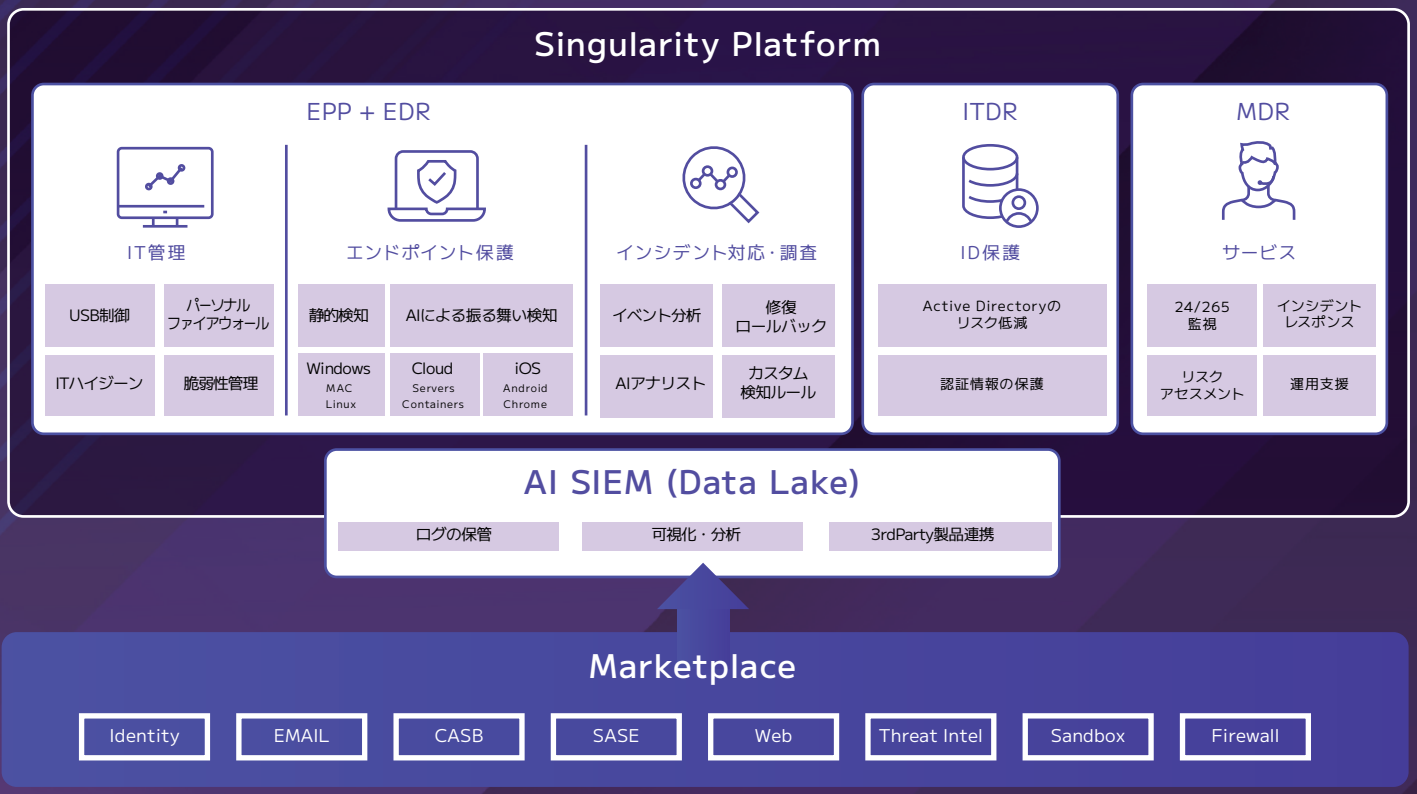
SentinelOne

セキュリティ担当者の運用負荷を解放する



SentinelOneを導入する3つのメリット

EDRに注目が集まる一方で、同製品が発するアラートの分析や対処には専門性が求められ、扱いづらいという課題があります。そうした課題を解消するのが、洗練されたAIを活用した防御と検知、高度な自動対応機能を備える自律型エンドポイントセキュリティ製品であるSentinelOneです。

多段のエンジンで高い検知力を実現

ファイル構造解析（NGAV）、振る舞い検知エンジン（EDR）を標準実装しています。 そのため、近年流行しているランサムウェアやファイルレス攻撃に対しても高い防御力や検知力を有します。第三者評価MITRE Engenuity ATT&CK Evaluationsでは検知漏れ0%を示しています。

専門的なスキルがなくても運用が可能

ポリシー設定がシンプルで、複雑なチューニングは不要。インストール後速やかに運用を開始できます。クラウド管理コンソールの利用により、煩雑なサーバー管理やシグネチャの管理が不要です。
また、管理コンソールは日本語表示に対応しています。

人手に頼らないインシデント対応で負荷を軽減

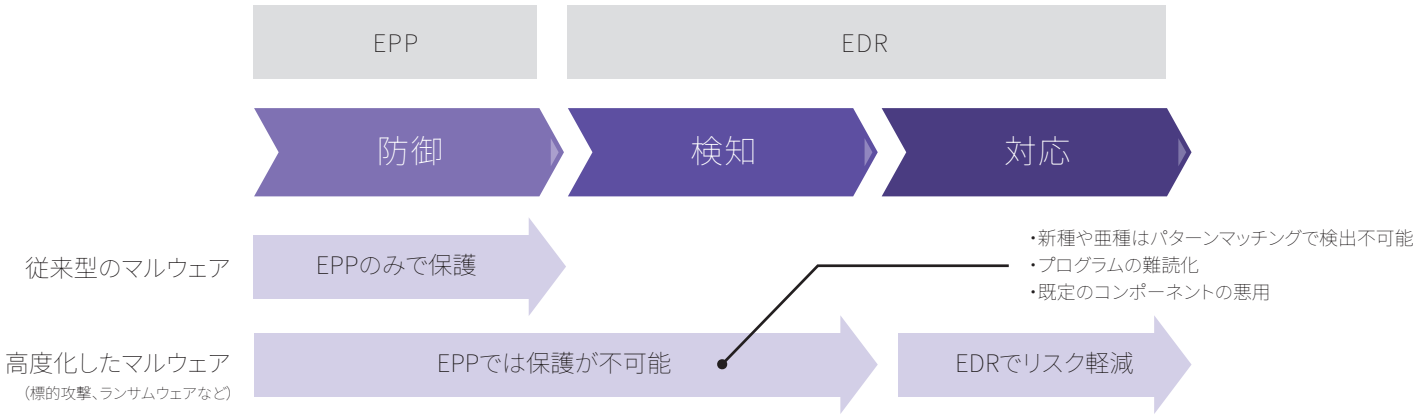
端末内の挙動分析が自動化されているため、高度な攻撃も自律的かつ即時に対応可能。検知・防御・隔離まで一貫して実行します。
さらに万が一、汚染や暗号化をされた場合でもワンクリックで元通りにできる修復機能を実装しているため速やかに業務を継続することができます。

エンドポイントの保護をさらに強化

SentinelOne × 東京エレクトロン デバイス

EPP ＋ EDRが必要な理由　～ いまなぜEDRが必要なのか ～

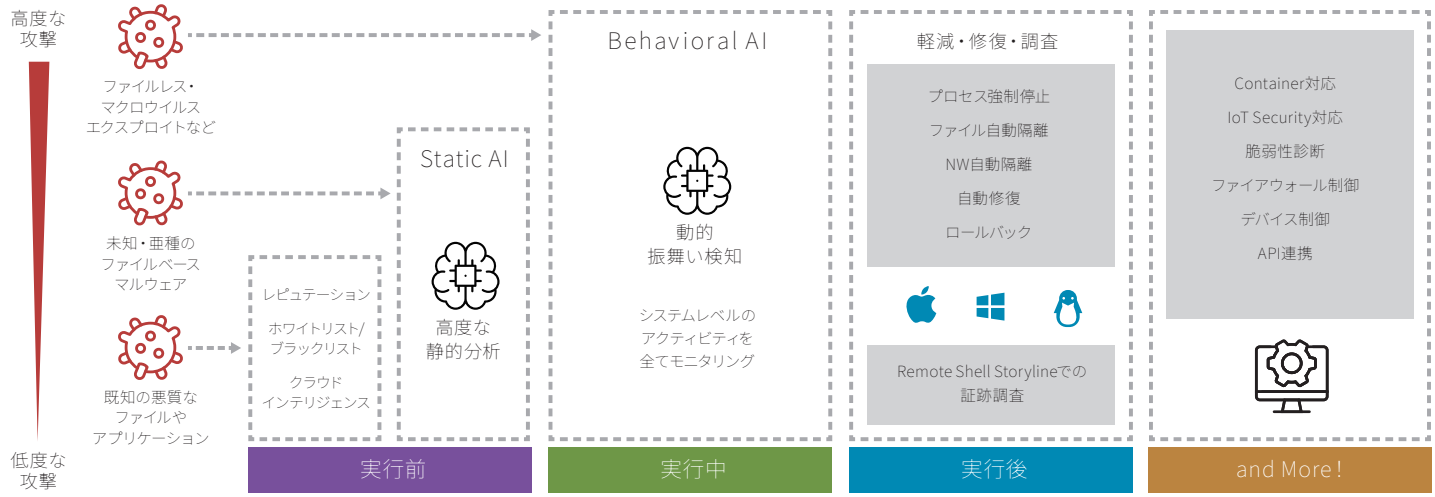
従来のエンドポイントセキュリティはEPPによる防御機能に頼ることが一般的でした。
しかし、攻撃の高度化に伴って脅威の侵入を完全に防ぐことが困難になったいま、感染後にいち早く感知できるか、
また脅威が見つかった後に迅速に対応できるかという観点からの対策が求められます。



EPPとEDRの役割と機能

	防御（EPP）	検知（EDR）	対応（EDR）
機能	パターンマッチングやNGAV（次世代アンチウイルス）でエンドポイントを保護	EPPが検出できなかった攻撃を振る舞い分析で検知	ネットワークからの分離、マルウェアの隔離、汚染箇所の修復

SentinelOne 製品の特徴



お問い合わせは、Webサイトの右記フォームよりお願いします。
https://cn.teldevice.co.jp/product/sentinelone/form.html

東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp/

本社：〒150-6234 東京都渋谷区桜丘町1-1 渋谷サクラステージ SHIBUYAタワー35階
大阪 ：〒540-6033 大阪府大阪市中央区城見1-2-27 クリスタルタワー33階
名古屋：〒451-0045 愛知県名古屋市西区名駅2-27-8 名古屋プライムセントラルタワー8階