net one Partners

ディープラーニングによる「予防ファースト」であらゆるプラットフォームのデータを保護

従来のマルウェア対策の限界を破った「Deep Instinct Data Security X」

過去から現在に至るまで、外部からの脅威の侵入を防ぐアンチマルウェア製品は、企業のセキュリティ対策として活用されてきました。それでも侵入を100%防ぐことができないことから、昨今では侵入を前提とした対策であるEDRなどの対策が広まっています。こうした「従来の侵入防御対策」「侵入を前提とした事後対策」では、防御が不十分であることや運用負荷が高いなどの課題があります。そこで今改めて注目を集めているのが、ディープラーニング技術によって従来型セキュリティ対策の限界を打ち破った「Deep Instinct Data Security X」です。

複雑化するサイバー攻撃と企業が対応してきたセキュリティ対策

サイバー攻撃によって企業の重要情報が漏えいする事故が後を絶ちません。IPA（情報処理推進機構）が2025年1月に発表した「情報セキュリティ10大脅威 2025」によると、主要な脅威としては「ランサム攻撃による被害」「サプライチェーンや委託先を狙った攻撃」「システムの脆弱性を突いた攻撃」「機密情報等を狙った標的型攻撃」であり、この傾向は10年ほど大きく変わっていません。

こうした脅威の多くは企業の重要な情報の窃取を目的としています。デジタル化が進んだ今日では、データが企業の重要な経営資産となっており、サイバー攻撃者はいかにしてそうしたデータを奪い、企業から金銭を脅し取れるかどうかに最大限の力を注いでいるのです。

もちろん企業は、ランサムウェア対策やサプライチェーン対策、脆弱性対策、標的型攻撃対策に予算をかけて取り組んできました。しかし、サイバー攻撃は減るどころか増えており、被害総額や被害対象も広がっているのが現実です。

サイバー攻撃に対して、効果的なセキュリティ対策を講じることがなぜ難しいのか。様々な対策で語られているようにデータの置き場所は多様化しています。オンプレミス環境だけでなく、複数のデータセンターやクラウドサービス、工場や店舗などのエッジ環境にまで多岐にわたっています。

一方で、サイバー攻撃自体は非常に巧妙でありながら簡単なものになってきています。かつてサイバー攻撃は技術力を持つ限られた人間が主導するケースがほとんどでしたが、誰でも簡単に攻撃に参加できるようなツールがダークWeb上に存在し、攻撃手法も未知の脆弱性を突く高度な攻撃やAIを使った攻撃も行われています。

セキュリティ対策は、話題になったサイバー攻撃にその都度対応するように強化されてきた経緯がありますが、攻撃側と防御側はいたちごっこになりやすく、その結果として侵入されることを前提としたEDR（Endpoint Detection & Response）製品の導入が進められてきました。

従来型セキュリティ対策の問題点

しかしそもそもなぜ従来型セキュリティ製品は攻撃を検知しにくくなったのでしょうか。

従来は、基本的にシグネチャと呼ばれるマルウェアを識別するためのパターンを用意しておき、それに該当する場合は検知するというパターンマッチングの方式を採用しています。しかし、この方式では未知のマルウェアから攻撃を受けた場合に対応できません。近年では、新種のマルウェアが生成されるスピードはかつてないほど高まっており、防御側がそれに追いつかない状況になっています。

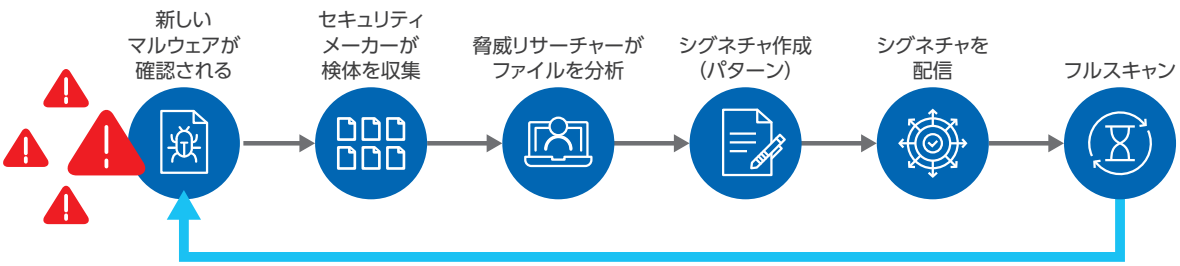
もちろん、これらの課題に対応するためにさまざまな新しい技術が開発されてきました。例えば、疑わしいと思われるファイルを安全な隔離環境で展開して挙動を確認するサンドボックスや機械学習によってその振る舞いを分析する手法などが代表的です。

ただ、こうした機能も攻撃側が作り出す亜種の量や、巧妙な攻撃を確実に検知することは難しいのが現状です。例えば、サンドボックスで挙動を確認しても未知の脅威は正しい検出ができなかったり、機械学習による振る舞い分析でも検知率の限界や誤検知が多いという課題が残りました。

改めて検討するべき「侵入の防御」

上記の背景から、脅威の侵入を100%防ぐことが困難になったために事後対策を行うという考え方が普及してきました。しかし、侵入を前提とした対策は既に侵入されてしまった状態であり、対応は必然的にリアクティブなものになります。またログデータの蓄積や解析など運用コストも高いという課題があります。本来の目的は会社の重要な資産である「データ」を守ることにあります。複雑な分析や高いコストで運用することではありません。侵入の段階で脅威を大幅に削減できればEDR/NDRに代表される事後対策側での運用負荷の低減、コスト低減を実現できるようになります。

これを実現するためには、昨今の巧妙な攻撃を受けても侵入を予防できる、より優れた次世代の技術にアップグレー



日々膨大に発生する未知マルウェアに対しては間に合わない!

シグネチャに依存した脅威の検知の方式は、昨今のマルウェア生成のスピードに追いつかない

ドする必要があります。具体的にはディープラーニングによる高度な学習モデルによって、未知のマルウェアでも非常に高い精度で侵入を防ぐことができる技術です。これを実現する製品については後ほど解説します。

企業が見過ごしがちな対策と盲点

昨今のセキュリティ動向を踏まえてもう1つ重要な視点があります。ここまで侵入前に防ぐか侵入後に対処するかという点を触れてきましたが、企業が最終的に守るべき重要なものの1つが「データ」です。ランサムウェアをはじめデータを標的とする攻撃が広まる中では、企業はそうしたデータを起点に対策を考える「データセキュリティ」の視点を持つ必要があります。

例えば、DDoS攻撃を受けてサーバがダウンするケースを考えてみましょう。確かに業務に影響は及ぶものの、データそのものが奪われるわけではなく、攻撃者としては売却できる材料を得ることもできません。そのため企業に対する脅しとしての効果は限定的です。一方で、企業の重要なデータが失われたり、外部に流出した場合はどうでしょうか。顧客情報や知的財産が漏洩すれば、信用の失墜や法的責任、さらには事業継続への影響といった深刻な問題につながります。だからこそ、ランサムウェアは企業にとって大きな脅威となり、データそのものを保護することが極めて重要なのです。

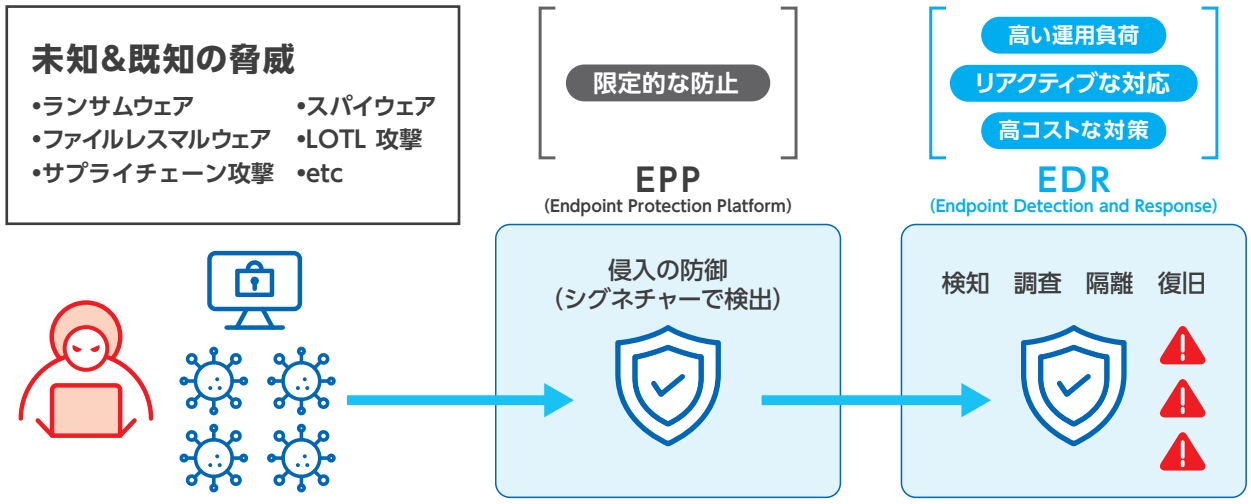
もっとも、対策を行うことは容易ではありません。なぜなら持っているデータは顧客ごとに違い、その重要性もまたそれぞれだからです。そのためにはデータ1つひとつの中身を可視化して重要性を分類し、ポリシーなど定義していかなければなりません。これだけデータが膨大で、保存場所も点在している中でそれを完結させるのは大変な時間と労力が必要になります。

高度なAI技術を活用した Deep Instinct Data Security X

データセキュリティを実現するために、データの棚卸しから管理ポリシーの策定、リスクの評価、対応の優先順位付けなど、全社的で長期にわたる取り組みが必要になります。しかし、ここに時間をかけて対策しているだけでは攻撃者の後手を踏み続けることになりかねません。もちろん将来的にはこうした対策を迅速に実現するためのツールも出てくる可能性がありますし、DLP対策などはそのためのものでもありますが、まだまだ時間と労力を掛けたソリューションであるのが現実です。だからこそ、今できる対策=外部の巧妙な攻撃からデータを守ることから始めるべきではないでしょうか。

これを実現するのが「Deep Instinct」です。同社は2015年に米国で設立されたセキュリティ企業であり、特許取得済みの独自ディープラーニングフレームワークによる脅威検知の仕組みを最大の特徴としています。世界2000社、200万ユーザーに採用されています。

Deep Instinctは2024年に製品群を「Data Security X（DSX）」へリブランドし、現在では「ディープラーニングによって、あらゆる脅威を阻止する予防ファースト」と「あらゆるプラットフォームのデータを保護するアプローチ」をコンセプトとし、データセキュリティを包括的にサポートするソリューションを提供しています。具体的には4つの製品で構成されており、エンドポイントにおいて脅威の侵入を阻止する主力製品「DSX for Endpoints」のほか、カスタムアプリケーション（ファイル転送、メール、開発基盤など）向けの「DSX for Applications」、従来のNASストレージ向けの「DSX for NAS」、クラウドストレージ向け「DSX for Cloud」があります。



限定的な防止であった「侵入の防御」を新たな仕組みに刷新すればEDRの負荷も軽減可能

●ディープラーニングによる
アンチマルウェア生成エンジンDSX Brain

サイバーセキュリティ専用にゼロから設計された世界で唯一のディープラーニングフレームワークを使い、Deep Instinctが提供する全プラットフォームでリアルタイムに脅威を判定し防御できる、市場で最も高速かつ効果的なゼロデイ脅威予防ソリューションです。

●エンドポイント向け次世代アンチウイルス製品
DSX for Endpoints

従来のEPP/EDRでは止められない脅威を侵入時で食い止める圧倒的な予防力を持ったエンドポイント製品です。未知の脅威でも99%以上で防御し、0.1%の誤検知率という高い精度を実現しています。AIモデルを歪ませる敵対的AIの攻撃や複雑な攻撃にも対抗し、エンドポイントでのマルウェア感染を防ぐことができます。また、パターンファイル更新や定期的なフルスキャンが必要ないため、運用がシンプルであることも大きなメリットです。

●カスタムアプリケーション向けDSX for Applications

サービス基盤等既存のワークフローとREST API またはICAPにて連携させることで高いスピード、拡張性、柔軟性によりアプリケーション上での悪意のあるファイルを検知するエージェントレスのファイルスキャン製品です。クラウドに依存せずクローズド環境でも動作する点、悪性・良性を高速に判定できる性能や膨大なファイルもスキャンできる拡張性が特徴です。

●ストレージ向けDSX for NAS

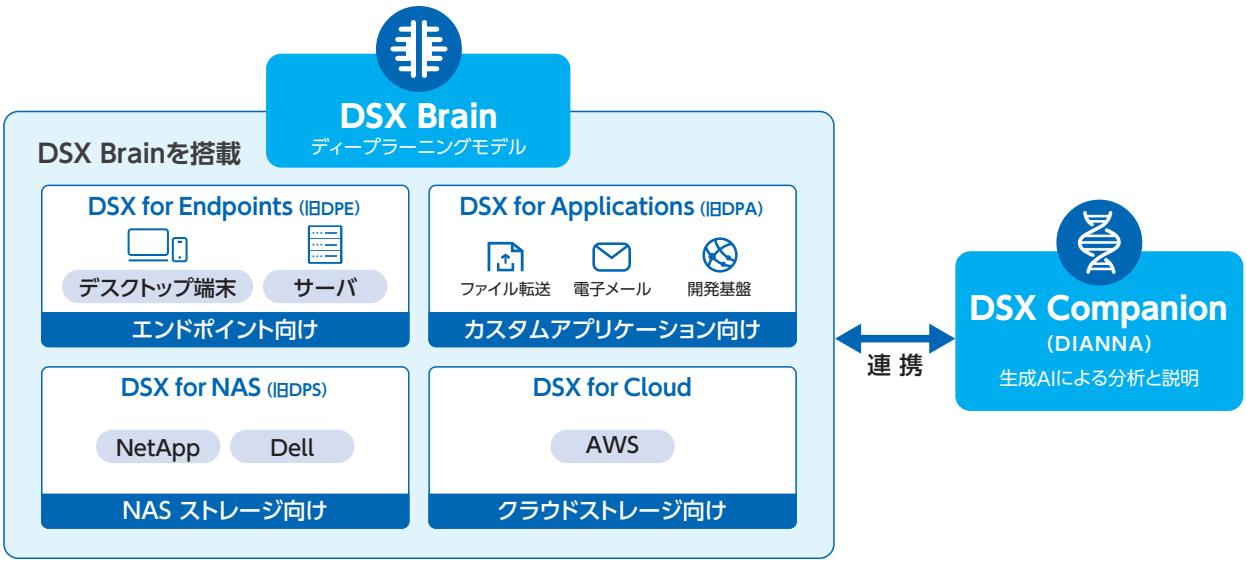
ストレージ製品上でのランサムウェアやその他マルウェアのファイル混入による感染リスクを減らし 大切なデータを脅威の侵入から保護する製品です。ストレージインフラストラクチャと簡単に統合し、現状ではDell EMCとNetApp とのスキャン連携に対応しています。

●クラウドストレージ向けDSX for Cloud

クラウド上のマルウェア混入による被害からデータを保護します。Amazon S3環境に対応しており、同環境上の悪意のあるファイルを隔離することができます。効率的なスキャンによる高いコスト効率とCloudFormationテンプレートを使用した高速デプロイが特徴であり、自動スケーリングとロードバランシングにも対応します。

これらの4製品に加え、Deep Instinctでは、生成AIによって多様なマルウェア検体の分析と解説レポートを提供する「DSX Companion」を提供し、セキュリティ運用業務を支援します。

経営資源となった重要データをサイバー攻撃から守るためには、シグネチャベースのマルウェア対策では不十分であり、かといってEDRのような事後対策に依存することは運用やコストの観点から非常に難易度が高いと言えます。全体最適の視点で必要なのは、予防と事後対策をバランスよく実施することです。ぜひ、Deep Instinctを活用してコスト効果の高いセキュリティ対策を実現していただければと思います。



Deep Instinct Data Security Xの全体像

net one Partners

問合わせ先
ネットワンパートナーズ株式会社　https://www.netone-pa.co.jp/
本　社　〒100-7025 東京都千代田区丸の内 2-7-2 JPタワー
西日本オフィス　〒532-0003 大阪市淀川区宮原 3-5-36 新大阪トラストタワー