Symantec ™ Endpoint Protection 14

データシート : エンドポイントセキュリティ

概要

昨年は、4 億 3,100 万もの新しいマルウェアの亜種が確認され、ランサムウェア攻撃は多様化し、2 倍以上のゼロデイ脅威が発生しました[1]。企業は、今日の大規模で複雑なネットワークと、急速に進化する脅威の対応に苦慮しています。マルウェアの感染阻止に向けて、多数のベンダーや新興企業が新しい方法やポイントソリューションを提供しています。しかし、それらによる保護はどれも限られたものです。エンドポイントセキュリティは依然として重要ですが、効果的なソリューションの提供はかつてないほど困難になっています。

今日の高度な脅威から保護するためには、エンドポイントを標的としたあらゆる手口による脅威を阻止する必要があります。これを実現するには、次のような機能が必要です。

- 未知の脅威を検出してランサムウェアやゼロデイ攻撃を阻止する高度な技術
- 広く普及しているアプリケーションやオペレーティングシステムを狙うメモリ悪用の防止
- リアルタイムで脅威を防止する、世界でも最高クラスに充実したグローバル脅威インテリジェンスへのアクセス
- 脅威を迅速に阻止するための、対応の統合運用管理
- パフォーマンスに影響を与えずにすべてのデバイスに実証済みの保護策

Symantec Endpoint Protection 14 は、攻撃チェーン全体を対象として多層防御を提供する包括的なアプローチで、最新の脅威に対応するように設計されています。Symantec Endpoint Protection 14 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を活用して、多次元機械学習、レピュテーション分析、リアルタイムの振る舞い監視を利用した次世代の技術により、高度な脅威を効果的に阻止します。また、企業全体を保護するうえで同じくらい重要となる、基本的な防御技術も備えています。Symantec Endpoint Protection 14 は、セキュリティインフラの他の製品と統合できる単一の管理コンソールと軽量のエージェントによって、脅威への迅速な対応を行います。これにより、パフォーマンスに影響を与えずにクラス最高のエンドポイント保護[2]を提供します。

攻撃チェーン全体に包括的な保護

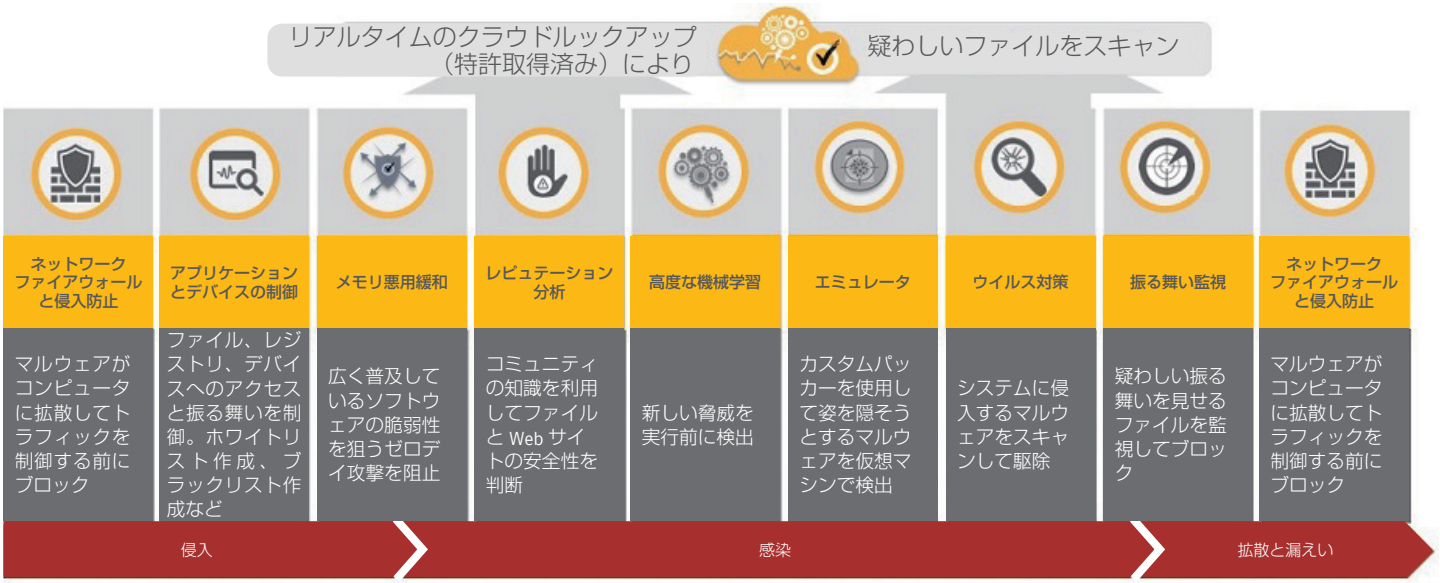
次世代の技術と基本技術とを組み合わせることにより、エンドポイントがどのような攻撃を受けても、パフォーマンスに優れた軽量のエージェントが高度な脅威や急速に変異するマルウェアを阻止します。

侵入:

- **ネットワーク侵入防止、URL とファイアウォールポリシー:** シマンテックのネットワーク脅威防止技術は、ネットワーク内を流れる受信データと送信データを分析し、脅威がエンドポイントに到達する前に阻止します。Web ベースの攻撃から保護するために、ルールベースのファイアウォールおよびブラウザ保護機能が用意されています。基本的に、強力なネットワーク保護を備えておけば、エンドポイントに到達する前に脅威の半分以上を検出できます。

[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 2016 年版』
[2] AV-TEST.Org から 2016 年 Best Protection Award を受賞

- **アプリケーション振る舞い制御:** ファイルおよびレジストリへのアクセスと、プロセスの実行方法を制御します。
- **デバイス制御:** 選択したハードウェアのアクセスを制限し、情報をアップロードまたはダウンロードできるデバイスの種類を制御します。外部メディア制御をアプリケーション制御と組み合わせて、より柔軟な制御ポリシーを適用することもできます。
- **悪用防止:** 広く普及しているソフトウェアでベンダーからパッチがまだリリースされていない脆弱性を狙った Heap Spray、SEHOP 上書き、Java エクスプロイトなどのゼロデイ攻撃でも、無効化します。この技術はシグネチャ不要であり、欠陥、バグ、脆弱性の有無にかかわらず機能します。



感染:

- **悪用防止:** マルウェアを検出して感染を防止する役割も果たします。
- **レピュテーション分析:** シマンテックのインテリジェンスネットワークを利用した独自のレピュテーション分析で、数百億におよぶユーザー、ファイル、Web サイトの関連付けを行います。これにより多くの脅威を未然に阻止するとともに、急速に変異するマルウェアから防御します。ファイルのダウンロード回数、生存期間、ダウンロード元などの主要なファイル属性を分析します。これにより、ファイルがエンドポイントに届く前にファイルが悪質かどうかを正確に判別するとともに、レピュテーションスコアを付与します。ファイルレピュテーションを利用すれば、スキャンの対象はリスクを伴うファイルだけに絞れるので、処理の負荷を大幅に軽減できます。
- **機械学習:** エンドポイントでの多次元機械学習によって新しい未知の脅威を阻止できるので、シグネチャへの依存を減らすことができます。グローバルインテリジェンスネットワークで把握している安全なファイルと悪質なファイルの数兆個のサンプルを使用して機械学習のトレーニングを行うことで、極めて低い誤検知率を実現します。
- **エミュレーション:** 高速エミュレータは、ポリモーフィック型カスタムパッカーを使用して姿を隠そうとするマルウェアを検出します。静的データスキャナは、軽量の仮想マシンを用いて数ミリ秒で各ファイルを実行することにより脅威の正体を暴くので、検出率もパフォーマンスも向上します。
- **ウイルス対策ファイル保護:** シグネチャベースのウイルス対策機能と高度なファイルヒューリスティックによって、システム上のマルウェアをスキャンして駆除し、ウイルス、ワーム、トロイの木馬、スパイウェア、ボット、アドウェア、ルートキットから保護します。

- **振る舞い監視:** Symantec Endpoint Protection に搭載された振る舞い監視は、少数の脅威がエンドポイントまで検出されずに到達した場合でも、非常に効果的です。機械学習を利用してゼロデイ攻撃からの防御を実現するとともに、実行中のファイルの振る舞いを約 1,400 の条件に基づいてリアルタイムで監視してリスク判断を行い、新しい未知の脅威を効果的に阻止します。

拡散と漏えい:

- **振る舞い監視:** 振る舞い監視は、感染の拡大を阻止する役割も果たします。
- **ネットワーク侵入防止、URL とファイアウォールポリシー:** ネットワークを流れる受信データと送信データを分析して、脅威を阻止します。

グローバル脅威インテリジェンス: シマンテックの次世代技術では、リアルタイムのクラウドルックアップ技術（特許取得済み）を利用して、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にすばやくアクセスできます。これにより、脅威の最新手口に関する詳細な情報を機械学習で取り込み、リアルタイムで更新されるクラウドアルゴリズムを使用してすべてのエンドポイントの保護を最大限に強化できます。157 カ国に配備された 1 億 7,500 万のエンドポイントと 5,700 万の攻撃センサーから収集されたデータが、高度なスキルを持つ 1,000 人以上の脅威研究者によって分析されます。その結果を取り入れた革新的かつ最先端のセキュリティソリューションで脅威に対抗するのです。

高度な機能により、優れたパフォーマンスを実現

Symantec Endpoint Protection に搭載された多彩な技術は、ネットワーク速度やユーザーの業務を妨げないように最適化されています。第三者機関によるパフォーマンステストでも、一貫して最高レベルの結果を出しています。

- Intelligent Threat Cloud の高速スキャン機能は、パイプライン、信頼伝搬、バッチクエリーなどの高度な技術を採用しています。そのため、すべてのシグネチャ定義をエンドポイントにダウンロードしなくても高い効果を発揮できるようになりました。最新の脅威情報のみがダウンロードされるため、シグネチャ定義ファイルのサイズが最大 70% 削減され、使用する帯域幅も少なくなっています。
- エンドポイントでの高度な機械学習により効果がさらに増すため、ダウンロード回数が減るほか、誤検知による業務中断に伴う生産性の低下も最小限に抑えられます。
- 単一の軽量エージェントは、機械学習、悪用緩和、エンドポイントにおける検出および対応（EDR）、マルウェア対策など、通常ならば複数のエージェントが必要になるほどの多彩な技術と機能を兼ね備えています。これにより、エンドポイントの管理対象エージェントの数を減らしてパフォーマンスを向上できる可能性があり、それと同時に IT 部門の負担と総所有コストを低減できます。

簡単な統合により、エンドポイントでの対応を統合運用管理

Symantec Endpoint Protection が備える単一のコンソールとエージェントは、オペレーティングシステム、プラットフォーム、あらゆる規模の企業に保護を提供します。

- **Power Eraser:** リモートで実行できる強力なツールで、APT（Advanced Persistent Threat）を検出して執拗なマルウェアを除去します。
- **ホストインテグリティ:** ポリシーを適用し、不正な変更を検出し、被害を評価することで、エンドポイントを確実に保護してポリシーへの準拠を確保します。管理対象システムが要件を満たしていない場合には、隔離することもできます。脅威検出製品と併用して、感染したエンドポイントを隔離するための対応を統合運用管理すれば、エンドポイントの修復またはイメージの再適用が完了するまでの間、感染の拡散をいち早く阻止できます。

- **システムロックダウン:** 問題ないと確認済みのホワイトリストアプリケーションのみ実行を許可するか、問題のあるブラックリストアプリケーションの実行を阻止することができます。Symantec Advanced Threat Protection（ATP）と Secure Web Gateway では、プログラム可能な API を使用して SEP 管理（SEPM）コンソールと通信するとともに、新しく検出された悪質なアプリケーションがあればアプリケーション制御を使用してブラックリストに登録する対応を統合運用管理します。Windows®、Mac®、Linux®、仮想マシン、組み込みシステムに対応しています
- **Secure Web Gateway との統合:** 新しいプログラム可能な REST API により Secure Web Gateway などの第三者の製品と統合することで、エンドポイントでの対応を統合運用管理して、感染の拡大を迅速に阻止できます

- **EDR コンソール（ATP:Endpoint）との統合:** Symantec Endpoint Protection は、攻撃に優先順位を付けることで APT や標的型攻撃を検出、対応、阻止する Symantec EDR コンソール（Advanced Threat Protection（ATP:Endpoint））と統合されています。EDR（エンドポイントにおける検出および対応）機能は Symantec Endpoint Protection に組み込まれているため、追加のエージェントを配備する必要はありません。

保護、パフォーマンス、対応

Symantec Endpoint Protection はエンドポイント保護において不動のリーダーです。

- SE Labs 社[3] による採点で何度も AAA 評価（最も高いスコア）を獲得[3]
- A/V Test[4] で、18 カ月連続してゼロデイ攻撃を 100% 防御
- Gartner 社のマジッククアドラント[5] で、14 年連続して「リーダー」に選出

[3] SE Labs 社 : https://selabs.uk/en/reports/enterprise
[4] AV Test: https://www.av-test.org/en/antivirus/business-windows-client/
[5] Gartner 社のマジッククアドラント（2016 年 2 月）

クライアントワークステーションおよびサーバーシステムの要件 *	
Windows オペレーティングシステム	**仮想環境**
Windows Vista（32 ビット、64 ビット）	Microsoft Azure
Windows 7（32 ビット、64 ビット、RTM、SP1）	Amazon WorkSpaces
Windows 7 Embedded Standard	VMware WS 5.0、GSX 3.2、ESX 2.5 以降
Windows 8（32 ビット、64 ビット）	VMware ESXi 4.1 ～ 5.5
Windows 8 Embedded（32 ビット）	VMware ESX 6.0
Windows 8.1	Microsoft Virtual Server 2005
Windows 10	Microsoft Enterprise Desktop Virtualization（MED-V）
Windows Server 2008（32 ビット、64 ビット、R2 を含む）	Microsoft Windows Server 2008、2012、2012 R2 Hyper-V
Windows Essential Business Server 2008（64 ビット）	Citrix XenServer 5.6 以降
Windows Small Business Server 2011（64 ビット）	Oracle VM Virtual Box
Windows Server 2012（64 ビット、R2 を含む）	**Linux オペレーティングシステム(32 ビット版および 64 ビット版)**
Windows Server 2016	Red Hat Enterprise Linux
Windows ハードウェア要件	SUSE Linux Enterprise（サーバー / デスクトップ）
1 GHz 以上の CPU	OEL（Oracle Linux）
512 MB の RAM（1 GB を推奨）	CentOS
1.5 GB のハードディスクの空き容量	Ubuntu
Macintosh オペレーティングシステム	Debian
Mac OS X 10.9、10.10、10.11、Mac OS 10.12	Fedora
Mac ハードウェア要件	**Linux ハードウェア要件**
64 ビット Intel Core 2 Duo 以降	Intel Pentium 4（2 GHz 以上の CPU）
2 GB の RAM	1 GB の RAM
500 MB のハードディスクの空き容量	7 GB のハードディスクの空き容量

Manager のシステム要件	
Windows オペレーティングシステム	**ハードウェア**
Windows Server 2008（64 ビット、R2 を含む）	Intel Pentium デュアルコアまたは同等品以上
Windows Server 2012（R2）	2 GB の RAM（8 GB を推奨）
Windows Server 2016	ハードディスクに 8 GB 以上の空き容量
Mac ハードウェア要件	**データベース**
Microsoft Internet Explorer	埋め込みのデータベースが付属。または次から選択 :
Mozilla Firefox	SQL Server 2008 R2、SP3、SP4
Google Chrome	SQL Server 2012（RTM）- SP1、SP2
Microsoft Edge	SQL Server 2014、RTM、SP1
	SQL Server 2016

* システム要件の一覧についてはシマンテックのサポートページをご覧ください

** Symantec ™ Endpoint Protection 12.1.6 MP1a でサポートが追加されました

注意 : Symantec ™ Endpoint Protection 12.1.6 MP2 は Mac OS X10.11 をサポートしています

詳細情報

無償体験版をご利用ください

60 日間の無償体験版をダウンロードして、業界をリードするエンドポイント保護のソリューションをお試しください。

https://trial.symantec.com/lp?pid=1-ja-jp&q=2r.3r.5r.6.7r.9r&cid=70150000000bxraAAA

Gartner 社がエンドポイント保護プラットフォームの Magic Quadrant でシマンテックをリーダーとして格付けした理由について、第三者によるレビューをご参照ください。

http://www.symantec.com/endpoint-protection/news-reviews

シマンテックの Web サイト

http://www.symantec.com/jp または http://go.symantec.com/sep

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

E1610DS0-IN-21320633-6