日々変化するサイバー脅威に対抗する多層化アプローチ

サイバー脅威のトレンド

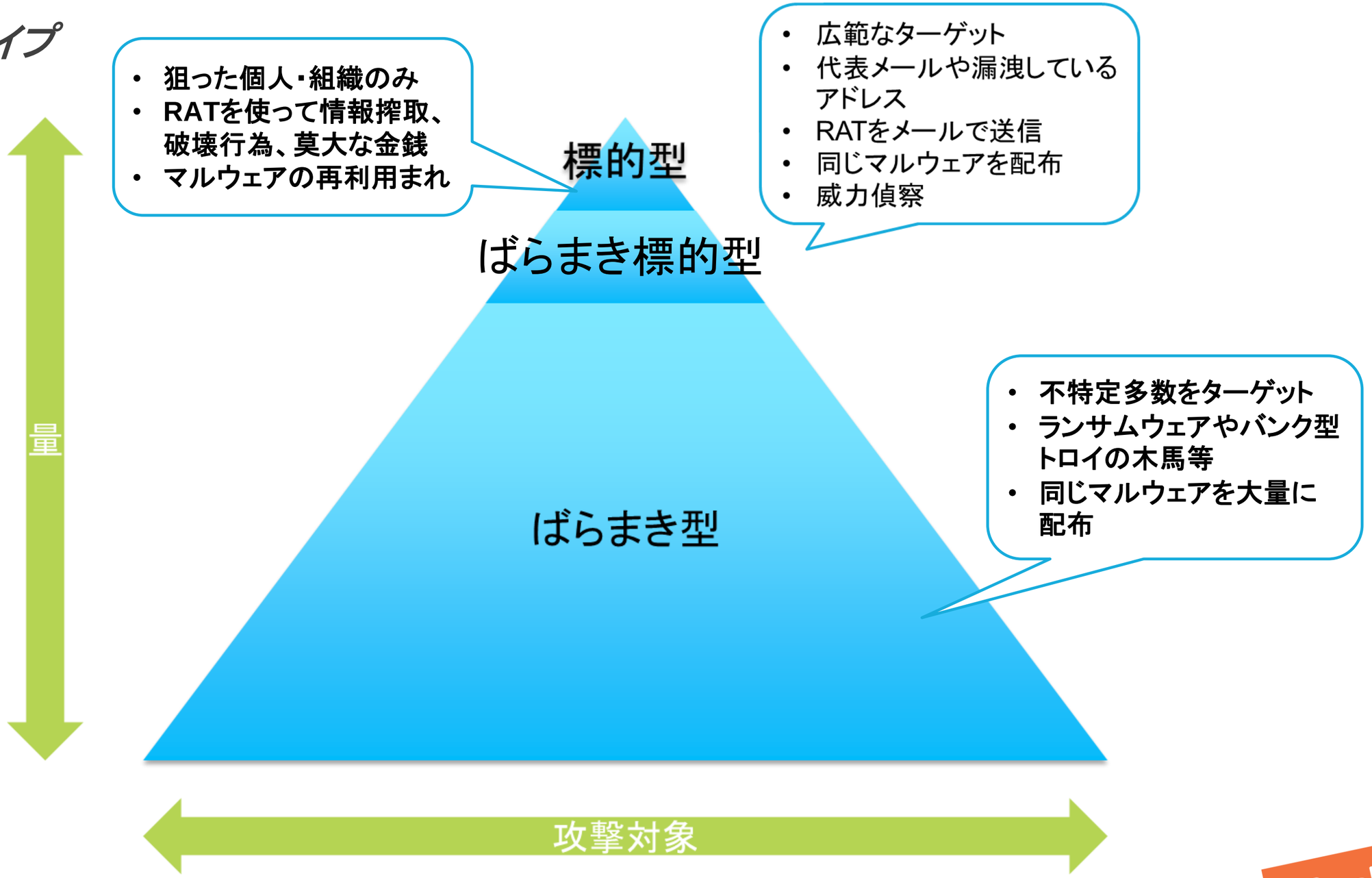
現在、主流となっているサイバー脅威

- バンキング型トロイの木馬
  - Dridex, Shiotob, Rovnix
- ランサムウェア
  - Locky, TeslaCrypt, Nymaim
- ダウンローダー
  - Rockloader, Bartallex, Andromeda,
- RAT (Remote Access Tool)
  - NanoCoreRAT, NetWireRAT

2016年4月に WildFire に送信されたマルウェアのTop-10

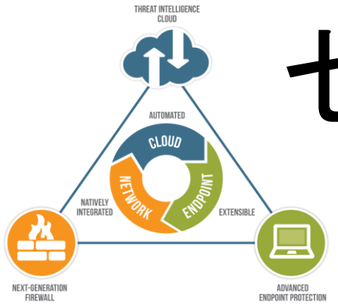
SHA256	マルウェア	タイプ	セッション数
a565....aa5a	Andromeda	ダウンローダー	33133
a91c....07ea	Shiotob	バンキング型トロイの木馬	25007
617a....a0fe	Shade	ランサムウェア	6222
b3e0....b3e7	Shiotob	バンキング型トロイの木馬	5175
f435....359f	TeslaCrypt	ランサムウェア	2578
f597....2cb7	Pushdo	スパム型ボット	2093
7c36....9b64	Rockloader	ダウンローダー	1959
89e7....2963	Andromeda	ダウンローダー	1931
14e7....fc34	Shiotob	バンキング型トロイの木馬	1677
f2e4....f7f6	Bartallex	マクロ型ダウンローダー	1271

攻撃のタイプ


標的型
ばらまき標的型
ばらまき型
量
攻撃対象
• 狙った個人・組織のみ
• RATを使って情報搾取、破壊行為、莫大な金銭
• マルウェアの再利用まれ
• 広範なターゲット
• 代表メールや漏洩しているアドレス
• RATをメールで送信
• 同じマルウェアを配布
• 威力偵察
• 不特定多数をターゲット
• ランサムウェアやバンク型トロイの木馬等
• 同じマルウェアを大量に配布

サイバー脅威のトレンド

- ばらまき型は特定の業界を狙わない
  - メールアドレスがリストに載っている業界が上位
  - 1日に数十万単位で送られる
- 標的型攻撃は狙ってくる
  - 高度な標的型から　ばらまき標的型まで
  - 知的財産をはじめとする情報窃取を目的
- 業界問わず攻撃は必ずくる　＝　適切な防御が必要
  - プライオリティとポリシー（グランドデザイン）
  - メールとWebは重要な経路（入口・出口対策）
  - ユーザ教育（ソーシャルエンジニアリング対策）
  - システムやアプリケーションのパッチ適用（脆弱性対策）
  - 未知の脆弱性への耐性（ゼロデイ対策）
  - 情報の管理とバックアップ（情報漏洩・紛失対策）
- ランサムウェアはビジネスとして成立
  - 既存も新規も活発に活動
- ランサムウェアによって、暗号化された場合、復号は難しいことが多い
- 防御可能なポイントはいくつかある



セキュリティプラットフォームによる多層化防御アプローチ

防御することを前提としたプラットフォーム

1

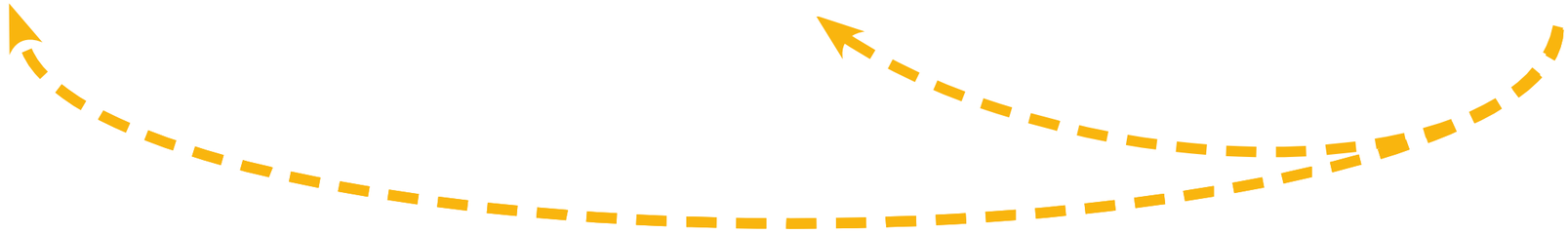
攻撃面の最小化

2

既知の脅威からの防御

3

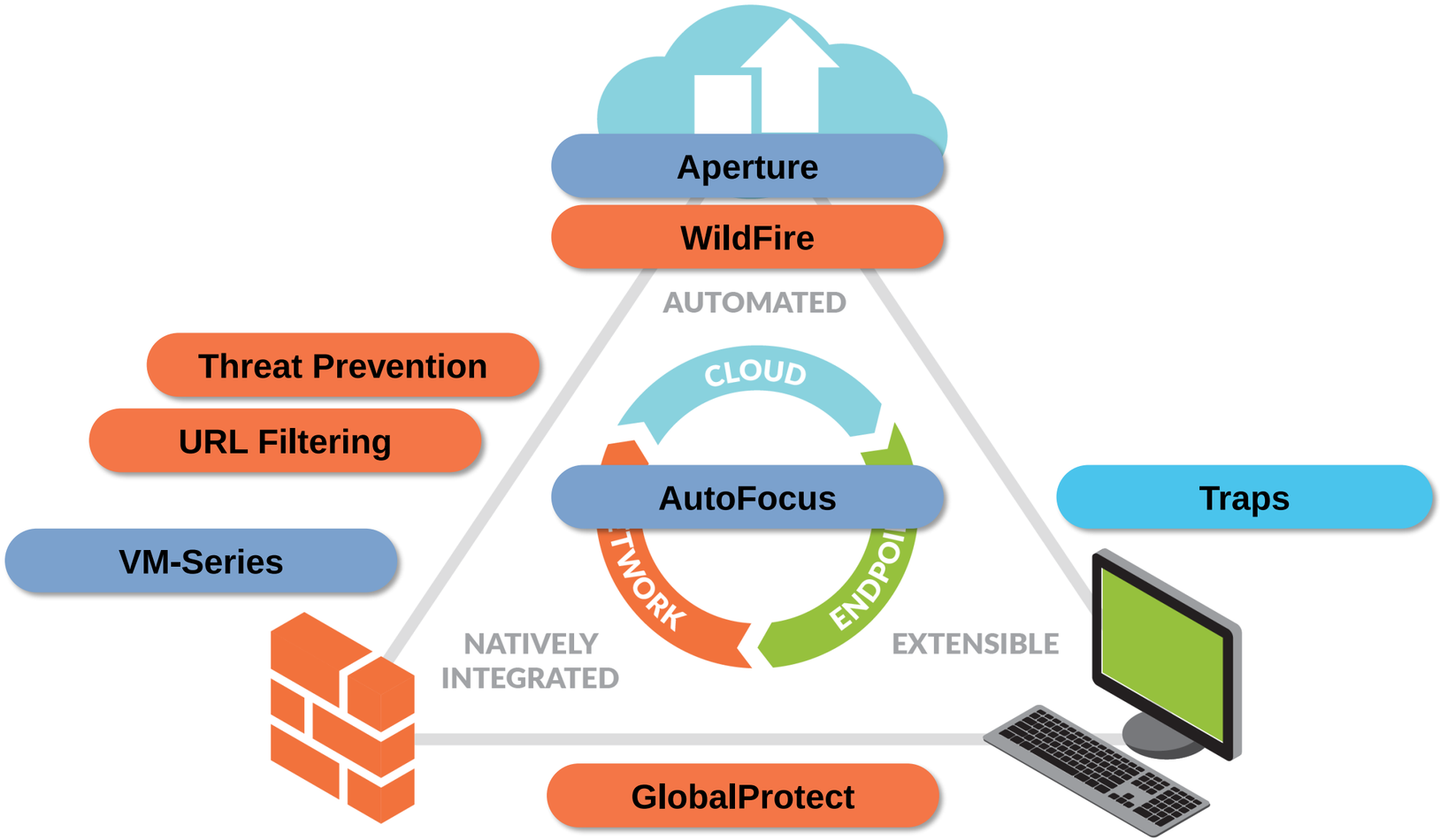
未知の脅威の識別と防御



自動的に未知の脅威を既知の脅威へ

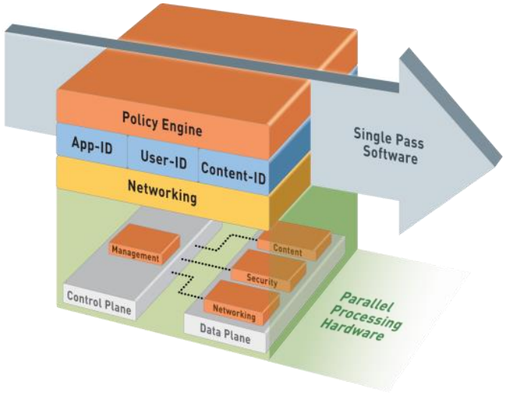
新しい防御機能を使用してネットワークを再プログラム

次世代 セキュリティ プラットフォーム



次世代ファイアウォールの特徴と攻撃面を最小化する多層方式

1. ポート番号やプロトコル・暗号化に関わらず、全ての**アプリケーションを識別**し、その中に埋もれる非正常通信（不明なアプリケーション）までもすべて**可視化**
2. 全ての通信を利用**ユーザレベルで識別**して制御＆記録
3. 脆弱性攻撃、情報漏えい、マルウェア等の**既知の脅威**に対してリアルタイム防御
4. **未知の脅威**についてはクラウドを活用しリアルタイムで分析して、結果を自動的な防御にフィードバック
5. 従来のネットワーク環境以外に、**仮想化環境**ならびに**モバイル環境**に対しても同様のセキュリティを実施



プロトコル分析 ベース

- App-ID

ヒューリスティック ベース

- 自動相関エンジン
- ボット検出

シグネチャ ベース

- アンチウィルス
- アンチスパイウェア
- 脆弱性防御（IPS）

サンドボックス ベース

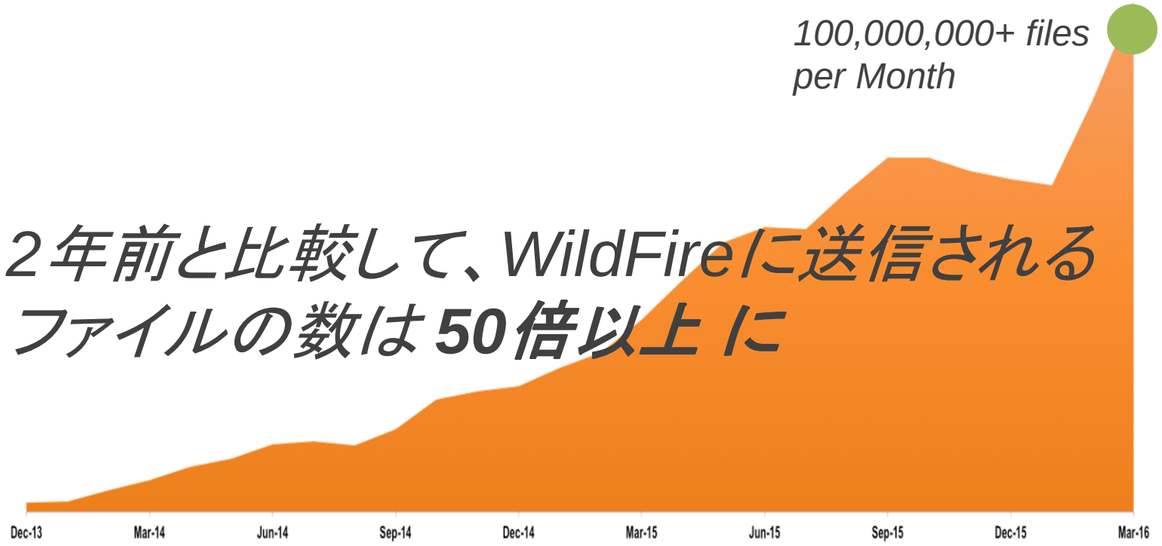
- WildFire

脅威インテリジェンスクラウド：WildFire

- クラウド上にあるサンドボックス環境でファイルを分析し、未知のマルウェアを発見＆防御するためのサービス
- 世界中のお客様環境で発見されたマルウェアに対して、シグネチャを自動生成し配信

※WildFire サービスの利用にあたっては、利用する次世代ファイアウォール上で追加のサブスクリプションが必要です

グローバルで10,000社・30,000台以上が利用
検査されるファイル数：
一日当たり 約300万 / DAY
発見されるマルウェア：
一日当たり 約4万 / DAY



*2年前と比較して、WildFireに送信されるファイルの数は **50倍以上** に*

WildFire 上で検査されるファイル数の推移

Traps™ エンドポイント防御

ADVANCED ENDPOINT PROTECTION

エクスプロイト防御
ゼロディ脆弱性を含むエクスプロイトをブロック

マルウェア防御
未知・既知を含む幅広いマルウェアをブロック

フォレンジックデータの収集
攻撃を受けた際に分析に必要なデータを保存

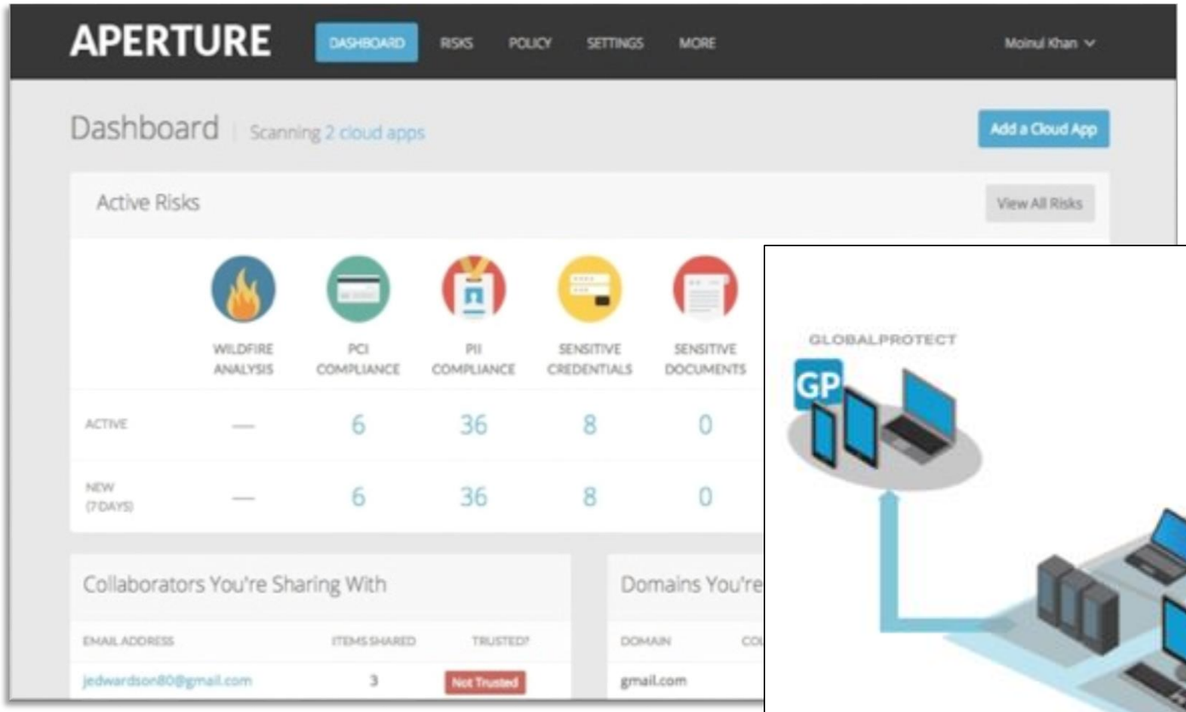
シンプル、軽い、分かり易い
エンタープライズ環境での利用・運用をベースに設計

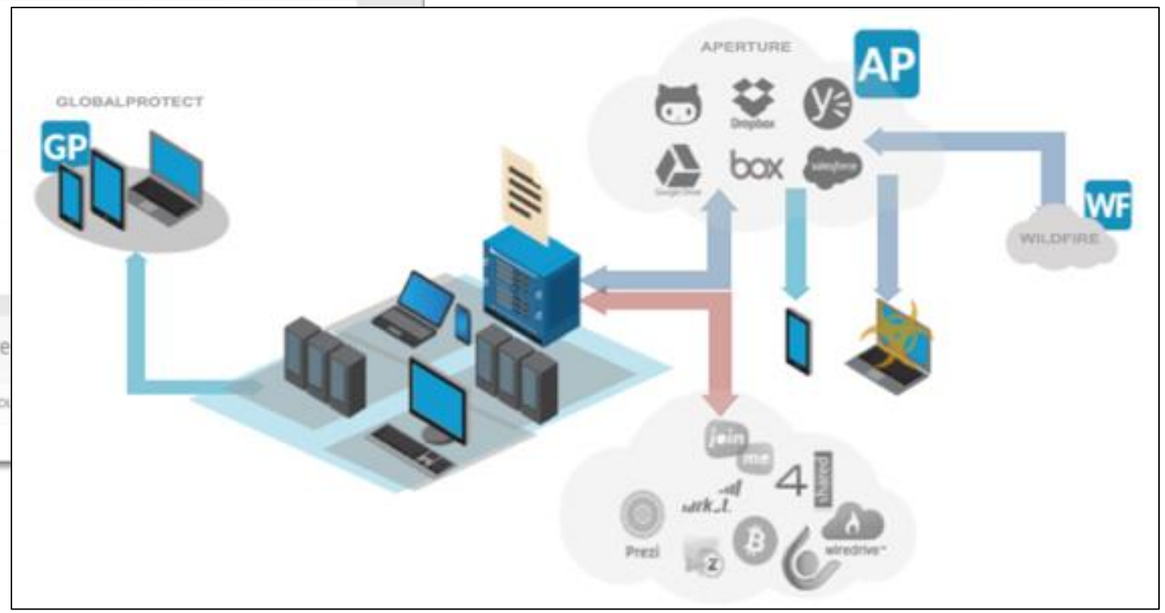
ネットワークおよびクラウドとの連携
脅威情報を交換することにより統合的なセキュリティを実現

Traps

Advanced Endpoint Protection

SaaSセキュリティ：APERTURE





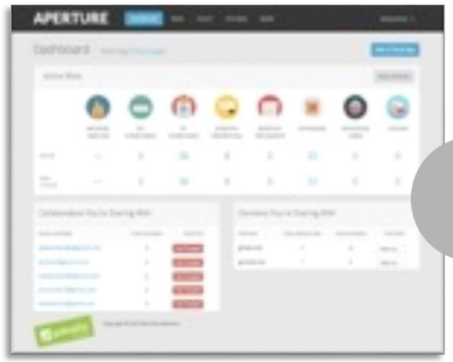
詳細なコンテンツ検査
および アナリティクス

コンテキストによる
データ公開の制御

機械学習による
ファイルの分類

マルウェアの
検出＆除去

APERTURE による SaaS セキュリティ



APERTURE

APERTURE

WF

WILDFIRE

GP

Dropbox

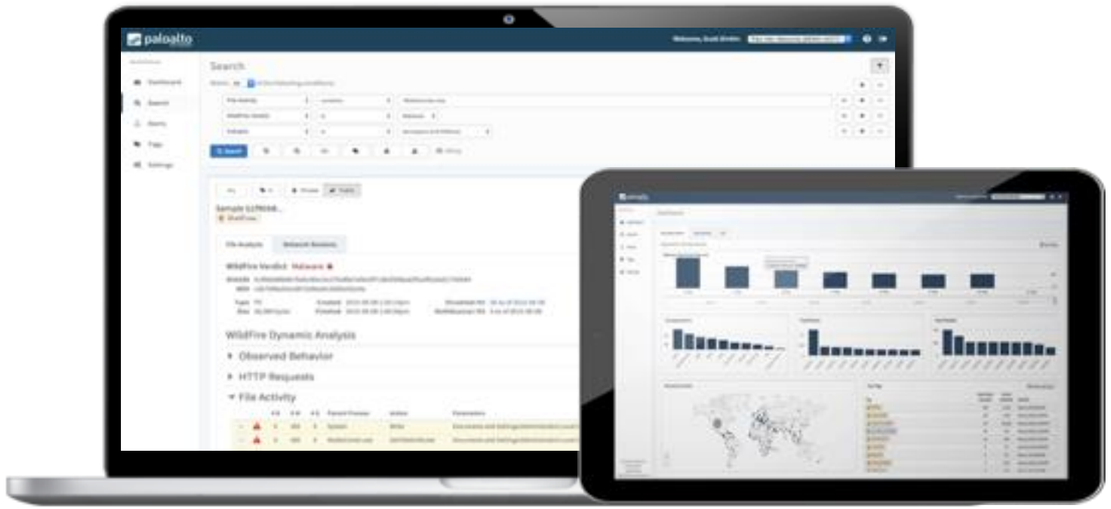
box

salesforce

OneDrive

Google Drive

脅威インテリジェンスサービス：AUTOFOCUS



イベントの優先度の設定

ユニークな標的型攻撃を発生時に特定

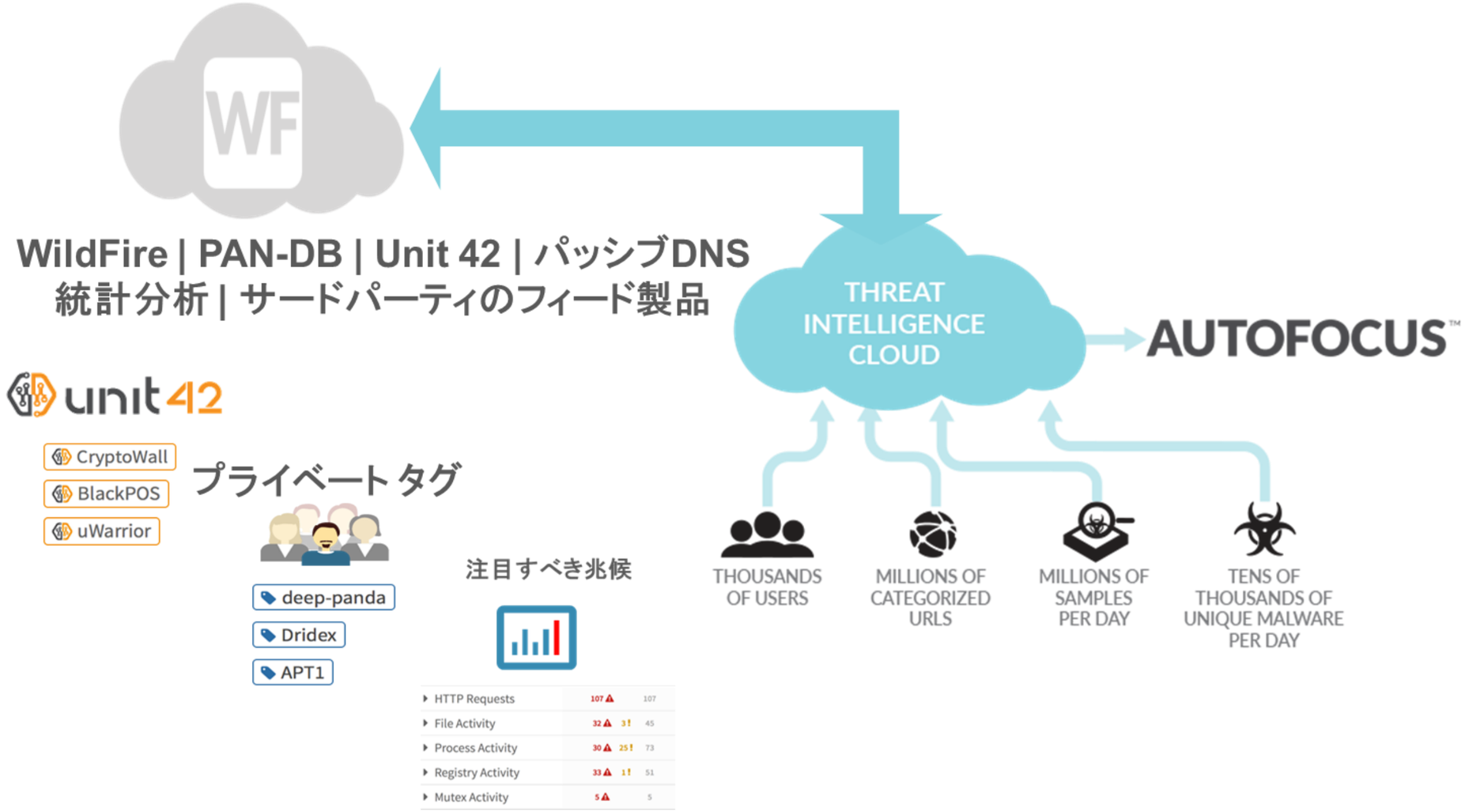
コンテキストおよび検索

悪意のある人物、組織的攻撃、攻撃手法の迅速な調査

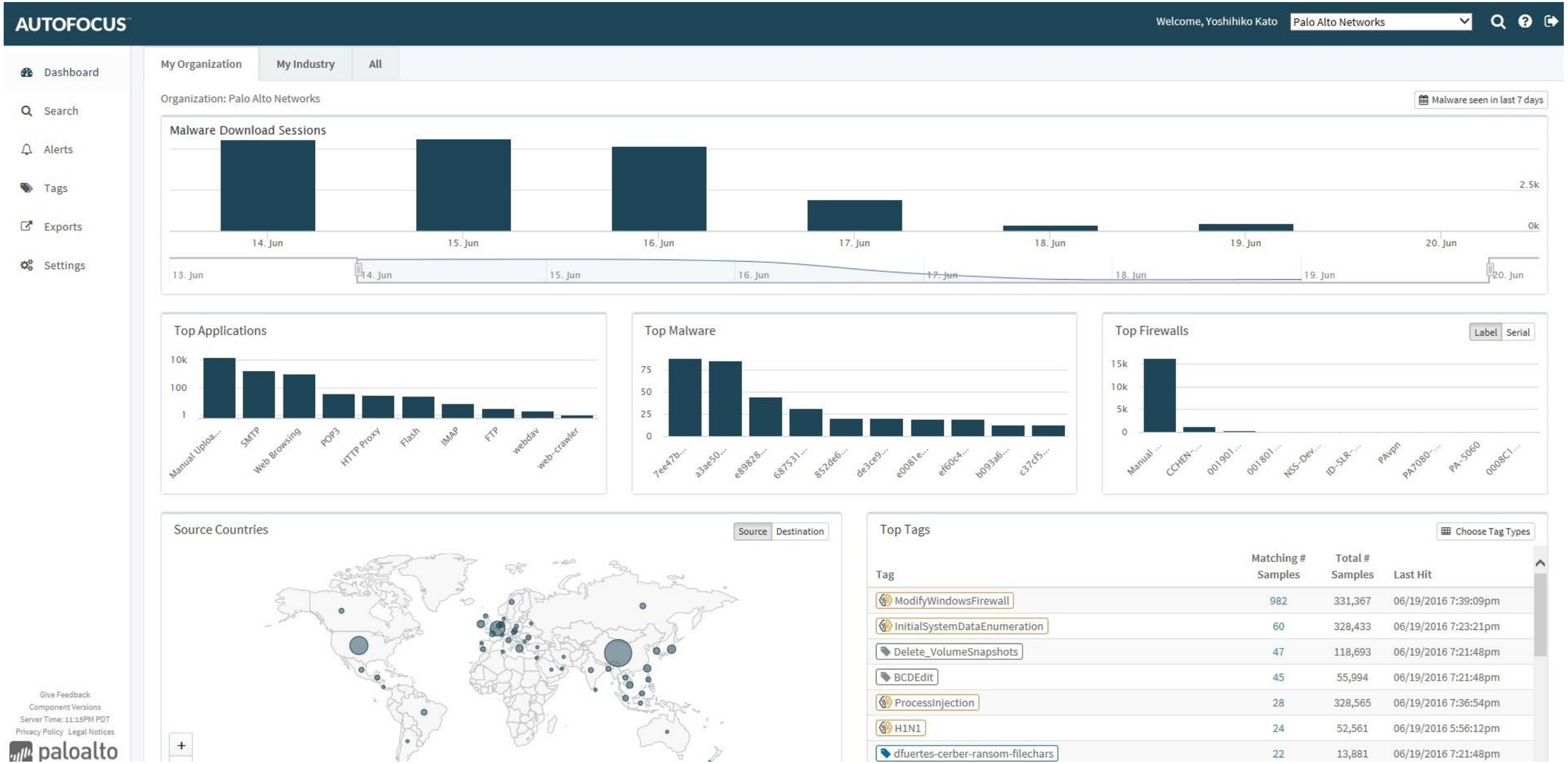
プロアクティブな対応

セキュリティ侵害が発生する前に、攻撃のライフサイクル全体を対象とする防御を実現

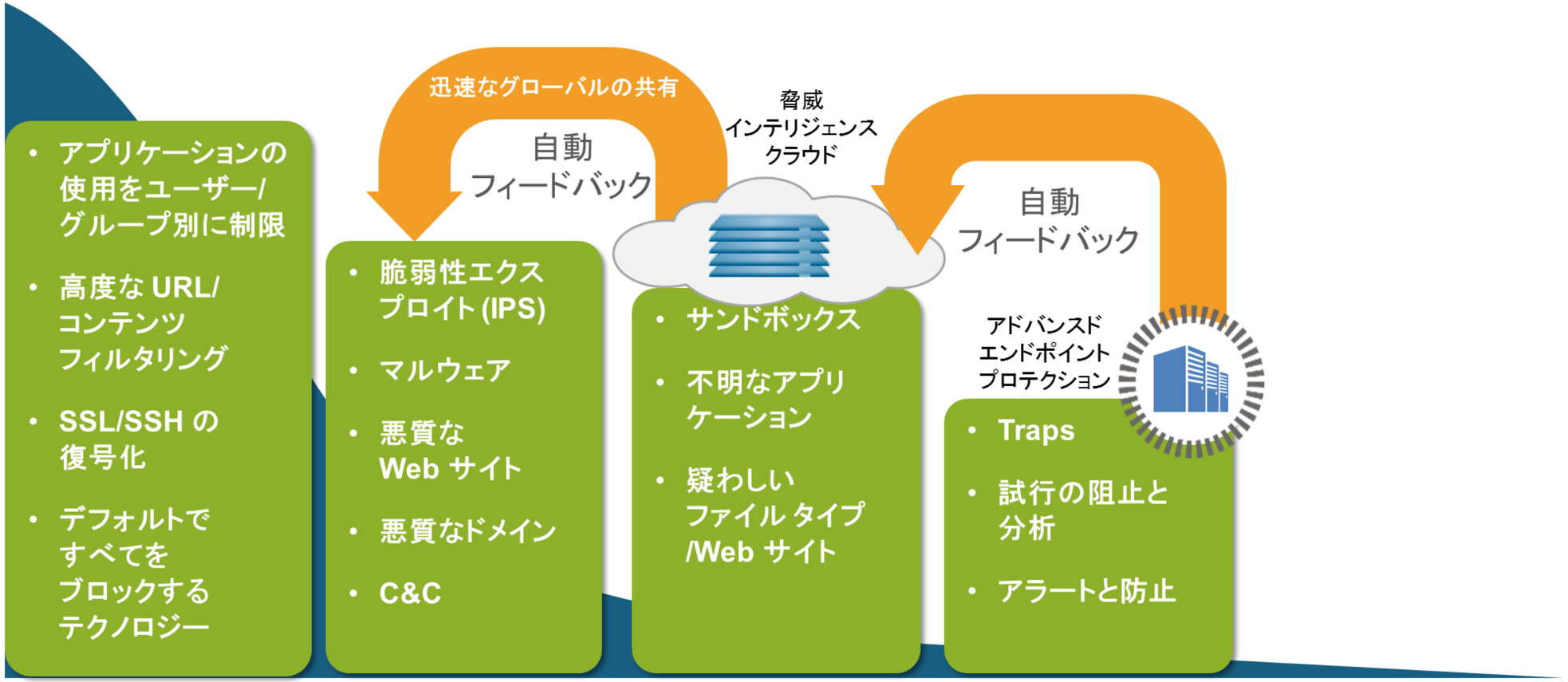
AUTOFOCUSに蓄積される脅威データ



AUTOFOCUSの画面イメージ



Palo Alto Networks 次世代セキュリティプラットフォームによる多層防御



ポジティブな制御を適用	既知の脅威を阻止	未知の脅威を検出	マルウェアの実行を阻止