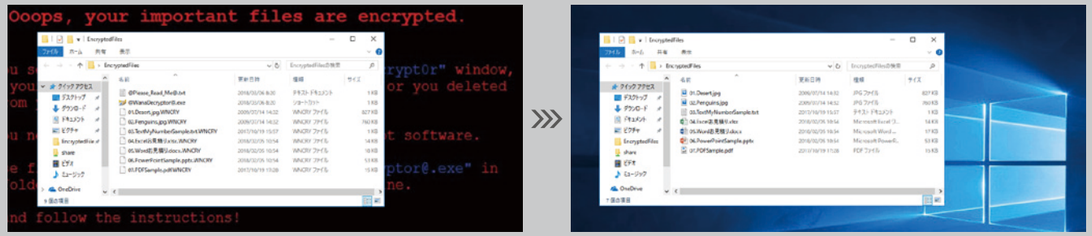
ランサム感染時のロールバック機能（Windows）

VSS（ボリューム・シャドー・コピー・サービス）を利用し、暗号化されたファイルのロールバックが可能です。

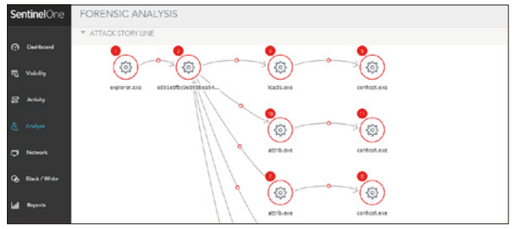


250以上のAPIを提供

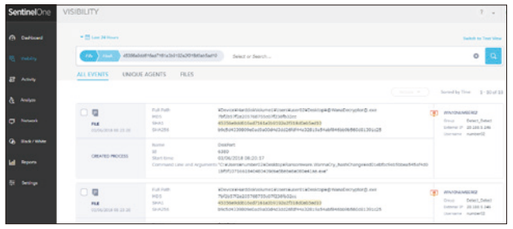
SentinelOneは250以上のAPIを提供して、幅広いセキュリティ製品群と連携できます。
これにより既に所有しているセキュリティ製品とエコシステムを形成することが可能となりました。

Firewall　SIEM　Mobile　CASB　Orchestration　Platform　Threat Intel　IT Ops

端末内のアクティビティを可視化



外部からの攻撃の様子をストーリーラインで表示



Deep Visibility機能でIOC情報を収集

USER'S VOICE

事例 1　大手化粧品メーカー

毎週8〜10台に上る感染端末の復旧作業は100時間にも及んでいました。従来型のAVソフトは全く効果を発揮しませんでしたが、SentinelOneを導入することにより劇的に改善されました。

事例 2　大手建設会社

私たちはセキュリティのスペシャリストを雇うことなく、自身で導入し、維持できるセキュリティソリューションを探していました。SentinelOneだけがその要求に答えてくれました。

東京エレクトロン デバイス株式会社
CNカンパニー
http://cn.teldevice.co.jp
新宿：〒163-1034 東京都新宿区西新宿3-7-1 新宿パークタワー S34階
Tel.03-5908-1990　Fax.03-5908-1992
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
Tel.06-4792-1908　Fax.06-6945-8581
つくば：〒305-0033 茨城県つくば市東新井15-4 関友つくばビル 7階
Tel.029-848-6030　Fax.029-848-6035
お問い合わせは、Webサイトの下記フォームよりお願いします。
https://cn.teldevice.co.jp/product/sentinelone/form.html

SentinelOne™

東京エレクトロン デバイス

EPP＋EDRという必然

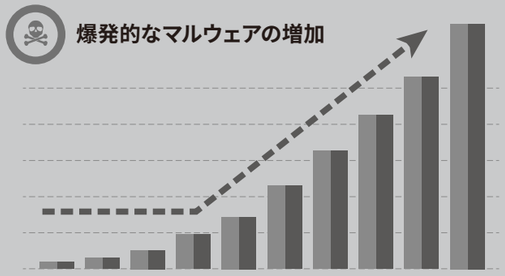
SentinelOne Endpoint Protection Platform

引き続き主要な攻撃目標であり続けるエンドポイント。そしてひとたびインシデントが発生すれば、企業の貴重な『時間』が失われてしまう事実。
「SentinelOne Endpoint Protection Platform」は、洗練された機械学習による防御と検知、高度な自動対応をマシンスピードで実現する自律型エンドポイントセキュリティ製品です。

課題　高度な外部脅威からエンドポイントは守られているか？

課題 01

爆発的なマルウェアの増加



課題 02

悪質化するランサムウェア

- □ **個人・企業を問わず**攻撃の対象に
- □ 要求される身代金の**平均額が増加**
- □ 身代金要求型ではない**破壊型ランサムウェア**の登場
- □ **Ransomware as a Service（RaaS）**等のエコシステム

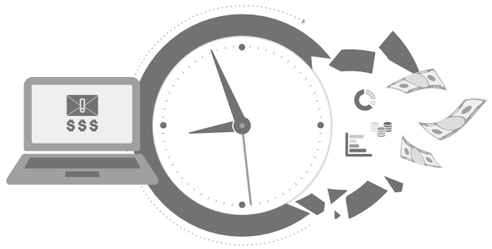
課題 03

ファイルレス攻撃の台頭

- □ **メモリ上にのみ存在**する攻撃手法
- □ **Powershell**の悪用
- □ ファイルベース解析の**無力化**
- □ ファイル型に比べ**高い攻撃成功率**

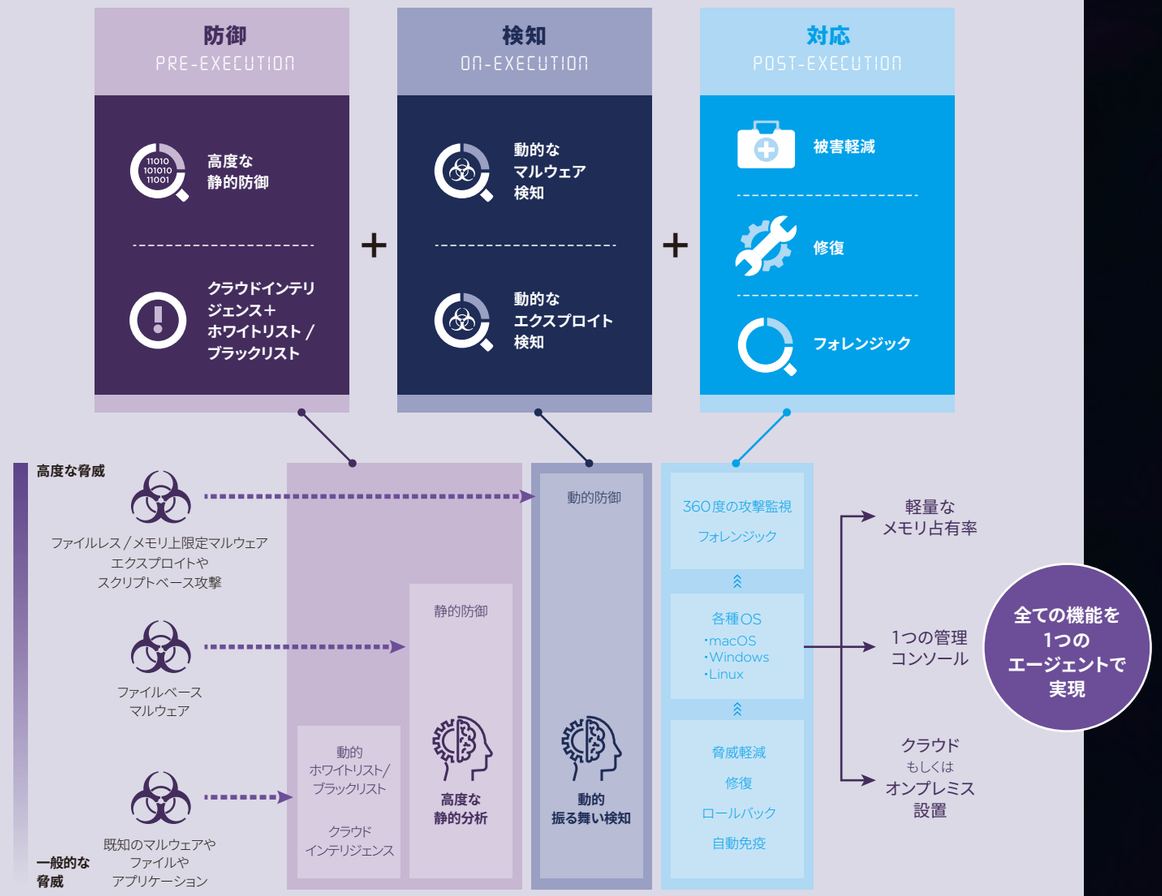
そして、ひとたびインシデントが発生すれば
貴重な『時間』が失われてしまう

失った『時間』は取り戻せない



解決　SentinelOne Endpoint Protection Platformでの脅威のライフサイクルへのマルチレイヤーアプローチ

SentinelOne Endpoint Protection Platformの概念



セキュリティ対策に求められるあらゆる機能を完備

防御
PREVENTION
既知・未知問わず、ファイルベースマルウェアがエンドポイントのディスクに書き込まれたタイミングで機械学習エンジンによりブロック

検知
DETECTION
ユーザーレベル・カーネルレベルの全アクティビティを監視。機械学習エンジンによりエクスプロイト、ファイルレス、高度なマルウェアの振る舞い等を自動的に検知

軽減
MITIGATION
プロセスの強制終了、ファイル隔離、端末のネットワーク切り離し、アラート通知を即時実行

修復
REMEDIATION
改変・追加されたレジストリキー、ファイル、スケジュールタスク等を迅速に自動復旧。ランサムウェアに暗号化されたファイルの復旧までも実現

調査
FORENSICS
開始から終了までの攻撃内容を360度リアルタイムで記録、コンテキストを取得