チェック・ポイント SandBlastアプライアンス

チェック・ポイント SandBlastアプライアンス

新しい脅威や未知の脅威を徹底阻止

製品のメリット

- 文書や実行可能ファイルを利用した新しい攻撃や未知の攻撃を阻止
- 攻撃者による検出回避は事実上不可能
- 既存のセキュリティ・インフラストラクチャの活用によりコストを低減
- 管理、監視、レポートの統合で最大限の保護を実現
- 新しい攻撃に関する情報をThreatCloud™経由で自動共有し、セキュリティを強化

製品の特徴

- Adobe PDF、Microsoft Office、Java、Flash、実行可能ファイル、アーカイブ・ファイルなど、40種以上のファイルに埋め込まれた未知のマルウェアを検出
- 複数のWindows環境を標的とする攻撃にも対応
- 月間10万～ 200万のファイルの検査を可能にする複数のアプライアンスを提供
- Threat Extractionにより、悪用可能なコンテンツを削除し、安全なファイルを遅延なしで転送可能
- 独自のCPUレベルの技術により、マルウェアが展開、検出を回避する前に検出

課題

サイバー攻撃が高度化の一途を辿る昨今、標的型攻撃では、その第一歩として、ダウンロードさせたファイルや電子メールの添付ファイル経由でソフトウェアの脆弱性を悪用するケースが増加しています。

このような攻撃では、シグネチャが存在しないまったく新しい攻撃コードや、既知のコードの改変版が使用される場合が多く、標準的なセキュリティ・ソリューションでは検出できません。特に毎日のように新しく出現する改変版には無力です。新しい脅威や未知の脅威に対処するために必要となるのは、シグネチャに依存しない新たなソリューションです。

解決策

回避能力を備えたマルウェアでも検出可能なCheck Point SandBlast Zero-Day Protectionは、危険性が高い攻撃からも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転送します。このソリューションの核となるのが、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です。

SandBlastソリューションの一翼を担うThreat Emulationエンジンは、攻撃コードの実行段階でマルウェアを検出し、攻撃者が組み込んだ検出回避技術によるサンドボックスのすり抜けを阻止します。ネットワークに届いた送信ファイルは、まず隔離、検査されます。仮想サンドボックス内で実行して不正な振る舞いの有無を確認し、見つかった場合は通過を阻止します。この革新的なソリューションは、CPUレベルの検査とOSレベルのサンドボックス分析を組み合わせて、危険性の高い攻撃コードやゼロデイ攻撃、標的型攻撃による感染を防ぎます。

さらに、Threat Extractionは、悪用される可能性を持つコンテンツを瞬時に削除し、無害化した状態でユーザに転送します。具体的には、アクティブ・コンテンツや各種の埋め込みオブジェクトなど、悪用可能なコンテンツをすべて抽出したうえで、危険性のないコンテンツのみでファイルが再構成されます。元の不審なファイルへのアクセスは、SandBlast Zero-Day Protectionにより隅々まで分析され、無害と判断されるまではブロックされます。悪用可能なコンテンツが削除されるためユーザは、高度なマルウェアやゼロデイの脅威に悩まされずに、コンテンツへの即座のアクセスが可能となります。

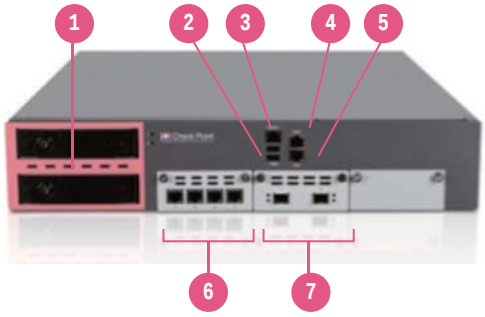
SandBlastアプライアンス

チェック・ポイントでは、幅広いSandBlastアプライアンスを用意しています。いずれのアプライアンスも、法規制やプライバシー上の理由からSandBlast Threat Emulationのクラウド・サービスの利用が困難なお客様に最適です。

Check Point
SOFTWARE TECHNOLOGIES LTD.

TE1000X SandBlastアプライアンス

1. 2TBハードディスク x 2
2. USBポート x 2
3. コンソール・ポート
4. 管理ポート（10/100/1000Base-T）
5. 同期ポート（10/100/1000Base-T）
6. 10/100/1000Base-Tポート x 4
7. 10GBase-F SFP+ポート x 2



導入オプション

次のいずれかの導入オプションで脅威をエミュレートできます。

1. プライベート・クラウド：チェック・ポイントのセキュリティ・ゲートウェイよりSandBlastアプライアンスにファイルを送信し、エミュレートします。
2. インライン：SandBlastアプライアンスをインラインまたはSPANポートで導入し、Threat Emulation、Threat Extraction、Antivirus、Anti-Botの各種Software Bladeを利用してトラフィックを保護するスタンドアロン型のオプションです。

包括的な脅威対策

SandBlastアプライアンスは、アンチウイルス、アンチボット、Threat Emulation（サンドボックス分析）、Threat Extractionの各種技術を活用して、既知および未知の脅威から保護します。

SandBlastによるゼロデイ攻撃からの保護

SandBlast Threat Emulationは、スピード、精度ともにクラス最高レベルのサンドボックス・エンジンにより不審なファイルを分析し、攻撃者による組織ネットワークへの侵入を阻止します。

既知の脅威の検出

Antivirus Software Bladeは、ThreatCloud™から配信されるリアルタイムのウイルス・シグネチャを使用して、既知のマルウェアをゲートウェイで検出、遮断します。一方Anti-Bot Software Bladeは、ボットに感染したコンピュータを検出し、ボットと指令（C&C）サーバ間の通信を遮断して被害の拡大を防止します。

回避能力を備えたマルウェアも検出

従来型のサンドボックス・ソリューションはOSレベル、すなわち攻撃者が脆弱性を悪用しコードを実行した後に、マルウェアの振る舞いを検出します。そのため、検出を容易に回避されてしまいます。

SandBlast Threat Emulationは、CPUレベルでの命令フローを監視する独自のCPUレベルの検査エンジンを活用して、OSのセキュリティ機能をすり抜けようとする攻撃を検出するため、悪意のあるコードが実行される前に効果的に阻止できます。

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、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 Threat Extractionは、アクティブ・コンテンツや埋め込みオブジェクトなど悪用可能なコンテンツを削除し、潜在的な脅威のないファイルを再構成します。そして、無害化したコンテンツを遅延なしでユーザに転送します。

Threat Extractionを設定する場合は、再構成後の文書ファイルを直ぐにユーザに転送する、またはSandBlast Threat Emulationの応答を待機してから再構成の必要性を判断するかを選択できます。

暗号化通信を検査

多くの一般的なセキュリティ・ゲートウェイを通過するSSLやTLSトラフィックは、攻撃者にとって組織による不正ファイルの検出を回避できる有用な攻撃経路です。チェック・ポイントの脅威対策では、このような保護されたSSLやTLSトンネルの内部を検査してファイルを抽出、実行し、トラフィックに潜む脅威を検出します。

Threat Emulationの詳細レポート

ファイルをエミュレートするたびに詳細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。ファイルをシミュレートしている間のスクリーンショットも確認できます。

ThreatCloudエコシステム

Threat Emulationが脅威を新たに検出すると、シグネチャが作成され、Check Point ThreatCloudに送信された後、他のチェック・ポイント・ゲートウェイにも配信されます。新たに見つかった未知の攻撃は既知の脅威として登録されるため、拡散を未然に防げるようになります。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。

技術仕様

	TE100X	TE250X	TE1000X	TE2000X / TE2000X HPP
				
パフォーマンス				
推奨検査ファイル数/月	10万	25万	100万	150万/200万
推奨ユーザ数	最大1,000	最大3,000	最大10,000	最大20,000
スループット	150 Mbps	700 Mbps	2 Gbps	4 Gbps
仮想マシン数	4	8	28	40 / 56
ハードウェア				
ディスク容量	1 TB HDD		ホットスワップ対応の冗長デュアル2TB HDD（RAID1）	
LOM	なし			
スライド・レール（22"～32"）	標準装備			
ネットワーク				
10/100/1000 Base-T RJ45	5	9	6	6
10GBase-F SFP+	-	-	2	4
拡張スロット	未使用			
寸法				
筐体デザイン	1U	1U	2U	2U
メートル（W x D x H）	435 x 448 x 44 mm	438 x 621 x 44 mm	438 x 561 x 88 mm	
重量	7.7 kg	9.8 kg	17.05 kg	
使用環境				
動作時	温度：0º～40ºC 湿度：20～90%（結露なきこと）			
非動作時	温度：-10˚～70˚C 湿度：20～90%（結露なきこと）			
電源				
ホットスワップ対応デュアル	-	オプション	標準装備	
AC入力電圧	100-240V			
周波数	47-63 Hz			
電源仕様（電源1台）	250W	400W	400W	400W
消費電力（最大）	50.4W	104W	225.6W	
熱出力（最大）	172.2 BTU/h	355.7 BTU/h	771.5 BTU/h	
適合規格				
安全性	CB、UL、Multiple Listing、LVD、TUV			
エミッション	FCC、CE、VCCI、RCM			
環境	RoHS			

アプライアンス・パッケージ

基本構成 [1]	
TE100X SandBlast Appliance（1年間のThreat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス、仮想マシン4台分のMicrosoft WindowsおよびOfficeライセンスを含む）	CPAP-TE100X-4VM
TE250X SandBlast Appliance（1年間のThreat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス、仮想マシン8台分のMicrosoft WindowsおよびOfficeライセンスを含む）	CPAP-TE250X-8VM
TE1000X SandBlast Appliance（1年間のThreat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス、仮想マシン28台分のMicrosoft WindowsおよびOfficeライセンスを含む）	CPAP-TE1000X-28VM
TE2000X SandBlast Appliance（1年間のThreat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス、仮想マシン40台分のMicrosoft WindowsおよびOfficeライセンスを含む）	CPAP-TE2000X-40VM
TE2000X High Performance Pack SandBlast Appliance（1年間のThreat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス、仮想マシン56台分のMicrosoft WindowsおよびOfficeライセンスを含む）	CPAP-TE2000X-56VM-HPP
Software Bladeパッケージ [1]	
Threat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス1年間更新パッケージ（TE100X Appliance用）	CPSB-TE-100-1Y
Threat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス1年間更新パッケージ（TE250X Appliance用）	CPSB-TE-250-1Y
Threat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス1年間更新パッケージ（TE1000X Appliance用）	CPSB-TE-1000-1Y
Threat Emulation、Threat Extraction、Antivirus、およびAnti-Botサービス1年間更新パッケージ（TE2000XおよびTE2000X HPP Appliance用）	CPSB-TE-2000-1Y

[1] 2年分および3年分のSKUも用意されています。オンラインの製品カタログをご覧ください

アクセサリ

インタフェース・カード、トランシーバ	
10G Fiberポート用SFP+トランシーバ・モジュール - ロング・レンジ（10GBase-LR）	CPAC-TR-10LR
10G Fiberポート用SFP+トランシーバ・モジュール - ショート・レンジ（10GBase-SR）	CPAC-TR-10SR
スペア、その他	
AC電源（TE250X用）	CPAC-PSU-TE250X
交換用部品キット（ハードディスク・ドライブ x 1、電源 x 1）（TE1000XおよびTE2000X Appliance用）	CPAC-SPARES-TE1000X/2000X

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 EDB39C0 2015.10