Symantec™ Advanced Threat Protection 2.2: Network

データシート: Advanced Threat Protection

現状と課題

今日の高度な攻撃は、正当な Web サイトの陰に隠れ、新種または未知の脆弱性を悪用し、ネットワークベースの各種プロトコルを通じて標的の企業に侵入しています。これらの攻撃は通常のネットワークベースのセキュリティ対策をすり抜けるように設計されています。こうして攻撃者は被害者のインフラに侵入し、重要なシステムとデータを侵害します。ネットワークセキュリティ製品がこれらの攻撃を認識できた場合でも、特定の攻撃についての詳細情報は優先度の低い長大な警告リストの陰に埋もれていることが多く、アナリストが本当の問題を見い出すことは非常に困難です。

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: Network

Symantec™ Advanced Threat Protection: Network は Symantec™ Advanced Threat Protection（ATP）ソリューションを構成するモジュールの 1 つです。エンドポイントからネットワーク、電子メール、Web トラフィックまでを幅広く網羅して、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ます。このソリューションは、ハードウェアアプライアンスと仮想マシンのどちらでもご利用いただけます。Symantec ATP: Network はシマンテックの大規模なグローバルセンサーネットワークによるインテリジェンスを活用して、単体製品では見逃してしまう脅威を検出して調査します。ネットワークを出入りする全トラフィックを監視するため、高度で多彩な検出テクノロジを利用したトラフィック検査が可能です。

疑わしいファイルは Symantec Cynic™ サンドボックスシステムに自動送信されるので、最も複雑で検出の難しい高度な攻撃でも素早く検出できます。Symantec Advanced Threat Protection の Endpoint モジュール、Email モジュール、Roaming モジュールを併用することも可能です。これにより、それらの制御ポイントで検出された脅威イベントを Symantec ATP で相関分析してインシデントに優先順位を付与できるため、最も深刻なインシデントに集中対応できます。シマンテック製品の保護下にある企業内の制御ポイントで発生した関連イベントが、シマンテックの Synapse™ 相関分析テクノロジによって自動集約されるため、高度な攻撃の活動を 1 カ所から確認できます。

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. 『Kenna Security Report, 2015（2015 年 Kenna セキュリティレポート）』

主な機能と特長

- Symantec™ Advanced Threat Protection: Network をインストールしてから標的型攻撃の検出の開始まで 1 時間弱
- シマンテック製品の保護下にある各種の制御ポイントのイベントで相関分析を実施して最も深刻なインシデントに優先度を付与することで、セキュリティアナリストが調査すべきインシデント件数を大幅に削減
- レピュテーション分析、IPS、シマンテック独自のクラウドベースのサンドボックスとデトネーションなど多彩なテクノロジを活用して、他の製品では見逃されるステルス性の高い脅威も検出
- ファイルや URL が悪質と判断された時点で、ブラックリストまたはホワイトリストに登録
- 公開 API、サードパーティ製の SIEM、ワークフローツール統合を使用して、社内のインシデント対応フローをカスタマイズ
- ハードウェアアプライアンスと仮想マシン(VM)のどちらでも利用可能

高度な攻撃の検出

業界最高レベルの検出能力と精度[3]

Symantec Advanced Threat Protection: Network は、一般的なネットワークプロトコルを通じて企業に侵入しようとする高度な脅威を検出します。今日のネットワーク保護ソリューションは、攻撃の検出手段としてサンドボックス機能に大きく依存しています。一方、Symantec Advanced Threat Protection: Network は、Cynic の革新的なサンドボックスやデトネーションに加えて、各種の保護テクノロジをすべて備えています。

Symantec ATP: Network はレピュテーションベースのテクノロジである Symantec™ Insight を活用して、ファイルが最初に確認された時期、インターネットでのファイルの拡散状況など、数多くの高度な技術に基づいて疑わしいファイルを特定します。また、受信した疑わしいネットワークトラフィックを特定できるほか、悪質なコマンドアンドコントロールサーバーと通信しているネットワーク内のマシンを発見するのにも役立ちます。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 Symantec DeepSight™ からのデータフィードにより、インターネット上の新しい攻撃ソースについて最新状況を把握することができます。

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。Symantec ATP: Network は、企業が受信した疑わしいファイルを自動的に Cynic に送信します。Cynic はグローバル脅威インテリジェンスを統合した機械学習ベースの高度な分析を利用して、ステルス性や持続性が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を検出します。

3 Dennis Technology Lab 社、2015 年 12 月

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

Symantec Advanced Threat Protection: Network は、Symantec Advanced Threat Protection 製品シリーズの一部です。このシリーズには Network のほかに、Endpoint、Email、Roaming というモジュールが用意されています。Symantec ATP には Symantec™ Synapse 相関分析テクノロジが搭載されており、すでにインストールされている Symantec Endpoint Protection や Symantec Email Security.cloud を利用して、制御ポイントで発生した疑わしい活動を集約します。

この相関分析テクノロジは、タイプやスコープや複雑性などのさまざまな属性を基にして、脅威の優先順位を自動的に決定します。たとえば、従来型のネットワークセキュリティ製品が、企業内の従業員のマシンに送信された不審なファイルを検出したとします。これまでは、セキュリティアナリストは不審なファイルを受信したエンドポイントマシンに手動でアクセスして、そのファイルが適切にブロックされているか、このコンピュータから削除されているかを確認する必要がありました。Symantec Advanced Threat Protection: Network では、ネットワークに潜在的な脅威が侵入したことが検出されると、Synapse 相関分析テクノロジによって、エンドポイントの Symantec Endpoint Protection でその脅威がブロックされているかどうかが自動的に判別されます。脅威がブロックされている場合、それらの攻撃にはアナリストのリスト上で低い優先順位が付与されます。そのため、アナリストが調査する対象となるセキュリティイベントの件数を大幅に削減できます。

既存の資産を活用

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。公開 API があれば、予算を投じ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。

Symantec Advanced Threat Protection: Network を新しく導入してから攻撃の検出が開始されるまで、わずか 1 時間足らずです。また、この製品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。たとえば、「ウイルス BAD.EXE が検出されました」といった従来のセキュリティデータではなく、「コンピュータ A が Web サイト C.com から B.EXE というファイルをダウンロードしました」といった詳細なデータをエクスポートできます。さらに、Symantec Advanced Threat Protection: Network は Symantec™ Managed Security Services で監視できます。

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

システム要件

ユーザーインターフェース用のブラウザクライアント

Microsoft Internet Explorer 11 以降
Mozilla Firefox 26 以降
Google Chrome 32 以降

仮想アプライアンスの配備

VMware® ESXi 5.5、6.0
Intel 仮想化テクノロジ対応

仮想マシン（VM）の要件

- CPU x 4（物理または論理）
- 32 GB 以上のメモリ
- 500 GB 以上のディスク容量

物理アプライアンスの配備

	アプライアンスモデル 8840	アプライアンスモデル 8880
フォームファクタ	1U ラックマウント	2U ラックマウント
CPU	Intel Xeon 4 コア x 1	Intel Xeon 14 コア x 2
メモリ	32 GB	96 GB
ハードディスク	RAID 1 2 x 1TB ドライブ	RAID 10 4 x 300GB HDD 400GB SSD Write Intensive x 1
電源	350W 冗長 PSU x 2	750W 冗長電源 x 2
ネットワークインターフェースカード	1 ギガビットイーサネットカード x 2 1 ギガビット内蔵イーサネット x 2	10 ギガビットイーサネットポート x 4 1 ギガビット内蔵イーサネット x 4
	WAN と LAN のペア x 1 管理ポート x 1 iDRAC ポート x 1	WAN と LAN のペア x 2（10 ギガビット） 管理ポート x 1（1 ギガビット） iDRAC ポート x 1

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