リアルな企業のニーズから知る、いまEDTDが求められる理由とは?

従来のマルウェア対策だけでは十分に防げない、ゼロデイ攻撃をはじめとした未知の攻撃が急増したことにより、多くの日本企業が脅威に晒されている。このような状況を受け、キヤノンマーケティングジャパン(キヤノンMJ)が2019年5月にリリースしたのが、法人向けESETセキュリティ ソフトウェア シリーズのクラウド型ゼロデイ攻撃対策製品「ESET Dynamic Threat Defense(EDTD)」だ。既存のESET製品と連携し、ゼロデイ攻撃に用いられる未知の高度で巧妙なマルウェアに対する検出力・防御力をさらにもう一段高めるクラウドサービスであるEDTDは、リリースから1年を待たずに数多くの日本企業に導入され、実績を上げている。

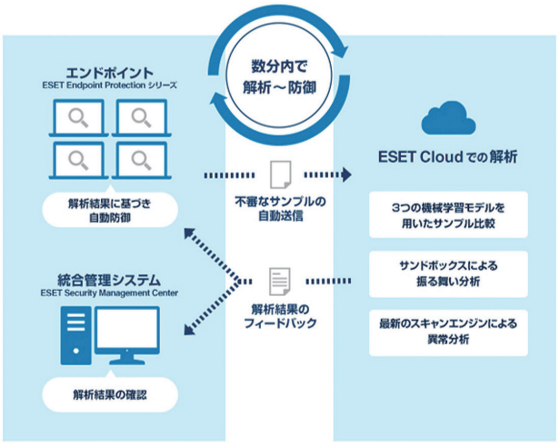
そこで本稿では、日々顧客の声を直接聞いている、キヤノンMJ セキュリティソリューション企画本部 セキュリティソリューション事業企画部 セキュリティソリューション促進第一課 峯森 惇平氏にインタビューを行った。同氏はセキュリティ専門家として、社内や販売パートナーの営業担当者へ技術的なアドバイスを行い、パートナー各社のスキルアップに取り組むなど、各種支援を行う立場にある。エンドポイントセキュリティに対する各社の具体的なニーズや課題感、得られた成果について、EDTDに関する具体的な顧客の声を聞いた。

キヤノンマーケティングジャパン株式会社
セキュリティソリューション企画本部
セキュリティソリューション事業企画部
セキュリティソリューション促進第一課
峯森 惇平氏

脅威の防御

クラウド型ゼロデイ攻撃対策　ESET Dynamic Threat Defense

未知の高度な攻撃をクラウドテクノロジーで自動解析・自動防御



- NGAV的なクラウドサービス
- 100%白黒判定ができない不審なサンプルをクラウドで自動送信し、多段階に解析
- 解析は数分で完了、悪質な場合は全端末にフィードバックされ自動ブロック
- サンプルの解析結果をレポートとして可視化
- エージェントレス

クラウド型ゼロデイ攻撃対策製品「ESET Dynamic Threat Defense(EDTD)」

実際に触ってもらうことで良さを実感してもらえる

――エンドポイントセキュリティ対策について、各企業ではどのような意識を持っていると感じますか。

峯森氏：サイバーセキュリティ対策のなかでも、エンドポイントセキュリティ対策を特に強化しなくてはならないという意識を強く感じます。サプライチェーンに関する国内のさまざまなガイドラインでも、最近はエンドポイントセキュリティの強化を要件としているケースが増えているので、そうした影響も大きいのではないでしょうか。

とりわけ当社のコアドメインである中堅中小企業では、SSL/TLSで暗号化された通信をデコードしきれないゲートウェイセキュリティ製品を使用しているケースが多いです。するとメールやWebを通じて送り込まれる不正なファイルなどもエンドポイントだけで防御しなくてはならないので、より関心が高くなります。

――エンドポイントセキュリティを強化すべく、ESET製品を導入した企業の規模や業界などの分布を教えてください。

峯森氏：業界についてはほぼ偏りはなく幅広い業界で導入いただいています。企業規模に関しては最も多いのは数台から数百台ライセンスの規模ですが、最近では1,000台を超える規模の企業も増えています。

――どのような点を評価してESET製品を導入しているケースが多いのでしょうか。

峯森氏：導入前は軽快な動作やコストパフォーマンスを評価いただいて決定されるケースが多く、導入後にはそれらに加えて安定性や運用のしやすさ、サポートの質の高さなどを評価いただくケースが多いと感じています。一方、ESET製品を販売する営業担当者からは、実際に試用してもらえば良さがわかってもらえるので、とても販売しやすい製品だという声をよく聞きますね。

NGAVを検討する企業が増えている背景とクラウド型ゼロデイ攻撃対策製品EDTDが選ばれる理由

――NGAV（次世代アンチウイルス）に関して、企業の担当者はどれぐらい必要性を感じていると見ていますか。

峯森氏：現在では新種や亜種のマルウェアが1日あたり数十万件も出現するようになっているので、不審なファイルを検出できるようになるまでの「早さ」を求める傾向は急速に強まっています。当然そのようなお客様はNGAVを検討するようになるので、ニーズは確実に増えていますね。ただし、まだまだ「投資」ではなく「コスト」と捉える企業も多いことから、費用との兼ね合いで断念して現状に甘んじてしまうケースもあるようです。

――NGAVを検討している企業が結果としてEDTDを導入するケースも多いと聞きました。問い合わせをするまでの経緯には、どのようなものが目立ちますか。

峯森氏：最近、攻撃者はメインターゲットの大企業や公的機関を直接狙うのではなく、よりセキュリティレベルの低い取引先や子会社などを標的にして攻撃するサプライチェーン攻撃が増えています。そのため多くの企業や公的機関では、取引先や子会社などに対して、より進んだセキュリティ対策を求めるガイドラインを課すようになっています。セキュリティ強化の要望に応えるべくNGAVを比較検討するなかで、EDTDの存在を知ってお問い合わせいただくケースが多いと感じます。

――導入前の企業はEDTDに対して、どのようなイメージや期待を持っているのでしょうか。

峯森氏：高度かつ巧妙なゼロデイ攻撃のリスクに「いち早く」対応を行うためのツールというイメージが強いのではないでしょうか。これに加え、ESET製品において基本となるアンチウイルス製品「ESET Endpoint Protection（EEP）」をすでに利用していただいているお客様には、EEPの魅力のひとつである動作の軽快さを、EEPとクラウド連携するEDTDであれば損なわないという点も評価いただいています。

また、当社としてはEDTDに対してNGAVという側面からのプロモーションはこれまで積極的に行っていなかったので、検討をはじめた当初はNGAVだとは知らなかったというお客様も多いです。しかしEDTDについてご説明すると、限りなくNGAVと近いことができるとおわかりいただけるようです。さらに、ESET Security Management Center（ESMC：管理サーバー）の設定画面からEDTDを有効にするだけで、あとは自動的に連携して処理が実行され、未知や亜種のマルウェアも検知できるようになるという導入・運用のしやすさ、単体ソリューションでないことによる低コストさなども、多くのお客様から評価いただいています。

――すでにESET製品を利用している企業がEDTDを追加する理由は、どのようなものが多いですか。

脅威の防御

エンドポイント保護プラットフォーム　ESET Endpoint Protectionシリーズ

アンチマルウェアを中心とした、エンドポイントセキュリティ対策の基盤

- 軽快な動作、誤検知率の低さ
- 高い検出力を支える、機械学習やヒューリスティックなどのテクノロジー
- 複数の高度なテクノロジーにより、エンドポイント単体で多層防御を実現
- 実行前・実行時・実行後の複数タイミングでもれなく検査

ESET製品において基本となる「ESET Endpoint Protection（EEP）」

峯森氏：これまでもお話したように、導入が非常に簡単であることが大きいでしょうね。既存のESET製品も多層防御により高い検知率を誇っているためお客様満足度も高いのですが、前述のようにサプライチェーン側からの要望でエンドポイントセキュリティ対策の強化が迫られているケースが増えています。そうしたなか、既存のEEPに追加するだけで、サンドボックスの機能や機械学習（AI）の技術を取り入れた最新のクラウドセキュリティソリューションが使えるようになるというのは、大きな魅力に感じていただけるようです。

――新規の顧客についてはいかがでしょうか。

峯森氏：ESET製品を新規に検討されているお客様には、提案時に評価版を発行させていただいています。検証時に他社のアンチウイルスソフトでは検知できなかったマルウェアをEDTDが検知するケースも多くあり、EDTDの性能を体感していただくとともに、その必要性を感じて導入いただくというケースが目立っています。

――では、EDTDの導入後に寄せられる声としてはどのようなものがありますか。

峯森氏：EDTDは未知の脅威に対する自動防御も可能ですので、とにかく運用が楽だという声をよく聞きますね。もちろん、EDTDを利用していたために未知の脅威から自社を守ることができたというケースも数多くありますが、お客様にとってもセキュリティ上の機密事項ですので、具体的にお話することではできません。 当社のエピソードであればDoc/Agent.DZの事例※を報告しているので、ご確認ください。

より広い企業に
より素早い防御を提供していく

――これからEDTDの導入を検討しようとしている企業に向けてメッセージをお願いします。

峯森氏：マルウェアはますます高度化かつ巧妙化していますので、その対策として、検知率だけでなく、導入・運用のしやすさや費用対効果にも優れた製品を検討したい場合には、ぜひ一度EDTDを評価いただきたいです。EEPの軽快な動作と高い検出力に加え、ゼロデイ攻撃のリスクにいち早く対応できることを、きっと実感していただけるはずです。

――最後に、EDTDに関する今後の展開を聞かせてください。

峯森氏：すでに2020年2月に実施済みですが、多くのお客様からのご要望に応えて、EDTDの提供範囲をこれまでの最小250ライセンスから最小100ライセンス以上へと大幅に

拡大しました。これにより、サイバー攻撃のターゲットとなりやすい大企業はもちろん、サプライチェーン攻撃で狙われるその関連会社や子会社でも未知の脅威に対する体制を整えることができるはずです。

そして次のバージョンアップでは、プロアクティブな防御機能が備わる予定ですので、未知の脅威の防御もこれまで以上に素早く行えるようになるでしょう。

――未知の脅威への防御力もより強力になりそうですね、ありがとうございました。

※ キヤノンMJ運営 マルウェア情報局「2019年6月 マルウェアレポート」より

クラウド型ゼロデイ攻撃対策製品

ESET DYNAMIC THREAT DEFENSE

イーセット ダイナミック スレット ディフェンス

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/edtd/

ESET Endpoint Protectionシリーズの検出力・防御力をさらに高めるクラウドサービスです。ゼロデイ攻撃に用いられるような未知の高度なマルウェアに対する検出・防御の即時性を高め、ESET Endpoint Protectionシリーズのユーザーは、端末への新規プログラムインストールをする必要がなく、手軽に多層防御機能を強化することができます。

開発元：ESET, spol. s r.o.

製品に関する情報はこちらでご確認いただけます。

セキュリティソリューション ホームページ
canon.jp/it-sec

●お求めは信用のある当社で

キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南2-16-6 CANON S TOWER

2020年4月現在
MEDET20041000MUR-645