HITACHI
Inspire the Next

次世代エンドポイントセキュリティ製品

パロアルトネットワークス Traps

3つの防御アプローチで攻撃を未然に防ぐ

未知のマルウェアや新たな脆弱性を使用した標的型攻撃など、攻撃は多様化しています。
単一機能によるセキュリティ対策ではもはや安全とは言えません。
Trapsは3つの新しい防御アプローチで、
さまざまな攻撃を、既知・未知を問わず未然に防ぎます。

Traps 3つの防御アプローチ

WildFire

パターンマッチング+サンドボックスの機能を提供するクラウド環境

パターンマッチングによる
既知マルウェアの検知

サンドボックスによる
未知マルウェアの振る舞い分析

機械学習

膨大なデータに基づく先進的な
機械学習エンジンでマルウェアを検知

脆弱性防御

アプリケーションの脆弱性を悪用した攻撃を
既知・未知を問わず防御

Trapsの特長

定期スキャンが不要

従来のアンチウイルス製品と異なり、定期的な全ファイルスキャンが不要で、ストレスなく利用が可能

軽量な動作

ディスク使用量、CPU使用率が低く、業務効率に影響を与えず効率的に利用可能

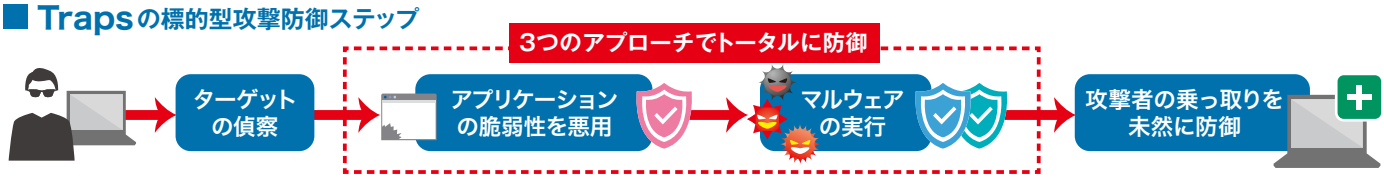
詳細なログ分析

攻撃された際のメモリダンプを含む多種のログデータを収集できるため、その後の詳細な調査、分析が可能

株式会社 日立ソリューションズ

防御アプローチの詳細

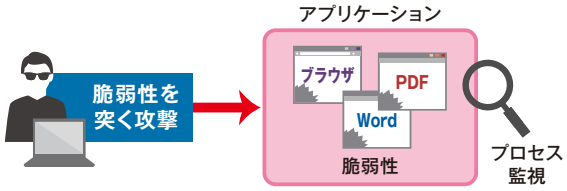
Trapsの標的型攻撃防御ステップ



脆弱性対策

脆弱性防御

脆弱性を悪用した攻撃で、共通して利用される攻撃手法をプロセス上で常時監視。攻撃手法自体を阻止するため、脆弱性の既知・未知問わずに防御。プロセスを監視する検知手法のため、ファイルタイプに依存せず、ファイルが介在しない脆弱性攻撃も防御可能。



マルウェア対策

WildFire

- 世界中に導入されたパロアルトネットワークス製品から、最新マルウェア情報を収集。この情報を基に、パターンマッチングで既知のマルウェアを検知し、実行を阻止。
- 未知のファイルをクラウド上の仮想環境で実行。振る舞い分析によりマルウェアを検知し、実行を阻止。

機械学習

WildFireで収集した膨大な数のファイルから、マルウェアファイルに共通する特徴をさまざまな観点で抽出。特徴を学習したエンジンでマルウェアを検出し、実行を阻止。

■ 一般的なマルウェア対策製品のマルウェア種類別検出可否

対策製品種類＼マルウェア種類	既知	未知(亜種)	未知(新種/カスタマイズ化)
パターンマッチング型製品	○ パターンファイルとの照合により確実にブロック	△ パターンファイルに合致するとは限らない	× パターンファイルで対応できない
サンドボックス型製品	△ 高精度な検出が可能だが解析時間が必要	△ サンドボックス回避技術により検知できない場合もあり	○ 回避技術の懸念はあるが、未知のマルウェアに有効
機械学習型製品	△ 特徴から外れるものは検出漏れが発生	○ 亜種は特徴が似るため機械学習が得意とする分野	× 特徴を外す完全な新種には対応できない
Traps	○	○	○
	Trapsはこれら全ての技術を用いて既知・未知のマルウェアを検出可能!		

従来のアンチウイルス製品との違い

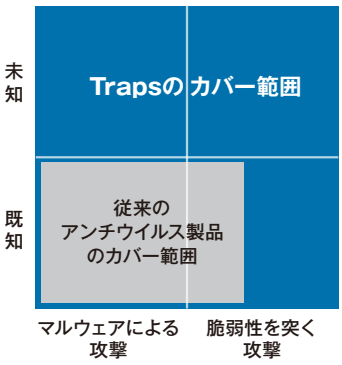
Traps

脆弱性、マルウェアの両方の攻撃に対応可能です。
既知はもちろん未知の攻撃も防御できるため、日々進化する攻撃に柔軟に対応できます。

従来のアンチウイルス製品※

主に既知のマルウェア対策に特化しています。
そのため、近年増加する脆弱性攻撃や未知のマルウェアには対応できません。

※パターンマッチングによるエンドポイントのアンチウイルス製品



株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/paloalto/sp/

S16K-12-02 | 2017.01