



2人でのセキュリティ運用を支えるTrend Vision One™ クラウド・オンプレミス環境のセキュリティを集約 効率良い運用を実現



株式会社ヤオコー



<https://www.yaoko-net.com/>



埼玉県、日本



小売業



社員 4,347名（2024年3月末時点）

導入製品・ソリューション

- Trend Vision One - Endpoint Security™
- Trend Vision One - Attack Surface Risk Management™
- Trend Vision One - Attack Surface Risk Management for Cloud™
- Trend Micro Apex One™ SaaS with XDR
- XDR: Endpoint and Server
- Trend Service One Complete

利用環境

- アマゾン ウェブ サービス (AWS)
- Microsoft Azure
- オンプレミス

導入効果

- EDRをはじめセキュリティを Trend Vision One に集約することで日々のセキュリティ運用を効率化
- 本部や店舗のクライアントPCからクラウド上のサーバまで多様な環境のセキュリティを一元管理
- マネージドサービスの活用によってEDRのアラート確認にかかる時間を大幅に削減

Before	After
DXやCXを支えるためにセキュリティの在り方をイチから見直し。本部・店舗・クラウドと多様な環境のセキュリティを少人数で効率よく強化する方法を模索していた。	EDRを中心にTrend Vision Oneにセキュリティを集約。マネージドサービスも活用することでセキュリティ運用にかかる工数の大幅削減を実現できた。

導入の背景

首都圏に200店超の店舗を展開し、35期連続で増収増益を続けるヤオコー。スーパーマーケット業界の営業収益ランキングでも上位をキープし続けるヤオコーでは「IT施策はビジネスに直結する」（小笠原氏）という考えから情報システム部門に相当するデジタル統括部は営業部門に属し、業績拡大につながる次の一手としてDXやCXを中心に積極的な取り組みを進めている。IT施策への注力と並行して「内部統制とコンプライアンス、そしてセキュリティはすべての企業にとって守らなくてはならない不変の柱と考えています」と語る藤森氏を中心に2022年頃から既存のセキュリティをイチから見直す動きが加速した。

しかし、セキュリティに関するガイドラインやセキュリティインフラの整備、社員教育などを進めている最中にサイバー攻撃が発生。幸い大きな被害は発生しなかったものの、経営層を含めて改めてセキュリティの必要性を認識したことでEDRを含めた具体的な対策についての検討が加速した。

お客様の課題

一度他社のEDR製品を導入したものの、運用にかけられるリソースが課題となった。EDRは日々検出されるアラートの確認や対処が必要不可欠だが、セキュリティ人材の不足が話題になる昨今、EDR運用に必要な知見を持った人材の確保は難しい。またシステムへの攻撃を防ぐEPPとシステム内に侵入した脅威をいち早く発見するEDRを別ベンダーの製品で実装すると、日々の運用や有事の際の問い合わせ、調査などにかかる工数が、ベンダーを統一した場合と比べて大幅に増加する。

さらにヤオコーでは本部、店舗、クラウドと複数の環境を抱えているため環境ごとに導入するセキュリティ製品が変わるとさらに運用負荷が増加してしまう。ヤオコーではIT人材の採用を強化しているがセキュリティ運用だけに人員を割けるわけではないため、運用負荷を抑えつつ、セキュリティを強化できる方法を探していた。

ソリューション

そんな時に提案を受けたのがトレンドマイクロのTrend Vision One - Endpoint Security（以下、Endpoint Security）だった。Endpoint SecurityはクライアントPCやサーバにセキュリティエージェントを導入することで、マルウェア対策や脆弱性対策をはじめとする複数の防御機能や、EDRを1つの製品で提供するエンドポイント向けセキュリティ製品だ。Endpoint Securityは保護対象から収集したデータをトレンドマイクロが運用するTrend Vision Oneというセキュリティプラットフォームに集約。トレンドマイクロの潤沢な知見で分析することで、脅威に対する迅速な発見・対処を支える。

「セキュリティの強化は重要ですが、DXやCXのスピードを阻害しないということも重要なポイントです。」



小笠原 暁史 氏
株式会社ヤオコー
デジタル統括部長 兼
プロダクト開発担当部長

「セキュリティは一社で取り組めば充分というものではないと考えています。業界、ひいては日本の企業全体で対策をしていく必要があると考えています。」

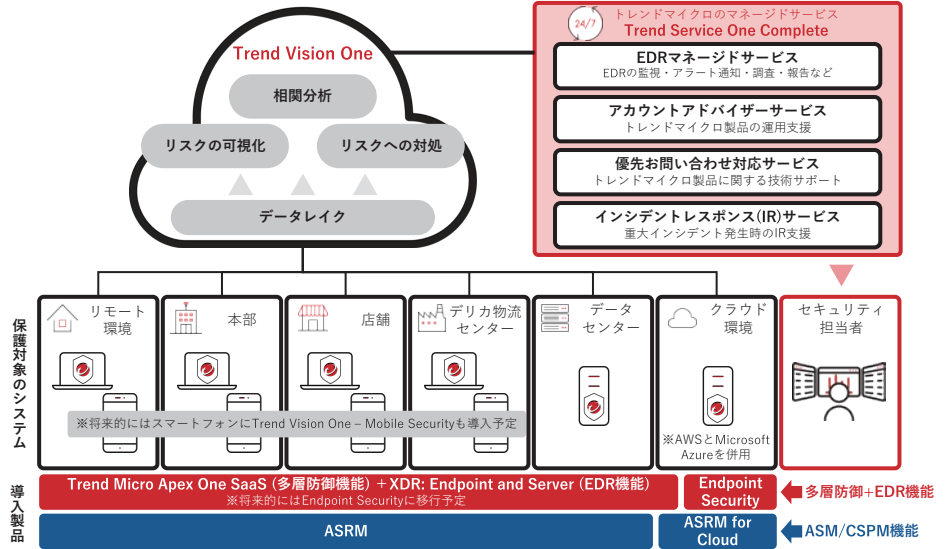


藤森 秀雄 氏
株式会社ヤオコー
デジタル統括部 IT基盤
ネットワーク/セキュリティ
マネジャー

「Trend Vision OneはUIが直感的でわかりやすく、導入後に操作に困ることが少なかった点も良いポイントでした。」



内田 晶子 氏
株式会社ヤオコー
デジタル統括部 IT基盤担当



選定理由

ヤオコーがEndpoint Securityの導入を決定した理由は大きく3つある。1つはトレンドマイクロ自身がTrend Service One CompleteというEDRのマネージドサービスを提供していること。24時間365日のEDR監視と有事の際の調査や対処の支援をトレンドマイクロに一任できるマネージドサービスのメリットは大きかった。2つめの理由はオンプレミスとクラウドを1つの製品で管理できること。Endpoint Securityはオンプレミス上のクライアントPCもクラウド上のサーバもまとめて保護できる。管理コンソールの統合や保護対象の一元管理、ベンダーの一本化によって日々の運用工数の圧縮が期待できた。そして3つめはTrend Vision Oneの拡張性。Trend Vision OneはEndpoint Security以外に、ネットワークやメール、モバイル端末向けのセキュリティ製品、External Attack Surface Management (EASM) やCloud Security Posture Management (CSPM)、Identity Threat Detection and Response (ITDR) といったASM機能を提供しており、それらの管理・運用もTrend Vision Oneに集約できる。

※EASMやITDR機能はTrend Vision One - Attack Surface Risk Management (以下、ASRM)、CSPM機能はTrend Vision One - Attack Surface Risk Management for Cloud (以下、ASRM for Cloud) で提供。

2023年に公開された総務省のASM導入ガイダンスを受けてASMの必要性も感じていたヤオコーにとって、エンドポイント領域以外のセキュリティ運用までTrend Vision Oneに統合できるのは非常に魅力的だった。「限られた人数でヤオコー規模の会社を守っていくのは正直厳しい部分もあり、セキュリティを統合的に監視する方法が必要だと考えていました。Trend Vision Oneの話聞き、「これだ」と思いました」(藤森氏)

導入効果

他社EDR利用時にはアラート内容の確認や対処に1件あたり30分~2時間ほどかかっていたため、複数件のアラートが上がった場合は1日対応に追われることもあった。それがエンドポイント領域のセキュリティをTrend Vision Oneに集約して、アラートの一次確認をトレンドマイクロのマネージドサービスが対応、対処が必要なもののみヤオコーにエスカレーションする運用に変更したことで、アラートへの対処時間を大幅に削減できた。また、CSPM機能を提供するASRM for Cloudを導入したことで「従来は、クラウド環境ごとに管理コンソールを開いて設定状況を確認する必要のあった設定不備がTrend Vision Oneの画面でまとめて確認できるようになり、効率よくリスクの把握と対処ができています」(内田氏)

今後の展望

ヤオコーでは、本部・店舗・クラウドを繋ぐネットワークや本部や店舗で活用の進むモバイル端末のセキュリティについてもTrend Vision Oneへの集約を前提に検討を進めていく予定だ。「今後サイバー攻撃がますます巧妙化する中で、組織の体制を含めてセキュリティを強化していく必要があると考えています。トレンドマイクロにはAIをはじめ新しい技術に対しても感度の高い伴走パートナーとして継続して支援をお願いしたい」と小笠原氏は語る。

トレンドマイクロ株式会社
www.trendmicro.com

TRENDMICRO、TREND MICRO、Apex One、Trend Micro XDR、Trend Service One Complete、およびASRMは、トレンドマイクロ株式会社の登録商標です。記載内容は2024年9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。※製品・サービスの導入効果は、ご利用企業・組織の方の声に基づくものであり、お客様のご利用状況により効果は異なります。Copyright © 2024 Trend Micro Incorporated. All rights reserved. [BR-CASE-281]

東京本社 〒160-0022 東京都新宿区新宿4-1-6 JR新宿ミライナタワー
TEL:03-4330-7601 (法人お問い合わせ窓口)
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7階
TEL:052-955-1221
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13階
TEL:06-6350-0330 (代表)
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7階
TEL:092-471-0562