HITACHI
Inspire the Next

SentinelOne
ご説明資料

株式会社 日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

Contents

1．近年の動向

1．近年の動向 -情報セキュリティ10大脅威2024-

HITACHI
Inspire the Next

『情報セキュリティ10大脅威2024』では「ランサムウェアによる被害」の順位が1位（9年連続ランクイン）

- 情報セキュリティ10大脅威2024

1位	**ランサムウェアによる被害**	6位	不注意による情報漏えい等の被害
2位	サプライチェーンの弱点を悪用した攻撃	7位	脆弱性対策情報の公開に伴う悪用増加
3位	内部不正による情報漏えい等の被害	8位	ビジネスメール詐欺による金銭被害
4位	標的型攻撃による機密情報の窃取	9位	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	修正プログラムの公開前を狙う攻撃（ゼロディ攻撃）	10位	犯罪のビジネス化（アンダーグラウンドサービス）

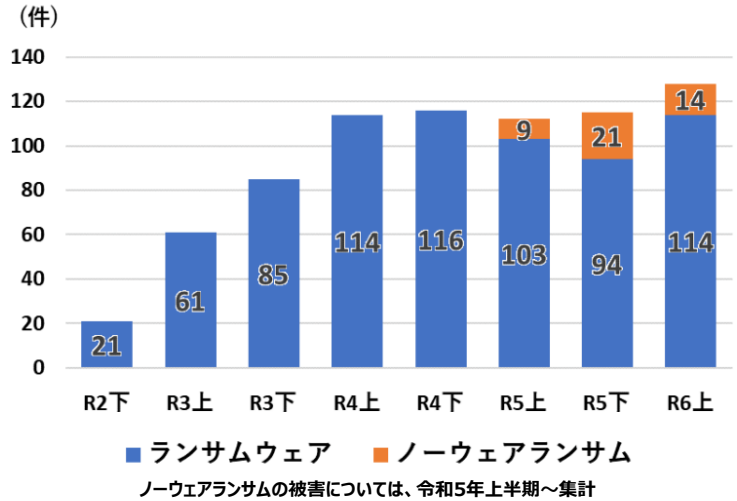
出典：IPA 『情報セキュリティ −10大脅威2024-』から

1．近年の動向 –ランサムウェアによる被害-

HITACHI
Inspire the Next

暗号化を行わずに恐喝を行うノーウェアランサム、RaaSなどの新たな手口によりランサムウェアの被害は拡大し続け、深刻化している

被害報告件数

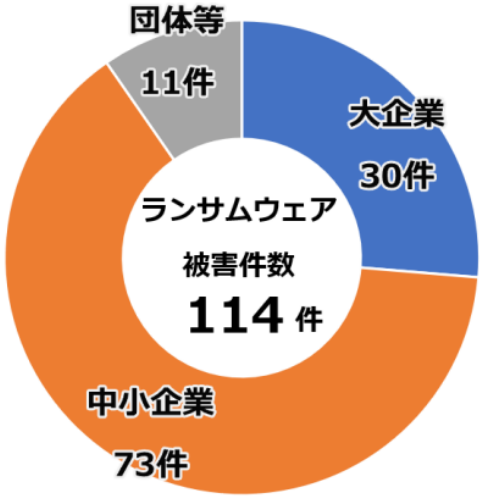


ノーウェアランサムの被害については、令和5年上半期～集計

ノーウェアランサムやRaaSなどの新たな犯行の手口からランサムウェアの被害は増加傾向

※RaaS（Ransomware as a Service）・・・ランサムウェアの開発・運営を行う者（Operator）が、攻撃の実行者（Affiliate）にランサムウェア等を提供し、その見返りとして身代金の一部を受け取る態様

規模別報告件数



会社規模や業種に関わらず被害が発生

出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

1．近年の動向 –必要なセキュリティ対策-

HITACHI
Inspire the Next

拡大し続ける被害・変化する手口に対して必要なセキュリティ対策

手口の変化・AIを悪用した
マルウェアの大量生成により
攻撃者の裾野が広がり続けている状況

侵入をゼロにするのは
非現実であり、不可能

既知・未知の脅威に関わらず
防御できる仕組み

侵入後にいち早く
被害を防ぎ、復旧する仕組み

脅威の検知・防御から軽減・復旧まで迅速に対応可能なセキュリティ対策

1．近年の動向 –SentinelOneによるセキュリティ対策-

HITACHI
Inspire the Next

SentinelOneを導入することにより
脅威の検知・防御から軽減・復旧まで、迅速に対応可能

SentinelOne

複数の検知エンジンを用いた検知・防御により
既知・未知のマルウェアをブロック

＋

AIにより自動的にダメージを軽減
マルウェア実行後も自動復旧によりインシデント対応が即時完了

2．SentinelOneの特長

2．SentinelOneの特長 -４つの特長-

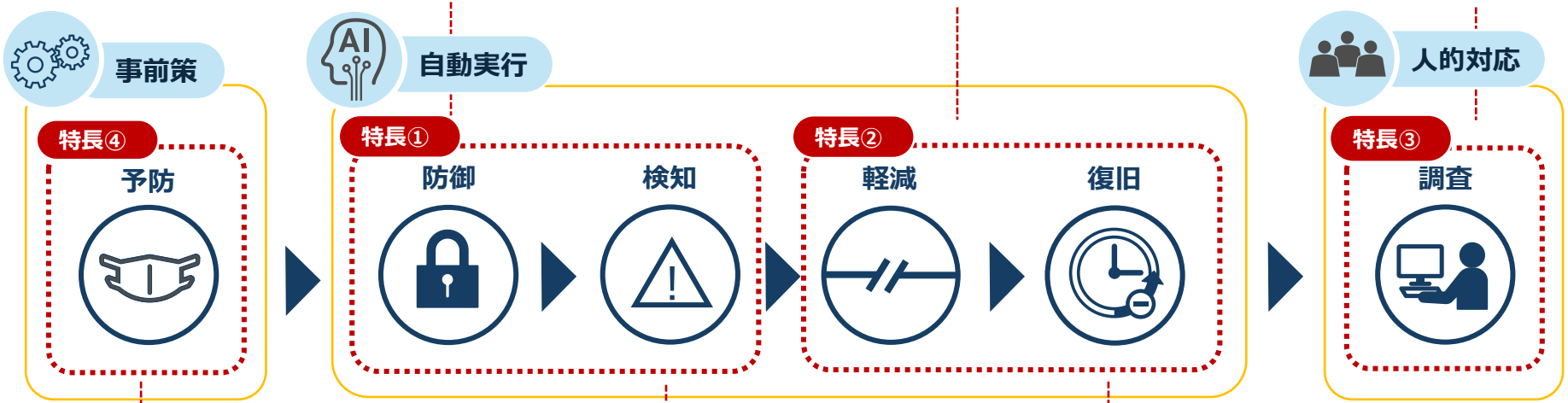
HITACHI
Inspire the Next

SentinelOneは４つの特長があり、
自動実行による検知・防御～軽減・復旧だけでなく、対処後の調査や事前の予防の機能を網羅

防御
- パターンマッチング、NGAVやEPP、EDRまでワンエージェントで提供
- 既知や未知のファイルベースのマルウェアに対応

軽減
- 疑わしいプロセスやファイルは自動停止、自動隔離
- 感染した端末をネットワークから自動隔離も可能

調査
- 脅威が取り除かれた状態で調査が可能
- 多様な調査ツールが利用可能



予防
- FWやUSBデバイスなどの制御機能や脆弱性診断機能により、脅威の予防が可能

検知
- ファイルレスなど、さまざまなマルウェアのふるまいを検知
- リアルタイムに脅威をコンテキスト化
- オフラインでも脅威を即時検知

復旧
- マルウェアでの汚染箇所を自動で完全復旧
- ランサムウェアに暗号化されたファイルを自動でロールバック

2．SentinelOneの特長 -①複数の検知エンジン-

特長①

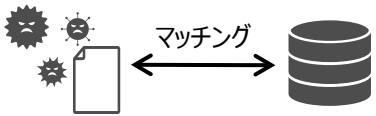
HITACHI
Inspire the Next

パターンマッチング、NGAV・EPPを搭載しており、既知・未知のマルウェアに対応
実行されたマルウェアに対してもAIによるふるまい検知を行い、さまざまな攻撃に対応可能

実行前のマルウェア対策

パターンマッチング

レピュテーションエンジン



既知のマルウェアに対する
シグネチャ方式の
パターンマッチング

NGAV・EPP

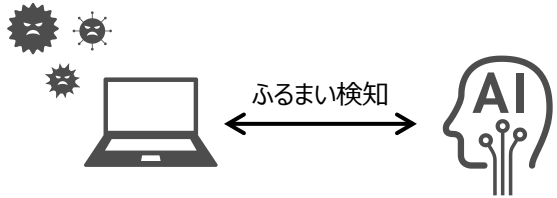
Static AIエンジン

未知のマルウェアに対する
ファイルの構造解析

実行中のマルウェア対策

Active EDR

Behavioral AI エンジン



ユーザーレベル・カーネルレベルの
ふるまいをエンドポイントのAIが
検知して防御するEDR

NGAV(New Generation Anti-Virus)：AIや機械学習などの技術を導入することで、従来型のアンチウイルスに比べて、検知精度の高いウイルス対策ソフト

EDR(Endpoint Detection and Response)：エンドポイントにおける不審な挙動を検知し、迅速な対応を支援するセキュリティソリューション

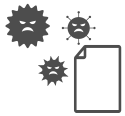
HITACHI
Inspire the Next

実行前のマルウェア対策

ファイルベースのマルウェアに対する静的解析

既知・未知のファイルベースの
マルウェアに対する複数の検知エンジン

既知のマルウェア



レピュテーションエンジン

既知のマルウェアに対する
シグネチャ方式のパターンマッチング

未知のマルウェア

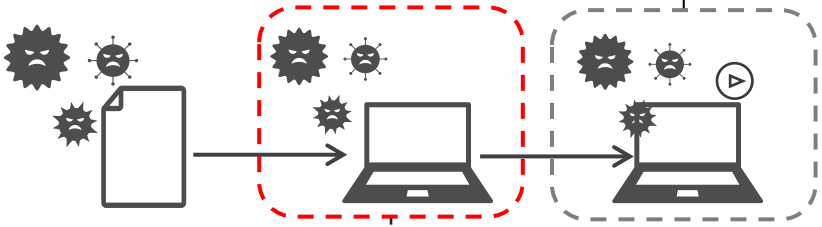
Static AIエンジン

未知のマルウェアに対する
ファイルの構造解析

ハードディスクへの書き込みタイミングで即時スキャン

通常の検知エンジン

ファイルが実行されたタイミングでスキャンするが、
動作していないマルウェアがハードディスク内に
存在するという状況がありうる



SentinelOneの検知エンジン

ハードディスクに書き込まれたタイミングで
即時スキャン開始

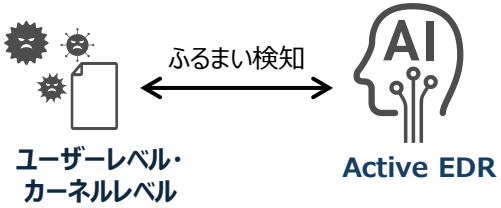
HITACHI
Inspire the Next

実行中のマルウェア対策

ふるまい検知エンジン ユーザーレベル・カーネルレベル

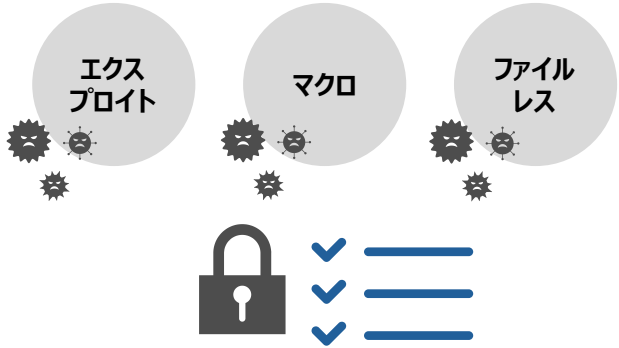
- エンドポイントのAIがふるまいを検知して防御するEDR
- ユーザーレベルのみならずカーネルレベルでのふるまいも検知

Behavioral AIエンジン



高い防御力

- Storyline機能でプロセスごとのふるまいを詳細かつ体系的にトレース
- Emotetやマクロ、PowerShellなどを使用したファイルレス攻撃も効果的に検知



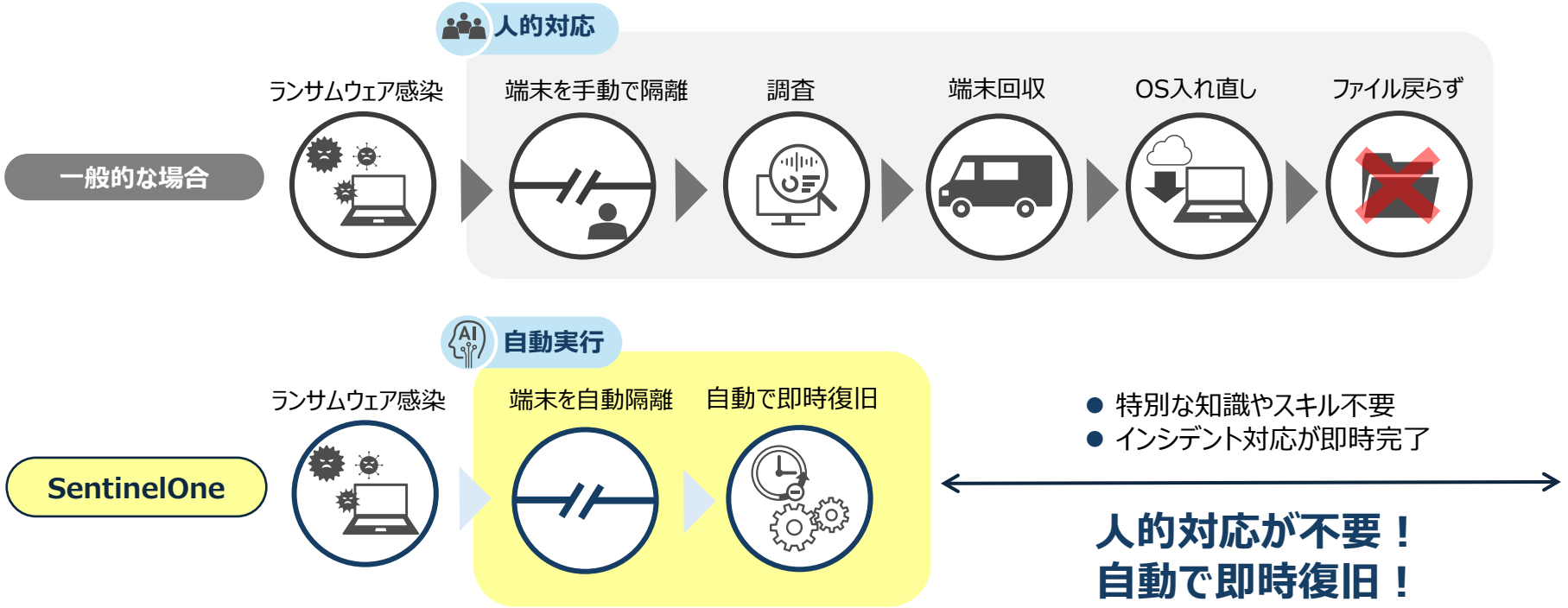
いつでもリアルタイムで保護

- エンドポイントにEDRのAI検知エンジンを搭載
- オフラインでもオンラインと同等の検知・対処を実現

2．SentinelOneの特長 -②AIによる自動対応-

HITACHI
Inspire the Next

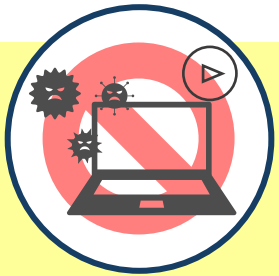
AIを用いて自動でダメージの軽減・復旧を行うため、インシデントの即時対応が可能
自動実行のため、特別な知識やスキルがなくても運用可能



2．SentinelOneの特長 -②AIによる自動対応：ダメージの軽減-

ダメージの軽減

プロセス停止

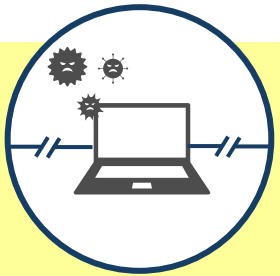


怪しい挙動を示したプロセスを
自動的に強制停止

ファイル隔離

被疑ファイルを特定ディレクトリへ
自動的に強制隔離し、暗号化

ネットワーク隔離



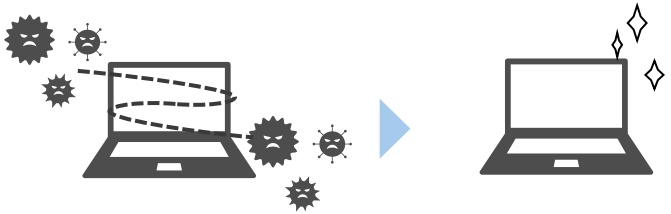
端末を自動的に
ネットワーク隔離

2．SentinelOneの特長 -②AIによる自動対応：自動復旧-

HITACHI
Inspire the Next

自動復旧

マルウェアでの汚染箇所を自動で完全復旧

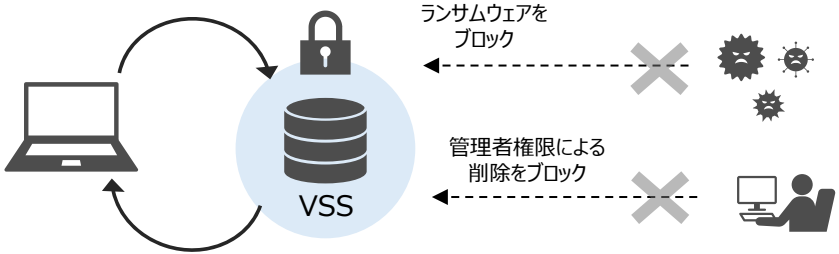


Remediate

- 攻撃途中の侵入段階で汚染された箇所を
  自動で完全に復旧
- マルウェア実行により書き込まれた一時ファイルや
  スケジュールタスク、レジストリ設定などを自動で完全復旧

Windows対応　　macOS対応

ランサムウェアによる暗号化ファイルを自動でロールバック



Rollback

- 4時間ごとにVSSのスナップショットを作成
- ランサムウェアによるVSSの破壊を未然に防止
- 管理者権限での削除に対してもプロテクト

Windows対応

2．SentinelOneの特長 -③調査のためのさまざまなデータツール-

HITACHI
Inspire the Next

インシデント発生時は、プロセスツリーにより詳細な情報の把握が可能
端末の常時ログ取得を行い、リモートからの端末調査も可能

プロセスツリーによる把握

Storyline

- 関連した挙動のプロセスを束ねて管理

リモートからの端末調査

Remote Shell ※Controlライセンス以上

- Windows ：PowerShell
- Mac ：Bash

端末の常時ログ取得

Deep Visibility ※Completeライセンス

- URLやファイルアクセスなど多彩な項目を取得
- 独自の検知ルールをカスタム可能

MITRE ATT&CKフレームワークに即した表記

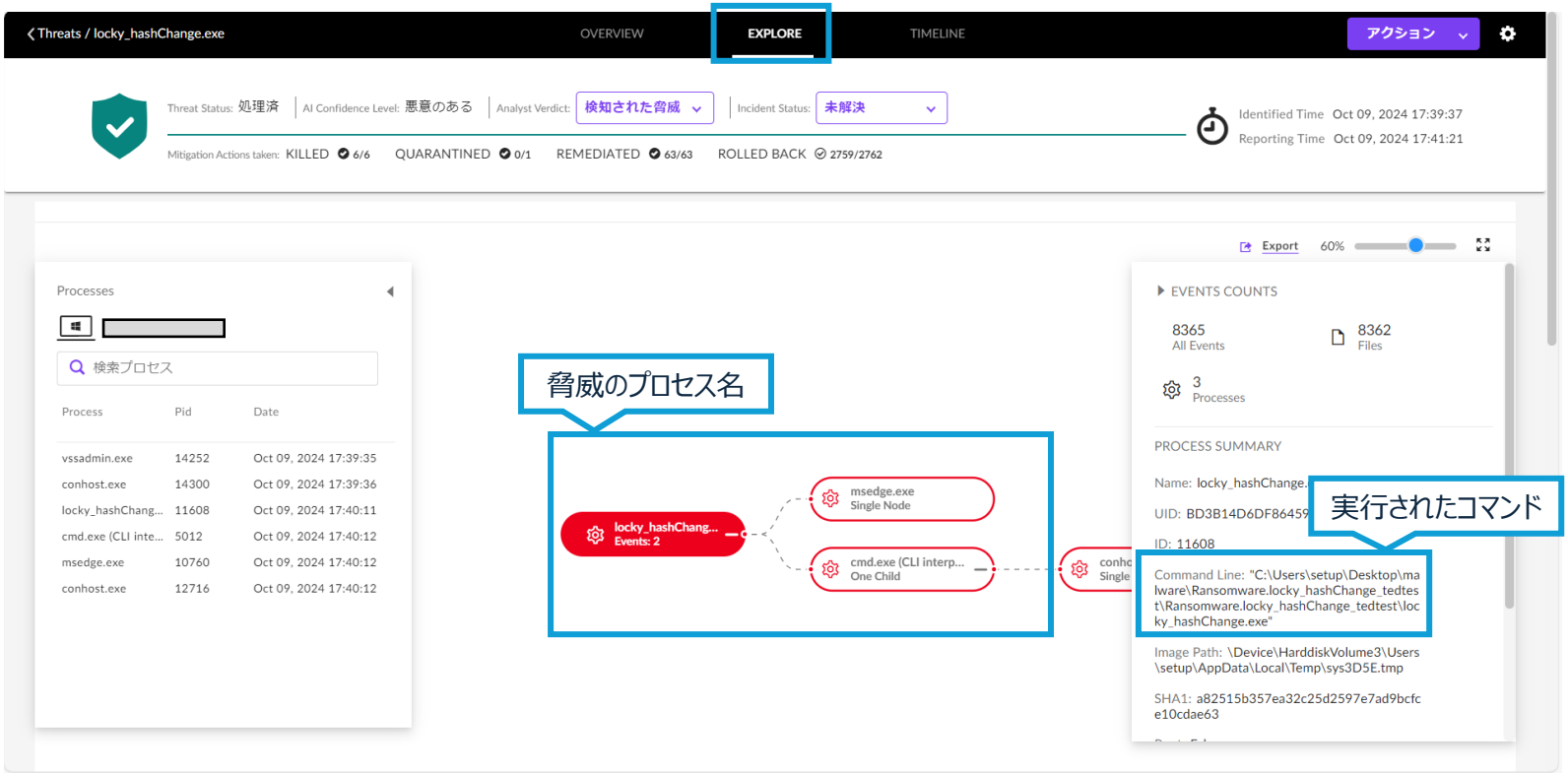
- 具体的なセキュリティ対策まで落とし込める
  フレームワークとして注目を集め、
  普及が進んでいるフレームワークに即した表記

2．SentinelOneの特長 -③調査のためのさまざまなデータツール-

HITACHI
Inspire the Next

プロセスツリーから、関連した挙動のプロセスが確認可能

Storyline

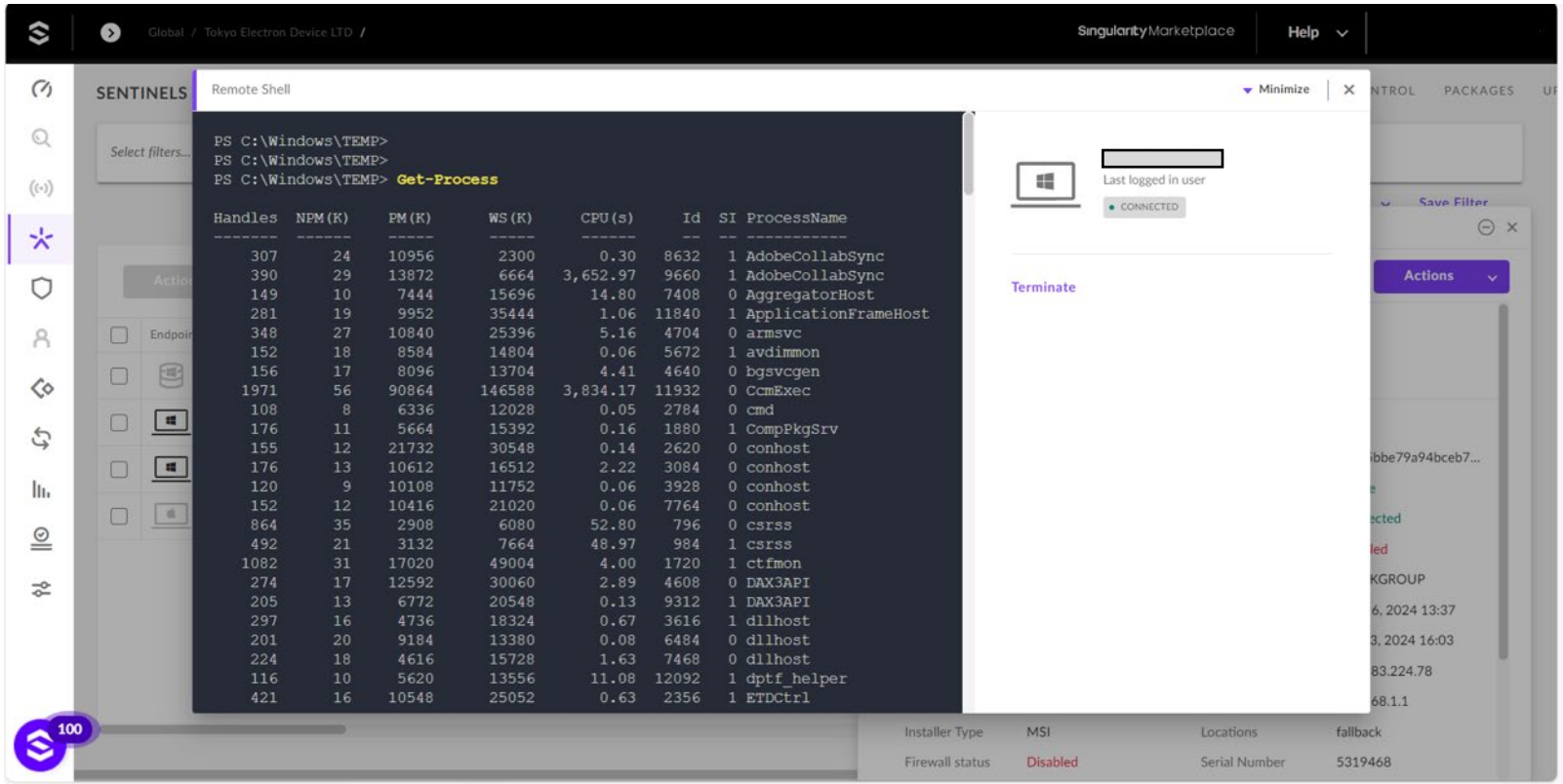


2．SentinelOneの特長 -③調査のためのさまざまなデータツール-

HITACHI
Inspire the Next

Remote Shellによる端末調査が可能

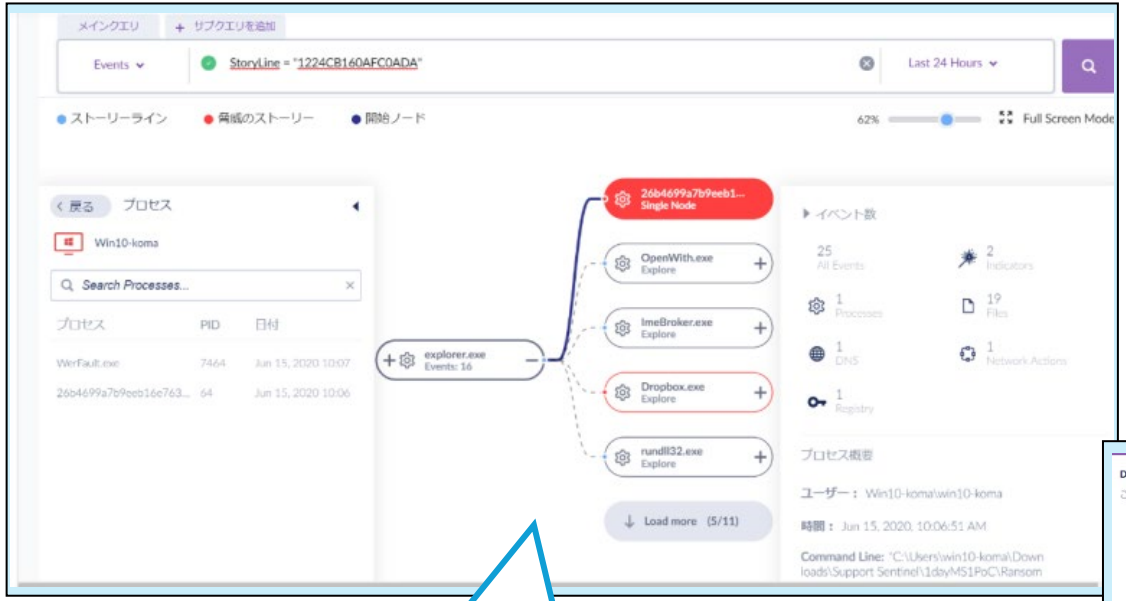
Remote Shell



2．SentinelOneの特長 -③調査のためのさまざまなデータツール-

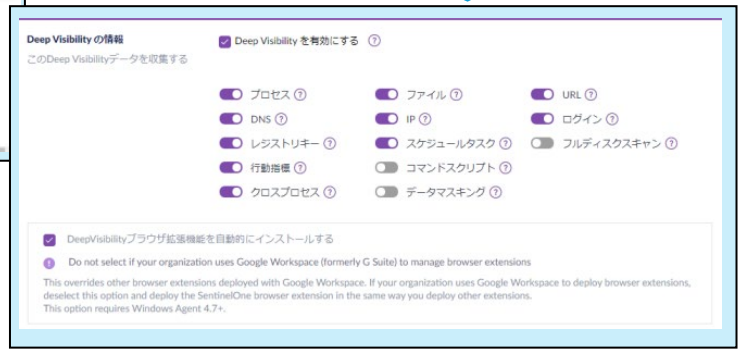
端末のログを常時取得し、詳細な調査が可能 ※Completeライセンス

Deep Visibility



常時ログ取得を行うため、
インシデント発生前の挙動についても
追跡調査が可能

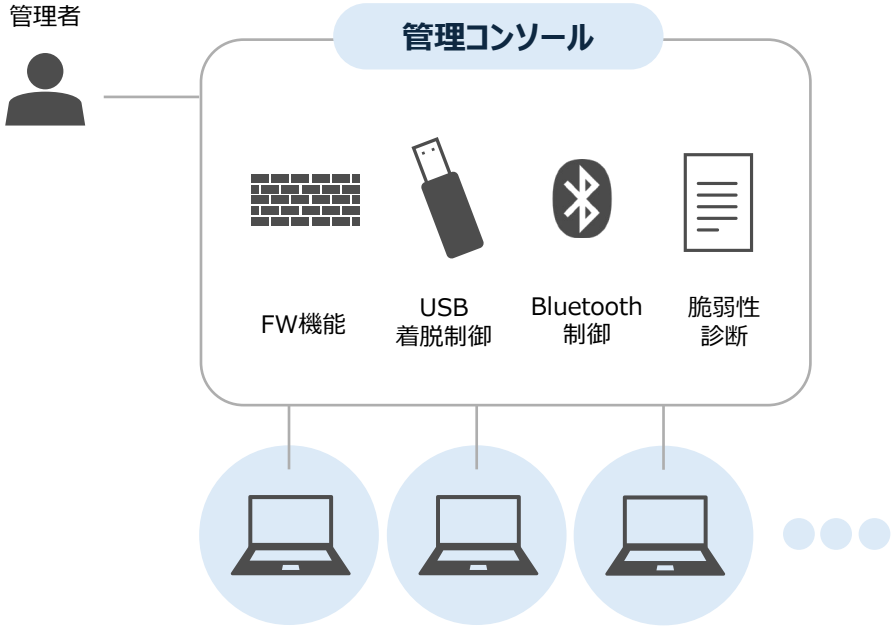
カスタム可能な検知ルール



2．SentinelOneの特長 -④事前対策機能-

HITACHI
Inspire the Next

FW機能やデバイス制御機能、さらに脆弱性診断機能を搭載しており、
脅威に対して予防が可能



FW機能 ※Controlライセンス以上

- レイヤ3/4での制御が可能
- FQDN制御
- 動的にポリシー変更を行うロケーションウェア機能

デバイス制御機能 ※Controlライセンス以上

- USB着脱制御
- USBのRead/Write
- Bluetooth制御

脆弱性診断機能 ※Controlライセンス以上

- アプリケーションの棚卸しとMITREのCVE情報を照合

Appendix. ライセンス別機能・OS別機能・参考価格

Appendix. ライセンス別対応機能

攻撃ステージ	機能	Core	Control	Complete
実行前対応	レピュテーションエンジン	✓	✓	✓
	Static AI エンジン	✓	✓	✓
実行中対応	Behavioral AI エンジン	✓	✓	✓
	ドキュメント・スクリプト攻撃	✓	✓	✓
	ファイルレス、脆弱性攻撃	✓	✓	✓
	ラテラルムーブメント	✓	✓	✓
	ネットワーク隔離	✓	✓	✓
実行後対応	修復	✓	✓	✓
	ロールバック	✓	✓	✓
	攻撃時のストーリーライン	✓	✓	✓
	Remote Shell		✓	✓
その他機能	ファイアウォール制御		✓	✓
	デバイス制御		✓	✓
	脆弱性診断		✓	✓
	Deep Visibility			✓

Appendix. OS別対応機能

攻撃ステージ	機能	Windows	macOS	Linux
実行前対応	レピュテーションエンジン	✓	✓	✓
	Static AI エンジン	✓	✓	✓
実行中対応	Behavioral AI エンジン	✓	✓	✓
	ドキュメント・スクリプト攻撃	✓	✓	✓
	ファイルレス、脆弱性攻撃	✓	✓	✓
	ラテラルムーブメント	✓		✓
	ネットワーク隔離	✓	✓	✓
実行後対応	修復	✓	✓	
	ロールバック	✓		
	攻撃時のストーリーライン	✓	✓	✓
	Remote Shell	✓	✓	✓
その他機能	ファイアウォール制御	✓	✓	
	デバイス制御	✓	✓	✓
	脆弱性診断	✓	✓	✓
	Deep Visibility	✓	✓	✓

※レガシーOS系では、一部の機能が制限されます。詳細については、当社までお問い合わせください。

Appendix. 参考価格

HITACHI
Inspire the Next

下記は、参考価格です。
最新の価格については、当社までお問い合わせください。

ユーザーレンジ	Core	Control		Complete	
	Workstation	Server	Workstation	Server	Workstation
100-500	¥12,330	¥19,260	¥14,580	¥54,090	¥26,550
501-1,000	¥10,080	¥15,840	¥11,970	¥44,370	¥21,780
1,001-2,000	¥9,180	¥14,220	¥10,800	¥40,050	¥19,710
2,001-5,000	¥7,920	¥12,330	¥9,360	¥34,650	¥17,010
5,001-10,000	¥6,840	¥10,620	¥8,010	¥29,790	¥14,670
10,001-25,000	¥5,670	¥8,910	¥6,750	¥24,930	¥12,240
25,001-50,000	¥4,590	¥7,110	¥5,400	¥20,070	¥9,900
50,001-	¥3,690	¥5,850	¥4,410	¥16,290	¥8,010

※それぞれの適応環境は下記を示しています。
Server･･･Windows Server/Linux
Workstation･･･PCクライアント

※1ライセンス/年間の価格(税別)です。

お問い合わせ

HITACHI
Inspire the Next

株式会社 日立ソリューションズ・クリエイト

Webでのお問い合わせ

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

表示に関する注意事項

HITACHI
Inspire the Next

■他社商品名、商標などの引用に関する表示

- SentinelOneは、SentinelOne, Inc.の登録商標です。
- Linuxは、Linus Torvaldsの米国およびその他の国における登録商標です。
- Microsoft Windowsは、米国、その他の国における米国Microsoft Corp.の登録商標です。
- MacはApple Inc.のサービスマークです。
- Bluetoothのロゴは、Bluetooth SIG, Inc.が所有する登録商標です。
- その他記載の会社名・製品名は、それぞれの会社の商標もしくは登録商標です。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2024年11月現在のものです。

サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。

■お問い合わせ情報について

お問い合わせ情報についてご相談・ご依頼いただいた内容は回答などのため、
当社の関連会社（日立ソリューションズグループ会社）および
株式会社日立製作所に提供（共同利用も含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。