“「こころ、はずむ、おいしさ。」の提供”を経営理念に掲げるエバラ食品工業株式会社。多くの家庭で愛用されている焼肉のたれ「黄金の味」や、「すき焼のたれ」などの調味料で、「人を惹きつける、新しいおいしさ」を食卓に届けている。同社のビジネスをデジタルで支えてきた情報システム部では、情報セキュリティ対策を強化するために、Sophos Intercept X Advanced with XDRおよびSophos MDRセキュリティサービスを採用した。

CUSTOMER-AT-A-GLANCE

こころ、はずむ、おいしさ。
エバラ

エバラ食品工業株式会社

所在地 本社　横浜市西区みなとみらい4丁目4番5号 横浜アイマークプレイス14階

WEBサイト　https://www.ebarafoods.com

ソフォスソリューションズ　Sophos Intercept X Advanced with XDR
Sophos Intercept X Advanced for Server with XDR
Sophos MDR Complete セキュリティサービス

SOCに該当するMDRセキュリティサービスまで、1社で対応してくれるSophosを選びました。

エバラ食品工業株式会社
情報システム部 DX推進課 課長
羽咋 有果 氏

1958年に設立したエバラ食品工業株式会社は、創業期から「冒険、反論、失敗の自由」という精神を受け継ぎ、独自性あふれる商品を生み出してきた。フルーツベースの焼肉のたれ「黄金の味」をはじめ、洋食屋の味を家庭で楽しめる「横濱舶来亭」や手軽に浅漬けが作れる「浅漬けの素」など、数多くの調味料で家庭の「食」や「暮らし」に貢献している。同社の情報システム部では、基幹系システムの開発や社内ITシステムの整備にDX推進など、ビジネスに不可欠なデジタル基盤の構築と整備に携わってきた。そして、情報セキュリティ対策にも積極的に取り組み、社内のセキュリティ基本方針の見直しをきっかけとして、Sophos Intercept X Advanced with XDRおよびSophos MDRセキュリティサービスを採用し、安全性の向上と運用負担の軽減を両立した。

ビジネスチャレンジ

「セキュリティ基本方針の見直しからEDRの必要性を認識」

エバラ食品工業株式会社が、情報セキュリティ対策の強化に取り組んだ背景について、情報システム部 DX推進課の羽咋有果課長は次のように切り出す。

「きっかけは、当社のセキュリティ基本方針の見直しでした。コロナ禍によりテレワークが急速に広がり、見えない部分への脅威に対する不安が増大しました。当社は20年以上にわたりエンドポイント保護プラットフォーム（Endpoint Protection Platform）を利用して、マルウェア対策をとってきました。しかし、EPPでは防ぎきれないサイバー攻撃に対し、脅威を検知して通知できるEDR（Endpoint Detection and Response）を導入する必要に迫られていました」。

EPPからEDRへの対策強化を検討した同

社だが、サイバー攻撃に対する検知機能には懐疑的な印象を持っていた。その理由について、羽咋氏は「以前、ネットワーク機器のセキュリティ監視製品を試験的に導入したのですが、誤検知とアラートの多さに戸惑ったのです。そのため、EDRのような検知機能を追加しても、的確にモニタリングできる人員や体制が整備できなければ、膨大なアラートの中からインシデントにつながる危険な予兆を発見できない、と実感していました」と話す。

テクノロジーソリューション

「NDIソリューションズ株式会社様の提案を前向きに検討しEDR製品を選定」

ウイルスやマルウェアに感染しないと端末の被害を認識できないEPPによる対策から、未知の脅威を迅速に検出し排除するEDRへの更新を決めた同社は、何通りかの方法を検討した。羽咋氏は「最初は、既存のEPPにEDR機能だけを別製品として追加する方法を検討しました。旧EPP製品は、長年使い続けていたので、その基盤を変えたくなかったのです」と検討の背景に触れ、「EDRは検討したいがEPPの入れ替えにかかる労力と導入漏れが一番の懸念でした。そこで、解消方法としてSophos社の全面協力による検証の充実と、具体的な検証方法の提示、そして迅速なQ&A対応、さらに、自社でもSophosを利用しているNDIソリューションズ株式会社様の伴走支援に期待しました」と話す。

EDR導入に取り組んできたDX推進課　有賀雅浩氏は、EDRへの更新を決めた理由を次のように話す。

「EPPとEDRを別々に導入してしまうと、インシデントが発生したときに問題の切り分けが複雑になる、と心配でした。また、2つのセキュリティ製品の運用管理は煩雑になり、結果として担当者の負担が増してしまいます。そこで、EDRを追加するのではなく、ひとつの製品でEDR機能を備えたセキュリティ製品へ更新することにしました。SophosはEPPベンダーで、EDRはもちろんですが、まずはEPPを強化し、そもそも感染しないことを目指しており、ランサムウェアの被害がゼロというのも大きな安心につながりました」。

エバラ食品工業株式会社
情報システム部 DX推進課
有賀 雅浩 氏

「Sophos Intercept X Advanced with XDRおよびSophos MDRセキュリティサービスを採用」

ひとつの製品でEDR機能を備えた製品の導入を決めた同社では、最終的にSophos Intercept X Advanced with XDRを

選定した。その決め手について、羽咋氏は「Sophos MDR（Managed Detection and Response）サービスが、Sophos Intercept X Advanced with XDRに決めた理由です。EDR製品であるIntercept X Advanced with XDRとSOCに該当するMDRセキュリティサービスまでオールインワンで提供してくれるSophosを選びました」と説明する。

ビジネスインパクト

「MDRセキュリティサービスのレスポンスの速さと信頼感を高く評価」

Sophos Intercept X Advanced with XDRとMDRセキュリティサービスの導入は、2022年9月に本社からスタートしグループ企業へと広がっていった。その過程で、EPPとEDRの違いを実感する出来事が起きた。有賀氏は「旧アンチウイルスソフトを導入しているPCと、Sophos Intercept X Advanced with XDRが、同じマルウェアに感染する被害が発生したのです。Sophos Intercept X Advanced with XDRは、検知から駆除、復旧まで、すべて自動で対処してくれました。MDRのおかげで、情報システム部では結果を確認するだけで良かったのです。一方、旧EPPではPCを保護するためにネットワークを遮断する挙動をしたため、ネットワークにつながらず復旧作業が必要となりました。まさに、EPPとEDRが業務に与える影響の差を痛感する出来事でした」と振り返る。

EDRの安全性と利便性を実感した同社では、当初の予定ではクライアントPCへの導入だけを計画していたSophos Intercept X Advanced with XDRをサーバーへも展開した。

さらに有賀氏は「MDRセキュリティサービスのレスポンスの速さにも驚かされました。何か問題があると、すぐに連絡が来ます。必要があればオンライン会議が開催され、海外のエンジニアと同時通訳のスタッフが参加して、こちらが対応するべきアクションを的確に指示してくれます。もちろん、Sophos Intercept X Advanced with XDRをインストールしているPCであれば、MDRセキュリティサービスがリモートで対処してくれるので、担当者の業務負担も大幅に軽減されます」と評価する。

羽咋氏も「圧倒的な安心感が得られるようになりました。以前は、マルウェア感染時の対処は自分たちで行うしかなかったのですが、MDRセキュリティサービスによって、その心配が一切なくなりました。『Sophosが入っている』という信頼感から、DX推進課としても本来の業務に注力できるようになりました」と導入の効果を語る。

フューチャービジョン

「ゼロトラストも見据えてSophosのサービスやセキュリティ対策に期待」

今後に向けたセキュリティ対策について、羽咋氏は「セキュリティ基本方針の見直しの一環として、エンドポイントに頼りすぎないセキュリティ対策の強化も検討しています。今後は、境界型の防御ではなく『ゼロトラストを前提としたセキュリティモデル』を構築していく計画です」と語る。

SOPHOS