Network Defense

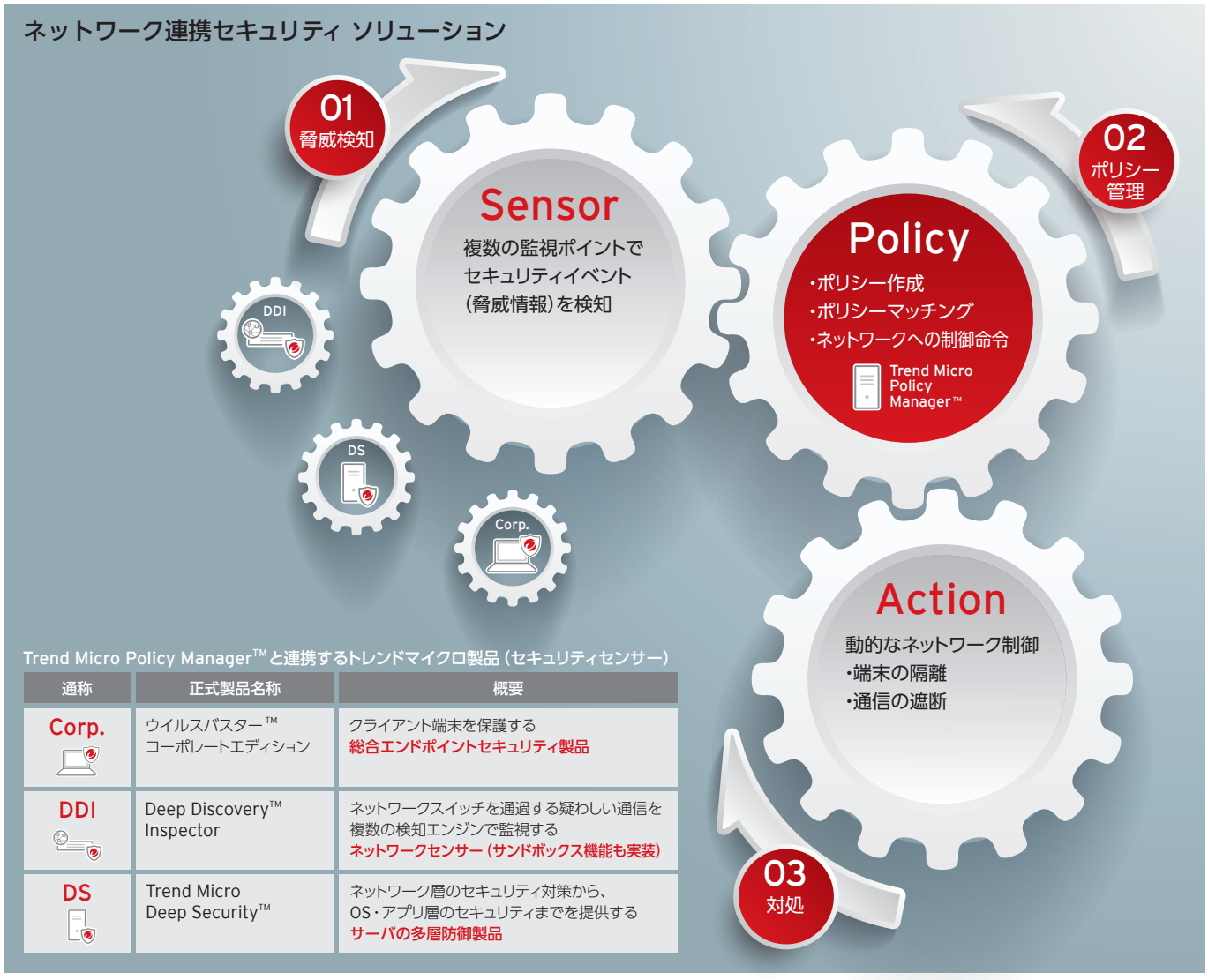
Trend Micro Policy Manager™

セキュリティ脅威への初動対応を自動化する
連携セキュリティ ソリューション

迅速な初動対応を可能にする
効果的なサイバー攻撃対策とは?

ネットワーク製品との自動連携により、被害の拡散防止・極小化

Trend Micro Policy Manager™ は、ITインフラ上の複数の監視ポイントでセキュリティ製品が検知したイベントをトリガに、アライアンスパートナー製品と連携し、企業の運用ポリシーに紐づいた動的なネットワーク制御を実行します。それにより、不正なPCやサーバのネットワークからの隔離、および不正な通信の遮断等の初動対応を自動化し、セキュリティリスクの拡散防止と極小化を実現します。



Trend Micro Policy Manager™と連携するトレンドマイクロ製品(セキュリティセンサー)

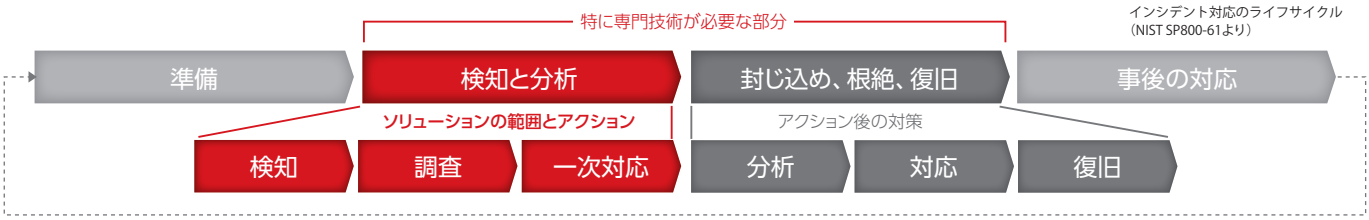
通称	正式製品名称	概要
Corp.	ウイルスバスター™ コーポレートエディション	クライアント端末を保護する **総合エンドポイントセキュリティ製品**
DDI	Deep Discovery™ Inspector	ネットワークスイッチを通過する疑わしい通信を複数の検知エンジンで監視する **ネットワークセンサー(サンドボックス機能も実装)**
DS	Trend Micro Deep Security™	ネットワーク層のセキュリティ対策から、OS・アプリ層のセキュリティまでを提供する **サーバの多層防御製品**

課題と対処

- イベント通知（ログ）が多く、優先順位付けが困難
- リアルタイムなリスク回避が困難
- 担当者によって運用レベルにバラつきが生じる

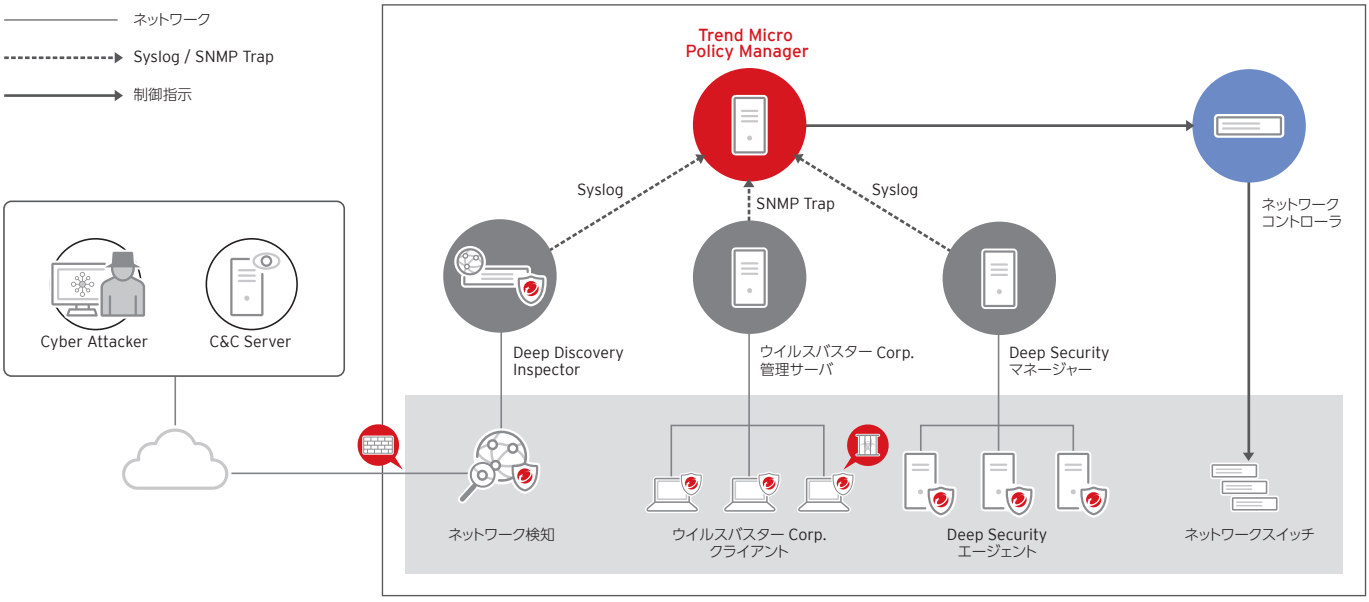
セキュリティ脅威の検知・特定から、初動対応までを、企業ごとの運用ポリシーで自動化。速やかな対応が可能となり、管理者のスキルにも人為的ミスにも左右されない安定した運用を実現。

対応範囲



本ソリューションの適用範囲は、インシデント対応のライフサイクルにおける、検知と分析（検知、分析、一次対応）にあたり、迅速な対応が必要なそのプロセスを自動化することで脅威の拡散のリスクを低減させることが可能です。

システム構成



センサー

- Sandboxによる検知
- マルウェア、C&C Callbackの検知
- 内部拡散活動の検知
- 情報リーク通信の検知
- マルウェア感染の検知

ポリシー管理

- ポリシー管理、マッチング
- 制御指示
  - 隔離、通信遮断
  - 管理者メール通知
  - 一時停止、切り戻し等

ネットワークコントローラ

- 制御実行
  - 隔離、通信遮断
  - 管理者メール通知
  - 一時停止、切り戻し等

ネットワーク制御

- 不正なプログラム感染端末の隔離
- 不正なコールバック通信のブロック
- 調査後の切り戻し

詳しくは ▶ www.go-tm.jp/tmpm

TREND MICRO トレンドマイクロ株式会社

お問い合わせ先

東京本社
〒151-0053 東京都渋谷区代々木2-1-1
新宿マインズタワー
TEL.03-5334-3601（法人お問い合わせ窓口）
FAX.03-5334-3639

大阪営業所
〒532-0003 大阪府大阪市淀川区宮原3-4-30
ニッセイ新大阪ビル13F
TEL.06-6350-0330　FAX.06-6350-0591

名古屋営業所
〒460-0002 愛知県名古屋市中区丸の内3-22-24
名古屋桜通ビル7F
TEL.052-955-1221　FAX.052-963-6332

福岡営業所
〒812-0011 福岡県福岡市博多区博多駅前2-3-7
シティ21ビル7F
TEL.092-471-0562　FAX.092-471-0563

www.trendmicro.co.jp

TREND MICRO、Trend Micro Policy Manager、Deep Discovery Inspector、Deep Security、Trend Micro Deep Security、およびウイルスバスターはトレンドマイクロ株式会社の登録商標です。
本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。
記載内容は2017年5月現在のものです。内容は予告なく変更になる場合がございます。
Copyright©2017 Trend Micro Incorporated. All right reserved.

BR-TMPM-002