SentinelOne

STARS

人より速く。
脅威より先に。

AIが実現する、自動対応型EDR
SentinelOne

SentinelOneとは

2,000+
Employees
従業員数

10,880+
Customers
導入企業数

NYSE
Listed
2021年6月 上場

24/365
Global Support
24時間365日サポート

本社
カリフォルニア州
マウンテンビュー

技術拠点
イスラエル・カリフォルニア・
ボストン・フランス

データセンター
アメリカ・ドイツ・
APAC（AWS GovCloud）



日本進出
2017年

スポンサー
アストンマーティン
F1チーム

FORMULA ONE® TEAM

PGAツアー
ゴルファー

SentinelOne

STARS

SentinelOne

導入実績

導入実績

SentinelOne

世界をリードする巨大エンタープライズ企業を保護

ASTON MARTIN	AUTODESK	cars.com	CENGAGE
EA	ESTĒE LAUDER	fiverr.	flex.
havas	HITACHI Inspire the Next	KENNETH COLE new york	McKESSON
NORFOLK SOUTHERN	norwegian	O'NEILL	POLITICO
SAMSUNG	Shutterfly	Sysco	workday

Fortune誌格付け
10中3 社で採用

グローバル企業
2000
社の数百社にのぼる企業

国内企業
600
社以上の団体や企業で導入

本社
カリフォルニア州
マウンテンビュー

技術拠点
イスラエル・カリフォルニア・
ボストン・フランス

データセンター
アメリカ・ドイツ・
APAC（AWS GovCloud）



日本進出
2017年

スポンサー
アストンマーティン
F1チーム

FORMULA ONE TEAM

PGAツアー
ゴルファー

SentinelOne

STARS

SentinelOne

信頼性（レポート）

信頼性 — Gartner社調査

SentinelOne

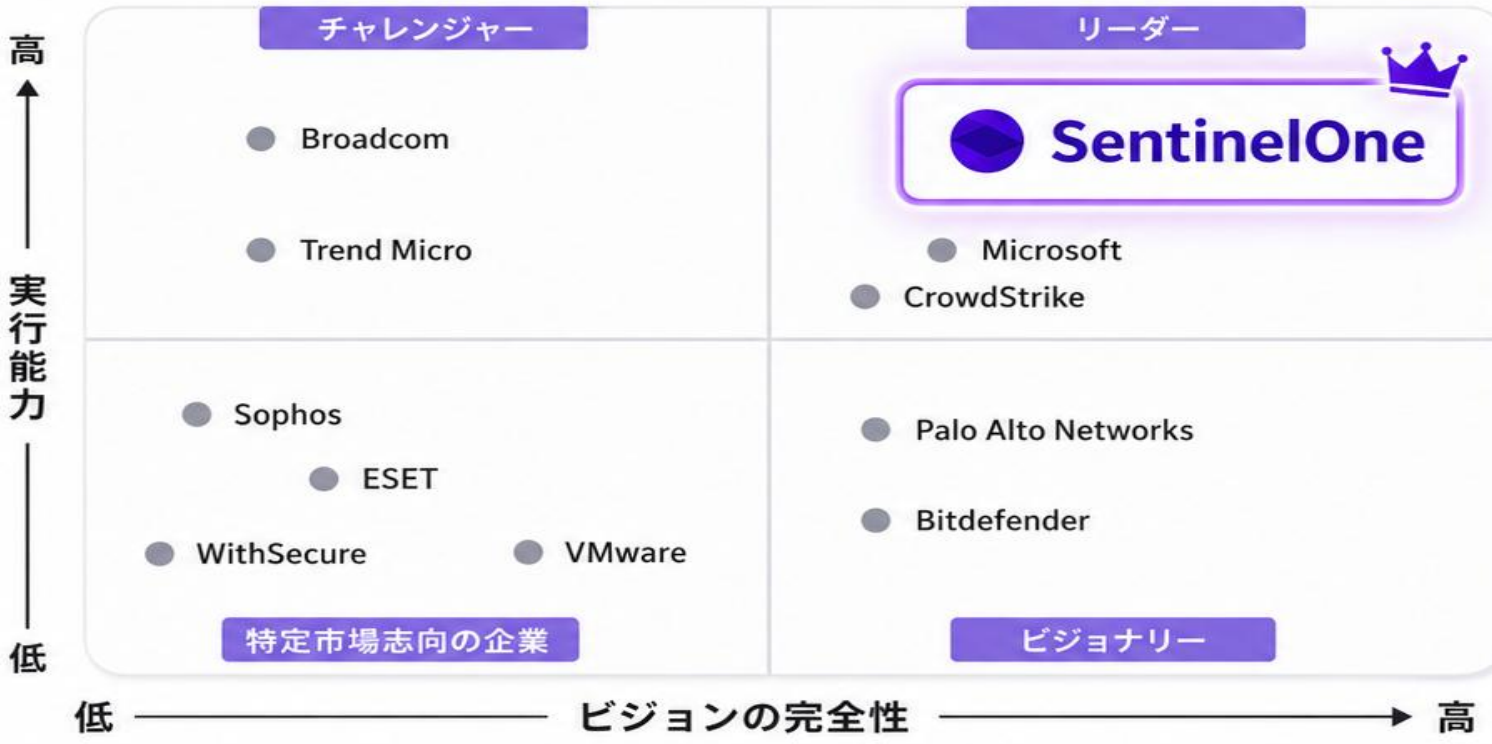
Gartner社が認めた最高評価のEDR

世界最大級のIT評価機関「Gartner」の調査でリーダー評価を獲得！

90+
導入国
世界中で選ばれている

Leader
最高評価
Gartnerリーダー評価獲得

AI
自動防御
AIで脅威を自動で検知・対応



業界トップ評価
Gartnerのリーダーに選出

世界90ヵ国以上
世界中の企業で導入

AIで脅威を自動検知
次世代の自動防御を実現

Gartner社調査 ― 評価ポイント

SentinelOne

Gartnerが認めた4つの強み

1
全ユースケースで
最高スコア

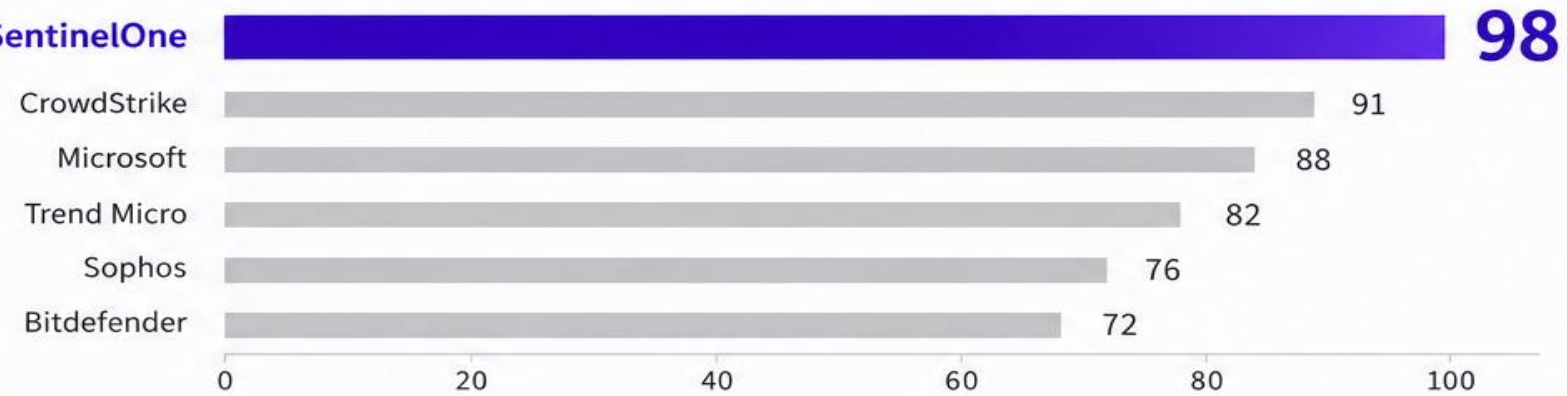
2
MDRへの投資拡大で
成長を加速

3
EDRの重要機能で
最高スコア

4
グローバル市場で
高いプレゼンス

Gartner評価スコア比較
(Endpoint Protection Platform部門)

SentinelOne
98
最高スコア



Gartner評価が重要な理由

- 世界中の企業が判断材料に活用
- 製品の実力を客観的に評価
- IT意志決定者の信頼が高い調査
- ベンダーに依存しない第三者評価
- グローバル基準の信頼性

信頼性 — MITRE社調査

SentinelOne

MITRE社は世界の脆弱性を管理する信頼の機関

脅威の原因を特定する「CVE-ID」を発行し、世界の安全を支えています



脅威の原因を特定

世界中の脅威を収集・分析し
原因を特定

信頼のセキュリティ基盤

世界中の企業や政府が利用する
安全の土台

世界中で利用

多くの企業や組織が
情報を共有して対策

MITRE ATT&CK — 100% Visibility達成

SentinelOne

MITRE ATT&CK 100% Visibilityを達成！

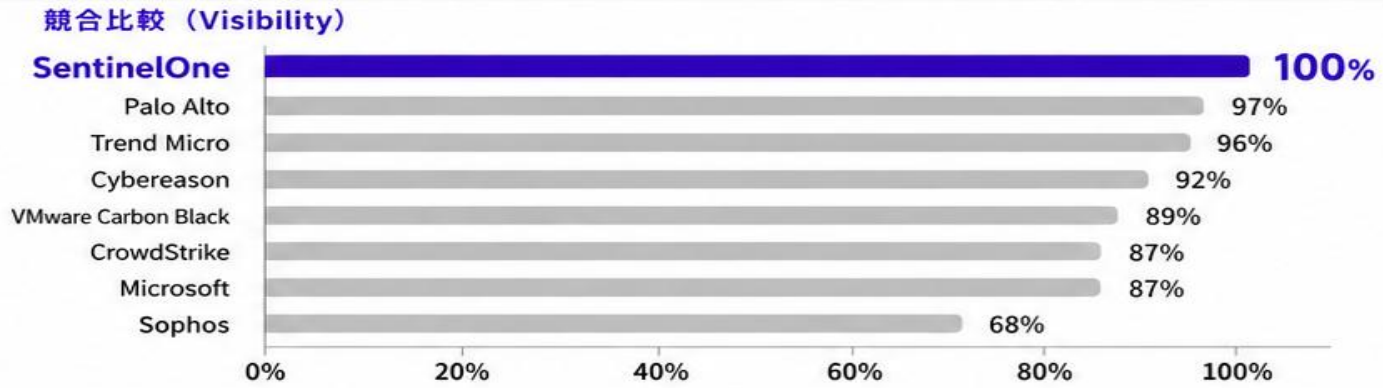
攻撃のすべてのステップを見える化し、確実に検知・対応します

100%の可視性
MITRE ATT&CK の全174ステップをカバー

最高の分析カバレッジ
全174ステップのうち159ステップを分析

遅延ゼロ
モディファイアの遅延なしで検知

構成変更ゼロ
設定変更なしですぐに利用可能



評価履歴

評価対象	評価年	Visibility（可視性ステップ数）
APT3	2018	101 / 136
APT29	2019	127 / 134
Carbanak+FIN7	2020	174 / 174

見逃さない
攻撃のステップを
すべて可視化

世界最高レベル
他社を上回る分析力で
検知・対応を強化

信頼の基準
MITRE公式フレームワークで
高い信頼性を確保

安心の実績
100%の可視性で
セキュリティを最適化

07 | MITRE調査 ー 誤検知が少ないEDR(2021)

SentinelOne

誤検知がとても少ないEDR No.1

本当に危ないものだけを、見逃さずに検知します

3つの「ゼロ」を達成！



イベント収集ミス
ZERO

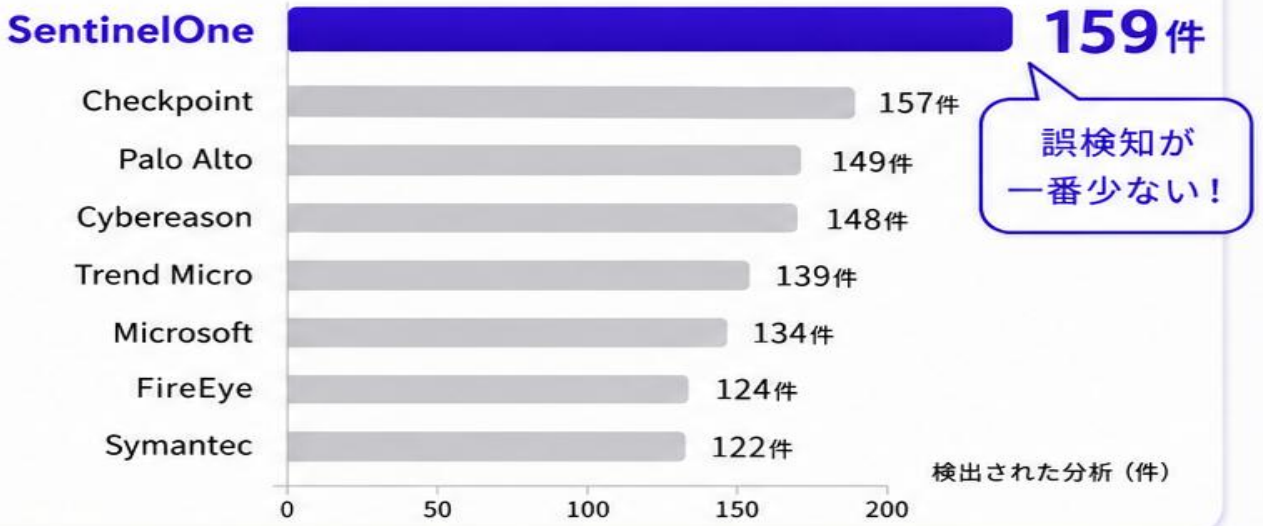


設定変更のミス
ZERO



遅延検知
ZERO

誤検知の少なさ No.1



だから安心！

迷わない・遅れない・間違えない
本当に信じられるセキュリティ

見逃さない
本当に危ないものだけを
しっかり検知

間違えない
余計な検知が少なく
運用がシンプル

すぐに見つける
リアルタイムで素早く検知
被害を最小化

業界トップクラス
世界の調査で
高い評価を獲得

MITRE調査 ― 誤検知が少ないEDR(2022)

SentinelOne

2年連続

誤検知がとても少ないEDR、No.1

本当に危ないものだけを、見逃さずに検知します

最高の分析能力
No.1



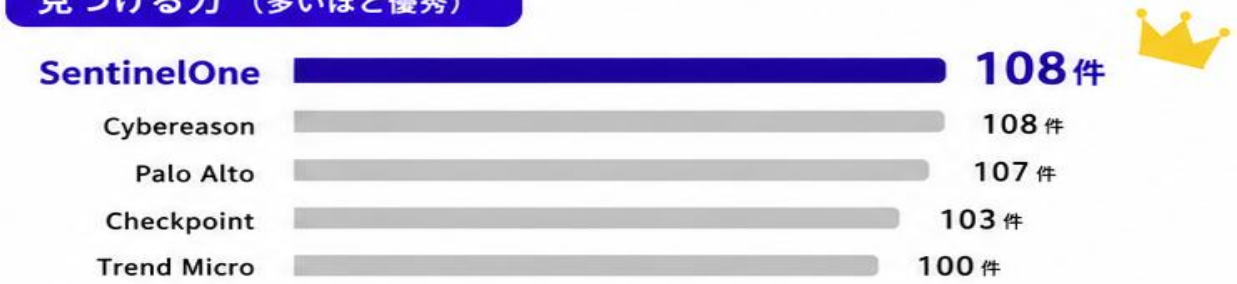
全ての脅威を
100%防御



検知の遅延
ZERO



見つける力 （多いほど優秀）



ムダな検知 （少ないほど優秀）



ムダな検知が
最小！

見逃さない
本当に危ないものだけを
見逃さずに検知

設定いらず
難しい設定やチューニングなしで
すぐに使える

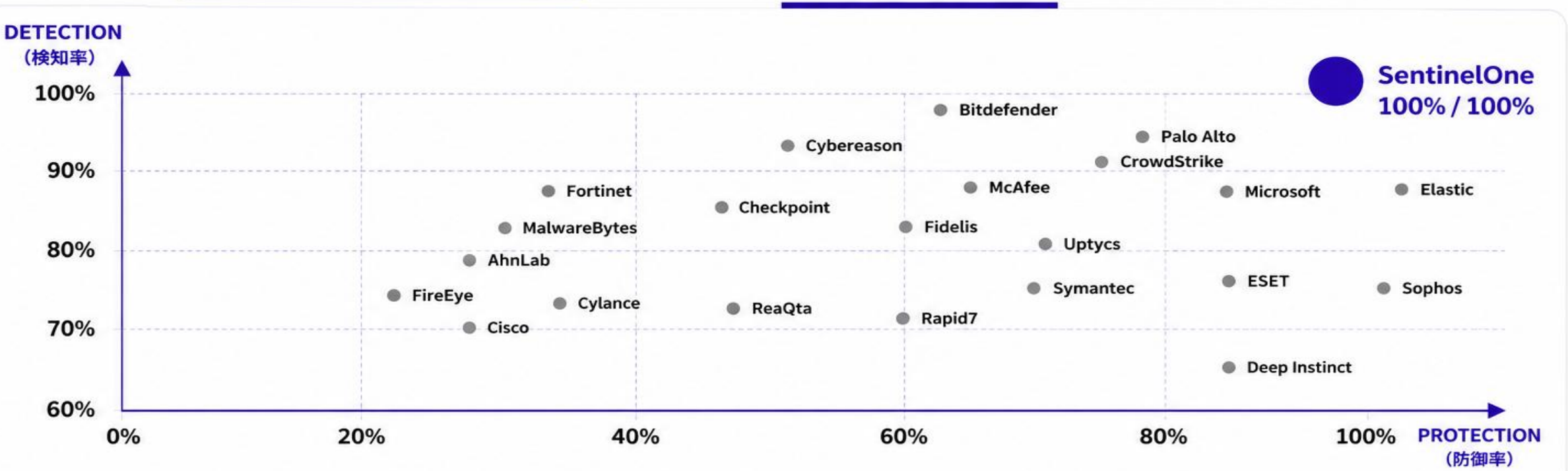
すぐに見つける
リアルタイムで素早く検知し、
被害を最小に

業界トップクラス
世界の調査で
トップ評価を獲得

MITRE FIN7試験 — 唯一100%達成

SentinelOne

セキュリティベンチマークFIN7試験の結果、SentinelOneのみが100%の検知を達成



FIN7試験とは？

実在する攻撃グループFIN7が使用する
攻撃手法を再現し、製品の検知・防御能力を
評価するMITRE主導のベンチマークです。

検知率（DETECTION）

攻撃の兆候をどれだけ
正確に見つけられたか
を測定します。

防御率（PROTECTION）

攻撃をどれだけ
ブロックできたか
を測定します。

右上が理想のポジション

検知も防御も100%に近いほど、
セキュリティ製品としての
総合力が高いことを示します。

SentinelOneは唯一の100%/100%を達成

検知・防御の両面で他社を圧倒する
最高レベルの保護能力を証明しました。

MITRE調査 ― SentinelOne検知結果

SentinelOne

MITRE調査で実証された、SentinelOneの圧倒的な検知能力

1

100% Protection

100%

9種類のMITRE ATT&CKテストのうち
9種類すべて防御成功

2

100% Detection

100%

19段階の攻撃ステップのうち
19段階すべて検知

3

100% Real-Time

100%

検知の遅延時間ゼロ
（0 Delays）

4

99% Visibility

99%

109段階の攻撃サブステップのうち
108段階を可視化

5

99% Highest Analytic Coverage

99%

109種類の検知のうち
108種類を分析

攻撃を見逃さない
100% Detectionで
攻撃を確実に検知

気づくのが遅れない
0 Delaysで
攻撃を即時検知

何が起きたか把握できる
99% Visibilityで
攻撃の全体像を可視化

AIが攻撃を正しく分析
99% Analytic Coverageで
攻撃内容を正確に理解

現実の攻撃にも強い
100% Protectionを連成し
最高レベルの防御を実証

一言まとめ

「見つける・理解する・止める」

この3つを高いレベルで実現できることが、
SentinelOneが世界中で評価される理由です。

SentinelOne

STARS

SentinelOne

EDR概要

EDR概要 ― エンドポイントの検知と対応

SentinelOne

Endpoint Detection and Response ＝ エンドポイントの検知と対応

侵入を“許さず”、被害を“拡大させず”、致命傷を“回避”する

攻撃発生から被害を防ぐまでの流れ

1 **侵入**
攻撃者が社内に侵入

2 **発見**
異常な動きを
早期に見つける

3 **対処**
脅威を止めて
被害の拡大を防ぐ

4 **致命傷回避**
被害を最小限に抑え
業務を守る

5 **復旧・継続**
安全を確保し
業務を継続

EDRを導入するメリット

- 攻撃を早く見つける
- 被害を最小限に抑えられる
- 業務停止を防げる
- ランサムウェア対策になる

SentinelOne

STARS

SentinelOne

EPPとEDR比較

EPPとEDR比較 ― 従来製品の現状

SentinelOne

EPPは防ぎきれない攻撃が半数以上存在

EPP（従来のアンチウイルス）

ウイルス対策ソフトで
約45%をブロック

防げない攻撃が55%

- Emotet（なりすまし）
- ランサムウェア（暗号化）
- ハッキング（不正アクセス）



EDRの役割

- 侵入後の検知
- 被害の拡大を防止
- 迅速な対応を実現

**EDRは「侵入を防ぐ」だけでなく
「侵入後の検知と対応」で被害を最小化する仕組みです**

EPPとEDR ― 世代比較

SentinelOne

セキュリティは、EPPからEDRへ

EPP（従来のアンチウイルス）

防御 → 入口でブロック

検知後は → 対応できない

既知の脅威にしか対応できない

EDR（第4世代）

❶ 検知 → 侵入を見抜く

❷ 対応 → 被害の拡大を防ぐ

❸ 復旧 → 素早く復旧

❹ 強化 → 再発を防止

侵入を見抜き、被害を最小化し、元に戻す

EDRがもたらす価値

- 攻撃を早期に検知
- 被害の拡大を確実に防止
- 迅速な対応で業務を継続
- 継続的な強化で再発を防止

EDRは、「見つける・止める・元に戻す」を実現する次世代のセキュリティ

EPPとEDR — 詳細機能

SentinelOne

SentinelOneは、EPP（防御）＋ EDR（検知・対応）をワンストップで提供

EPP（マルウェア防止）

侵入前検査
ファイル・コードスキャン

早期検知
ふるまい検知（AI）

防御
マルウェアをブロック

SentinelOne

EDR（侵入後の対応）

調査
リアルタイムで可視化

対応
攻撃の全体像を把握

復旧・強化
被害を最小化し再発を防止

EPPとEDRを1つに統合

- 侵入を防ぐ
- 素早く見つける
- 被害を最小化
- 確実に元に戻す

「防ぐ」だけでなく、「見つける・調べる・復旧する」まで自動で対応

用語補足

SentinelOne

セキュリティでよく使う言葉を、やさしく説明します！

定期ファイル



決まった時間に
ファイルをチェック！

パターンマッチング



悪いものの形を見つけて
似ているものを探す！

サンドボックス



あやしいものを安全な箱に入れて
動きをかくにん！

レビューテーション



みんなの評判から
安全かどうかを判断！

スタティックAI



ファイルを開く前に
AIがチェック！

ダイナミックAI



実際に動かしてみて
AIがかくにん！

ラテラルムーブメント



悪い人がネットワークの中で
横に広がる動きを見つける！

アタックストーリーライン



攻撃者がどう動くかを
つなげて見える化！

ロールバック



元の安全な状態に
もどすこと！

こんな流れで守ります！



見つける
（検知）

→



止める
（対応）

→



調べる
（原因を確認）

→



元にもどす
（復旧）



「見つける・止める・調べる・もどす」まで、自動でやってくれます！

EPPとEDR ― エンドポイント世代の移り変わり

SentinelOne

セキュリティは、ここまで進化しました！

昔のウイルス対策

入り口を守るだけ

McAfee　Symantec



- 決まったウイルスしか見つけられない
- 中に入られると気づけない
- 直すのがむずかしい

今までのEDR

中を見て、気づいてくれる

Microsoft　CORTEX BY PALO ALTO NETWORKS

vmware Carbon Black　CROWDSTRIKE



- プロが見てくれるから安心
- たくさんの記録をためてくれる
- 直すのに時間がかかることも

SentinelOneのEDR

次の時代のスタンダード！

AIがずっと守ってくれる

SentinelOne

- AIがいつもパソコンを見守る
- 人がいなくても自動でチェック
- 中に入られてもすぐに気づく
- すぐに自動でブロック（止める）
- やられた後も、もとに戻せる

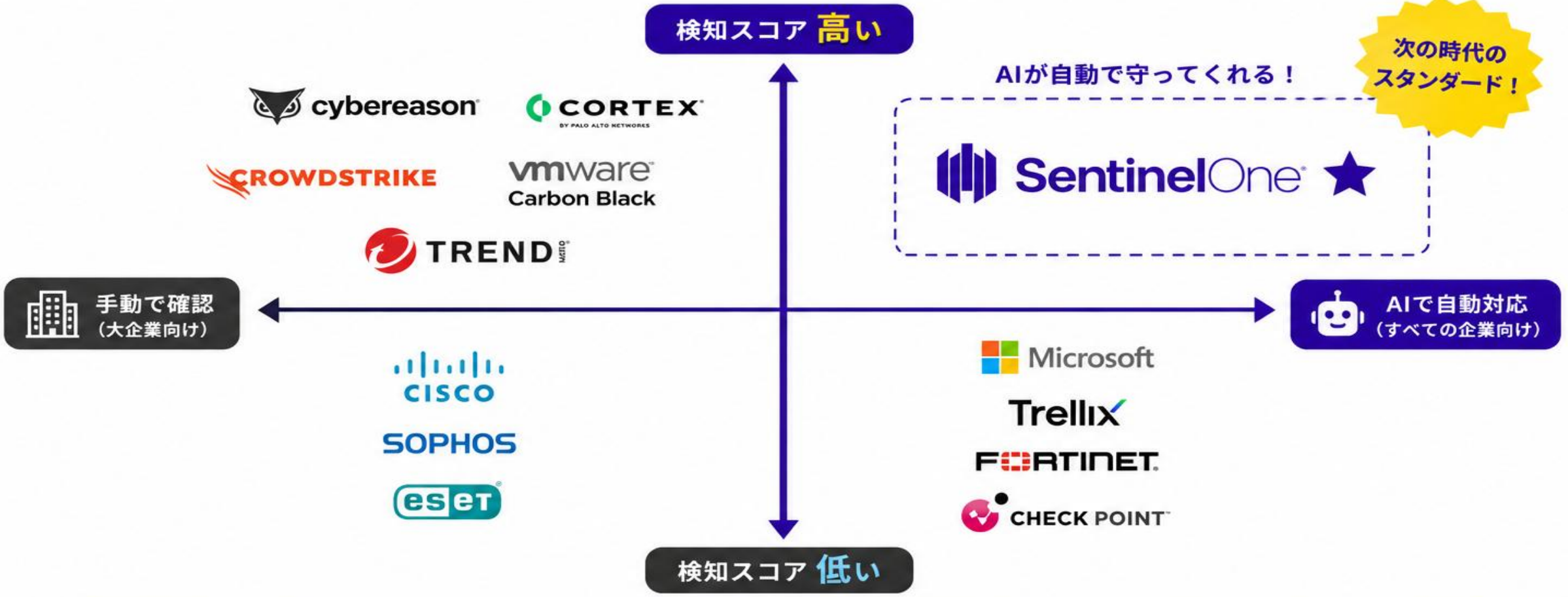
これからのセキュリティは、

「見つける→止める→直す→もどす」まで、AIが自動でやってくれます！

EPPとEDR ― 検知スコア比較（参考）

SentinelOne

検知力で選ぶなら、SentinelOne！



これからのセキュリティは、AIで「見つけて・止めて・自動で守る」時代へ！

SentinelOne

STARS

SentinelOne

サービス特徴

サービス特徴 ― 3つのコア技術

SentinelOne

3つの技術で、攻撃からあなたを守ります！



01 対策実行型 XDR



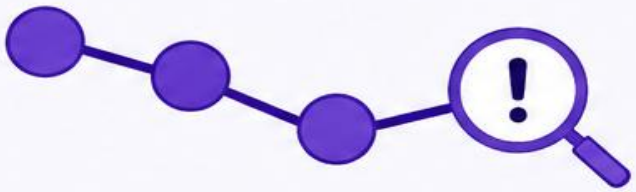
- 悪いものをすぐ見つける
- すぐに止めて直せる
- いろんなパソコンに対応

02 分散型 AI



- たくさんの場所でAIが見守る
- いらない集中管理はしない
- 強い攻撃もAIで見抜く

03 Storyline™



- 攻撃の流れを自動でつなぐ
- 見やすい形で分かりやすく
- 長い時間のデータもまとめる

これからのセキュリティは、
「見つける → 止める → 直す」まで自動でやってくれます！



サービス特徴 ― 圧倒的スピード

SentinelOne

圧倒的なスピードでウィルスを駆除、正常化に戻します

	水際対策	① 感染検出	② 調査	③ 封じ込め	④ 修復
従来型 ウィルス対策	水際ブロック	すり抜け	× 対応不可		
従来型 EDR	水際ブロック	検出	1時間	1時間	1時間
自動型EDR SentinelOne	水際ブロック	すり抜け→インシデント発生	検出	1秒	1分 → 1分

超高速解決

スピードが違うと、被害が変わります！

感染の初期段階で検出し、すぐに対応することで、被害の拡大を防ぎ、ビジネスへの影響を最小限に抑えます。

- 早い検出で被害を最小化
- 業務停止時間（ダウンタイム）をゼロに近づける
- 安心・安全なビジネス環境を実現

サービス特徴 ー スピード解決イメージ

SentinelOne

自動だから、すぐ直る！

事故が起きてから元どおりになるまでの時間

一般的な手動型EDR



自動型EDR SentinelOne



自動だから安心！

- 早く見つける
- すぐに止める
- すぐ元どおりに



サービス特徴 ― 自動化の優位性

SentinelOne

ぜんぶ自動だから、すぐに元どおり！

AIが最初から最後までやってくれる！

一般的な手動型EDR

1 見つける → 2 隔離する → 3 調べる → 4 直す → 5 元に戻す

時間がかかる…

5分～60分

自動型EDR SentinelOne

1 見つける → 2 自動で隔離 → 3 AIが調べる → 4 自動で直す → 5 自動で復元

ぜんぶ自動で

たったの1分！

早く見つける
すぐに気づいて守る！

すぐに止める
広がる前にブロック！

すぐに元どおり
ビジネスを止めない！

自動型EDR「SentinelOne」なら、AIが最初から最後まで守ってくれる！

サービス特徴 ― 競合他社との機能の違い

SentinelOne

SentinelOneは、難しいことを自動でやってくれる“見守り番”！

みんなのパソコンやデータを、まるごと守ります。

SentinelOneのすごいところ

- **自動で守る！**
  ウイルスやトラブルを自動で防いでくれる
- **はやく見つける！**
  あやしい動きをすぐに見つける
- **すぐに知らせてくれる！**
  大事なアラートをすぐに教えてくれる
- **パソコンが重くならない！**
  使っていてもサクサク動く
- **ぜんぶまとめて安心！**
  いろんな機能がひとつに入っている



SENTINELONE
がまもるよ！

他の会社の困りごと

- **手でやるからミスがこわい**
  人がやるから、見逃しがあるかも…
- **見つけるのがおそい**
  気づいたときには、もうおそいかも…
- **大事な知らせを見逃すかも**
  たくさんのアラートで、わからなくなる…
- **パソコンが重くなることも**
  動きが遅くなって、使いにくい…
- **いろいろなツールがバラバラ**
  たくさんのツールを使い分けるのが大変…

- **まるごと自動で守るから安心！**
  ウイルス・不正アクセス・情報漏えいを
  ぜんぶまとめてガード！
- **安全なのにサクサク快適！**
  仕事や勉強のじゃまをせず、
  パソコンを軽く保つ！
- **専門の人がいなくても大丈夫！**
  かんたんに使えて、はじめてでも安心！

★ 「人を増やさず、セキュリティレベルを上げる」 それがSentinelOneの大きな価値です！

サービス特徴 ー SentinelOneが最適な企業

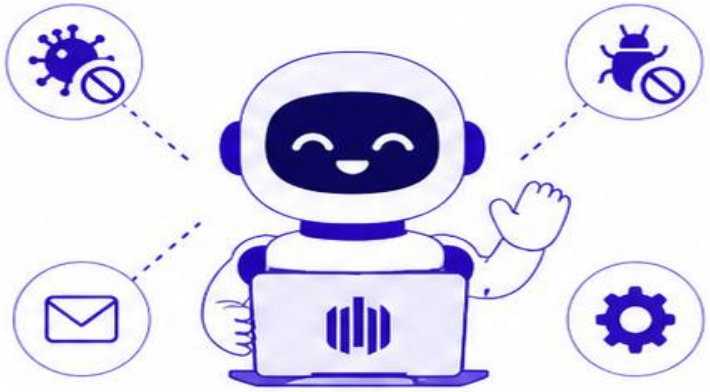
SentinelOne

あなたの会社のセキュリティの悩みを まるごと解決！

どんな環境でも安心

- 会社の大きさに関係なく使える
- インターネットでも社内ネットでもOK
- オフィスでもテレワークでも守れる
- 専門知識がなくてもかんたんに使える

AIが自動で守ってくれる



- 検知（見つける）
- 隔離（止める）
- 修復（直す）
- 復元（元に戻す）

＼ すべて自動でおまかせ！ ／

こんな悩みをまるっと解決

- 攻撃を止めたい・被害を最小限にしたい
- いろいろなソフトを1つにまとめたい
- 業務を止めずに早く復旧したい
- 担当者が少なくても運用したい
- セキュリティ運用をもっと楽にしたい
- たくさんのセキュリティ製品をまとめたい
- テレワーク環境もしっかり守りたい

多くの企業で利用されています ▶ AIが自動ですべて対応 ▶ 人手が少なくても安心して運用可能 ▶



「専門担当者がいなくても守れる」 それが SentinelOne の大きな強みです。

SentinelOne

STARS

ご覧いただきありがとうございました

お気軽にご相談ください。

info@stars203.com

http://stars-hp.website/

090-9880-0922

お問い合わせはこちら →