セキュリティ

Symantec™ Endpoint Protection 14

世界No.1シェア※
ますます高度化、巧妙化するサイバー攻撃に対抗！
進化したシマンテックのエンドポイントセキュリティ

世界シェア NO.1※

※出展：IDC, Worldwide Endpoint Security Market Shares, 2014: Success of Midsize Vendors (2015年12月, US40546915) 企業向け 2014年売上金額ベース

既存のセキュリティ対策をすり抜けるために

高度化、巧妙化を続けるサイバー脅威

escalation

標的型攻撃　ゼロデイ攻撃　ランサムウェア
水飲み場攻撃　スピアフィッシング　DDOS攻撃・・・・・

サイバー脅威の大幅な増加と攻撃手法の高度化

昨今の脅威は、ネットワーク環境や脆弱性などを悪用して、既存のセキュリティを回避する手法を巧みに利用しています。その結果、ここ3年で10億もの未知のマルウェアが出現し、気づかれないようにエンドポイントに侵入しています。

4億3,100万

2015年にシマンテックが見つけた新種のマルウェアの数

対前年 36% UP

DAY 0

+125%

2014年から2015年にかけての
ゼロデイ脆弱性の増加率

2倍以上に増加

23%

ゼロデイ脆弱性を狙う攻撃キット
エクスプロイトキットの利用率

Web攻撃ツールキット No.1

+55%

標的型攻撃の手口に利用される
スピアフィッシング攻撃

11人／1件で的を絞って発見が困難に

+35%

2014年から2015年にかけての
暗号化型ランサムウェア

2倍以上に増加

出典：シマンテック ISTRレポート（2016年）

エンドポイント保護のための労力が増大

80% のセキュリティ担当のITスタッフは、
エンドポイントセキュリティの維持は2年前よりも
さらに大変で労力を要すると感じている。

ビジネスへのインパクト

**従来の手法での
セキュリティ維持は困難**
新たな脅威の31%は、トッププライオリティで対応しなければならない。

生産性の低下
38%のセキュリティエンジニアは、マルウェア被害対応に追われている。

コストの増加
1度の標的型攻撃によって、平均約2億円の被害が発生している。

出典：ESG Endpoint Security Report

Symantec Endpoint Protection 14

激化するサイバー攻撃を防ぐために防御力を大幅に進化させた
シマンテック最強のエンドポイントセキュリティ

ますます高度化する標的型攻撃を強力に防御

標的型攻撃は、ゼロデイ脆弱性を悪用した攻撃やスピアフィッシングをはじめ、さまざまな手法を使い執拗で高度なものが増えて、企業には大きな脅威になっています。

従来の多層防御に先進の防御機能を追加搭載し、防御力を大幅に強化！

脅威の攻撃防御から、侵入を前提としたセキュリティ対策へ

サイバー脅威の増加と高度化で、単純に外部からのエンドポイントへの攻撃を防ぐだけでは対応が難しくなっています。これからは侵入されることを前提にした対策が必須です。

未知の脅威を検出する機能を強化して、脅威が実行される前にブロック！

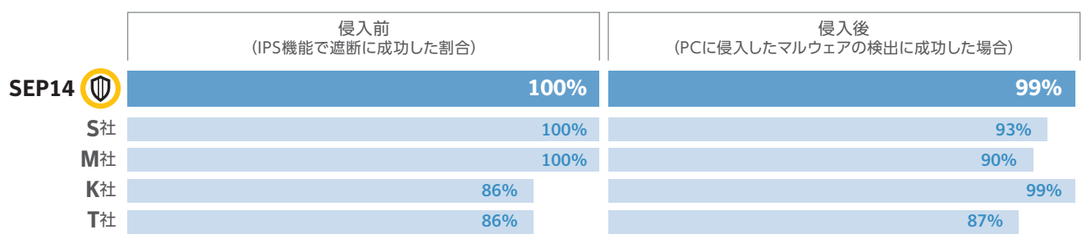
高度な防御体制を効率的かつ低コストで実現

高度な防御機能を備えるためには、無駄にエージェントやソリューションを増やす必要があり、コストや運用負荷が増加して、なかなか実行できない現実があります。

多彩で高度な防御テクノロジーの搭載で、1ソリューションで強力に防御！

- 攻撃の検出だけでなくマルウェアの駆除・修復までを実行
- 侵入したマルウェアをエンドポイント上で削除、修復まで可能
- EDR機能（Detection and Response）をSEPエージェントに搭載

Symantec Endpoint Protection 14の防御力は、脅威の侵入前も侵入後も他社に比べて絶大です。



出典：“Real world test for Drive by Downloads” & “Deliberate Downloads” from live domains hosting malware” by TASER

evolution 比類ないエンドポイントの防御力と進化したテクノロジー

Symantec Endpoint Protection 14 は、従来の防御テクノロジーに加え 新たに搭載した先進のテクノロジーで、高度化した脅威の連鎖をシャットアウトします。

Symantec Global Intelligence Network (GIN)

シマンテックは、世界最大規模のセキュリティ情報ネットワークを構築。
世界中から脅威情報を収集してすばやく解析を行い、その情報はSEPのセキュリティ機能と連動しながら他社にはまねのできない防御力を実現しています。

脅威活動の監視	・240,000以上のセンター群 ・200カ国以上へ展開
マルウェア	・1.3億台のシステムをモニター ・全世界11拠点のセキュリティレスポンス・センター
脆弱性情報	・266,400以上の脆弱性情報 ・21,300以上の連携ベンダー
イベント・ログ情報	・500万以上のおとりアカウント ・84億通以上/日のメール ・18億以上/日のWebリクエスト

最新情報をリアルタイムでルックアップ → Intelligent Threat Cloud

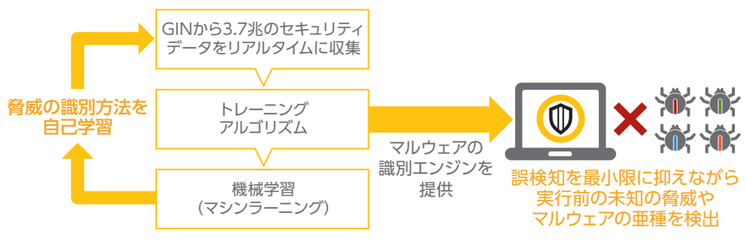
	ネットワーク	レピュテーション	機械学習	アプリケーション保護	アプリケーション制御	マルウェア検知	アンチウイルス	振るまい検出	修 復
	・ファイアウォール ・IPS(侵入防止)	ファイル安全評価	NEW	NEW	挙動の監視と制御	NEW	NEW		
		Insight™	SAPE	MEM		Emulator	Intelligent Threat Cloud	SONAR™	Power Eraser™
	PCに蔓延する前にネットワークを制御しマルウェアを遮断	ユーザーコミュニティの英知を使用し、ファイルの安全性を決定	新種のマルウェアや未知の脅威を検出誤検知を削減	シグニチャレスでアプリケーションのゼロデイ脆弱性を保護	ブラックリスト、ホワイトリストによるシステムロックダウン	パッカーにより検出を逃れるマルウェアを検出	システムに到達する前にマルウェアをスキャンして遮断	怪しい振るまいのファイルをリアルタイムで検出して遮断	感染した未知の脅威や既知の脅威を検出してクリーンアップ

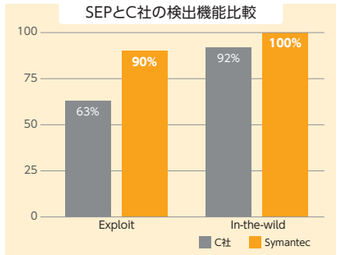
攻撃 → 感染 → 侵入 → 予防

NEW

SAPE(機械学習エンジン) Static Attribute Protection Engine

SAPEは、脅威を検出する機械学習エンジンです。GINで収集した膨大なマルウェアサンプルでトレーニングしたSAPE Classifiersをエンドポイントに提供し、これにより実行前の「新規」「未知」の脅威を検出します。

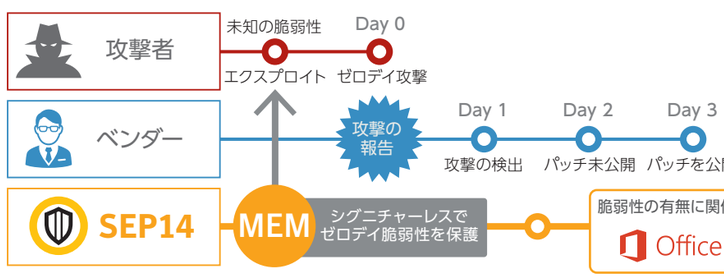


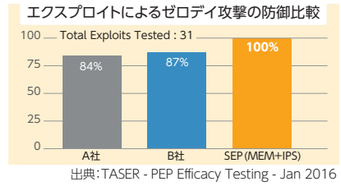


出典:AV-Comparatives and MRG Effitas Test, Feb 2016

Memory Exploit Mitigation (MEM)

エクスプロイトを使って未知の脆弱性を見つけ出してゼロデイ攻撃をしかけるサイバー犯罪が多発しています。MEMは、犯罪者の攻撃パターンの先を見越して、仮想パッチや定義ファイルがなくても脆弱性を保護します。

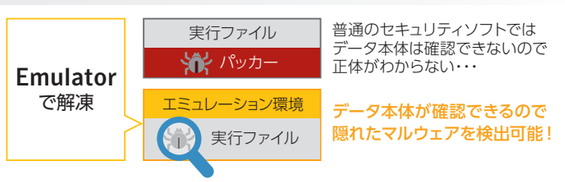




出典:TASER - PEP Efficacy Testing - Jan 2016

Emulator

サイバー犯罪者の常套手段として、既知のマルウェアを検知されないようにパッカー(圧縮や難読化)で正体を隠してユーザーに送り込んできます。2015年には、パックされていた脅威は83%もあり検出が難しくなっています。

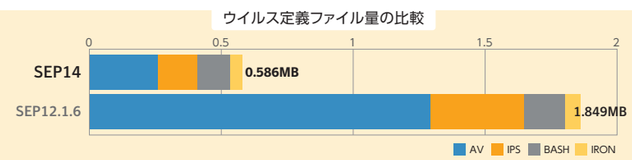


Intelligent Threat Cloud

シマンテックが所有する世界最大規模の脅威監視ネットワーク(GIN)からの情報をリアルタイムでクラウドルックアップすることで、ウイルス定義ファイルのみに頼る防御から脱却し、迅速かつ快適に新たな脅威に対応することができます。

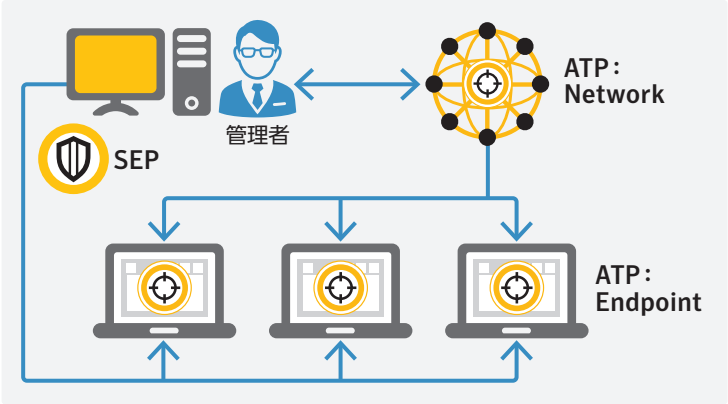
- 最新の情報で脅威を検出
- 定義ファイルを劇的に削減

SEPの旧バージョンに比べると使用する定義ファイルのデータ容量は**約1/3**になりました。



Symantec Endpoint Detection and Response (EDR)

Symantec Endpoint Protection (SEP) と Symantec Advanced Threat Protection (ATP:Endpoint) との連携で、マルウェア感染後の迅速な対応を可能にするEDRが簡単に導入できます。



エンドポイントを可視化して脅威を封じ込め

ATPとSEPを連携させると、アプリケーション、ログ、起動プロセスなどのエンドポイント情報の収集が可能になります。管理者は、収集した情報をもとにマルウェアの特定や削除などの作業が一元的に行えます。

Flight Data Recorder

エンドポイントの活動を継続して記録し、可視化することで、インシデントの範囲と追跡を可能にします。

Real-time endpoint Search

EOCクエリーを実行し、SEP管理サーバーとATP、SEPに接続し、直近の情報を収集します。

Symantec Advanced Threat Protection (ATP)

ATPは「ATP:Network」「ATP:Endpoint」「ATP:Email」の3つのエージェントと、シマンテックが独自開発した「Cynic」「Synapse」で構成されます。すでにSEPを導入している場合は、新しいエージェントをインストールする必要がなく、既存の資産を有効に活用できます。

ATP:Network
ネットワークプロトコルを通じて侵入しようとする高度な脅威を検出

ATP:Endpoint
すべてのエンドポイントを対象に、高度な攻撃の検出、優先順位付け、修復を行う

ATP:Email
電子メールを通じてに侵入しようとする高度な脅威を検出

Symantec Cynic
クラウドベースのサンドボックスおよびペイロードのデトネーションサービスです。不審なファイルを仮想と物理の両環境で実行して検出します。

Symantec Synapse
不審な活動を集計して関連付け、それをGINの脅威情報に結びつけることで、最もリスクとなるイベントだけを特定して対応に優先順位を付けます。

Symantec Endpoint Protection 14 システム要件

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

Windows オペレーティングシステム:
Windows Vista(32ビット, 64ビット), Windows 7(32ビット, 64ビット, RTM and SP1), Windows 7 Embedded Standard, Windows 8(32ビット, 64ビット), Windows 8 Embedded(32ビット), Windows 8.1, Windows 10, Windows Server 2008(32ビット, 64ビット, R2を含む), Windows Essential Business Server 2008(64ビット), Windows Small Business Server 2011(64ビット), Windows Server 2012(64ビット, R2を含む), Windows Server 2016

Macintosh オペレーティングシステム:
Mac OS X 10.9, 10.10 10.11 Mac OS 10.12

Linux オペレーティングシステム(32ビット、64ビット):
Red Hat Enterprise Linux, SuSE Linux Enterprise(サーバー/デスクトップ), Oracle Linux(OEL), CentOS, Ubuntu, Debian, Fedora

仮想環境:
Microsoft Azure, Amazon WorkSpaces, VMware WS 5.0, GSX 3.2, ESX以降, VMware ESXi 4.1 - 5.5, VMware ESX 6.0, Microsoft Virtual Server 2005, Microsoft Enterprise Desktop Virtualization (MED-V), Microsoft Windows Server 2008, 2012, 2012 R2 Hyper-V, Citrix XenServer 5.6以降, Virtual Box by Oracle

ハードウェアの必要条件:
Windows:1GHz以上のCPU, 512MB以上のRAM(1GB以上を推奨), 1.5GB以上のハードディスク空き容量

Mac:64ビットのIntel Core 2 Duo以上のCPU, 2GB以上のRAM, 500MB以上のハードディスク空き容量

intel:Intel Pentium 4 (2GHz以上のCPU), 1GB以上のRAM, 7GB以上のハードディスク空き容量

Manager システム

Windows オペレーティングシステム:
Windows Server 2008(64ビット、R2を含む), Windows Server 2012(R2), Windows Server 2016

ハードウェアの必要条件:
Intel Pentium Dual-Core以降, 2GB以上のRAM(8GB以上を推奨), 8GB以上のハードディスク空き容量

Web ブラウザ:
Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Microsoft Edge

データベース:
内蔵されているデータベースを使用、または以下から選択:SQL Server 2008 R2 SP3, SP4, SQL Server 2012, RTM - SP1;SP2, SQL Server 2014, RTM SP1, SQL Server 2016

※最新のシステム要件は、http://www.symantec.com/ja/jp/business/endpoint-protection でご確認ください。

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
シマンテックセールスインフォメーションセンター(法人向け)
■電話受付時間:10:00 ~ 12:00、13:00 ~ 17:00
(土、日、祝日、年末年始を除く)
■電話:03-4540-6226 FAX:03-6892-3916
www.symantec.com/jp/

お問い合わせ

E1611SG1-cn-SEP14