物流・エネルギー分野で革新的なソリューションを提供しているトーヨーカネツがセキュリティ対策を強化した。未知の脅威であるサイバー攻撃にも対応できる防御体制を築くためだ。ただし、人的リソースが限られるので、運用管理の負担を増やすことはできない。この課題を解決したのが、ソフォスの次世代型エンドポイントツールである。

CUSTOMER-AT-A-GLANCE

トーヨーカネツ株式会社

トーヨーカネツ株式会社
東京都江東区南砂
二丁目11番1号

社員数
996名（2019年3月期、連結）

Webサイト
https://www.toyokanetsu.co.jp/

ソフォスソリューション
Sophos Intercept X

現在、当社は「攻め」のIT投資に向けて土台づくりを進めているところです。
サイバー攻撃に備えたセキュリティ対策は、土台づくりとして必要なIT基盤です。
2020年にオリンピック・パラリンピック大会を控えており、
テレワーク環境構築に向けて、社外でも強固な防御態勢を築きたいと
考えました。

トーヨーカネツ株式会社
コーポレート本部　経営企画部 経営企画グループ 兼 総務部 情報システムグループ
主査　情報処理安全確保支援士　　宮川 嘉正 氏

1941年に工業窯炉の製造・販売事業者として創業したトーヨーカネツ（当時の社名は東洋火熱工業）。「優れた技術、製品、サービスを裏付けとして持続的に成長・発展するグループ」を経営ビジョンに掲げる同社は、顧客や社会の要請に基づいて事業を拡大してきた。現在は、仕分け・ピッキングシステムや情報化技術に関して顧客から高い評価を受けている物流ソリューション事業と、原油や液化天然ガスなどの貯蔵タンクを世界各地に5700基以上納入している機械・プラント事業を経営の柱としている。2019年に同社は、セキュリティ対策の強化に乗り出す。未知の脅威に備えることが大きな狙いだ。

ビジネスチャレンジ

これまで同社は、世界的に大きなシェアを持つセキュリティベンダーのアンチウイルスソフトを利用していた。シグネチャ（マルウエアの特徴的なパターン）でマルウエアを検知する仕組みのツールだ。

同社のIT投資を統括する情報システムグループは、セキュリティ対策を見直し、強化が必要だと判断したという。手口が巧妙化するサイバー攻撃を防御するためだ。ファイアウォールなど他のセキュリティツールも導入しているが、修正プログラムが提供される前に脆弱性を突くゼロデイ攻撃や、長期間にわたってターゲットを分析して攻撃するAPT攻撃（Advanced Persistent　Threat：持続的標的型攻撃）などはシグネチャベースのツールでは検知できない。攻撃者が社内に侵入していても、全く気づかないという恐れもあるのだ。

社内・社外の場所に関係なく、
エンドポイントを守れるような防御体制が必要

と考えていました。

Intercept Xは、この要件に最適なソリューションでした。

導入コストがそれほど高くなかった点も選定の決め手となりました。

トーヨーカネツ株式会社
コーポレート本部　総務部 情報システムグループ
堀 聖彦 氏

実害は被らなかったものの、サイバー攻撃が対岸の火事ではないと感じるような出来事もあった。ビジネスを装って金銭をだまし取る「ビジネスメール詐欺（BEC：Business E-mail Compromise）」が横行した2〜3年前に、同社にも攻撃者からのメールが届いたという。

情報システムグループでは自社のセキュリティ対策を見直すため、2018年に外部のコンサルティング会社の診断を受けた。この結果を示すなど、経営層にセキュリティ対策の強化が必要なことを訴えた結果、投資に向けた意思決定が下された。

テクノロジーソリューション

新たなソリューションを検討するに当たって、情報システムグループは付き合いのあったベンダーに相談を持ちかけた。合計で16ものソリューションの説明を受けたという。そうした中で、新たに導入するツールに対して次のような要件を固めていった。

大前提となるのが、シグネチャに頼らずに未知の脅威にも対応できることだ。これに加えて、社内のネットワークに接続された端末だけでなく、社外からアクセスする端末を防御できることも要件の一つに掲げた。情報システムグループでセキュリティ対策の中核を担っている堀聖彦氏は「ネットワークの境界を防御するだけではなく、端末やサーバーなどのエンドポイントそのものを守りたいと考えました」と語る。この要件に当てはまるのが、次世代のセキュリティ対策とも呼ばれる「EDR（Endpoint Detection and Response）」に分類されるソリューションだ。

運用管理が容易であることも重要な要件だった。対象となるPCは合計で約1000台。情報システムグループに属する11人の社員のうち、セキュリティ対策を担当しているのは堀氏を含めて2〜3人しかいない。どんなに高機能なソリューションであっても、日常の運用に大きな手間がかかるのではセキュリティ対策が破綻する恐れがある。

この要件で絞り込んだところ、6種のEDR製品が選定対象に残った。情報システムグループが最終的に選んだのが「Sophos Intercept X」である。最新のテクノロジーが搭載されたEDR製品であることに加え、ほかのソリューションよりも圧倒的にコストパフォーマンスが優れていた点が決め手になったという。

Intercept Xは、クラウドと連携してさまざまな脅威を検知してエンドポイントを防御する機能を備えている。 マルウエア対策では、 シグネチャを使わずにディープラーニング（深層学習）技術でマルウエアを検知することが大きな特徴だ。 世界に5拠点あるソフォスの研究所「SophosLabs」が持つ100万件以上のマルウエアサンプルを教師データとして学習したAI（人工知能）エンジンを搭載。このエンジンが、エンドポイントで実行されるマルウエアの特徴を自動的に検知する。学習データは常に更新されるため、最新の脅威にも対応。ゼロデイ攻撃やAPT攻撃など、シグネチャでは検知できないような未知の脅威にも対応できるのだ。

ランサムウエア対策機能である「CryptoGuard」も搭載する。これは、ファイルやフォルダの暗号化が始まると同時にファイルのバックアップを実行する機能。暗号化が正規のソフトやユーザーの意図によるものあれば、そのまま暗号化を継続させる。もしも、悪意あるプロセスによる暗号化であれば、この処理を自動的にブロックするとともに、バックアップからファイルを自動的に復元する。

運用管理も容易だ。ソフォスのソリューションにはベストプラクティスのポリシー設定がビルトインされているからだ。設定変更も「Sophos Central」というクラウドベースの管理コンソールから一元的に実行できる。

導入した結果

トーヨーカネツは3ヶ月の準備期間を経て2019年9月からの約1カ月で全社への導入を完了。導入後には月に50件から100件のマルウエアを侵入前に駆除しているという。駆除されたマルウエアの経路をたどれることに加え、最新のセキュリティパッチが適用されていない端末も容易に把握できるようになった。さらに、クライアントの状況をレポート化して経営層へ定期的に報告できるようになったので、経営層のセキュリティへの関心の高まりにもつながっているという。宮川氏は「将来的にはゼロトラストモデルとDLP（Data Loss Prevention：情報漏洩対策）を実現したいと考えています」と抱負を語る。

現在、同社は「攻め」のIT投資に向けて「土台づくりのまっ最中」（宮川氏）だという。セキュリティツールというと「守り」の役割だと考えがちだが、今回のシステムは「攻め」へ向けた取り組みの土台として位置付けられる。社外からでもオフィス内にいるときと同様にPCを利用できるようになり、ビジネスの機動力向上につながるからだ。

SOPHOS