SOPHOS

CUSTOMER CASE STUDY　**株式会社バロックジャパンリミテッド**

「挑戦」を企業理念として2000年に創業された株式会社バロックジャパンリミテッド。同社は、ハイカジュアルブランド「MOUSSY（マウジー）」をはじめ、時代の空気を体現するコレクションのSLYや、セレクトショップのSHEL'TTERなど、ファッションセンスの高い女性に人気のブランドを展開している。同社の情報システム部では、服飾産業界にも広がるランサムウェア被害の事例を危惧して、増大するサイバー攻撃に備えるために、SophosのIntercept X Advancedを導入した。

CUSTOMER-AT-A-GLANCE

BAROQUE JAPAN LIMITED

株式会社バロックジャパンリミテッド

所　在　地　〒153-0042
東京都目黒区青葉台4丁目7番7号　住友不動産青葉台ヒルズ

従 業 員 数　1,502名（連結従業員数、契約社員を含む 2022年2月末時点）

WEBサイト　https://www.baroque-global.com/jp

ソフォスソリューションズ　Intercept X Advanced

旧世代のエンドポイントセキュリティでは、検知できないマルウェアに対しても、振る舞い検知機能を備えたIntercept X Advancedならば対応できると考えて採用しました。

株式会社バロックジャパンリミテッド
経営企画本部　情報システム部　運用グループ
松本 邦裕氏

2000年に渋谷109店で展開したハイカジュアルブランド「MOUSSY（マウジー）」を起点に、若い女性を中心に人気ブランドとして成長してきた株式会社バロックジャパンリミテッド。同社は、自社ブランドが創造する「文化」を世界へ発信するという「挑戦」を企業理念に掲げ、小売業の未来を変えるイノベーションを推進している。同社の情報システム部では、事業の成長を支えるためのシステム開発や運用に貢献し、長年にわたって情報セキュリティ対策にも取り組んできた。その取り組みの中で、旧世代のエンドポイントセキュリティでは、増大するランサムウェア攻撃への対応が及ばないと判断して、AI（ディープラーニング）で未知のマルウェアを検知できるIntercept X Advancedを採用した。

ビジネスチャレンジ

「ランサムウェア攻撃がアパレル産業界にも広がり脅威への備えが急務」

株式会社バロックジャパンリミテッドの経営企画本部　情報システム部で、セキュリティ対策を含めたシステム全般の運用を担っている松本邦裕氏は、Intercept X Advancedを採用した背景について、次のように振り返る。

「以前よりテレワークができるようにVPNの環境を構築していましたが、使用していたエンドポイントセキュリティ製品がオンプレミスで運用する管理サーバーに接続しないとパターンファイルが更新されない時代がありました。2019年中にその製品がクラウドに対応し、その直後コロナ禍によりテレワークが本格化しましたがパターンファイル更新やウイルス検知情報のアップロードなどがクラウド化していたおかけで安心して運用することができました。その経験からエンドポイントセキュリティを刷新するにあたっては、最初からクラウドを前提とした

新世代の検知機能を備えた製品を選ぶべきだと考えるようになりました。」
テレワークの利用が普及する以前から、旧世代のエンドポイントセキュリティでの防御に懸念を抱いていた情報システム部では、服飾産業にもサイバー攻撃のリスクが高まっているという危機感も持っていた。松本氏は「経営層も情報セキュリティ対策については、強化する必要性を実感していました。そんなときに、大手衣料品チェーンがランサムウェアを使ったサイバー攻撃を受けて、全国の店舗に影響が出る被害が発生しました。そこで、当社でも情報セキュリティ対策をより強固なものにする必要があると考えました」と補足する。

テクノロジーソリューション

「未知のマルウェアを検知できるIntercept X Advancedの振る舞い検知機能に注目」

情報セキュリティ対策を強化するために、情報システム部では従業員のITリテラシーを高めるトレーニングも重要だと考え、同部の企画・開発グループの堀井美希氏が、その対応にあたった。堀井氏は「メールを悪用したフィッシング攻撃から、サイバー攻撃の被害が拡大する事件が増えていたので、従業員のセキュリティ意識を向上させる必要がありました。そこで、当社のパートナー企業に相談して、フィッシング攻撃シミュレーション/トレーニングのSophosPhish Threatを紹介してもらいました。それがきっかけで、SophosのIntercept X Advancedというエンドポイントセキュリティ製品を知りました」と話す。
Sophos Phish Threatをきっかけに Intercept X Advancedを知った松本氏は「ランサムウェア対策テクノロジーに注目しました。また、パターンファイルに依存せずに、高度な機械学習システムを使用して、未知の脅威に対する防御も強化されている点を高く評価しました。旧世代のエンドポイントセキュリティでは、検知できないマルウェアに対しても、振る舞い検知機能を備えたIntercept X Advancedならば対応できると考えて採用しました」と選定の理由を説明する。
社内アプリの検証をしていく中で分かったことして、複数の段階で怪しい振る舞いパターンをどこかの時点で検知するとそれ以降の動作を止めるので、旧他社製品でマルウェアが一度すり抜けてしまうと全く検知しなくなることを考えるとかなり安心感がある。

株式会社バロックジャパンリミテッド
経営企画本部 情報システム部 企画・開発グループ
堀井 美希氏

ビジネスインパクト

「運用管理が容易になり安全性も向上」

Intercept X Advancedへの更新にあたり、情報システム部では2022年7月から

部署単位に順次テストを開始した。テストにあたって松本氏は「検証したのは、既存の業務アプリが正しく動作するかどうかでした。エンドポイントセキュリティ製品の多くは、国産の服飾用CADソフトなどメジャーではないソフトウェアをマルウェアと認識してしまうのでマルウェアと認識されないように設定を追加・変更する必要があります。旧他社製品では場合によってはアプリの開発元に確認してその内容を設定するなどの手間がありましたが、Intercept X Advancedでは検知されたソフトをホワイトリストに登録するだけで誤認を回避できたので、とてもスムーズに検証が進みました」と評価する。

約1ヶ月の検証期間を経て、2022年8月から本格的な更新がスタートした。堀井氏は「8月が旧製品の更新期限だったので、そのタイミングで本社PCをIntercept X Advancedに変更しました。最初に、本社にあるWindows PCへActive Directoryのグループポリシーで配信しました」と話す。

松本氏は「Intercept X Advancedに変更してから、ファイル共有サイトへの注意喚起やZIP暗号化されたファイルへの警告など、以前よりも警戒のレベルが向上したように感じます。また、運用管理の面でも、Intercept X Advancedの管理サイトは使いやすいので、旧他社製品よりも作業効率が良くなったと思います」と効果に触れる。

フューチャービジョン

「LinuxサーバーやMac OSの保護も推進」

今後に向けた情報セキュリティ対策について、堀井氏は「本社のWindows PCはすべて更新できましたが、MacOSやLinuxサーバーへの展開はこれからになります。Mac OSでは、Active Directoryのグループポリシーが利用できないので、Intercept X Advancedのインストール先URLを案内するといった方法を検討しています。また、Linuxサーバーではエクスプロイト対策が重要になるので、Intercept X Advancedで攻撃への防御が強化されると期待しています」と説明する。

松本氏も「クライアントPCのランサムウェア対策は、Intercept X Advancedで対応できると考えています。ただ、サーバーに関してはバックアップ方法も含めてトータルでランサムウェア対策を強化していくべきだと捉えています。今回の更新は、旧他社製品からの置き換えが中心で、以前にできていた防御に加えて振る舞い検知やランサムウェア対策を強化しました。今後に向けては潜在的な脅威の検出や、影響を受けたデバイスの把握や可視化が重要になると考えています。その意味では、EDR（Endpoint Detection and Response）やXDR（Extended Detection and Response）などの対策も検討していきたいです」と展望を語る。

SOPHOS