PALO ALTO NETWORKS

最新動向のご紹介

2018年12月13日

パロアルトネットワークス株式会社
金融営業本部
本部長　中道良成

Agenda

Ⅰ 会社最新状況アップデート

Ⅱ 金融業界における動向

Ⅲ パロアルトネットワークスが提供するセキュリティソリューション

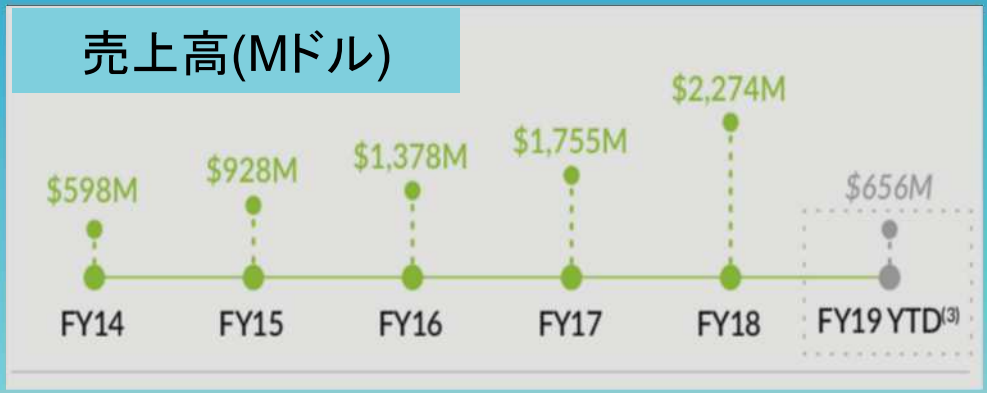
Ⅳ 金融機関様の導入事例

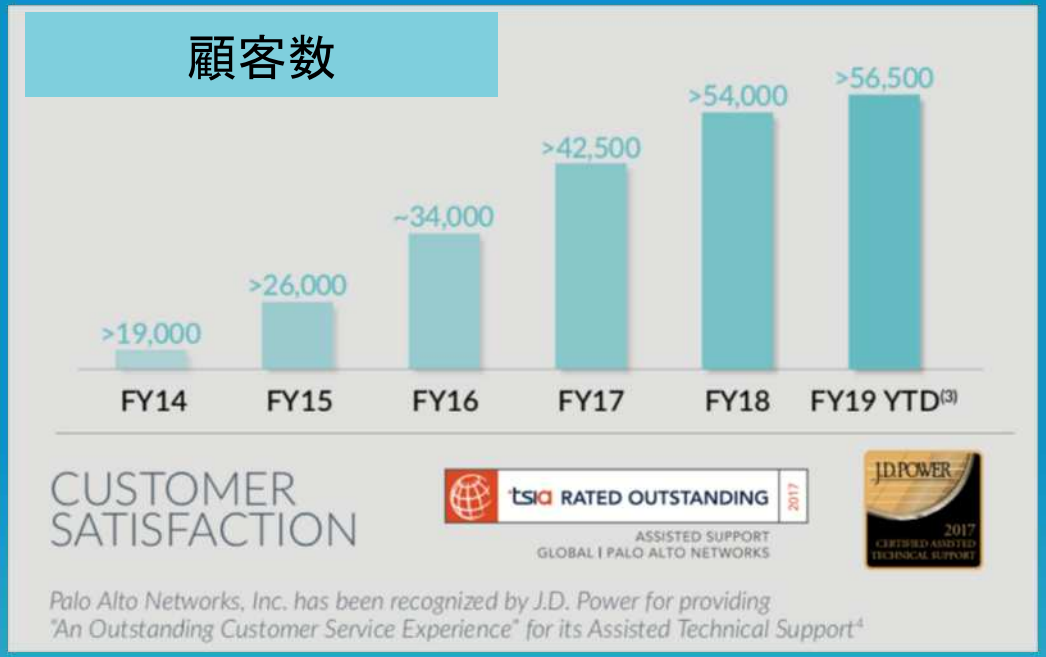
Ⅰ　会社最新状況アップデート

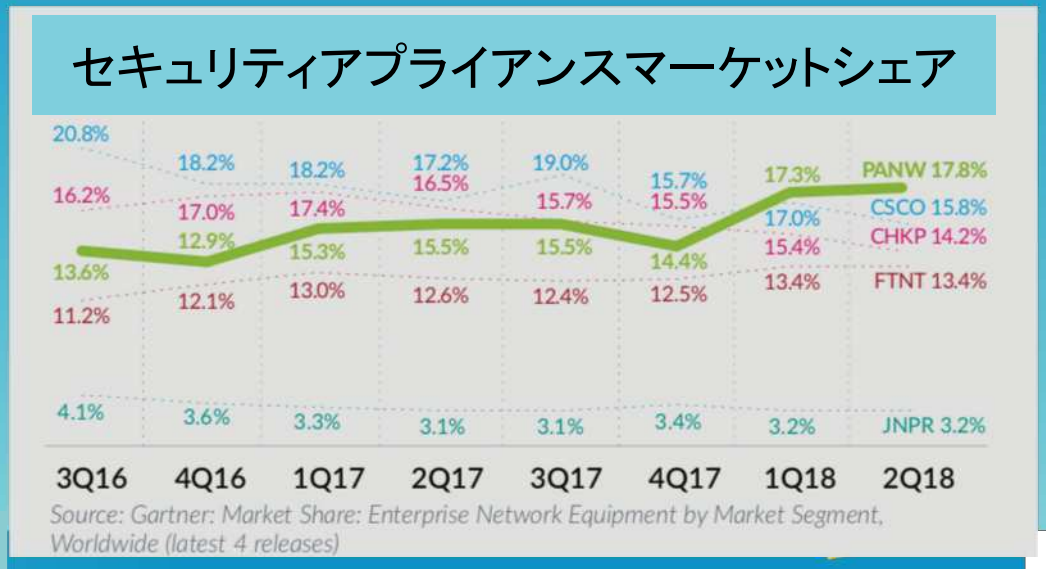
会社アップデート

FY19 Q1 (8月ー10月) 四半期概況

- 売上高が前年同期比で 31%増 の$656M(¥754億)
- 年間平均成長率 約30%
- マーケットシェアが17.8%に拡大
- 150ヵ国、56,500社以上のお客様が利用、四半期ごとに新規に1,000社以上のお客様が導入
- 4,000社以上のお客様がTraps製品を導入
- 2005年設立、2012年NYSE上場（PANW)







第３者機関評価

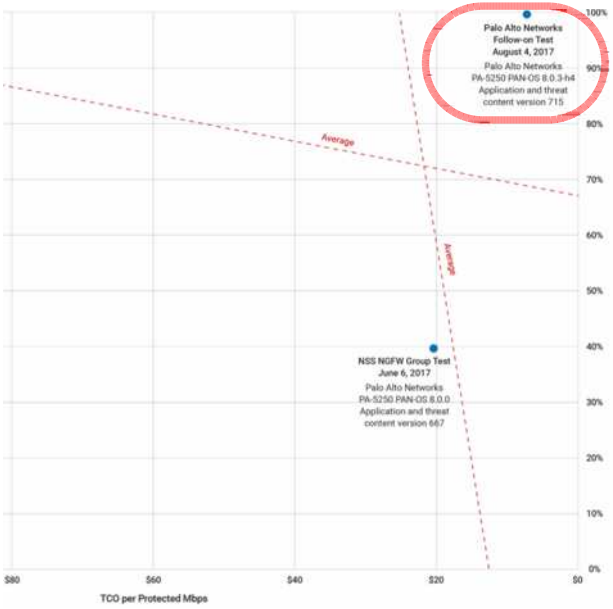
Gartner
パロアルトネットワークス社は
7年連続でリーダーと評価
されています。

Enterprise Network Firewalls

Figure 1. Magic Quadrant for Enterprise Network Firewalls

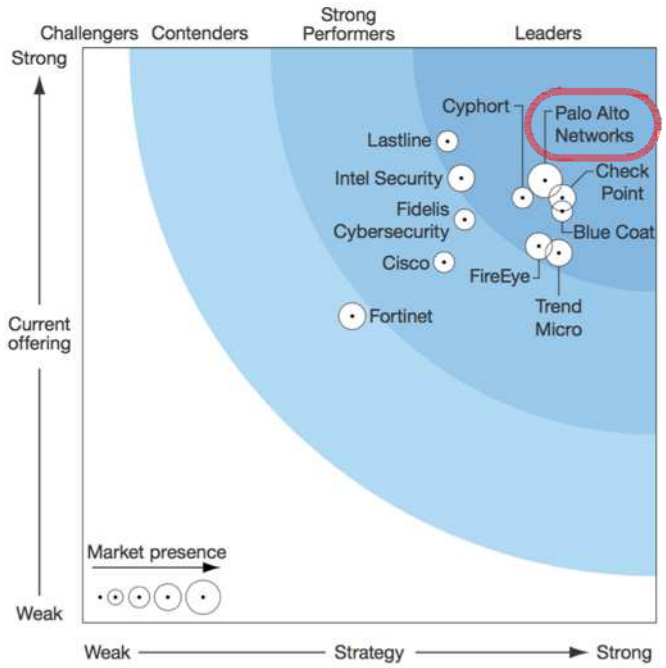
Source: Gartner (October 2018)

NSS Lab の
Next Generation Firewall
の評価でRecommendedを獲得



FORRESTER®

FORRESTER 社のマルウェア自動分析
のリサーチでリーダーを獲得。
WildFireが最高の評価を受ける。



PALO ALTO NETWORKS IS POSITIONED AS A LEADER IN THE GARTNER MAGIC QUADRANT FOR ENTERPRISE NETWORK FIREWALLS*

Palo Alto Networks is positioned as a Leader for the seventh consecutive time

Gartnerのマジッククアドラントにて
パロアルトネットワークス　次世代ファイアウォールが**７年連続でリーダー**のポジションに
(一番右上の最高の評価に)

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (October 2018)

Gartner, Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, 4 October 2018

金融業界へのセキュリティ啓蒙として参画

Financials ISAC Japan Information Sharing and Analysis Center

弊社は金融ISAC - 2015年5月から加盟
最上位のアフェリエイト会員ゴールド

金融ISAC会員数は363社
(2018年11月27日時点)

金融ISAC会員向けに以下の支援を実施
- 脅威インテリジェンスレポートの提供
- 脅威情報の配信
- 製品実感・運用セミナーの開催

FIEC 金融情報システムセンター
The Center for Financial Industry Information Systems

金融情報システムセンター – 2014年9月から
賛助会員として加盟

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

早期警戒グループ会員、脅威情報の連携

フィッシング対策協議会
Council of Anti-Phishing Japan

2015年4月から正会員として加盟
共有されたフィッシングサイトの情報をPAN-DBの
Phishingカテゴリに1時間以内に反映

新CEO　Nikesh Arora(ex.Google, Softbank) クラウドにシフト

CNET Japan ＞ ニュース ＞ 企業・業界

元ソフトバンクCOOのアローラ氏、パロアルトネットワークスCEO就任へ

Stephanie Condon （ZDNet.com） 翻訳校正： 編集部 2018年06月04日 11時19分

シェア 12 ツイート B! 2 Pocket 24 G+ 印刷 メール 保存 クリップ

Palo Alto Networksは米国時間6月1日、取締役会がNikesh Arora氏を最高経営責任者（CEO）兼会長に指名したことを発表した。Arora氏は以前、ソフトバンクで最高執行責任者（COO）を務めていた人物だ。

Arora氏は2014～2016年の間、ソフトバンクのCOO兼プレジデントを務めた。ソフトバンクの幹部就任前には、Googleで最高ビジネス責任者を務めた。Palo Altoは同氏について、「Googleの検索事業の売り上げが20億ドルから600億ドルに成長する中で重要な役割を果たした」としている。

Agenda

Ⅰ 会社最新状況アップデート

Ⅱ 金融業界における動向

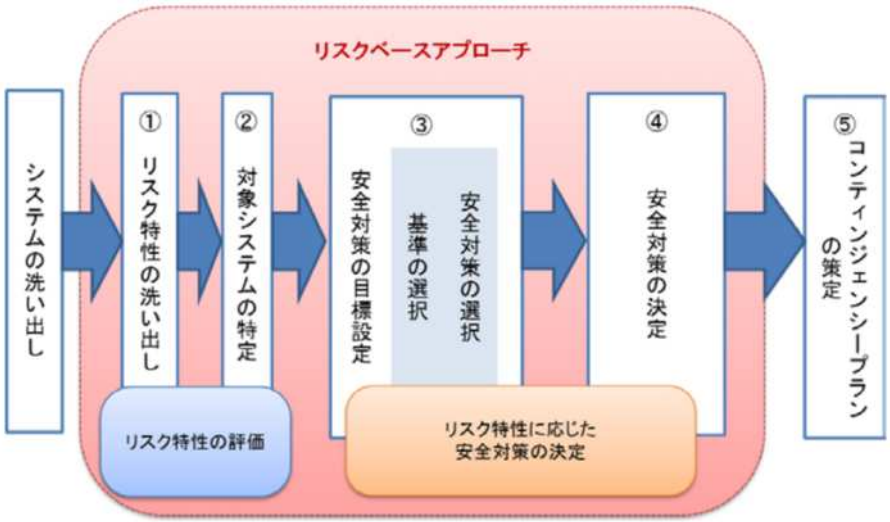
Ⅲ パロアルトネットワークスが提供するセキュリティソリューション

Ⅳ 金融機関様の導入事例

Ⅱ 金融業界における動向

安全対策基準 第9版 (平成30年3月)

今回の改訂では、安全対策の考え方として、“リスクベースのアプローチ”の考え方を取り入れている。



経営層

顧客の利便向上や企業価値の最大化を目指して経営資源配分と最適な安全対策が決定され、残存リスクに対して適切に対応されている限りにおいては、その責任は果たされていると解される。

クラウド利用

金融機関においては、クラウド事業者との責任分界点を理解したうえで、利用するクラウドサービスのリスクの特性に応じた適切な統制が行えるかどうかを確認することが重要となる

金融機関を取り巻く環境の変化

現在

- 第3者評価によるセキュリティの見直し
- 入口・出口対策の投資効果判断、運用コスト、フローの見直し
- クラウド向けセキュリティ対策の検討
- CSIRT 体制整備・運用改善
- 金融ISAC、地域金融間の連携
- 仮想通貨対応

今後

- IT資産を持たいない戦略へのシフト
- デジタルトランスフォーメーション
- クラウド利用前提のITガバナンス整備
- 働き方改革への対応
- 脅威インテリジェンスの導入
- セキュリティ製品の有効活用

⇨ 省力化・自動化・効率化が課題

Agenda

Ⅰ 会社最新状況アップデート

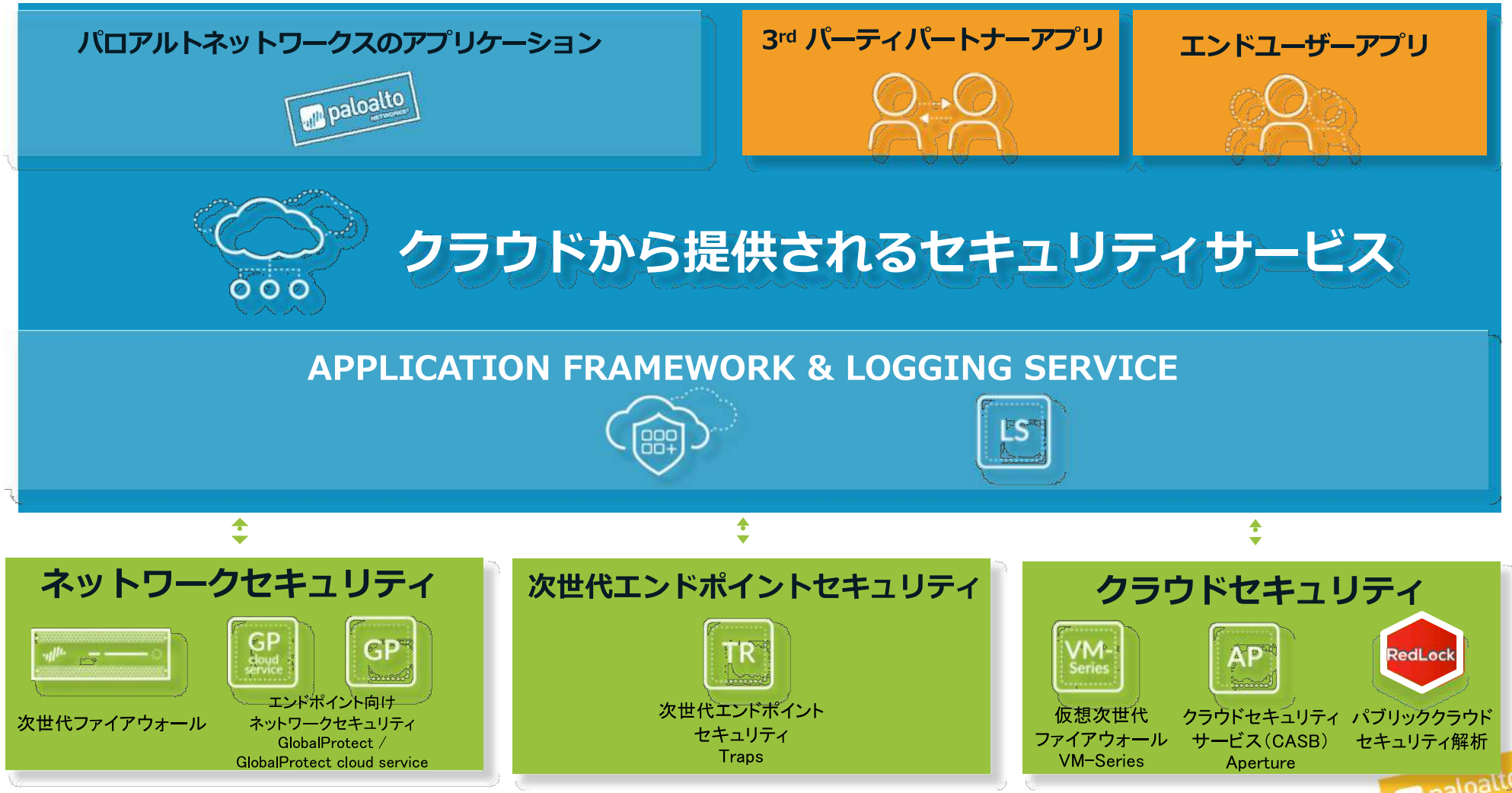
Ⅱ 金融業界における動向

Ⅲ パロアルトネットワークスが提供するセキュリティソリューション

Ⅳ 金融機関様の導入事例

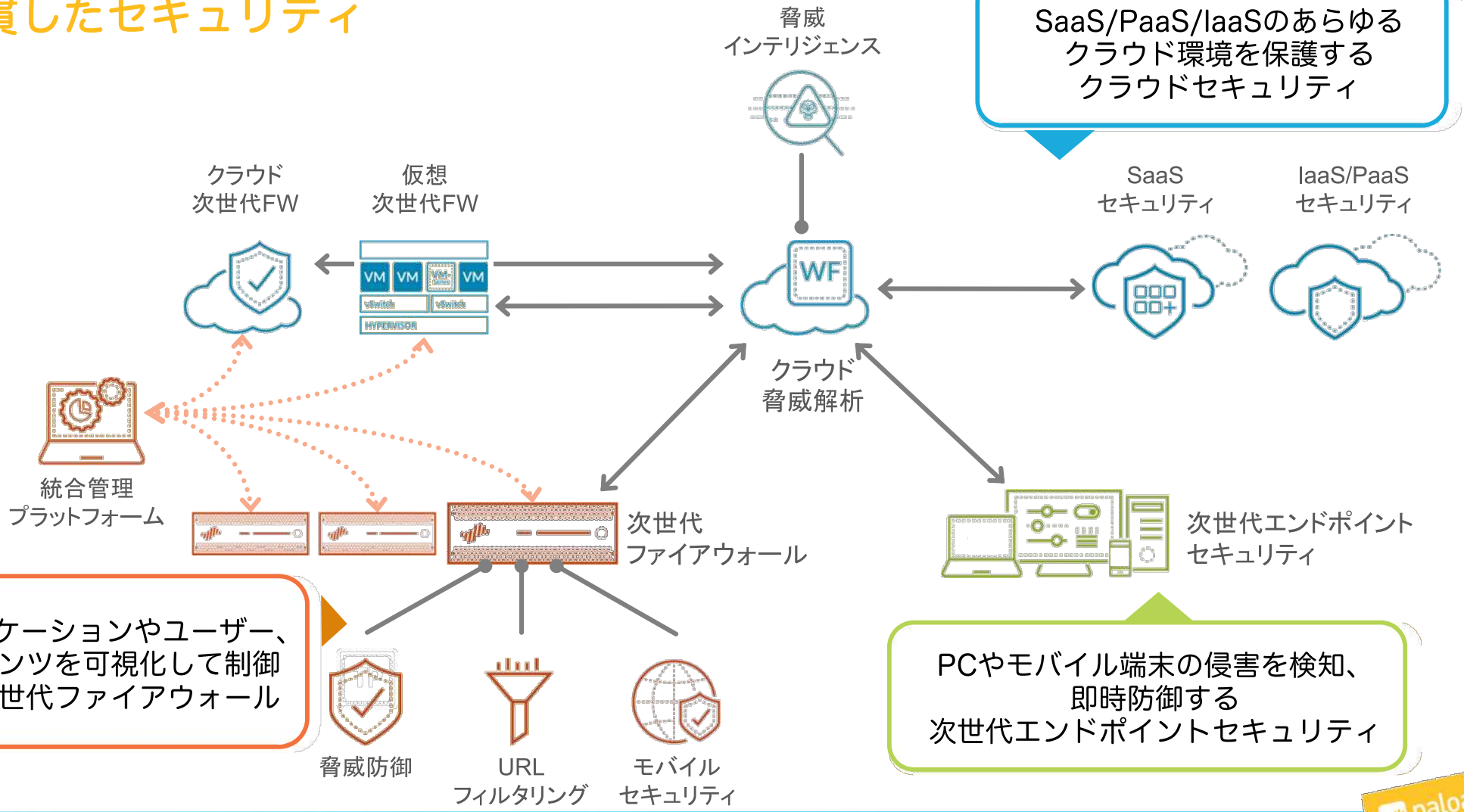
Ⅲパロアルトネットワークスが提供する
最新セキュリティソリューション

パロアルトネットワークス
“セキュリティー・オペレーティング・プラットフォーム”



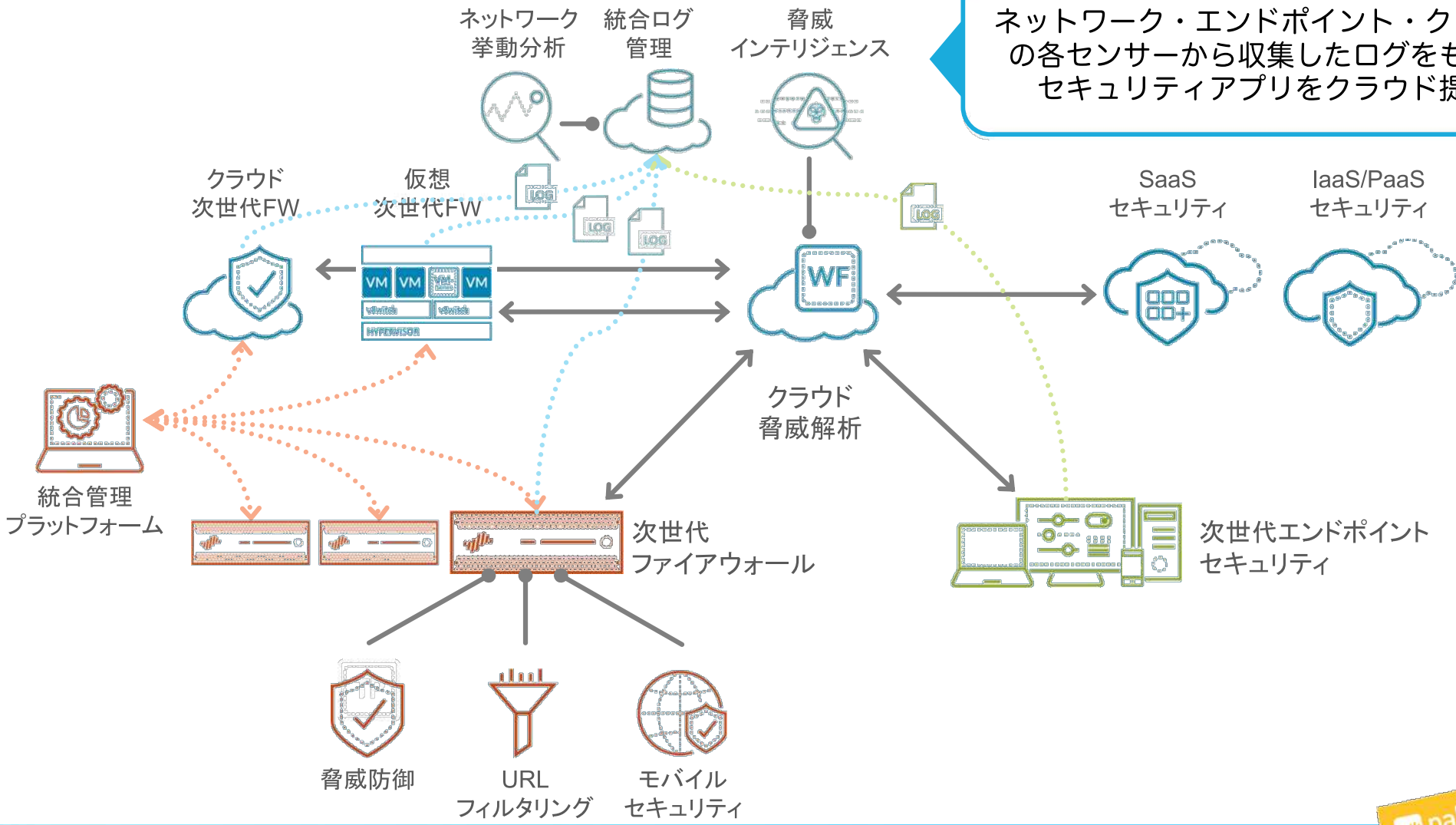
 |

パロアルトネットワークス　変革
一貫したセキュリティ

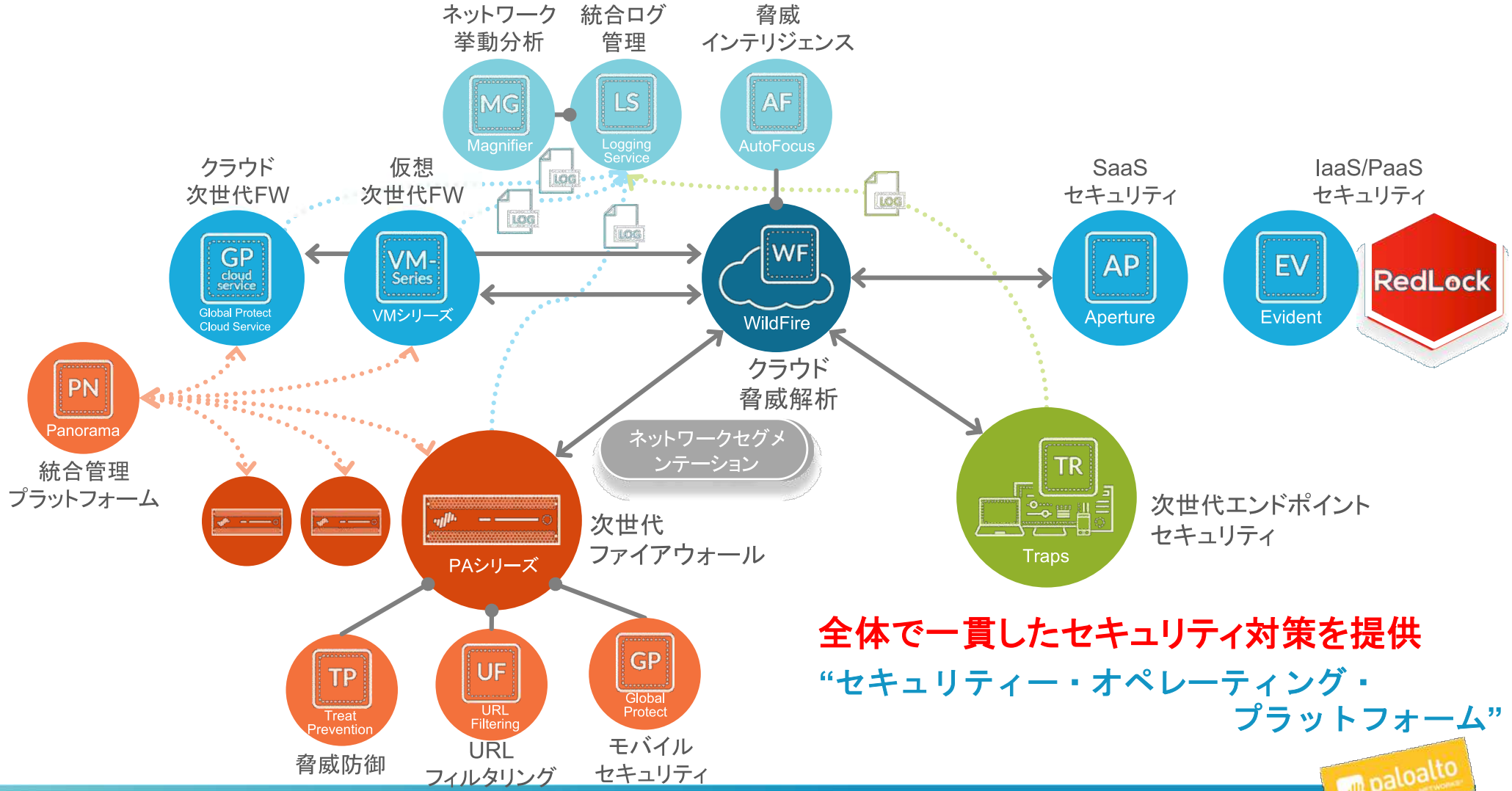


 |

パロアルトネットワークス　変革



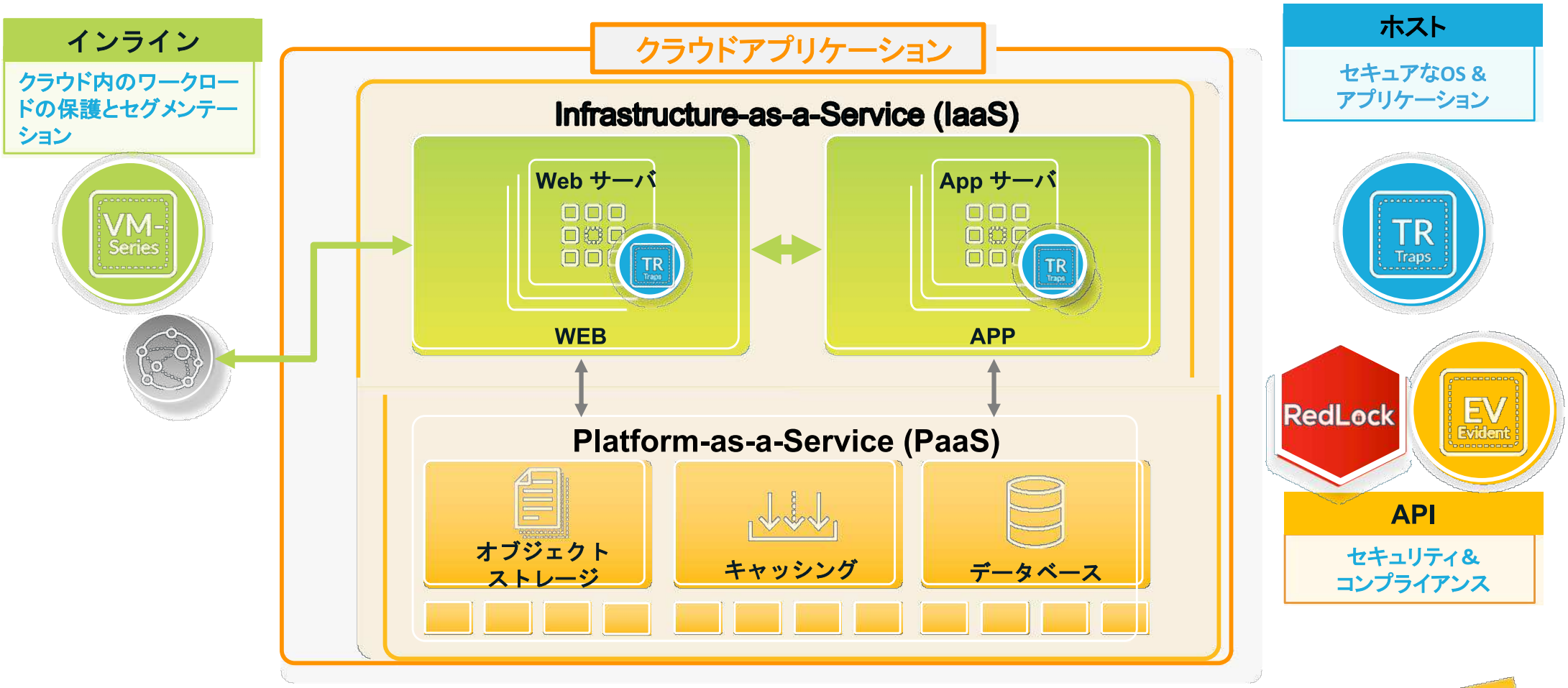
製品ポートフォリオ 全体像



全体で一貫したセキュリティ対策を提供

“セキュリティー・オペレーティング・プラットフォーム”

パブリッククラウド向けのセキュリティアプローチ



 |

A Tip　　お役立ち情報

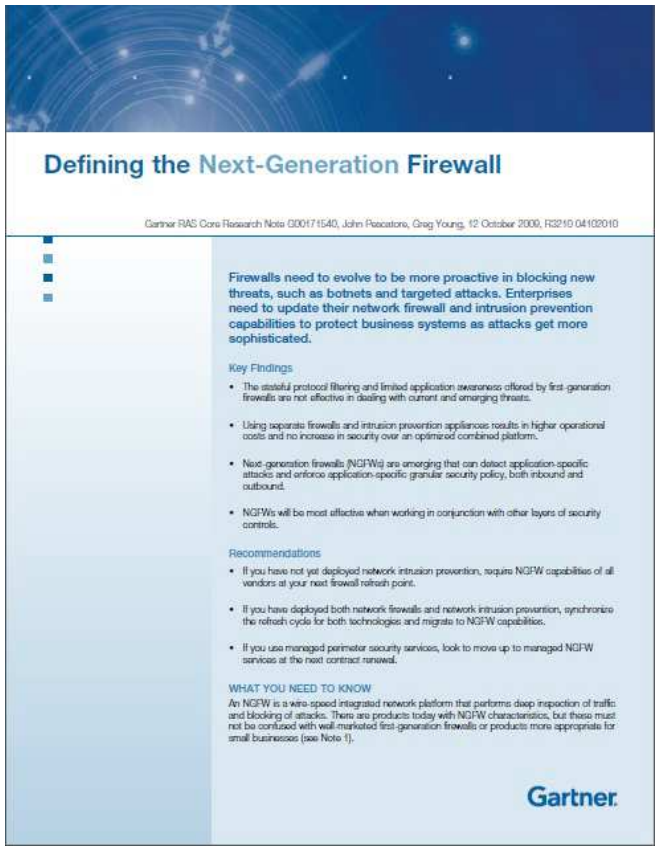
ところで、、、、、、、、

今さら聞けない
「次世代ファイアウォール、とは？ 」

そして、なぜ
「パロアルトネットワークス？」 なのか。

 |

次世代ファイアウォールとは？



Defining the Next-Generation Firewall

Gartner RAS Core Research Note G00171540, John Pescatore, Greg Young, 12 October 2009, R3210 04102010

Firewalls need to evolve to be more proactive in blocking new threats, such as botnets and targeted attacks. Enterprises need to update their network firewall and intrusion prevention capabilities to protect business systems as attacks get more sophisticated.

Key Findings

- The stateful protocol filtering and limited application awareness offered by first-generation firewalls are not effective in dealing with current and emerging threats.
- Using separate firewalls and intrusion prevention appliances results in higher operational costs and no increase in security over an optimized combined platform.
- Next-generation firewalls (NGFWs) are emerging that can detect application-specific attacks and enforce application-specific granular security policy, both inbound and outbound.
- NGFWs will be most effective when working in conjunction with other layers of security controls.

Recommendations

- If you have not yet deployed network intrusion prevention, require NGFW capabilities of all vendors at your next firewall refresh point.
- If you have deployed both network firewalls and network intrusion prevention, synchronize the refresh cycle for both technologies and migrate to NGFW capabilities.
- If you use managed perimeter security services, look to move up to managed NGFW services at the next contract renewal.

WHAT YOU NEED TO KNOW

An NGFW is a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks. There are products today with NGFW characteristics, but these must not be confused with well-marketed first-generation firewalls or products more appropriate for small businesses (see Note 1).

Gartner.

調査会社毎に
定義は若干異なるが、
大体以下の機能を
実装している製品を指す

アプリケーション識別に基づいた
アクセス制御

ユーザ識別

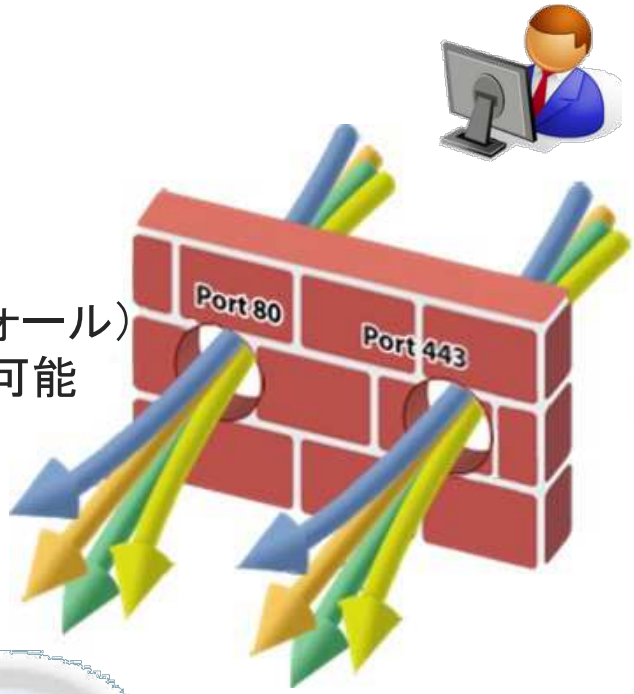
次世代FWの成り立ち

 |

次世代FWの成り立ち

- インターネットの普及に伴い、
  様々なWebサービスが乱立

- 従来のポートベースのFW（ファイアウォール）
  では、これらを制御するのはもはや不可能



- なぜならば、これらのWeb
  サービスは、80番ポート、
  443番ポートでサービスを
  提供しているため、ポート
  ベースのFWでは、すべて
  通すか、すべて止めるかの
  極端な制御しかできない

 |

次世代ファイアウォールとは？

＜前世代FW＞従来のポートベースのFW（ファイアウォール）では、様々なwebサービス制御するのはもはや不可能

パロアルトネットワークスの次世代FWは、一般的な次世代ファイアウォールの枠に収まらない、様々なセキュリティ機能を実装しています

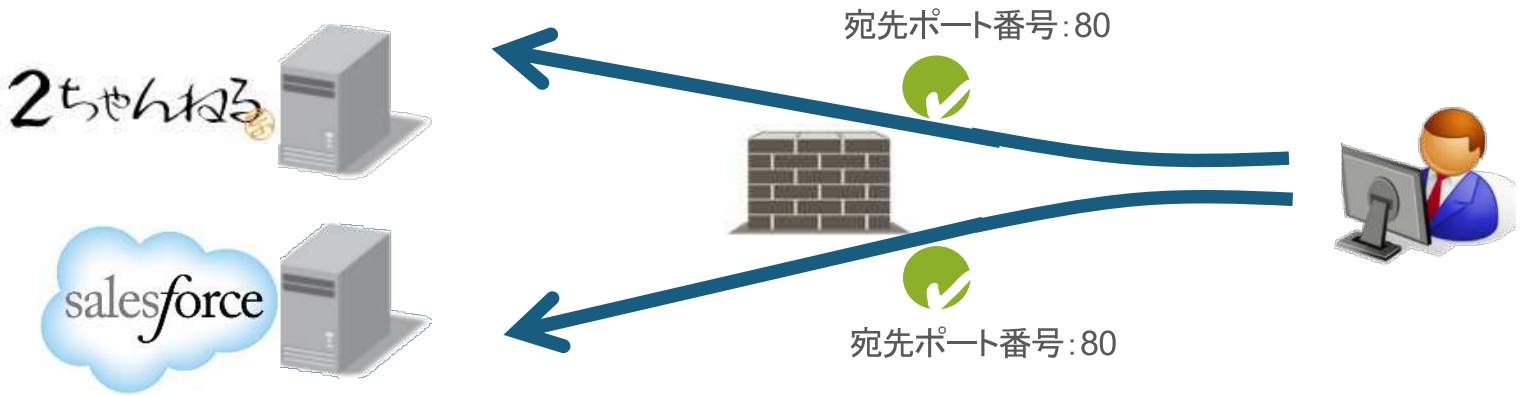
- アプリケーション識別に基づいたアクセス制御
- ユーザ識別
- IPS

- Anti-Virus
- Anti-Spyware
- URL Filtering
- File Blocking
- Botnetレポート
- WildFire

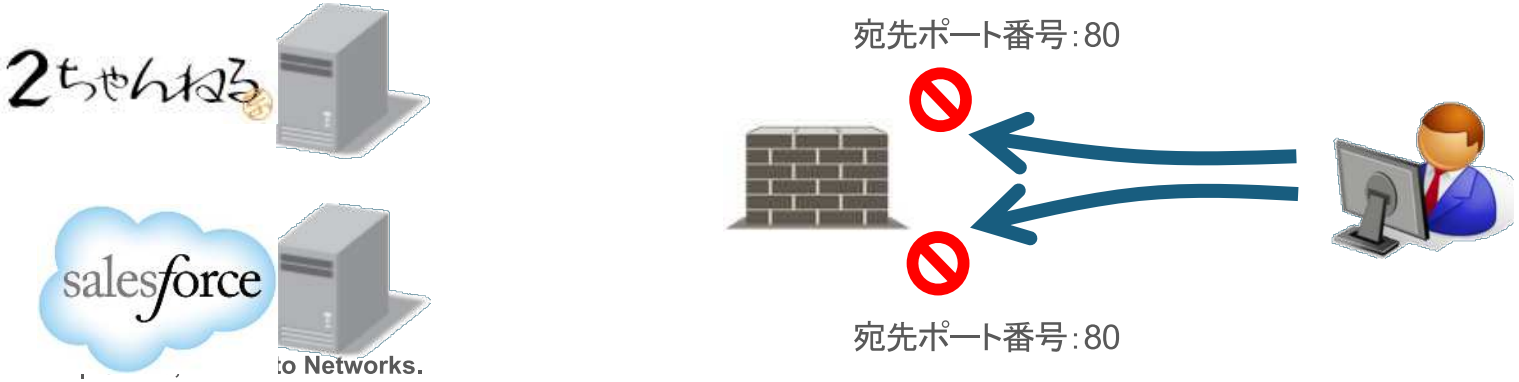
パロアルトネットワークスの次世代FW

従来のポートベースのFWの動作

- 80番ポート宛ての通信を許可

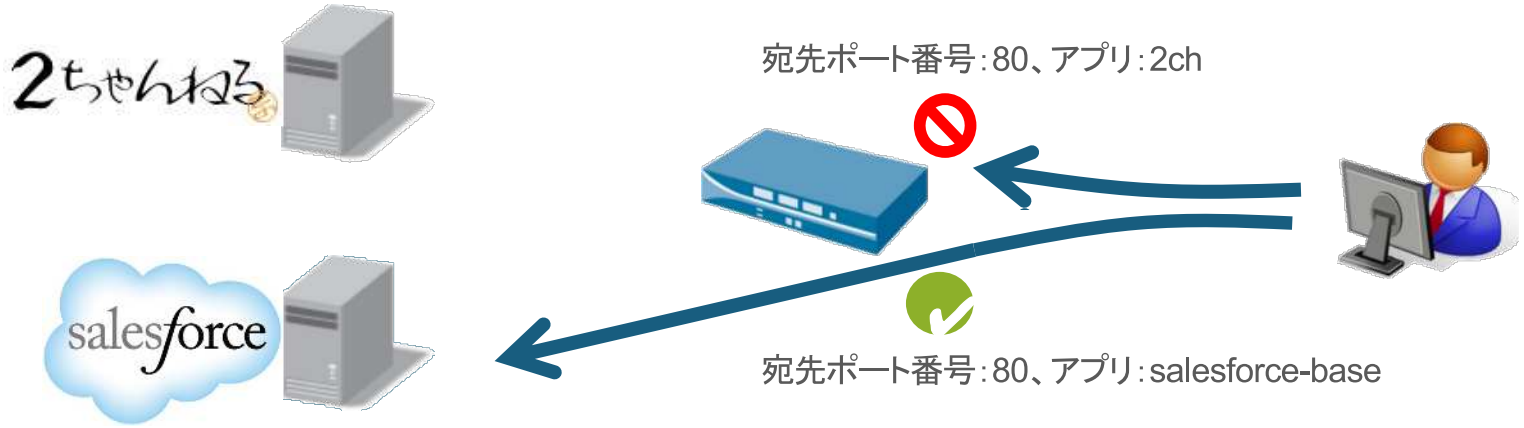


- 80番ポート宛ての通信をブロック



次世代FWの動作

- 次世代FWの動作



同じ80番ポート宛ての通信でも
アプリケーション毎に
アクセス制御が可能

次世代FWのログ

Receive Time	Source	Destination	From Port	To Port	Application	Action
04/10 11:34:19	192.168.20.101	206.223.153.10	47817	80	2ch	deny
04/10 11:34:16	192.168.20.101	63.140.45.105	47738	80	salesforce-base	allow

次世代FWの成り立ち

- 「アプリケーション識別に基づいたアクセス制御」は、どのように使うのか？
- 主な用途は2つ
  - ①セキュリティ向上
    - 脅威の侵入や情報漏洩のリスクを削減
      - 掲示板、SNSアプリケーションのブロック
      - ファイル共有アプリケーションのブロック
  - ②業務の生産性向上
    - 業務に必要のない通信をブロック
      - SNSやオンラインゲームのブロック
      - 動画通信をブロック

 |

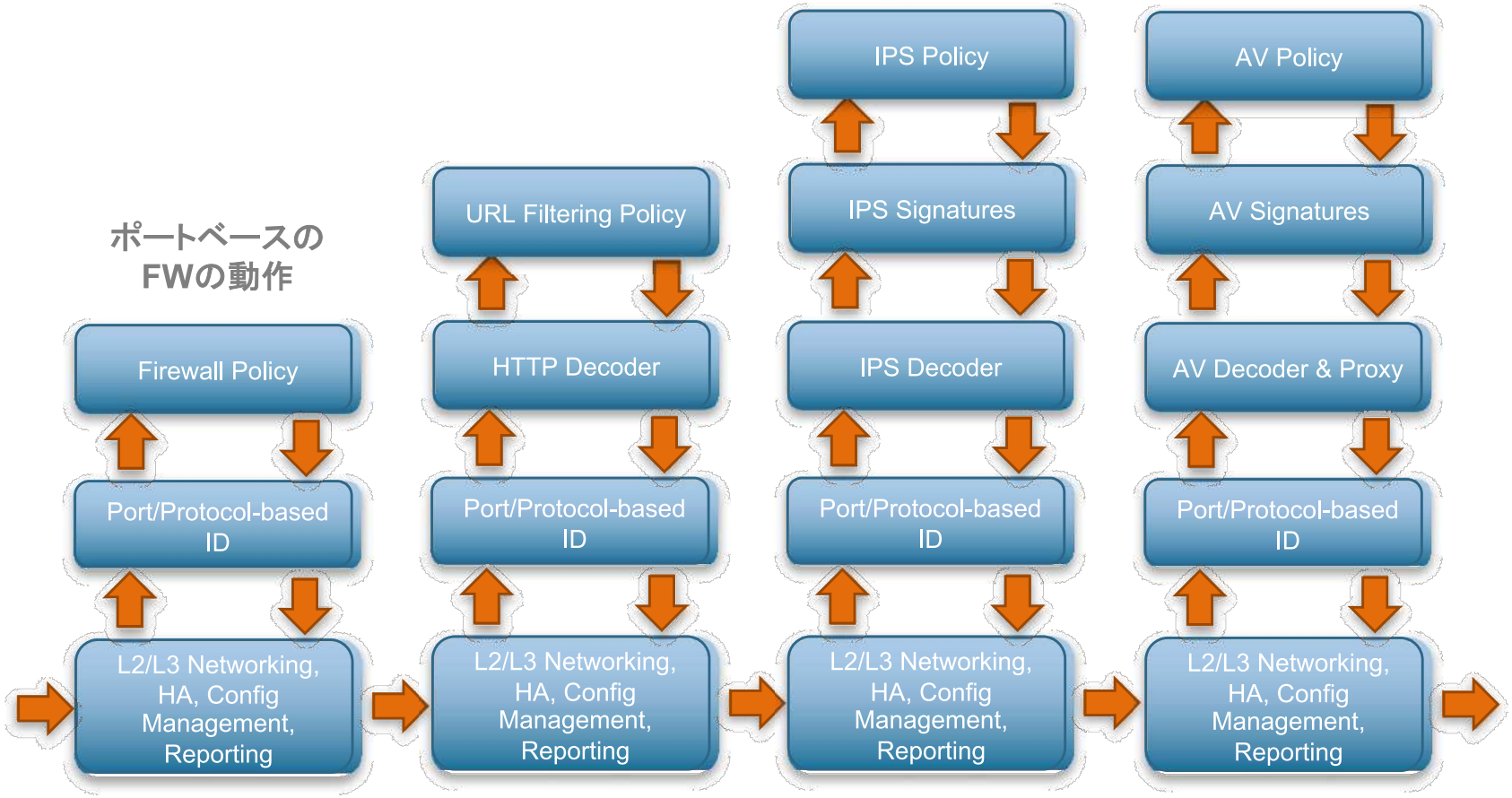
次世代FWの成り立ち

ポートベースのファイアウォールから失われた
“アクセス制御”機能を取り戻す！

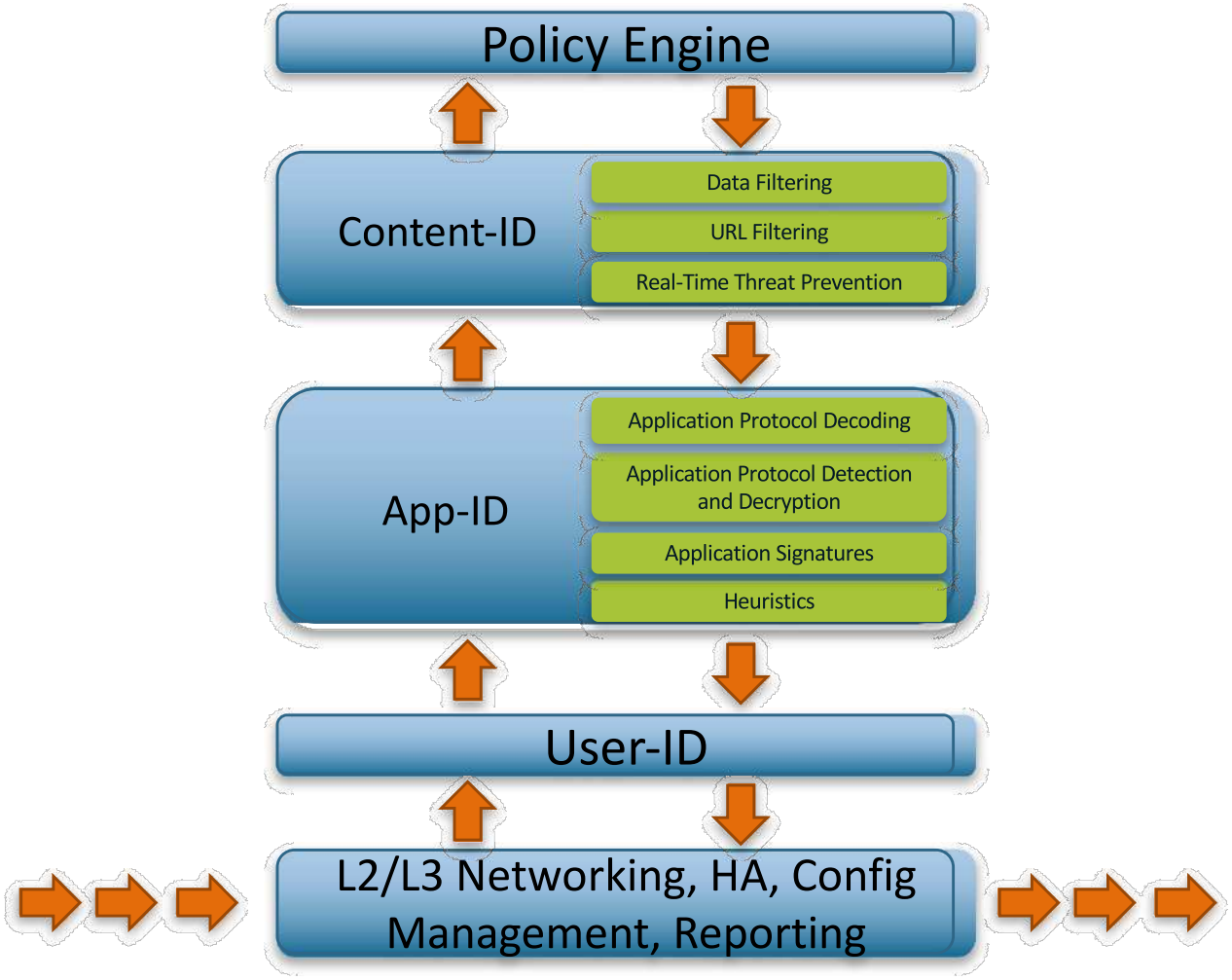
 |

従来のファイアウォール/UTM製品のアーキテクチャ

⇒ アーキテクチャの特徴からパフォーマンスレベルが低い



当社Single-Pass Parallel Processing (SP3):
高速処理を実現した先進のアーキテクチャ ⇒ パフォーマンスレベルが高い



ゼロトラストに基づくセキュリティー対策が必要

ゼロ・トラスト・ネットワーク・セキュリティーとは？

Forrester ResearchのアナリストJohn Kindervag氏が提唱したもので、

「既存のトラストモデルは破綻しており、“検証して信頼しない”という概念に変え、ユーザー、パケット、インターフェース、ネットワークなどに対して常に疑いをもって接すること」という性悪説に基づく概念。 ***Trust is a Vulnerability 信頼こそ脆弱性***

悪意のある者の行動だけではなく、善意の行動がセキュリティーリスクを増幅させる時代、
特にパブリッククラウドにおいてその傾向が顕著になってきている

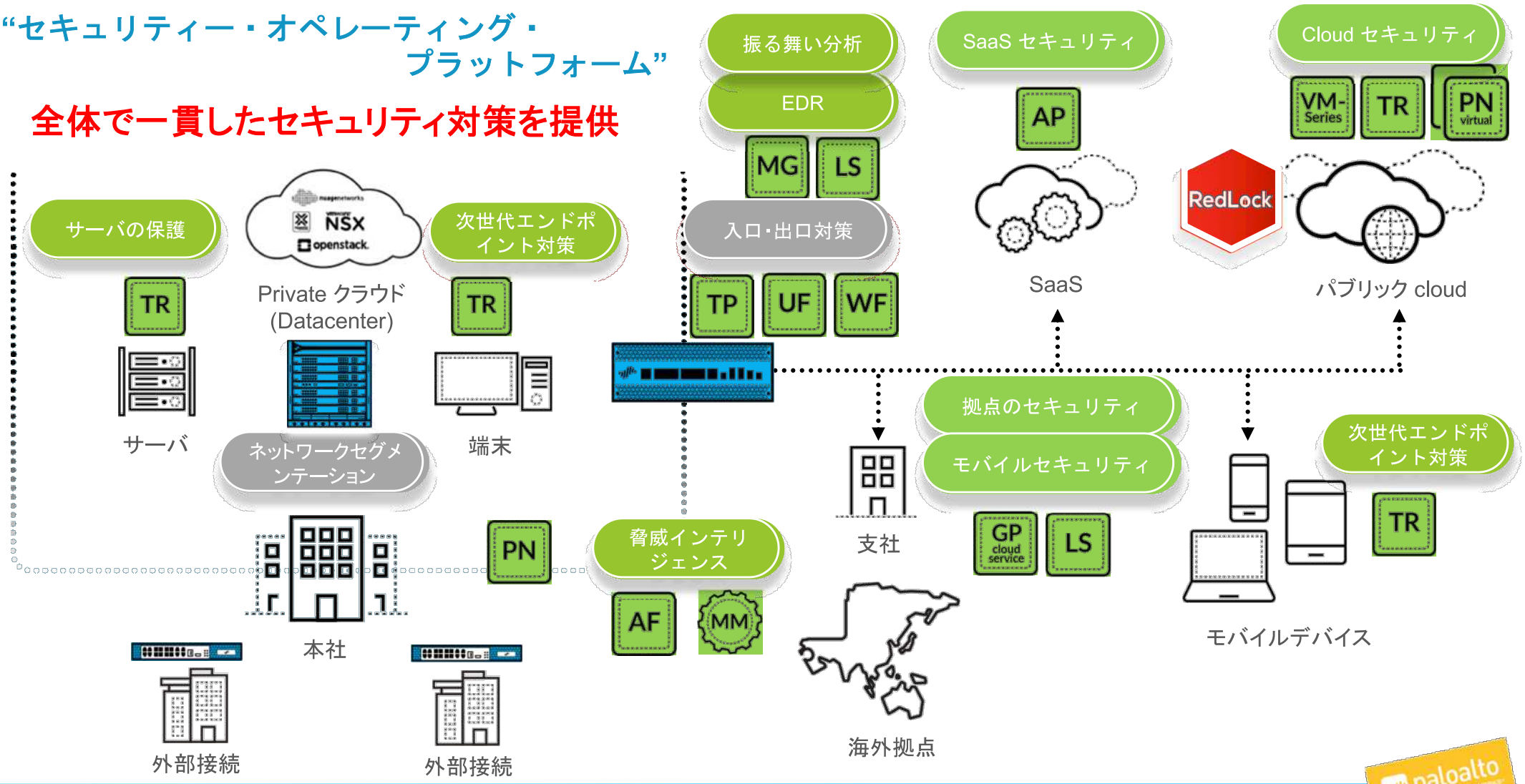
クラウドインシデントの特徴

“2022年までに起こるクラウドでのセキュリティ事故の95%はユーザー起因によるもの”
- GARTNER

パロアルトネットワークスが提供するプラットフォーム

“セキュリティー・オペレーティング・プラットフォーム”

全体で一貫したセキュリティ対策を提供



 |

次世代Firewall（物理、仮想環境）

アプリケーションを安全に使用できるようにし、高度な最新の脅威を阻止します。物理、仮想環境の環境に統一のセキュリティポリシーを適用可能で、入口・出口対策に最適です。

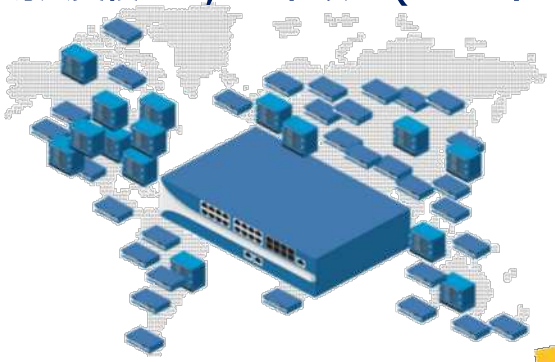
特徴：

- ポート番号やプロトコル・暗号化に関わらず、全てのトラフィックをアプリケーションとして識別
- 全ての通信を利用ユーザ毎に識別し、仕事の役割に合わせて通信をコントロール
- 脆弱性、既知のマルウェア、悪意のあるDNS、C&C通信を検知・遮断
- URLフィルタリング機能で悪意のあるサイト、C&Cサイトへの接続を検知・遮断
- 世界中で検出された未知の脅威をWildFire シグネチャ(5分間隔)を利用して遮断

物理Firewall :
PA220～PA7000シリーズは、100MB～200Gbpsの帯域に対応

仮想Firewall:
Private Cloud – Vmware Esxi, NSX, KVM, Hyper-V,
Public Cloud – AWZ, Azure, Google Cloud

導入実績: 56,500社以上 (2018年10月時点)



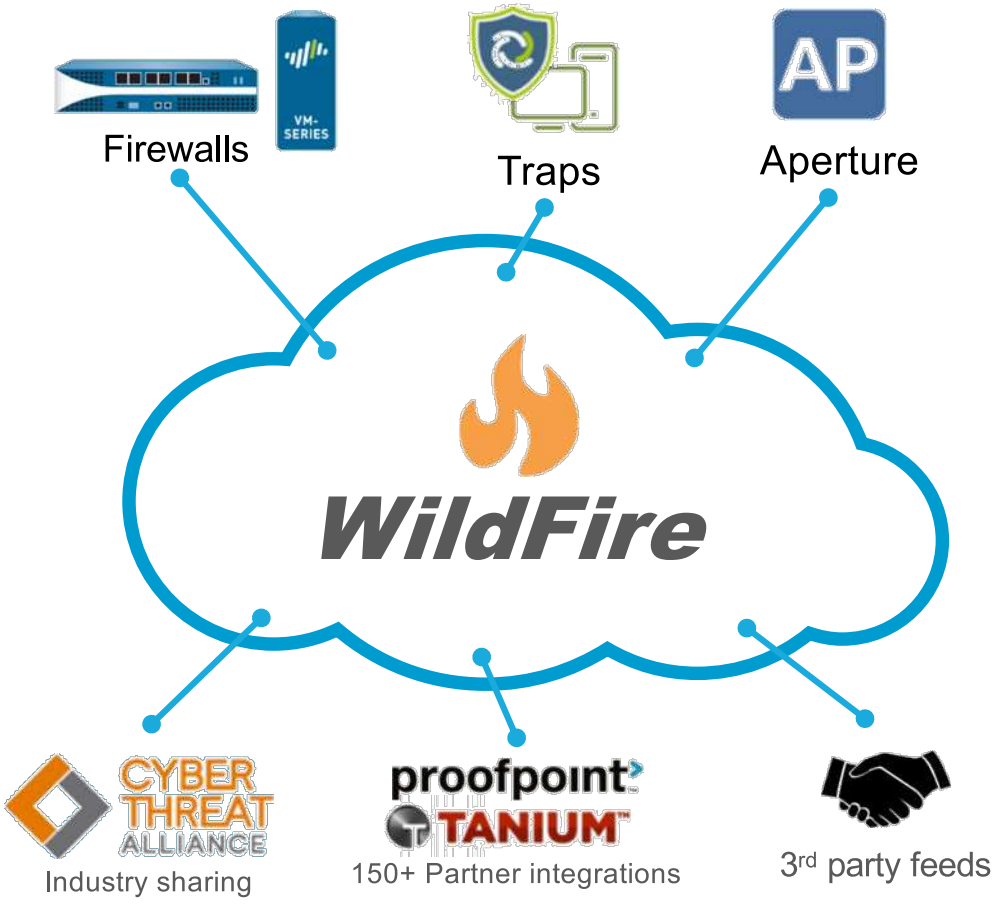
WildFire　クラウド脅威インテリジェンス解析サービス

300M+
ユニークな分析サンプル/毎月

60-70%
Top アンチウィルベンダーの未対応の割合

>26,500
WildFire利用のお客様数

300K+
1日に5分毎に配信するアンチウィルス、アンチスパイウェアのシグネチャ数



 |

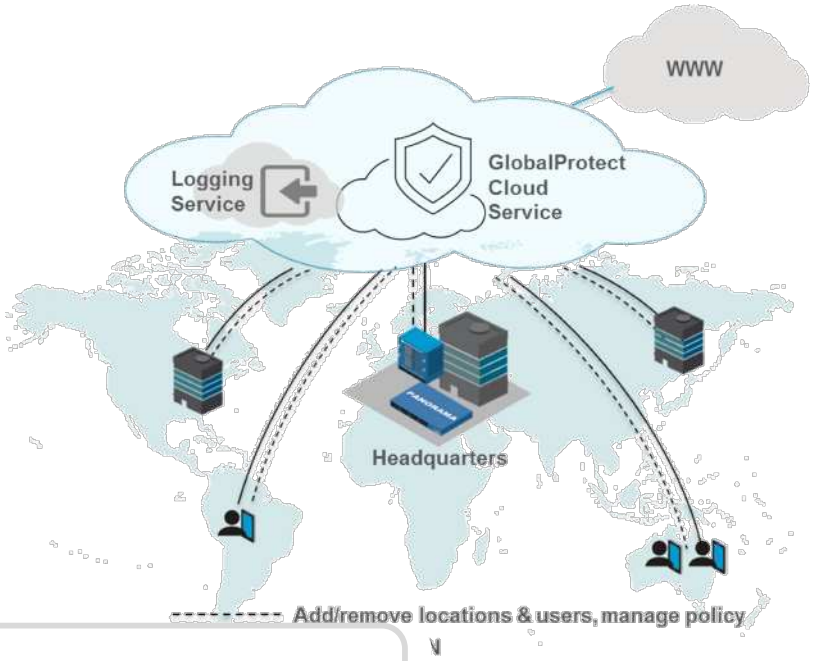
Global Protect Cloud Service　拠点/モバイル対応次世代セキュリティー

リモート拠点やモバイルユーザに向けに次世代Firewallを使用した入口・出口対策をクラウドセキュリティサービスとして提供します。初期費用、メンテナンス不要で、サービスとして次世代Firewallを利用可能です。

特徴:

- 高度化する脅威に対して入口・出口対策の多層防御を提供
- 本社と拠点、モバイルユーザーに一貫したセキュリティを適用
- 常に最新のセキュリティが適用され、メンテナンス作業不要(*1)
- 柔軟に帯域、ユーザ数を拡張可能のため、共通ゲートに最適

*1 PAN-OS アップデート、Signature 適用



システム要件:

- Global Protect Cloud service ライセンス
- Logging Service ライセンス
- Panorama 8.0.6 以上

ライセンス体系:

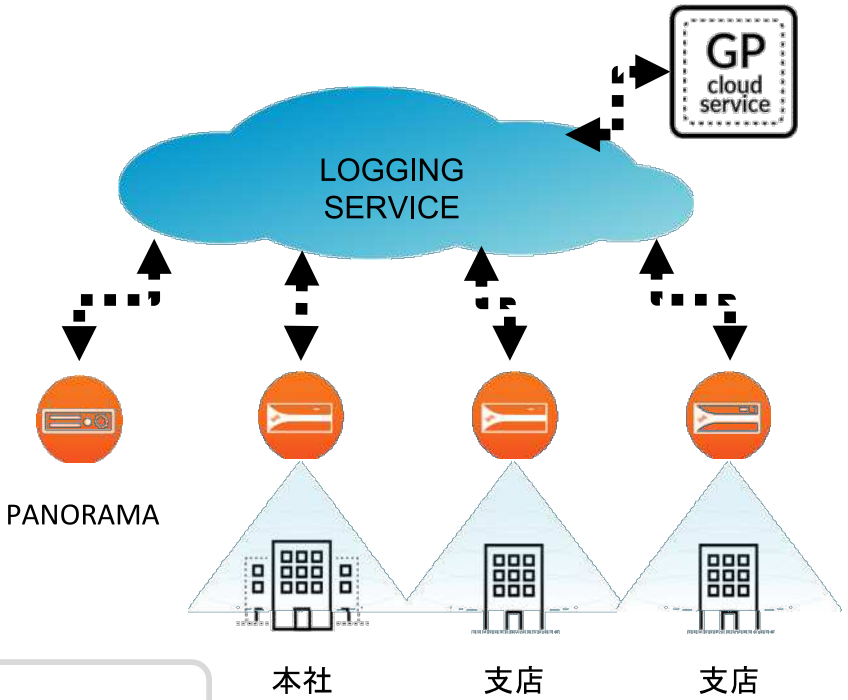
拠点　- 帯域に応じた契約
モバイルユーザー 数に応じた契約

Logging Service　ネットワークセキュリティーログ収集・保存

Logging Service は、次世代Firewallおよび、Global Protect cloud service から出力されるログデータを収集して保存するサービスです。

特徴:

- ライセンス契約後、簡単に展開可能
- アップグレードやメンテナンス不要
- ログの冗長性、拡張性を確保
- SOC2 Type 2の認証済み
- アプリケーションフレームワークでの活用が可能



システム要件:

- Logging Service
- Panorama 8.0.6 以上
- PAN-OS 8.0.6 以上

ライセンス体系:

- Logging Service 2TB単位
- Panorama ライセンス

Magnifire (Agentless EDR)　ネットワーク挙動分析クラウドサービス

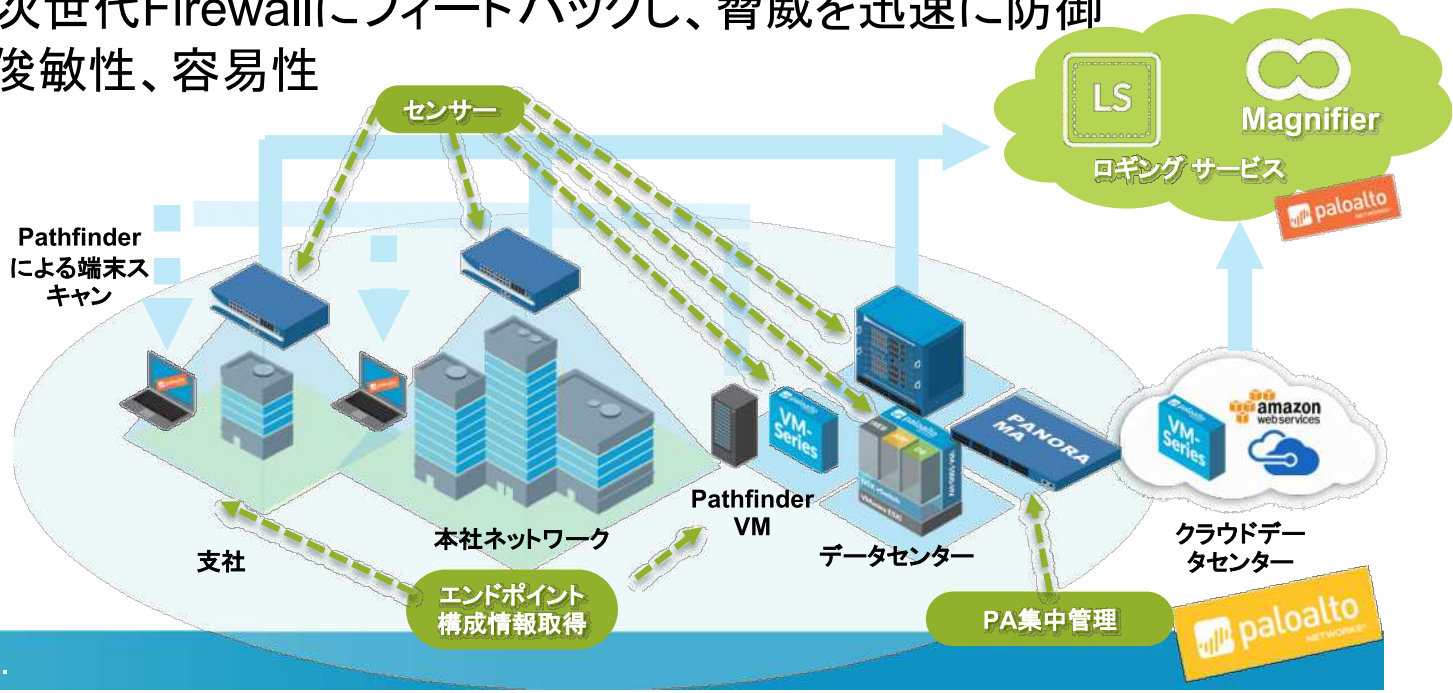
各種センサーから収集したトラフィックログを機械学習で分析し、標的型攻撃や悪意のある内部犯行などのエンドポイントに侵入した攻撃の挙動を自動検出します。検出後には、次世代Firewallが脅威を阻止することで、迅速な防御を提供

特徴:

- 検出の自動化 - 次世代Firewall から収集する豊富なデータを蓄積し、攻撃の挙動を検出
- 調査 - エンドポイント解析サービス「Pathfinder」から端末の情報を自動収集
- レスポンス - 検出された脅威を次世代Firewallにフィードバックし、脅威を迅速に防御
- クラウド利用 - 導入の拡張性、俊敏性、容易性

Magnifier の要件:

- Logging Service
- Panorama 8.0.6 以上
- PAN-OS 8.0.6 以上



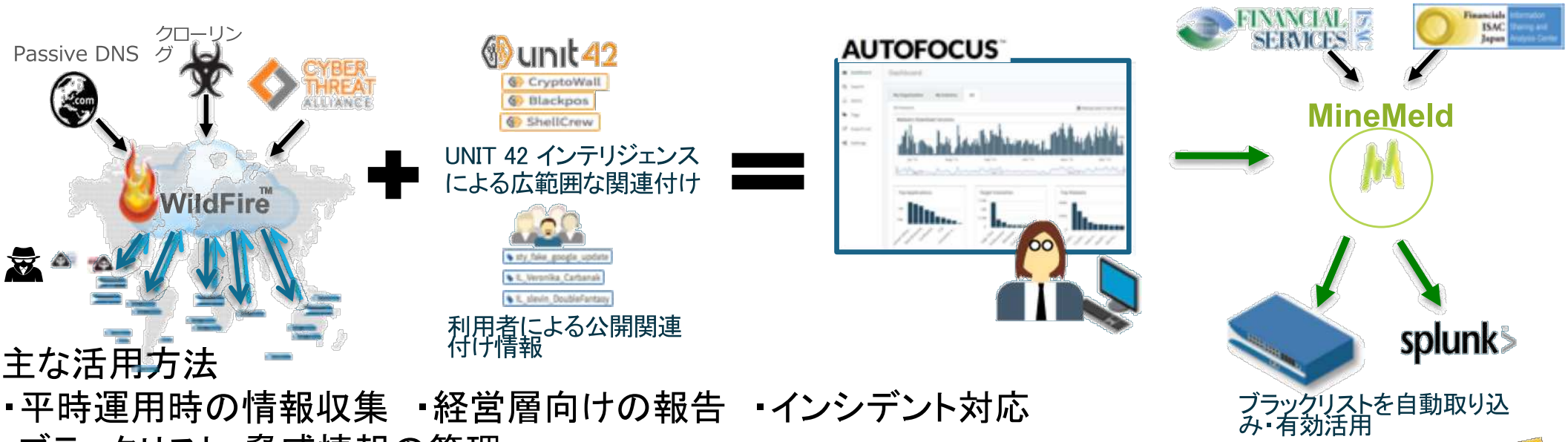
 |

Autofocus 脅威インテリジェント自動化サービス

脅威情報データベース。未知の脅威情報は自動的にネットワークのイベントとタグ付けされ、自社、同じ業界の脅威情報の可視化、インシデント対応の迅速化に貢献します。

特徴:

- 最新の脅威・業界別の動向をリアルタイムに把握、脅威の優先順位付けが可能
- セキュリティの外部委託ベンダーの可視化、自社のインシデント対応に活用
- 外部の脅威情報を取り込みブラックリストツール(Minemeld) として管理可能



主な活用方法

・平時運用時の情報収集　・経営層向けの報告　・インシデント対応

・ブラックリスト・脅威情報の管理

 |

Traps (SECDO社の買収により、スレッドレベルのアクティビティログ収集機能EDRを統合)

次世代エンドポイント製品。WildFire と連携し、端末で未知の脅威、脆弱性攻撃を遮断します。
管理コンソールをクラウドサービスとして提供することで、導入が容易です。
Trapsは3つの強みを持ち、エンドポイント対策を強化します。

既知と未知のマルウェアを多層防御

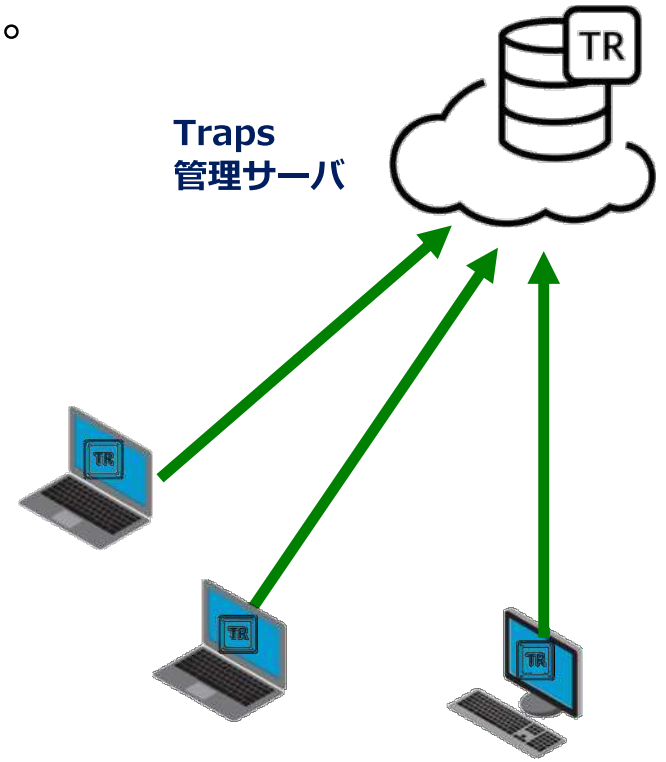
WildFireと連携し、解析済みのマルウェアの起動を確実に抑え、未知のファイルは、機械学習エンジン(AI)により静的解析し、起動を阻止。さらに、WildFire にてマルウェアを分析し、脅威を判定します。

マルウェア情報をスピーディーに共有、対応

次世代ファイアウォールやTrapsから送られた未知のファイルをすばやく分析。世界中のお客様と共有することで、数分前に発見されたマルウェアの起動をTrapsで確実阻止することができます。

ゼロデイ脆弱性への対応ができる

脆弱性を悪用するための手法を阻止することで、ゼロデイ脆弱性や、パッチが適用されていない脆弱性を突く攻撃を阻止。脆弱性攻撃からのマルウェア侵入を防ぎます。



 |

Agenda

Ⅰ 会社最新状況アップデート

Ⅱ 金融業界における動向

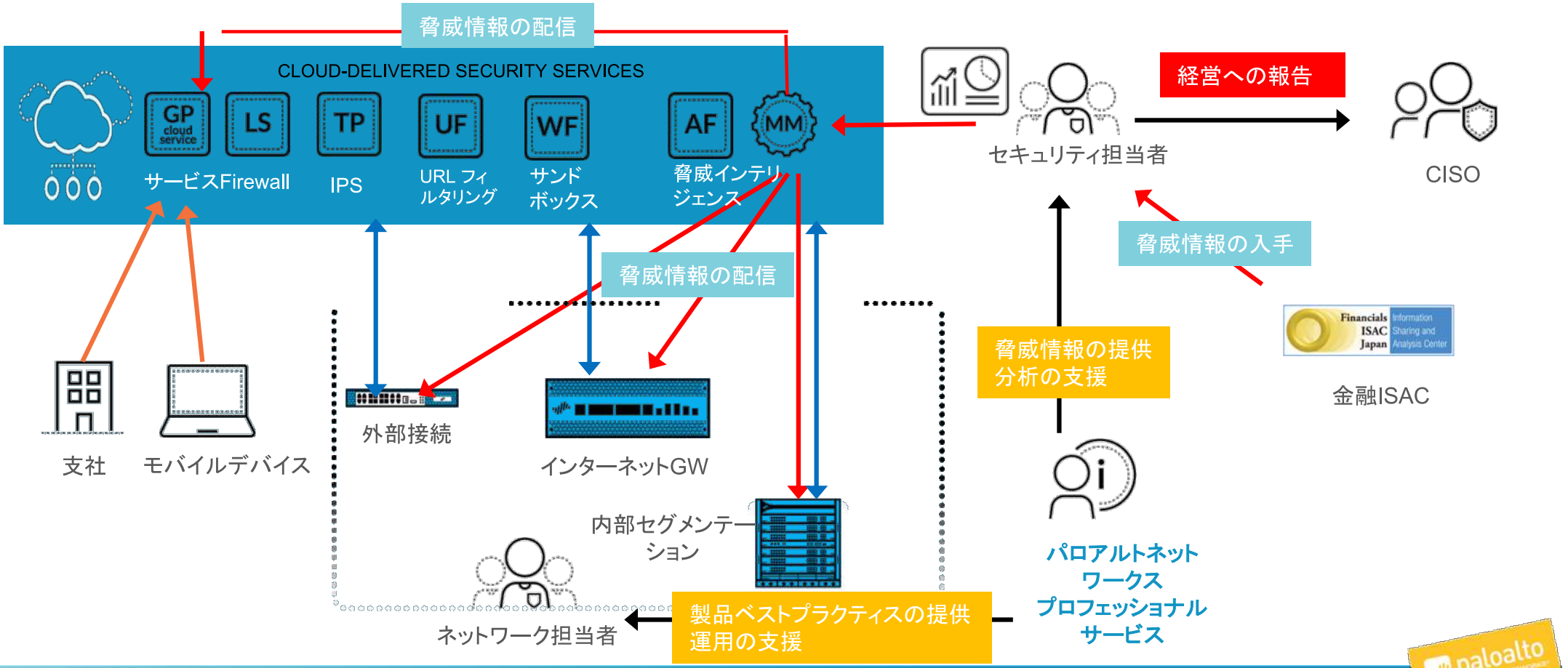
Ⅲ パロアルトネットワークスが提供するセキュリティソリューション

Ⅳ 金融機関様の導入事例

Ⅳ 金融機関様の導入事例

脅威インテリジェンスを活用した入口・出口対策

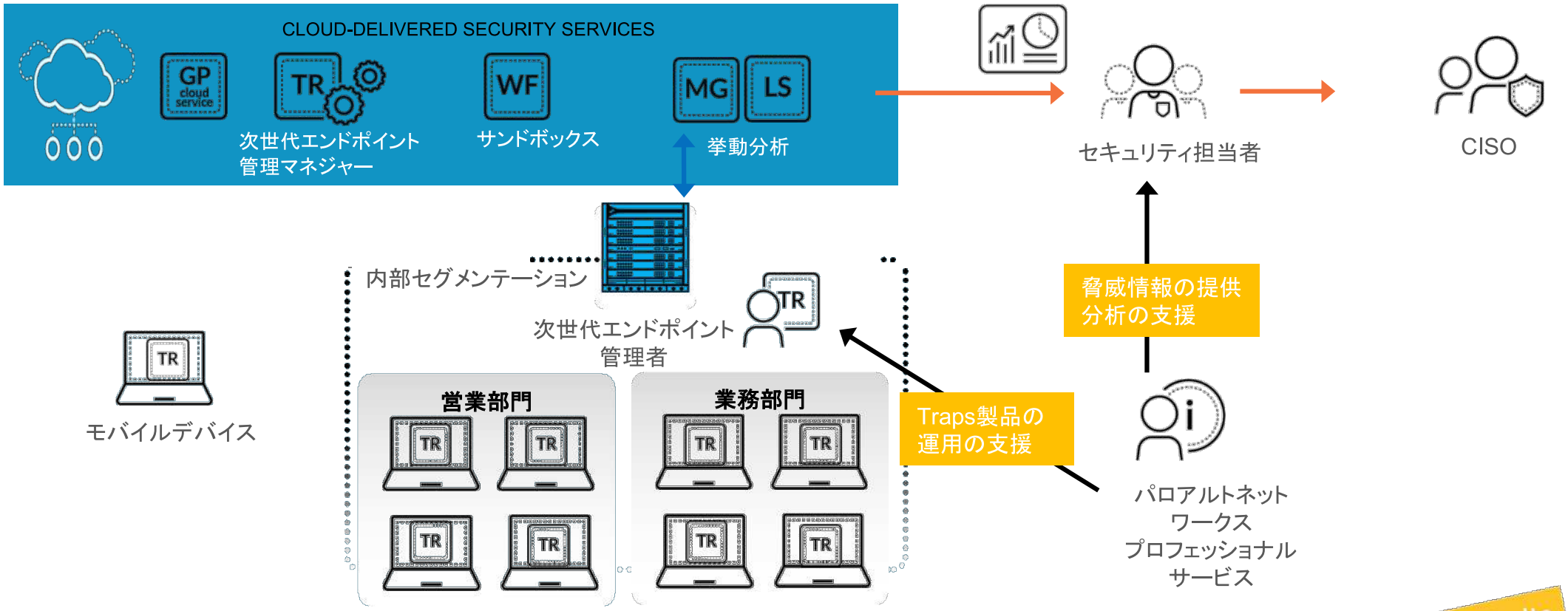
本社、支社、モバイルデバイスのすべての環境において、脅威インテリジェンス、製品のベストプラクティスを活用したシンプルなセキュリティ対策を実現



 |

内部対策

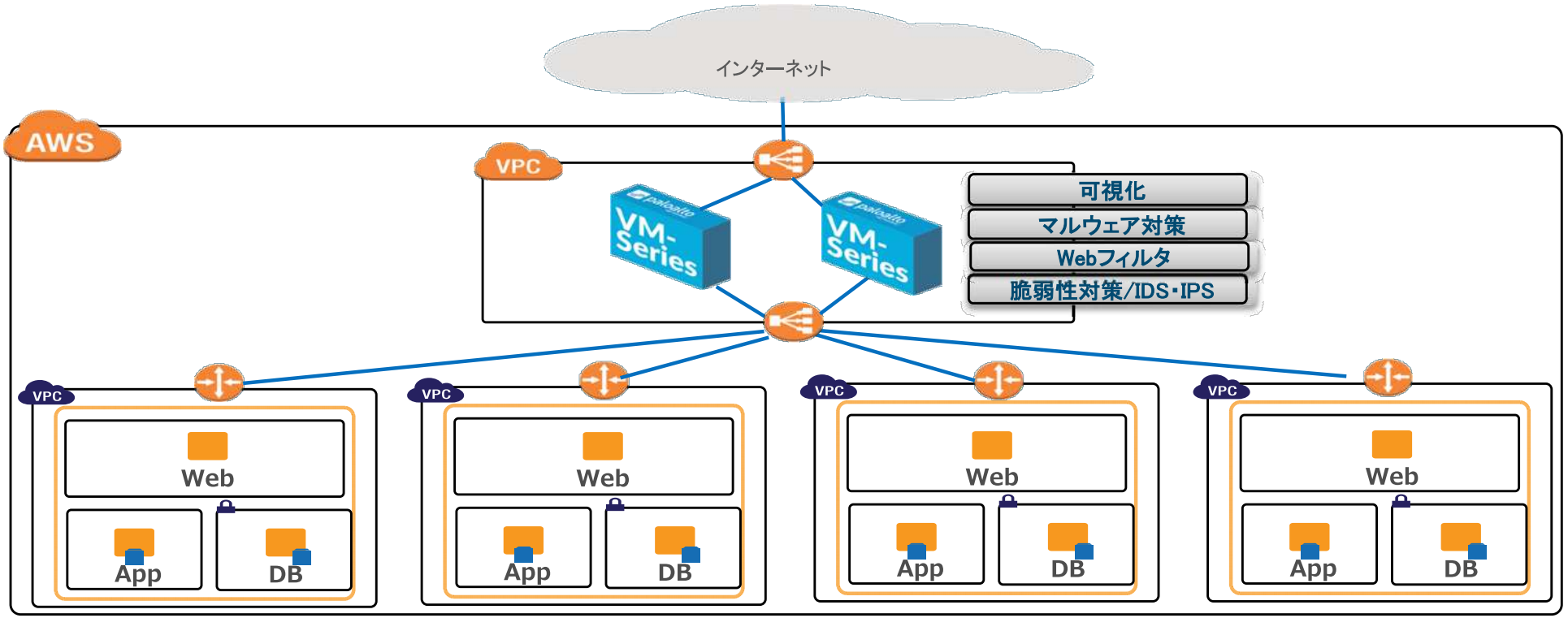
お客様の課題に合わせて、エンドポイント対策、内部セグメンテーション、挙動分析をクラウドーサービスと連携して個々に提供



 |

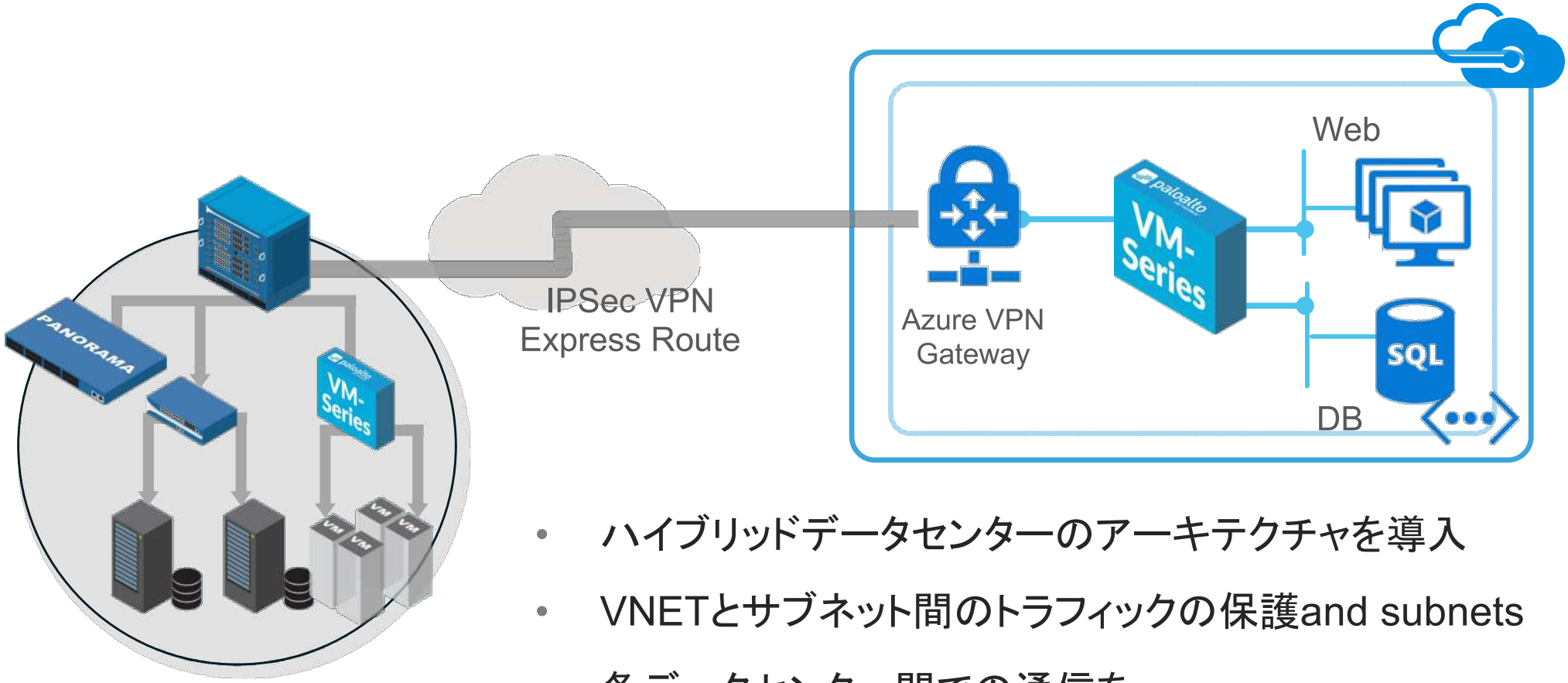
<事例1> Public Cloud セキュリティ対策

パブリッククラウドの入口・出口対策。物理環境と同様のコンセプトで、共通ゲートを構築し、ハブアンドスポークモデルで複数のVPCに対してセキュリティを提供



 |

〈事例2〉 Azure 環境でのハイブリッドデータセンター

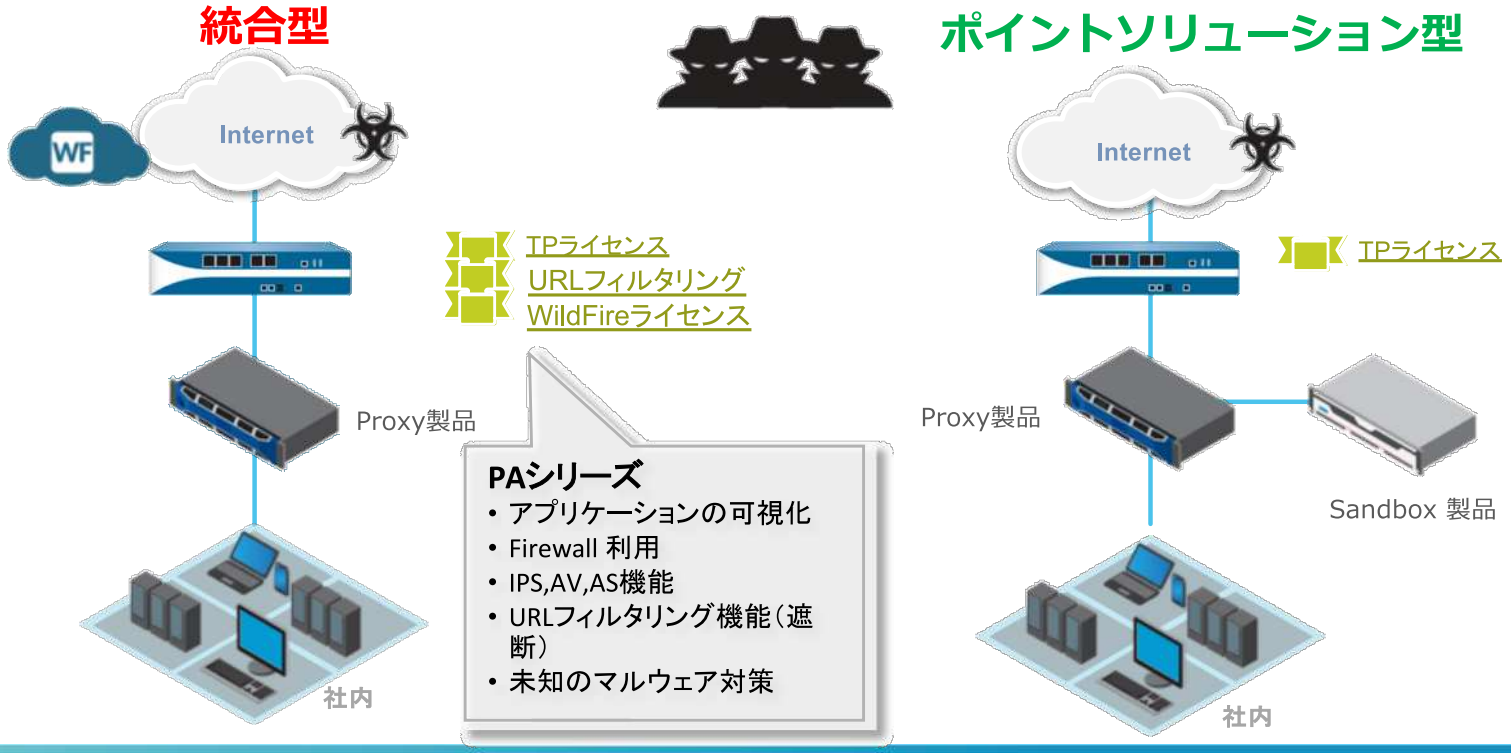


- ハイブリッドデータセンターのアーキテクチャを導入
- VNETとサブネット間のトラフィックの保護and subnets
- 各データセンター間での通信を
  アプリケーションレベルで可視化・コントロール
- 横へ展開する脅威を防御

<事例3> 国内金融機関 入口・出口対策の強化

インターネットゲートウェイ製品として利用。
お客様の環境により以下の2つの利用形態が存在。最近は統合型の利用形態が圧倒的多数。

- 統合型 (Firewall、IPS、URLフィルタリング、サンドボックス)
- 機能毎にベンダーを分けるポイントソリューション型



 |

<事例4> 脅威インテリジェンスの活用

脅威インテリジェンスを活用した**CSIRT運用**。AVベンダーに依存すること無く、最新の脅威の把握、分析が可能。パロアルトネットワークスが脅威の遮断について適宜アドバイスし、最新の脅威に対する防御設定を最新の状態に保ち、**脅威を大幅に削減**。

AUTOFOCUS™ & Palo Alto Networks プロフェッショナルサービス

① お客様宛に届いた未知、既知のマルウェア分析結果と影響範囲について実用的な情報を提供

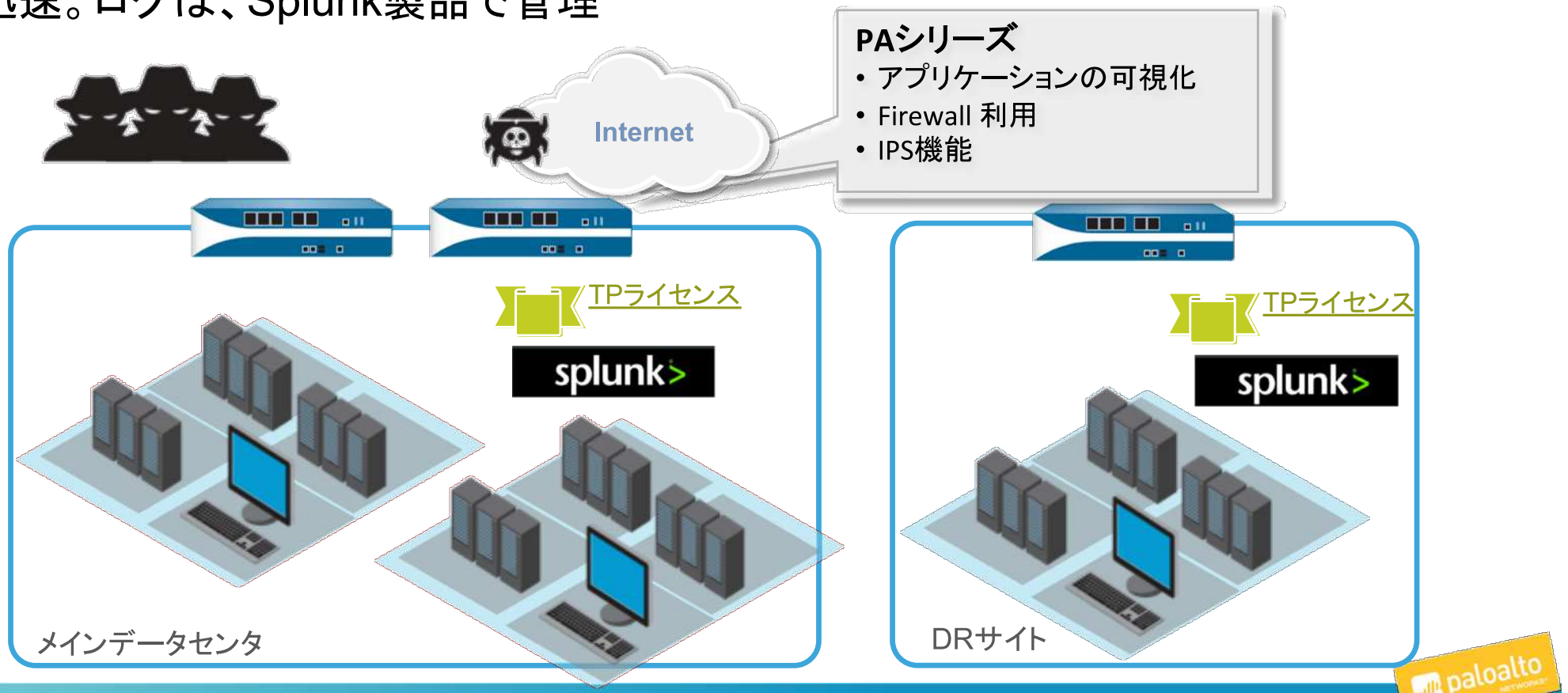
② WildFireのデータを基に、経営陣を意識したグローバル、国内、金融業界の脅威トレンド情報を提供

③ 最新の脅威情報から未知・既知の脅威を遮断するためのに必要な対策について助言

 |

<事例5> データセンター入口対策

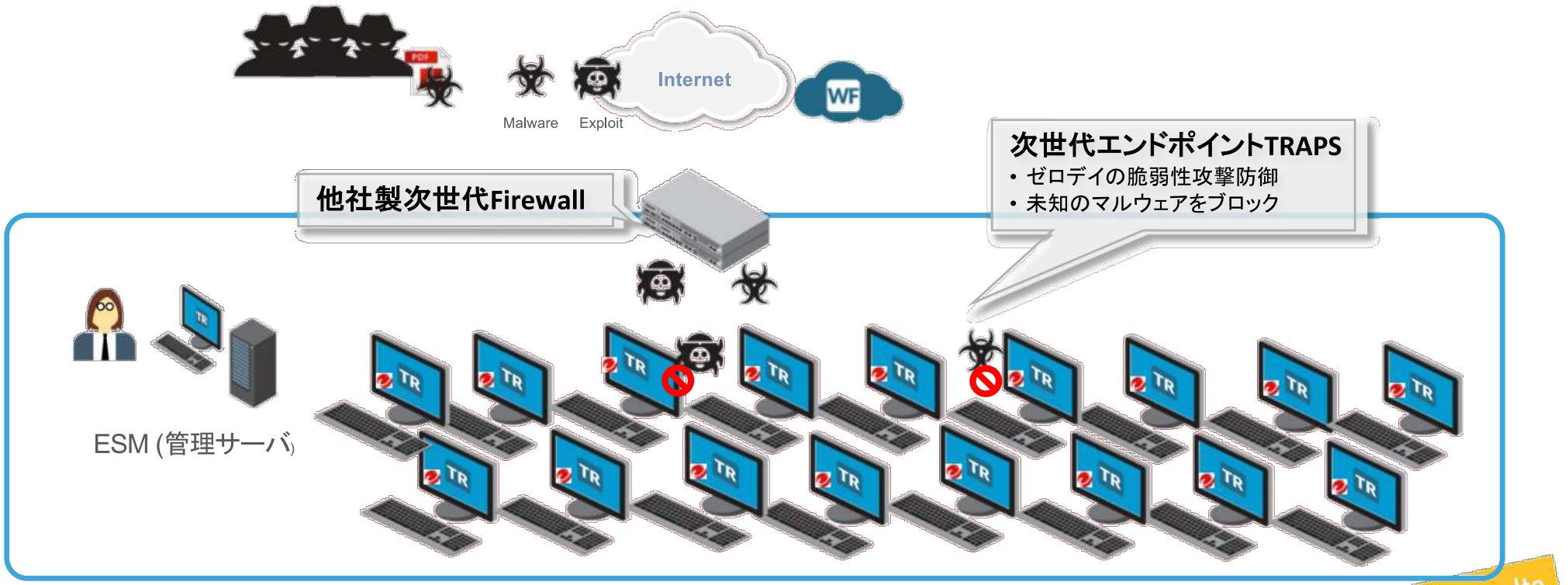
FW、IPSと別々に導入していた環境を、1台に**統合**し、**コスト削減を実現**。
Unit42による未知の脆弱性の発見、他社(IPSベンダー)と比較してもシグネチャのリリースが迅速。ログは、Splunk製品で管理



 |

<事例6> エンドポイントの対策

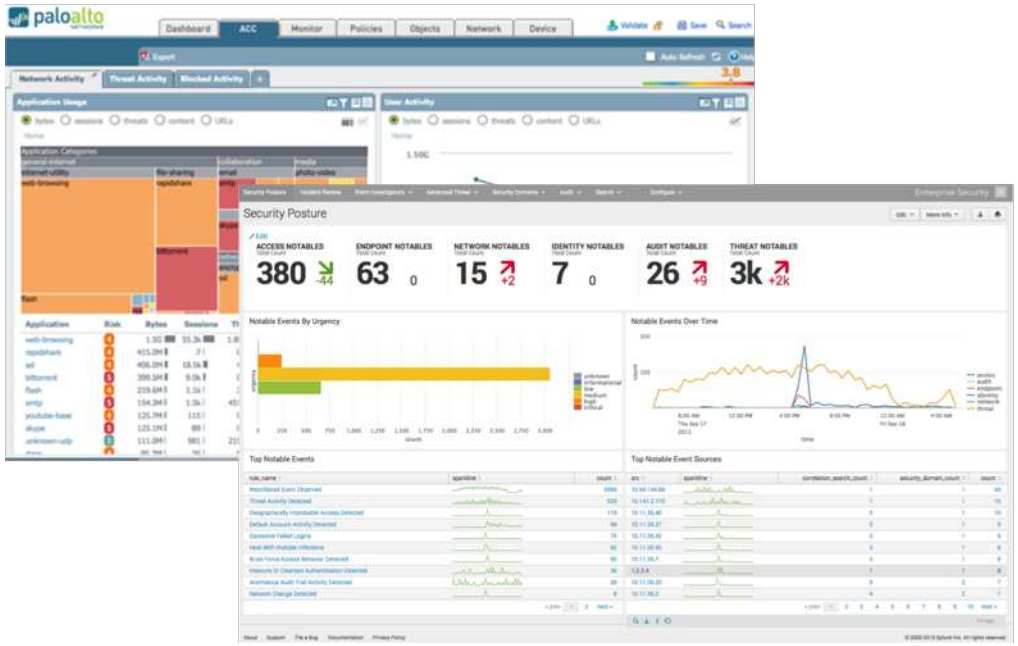
未知の脅威対策（エクスプロイト検知・防御、マルウェア検知防御）として、
Traps 製品を導入。導入から数ヶ月で既存のAV製品をすり抜けるマルウェアを多数検知。
お客様は、**AV製品の効果が低い**ことを再認識。



 |

〈事例7〉 ログ管理基盤 SIEM連携

Firewall が出力するログを Splunk に取り込み、相関分析を実施可能。
Palo Alto Networks App for Splunk により**デバイス上と同様の可視化を実現**



Palo Alto Networks App for Splunk
https://splunkbase.splunk.com/app/491/

 |

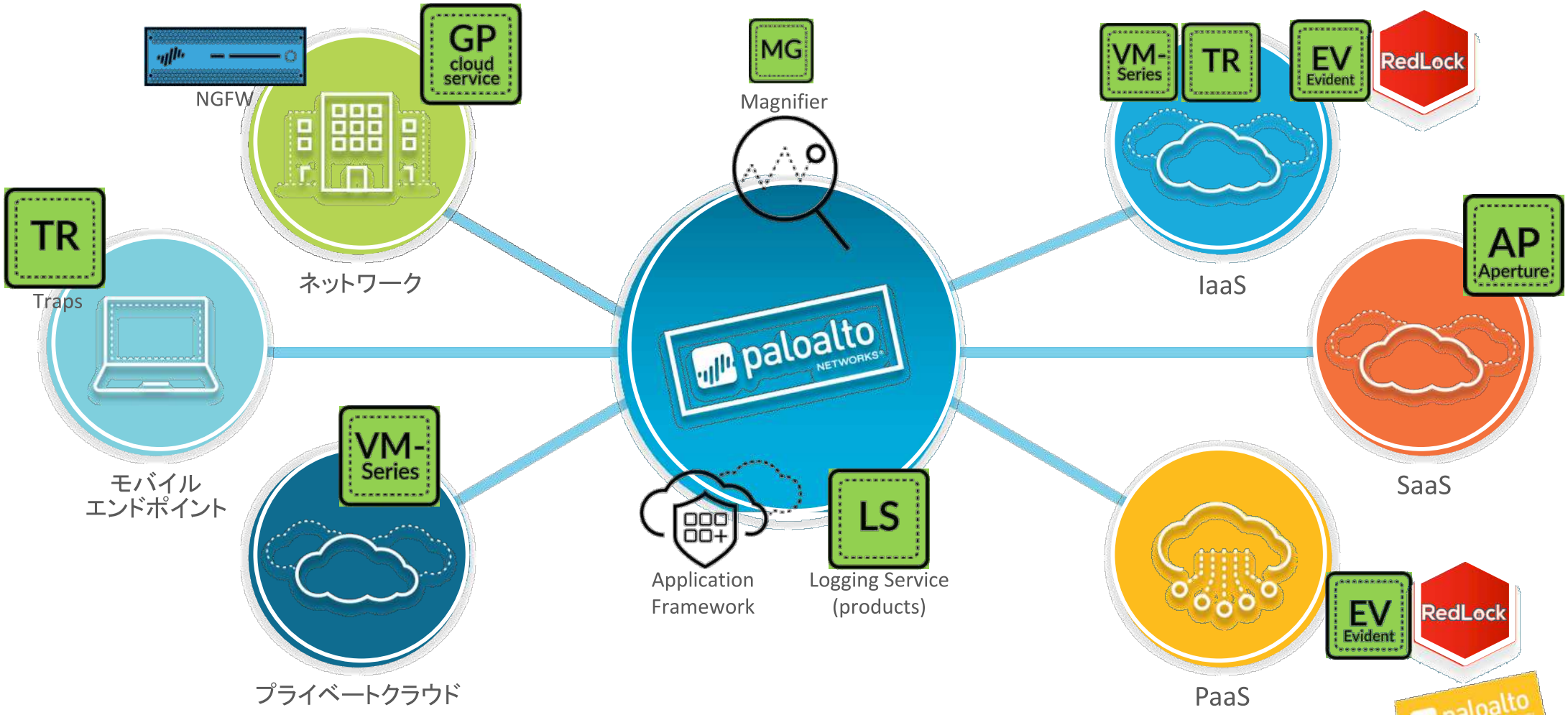
セキュリティ戦略のためのコンパス

完全な可視化
可視化は必須

素早い脅威対応
リアルタイム解析
アクション自動化

一貫した
セキュリティ
セキュリティシステムの
基盤化

“セキュリティー・オペレーティング・プラットフォーム”が
どこでも一貫したセキュリティを提供し，データを守ります



THANK YOU

Email: ynakamichi@paloaltonetworks.com