日立ソリューションズ

HITACHI
Inspire the Next

パートナー事例

株式会社インターネットイニシアティブ 様

CylancePROTECT®

重要性を増すエンドポイント対策の商材として、機械学習を用いたマルウェア対策製品を採用

日本初の国内インターネット接続事業者として1992年に創業した
株式会社インターネットイニシアティブ(IIJ)。
同社は、セキュリティ事業における新たな取り扱い商材として、
エンドポイントマルウェア対策製品を検討。
評価検証を経て、機械学習による検出エンジンを搭載した
「CylancePROTECT」を採用しました。

BlackBerry
CYLANCE
×
IIJ Internet Initiative Japan

採用のポイント

- 日々増え続ける未知のマルウェアに対して、有効な対策であること
- 煩雑な設定が不要で、導入後の運用が容易に行えること

特長

- 機械学習を用いることにより、「既知」「未知」を問わず、マルウェアの高精度な検知が可能
- クラウド上の管理コンソールから運用ポリシーなどの各種設定を行うことができ、運用者の負荷を軽減

採用の経緯とポイント

圧倒的な検知率の高さと、運用のしやすさが採用のポイント

IIJは、1994年より20年以上にわたりセキュリティビジネスを展開しており、主として、セキュリティ防御対策サービスの提供と、お客様の個別の要望に応じたインテグレーションビジネスを手がけています。こうした状況で、「CylancePROTECT」に着目したポイントは大きく2つあります。

1つは、未知のマルウェアに対して有効な対策であることです。従来のパターンマッチングによるマルウェア対策では、日々増え続ける新たなマルウェアに対して、後手に回ってしまいます。そこで有効なのが「CylancePROTECT」です。

「弊社では、機械学習をはじめとするAIの活用を、全社で積極的に進めていこうと考えています。また、セキュリティについては、脅威と対策がいたちごっこの状態で、今後、IoTで多くの『モノ』がネットワーク接続される中で、セキュリティ対策とインシデント検知、対応の時間軸は変わってきます。その構造を打ち破る新たなアプローチの対策製品や技術を探していました」(神田氏)

「ゲートウェイでのセキュリティ対策についてはサンドボックスなどの技術がかなり普及しつつありますが、攻撃を100%止めることはできていません。そこで、昨今は改めてエンドポイント対策が重要視されつつある状況です」(神田氏)

「近年、従来型のパターンマッチングによるエンドポイントマルウェア対策製品のマルウェア検知率低下が課題となっています。そのため最近では、マルウェア感染を前提に、侵入後の対応に注力するEDR(Endpoint Detection and Response)製品に注目が集まってきています。しかし、我々は、検知率を高めていく余地がまだあるのではないかと考えており、そのようなアプローチのエンドポイント製品はないのかと探していました」(加賀氏)

「CylancePROTECT」は機械学習を用いることにより、「既知」「未知」を問わず、マルウェアの高精度な検知を実現しています。

もう1つは、導入後の運用がしやすいことです。

「他製品は導入、実装のために必要な設定が細かくできる代わりに、運用が非常に煩雑という問題がありましたが『CylancePROTECT』は、クラウド上の管理コンソールから必要な設定を簡単に行うことができ、導入するお客様にメリットが高いと考えます」(松本氏)

「CylancePROTECT」は、クラウドサーバ上で運用ポリシーなどの各種設定を行うことでエンドポイントを管理できます。また、拠点が分散している環境でも一元管理が可能で、運用者の負荷を軽減します。

Interview

株式会社
インターネットイニシアティブ
セキュリティ本部
副本部長
神田　恭治 氏

株式会社
インターネットイニシアティブ
セキュリティ本部
セキュリティビジネス推進部
インテグレーション課長
松本　弘明 氏

株式会社
インターネットイニシアティブ
セキュリティ本部
セキュリティビジネス推進部
インテグレーション課
シニアテクニカルマネジャー
加賀　康之 氏

検討時の取り組み

評価検証により、検知率の高さと誤検知の少なさ、運用面での使い勝手を確認

「CylancePROTECT」の本格的な評価検証は、2016年4月頃から行われました。評価検証には大きく2つのポイントがありました。

「1つ目は、メーカーから公開されている検知精度と相違ないかを検証するために、社内にある独自の検体を使って、検知するかどうかを客観的に評価しました。また、OSや他のアプリケーションに対して悪影響がないかといった点や、誤検知のリスクについても時間をかけて確認しました。

2つ目は、業務端末にエージェントをインストールし、通常業務に支障がないかの運用テストを行いました。営業部門や開発部門など、徐々に適用部門を広げ、100台以上で評価しました。運用テストの中で、保守サポートに必要なリモートアクセスツールを、検知の対象外とする設定を行うなど、いくつかの除外設定はあったものの、大きな問題はありませんでした」（松本氏）

その後、いくつかの課題を解消して、2016年5月にパートナー契約を締結しました。

採用後

日立ソリューションズのサポート体制、製品の検知精度には満足

2016年5月から「CylancePROTECT」の販売を開始し、お客様への提案、導入が進んでいます。日立ソリューションズには、仕様についての問い合わせ対応など迅速で満足しています。今後も、メーカーへの改善要望など代理店としてのサポートに期待しています。

「日立ソリューションズには、課題やトラブル発生時の対応も手厚く、スピーディーに動いていただいています。たとえば、トラブル発生時の環境を日立ソリューションズ側でも用意していただき、同じ現象を再現させる事などを協力してもらっています。また、メーカーと連携して、さらなる製品の機能改善に今後もご協力をいただけると嬉しいです」（松本氏）

「日立ソリューションズとは、『CylancePROTECT』以前にも、ファイアウォール製品などで取引がありました。これまで様々な海外メーカーのセキュリティ製品の一次販売代理店を手がけた実績があり、販売支援から導入後の保守サポートについても期待しています」（加賀氏）

また、社内の各部署で評価導入をしていますが、誤検知などによる業務への影響もでていません。

「社内展開後、ある程度の誤検知も覚悟していましたが、現時点では誤検知はほとんどありません。ファイルが隔離されたり、使えないアプリケーションがあったりしたら知らせるよう周知していますが、最初に数件報告があった程度で、ホワイトリストの登録などの設定を行えば必要なファイルやアプリケーションが誤検知されることはありません」（松本氏）

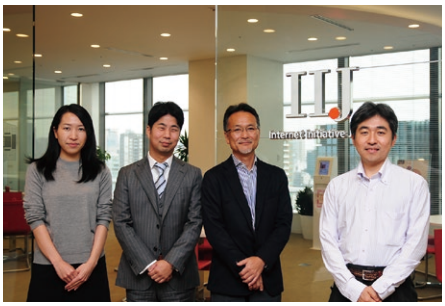
今後の展望

さらに付加価値の高いソリューションに育てていきたい

「CylancePROTECT」が、お客様にとってより良い製品になっていくことを期待しています。

「弊社が管理するプライベートクラウド環境に管理サーバーを構築できるようになれば、さらに付加価値を高めることができます。たとえば、仮想デスクトップと組み合わせれば、マネージド環境でトラフィックを完結でき、よりセキュアに利用できるようになります。また、ネットワーク使用量を節約することができ、さらなるお客様のメリットにつながると思います」（松本氏）

「機械学習のアルゴリズムがこのソリューションの一番大事なコア技術で、メーカーはそこに多くのリソースを注いでいると思います。しかし、お客様に導入した後は、運用のしやすさも同じくらい重要になってきます。コア技術は大事にしつつ、導入、運用のしやすさについて日立ソリューションズに協力いただきながら、継続的な機能改善を期待します」（神田氏）



セキュリティ本部の皆様

Company Profile

株式会社インターネットイニシアティブ

本社所在地	東京都千代田区富士見2-10-2 飯田橋グラン・ブルーム
設立	1992（平成4）年12月3日
従業員数	3,108名（連結）
事業内容	インターネット接続サービス、WANサービスおよびネットワーク関連サービスの提供など

http://www.iij.ad.jp/

本事例のwebページはこちら
www.hitachi-solutions.co.jp/cylance/case04/

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/

J17K-05-05　2023.07