サイバー・セキュリティ
エンドポイントの選択
（ウィルスソフト）

Sophos Authorized Partner

株式会社リナ・システム

LYNA

2020年

Ver.2.1

はじめに

- エンドポイントセキュリティ・ソリューションに何が必要なのかを理解しているでしょうか。IT およびセキュリティの専門家を対象にした調査では、
  - 87% が、この 1年で脅威がさらに複雑化したと回答
  - 60% が、現在のサイバー攻撃対策では サイバー脅威に十分に対抗できないと回答
  - 60% が、今後 12ヶ月の間に機械学習の導入を計画
  - 56% が、機械学習とディープラーニングの違いを理解していない
  - 46% が、エクスプロイト対策技術を導入済みと回答したが、3 分の 2 はエクスプロイト対策技術が 実際にどのようなものかを理解していない

- 多くの人がエンドポイントセキュリティとは何であるのかを把握していません。企業にとって最適な保護の導入をご提案いたします。

エンドポイントの脅威

単に「ウイルス対策ソリューション」と呼ばれることもあるエンドポイントセキュリティソリューションは、環境の変化とともにエンドポイントの脅威を防止する多様な基本的(従来型)なアプローチと最新 (次世代型)のアプローチを含むように進化しています。

ソリューションを評価する際には、幅広い脅威を阻止する包括的な技術を搭載したソリューションを探すことが重要です。また、阻止の対象となる脅威を理解することも重要です。

最近のエンドポイントの脅威

- **ポータブル実行可能ファイル (マルウェア):**
  多くの場合、エンドポイントプロテクションの検討に際して一番の関心事はマルウェア (悪意のあるソフトウェアプログラム) です。マルウェアには、既知のマルウェアに加えて、未知マルウェアが含まれます。多くのソリューションが未知のマルウェアの検出に苦戦している一方で、SophosLabs は未知のマルウェアを毎日約 40万件検出しています。ソリューションは、特定されないように変更が加えられたパッケージファイルやポリモーフィック型ファイルを発見することに長けている必要があります。
- **PUA (不要と思われるアプリケーション):**
  PUA は厳密に言えばマルウェアではありませんが、アドウェアと同様、自分のマシンで実行するのは避けたいアプリケーションです。クリプトジャッキング攻撃に使用されるクリプトマイニング用プログラムの増加に伴い、PUA の検出はますます重要になっています。
- **ランサムウェア:**
  過去 1年間に半数以上の企業がランサムウェア攻撃を受けており、そのコストは平均 133,000ドルに達しています。ランサムウェアには主に、ファイルを暗号化するものとディスクを暗号化するもの (ワイパー) の 2タイプがあります。最も一般的なファイル暗号化プログラムは、標的ユーザーのファイルを暗号化し、身代金を要求します。ディスク暗号化プログラムは、ファイルだけでなくハードドライブ全体をロックしたり、完全消去したりします。
- **エクスプロイトベース/ファイルレスの攻撃:**
  すべての攻撃がマルウェアを使用するわけではありません。エクスプロイトベースの攻撃では、ソフトウェアの不具合や脆弱性を利用してコンピュータにアクセスし制御する手法が用いられます。このような攻撃で一般的に使用されるのが、武器化されたドキュメント (通常は、損害を与えられるように細工や改ざんが施された Microsoft Office プログラム) と悪意のあるスクリプト (多くの場合、正規のプログラムや Web サイトに隠された悪意のあるコード)です。その他には、マルウェアを使用してブラウザに感染しトラフィックの表示と操作を可能にするMITB (Man-in-the-Browser: マンインザブラウザ) 攻撃や、C&C サーバーとの通信などを目的にWeb トラフィックを利用する悪意のあるトラフィックなどがあります。
- **持続的な攻撃手法:**
  多くのエンドポイント攻撃には、複数の段階と複数の手法が必要です。持続的攻撃の手法の例として、権限昇格 (攻撃者がより高い権限でシステムにアクセスするための方法)、認証情報の窃取 (ユーザー名とパスワードを盗むこと)、コードケイブ (正規のアプリケーションに悪意のあるコードを隠すこと) などが挙げられます。

最新技術（次世代型）と基本技術（従来型）の違い

名前は違っていてもウイルス対策ソリューションは以前から存在しており、既知の脅威に対して非常に効果的であることが証明されています。

従来のエンドポイント保護ソリューションは、さまざまな基礎技術が用いられてきました。しかし、脅威環境が変化するにつれて、それまでには見られなかった**マルウェアなどの未知の脅威**がますます一般化しつつあります。そのため、新しい技術が市場に参入してきています。購入検討時には、「次世代」セキュリティとも呼ばれる最新のアプローチと、実績のある基本的なアプローチが組み合わされたソリューションを探してください。主要な機能は次のとおりです。

基本技術（従来型）

- **マルウェア対策/ウイルス対策:**
  既知のマルウェアをシグネチャベースで検出します。マルウェアエンジンには、実行ファイルだけでなく、その他のコード (Web サイトに隠された 悪意のある JavaScript など) も検査する機能が必要です。
- **アプリケーションロックダウン:**
  アプリケーションをインストールして実行する武器化された Office ドキュメントなど、アプリケーションの悪意のある挙動を防止します。
- **挙動監視/ホスト侵入防止システム (HIPS):**
  この基本技術は、未確認のウイルスや不審な挙動からコンピュータを保護します。実行前および実行時の挙動分析の両方が必要です。
- **Web プロテクション:**
  既知の悪意のある Web サイトの URLルックアップとブロック。ブロック対象のサイトには、JavaScript を実行してクリプトマイニングを行うサイトや、ユーザー認証情報やその他の機密データを収集するサイトが含まれる必要があります。
- **Web コントロール:**
  管理者はエンドポイントのWeb フィルタリング機能を使用することで、ユーザーにインターネットからのダウンロードを許可するファイルタイプを定義できます。
- **データ損失防止 (DLP):**
  攻撃者を発見できない場合、攻撃者がデータの抽出を試みると、DLP 機能によって一部の攻撃の最終段階を検出・阻止することができます。そのためには、さまざまなタイプの機密データを監視する必要があります。

最新技術（次世代型）

- **機械学習:**

  機械学習には、ディープラーニング型ニューラルネットワーク、ランサムフォレスト、ベイジアン、クラスタリングなど、さまざまな方法があります。方法論にかかわらず、機械学習を用いたマルウェア検出エンジンは、シグネチャに依存せずに既知および未知のマルウェアを検出するように構築する必要があります。機械学習の利点は、これまでに確認されたことがないマルウェアを検出できることで、全体的なマルウェア検出率の向上が期待されます。企業は、検出率、誤検出率、および機械学習ベースソリューションのパフォーマンスへの影響を評価する必要があります。

- **エクスプロイト対策:**

  エクスプロイト対策テクノロジーは、攻撃チェーンで使用されるツールと手法を阻止することによって攻撃者を拒否するように設計されています。たとえば、EternalBlue や DoublePulsar などのエクスプロイトは、NotPetya や WannaCry ランサムウェアを実行するために使用されました。エクスプロイト対策テクノロジーは、マルウェアの拡散と攻撃の実行に使用される比較的少数の手法を阻止します。これにより、未知のものであっても数多くのゼロデイ攻撃を回避することができます。

- **ランサムウェアに特化:**

  一部のソリューションには、ランサムウェアによるデータの暗号化を防止するように特別に設計された技術が搭載されています。多くの場合、ランサムウェアに特化した技術は、影響を受けたファイルの修復も実行します。ランサムウェアソリューションは、ファイルを暗号化するランサムウェアだけでなく、ハードディスクのマスターブートレコードを改ざんするワイパー攻撃をするランサムウェアも阻止できなければなりません。

最新技術（次世代型）つづき

- **認証情報の盗難防止:**
  メモリ、レジストリ、ハードディスクから認証用パスワードやハッシュ情報が盗まれるのを防止するためのテクノロジーです。
- **プロセスの保護 (権限昇格):**
  持続的攻撃の一環として権限を昇格させる目的でプロセスに特権付き認証トークンが挿入されているかどうかを判断する保護機能が組み込まれています。この 機能は、既知または未知の脆弱性が最初に認証トークンを盗むために利用されたかどうかにかかわらず、効果的であるはずです。
- **プロセスの保護 (コードケイブ):**
  正規アプリケーションの存在を利用しようとする攻撃者が好んで使用するコードケイブや AtomBombing などの技術を阻止します。攻撃者はこれらの呼び出しを悪用して、別のプロセスにコードを実行させる可能性があります。
- **EDR (Endpoint Detection & Response) テクノロジーと根本原因分析:**
  EDR を始めとする分析ツールは、攻撃の防止に重点を置くのではなく、過去に検出されたインシデントを分析して対応します。また、一部のツールは、これまで検出されていなかった攻撃を検出するハンティング機能も搭載しています。ツールを検討する際には、自社IT チームの規模およびスキル セットに見合った複雑さと使いやすさのツールを選択することが重要です。
- **インシデントレスポンス / Synchronized Security:**
  エンドポイントツールは少なくとも、今後のインシデントを回避できるよう発生済みのインシデントについて知見を提供するものでなければなりません。インシデント解析者の介入を必要とせずに、自動的にインシデントに対応し、脅威の拡散を防止したり被害を最小限にとどめたりできるものが理想です。インシデント対応ツールは、ネットワークセキュリティツールだけでなく他のエンドポイントセキュリ ティツールとも通信できることが重要です。

「プラスの力」– 複数の手法よる包括的エンドポイントセキュリティを実現

1つの主要機能だけに注目すべきではありません。それ以外にも、機械学習などの最新技術と、現在も有効であることが証明されている基本アプローチの両方を備えたソリューションを探してください。業界トップレベルの機能であっても、1つの主要機能に依存することで、単一障害点の影響を受けやすくなります。それとは対照的に、複数の強力なセキュリティレイヤーで構成される多型防御アプローチを導入することで、より広範囲の脅威の阻止が可能になります。これは、基本的な手法に機械学習、エクスプロイト対策、ランサムウェア対策、EDR などを追加していく方法で、一般的に「プラスの力 (the power of the plus)」と呼ばれています。

エンドポイントセキュリティを評価するうえで、各ベンダーにソリューションに組み込まれている手法を確認する必要があります。それぞれのコンポーネントはどの程度の強度を備えているか、どの脅威を阻止するように設計されているのか、1つの主要機能に依存していないか、その機能が突破された場合に何が起こるか、という点を検討してください。

Sophos Intercept X

◆ 卓越したエンドポイント保護

Sophos Intercept X は、ディープラーニングによるマルウェアの検出、エクスプロイト対策、ランサムウェア対策などを組み合わせて活用することにより、多種多様な攻撃をブロックします。

◆ 主な特長

- マルウェア検出エンジン - ディープラーニングを活用して最高位の検出率を実現
- エクスプロイト防止 - ソフトウェアの脆弱性を悪用する攻撃をブロック
- 敵対行為に対するアクティブな抑止 - マシン上に悪意のあるプログラムが常駐するのを阻止
- 根本原因解析 - マルウェアが加えた変更や感染経路が一目瞭然
- ランサムウェアに特化した 保護テクノロジー
- Intercept X Advanced は、最新の技術と基本的なアプローチを組み合わせて、お客様の既存のエンドポイントセキュリティを強化します。

攻撃手順

【有効な対策 】
・Web
プロテクション
・メールプロテクション

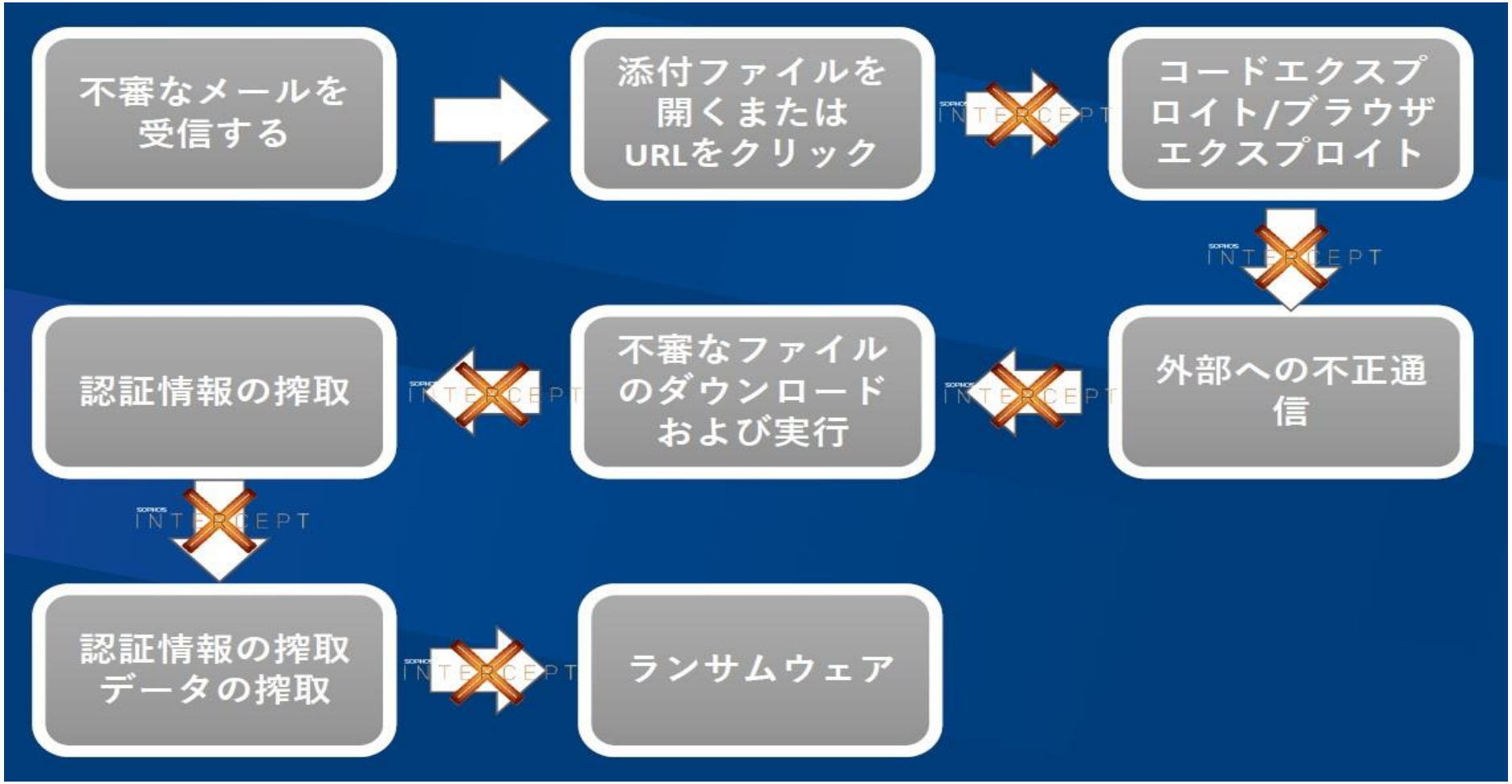
【有効な対策 】
・エクスプロイト対策
(コード メモリ 他)
・アプリケーション
ロックダウン
・アプリケーション
コントロール

【有効な対策 】
・人工知能
(DEEPLEARNING 型 AI)
・HIPS
(振る舞い検知
解析)

【有効な対策 】
・MALICIOUS
TRAFFIC
DETECTION
(不正な通信を検知)

【有効な対策 】
・アンチランサムウェア
・認証情報搾取対策
・動的解析型振る舞い
検知
・根本原因解析

負の連鎖を断ち切ることが超重要



機能比較

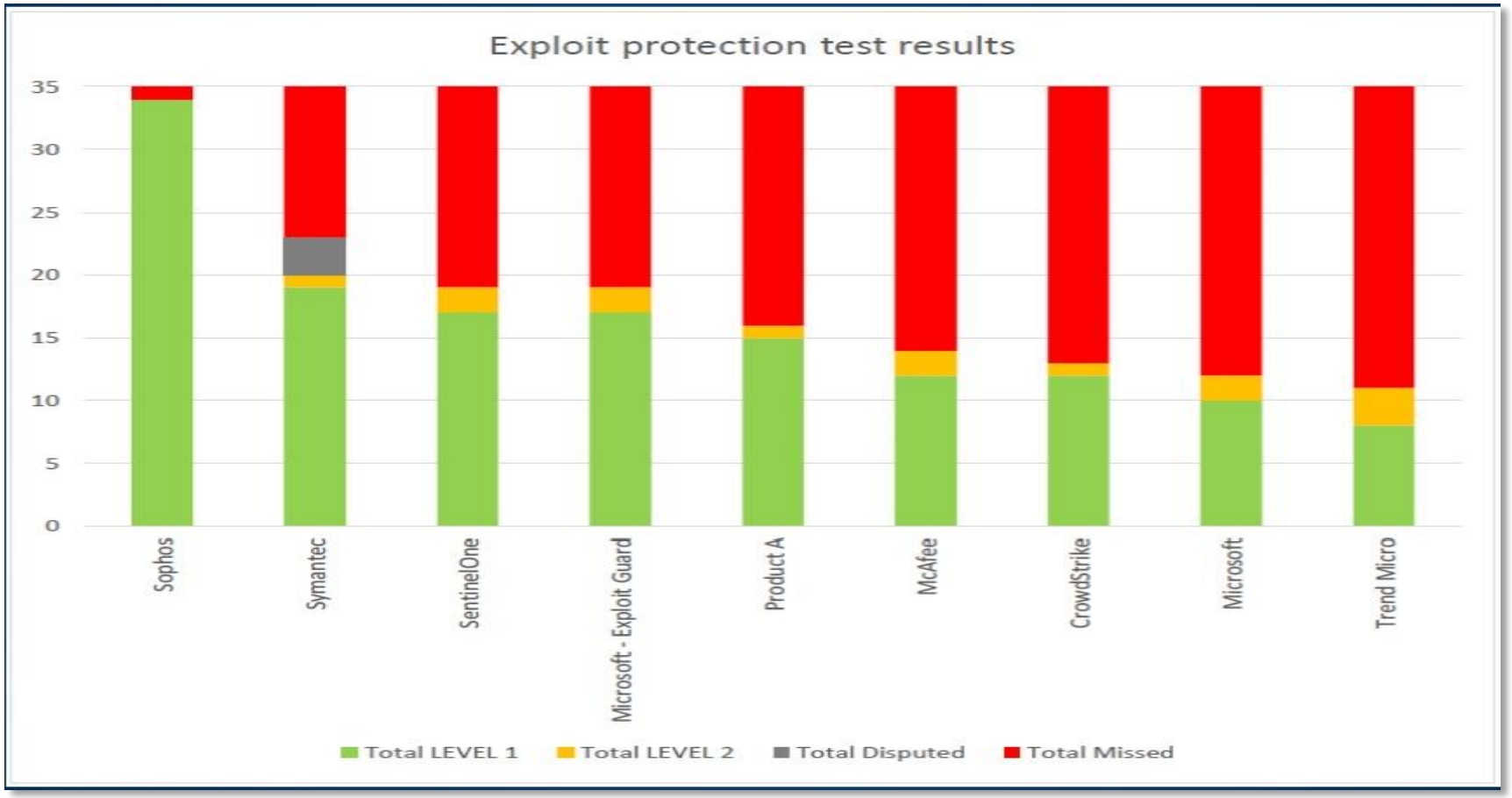
	Sophos	Tm社	
簡単な管理	○	✖	「統合管理機能「、「ポリシー管理」
Synchronized　Security	○	✖	「Synchronized　Security」
ディープラーニング	○	✖	「機械学習」
25種以上のエクスプロイト防止技術	○	✖	「エクスプロイト防止」
1台のコンソールからWindows,Mac,Linux デバイスを保護	○	✖	「マルチプラットフォーム管理」
デバイスコントロールの統合とデータ損失防止	○	✖	「デバイスコントロール」、「データ損失防止」

（詳細資料あります）

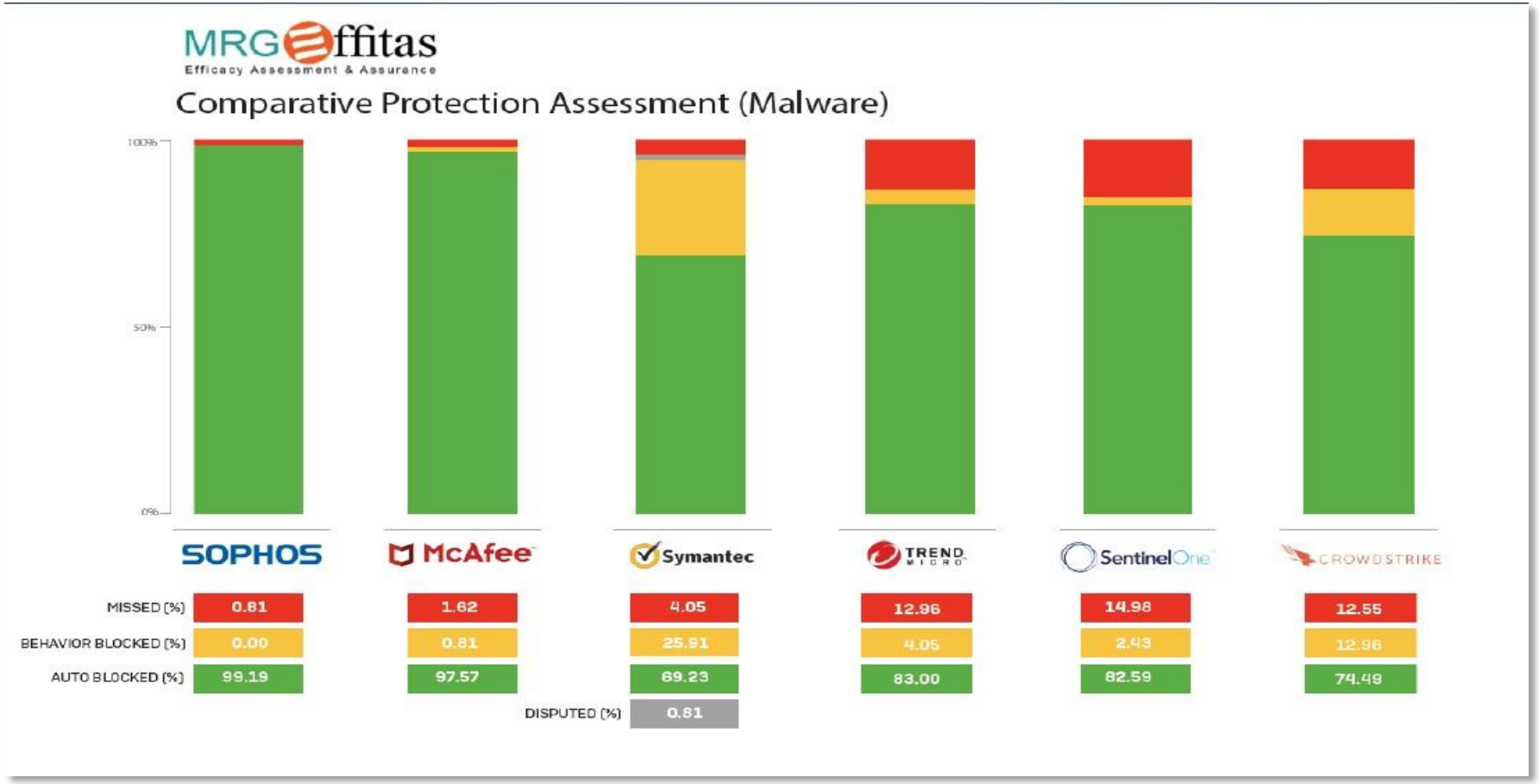
ライセンス比較

エンドポイントライセンスの比較		Sophos					Trend Micro		
		Endpoint Protection Advanced	Endpoint Exploit Prevention	Central Endpoint Protection	Intercept X Advanced	Intercept X Advanced with EDR	Worry-Free Services Advanced	Enterprise Security for Endpoints	Smart Protection Complete
防止	Web セキュリティ	✓	×	✓	✓	✓	✓	✓	✓
	Web コントロール / カテゴリベースの URL ブロック	✓	×	✓	✓	✓	✓	Worry-Free は対応、Apex One は非対応	Worry-Free は対応、Apex One は非対応
	デバイスコントロール (例: USB)	✓	×	✓	✓	✓	✓	×	✓
	アプリケーションコントロール	✓	×	✓	✓	✓	✓	×	✓
	ブラウザエクスプロイト防止機能	×	✓	×	✓	✓	✓	✓	✓
	データ損失防止	✓	×	✓	✓	✓	✓	×	✓
	エクスプロイト防止	×	✓	×	✓	✓	✓	✓	✓
	機械学習	×	×	×	✓	✓	✓	✓	✓
検出	悪質なトラフィックの検出 (MTD)	✓	×	✓	✓	✓	×	✓	✓
	CryptoGuard ランサムウェア対策	×	✓	×	✓	✓	✓	✓	✓
対応	Synchronized Security Heartbeat	×	×	✓	✓	✓	×	×	×
	エンドポイント検出 / 対応 (EDR)	×	×	×	×	✓	×	×	×

第3者機関の評価（エクスプロイト検知）



第3者機関の評価（マルウェア検知）



エンドポイントに加え

	一般的なウィルスソフト	Sophos社製FirewallXG（UTM)
ネットワークの侵入・保護	×	◎
なりすましメール	×	○
脆弱（ぜいじゃく）性への攻撃	△	○
DDos攻撃（集中砲火）	×	○
アカウント乗っ取り	×	○
フィッシング詐欺	△	○
ワンクリック詐欺	×	○
未知のウィルス	×	◎
外部媒体の管理（USBメモリなど）	×	管理
迷惑メール	ブロック	ブロックと送信

包括的な次世代セキュリティ対策

- セキュリティ対策とコンプライアンス遵守に不可欠
  - 高度なネットワーク機能、保護機能、ユーザ、アプリケーションの制御

管理	ファイアウォール管理機能	集中管理機能	ステータスと警告	レポートとログ
ユーザとアプリの制御	ユーザ識別	アプリケーションコントロール	Webコントロール	コンテンツ制御
保護機能	ファイアウォールとIPS	クラウド型サンドボックス	マルウェア対策 業務アプリケーション	Webプロテクション メールとデータ
ネットワーク	ルーティングとブリッジ パフォーマンス	ゾーンのセグメント化 VPN	トラフィックシェービング RED VPN	ワイヤレスコントローラ 暗号化されたトラフック

究極のコンビネーション

◆ 最新のランサムウェアや高度な脅威から保護

セキュリティ、使いやすさ、解析力のすべてに優れた製品

隠れたリスクを顕在化

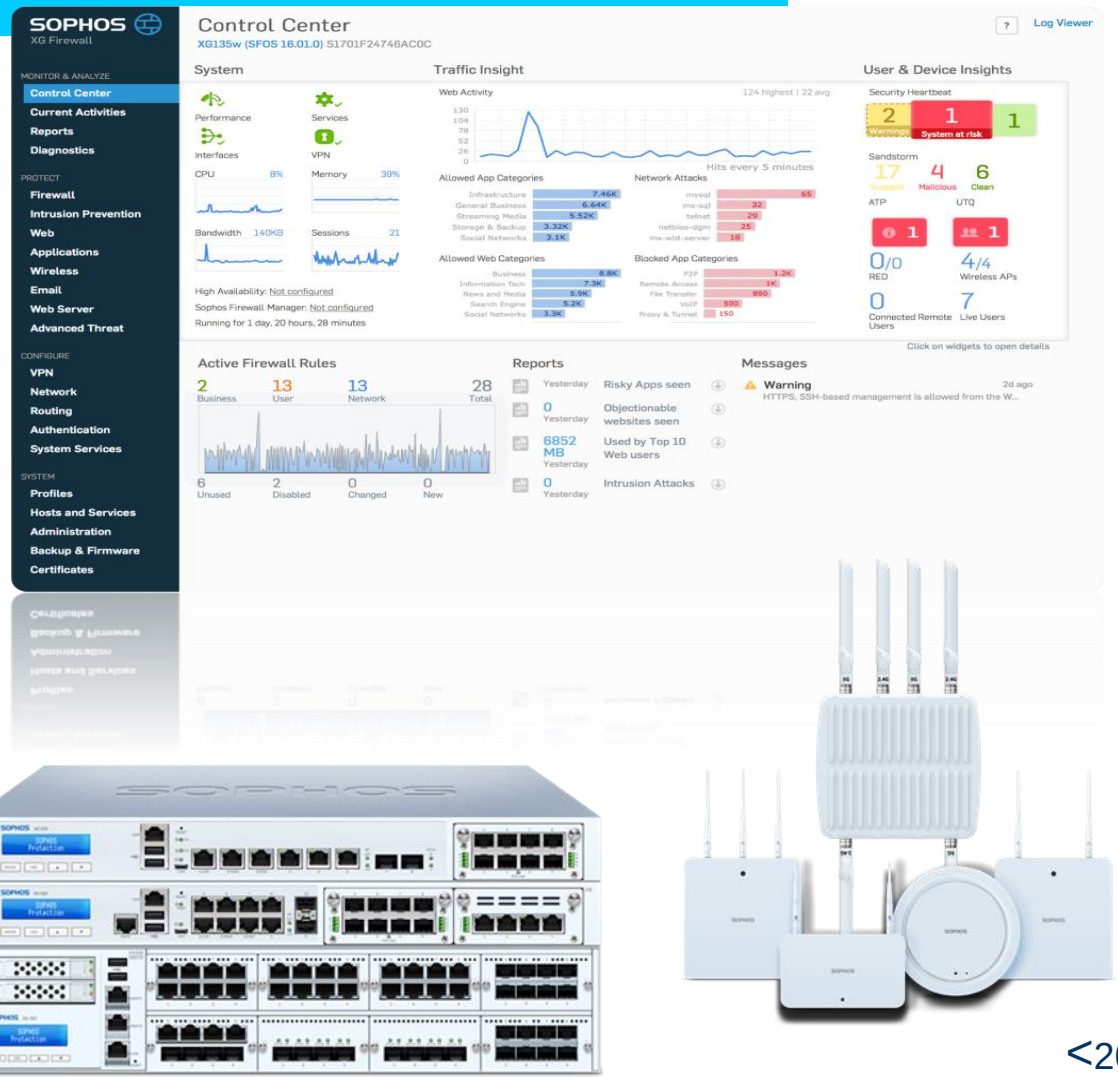
- ✓アプリ、ユーザー、悪質プログラム、脅威
- ✓見やすく色分けされたダッシュボード
- ✓豊富なレポート機能を搭載
- ✓問題を先回りして阻止

ネットワーク脅威をブロック

- ✓多様な保護機能
- ✓IPS、APT、サンドボックス
- ✓Web コントロールとアプリケーションコントロール
- ✓単一画面から簡単に管理

インシデントへの自動対応

- ✓独自技術の Security Heartbeat™
- ✓エンドポイントのセキュリティ状態をルールに反映
- ✓感染システムをすばやく特定
- ✓感染システムを自動的に隔離



おわりに

サイバー脅威が複雑化し、数も増加し続けるにつれて、エンドポイントの効果的な対策を導入することがこれまで以上に重要になっています。

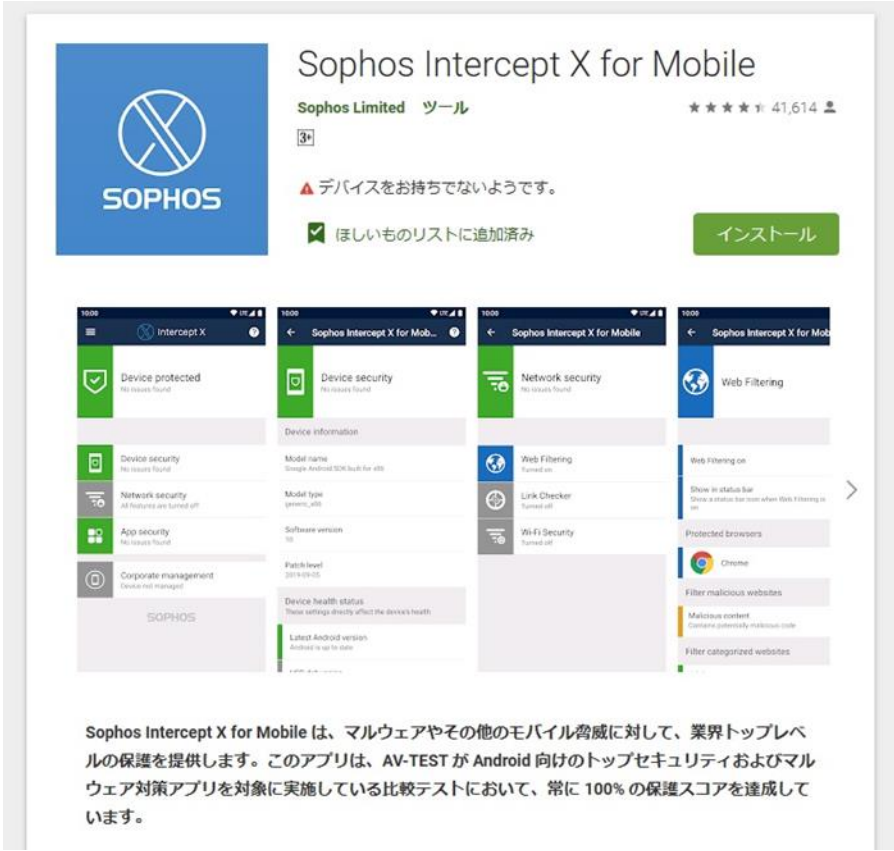
ブロックする必要がある脅威を把握し、利用可能なさまざまなセキュリティテクノロジーを理解することで、最適なエンドポイントセキュリティを選択し、今日の攻撃に対抗する最善の防御を実現できます。

付録（情報管理が不適切な場合の処罰など）

情報の種類	根拠法による規定		処罰など
個人情報 （マイナンバーを含む）	個人情報保護法	1)虚偽申告命令違反	6か月以下の懲役または30万円以下の罰金、業務停止命令
		2)データベース提供材	1年以下の懲役または50万円以下の罰金
	民法（不法行為による損害賠償709条）		損害賠償
	建設業法		役員または使用人が懲役刑に処せられた場合は営業停止命令
	マイナンバー法 （個人及び法人に対して）		秘密を漏らし、または盗用した者は、3年以下の懲役もしくは150万円以下の罰金。行為者を雇用する法人にも罰金
会社から預かった秘密情報 （外部非公開データなど）	不正競争防止法の営業秘密不正取得・利用行為など		損害賠償、信頼回復措置
自社の秘密情報 （非公開ノウハウなど）	不正競争防止法の営業秘密不正取得・利用行為など		善管注意義務違反に対する関係者からの損害賠償請求（経営者に対する民事訴訟）
上場会社の株価に影響の可能性がある未公開の内部情報	金融商品取引法		内部情報をもとに取引が行われた場合、罰金または課徴金の可能性

付録（個人のスマホユーザへ）

無償で使えるスマホセキュリティソフト
・App StoreまたはGoogle Playから「sophos」で検索
・ダウンロードして安全のためお使いください



連絡先

お薦めしたいSophos製品

- FirewallXG　:UTM
- InterceptX　:End Point
- Phish　Treat:社員教育用
- Cloud Optix:Cloud環境向け

株式会社リナ・システム
http://www.lyna.co.jp
〒102-0074
千代田区九段南4-4-5 さかきばらビル2F
電話 03-3262-6641
Mail: isao-Odakura@lyna.co.jp

◆都営地下鉄新宿線 市ヶ谷駅A3出口より徒歩3分
◆JR市ヶ谷駅より徒歩6分