentinelOneの影響力

SentinelOne™

SentinelOne企業概要

会社規模

従業員数	2000
顧客数	8000+
上場	2021年6月IPO（潤沢な投資資金）

サポート体制

グローバルサポート	24時間365日
VIGILANCE MDR	24時間365日

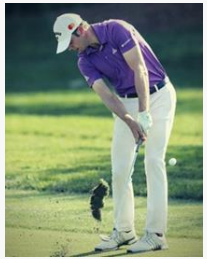
拠点

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 OneTM Team

USPGAツアーゴルファー　Sam Burns



導入実績

Fortune誌 格付け上位10中3社で採用（製造 / 金融 / エネルギー）されるなど
8000を超える顧客への導入実績があります

国外での導入実績

- McKESSON 医療小売
- flex EMS
- jetBlue 航空チケット予約
- ASTON MARTIN 自動車メーカー
- POLITICO メディア
- NORFOLK SOUTHERN 鉄道
- AUTODESK CAD
- norwegian 航空
- ESTĒE LAUDER 化粧品
- havas 広告
- FIMBANK 金融

国内での公開導入事例

SBSホールディングス	運輸
アンドパッド	IT
駒沢大学	文教
オンデーズ	メガネ
株式会社ショクブン	食品
ビーグローバル	人材
株式会社R4	人材
メディケアー	医療

その他国内1000程度

世界で高い評価を獲得

導入企業数は国内トップクラス

EDR検知性能テストでも
3年連続トップクラス

セキュリティベンター
上場評価額歴代1位

Gartner Magic
Quadrant for EPP
Leader

MITRE ATT&CK 2021
検知率100%
※唯一

導入実績
1000社以上

SentinelOneの影響力

SentinelOne はガートナーで

再びLeaderに選ばれました

SentinelOne の優位性

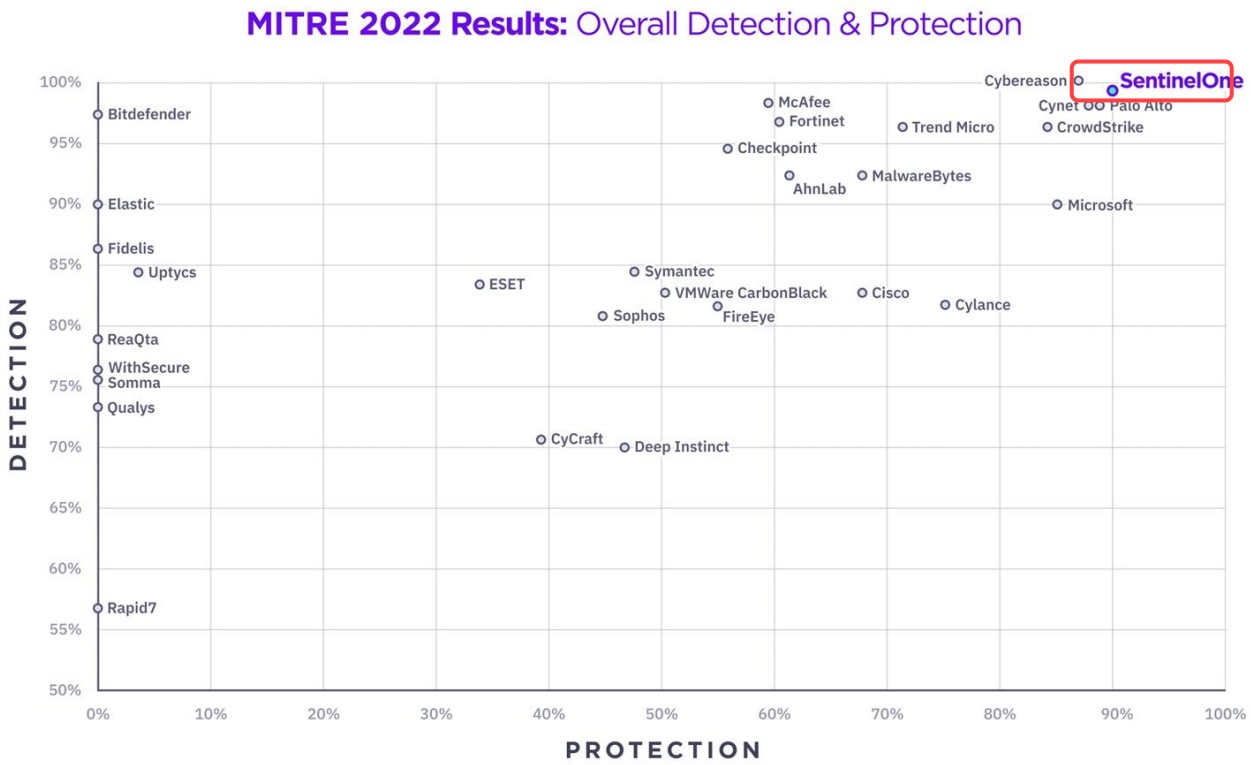
1. すべてのタイプの組織に適したEDR/XDR
2. IDセキュリティの網羅
3. MITRE ATT&CKで連続してリーダー的な位置付け
4. 多くのOSをサポート
5. 高度なMDRサービス提供
6. グローバルでのプレゼンス

EDRの中での優位性

1. 2022年のMITRE ATT&CK評価結果
    a. MITRE ATT&CKで100% Visibilityを達成
    b. 誤検知が少ないEDRとしての評価
2. エンドポイント製品の世代の移り変わり
3. SentinelOne 自動監視の優位性
4. 自動ロールバック機能
    a. 修復(根絶)＆ロールバック機能の仕組み
5. 企業規模別、おすすめ動作モード
6. ネットワーク隔離のダウンタイムが最小限
7. インシデント対応のスピードによるリスクの差
8. 自動化されたEDRの３つのメリット

SentinelOne™

2022年版　MITRE Engenuity ATT&CK ベンチマーク Wizard Spider + Sandworm

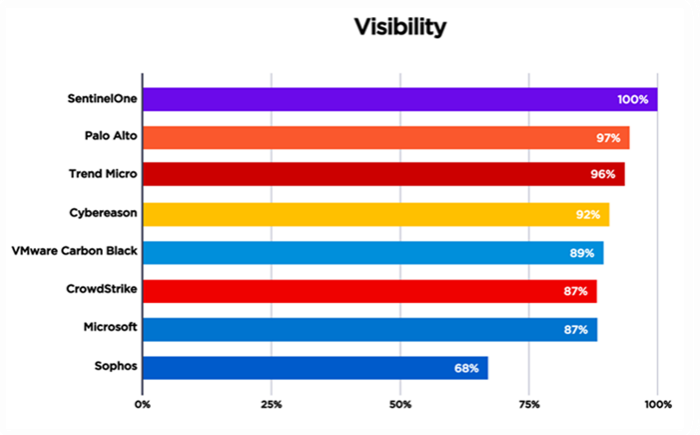


出典

SentinelOneの見解｜2022年のMITRE ATT&CK評価結果

MITRE ATT&CKで100% Visibilityを達成

- 100%の可視性 – 174ステップ中174ステップ
- 最高の分析カバレッジ – 174ステップ中159ステップ
- 遅延モディファイアがゼロ
- 構成変更モディファイアがゼロ



Evaluation Summary

These are the evaluations that SentinelOne has participated in:

Evaluations	Detection Count	Analytic Coverage	Telemetry Coverage	Visibility
APT3 (2018)	105 across 136 substeps	8 of 136 substeps	97 of 136 substeps	101 of 136 substeps
APT29 (2019)	290 across 134 substeps	123 of 134 substeps	109 of 134 substeps	127 of 134 substeps
Carbanak+FIN7 (2020)	333 across 174 substeps	159 of 174 substeps	164 of 174 substeps	174 of 174 substeps

誤検知が少ないEDRとしての評価

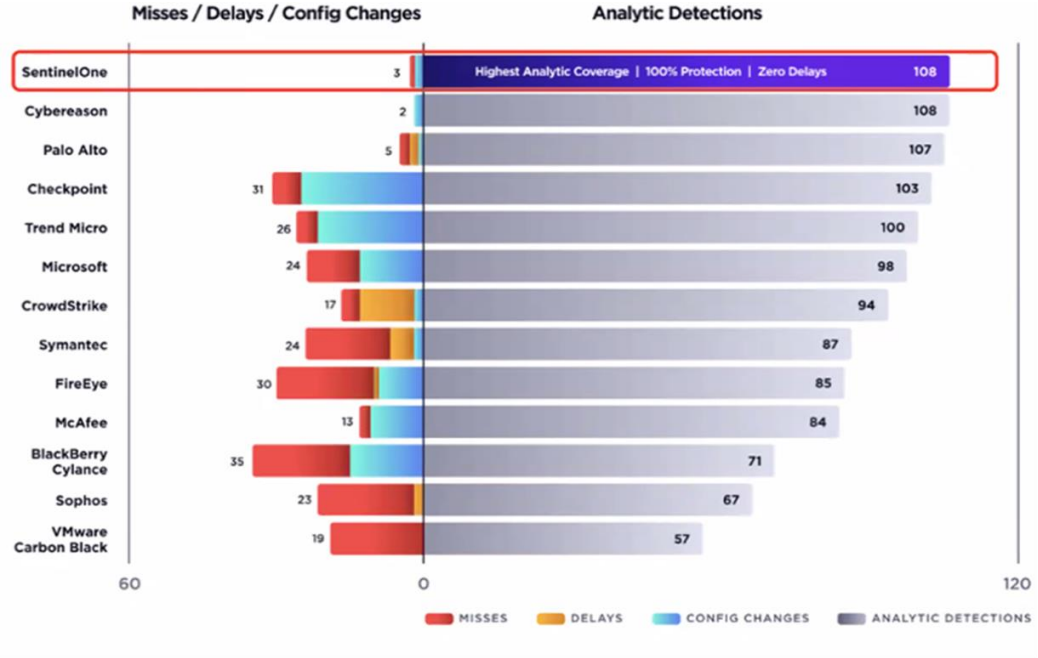
2年連続で高い分析能力を証明（2022）

分析能力が最も優れている

- 再考の分析能力（2年連続）
- 全ての脅威を100%防御
- ZERO検知遅延

出典

mitre att&ck results data



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

アンチウイルス

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

Microsoft　CORTEX

Carbon Black　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™

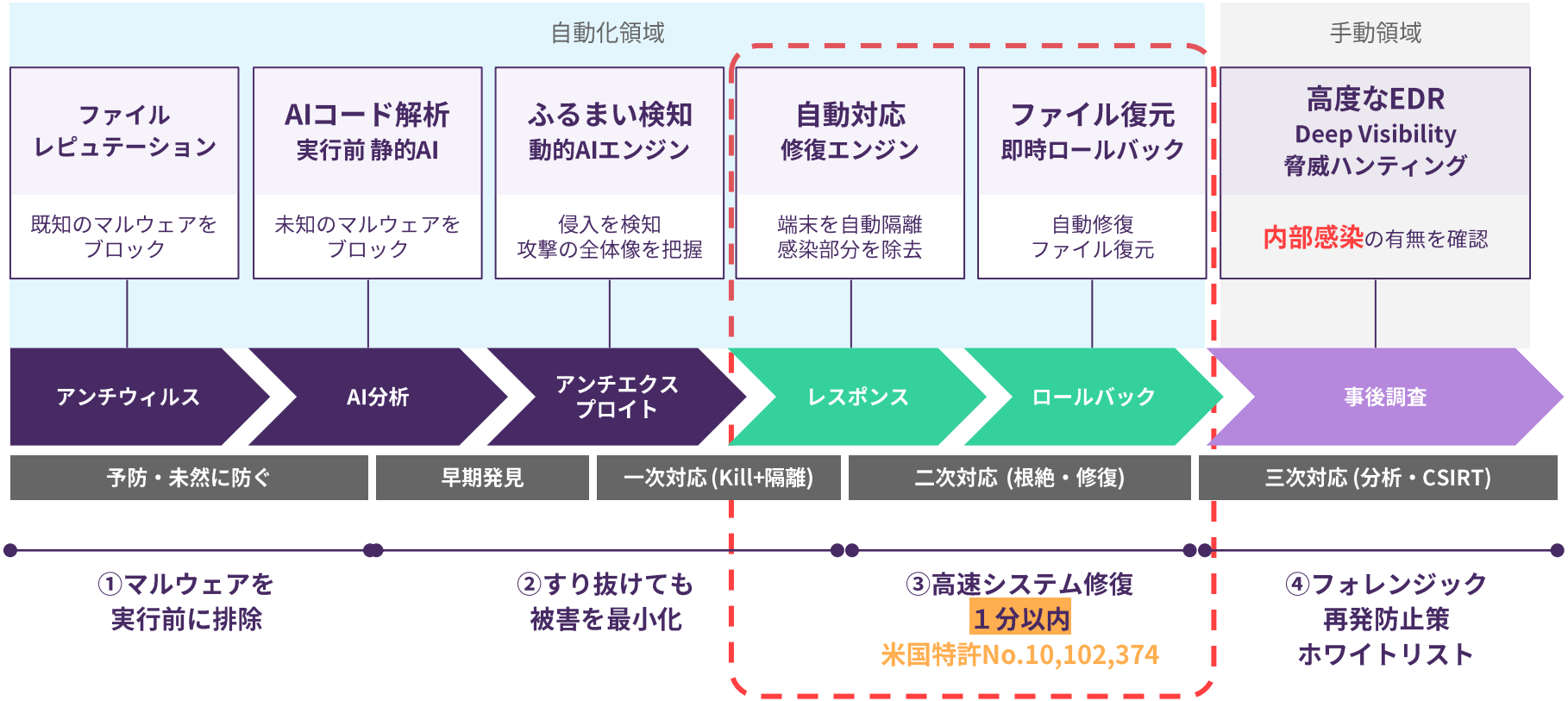
端末ベースの自律AIとクラウド

- 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

多くのEDR製品が自動化を目指している

SentinelOne 自動監視の優位性

Singularity XDR



自動ロールバック機能

一般的なウィルス対策ソフトをすり抜ける脅威を
SentinelOneの振る舞い検知エンジンで検出し、
ランサムウェア被害にあったファイルを
瞬時に元通り修復します。

８年間、一度も破られた事がない
最強のランサムウェア対策

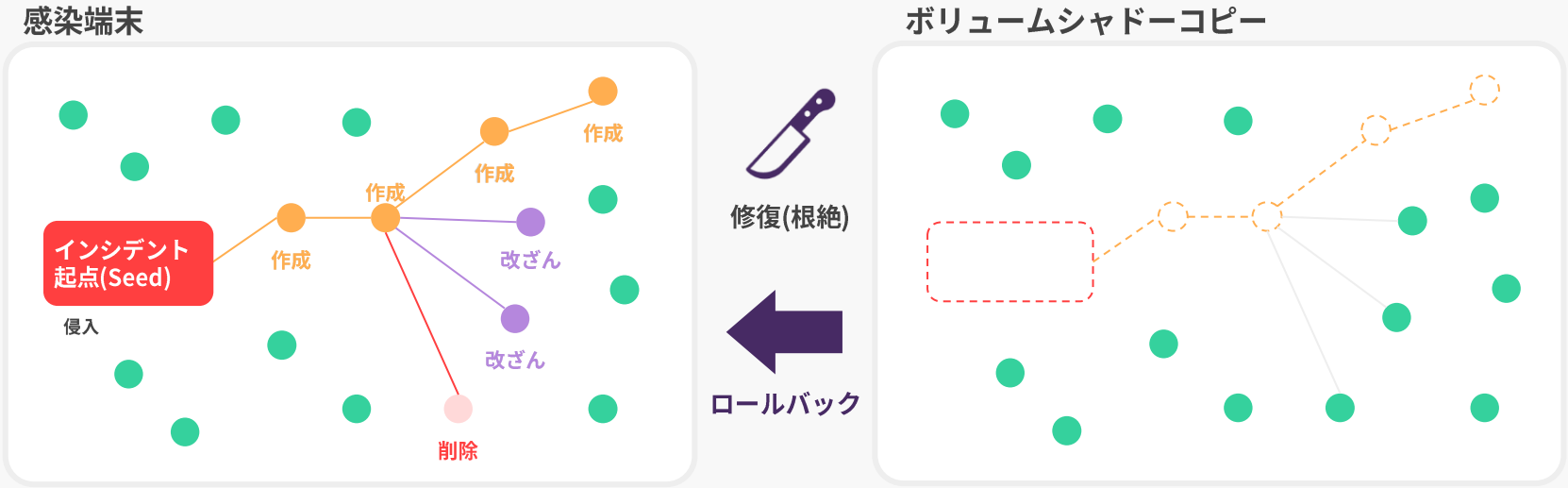
デモ動画

https://youtu.be/-Be8Dh_Q_Uc

一般的なアンチウィルスソフトでは検知できない脅威に
対するSentinelOneの自動修復を再現し
デモンストレーションしています。

修復(根絶)＆ロールバック機能の仕組み

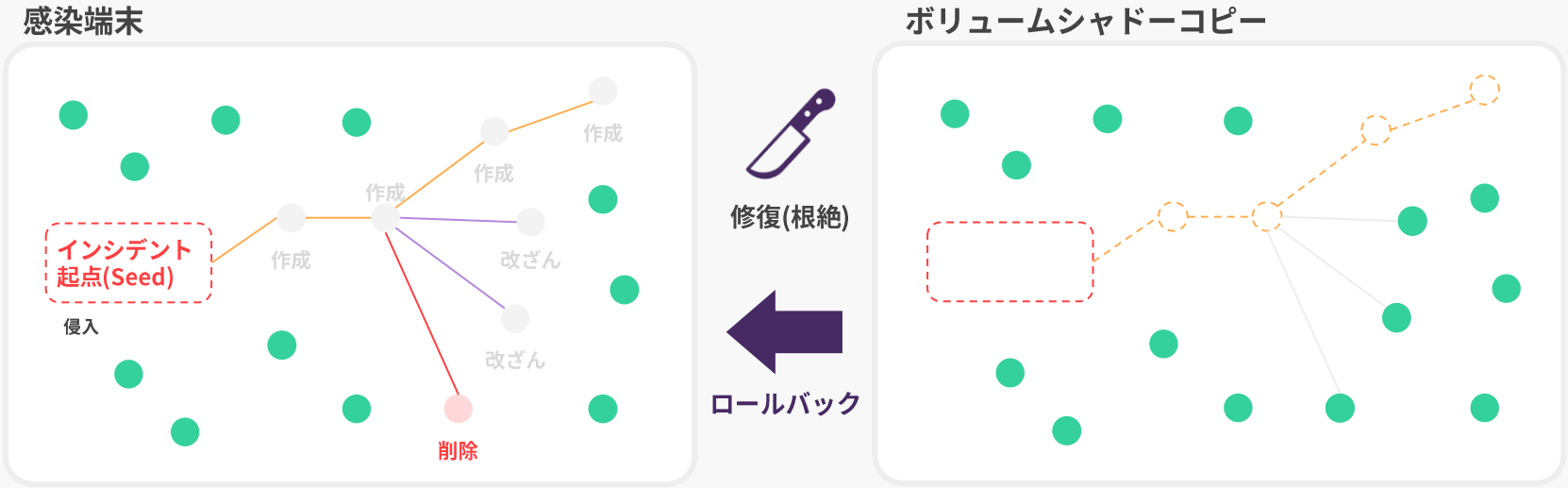
ボリュームシャドーコピーとTrue Contextを照合し、必要最低限を部分移植する。
検知されてから0.1秒以内に修復作業を開始する



※Windows OSのみ対応

修復(根絶)＆ロールバック機能の仕組み

ボリュームシャドーコピーとTrue Contextを照合し、必要最低限を部分移植する。
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

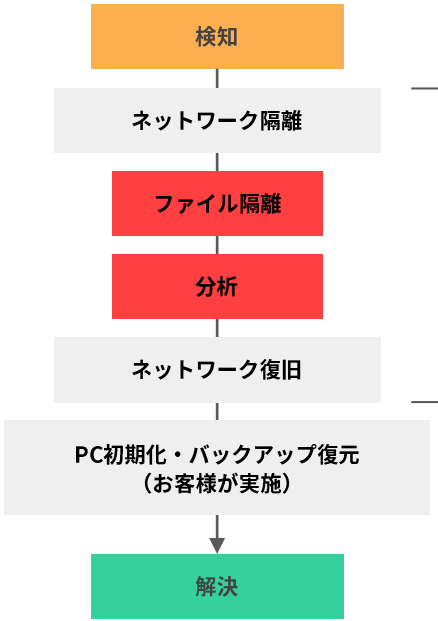
企業規模別、おすすめ動作モード

SentinelOneをフルオートモードを活用する事で、
運用コストをかけずにEDRを導入できます

規模	動作モード	EDR運用	運用コスト
中小企業	フルオート	なし	ゼロ
中堅企業	セミオート	内製運用	社内リソース
大手企業	セミオート	外部監視サービス	他者に比べて安価

ネットワーク隔離のダウンタイムが最小限

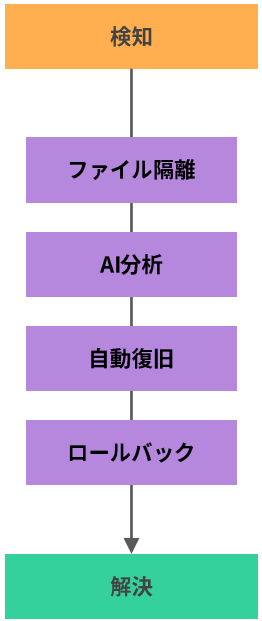
一般的なEDR



ダウンタイム
完了まで5分～60分

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



ダウンタイム無し
完了まで1分

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。

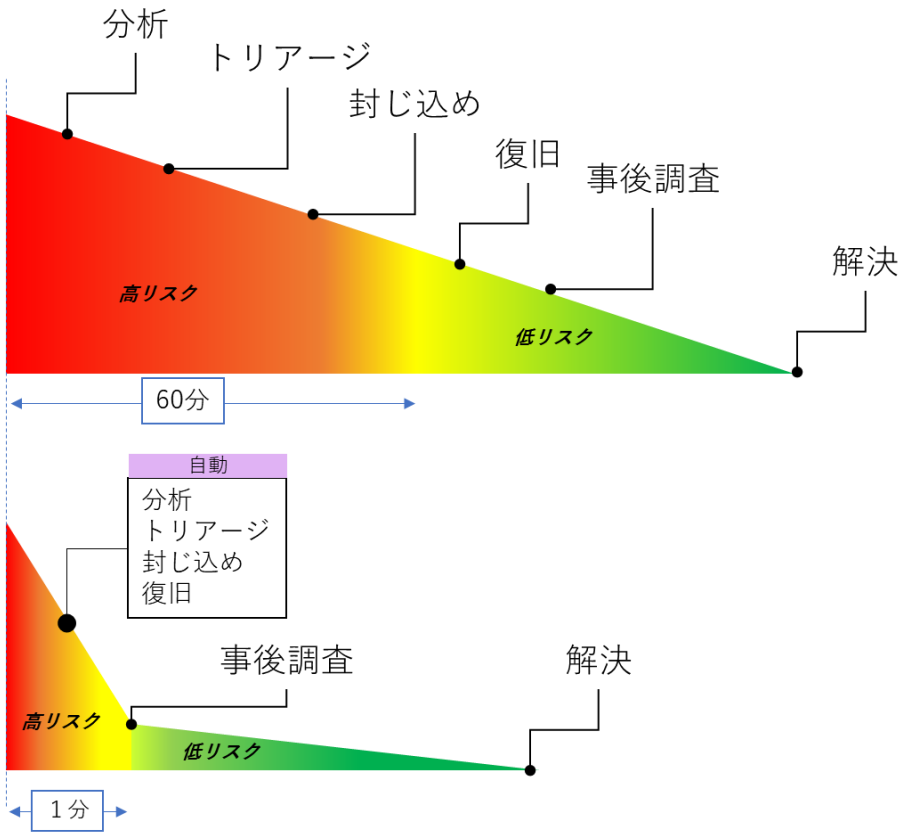
インシデント対応のスピードによるリスクの差

一般的なEDR

調査しながら段階的に対処するため
安全圏に到達するまで時間がかかる

SentinelOne

瞬時に安全圏に到達してから
事後調査する



自動化されたEDRの３つのメリット

1

低コスト

圧倒的に進んでいる
AI による自動運用により
運用コストを抑えられる。

2

ダウンタイムの短さ

AIの自動修復により
業務が止まる時間が無くなり、
すぐに業務に戻ることが可能。

3

安全性

人為的に対応を行うよりも
88 倍のスピードで
安全な状態まで復元するため、
より安全に。

３つのメリットを包括した**自動運用型EDR のメリット**などが入ります

製品仕様

1. 基本ライセンス概要
2. サブスクリプション機能比較
3. ネットワーク要件
4. エージェント要件
5. Windowsエージェントのシステム負荷(参考値)
6. プロダクトライフサイクル
7. 主な機能一覧

SentinelOne™

基本ライセンス概要 ※本資料ではCore部分について解説

Singularity XDR

Singularity Core

Singularity Core は、脅威ファイルやマクロの検査からファイルレス攻撃まで、様々な攻撃テクニック（MITRE ATT&CK対応）を検知する高度なAIエンジンを備えたNGAV 機能に加え、特許技術であるストーリーライン機能が脅威に関連するプロセスの行動を追跡し、受けた侵害を自動修復する機能を備えた基本ライセンスです。
管理コンソールはクラウド上にありますが、エージェントはクラウドとの接続が切れた状態でもフルにエンドポイント守ります。SentinelOne は自律型のAIエンジンを採用しているため、個々のエージェントが自律して脅威を検知し防御と修復を行えます。
SentinelOne をご採用いただくことで、企業規模にかかわらずセキュリティ対応（検知・防衛・対応・復旧）のリソースとコストを最適化しつつ、確実なセキュリティ対策を実施することが可能となります。
攻撃の防御だけではなく、脅威ハンティングにより能動的に侵入者を見つけて封じ込めたり、カスタムルールを使った様々な監視と対応を実施したい場合は Singularity Complete が必要になります。

Singularity Control

Singularity Control は Core の機能に加え、デバイス制御の機能を追加することでセキュリティ対策をより強固なものにするためのライセンスです。エージェントによる USB デバイス、 Bluetooth、ファイアウォールの制御を管理コンソールから一括管理することにより、エンドポイントにおける侵入やデータ漏洩などのリスクを制御することができます。
更に Control では、エンドポイントにインストールされたアプリケーションのインベントリリストや脆弱性情報（Beta)およびネットワーク探索によるエージェント未導入デバイスの探索と管理機能も提供します。

Singularity Complete

Singularity Complete は Core と Control の機能に加え、エンドポイントから定期的にデータを収集し、クラウドの分析プラットフォームに蓄積することで自由にイベントを検索したり、Core で見つけた脅威の影響範囲を詳細に調査できます。更にユーザーが自由に検知・対応ルールを作成できるカスタムルール機能を提供するライセンスです。
蓄積されたデータは、脅威の有無にかかわらずストーリーライン機能により各プロセスから派生する行動が全て一連の流れ（ストーリー）として容易に抽出できるため、脅威ハンティングにおいて脅威行動の追跡にかかる時間を大幅に短縮することができます。
また、ストーリーライン機能がプロセスの行動を詳細に記録しているため、脅威として特定した一連の流れにおいて実行された侵害をワンクリックで修復することができます。

サブスクリプション機能比較

機能		CORE	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エア	○	○	○
	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	-	○	○
	アクセス制御（Firewall）	-	○	○
	脆弱性管理	-	○	○
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	-	-	○

ネットワーク要件

管理サーバー (SaaS)	
管理サーバー所在	AWS Tokyoリージョン
通信ポート	TCP/443 (HTTPS)
管理者	https://apne1-1001.sentinelone.net:443 https://www.google-analytics.com:443 https://cdn.pendo.io:443 https://data.pendo.io:443 https://sentry.io:443
エージェント通信要件	
エージェント接続先URL (共通)	https://apne1-100１1.sentinelone.net:443
Complete機能利用時のURL	https://dv-ap-prod.sentinelone.net:443 https://ioc-gw-prod-ap-1a.sentinelone.net:443 https://ioc-gw-prod-ap-1c.sentinelone.net:443
RSO機能利用時のURL	https://file-services-ap-northeast-1-prod.sentinelone.net:443 https://ap-northeast-1-prod-remote-scripts.s3.ap-northeast-1.amazonaws.com:443 https://ap-northeast-1-prod-remote-scripts-uploads.s3.ap-northeast-1.amazonaws.com:443
エージェント トラフィック量	
Windows OS	通信量 1日に4 - 8 MB（Completeの場合 +11 MB）
Mac OS	通信量 1日に2 - 4 MB（Completeの場合 +25 MB）
Linux OS	通信量 1日に13 -17 MB（Completeの場合 +52 MB）

管理画面対応ブラウザ
Google Chrome
Safari
Firefox
Microsoft Edge

エージェント要件　※2023年3月現在（最新情報はお問い合わせください）

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
Windows 10	Windows Server 2019
Windows 8 / 8.1	Windows Server 2016
Windows 7	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	
Windows Mobile / Windows 10 IoT Core	
64bit/32bit対応｜ ARM CPU非対応	

mac OS
macOS latest Beta (13)
macOS Monterey (12)
macOS Big Sur (11)
macOS Catalina (10.15)
macOS Mojave (10.14)
macOS High Sierra (10.13)
macOS 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
Virtuozzo 7, Scientific Linux 7,6, AlmaLinux 8.4-9.0, RockyLinux 8.4-9.0
Oracle 6.9-9.0
Fedora 25-30, 31(5.5.x), 32-36

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

ハードウェア最低要件

Windows　端末	
CPU	1GHz Dual-core
Memory	2 GB 以上
HDD容量	3GB 以上 10%以上の空き
ARM チップ非対応	

mac OS　端末	
CPU	1GHz dual core
Memory	2GB
HDD容量	2GB以上の空き
Intel/Apple チップ対応	

Linux 端末	
CPU	2GHz dual core
Memory	4GB
HDD容量	2GB以上の空き
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。
ppc64, 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) メモリ容量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 時間毎にVSSバックアップを取得します
ネットワーク	通信量 1日に4 - 8 MB（Complete の場合 追加で11 MB）程度
プロセス	Sentinel Service Host External Engines Sentinel Service Host Sentinel Static Engine Scanner SentinelOne Agent

プロダクトライフサイクル

メジャーバージョンのGAは毎四半期にリリースされます。

GA バージョン表記：[年].[1-4].[マイナーバージョン].[ビルド番号]（2022年Q1：22.1.2.1234）

各メジャーバージョンのライフサイクルは以下のとおりです。

エージェントバージョンのサポート期間	
GA バージョンのリリース後3ヶ月まで	不具合の原因特定及び回避策を提示し、次期バージョンにて修正を提供します。 緊急度の高い不具合に関して、同バージョンの SP 版にて修正を提供します。 ※ SP 版は約２週間サイクルでリリースがスケジュールされます。
GA バージョンのリリース後6ヶ月まで	不具合の原因特定及び回避策を提示し、次期バージョンにて修正を提供します。
GA バージョンのリリース後6ヶ月経過後	当バージョンはサポート終了（EOS）となり、サポートを受けるためには現在のサポートバージョンに更新頂く必要があります。
GA バージョンのリリース後15ヶ月経過後	当バージョンはサポート終了（EOL）となり、管理コンソールとの互換性や更新に対する保証が無くなります。

主な機能一覧

機能	詳細
Reputationエンジン	Sentinel Cloudデータベースと照合して検知
Static AIエンジン	脅威モデルによる静的検知
Behavioral AIエンジン	ふるまい検知エンジンによる検知
Documents, Scriptsエンジン	Excelマクロやバッチ処理の検知
Lateral Movement エンジン	侵入後の内部二次感染を検知
Anti Exploitation エンジン	マルウェアが侵入する瞬間の動きを検知
PUAエンジン (macOSのみ)	潜在的に問題のあるアプリを検知
Interactive Threat エンジン	対話型のコマンド脅威を検知
自動ファイル隔離	検知されたマルウェア本体を安全なフォルダに移動
自動・ワンクリック修復	マルウェアによる感染のおそれがある範囲のデータを除去
自動・ワンクリックロールバック	マルウェアに削除・書き換えられたファイルを復元 ランサムウェアの暗号化ファイルを復元
インシデントアラート機能	検知したアラートの情報をEmailで受信
Slackインシデント通知機能	検知したアラートの情報をSlack Webhookで受信
レポート機能	定期的な統計情報をPDF等で送信
Syslog機能	管理コンソールのログをSyslogで転送

機能	詳細
ハッシュ除外	ハッシュ値により誤検知を除外
証明書除外	コードサインにより誤検知を除外
パス除外	ファイルのパスで誤検知を除外
パフォーマンス・互換性除外	干渉・競合して不具合を起こすプロセスの監視除外
Firewall機能	Windowsのパーソナルファイアウォールを上書き制御
デバイス制御機能	USB・Bluetoothの接続を制御
条件付きFirewall	条件によって変動するFirewallを提供
アンチタンパー	セルフプロテクション機能によりSentinelOne自身とVSS領域をカーネルレベルで保護
タグ機能	エンドポイントを細かく分類するためのタグ機能
Deep Visibility	フォレンジックや脅威ハンティングを行うための機能
Rogue Device	SentinelOneをインストールしていない持ち込みPCやIoT機器を検知
アプリケーション脆弱性管理	アプリのインベントリから脆弱性のあるアプリを検出
シングルサインオン	SAMLプロトコルに対応
SentinelOne Market Place	XDR連携可能なサードパーティ製品との接続をワンクリックで完結するアプリマーケット。
Management API 2.1	SIEM製品などからアクセスしやすいフルオープンAPI

【SentinelOneサポートサービス】

sentinelOneを導入において様々なサポートサービスをご用意しております。

▶ 問い合わせサポート
メールによる各種問い合わせ対応

▶ 初期構築導入支援
sentinelOneの初期導入設定支援

▶ 運用標準化支援
運用ルール・ポリシー設定等の標準化支援

▶ ホワイトリスト登録支援
ホワイトリスト設定支援

▶ インシデントエスカレーション
検知済みインシデントの分析支援

▶ アクティブインシデント対応支援
インシデント検知時の調査・報告

▶ エージェントバージョンアップ代行
クォーター単位のバージョンアップ代行

▶ 月次レポーティング
レポートにより状況報告、リスクアセスメントを実施

お客様のご要望に合った支援のみをカスタマイズしてご提供致します。
ランサムウェア対策・感染後の対応など、お気軽にお問合せください。

日本の企業をICTのチカラでサポート！

株式会社
サンソウシステムズ

SentinelOneセールスチーム

メール：sentinel_sales@sansou.co.jp

〒110-0015
東京都台東区東上野2-1-11 サンフィールドビル
URL：http://www.sansou.co.jp/