日立ソリューションズ

HITACHI
Inspire the Next

導入事例

株式会社 白鳩 様

CylancePROTECT®

インナーウェアの通販を保護する AI(機械学習)を活用したマルウェア対策製品

京都を拠点にインナーウェアのインターネット通信販売事業を運営する
株式会社 白鳩(以下、白鳩)は、
顧客情報と購買履歴情報の漏洩を防ぐためのソリューションとして、
次世代マルウェア対策製品「CylancePROTECT」を導入。
検討開始から約2カ月という短期間で全社稼働にこぎつけました。
AIを活用したマルウェア対策により社内のセキュリティレベルは向上し、
それまで使用していた製品より、運用管理の工数も減少しました。

BlackBerry CYLANCE × SHIROHATO®

課題

- 既存製品はパターンファイルの更新が不安定
- 運用管理で手作業が散発的に発生

効果

- パターンファイルの配布方式ではないため、PCへの適用漏れがなく高精度なマルウェア対策が可能に
- 実用的なGUIの統合監視コンソールにより、手間を掛けない管理を実現

背景と課題

従前のセキュリティ対策では管理に多大な手間

白鳩は、男女のインナーウェアやルームウェアを、主にインターネットで販売している企業です。取り扱いブランド数は百数十、品番(SKU)の数は約13,000と多品種です。国内外からの注文は、京都にある本社内の配送センターから出荷しています。

その白鳩は、情報漏洩を防ぐためのセキュリティ対策に力を注いできました。通信販売において、商品配送と請求・入金業務には、顧客の氏名・住所・電話番号などの個人情報を保有する必要があるからです。またインナーウェアという商品の特性上、注文の詳細についても同様レベルでの漏洩防止対策が求められます。そのため個人情報保護法に規定されている安全管理措置にあるマルウェアの侵入を防ぐ仕組みは、欠かせない対策の一つでした。

そこで、以前からパターンファイル方式のマルウェア対策ソフトウェアを採用して、社内のパソコンにマルウェア対策を施していました。マルウェアが見つかるのは年に数件というレベルでしたが、検出能力に特に不満はなく、統合監視コンソールを使った集中管理も的確に行ってきました。もちろん、プライバシーマークも取得済みです。

「ただ、毎日使われているはずのパソコンが最新のパターンファイルに更新されていないというケースが時々起きていました。そのようなパソコンを監視コンソールで見つけたら、IT資産管理ツールにより、外部からエージェントを再インストールし最新の状態にするのですが、何らかの理由で失敗してしまうこともあります。その場合は、現場に直接出向き、手作業でエージェントを入れ替えるしかなく、ICT管理課にとっては結構な手間でした」(福井氏)

選定と導入

CylancePROTECTのPoCで検知能力と操作性を検証する

この状況を変えるには、マルウェア対策ソフトウェアをほかの製品に替えればよいのではないか——。

従来のマルウェア対策ソフトウェアの契約更新が迫った2019年11月、白鳩のICT管理課は製品乗り換えの道を探り始めました。新しく導入する製品に求める要件は、従来の製品と比較して、同等以上のマルウェア検知能力を持つことと、統合監視コンソールによる集中監視が可能で、運用管理に手間が掛からないことです。

Interview

株式会社 白鳩
ソリューション事業部
ICT管理課
課長代理
福井 智之 氏

株式会社 白鳩
ソリューション事業部
ICT管理課
武内 数磨 氏

相談を受けた日立ソリューションズは、AIを活用した次世代マルウェア対策製品「CylancePROTECT」を提案。さらに、評価用ライセンスを使ったPoC（概念実証）により、検知能力と操作性を検証することを勧めました。

PoCがスタートしたのは、11月中旬。「CylancePROTECT」の評価テストは少数のパソコンで動作検証を行うのが一般的ですが、白鳩は最初から多数のパソコンで実施することにしました。

「まず、ICT管理課の近くにあるパソコン約10台にIT資産管理ツールを使ってエージェントを一括配信するところから始めました。エンドユーザーには知らせずに実施しましたが、もちろん、何か問題が起きたらいったん立ち止まって考えるつもりでした。特に問題がなかったので、PoCの対象を順次拡大していき、11月末にはほとんどの社内パソコンへの組み込みが完了しました」（武内氏）

「『CylancePROTECT』を組み込むとすぐに全ファイルのスキャンが始まり、怪しいと思われるファイルが次々とリストアップされます。その多くは日立ソリューションズから『このようなファイルがマルウェアの可能性があるとして検出されているが、もし業務で必要なファイルである場合は、ホワイトリストに登録することでそれ以降は検出されないようになる』と教えられたので、それらをホワイトリストに登録していきました。また、エンドユーザーが使用した覚えがないものについては、隔離を実施。必要と確認された場合にはいつでも復元できるようにしました」（福井氏）

PoCが順調に進んだ背景には、統合監視コンソール用のサーバーを新たに設置・構築する必要がないこともありました。「CylancePROTECT」はクラウドで集中管理をする方式なので、従来は何週間も掛かっていたサーバー初期設定作業が不要です。また、以前から使っていたマルウェア対策ソフトウェアが見逃していたマルウェアらしきものも検出可能と確認したICT管理課は、PoCの中盤から「CylancePROTECT」のインストールと同時に既存製品をアンインストール。契約が完了すれば、すぐに本稼働に切り替えられる状態にしました。

2019年12月中には契約などの手続きが無事完了。「CylancePROTECT」は2020年1月1日から白鳩社内のすべてのパソコンで稼働を始めました。

成果と今後

使いやすい監視コンソールで管理の手間を削減

PoCの段階で既存製品のアンインストールを済ませていたこともあって、白鳩でのマルウェア対策ソフトウェアの乗り換えは無事に完了しました。セキュリティ上の空白期間が生じることもなく、顧客の個人情報や購買履歴情報は確実に保護されています。

「ファイルのスキャンに時間が掛かってパソコンが使えないなどの苦情がエンドユーザーから寄せられることもなく、『CylancePROTECT』はスムーズに稼働しています。あるパソコンだけが古いパターンファイルで稼働しているといったこともなくなったので、管理の手間も掛からなくなりました」（福井氏）

「『CylancePROTECT』の監視コンソールはシンプルな作りで、とても使いやすいGUIだと思います。どこにどんな機能があるかがすぐに分かり、操作に迷うことはありません。また日立ソリューションズの丁寧なサポートもあり、助かっています」（武内氏）

白鳩が社員に支給しているパソコンは、1人に1～2台。このほか、送り状の印刷などに使われているインターネット非接続のパソコンにも「CylancePROTECT」を組み込み、インターネットとのゲートウェイに設置した統合型ファイアウォールと組み合わせることによって、同社のセキュリティ対策をより強化することができました。

「2020年夏には本社の新社屋が完成し、当社はそちらに移転する予定です。パソコンの台数が増えるため、『CylancePROTECT』のライセンスを買い足さなければと考えています。また今後は、メールの誤送信防止や添付ファイルの自動暗号化といったセキュリティ対策にも着手する予定です。最近はクラウド方式のソリューションが増えてきたので、安価に利用可能になるのではと見越しています」（福井氏）

さらに白鳩では、セキュリティに対する社員の意識を高めるための取り組みにも力を入れています。同社の基幹システムはパブリッククラウド上で稼働しており、メールシステムなどにもクラウドサービスを利用中。そうした環境に即した使い方のルールも、業務の円滑な遂行を妨げない範囲で明文化していくことをめざしています。

個人情報の漏洩が決して許されないインターネット通販で、購買履歴情報の慎重な取り扱いが特に求められるインナーウェア類を販売している白鳩。セキュリティレベルを高め、安心・安全な業務体制のために、日立ソリューションズはこれからもさまざまな製品・サービスで同社を支援していきます。

Company Profile

株式会社 白鳩

本社所在地	京都府京都市伏見区竹田向代町21番地
設立	1974年8月20日
創業	1965年10月1日
従業員数	174人（2019年2月末時点）
事業内容	インナーウェアのインターネット販売および直営店舗「SHIROHATO」運営

https://www.shirohato.co.jp/

本事例のwebページはこちら
www.hitachi-solutions.co.jp/cylance/case13/

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/cylance/

J19S-11-04　2023.07