Symantec™ Advanced Threat Protection 2.2: Platform

データシート: Advanced Threat Protection

現状と課題

今日の高度で執拗な攻撃では、脆弱性、ソーシャルエンジニアリング、フィッシング Web サイト、あるいはこれらを組み合わせた手法が用いられます。いずれの場合も、標的の企業に侵入するためにエンドポイントシステムが利用されます。攻撃者は、企業のインフラに入り込むと、エンドポイントシステムを使用してネットワークを探索し、資格情報を盗み出してコマンドアンドコントロールサーバーに接続します。企業の重要なシステムとデータを侵害するためです。

問題は拡大の一途をたどっています。2015 年には 4 億 3,000 万件もの[1]新種のマルウェアが発見されました。シマンテックでは 2015 年以降、ゼロデイ脆弱性の 125% 増と標的型攻撃の 55% 増も確認しています。今や、脅威を防ぐだけでは十分とはいえません。攻撃者の動きは加速しています。遅かれ早かれ、攻撃者に侵入される日が来るでしょう。最新のレポート[2]によると、企業が脆弱性を発見してから修復するまでに平均で 120 日かかるといわれています。脅威を検出できず対応が遅れると、企業は脅威にさらされて大きな損失を被ります。知的財産や機密データの流失、財務的損失、企業イメージの低下、その他の損失が発生するでしょう。さらに、大量のアラートと感染ユーザーへの対応で IT 部門に大きな負担がかかり、ビジネスの混乱を招く可能性すらあります。

ソリューションの概要

Symantec™ Advanced Threat Protection Platform

Symantec™ Advanced Threat Protection（ATP）ソリューションは、複数の制御ポイントにわたって高度な脅威の検出から優先順位付け、調査、修復までを単一のコンソールから実施できる統合プラットフォームです。それぞれの制御ポイントは、攻撃者が企業に侵入するときに利用する経路を表します。現在、ATP: Endpoint、ATP: Network、ATP: Email、ATP: Roaming という 4 つの ATP モジュールが用意されています。これらのモジュールがそれぞれ異なる制御ポイントからのイベント情報を ATP プラットフォームに送信し、ATP プラットフォームがこれらの悪質なイベントを相関付けして優先順位を付けるため、セキュリティアナリストは最も深刻なイベントに集中して対応できます。

Symantec ATP は、世界最大規模の民間脅威インテリジェンスネットワークとローカルの企業のコンテキストを利用して、他の製品では検出できないステルス性の高い脅威を検出します。企業を狙った攻撃が現在活動中だと判明した時点で、インシデント対応者に通知が送信されます。Symantec ATP では攻撃の詳細情報も提供されるため、すべての脅威インスタンスに分単位で対処できます。新しいエンドポイントエージェントを配備する必要なく、複数の制御ポイントにわたって高度な脅威の検出、優先順位付け、修復を単一のコンソールから実行できる業界初のソリューションです。

1. 『シマンテックインターネットセキュリティ脅威レポート第 21 号』、2016 年 4 月
2. Dennis Technology Lab 社、2015 年 12 月

主な機能と特長

- 複数の制御ポイントにわたって高度な脅威の検出、優先順位付け、調査、修復を単一のコンソールから実行
- エンドポイント、ネットワーク、電子メール、Web トラフィックをすべてカバーしてステルス性の高い脅威を検出
- 包括的な可視化と早急な修復を実現するため、シマンテック製品の保護下にある各種制御ポイントのイベントで相関分析を実施、深刻度に応じて優先順位付け
- 1 回のクリックにより攻撃アーティファクトを分単位で封じ込めて修復
- 公開 API とサードパーティ製 SIEM との統合により、インシデント対応フローをカスタマイズ

複数の制御ポイントで高度な脅威を検出

すべての脅威データを 1 カ所で確認

統合プラットフォームである Symantec Advanced Threat Protection（ATP）ソリューションは、複数の制御ポイントで検出された悪質な活動を 1 つのビューにまとめて表示します。電子メールと Web は依然として悪質な攻撃の侵入経路として使用されることが多く、すべての攻撃でエンドポイントが標的になっています。シマンテックでは、高度な保護を提供するとともに IT 環境の脅威を包括的に可視化するため、4 つの ATP モジュールを用意しています。

1）ATP: Endpoint

新しいエンドポイントエージェントを配備する必要なく、エンドポイントにおける検出および対応（EDR）機能を提供します。業界最高レベルの脅威防御製品 Symantec Endpoint Protection を利用します。エンドポイントから侵害の兆候（IoC）を検出し、ワンクリックですべての脅威インスタンスを分単位で修復できます。

2）ATP: Network

ファイルレピュテーション分析、IPS、クラウドホスト型のサンドボックス、デトネーションなど複数のテクノロジを活用して、ステルス性の高い脅威を検出します。ネットワーク全体で IoC を検索し、悪質だと特定されたファイルや URL をブラックリストまたはホワイトリストに登録できます。

3）ATP: Email

スピアフィッシングなど電子メールを通じた標的型攻撃や高度な脅威から保護します。クラウドホスト型のサンドボックスおよびデトネーションと、Symantec Email Security.cloud を利用して、悪質な電子メールの脅威データを詳細に検出します。サードパーティ製 SIEM との緊密な統合で、攻撃に迅速に対応できます。

4）ATP: Roaming

企業ネットワーク外からインターネットにアクセスするユーザーを高度な脅威から保護します。クラウドホスト型のサンドボックスを利用して、暗号化トラフィックに潜む高度な脅威も検出して対処します。ユーザーがどこからアクセスしていても、Web トラフィック内の脅威を詳細に可視化します。

物理環境と仮想環境の両方に対応するサンドボックス

シマンテック製品は最新の高度に複雑な標的型攻撃を検出するために Cynic™ テクノロジを利用しています。これはシマンテックが独自に開発したもので、サンドボックス機能とペイロードデトネーション機能をクラウドベースで提供します。Cynic は高度な機械学習とグローバル脅威インテリジェンスを組み合わせ、ステルス性と持続性の高い脅威さえも検出します。詳細なデトネーションレポートには、プロセスやスタックのトレースのほか、ネットワークトレース(コマンドアンドコントロールの呼び出しトラフィック情報など)も含まれています。そのため、インシデント担当者はすべての関連情報を 1 カ所で入手して、攻撃コンポーネントに対して迅速な対処が行えます。今日、高度な攻撃の 28% は「仮想マシン認識型」です。通常のサンドボックスシステムで実行しても、疑わしい振る舞いを見せることはありません。これに対抗するため、Cynic には人間の振る舞いを模倣する回避対策テクノロジが組み込まれています。さらに、不審なファイルを物理ハードウェアでも実行し、従来のサンドボックステクノロジをすり抜ける攻撃でも検出します。

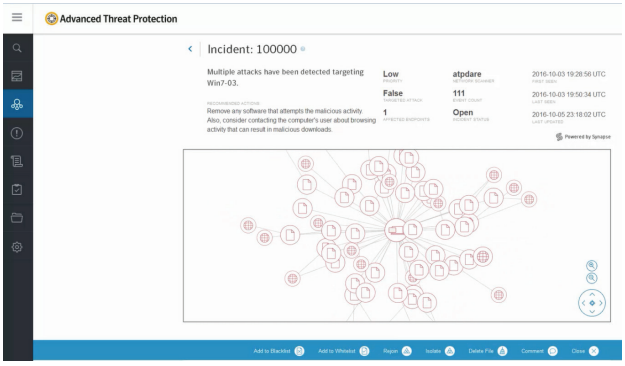
侵害の兆候を瞬時に検索

Symantec Advanced Threat Protection は、Dynamic Adversary Intelligence という新しい機能も備えています。標的型攻撃に関する包括的な調査から得られた実用的なインテリジェンスデータを、利用価値の高いフィードとして提供します。自社が脅威グループに狙われているかを迅速に確認できるため、標的型攻撃に対してより適切な対応がとれます。既知の侵害の兆候が含まれていないかどうか、新しい Dynamic Adversary Intelligence フィードが環境全体を自動的に検索するため、標的型攻撃を検出するまでの時間を短縮できます。

深刻なイベントの自動優先順位付け

現在のインシデント対応者はあまりにも多くのアラート処理に追われ、対応待ちのインシデントは増えるばかりです。Symantec Advanced Threat Protection ソリューションはシマンテック独自の Synapse 相関分析テクノロジを利用して、すべての制御ポイントで検出された疑わしい活動を集約します。Synapse は、タイプやスコープ、複雑性などのさまざまな属性を基に、脅威の優先順位を自動的に決定します。多発するアラートに悩まされることなく、最も深刻なイベントに集中対応し、特定の重要なイベントへの対応だけに注力できます。侵害を受けていて早急な対応を要するシステムがあれば、アラートですぐに通知されます。

複雑な攻撃も分単位で修復



Symantec Advanced Threat Protection をお使いになると、悪質なイベントが確認された際に、脅威のすべてのインスタンスに分単位で対処できるようになります。ボタンを 1 回クリックするだけでファイルを瞬時に削除したり、ファイルやドメインをブラックリストまたはホワイトリストに登録したりできるほか、企業内またはインターネット上の他のエンドポイントと通信できないようにエンドポイントを隔離できます。Symantec ATP Platform では、攻撃に関わる侵害の兆候についてすべての相互関係を含めた情報も、分かりやすく表示されます。アナリストはインシデントの影響を簡単に把握できるほか、特定の攻撃に使用されたファイル、ファイルのダウンロード元の IP アドレスや URL、影響を受けたレジストリキーなどをすべて、見やすい表示で確認できます。1 回のクリックで攻撃アーティファクトに対処できるため、攻撃の拡散を効果的に抑制できます。

既存の資産を活用

シマンテック製品への投資を最大限に活用

Symantec Advanced Threat Protection（ATP）ソリューションは、Symantec Endpoint Protection と Symantec Email Security.cloud という先進的な製品から脅威イベントを収集します。現在 Symantec Endpoint Protection を使用している場合は、新しくエンドポイントエージェントを配備しなくても、Symantec ATP Endpoint モジュールでエンドポイントにおける検出および対応（EDR）機能が提供されます。また、現在 Symantec Email Security.cloud を使用している場合は、Symantec ATP Email モジュールを入手すると、新しいエージェントを配備しなくても標的型攻撃やスピアフィッシング攻撃からの保護が可能です。

シマンテック以外の既存製品の活用

インシデント対応やセキュリティ監視を行うため、多くの企業には何らかのセキュリティ製品がすでに配備されています。Symantec Advanced Threat Protection はサードパーティ製の SIEM（Security Incident and Event Management）に豊富なインテリジェンスをエクスポートします。公開 API があれば、これまでに投資してきたそれらの製品も脅威調査に利用できます。さらに、Symantec Advanced Threat Protection は、SIEM の Splunk およびワークフローの ServiceNow という 2 つの有力な製品と統合されました。これにより、特別な設定なしでシマンテック製品の API を簡単に使用できるようになっています。このように自社のインシデント対応フローを最適化してカスタマイズできるため、既存の資産を最大限に活用できます。

シマンテックのサービスでセキュリティを最適化し、リスクを最小に、利益を最大に

どうぞセキュリティエキスパートにお問い合わせください。Symantec Advanced Threat Protection のトレーニング、プロアクティブな計画策定、リスク管理のほか、お客様に合わせたソリューションの導入、構成、評価も承っております。詳しくは、https://www.symantec.com/ja/jp/services/ をご覧ください

詳細情報

シマンテックの Web サイト

https://www.symantec.com/ja/jp/advanced-threat-protection/

株式会社シマンテック

〒107-0052 東京都港区赤坂1-11-44 赤坂インターシティ

www.symantec.com/jp

お問い合わせ

E1612DS0-IN-21369562