SentinelOne

データシート

Singularity™ EPP+EDR

防御、検知と対応、フォレンジック調査を統合

Gartner

Gartner、SentinelOneをリーダーに選定
2021年Gartner Magic Quadrant、エンドポイント保護プラットフォーム部門

攻撃の規模、スピード、巧妙さが進化を続け、第１世代の防御とEDRソリューションが既に時代遅れになっています

攻撃者が防御策をすり抜けたその瞬間から、ネットワーク接続の有無にかかわらず、エンドポイントで、リアルタイムで自律的な脅威検知とインシデント対応を開始する必要があります。 次世代の防御とEDR機能を1つのSentinelエージェントに統合したSentinelOne Singularity EPP+EDRなら、自律的にマシン速度で対策が実現できます。

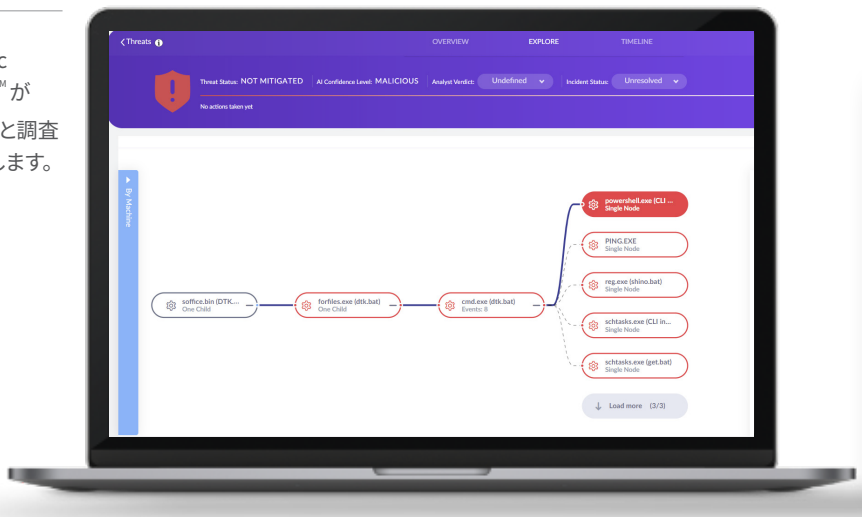
Deep Visibility™ & ActiveEDR™搭載

ActiveEDRが、振る舞いAIによりマシン上で不正プロセスを特定しイベントを相関分析してタグ付けします。自動的に攻撃Storyline™が構築され可視化されるので調査を加速できます。保護モードでは、攻撃を特定するだけでなく、感染を自動的に阻止します。さらに、不正な変更があったとしても、特許取得済みのワンクリック修復を使えば、スクリプトを組むことなく、アナリストがマシンを攻撃前の状態に戻すことができます。

堅固なフォレンジクス
直観的なシンプルさ

EDRは専門家でなければ使いこなせないという常識が覆されました。次世代EDRが、脅威検知とインシデント対応のMTTR（平均修理時間）を削減し、生産性を最大化します。データセンターやクラウドサービスプロバイダー、オフィス、リモートワークなど場所を問わず、すべてのOSや環境を対象に、あらゆるイベントをAIが常に監視します。一目瞭然の脅威ハンティングとフォレンジック調査結果が自動的に提供されます。誰でも簡単に習得できるので、脅威ハンティングとても身近になります。

Automatic Storyline™ がトリアージと調査を迅速化します。



SINGULARITY EPP+EDR

マシン速度で自律的なAI搭載の防御とEDR

主な機能

+ 自律的な統合EPP/EDR
+ EPPのみ、EDRのみ、複合モードを同一製品で提供
+ Linux、macOS、Windows、Kubernetes、Docker対応
+ オンライン/オフラインで保護、脅威検知とインシデント対応
+ Storylines自動イベント相関分析
+ 特許取得済みのワンクリック修復&ロールバック
+ MITRE ATT&CK®フレームワークによる攻撃TTPを実装
+ 柔軟なEDRデータ保持期間、オプションで14日-365日以上
+ すべてのOS対応のリモートフォレンジクス

Gartner peerinsights™

すぐれた顧客サービス、さらにすぐれた製品

★★★★★

IT部門シニアディレクター
医療

主な機能

- 複雑な脅威に対して**自律的にリアルタイムに**検知と修正を人的介入なしに実行します。
- Windows、Linux、macOSを対象に**妥協のない保護** - 物理、仮想、コンテナ、クラウド、データセンターなどどこでも対応します。
- **トリアージの迅速化および根本原因分析** インシデントインサイトおよび市場最高のMITRE ATT&CK® 連携によりMDRの有無にかかわらず実現しています。自動で相関分析と調査を実施するStoryline™。
- **ワンクリック修復 & ロールバック** インシデント対応を簡略化し、MTTR（平均修理時間）を削減します。
- **直観的なユーザーエクスペリエンス** 深い可視性、S1QLおよびSTAR™（Storyline Active Response）によって、セキュリティ運用における脅威ハンティング業務に高度なスキルが必要なくなります。
- **データ保持オプション** 14日から365日以上のあらゆるニーズに適合します。
- **迅速に導入可能** 相互運用性機能によって、高速でスムーズな展開が保証されます。
- **統合脅威インテリジェンス** 主要なサードパーティおよび当社専用ソースから提供される検知およびエンリッチ化に対応します。

READY FOR A DEMO?

詳細については、SentinelOneのウェブサイトをご覧ください

主な利点

+ 滞留時間削減
+ 迅速なインシデントレスポンス
+ MTTRの低減
+ アラート疲れの軽減
+ アナリスト生産性の向上
+ Singularity プラットフォームコンポーネント

MDRサービス

Vigilance MDRを利用することで、お客様はより重要な業務に集中できるようになります。多忙を極めるIT/SOCチームにとってまさに完璧なエンドポイント向けアドオンソリューションです。

2020年 MITRE ATT&CK
- 最小のミス
- 最大の相関
- 最高のデータエンリッチ化範囲

EPP部門で2020年 GARTNER MQ受賞
- リーダークアドラント
- Gartner定義の顧客プロファイルタイプの3つすべてで重要な機能の最高スコア獲得

2020年 FORRESTER WAVE™ EDR
「強力なパフォーマー」

2020年 KUPPINGERCOLE MARKET COMPASS
注目のEPDRイノベーター

SentinelOneはお客様を最も大切に考えています

継続的な測定と改善こそが、お客様の期待を超えるための推進力となっています。

Gartner peerinsights customers' choice™

97%
Gartner Peer Insights™の「お客様レビュアーの声」はSentinelOneを推奨

97%
顧客満足度

FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA

TEVORA
PCI DSS証明書
HIPAA証明書

Gartner peerinsights 4.9 ★★★★★

SentinelOne について

SentinelOneのサイバーセキュリティソリューションは、単一の自律型XDRプラットフォームにより、AIを活用して、エンドポイント、コンテナ、クラウドワークロード、IoTデバイス全体の防御、脅威検知、インシデント対応、および脅威ハンティングを提供しています。

jp.sentinelone.com
sales-japan@sentinelone.com
050-5213-0260

S1-SNGL-EPP-EDR-10022021