Datasheet

WatchGuard APT Blocker

進化し続けるマルウェアとゼロデイの脅威から防御

ゼロデイ攻撃に対抗するセキュリティ対策

ゼロデイ攻撃とはパッチやセキュリティ製品のシグネチャが提供される前に行われる未知の脆弱性を悪用した攻撃

シグネチャベースのウイルス対策は、従来通りゲートウェイにおける既知のマルウェアから防御する最前線の対策として非常に重要

APT Blockerは既知のマルウェアのみならず、未知のマルウェアへの対策を提供し、進化し続ける脅威からビジネスを防御

今日の８８%のマルウエアは既知のマルウェアが変異したもので、シグネチャベースのウイルス対策では検知できません。

"Malwise," IEEE Computers

ウイルス対策のみに依存するセキュリティ対策では、もはやビジネスを守ることはできません。今日のマルウェアは容易に変異して内部コードを変えることが可能になっているため、シグネチャでマルウェアを認識する従来のウイルス対策を簡単にすりぬけることが可能です。

次世代のフルシステムエミュレーション型サンドボックス

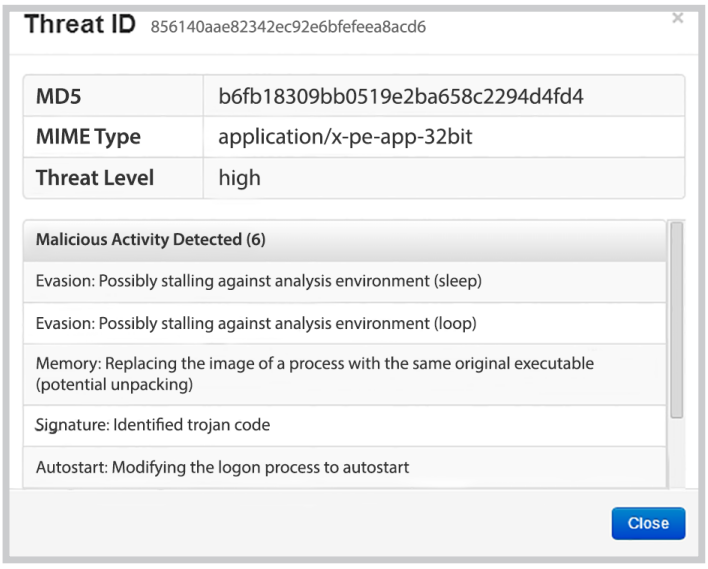
WatchGuard APT Blocker はファイルが不正なものであるかどうかを判定する「ふるまい検知」に重点をおいています。APT Blockerは疑わしいファイルを認識すると、クラウド上のサンドボックスに不審なファイルを転送し、サンドボックス上でエミュレーションを実行し、詳細分析を行い、マルウェアであるかどうかの判定を行います。

標的型攻撃（APT）を含む先進的なセキュリティの脅威はマルウェア検知のためのセキュリティ技術をすり抜けようとします。CPU、メモリなどの物理ハードウェアもシュミレート可能なAPT Blockerのフルシステムエミュレーションによりマルウェアの動作を完全に把握して可視化するため、先進的なマルウェアの検知をするぬける事は困難となります。

APT Blockerが分析するファイルタイプ

Windows上でのすべての実行形式ファイル
Adobe PDFファイル
MS Officeファイル（エクセル、ワード、パワーポイント、Visio）
Android アプリケーションインストーラ(APK形式)ファイル
圧縮ファイル(Windows ZIPファイル等)は解凍されます。

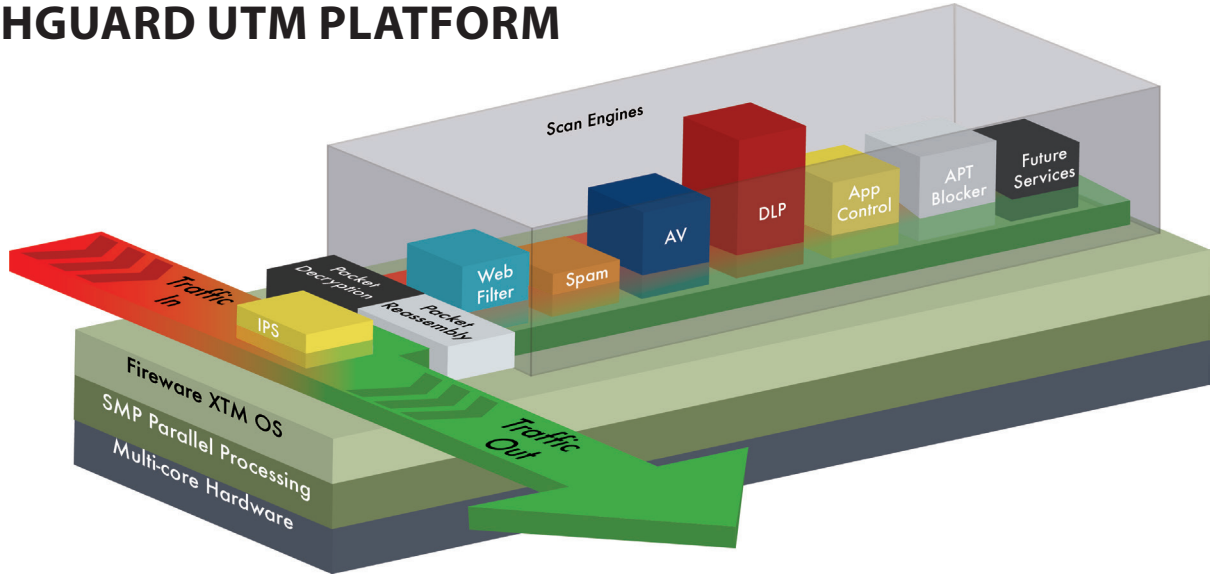
マルウェアの検出と比類のない詳細なマルウェアのレポート



APTレポートはファイルがマルウェアとして判定された根拠となる詳細な情報をレポートします。

APT Blockerは先進的なマルウェアに対する防御だけでなく、シンプルで直感的な対策を可能にします。さらにすべてのWatchGuard XTMシリーズに標準提供されるWatchGuard Dimension™により、強力なゼロデイ対策とネットワークに影響を及ぼすセキュリテリの情報をリアルタイムに判りやすい情報として可視化することが可能となります。

WATCHGUARD UTM PLATFORM



柔軟なアーキテクチャによりパフォーマンスの最適化とネットワークの脅威からの防御を実現

ウオッチガードのUTM(統合脅威管理)プラットフォームはネットワークトラフィックが完全なセキュリテリサービス(スパム対策から情報漏えい対策等)を最高のパフォーマンスレベルで運用できるよう設計されています。マルチコアプロセッサの処理能力を活用し、セキュリティプラットフォームは最大限のプロテクションと高速スループットを同時にバランスするようスキャンエンジンを管理します。CPU処理能力などのリソースは、データの流れとデータが必要とするセキュリティサービスに基づいて配分される。例えば、Webフィルタリングが、より多くの処理能力を必要とする場合には、CPUリソースの自動的な追加割当てを実施してWebトラフィックのスループットを維持し、安全なビジネスの継続を維持します。

容易なサブスクリプションの管理

セキュリテイサブスクリプションを含むWatchGuard XTMとFirebox T10の全てのセキュリテリ機能は一元的に管理され、ネットワークの状況をいつでもコンソールより管理する事が可能です。

KNOW WHAT'S HAPPENING ON YOUR NETWORK AT ALL TIMES

サービスによって認識されるすべてのセキュリティ活動についてのログが収集・保存され、インシデント発生時には迅速なセキュリティ対策のためのレポート生成を行います。

豊富なレポーティング機能、監視機能を含むすべての管理ツールはウォッチガード製品に標準で提供されますので、ハードウェア、ソフトウェアを追加で購入する必要がありません。

お問合せ:

ベストオブブリードUTM

ウォッチガードは市場において、最も信頼性の高いセキュリティソリューションを提供するためにベストオブブリード戦略を展開しています。業界内における先進的なテクノロジベンダと協業することにより、ウォッチガードはネットワークセキュリティサービスにおいて、オールスターのセキュリティ技術を提供します。

AVG websense TREND MICRO
CYREN SOPHOS lastline

AVG—ゲートウェイにおけるウイルス対策として、第三者機関のウイルスプリテンの評価テストにおいて高いパフォーマンスを継続した実証しています。

CYREN—特許取得済みのRPDR技術によるクラウドベースの効果的なスパム対策ソリューションを提供しています。1日に約40億件のメッセージをスキャ、検査を実施しています。

Websense—Websense セキュリティラボ と ThreatSeeker ネットワークに支えられるクラウド上の先進のデータベース情報をWebBlockerに提供

Trend Micro—IPS(不正侵入検知・防御)とアプリケーションのための最新のシグネチャを提供し、進化した脅威からの包括的な保護を実現

Sophos—情報漏えい防止機能を含む電子メールとエンドポイントセキュリティをグローバルの企業に提供

Lastline—クラウドベースのフルシステムエミュレーション分析技術との統合により、回避型の標的型攻撃を含むあらゆるマルウェアを検出

ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041 東京都港区麻布台1-11-9 CR神谷町ビル5階 Tel:03.5797.7205 Fax:03.5797.7207
http://www.watchguard.co.jp info-jp@watchguard.com

2015_03