SUCCESS STORY

TrendAI Vision One™ で「防御だけ」のセキュリティから「インシデント発生前のリスク管理+防御」を実現

東京美装興業株式会社

https://www.tokyo-biso.co.jp/

東京都、日本

社員 2,796名（2024年3月末時点）

導入製品・ソリューション:TrendAI Vision One™ – Cyber Risk Exposure Management、Endpoint Security

※ Trend Vision One™ - Attack Surface Risk Management、Endpoint Securityは、それぞれTrendAI Vision One™ Cyber Risk Exposure Management、Endpoint Securityに名称変更されました

導入の背景

1957年に設立し、オフィスビルの総合管理業務の第一人者として60年以上の歴史を持つ東京美装興業株式会社。新宿の本社を中心に北海道から福岡まで全国各地に支店を構え、多くのエンターテイメント施設、商業施設、オフィスビルの管理やメンテナンス業務を担っている。

ホールディングス体制への移行に伴い、グループ会社十数社が個別に実装していたセキュリティを東京美装ホールディングスのIT統括部に集約し、標準化したうえで管理/運用を一本化していく方針となった。

お客さまの課題

ホールディングス化以前は自社内の環境に管理マネージャを構築するオンプレミス型のエンドポイント向けセキュリティ製品を利用してクライアントPCやサーバをマルウェアから保護していた。

しかし、ホールディングス傘下のグループ企業のクライアントPCやサーバ、顧客施設に持ち込むPCの場合、オンプレミス型の管理マネージャに常時接続して最新のセキュリティ状態を保つのが難しいことをIT統括部では課題視。

セキュリティの標準化と強化を効率良く実現するために、オンプレミス型よりも管理しやすいSaaS型のセキュリティ製品への切り替えを検討しはじめた。

「脆弱性を抱える端末や不審なアクセスの数、CREMが算出したリスク値を見て、対応の必要性に対する認識がかわった」

柴田　勉 氏　IT統括部長

導入効果:

- マルウェア対策やEDRに加え、IPS機能を利用した脆弱性対策も実装することで、さらなるセキュリティ強化を実現。
- SaaS型セキュリティに切り替えることで、社内ネットワークに常時接続することが難しい持ち出し端末やホールディングス傘下のグループ企業の端末の保護を実現。
- 脆弱性やアカウントの侵害などいままで把握しきれていなかったリスクを可視化したことで既存のセキュリティ体制の見直しに貢献。
- リスクごとに深刻度が数値化されるため、対処の優先度付けが容易で、対処のスピードアップを実現。

ソリューション

こうした経緯で選ばれたのが統合サイバーセキュリティプラットフォームTrendAI Vision One™ を構成する製品の一つであるTrendAI Vision One™ – EndpointSecurity（以下Endpoint Security）だ。SaaS型のEndpoint Securityは管理マネージャの維持管理にかかる工数を削減でき、社外の端末も保護できる。

また、Endpoint SecurityはクライアントPCやサーバに対して、EPP（Endpoint Protection Platform）やNGAV（Next Generation Anti-Virus）と呼ばれるふるまい検知・機械学習型検索によるマルウェア対策、脆弱性を悪用する攻撃を防ぐ仮想パッチ（IPS）など多様な防御機能と、攻撃の兆候をいち早く検知・対処するEDR機能を1つの製品で提供する。

さらに東京美装ホールディングスはEndpoint Securityと同じTrendAI Vision One™ コンソールでTrendAI™ Vision One Cyber Risk Exposure Management（以下、CREM）も活用している。CREMは攻撃に悪用される可能性のあるアタックサーフェス（攻撃対象領域）を可視化し、迅速な対処を支援する製品。

「TrendAI Vision One™ という1つの管理コンソールで、マルウェア対策やEDR、アカウントの侵害有無、リスクの高い脆弱性の有無、セキュリティソフトの状態に至るまで確認できる点を高く評価している」

坪子 雅英 氏 IT統括部 係長

ソリューション（続き）

CREMでは、リスクの高い外部公開されたデジタル資産を把握するEASM（External Attack Surface Management）だけでなく、組織内でサイバー攻撃に悪用されるリスクが高い資産や脆弱性を把握するCAASM（Cyber Asset Attack Surface Management）、IDのセキュリティ状態を把握するISPM（Identity Security Posture Management）もアタックサーフェスとして可視化の対象にしている。

CREMを通して、それまでは明確に把握しきれていなかったシステム内に潜むリスクが顕在化。「脆弱性を抱える端末や不審なアクセスの数、CREMが算出したリスク値を見て、対応の必要性に対する認識がかわった」（柴田 氏）

今後の展望

東京美装ホールディングスのIT統括部では、Endpoint SecurityやCREMで検出したアラートへの対処自動化や、メール・Microsoft Teams、SharePoint Online、TrendAI Vision One™ - Email and Collaboration Securityによるセキュリティ強化を検討している。

セキュリティの基盤としてTrendAI Vision One™ を提供するTrendAIについては「昔からTrendAI製品を利用しているが不満はない、知名度があるため社員も安心して使えるという面もあり、今後も期待している」と柴田 氏は語る。

サイバーセキュリティの取り組みを一歩先へ

東京美装興業株式会社のような組織が、TrendAI Vision One™ を活用して、どのように「リアクティブ」から「プロアクティブ」なセキュリティへと進化を加速しているのかをご紹介します。

詳細はこちらから
https://trendaisecurity.com/ja

導入効果

Endpoint Securityによって、課題だった社内システム外の端末の保護を実現できた。

また運用開始後のアラートの多さが問題になることが多いEDRについても「アラートが絞られているので運用もしやすい」（坪子 氏）と評価。

CREMも、システム内のリスクを可視化するだけでなく、次に打つべき手を立てやすいため非常に重宝しているとのこと。現在は脆弱性やアカウント関連のリスクを中心にCREMが算出したリスク値をもとに日々対処を行っている。

脆弱性に関しては、CREMを通してリスクが高いと判断した端末の利用者に個別で正規パッチの適用を依頼するというオペレーションを実施している。

また、アカウントに関しては、Microsoft Entra IDとCREMを連携することでアカウント侵害の可能性がある挙動やアカウント漏洩のリスクを可視化できるようになった。インシデント発生前にパスワードの変更や強化を検討するといった対処が可能に。「これまではIDのふるまいについてはそれほど多くの注意を払っていなかったので、自分たちにとっても気づきになった」と柴田 氏は語る。

さらにTrendAI Vision One™ という共通のプラットフォームに複数のセキュリティ機能を集約したことは運用工数増加の抑制にも繋がった。複数のセキュリティ製品を導入すると、アラートの確認など日々の運用が煩雑になりやすく、インシデント発生時の調査や対処にも時間がかかりやすい。しかし複数のセキュリティ製品の運用をTrendAI Vision One™ の管理コンソールに集約することで運用工数の削減も実現できた。

実際に運用を担当する坪子 氏は「TrendAI Vision One™ という1つの管理コンソールで、マルウェア対策やEDR、アカウントの侵害有無、リスクの高い脆弱性の有無、セキュリティソフトの状態に至るまで確認できる点を高く評価している」と語る。

TrendAI™ について

TrendAI™ は、トレンドマイクロのエンタープライズ向け事業部門であり、AIセキュリティのグローバルリーダーです。AIの包括的な可視化と統合セキュリティの提供を通じて、組織に確かな信頼をもたらし、イノベーションを推進するとともに、リスクを最小化します。

現在、世界185か国において大手企業や政府機関に採用され、アイデンティティ、インフラ、データに至るまで、組織全体を横断したセキュリティを提供しています。AI Fearlessly.

https://trendaisecurity.com/ja