最新セキュリティ動向とランサムウェア対策

March2016

paloalto NETWORKS®

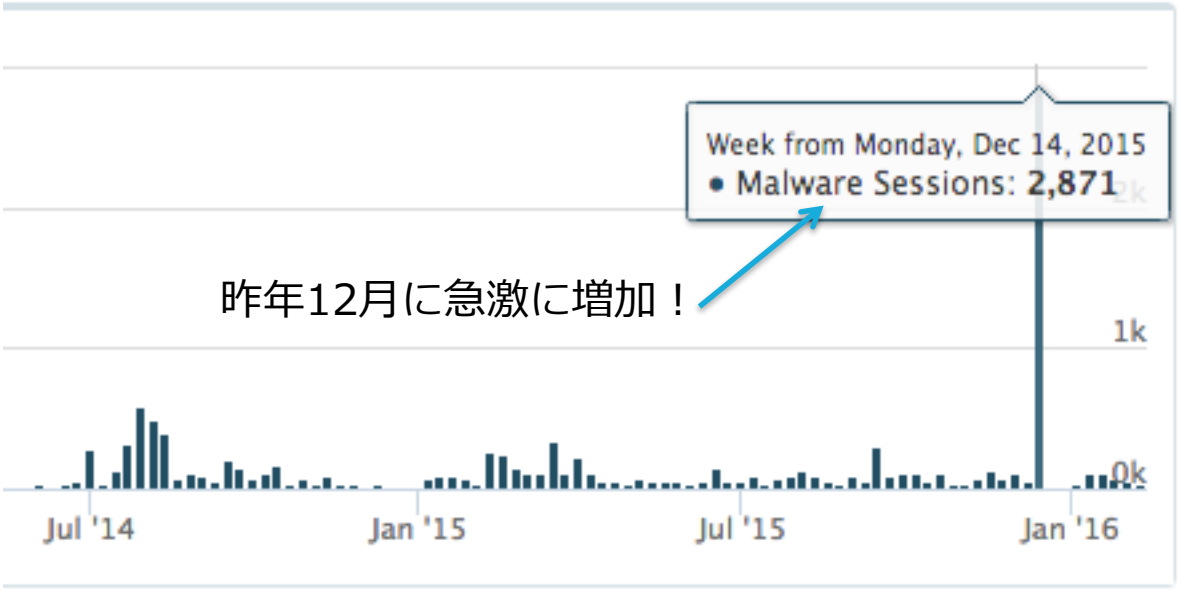
日本で拡散！ランサムウェアとは？

“実行されると端末内部や、
ネットワークドライブ上の
ファイルを暗号化
暗号化解除の為に金銭を要求する
身代金要求型ウィルス“

日本国内で作成されたランサムウェア

 © 2015, Palo Alto Networks. Confidential and Proprietary.

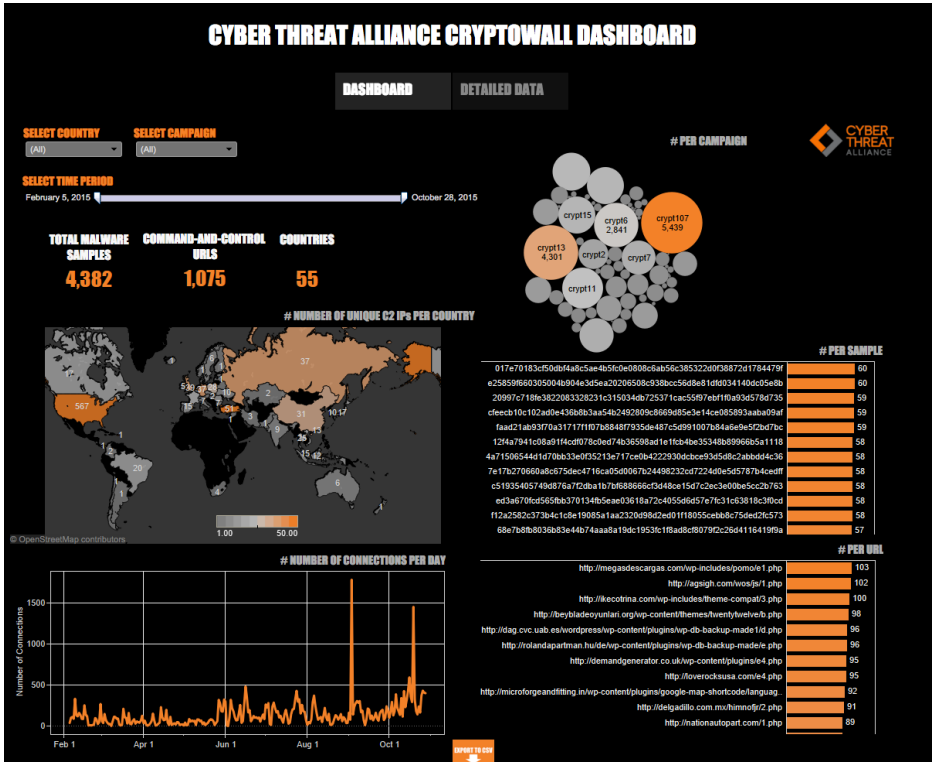
昨年末に日本国内に大量に出回っていたランサムウェア



日本国内のWildFire(サンドボックス)で検知したランサムウェア
実被害はそれ以上

 © 2015, Palo Alto Networks. Confidential and Proprietary.

CYBER THREAT ALLIANCE



CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

$325M in estimated damages across the globe

839 command and control URLs

5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples

 © 2015, Palo Alto Networks. Confidential and Proprietary.

paloalto NETWORKS

拡大してゆくランサムウェア

CRYPTOWALL RANSOMWARE COST USERS $325 MILLION IN 2015

by NewsEditor_ on November 2nd, 2015 in Industry and Security News.

Ransomw hospital offline, $3 by attackers

$17,000

CryptoDefense

CryptoWall

CryptoLocker

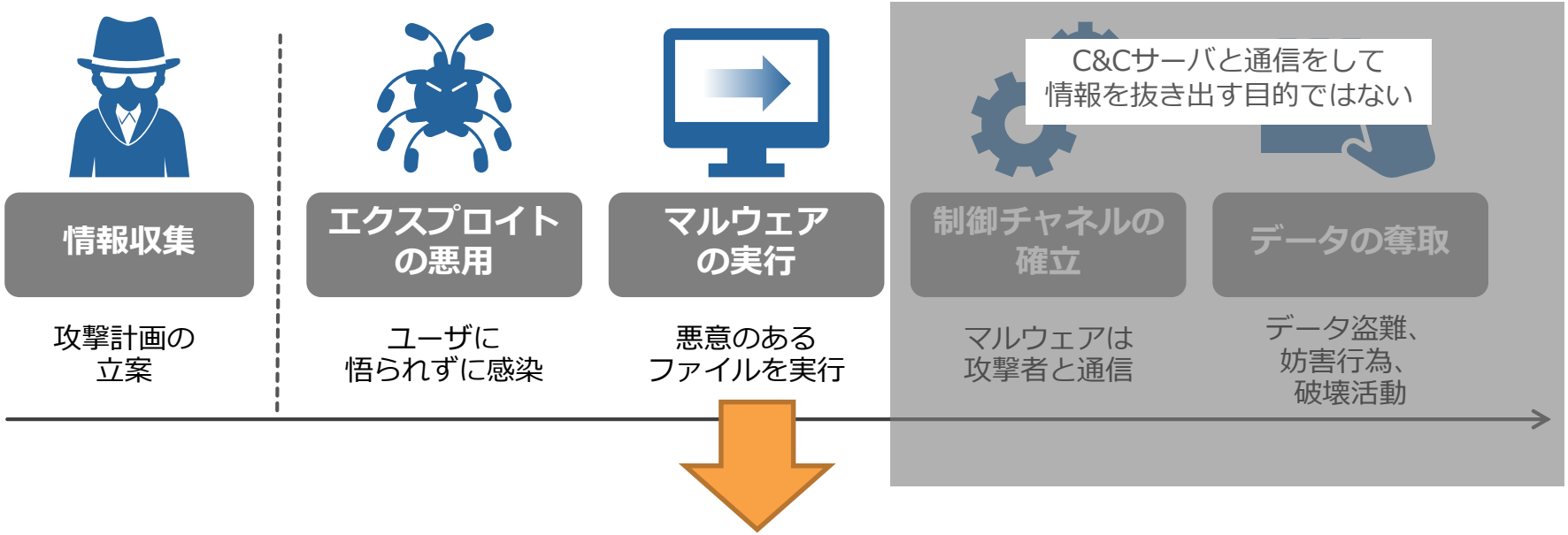
CryptoFF

CryptoJoker

> 20 Families

 © 2015, Palo Alto Networks. Confidential and Proprietary.

ランサムウェアは従来のサイバー攻撃の推移と大きな違いが



ランサムウェア対策に必要なのはファイルの取得の防止とファイル実行の防止

 © 2015, Palo Alto Networks. Confidential and Proprietary.

ランサムウェアの脅威とは・・・

実行したら即

OUT!!!!

大切な業務データが暗号化されてしまいます。

 © 2015, Palo Alto Networks. Confidential and Proprietary.

ランサムウェア対策には・・

 © 2015, Palo Alto Networks. Confidential and Proprietary.

点での防御ではなく、多層防御を使って守る必要があります！

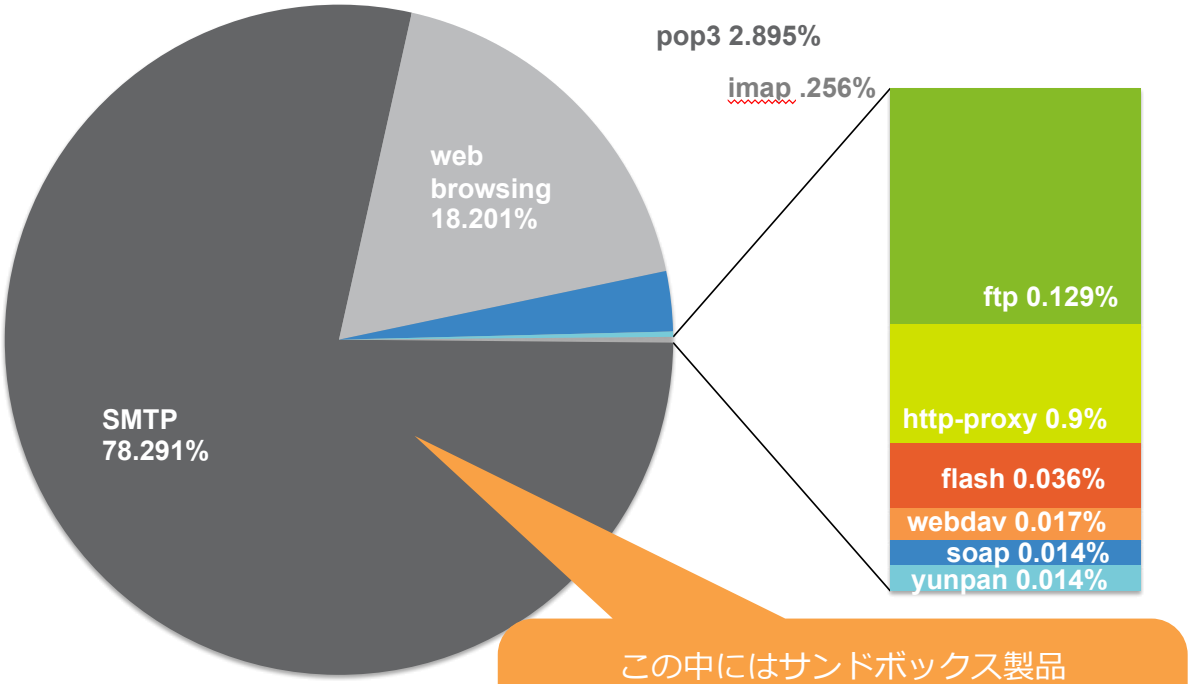
例えば物理的には多層防御を使って外的からの侵入を防ごうとするのは普通の事

・日本の城
　外堀、内堀など本丸への侵入を防ぐための施策

・データセンターへの入館
　入館申請から始まり、サーバ室入室のカードキーラックの施錠など

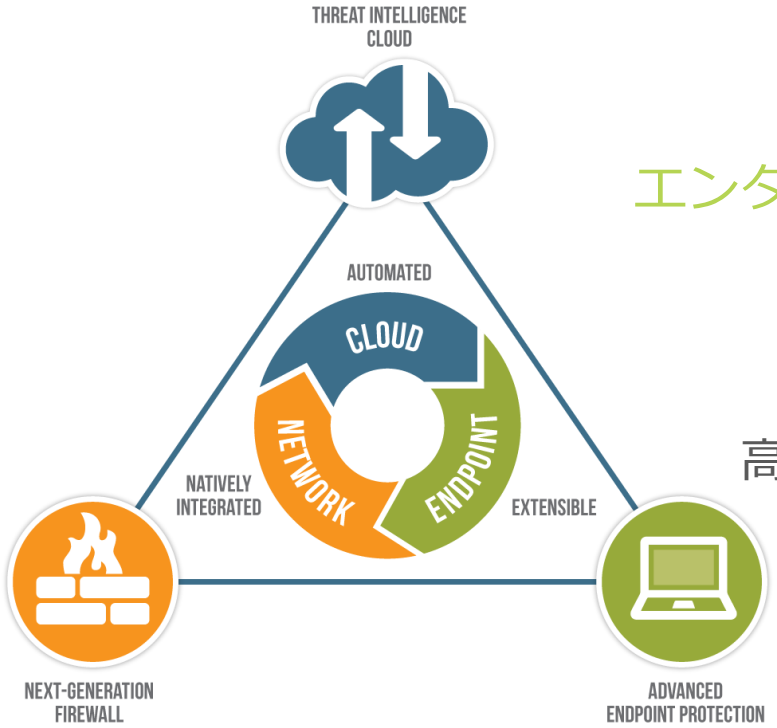
 © 2015, Palo Alto Networks. Confidential and Proprietary.

主なマルウェアの感染経路



この中にはサンドボックス製品
で検出できない、SSL通信や
パスワード付きZIPファイルなど
も含まれる

 © 2015, Palo Alto Networks. Confidential and Proprietary.



パロアルトネットワークスの提供する

エンタープライズセキュリティプラットフォームは

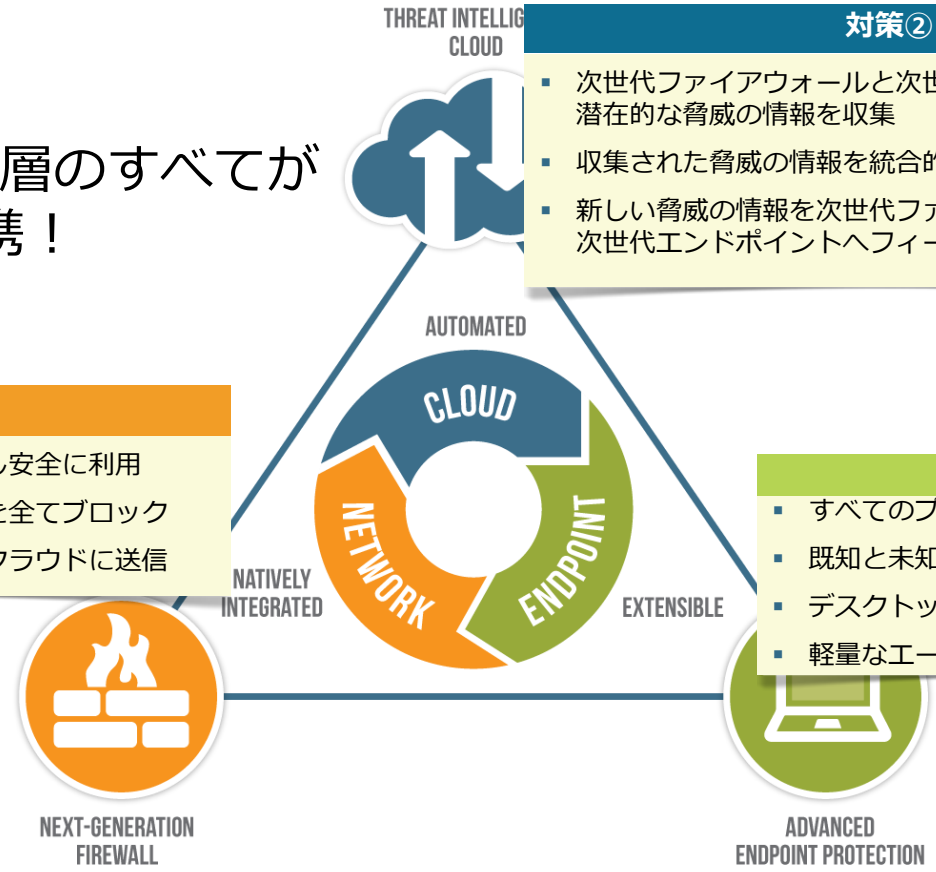
多層防御を提供

高度化するマルウェアの感染被害から守ります

 © 2015, Palo Alto Networks. Confidential and Proprietary.

ランサムウェア対策には多層防御が有効！

パロアルトなら多層のすべてが
自動連携！



対策①

- 全てのアプリケーションを可視化し安全に利用
- ネットワークベースで既知の脅威を全てブロック
- 未知の脅威は次世代セキュリティクラウドに送信

対策②

- 次世代ファイアウォールと次世代エンドポイントから潜在的な脅威の情報を収集
- 収集された脅威の情報を統合的かつ相関的に分析
- 新しい脅威の情報を次世代ファイアウォールと次世代エンドポイントへフィードバック

対策③

- すべてのプロセスとファイルを検査
- 既知と未知のエクスプロイトから防御
- デスクトップ/ 仮想化/ モバイル端末に対応
- 軽量なエージェントが最小リソースで稼働

 © 2015, Palo Alto Networks. Confidential and Proprietary.

次世代エンドポイント防御　“TRAPS”

Traps

Advanced Endpoint Protection

脆弱性を突く攻撃エクスプロイトを阻止！

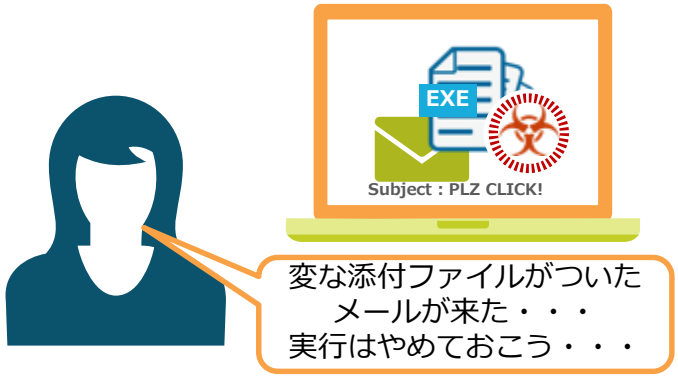
未知のマルウェア実行を阻止！

Trapsは、攻撃者が行う攻撃のための手法を阻害することで
攻撃を失敗に終わらせる、全く新しい考え方の
アドバンスト エンドポイント プロテクションです。

 © 2015, Palo Alto Networks. Confidential and Proprietary.

いつのまにマルウェアに感染・・・？

マルウェアは利用者が気がつかない間に実行され、感染するケースも

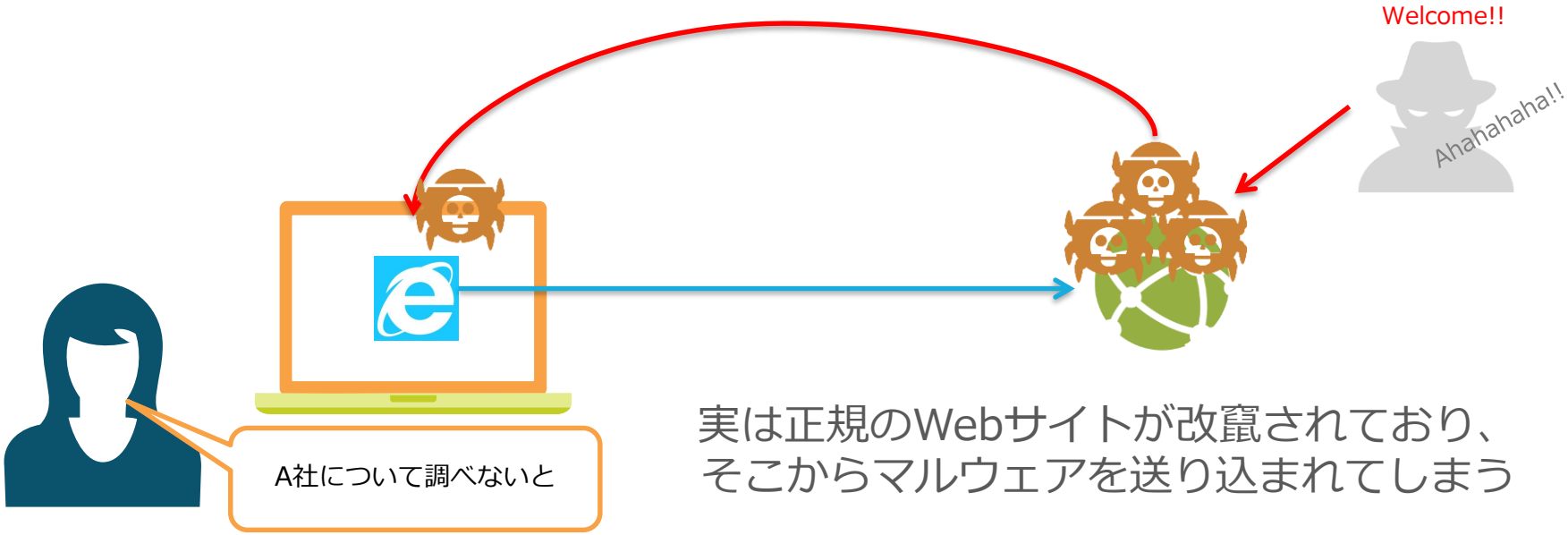


露骨に怪しいファイル実行しないが・・・

普通に見えるものは実行してしまう

 © 2015, Palo Alto Networks. Confidential and Proprietary.

メールではなく普通のWebサイトだと思って閲覧しても感染するケースも



実は正規のWebサイトが改竄されており、
そこからマルウェアを送り込まれてしまう

マルウェアは様々な経路で複数の手順を経て侵入してきます

 © 2015, Palo Alto Networks. Confidential and Proprietary.

直接マルウェアを送付しない場合に狙われるのは脆弱性

広く利用されているソフトウェアの脆弱性をつく
エクスプロイトを利用して攻撃者は巧みにマルウェアに感染させます

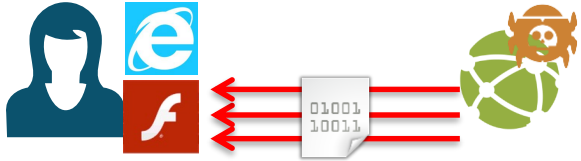
 © 2015, Palo Alto Networks. Confidential and Proprietary.

例えばこのような複数の手順で感染する事も

1.

Flashの脆弱性をつくエクスプロイを含んだ
改竄されたWebサイトを閲覧

2.

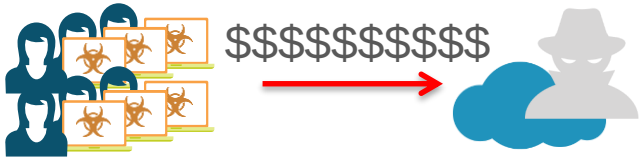


表示されたFlashによりエクスプロイトコードが
実行されFlashが分割されたマルウェア本体を
ダウンロードするドロッパーに

3.

ドロッパーがマルウェアの本体をダンロード、実行

4.



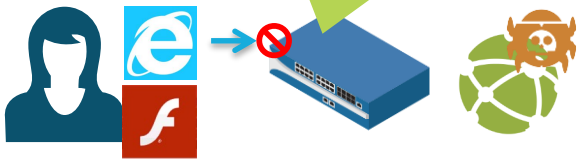
ファイルがロックされる！

 © 2015, Palo Alto Networks. Confidential and Proprietary.

では先ほどの例のような複数の手順での感染をどう守るのか？

改竄されたWebサイトへのアクセスは
URLフィルタでブロック可能

1.



Flashの脆弱性をつくエクスプロイを含んだ
改竄されたWebサイトを閲覧

 © 2015, Palo Alto Networks. Confidential and Proprietary.

では先ほどの例のような複数の手順での感染をどう守るのか？

IPS機能でエクスプロイトをブロック

2.

表示されたFlashによりエクスプロイトコードが
実行されFlashが分割されたマルウェア本体を
ダウンロードするドロッパーに

Trapsで端末上で実行される
エクスプロイトをブロック

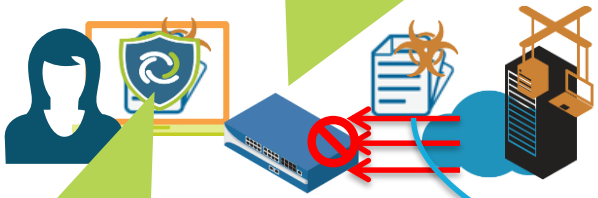
FlashファイルはWildFire(SandBox)でチェック
ドロッパーがダウンロードしてくる
すべてのファイルが検査対象

 © 2015, Palo Alto Networks. Confidential and Proprietary.

では先ほどの例のような複数の手順での感染をどう守るのか？

既知のマルウェアはアンチウィルス機能でブロック

3.



ドロッパーがマルウェアの本体をダンロード、実行

Trapsがマルウェアの実行を阻止

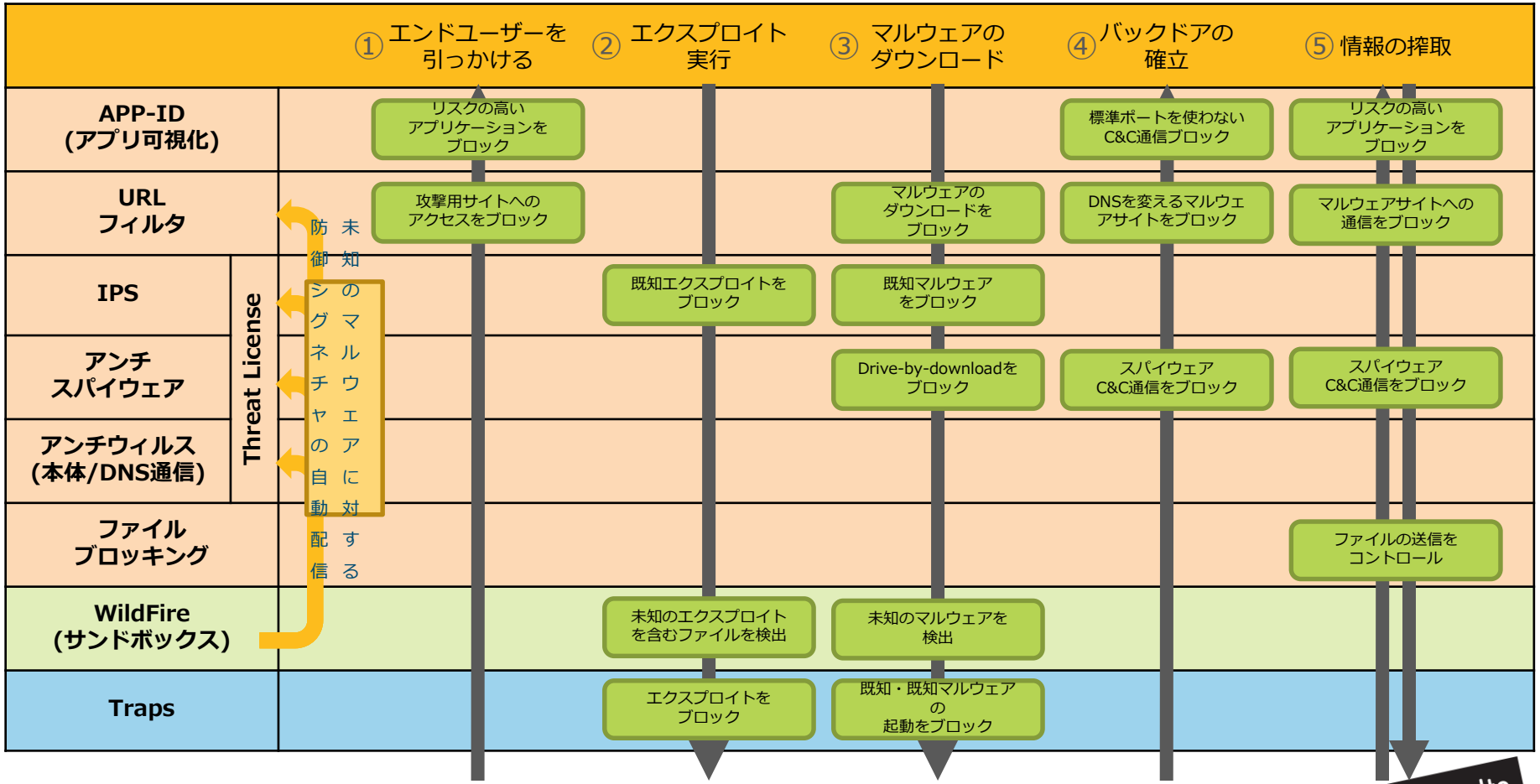
未知のマルウェアはWildFireにてチェック

 © 2015, Palo Alto Networks. Confidential and Proprietary.

エンタープライズセキュリティプラットフォームを利用した多層防御

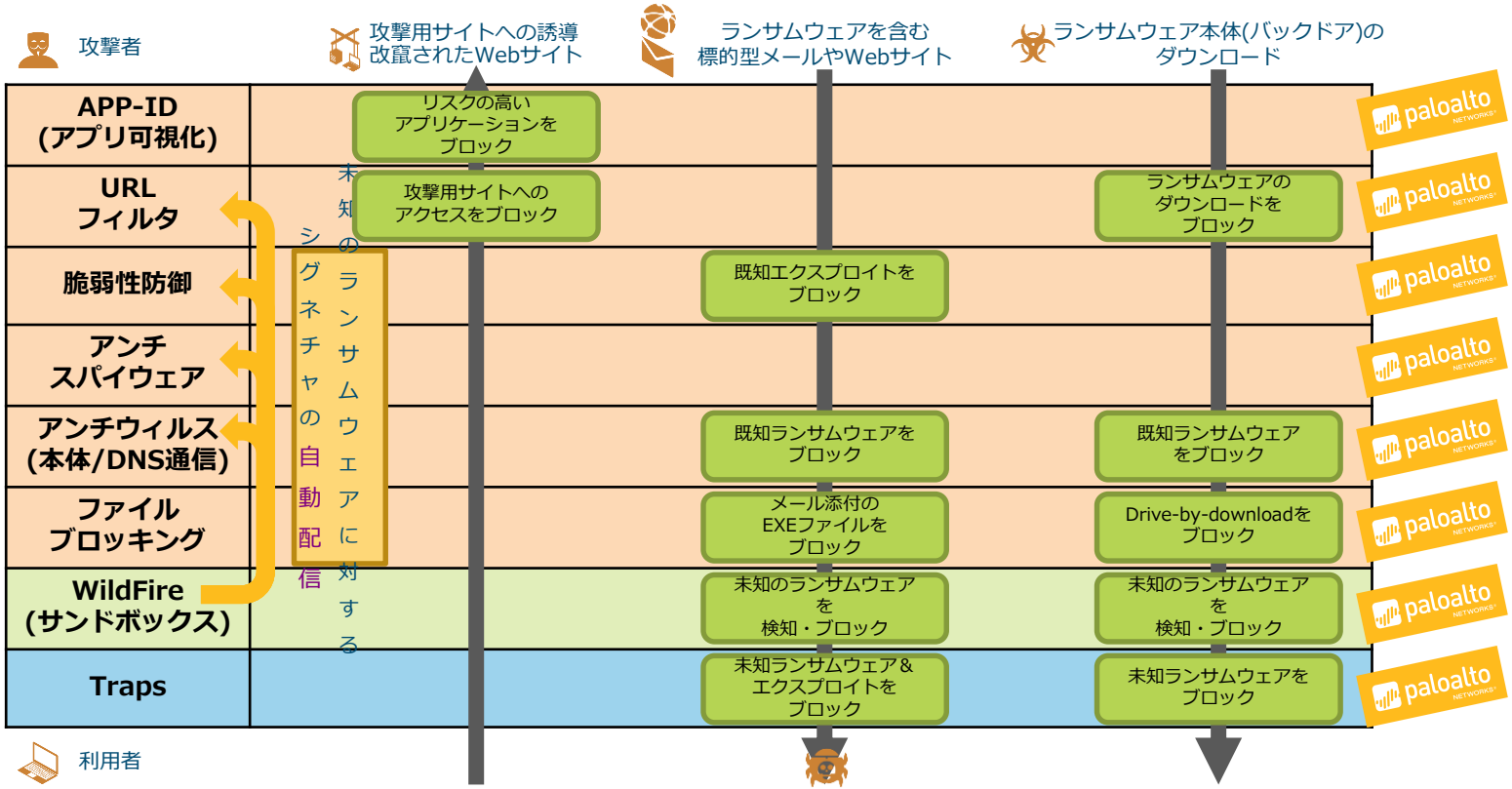
攻撃者は数々の防御をすべて突破しないと攻撃を成功させる事ができません

 © 2015, Palo Alto Networks. Confidential and Proprietary.



 © 2015, Palo Alto Networks. Confidential and Proprietary.

多層防御を利用したランサムウェア対策



 © 2015, Palo Alto Networks. Confidential and Proprietary.

ランサムウェア対策 ≠ サンドボックス製品

- サンドボックスをすり抜ける
  - ファイル自体をZIP暗号化、分割、サイズを大きくすれば検査できない（例 Flame）
  - 潜伏活動を行う前にInternet接続をチェックする等
- Web とメール以外の径路が検査できない
  - SSL通信（HTTPS, SMTP over SSL）
  - 独自暗号を行うP2P（i.e., SkypeやIM）、ファイル共有ソフト
  - ネットワーク内部での二次感染拡大で利用されるFTP等
  - ネットワークを経由しない感染（例 USBやメディア）
- ブロックする場合にはURLやIPアドレスベース（基本検知がメイン）
  - マルウェア自体に対するシグネチャ vs URL・IPアドレスベースでのブロック

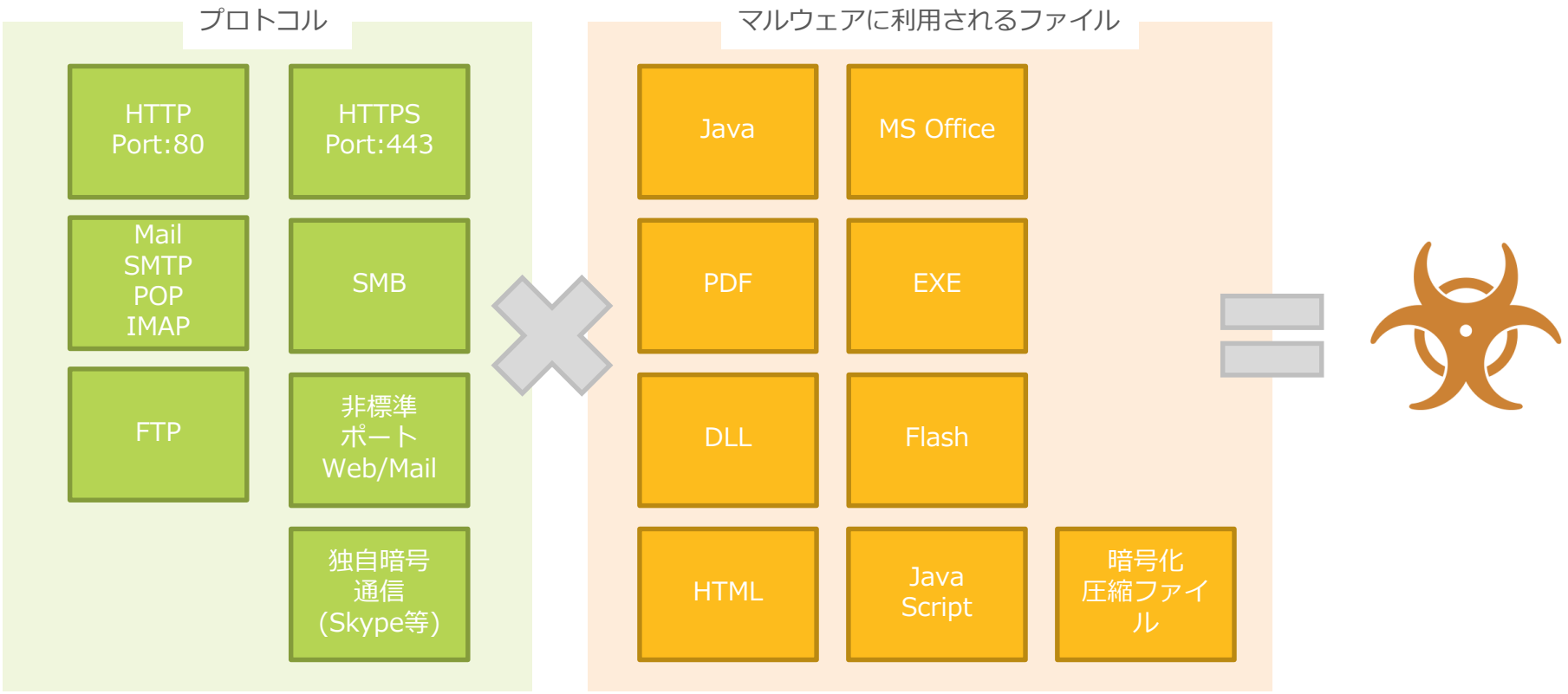
サンドボックスは優秀だが万能ではない
あくまでセキュリティを補完する技術の１つ

 © 2015, Palo Alto Networks. Confidential and Proprietary.

攻撃者も日々手を変え品を変え攻めてくる

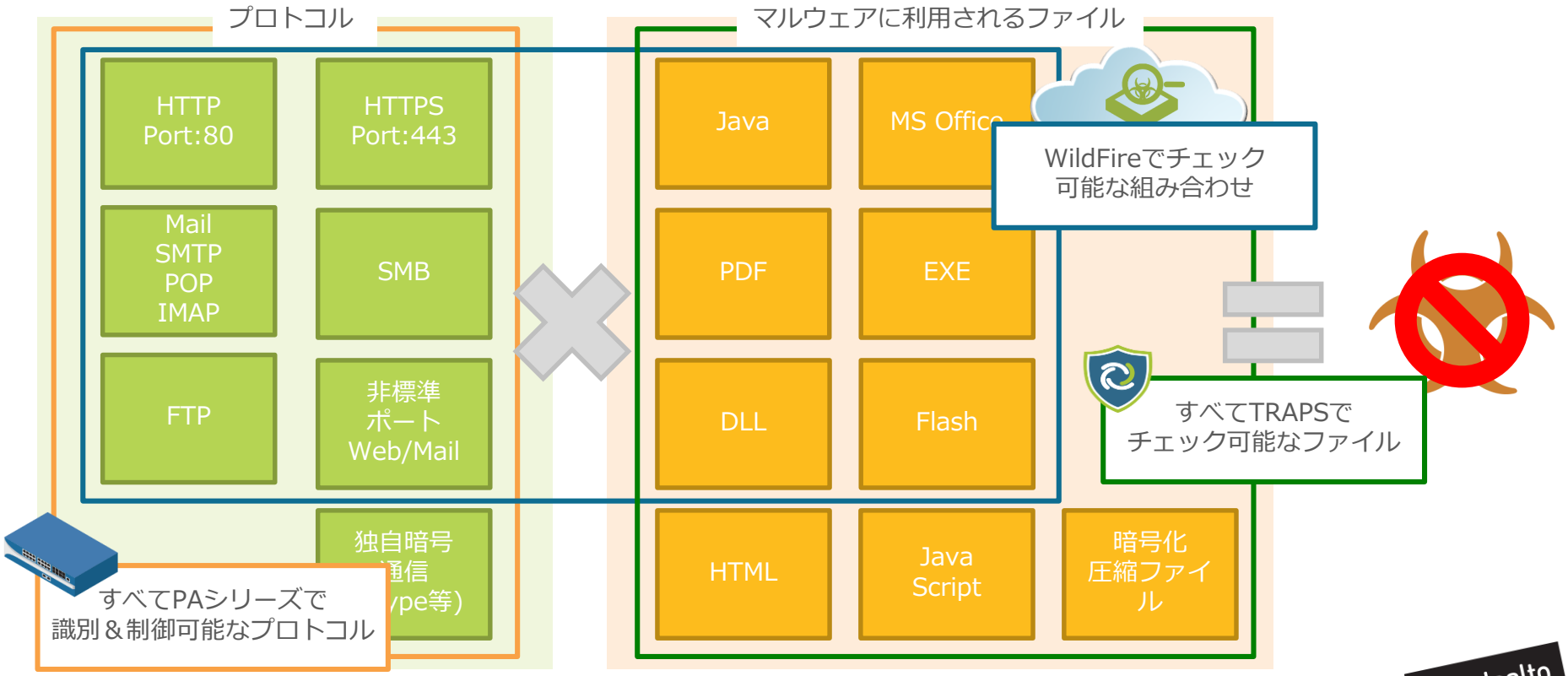
 © 2015, Palo Alto Networks. Confidential and Proprietary.

マルウェアは複数のプロトコルやファイルを利用するマルチフローで感染



 © 2015, Palo Alto Networks. Confidential and Proprietary.

エンタープライズセキュリティプラットフォームなら
複数のプロトコル、ファイルを利用して侵入するマルウェアのチェックが可能

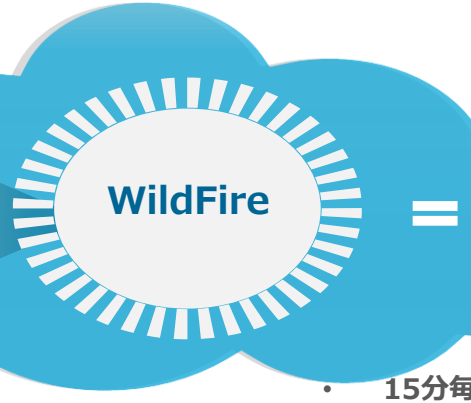


 © 2015, Palo Alto Networks. Confidential and Proprietary.

脅威インテリジェンスクラウド *WildFire™*

8,000 社以上
31,000 台以上

Email
SMTP
All ports
SSL encryption
All traffic
FTP
Endpoint
Data center
Web
Perimeter
All commonly exploited file types
3rd party data



未知の脅威を発見＆フィードバック
- マルウェア
- エクスプロイト（脆弱性攻撃）
- C&C通信
- DNSクエリー
- マルウェア配信サイト（URL）

※Web/Email/FTP等複数プロトコルに対応

キルチェーンに則した
インライン防御を提供
脅威情報を相関的に分析＆共有:

WildFire | 脅威防御 | URLフィルタ

- **15分毎に約312**の新しい AV シグネチャを配信
- **15分毎に約150**の新しい DNS シグネチャを配信
- **30分毎に約280**の新しい URL ルールを追加
- **14%**は ポート80番/25番以外で発見

- アップロードされるユニークなファイル数: 一日当たり 約200万
  - 70%がPDF, 12%がWord, PE/EXEが4%
- そのうち ~6% が未知含むマルウェア： 一日当たり 約3万
  - 発見されたマルウェアのうち 97%がPEフォーマット

 © 2015, Palo Alto Networks. Confidential and Proprietary.

パロアルトネットワークス製品を選択するメリット

1. 標的型攻撃に対し多層防衛の技術を持ち、検知＆防御を1台で実現可能
2. 防御機能を利用しても、パフォーマンスを十分に発揮出来る構造と処理能力を持つ
3. 柔軟な構成をとることが可能なため、最小限の機器構成で導入が可能
4. 統一されたレポートやログにより運用負荷を軽減することが可能
5. 最小限の構成で構築出来るため、導入・運用費用を抑えることが出来る

 © 2015, Palo Alto Networks. Confidential and Proprietary.

多層防御

エンタープライズセキュリティプラットフォーム

 © 2015, Palo Alto Networks. Confidential and Proprietary.

PALO ALTO NETWORKS
NEXT GENERATION SECURITY PLATFORM