Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT
SandBlast ZERO-DAY PROTECTION

Check Point SandBlast Zero-Day Protection

未知のマルウェアを検出、ブロックする次世代の脅威対策を実現

製品のメリット

- 業界トップとなる未知のマルウェアの検出率
- 攻撃者による検出回避は事実上不可能
- 攻撃の初期段階で脅威を検出、ブロック
- ファイルの迅速な再構成と安全なコンテンツの配信を実現
- 高額な損失に至る侵害やダウンタイムのリスクを低減
- 運用価値を最大限に高め、TCOを最小限に抑える統合型セキュリティ

製品の特徴

- CPUレベルでマルウェアを深部まで検査し、攻撃コードを検出
- さまざまな種類の文書、広く普及しているファイル形式に対応
- 既存のインフラストラクチャと連携、新しい機器のインストールは不要
- アクティブ・コンテンツなど、悪用可能なコンテンツを文書ファイルから除去
- 再構成したファイルをPDF形式に変換。元のファイル形式の維持も可能
- 脅威対策とセキュリティ管理の統合により、包括的なセキュリティと脅威の可視化を実現
- 新しい攻撃に関する情報をThreatCloud™経由で自動共有

[1]『チェック・ポイント セキュリティ・レポート2015年版』

課題

サイバー攻撃が激化する昨今、攻撃者は検出をすり抜けながら目的を達成するために、絶えず新たな戦略や手法を編み出しています。今日の攻撃者のエコシステムを利用すれば、攻撃コードや新たに見つかった脆弱性、あるいは技術スキルでさえも仲間と容易に共有できます。犯罪に手を染めてから日の浅い攻撃者でも、このようなリソースを活用して脆弱性やセキュリティ対策が不十分な組織を見つけ出し、既存のマルウェアのシンプルな亜種から新しいゼロデイの脅威や未知の脅威を作成できるのが現実です。

アンチウイルスや次世代ファイアウォールなどのセキュリティ・ソリューションが対応可能なのは、シグネチャやプロファイルが存在する既知の脅威のみに限られます。今や1時間に106個の新しいマルウェアが検出される状況の下で、未知の脅威からの保護はどうすれば実現できるでしょうか[1]。従来型のサンドボックス・ソリューションでも出現したばかりの未知のマルウェアを検出できますが、検査に時間を要するため、マルウェアを検出、ブロックするまでの間に感染被害が生じるおそれがあります。しかも、このような従来型のサンドボックスでは、検出に対する回避技術を備えた脅威に容易にすり抜けられてしまいます。

解決策

Check Point SandBlast Zero-Day Protectionは、脅威に対する次世代の防御レベルを実現する2つの独自機能、Threat EmulationとThreat Extractionを搭載しており、回避能力を備えたマルウェアも検出します。危険性の高い攻撃から包括的に保護しながら、安全なコンテンツをユーザに素早く確実に届けます。

SandBlast Threat Emulationは、CPUレベルの詳細な検査を実施し、展開を試みる危険性の高い攻撃が検出を回避する前に阻止します。さらに、OSレベルでも検査を行い、実行可能ファイルやデータ・ファイルなど、幅広い形式のファイルを調査します。このような独自の検査機能により、脅威の検出率を最大限に高め、攻撃者による検出回避も事実上不可能にします。

SandBlast Threat Extractionは、安全なコンテンツ、すなわちファイルに含まれる潜在的な脅威を除去し、再構成した安全なファイルをユーザへ迅速に転送する役割を担いこのソリューションを補完します。その際、業務に影響を及ぼしません。従来型のサンドボックスでは避けられない許容範囲以上の遅延を生じることなく、実運用環境上での防御モードが実現します。また、アラートだけに限らず、不正なコンテンツがユーザに配信されないようにブロックします。

このように、Check Point SandBlast Zero-Day Protectionは、危険性の高いゼロデイ攻撃や標的型攻撃に対する包括的な検出、検査、および保護を実現します。

回避能力を備えたマルウェアも検出

Check Point SandBlast Zero-Day Protectionは、他社のソリューションとは異なり、CPUレベルで検査を実施する独自の機能を搭載しており、攻撃が実行される前に阻止します。

現在、数千の脆弱性に対して数百万のマルウェアが生み出されています。しかし、サイバー犯罪者が脆弱性を悪用するために使用する手法は極めて限られます。Check Point SandBlast Threat Emulationエンジンは、CPUベースの命令フローを監視し、オペレーティング・システムやハードウェアのセキュリティ機能をすり抜けようと試みる攻撃を検出します。

攻撃コードを実行する試みを感染前の段階で検出することで、サンドボックスによる検出機能を回避される前に攻撃を阻止します。

マルウェアをより的確に検出

Check Point SandBlast Zero-Day Protectionでは、OSレベルの脅威エミュレーションにより、さらなる調査を実施します。ネットワークに送信されてきたファイルをインターセプトして無害なファイルを除外した後、不審なファイルを仮想環境で実行します。ファイルの挙動は、複数のオペレーティング・システムおよびバージョンで同時に検査されます。レジストリの改ざんやネットワーク接続の確立、ファイルの新規作成など、マルウェア特有の不審な活動を示したファイルにはフラグを設定し、さらに詳細に分析します。そして、不正と判断したファイルについてはネットワークへの侵入を阻止します。

詳細レポート

ファイルをエミュレートし、マルウェアであると判断されると、詳細なレポートが生成されます。レポートはシンプルで分かりやすく構成されており、ファイルの詳細情報や不審な活動に関する情報に加え、ファイルの実行に起因する悪意のある試みについての詳細な情報も網羅されています。また、ファイルをオペレーティング・システムでシミュレートしている間のスクリーンショットも表示されます。

ThreatCloud™ エコシステム

新たに検出された脅威の情報は、ThreatCloudの脅威情報データベースに送信されます。 ThreatCloudエコシステム全体が共有する新しい脅威のシグネチャは、他のチェック・ポイント・ゲートウェイの保護に役立てられ、脅威の拡散が未然に防止されます。ThreatCloudとの継続的な連携により、最新の脅威情報を配信する業界最先端の脅威対策ネットワークが実現します。

柔軟かつ容易に導入可能

Check Point SandBlast Threat Emulationは複数の導入形態をサポートしており、コスト・パフォーマンスに優れたソリューションとしてあらゆる規模の組織に適合します。ファイルは、既存のゲートウェイからチェック・ポイントのクラウド・サービスまたは自社運用のアプライアンスのいずれかに送信できます。

Check Point SandBlast Threat Extractionは、既存のセキュリティ・ゲートウェイにSoftware Bladeとして導入します。その処理は、ネットワーク全体への適用、または個人やドメイン、部門単位での適用も可能です。対象とするユーザやグループはニーズに応じて管理者が指定できるため、小規模から始めて徐々に拡大する運用も容易です。

プロアクティブな防御を実現しながら安全なコンテンツを迅速に転送

チェック・ポイントのソリューションでは、脅威対策のボトルネックとなるスピードや保護範囲、精度のトレードオフも解消されます。Check Point SandBlast Zero-Day Protectionの場合、他社のソリューションとは異なり、検出モードや防御モードに設定していても業務に影響を及ぼしません。

SandBlastを構成するThreat Extractionのコンポーネントは、マクロや埋め込みリンクなどの高リスクのコンテンツを削除して脅威を除去し、安全と確認された要素だけで文書を再構成します。

脅威を検出、ブロックするまでに時間を要する一般的な検出技術と異なり、Threat Extractionはすべてのリスクを予防的に排除するため、安全な文書ファイルを迅速にユーザに転送できます。

ビジネスに不可欠な多種のファイル形式に対応

Check Point SandBlast Zero-Day Protectionは、Microsoft Office（Word、Excel、Power Point）から、Adobe PDF、アーカイブ・ファイルに至るまで、ビジネス環境で広く普及しているさまざまな文書形式に対応しています。

包括的な統合ソリューション

Check Point SandBlast Zero-Day Protectionは、Check Point Security Managementと完全統合されているため、セキュリティ・ポリシーやプロファイルの作成、単一の統合プラットフォームからの設定が可能となります。またCheck Point SmartEventを利用すれば、組織を狙う脅威の網羅的な把握とレポート作成が可能で、セキュリティ・イベントの迅速な調査および解決が実現します。

最高水準のセキュリティを実現するバンドル

バンドル製品のNGTX（Next Generation Threat Extraction）パッケージは、Check Point SandBlast Zero-Day Protectionの保護機能に加え、IPS、Application Control、URL Filtering、Antivirus、Anti-Bot、Anti-Spamの各種Software Bladeが提供する機能を利用できます。以上の組み合わせにより、不正なファイルのダウンロードや危険なWebサイトへのアクセス、ボットによる通信が遮断され、被害の発生を未然に防ぐ包括的なセキュリティが実現します。すでにNGTP（Next Generation Threat Prevention）アプライアンスを導入している組織は、このTXのバンドル製品によって機能を追加できます。

Check Point SandBlast Zero-Day Protectionの仕様

Threat Emulation	
機能	**説明**
サポートするファイル形式	Adobe PDF、Microsoft Office、EXE、アーカイブ・ファイル、Flash、Javaアプレットなど40種類以上
サポートするエミュレーション環境	Microsoft Windows XPおよび7、Microsoft Office、Adobe Reader
使用環境（動作時）	SecurePlatformまたはGAiA

Threat Extraction	
機能	**説明**
サポートするファイル形式	Microsoft Office 2003-2013、Adobe PDF
パフォーマンス	ユーザ数8,000人の環境でスループットの低下は1%以下 1GBのメモリが必要
対応バージョン/OS	SecurePlatform、またはGAiAのR77.30以降

Zero-Day Protection：導入形態
分散型導入 – ネットワーク全体に導入され、センサとして動作するチェック・ポイントのセキュリティ・ゲートウェイがファイルやオブジェクトをSand Blastアプライアンスに転送し、検査を実施
インラインまたはSPANポートでの導入 – Sand Blastアプライアンスをインラインで接続 – ファイルやオブジェクトについてはTEアプライアンスによりインラインで調査を実施
MTA – メール転送エージェント（MTA）として動作するチェック・ポイントのセキュリティ・ゲートウェイが着信メールを受信し、コンテンツを検査または無害化してから、次のホップのメール・サーバに転送 – MTAはThreat EmulationとThreat Extractionの両方をサポート
Threat Prevention API – オープンAPIにより、文書ファイルをThreat Emulationによる検査用およびThreat Extraction用のアプライアンスに転送
Webブラウザの拡張機能 – ダウンロードされるファイルを無害化のために再構成

Check Point®
SOFTWARE TECHNOLOGIES LTD

WE SECURE THE FUTURE

製品に関するお問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F Tel:03(5367)2500 E-mail:info_jp@checkpoint.com http://www.checkpoint.co.jp

P/N EDB39D0 2015.10