パロアルトネットワークスについて

パロアルトネットワークス合同会社

2015年 6月 18日

paloalto NETWORKS®
the enterprise security company™

パロアルトネットワークスについて

ハイライト

2005年 設立
（本社：米国カリフォルニア州サンタクララ）
2012年 NYSE上場

“次世代ファイアウォール”の生みの親
ファイアウォール市場のマーケットリーダー

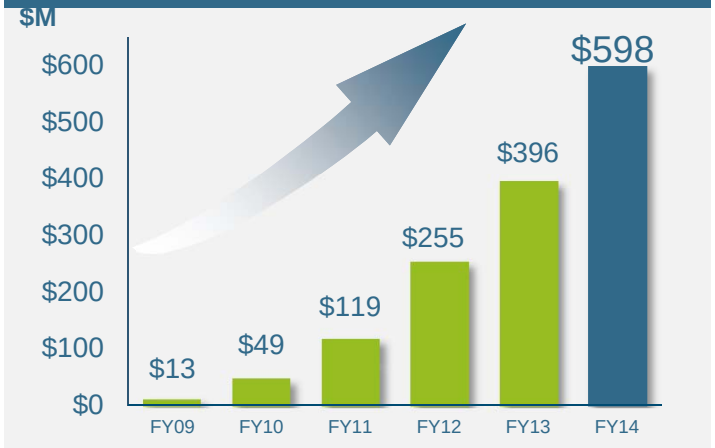
アプリケーションの安全な活用を実現
ネットワークの幅広いセキュリティニーズに対応

ハイエンドなお客様にも対応できる
グローバルでの販売体制
24時間365日のテクニカルサポート体制

圧倒的な技術力を持ったエンジニア集団と
経験豊富な経営陣

従業員数：ワールドワイドで 1600 名以上
世界22カ国、26拠点で事業展開

売上



顧客数

ファイアウォール市場のマーケットリーダー

“Palo Alto Networks は引き続き競合メーカーに影響を与え、**ファイアウォール市場自体を牽引**しており、リーダーと評価される。
その理由は次世代ファイアウォールというデザインによる部分が大きい。
市場全体が次世代ファイアウォールの方向に向かっており、継続的に競合製品を置き換えながら、**急激に売上とマーケットシェアを伸ばしており**、
市場を席巻しているためすべてのメーカーが反応せざるをえなくなっている”

＜ Gartner, April 2013 ＞

“パロアルトネットワークスは、ガートナーの調査企業の**最も競争力のある**NGFWショートリストに上げられ、ベンダー調査では、ほとんどのベンダーが競合するベンダーと言及している。

ガートナーのクライアントは、一貫してパロアルトネットワークスのApp-IDとIPSを高く評価し、**利便性と品質も競合他社の製品よりも高い**と評価している。

シンプルな料金体系は、競合他社製品と比較し調達際に有効

＜ Gartner, April 2014 ＞

エンタープライズネットワークファイアウォールの
マジック・クアドラント

Gartner

paloalto NETWORKS

脅威への対策　-CYBER THREAT ALLIANCEの設立-

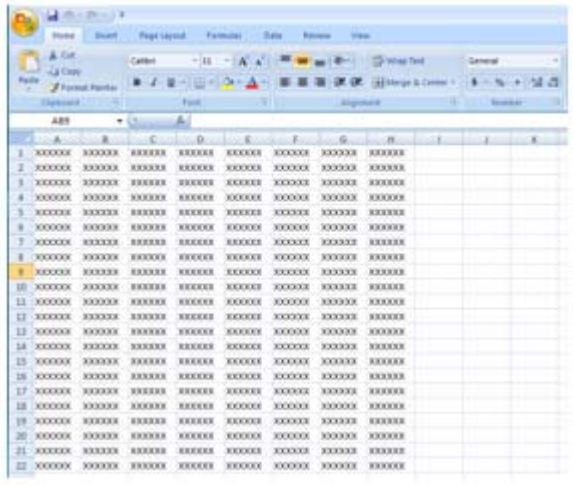
http://cyberthreatalliance.org/

2014年5月に Fortinet 社と Cyber Defense Consortium を共同設立。
9月には McAfee社,Symantec 社も加わり、クロスベンダでマルウェア情報を交換する取り組みも実施しております。
https://www.paloaltonetworks.com/company/press/2014/mcAfee-symantec-join-fortinet-palo-alto-networks-as-cofounders-of-the-industry-first-cyber-threat-alliance.html

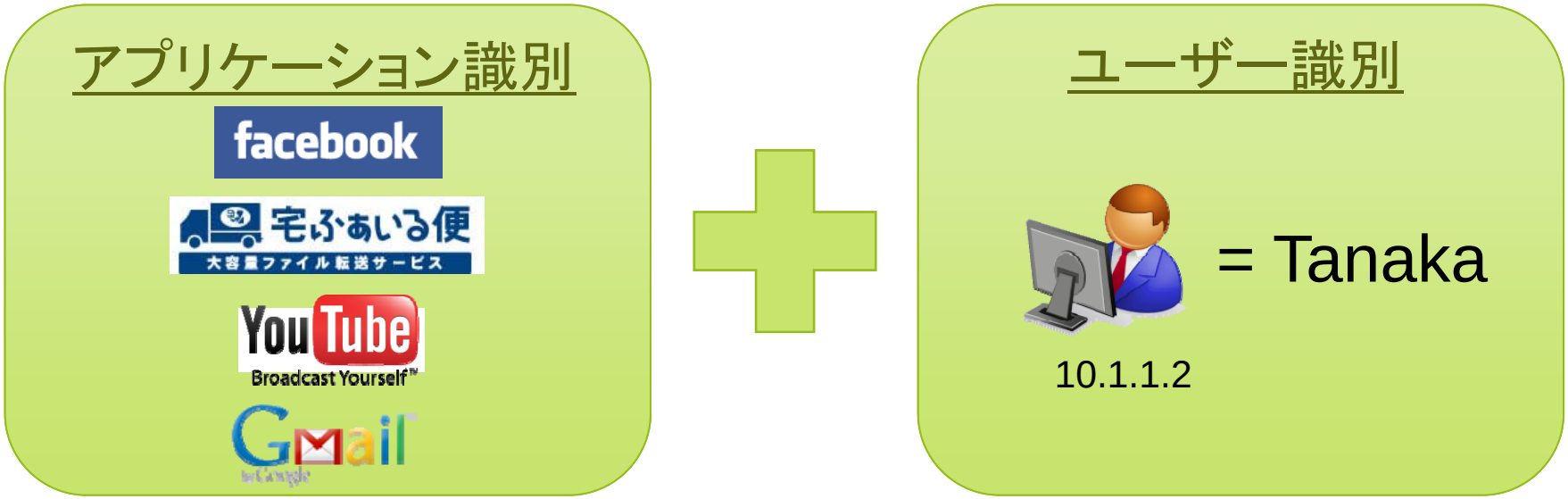
Unit 42

- Unit 42はPalo Alto Networks内のサイバーセキュリティ研究者やの業界の専門家で構成された集団で、最新の脅威についての情報を収集・調査・分析し、詳細や対策を広く提供しています。

- 実績例：DragonOK
  - 2015年4月、日本の企業・組織をターゲットとした中国の犯罪集団からの標的型攻撃を確認。
  - 一見無害に見えるMS Word, Excelを模したexeファイルを使用するケースが多く、今回は訃報を知らせるメールに、マルウェアを仕込んだexeファイルが添付されていた。
  - Unit 42はクラウド型サンドボックスWildFireと、WildFireにより収集される情報を元に相関分析を行うAutoFocusというサービスを利用し、「FormerFirstRAT」という新種のバックドアツールを発見。



これからのファイアウォールに求められること①



- アプリケーション識別
  - パスしても良いアプリケーションとブロックしたいアプリケーションが同じポート番号を利用している場合でも、アプリケーションを識別することで、適切な制御を適用する
- ユーザー識別
  - 組織の中では、アプリケーションの種類によって、ある人にはブロックしたいが別の人には使わせたいという場合があり、ユーザーを識別することで利便性を確保する

これからのファイアウォールに求められること②

- UTM(Unified Threat Management) 機能を付加したファイアウォールもありますが・・・
  - URLフィルタリング、アンチスパム、アンチウィルスなどが利用できる
- UTMのよくある問題点
  - ゼロデイアタックには対応できていない
  - ファイアウォールに機能を付加した経緯の製品では
    - UTM機能をenableにするとパフォーマンスが急激に劣化
    - ファイアウォールのログとUTMのログが別々に上がり、管理が煩雑

リアルタイム防御

パフォーマンス維持

容易なログ管理

次世代ファイアウォール　PAシリーズ

- ポート番号、プロトコル、暗号に関わらず**アプリケーションを識別**し制御
- IPアドレスに関わらず**ユーザを識別**
- 脆弱性攻撃、情報漏えい、マルウェア等の脅威に対して**リアルタイムに防御**
- 独自のシングルパスアーキテクチャで**パフォーマンスの劣化を抑え**高速処理を実現
- 全ての機能を**一つの管理画面**に集約、ユーザごと、アプリケーションごとにワンクリックで集計可能

パロアルトネットワークス製品ラインナップ

ネットワーク ロケーション	データセンター/ クラウド	エンタープライズ境界	分散型エンタープライズ /BYOD
次世代 ファイアウォール 製品群	   アプライアンス: PA-200, PA-500, PA-30x0, PA-50x0, PA-70x0 仮想ソフトウェア: VM-Series VM-100,200,300,1000-HV		
サブスクリプション サービス	脅威防御		
	URLフィルタリング		
	Global Protect™		
	WildFire™		
管理システム	Panorama および M-100 アプライアンス		
OS	PAN-OS™		

paloalto NETWORKS

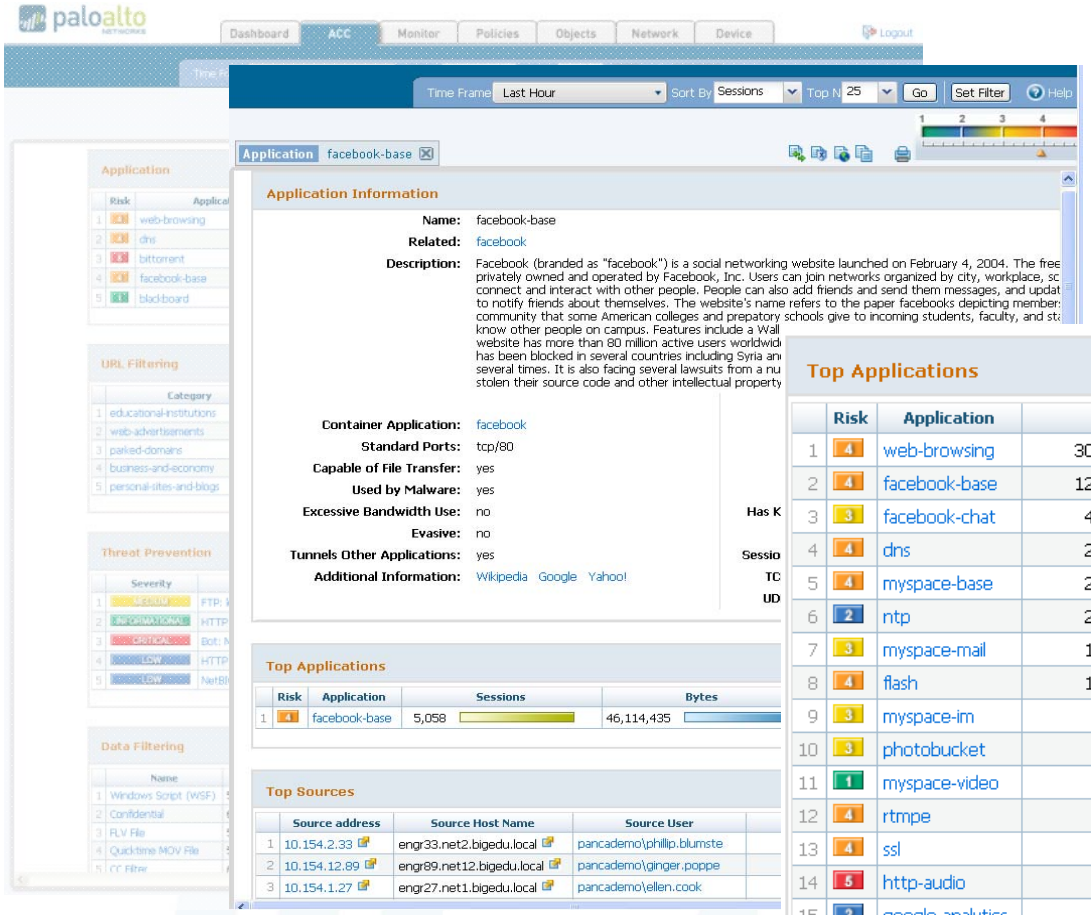
パロアルトネットワークス製品でできること

- ネットワークセキュリティを全方位でカバー
- ユニークな機能を多数搭載
- 複数のセキュリティ機能を使用しても、パフォーマンス劣化が少ない
- 潜在化しているセキュリティリスクを顕在化できる

分野	機能			
防御	ファイアウォール	ウイルス対策	スパイウェア対策	URLフィルタ
	IPS/IDS	標的型攻撃/ 未知の攻撃	ボットネット レポート	DOS攻撃
コントロール	アプリケーション 可視化/制御	ファイル/データ ブロック	SSL暗号化/復号化	QoS
運用／管理	ユーザー 識別/制御	SSL-VPN	ログの 一元管理	仮想化FW

トラフィックの可視化・制御

- **Web管理画面により、迅速かつ的確な情報可視化が可能**
- **通信の種別や脅威の種類を的確に分析することが可能**



アプリケーション,ユーザ単位、URLフィルタ、攻撃やマルウェア検出、データフィルタリング機能などの統計情報の概要を表示する管理画面

容易な運用監視 – 豊富なレポーティング機能

- 40種類を超える標準レポートを用意
- 必要に応じてカスタマイズレポートの生成が可能
- 確認したいレポートをPDF化してeMailで管理者へ送付可能