エンドポイントセキュリティ強化
してみませんか？

企業のビジネス活動を脅かす
巧妙なサイバー犯罪のリスク

②.侵入した攻撃者は社内を探索して重要情報を外部へ送出
ランサムウェアを使った2重脅迫なども発生

①.テレワークやクラウド利用の増加により
侵入経路の増加
これまでの対策では守り切れない場面も

③.これらの脅威から組織を守るために
セキュリティ担当者の運用負荷が増大。
人的リソースも不足

エンドポイントセキュリティ強化の「3つ」のポイント

XDRは運用の手間もかかるし、**誤検知**も多いのではないか	インシデントが発生した際に、しっかりと**対処できたかどうか**正確な情報がほしい	全ての端末にXDRを導入するのは**手間がかかる**のではないか
XDRの負荷を下げる機能との連携が理想	**インシデントの終息宣言を行う体制が理想**	**負荷をかけず導入できるXDRが理想**

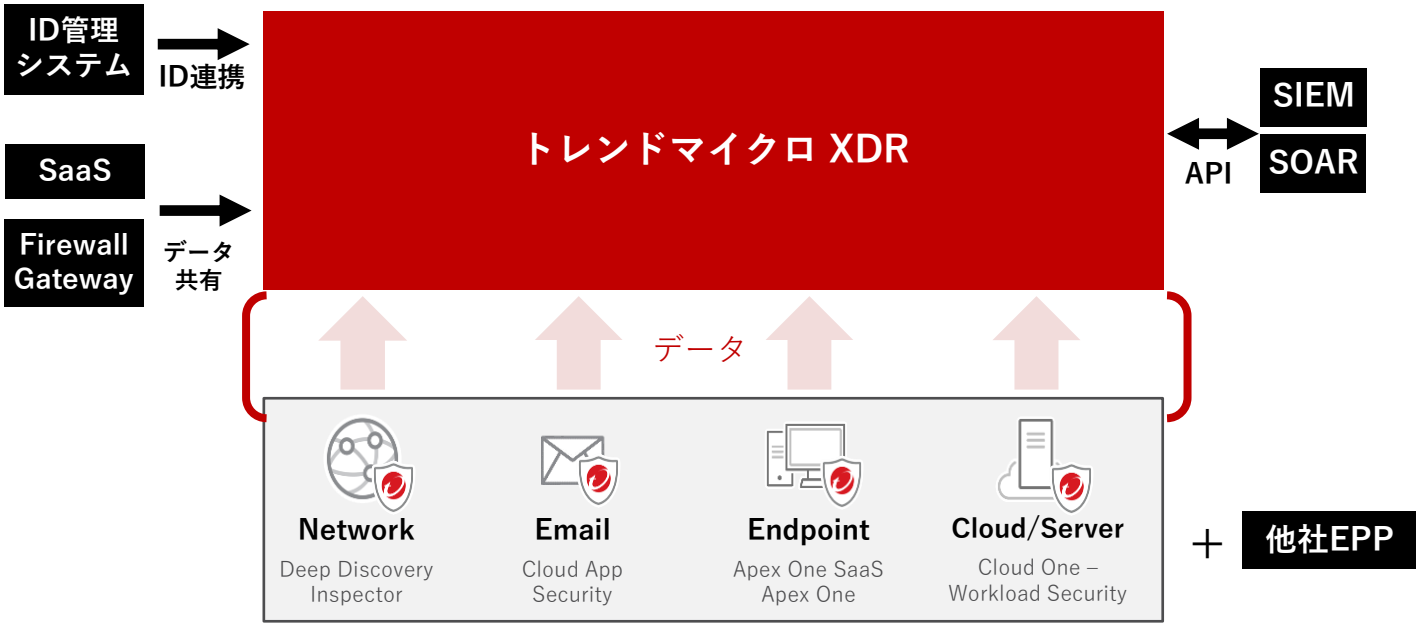
これらの課題を解決する「トレンドマイクロEDR/XDR」をご紹介します！

詳しくは裏面で！

企業向けエンドポイントセキュリティ製品
国内市場シェア14年連続No.1のトレンドマイクロが提供

Trend Micro XDR

エンドポイントだけでなく、「**多層レイヤー**」のログを分析し、脅威の全体像を可視化。
多くの「**3rd Party製品**」とも連携し、社内環境全体のセキュリティリスクを一元管理。



トレンドマイクロXDRのメリット

XDRは運用の手間もかかるし、**誤検知**も多いのではないか

インシデントが発生した際に、しっかりと**対処できたかどうか**正確な情報がほしい

全ての端末にXDRを導入するのは**手間がかかる**のではないか

強力なEPPと連携

トレンドマイクロのEPPにてほとんどの標的型攻撃をブロックすることができます。すり抜けてきた残りの脅威をXDRで対応することで運用負荷を軽減し、誤検知が少ない仕組みを実装することができます。

パターンファイルを活用したIR対応

トレンドマイクロのEPPでは有事の際、未知のマルウェアを解析し、パターンマッチングによる確実な駆除を実施することにより、することにより、インシデントの終息宣言をすることができます。XDRで検知し、パターンファイルで削除する連携が可能となります。

簡単導入

Apex One SaaSを導入されている方は、XDRを利用いただくにあたりインストーラによるセンサーの追加展開は必要ありません。
初期設定のみで簡単にご利用いただけます。

導入事例

モノを動かし、ミライをつくる。
UTOC
株式会社 宇徳

【従業員数】1952名（連結）
【業種】運送
【導入製品】XDR: Endpoint and Server
Apex One SaaS
Managed XDR Endpoints

【課題】
侵入を前提としたセキュリティ対策の強化をしたい。
万が一インシデントが起きた場合素早く対応を行うことで、被害の拡大を防ぎたい。

【導入効果】
EPP ですり抜けた脅威を素早く検知し、被害拡大前に対処可能になった。
リスクの高い検知の精査、調査、対処といった一連の流れはマネージドサービスが対応するため、**業務負荷を上げることなく、EDRの効果を実感**できた。

関連情報

説明資料/デモ動画/体験版　価格情報　Trend Service One（メーカーSOC）　問い合わせ

TREND MICRO