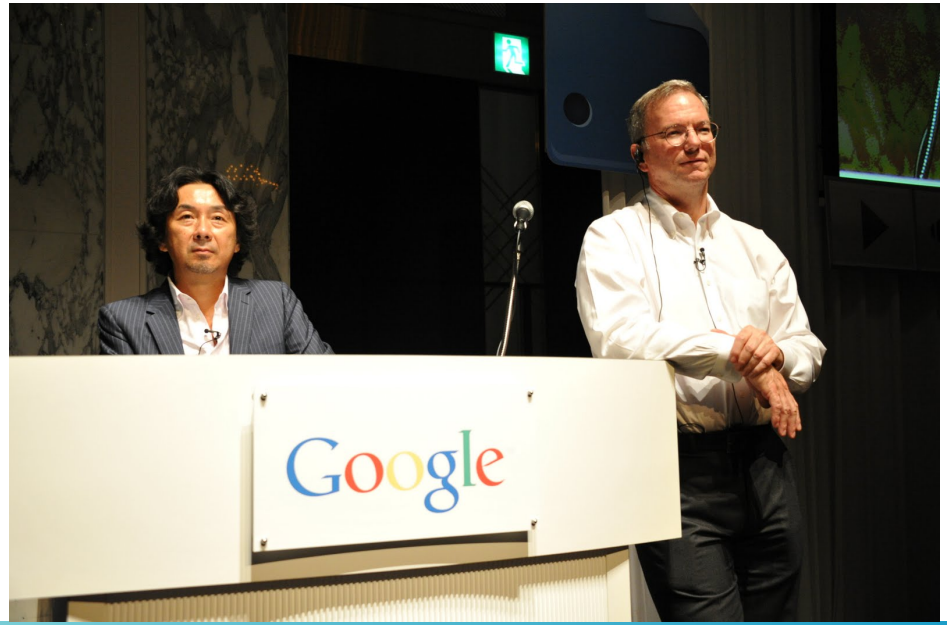
クラウドセキュリティとは

クラウドセキュリティスペシャリスト
泉　篤彦

自己紹介

- 泉　篤彦
- 2007年よりGoogleエンタープライズ部門クラウドSE



 © 2018, Palo Alto Networks. All Rights Reserved.

クラウドトレンドを考察

クラウドトレンド

- 2006年8月、グーグルの最高経営責任者のエリック・シュミット氏が、米・カリフォルニアで開かれた「サーチエンジン戦略会議」の中で、「ブラウザの種類も、アクセス手段も、パソコンかマックか、携帯電話かも無関係です。“雲(クラウド)”のような、巨大なインターネットにアクセスすれば、その利益、恵みの雨を受けられる時代になっています」という発言を受けて生まれた
- Googleファイルシステム(GFS)によるフルスケールする環境
- AI、マシンラーニング、Deepラーニングの基盤として必須の環境

 © 2018, Palo Alto Networks. All Rights Reserved.

セキュリティトレンドを考察

セキュリティトレンド

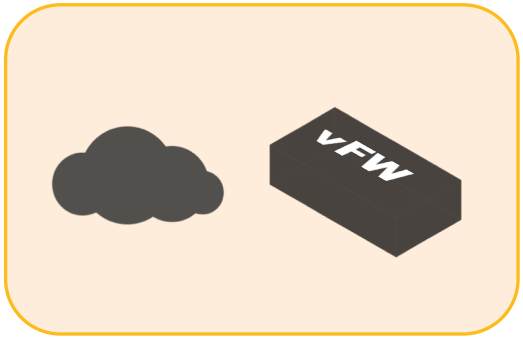
- ダークウェブ、アンダーグラウンドインターネット
- 企業化されたサイバーセキュリティ市場
- 安価なハッキングツール、アマチュアハッカーの台頭
- WindowsPCからパブリッククラウドにターゲットがシフト
- 攻撃側もクラウド、マシンラーニングをフルに活用

 © 2018, Palo Alto Networks. All Rights Reserved.

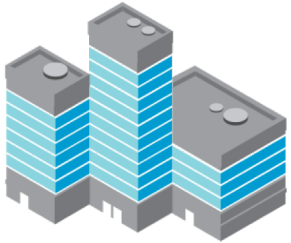
今考えなければいけない脅威対策とは

次世代脅威プリベンション

技術革新による生産性の向上

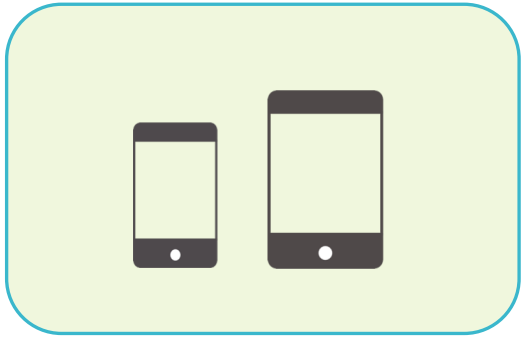


クラウドと仮想化



servicenow Office 365 zoom workday salesforce

SaaS
(Software as a Service)



モビリティとBYOD

IoT (Internet of Things)

 © 2017, Palo Alto Networks. All Rights Reserved.

サイバー攻撃トレンド

- ブルートフォースアタック
- パスワードリスト攻撃
- 標的型攻撃
- ゼロデイ攻撃
- ランサムウェア
- バックドア

 © 2018, Palo Alto Networks. All Rights Reserved.

アタックライフサイクルのすべてのステージで脅威プリベンション

アプリ、ユーザ、コンテンツベースでアクセスを制限

システムやアプリを脆弱性やマルウェアなどによる攻撃から防御

C&C通信をブロック

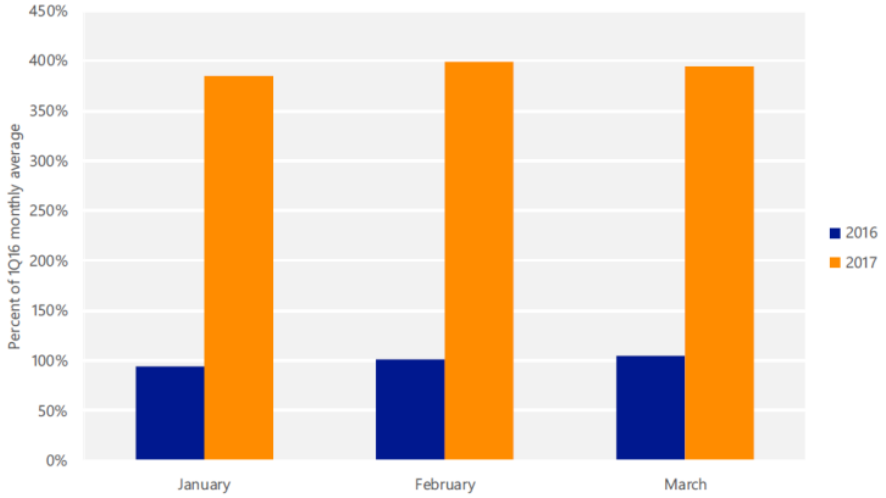
機密情報の持ち出しをコントロール

 © 2017, Palo Alto Networks. All Rights Reserved.

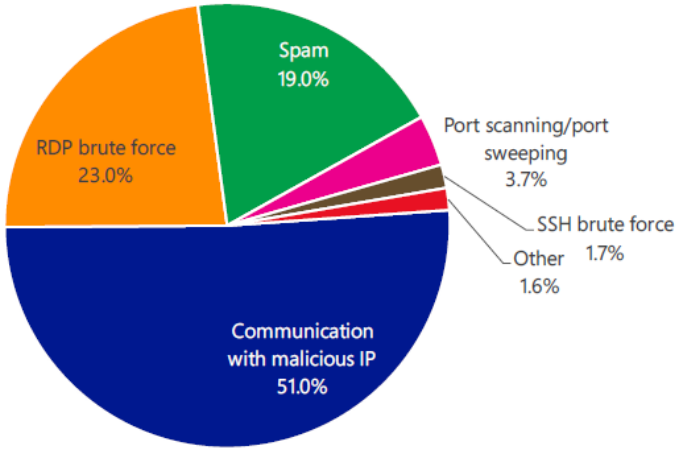
パブリッククラウドにおける脅威トレンド

Significant Increase in Cloud-Based Attacks in the Last Year

クラウド利用増加に伴い、アッタク件数も急増。2107年には前年度比300%増の様々な攻撃(フィッシング、ブルートフォース攻撃、3rdパーティからのハッキング)



Attacks on Cloud accounts: comparison between Q1 2016 to Q1 2017.
Source: Microsoft

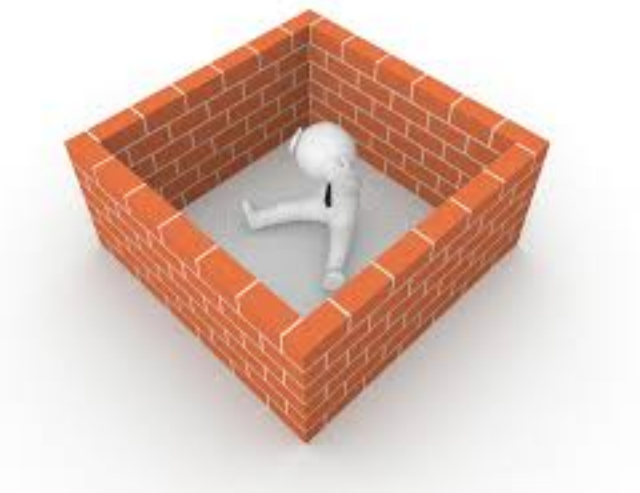


Types of attacks performed using compromised virtual machines in the Cloud

 © 2018, Palo Alto Networks. All Rights Reserved.

https://blog.sensecy.com/2017/09/25/significant-increase-in-cloud-based-attacks-in-the-last-year/

これまでオンプレで当然だったセキュリティがクラウドでどう変わるのか



 © 2018, Palo Alto Networks. All Rights Reserved.

クラウドセキュリティでは何を考えればいいのか

クラウドの責任共有とは

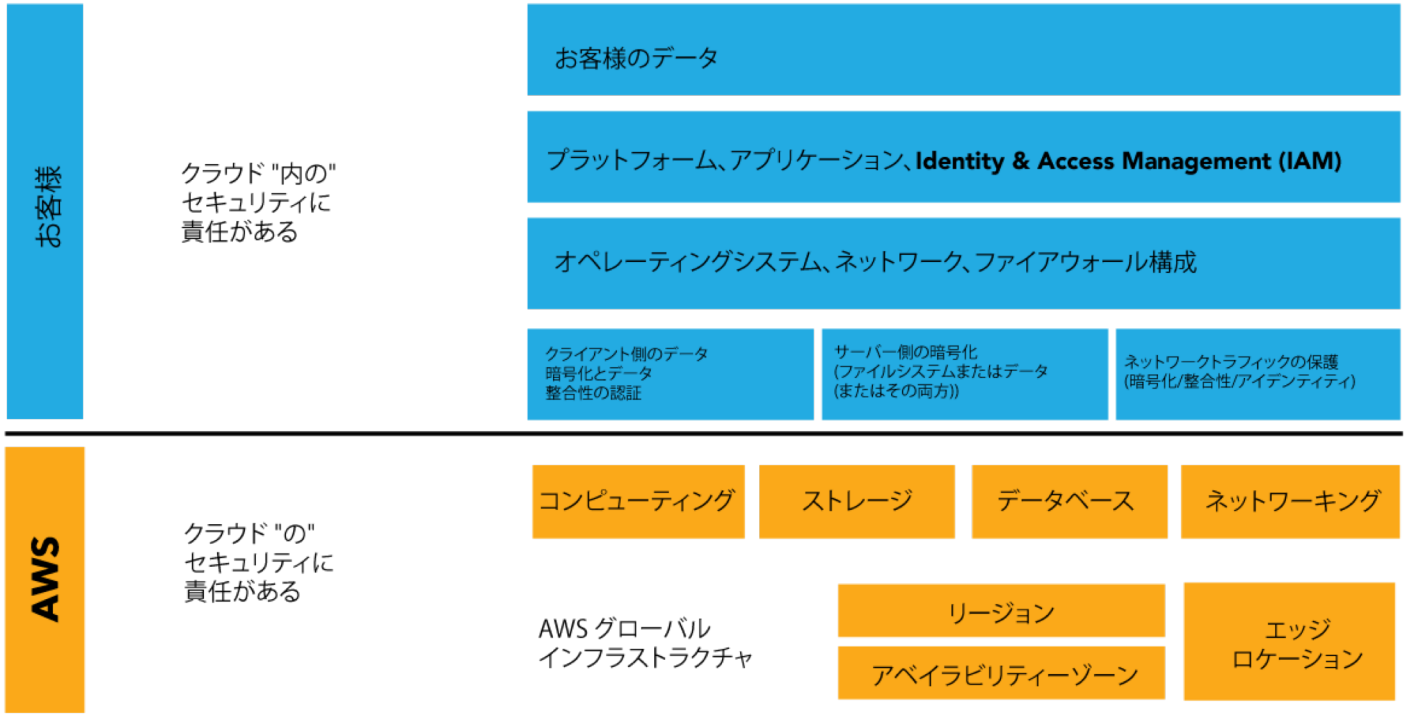
パブリッククラウドのセキュリティに関しての質問で多い「オンプレミスとの違いは？」
「クラウドベンダーが全て管理してくれるのでは？」
その違いが：

共有責任モデル

 © 2017 Palo Alto Networks, Inc. Confidential and Proprietary.

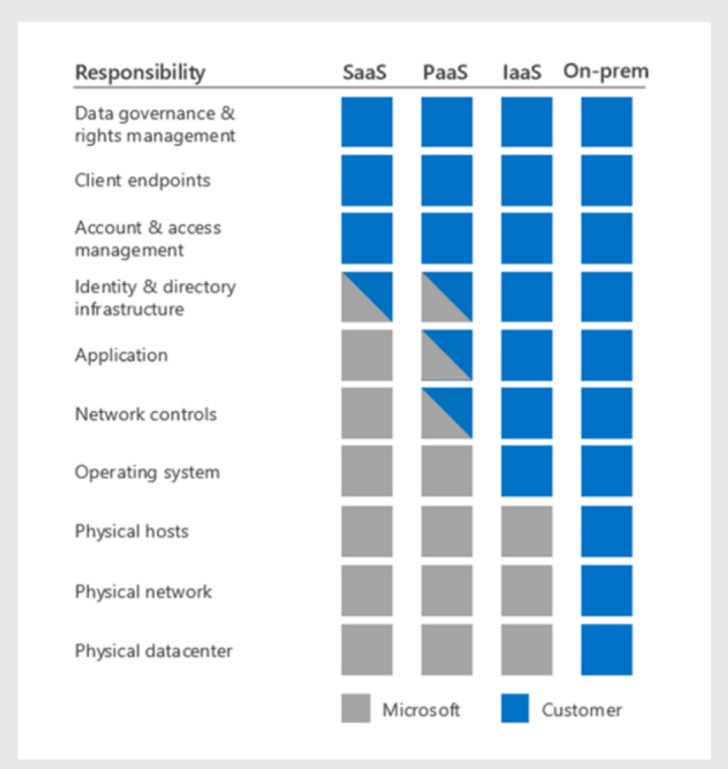
AWSの責任共有モデル

AWS は、AWS クラウドで提供されるすべてのサービスを実行する**インフラストラクチャの保護に責任を負います**。お客様は、ゲストオペレーティングシステムの管理 (更新やセキュリティパッチなど)、インスタンスにインストールしたアプリケーションソフトウェアまたはユーティリティの管理、AWS より各インスタンスに提供される**ファイアウォール (セキュリティグループと呼ばれる) の構成に責任を負います**。



 © 2017 Palo Alto Networks, Inc. Confidential and Proprietary.

Azureの責任共有モデル



Microsoft は、Microsoft Azure およびそのデータセンターの (入室に ID カードが必要なドア、フェンス、守衛などのセキュリティ保護の使用による) 物理的なセキュリティの責任を負います。

お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、および自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持ちます。

https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview

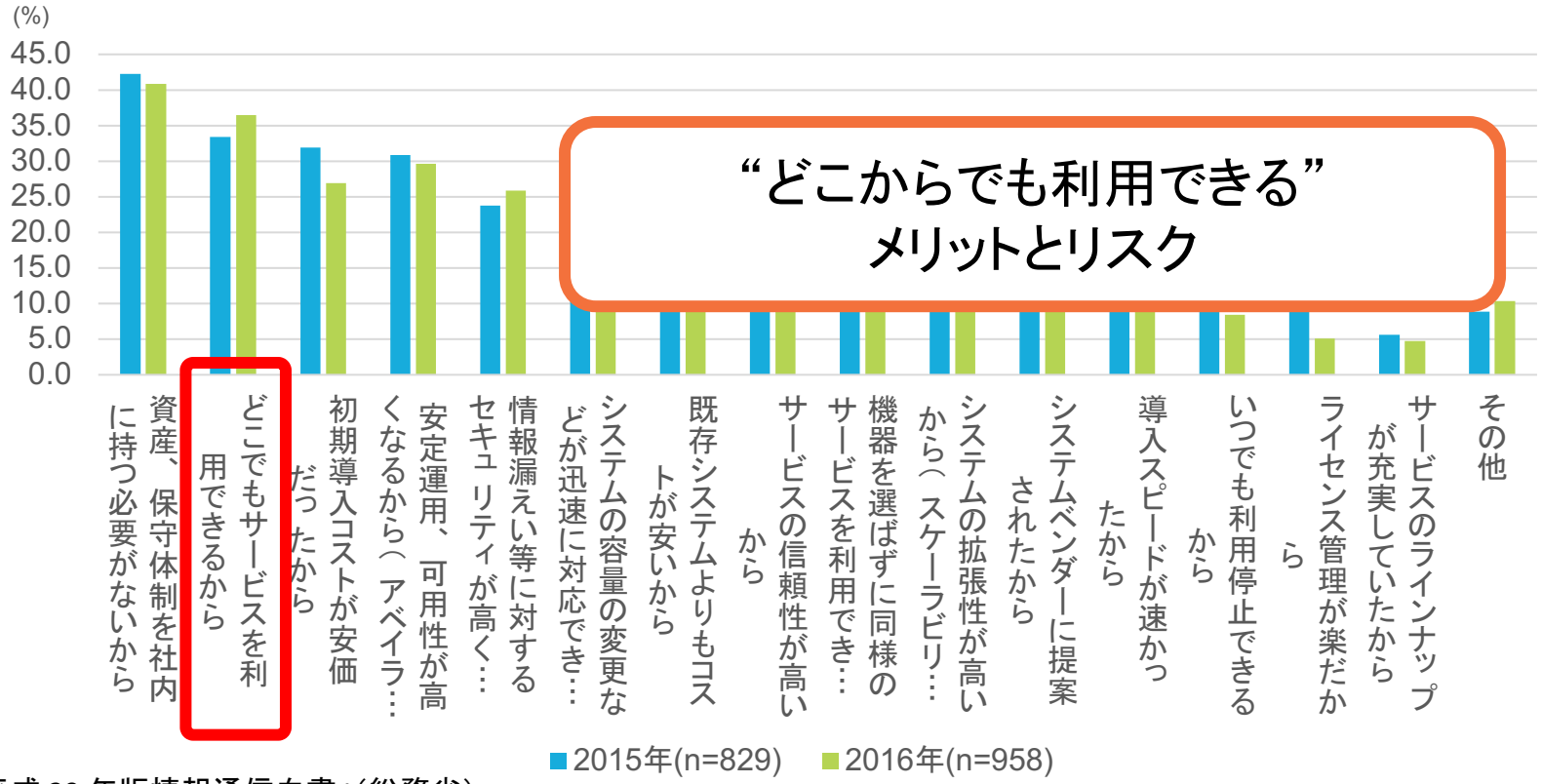
プラットフォーム別責任範囲

On Premises	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

自己責任　ベンダー責任

パブリッククラウド特有のセキュリティとは

クラウド サービスを利用している理由



“どこからでも利用できる”
メリットとリスク

出典:「平成 29 年版情報通信白書」(総務省)
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc262140.html

クラウド特有のインシデントとは

クラウドセキュリティアライアンス（CSA： Cloud Security Alliance）は RSA カンファレンス 2016 において、組織が直面するクラウドコンピューティング関連の脅威上位 12 種をまとめた ″the Treacherous 12″（「12 の危険」）を発表

- **データ流出**
  CSA によれば、通常、クラウドで流出が発生するのは、認証基準が甘い、パスワードの強度が不十分、証明書の管理プロセスがお粗末などのいずれかまたは複数が原因

https://www.digicert.com/blog/threat-landscape-in-the-cloud/

 © 2018, Palo Alto Networks. All Rights Reserved.

クラウドストレージの設定ミスによる情報漏えい事故

■米Verizon、1400万人の顧客情報が誰でもアクセス出来る状態で公開

2017年7月12日、米通信大手Verizonの加入者1400万人の個人情報が、Amazon S3上にURLさえ分かれば、誰でもアクセスしてデータをダウンロードできてしまう状態で公開されていた。

■ダウジョーンズ、400万人の個人情報がアクセス可能な状態で公開

こちらもUpGuardの調査で発覚した内容だ。ダウ・ジョーンズの出版物に対する数百万人の加入者の名前、住所、口座情報、電子メールアドレス、およびクレジットカード番号の最後の4桁の数字がAmazonのS3に保存されており、AWSのIDを保有しているユーザがURLを知っていればアクセス出来る状態で公開されていた。ダウ・ジョーンズは220万人の顧客が影響を受けていると述べているが、UpGuardはこの数字を400万人に近いと推定している。

■米シカゴの有権者180万人あまりの個人情報が一般にアクセスできる状態で露呈

UpGuardによると、データが露呈されていたのは、AWSのAmazon S3バケットが一般にアクセスできる設定になっていたことが原因だった。AWSのデフォルトの設定では、許可されたユーザーしかデータにはアクセスできないという。「もしこの設定を変更する場合は、データの露呈を確実に発見して是正するための対策を講じなければならない」とUpGuardは強調している。

出典　https://news.yahoo.co.jp/byline/ohmototakashi/20171106-00077827/

http://www.itmedia.co.jp/enterprise/articles/1708/21/news054.html

 © 2018, Palo Alto Networks. All Rights Reserved.

“どこからでも利用できる” というリスク

- クラウドの設定ミスが原因で、センシティブなデータが露呈する問題は過去にも見付かっている。UpGuardが引用したGartnerの推計によれば、**情報流出の70～99%は外部からの攻撃によるものではなく、社内の関係者によるITシステムの設定ミスに起因している**という。

- 市場環境として、サービスの無償トライアル機会の提供など、ユーザーが気軽に体験利用できる環境が整っている。また、ユーザー環境では、サービス利用に伴うシステム環境（ブラウザやネットワーク環境など）が、既に整備済みであることや、**導入に伴い必要とされるITの専門性が高くない場合が多い**

- その結果、ユーザー部門が自社のセキュリティポリシーやシステム化方針などへの影響確認を十分に実施せずに単独で導入してしまい、**全社的なシステム統制に影響を及ぼす恐れがある**

出典　https://japan.zdnet.com/article/35063430/3/

 © 2018, Palo Alto Networks. All Rights Reserved.

パロアルトネットワークスのご紹介

パロアルトネットワークスについて

2005年設立、本社米国。初の製品出荷は2007年

世界150カ国以上の42,500を超える企業や組織への導入実績

FY17 の収益は前年度比28%増の18億ドル、業界における急成長

Fortune100の企業の85社超、Global2000の企業の60%が採用

J.D. PowerとTSIAにより受賞したレベルの卓越したサポート体制

グローバルの従業員数：4300人以上

日本法人のパロアルトネットワークス株式会社は、2009年設立

 © 2017, Palo Alto Networks. All Rights Reserved.

パロアルトネットワークス近況

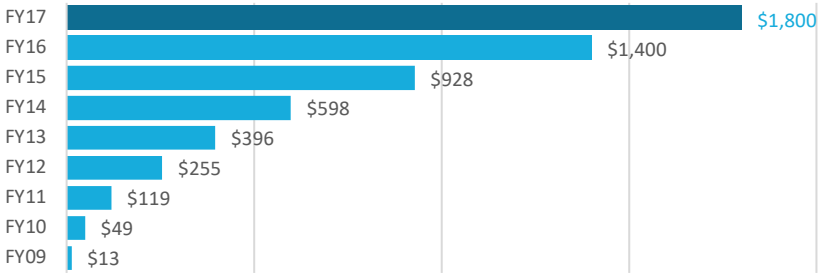
FY17 Q4財務状況

- 収益は前年度比**27%増、5億910万ドル**
- 継続収益ベースで前年度比 **43%、18億ドル増**
- 顧客数**42,500社超**

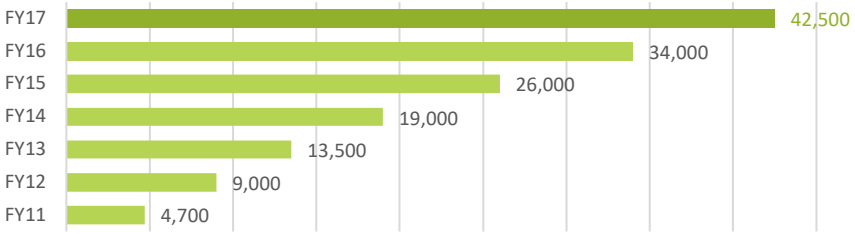
直近の発表

- Evident.io社買収
- Secdo社買収
- Application Framework

収益（百万ドル単位）



法人顧客数



 © 2017, Palo Alto Networks. All Rights Reserved.

エンタープラズグレードの次世代ファイアウォール

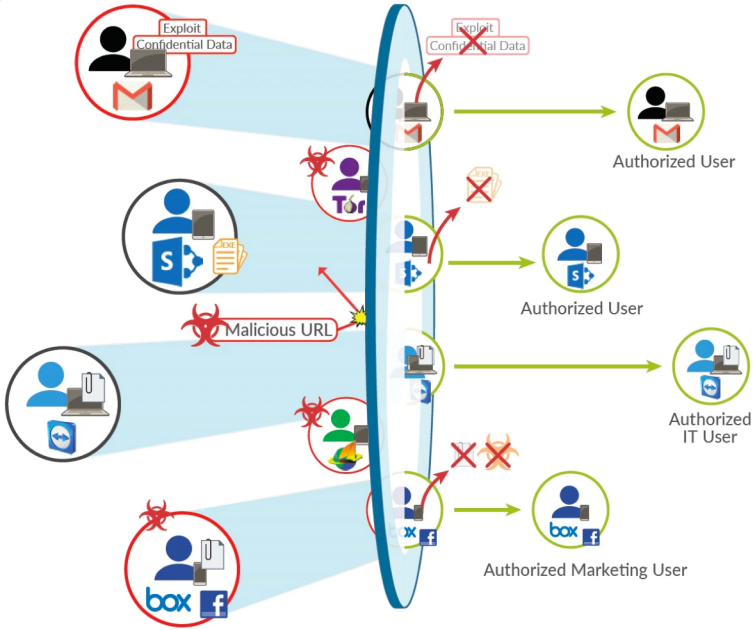
- 最大10倍のパフォーマンス強化
- 最大10倍の復号化パフォーマンス向上
- Front-to-back 冷却
- 最大35倍のSSLセッション増加
- 高いポート密度、柔軟なI / O

 © 2018, Palo Alto Networks. All Rights Reserved.

次世代ファイアウォールとは

これまでのIP・ポートベースの防御ではなくアプリケーション、ユーザー、コンテンツの3つを組み合わせることにより次世代のファイアウォールとして機能します

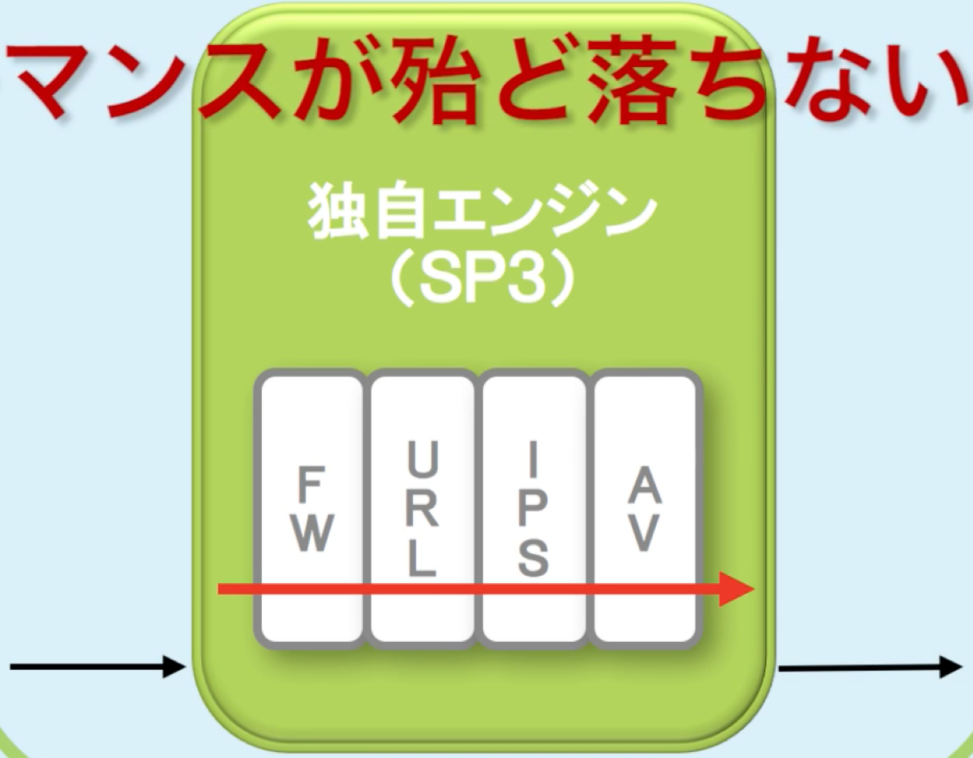
- App-ID
- User-ID
- Content-ID



 © 2018, Palo Alto Networks. All Rights Reserved.

Palo Alto Networksの
次世代ファイアウォール（シングルパス）

パフォーマンスが殆ど落ちない専用設計



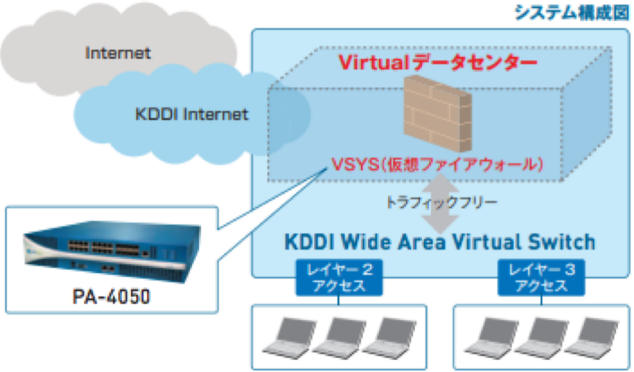
paloalto NETWORKS®

導入事例：KDDI様

顧客ユーザーにアプリケーション制御のセキュア通信を提供
「KDDI Wide Area Virtual Switch」で セキュアなインターネットサービスを実現

*「他のキャリアもKDDI WVSと同様のネットワークサービスを提供してくる中、差別化を図 る目的で『次世代ファイアウォール』を標榜しているPAシリーズが、次世代広域ネットワーク サービスに位置付けているKDDI WVSにふさわしいと考えたからです。具体的には、**アプリケーション、ユーザー、コンテンツを可視化してポリシーベースで制御するとともに脅威を防御するという点を高く評価しました**」（和氣氏）。*

システム構成図



「次世代広域ネットワークサービス『KDDI WVS』の提供において、他社キャリアとの差別化を目的で『次世代ファイアウォール』を標榜しているPAシリーズが最もふさわしいと考えました」

和氣二朗 氏
KDDI 株式会社
ソリューション商品企画本部
ソリューション商品企画部
商品企画１グループ
課長補佐

 © 2018, Palo Alto Networks. All Rights Reserved.

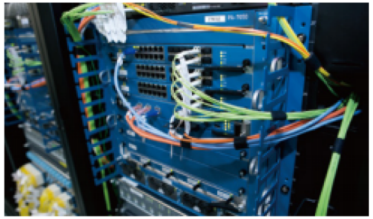
導入事例：筑波大学様

国内で初めてパロアルトネットワークス ハイエンドモデルPA-7050を導入

筑波大学
University of Tsukuba

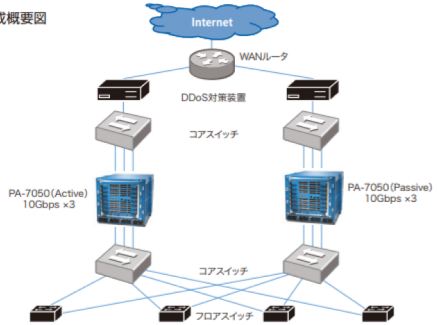
国立大学法人 筑波大学
茨城県つくば市天王台一丁目1番1号
https://www.tsukuba.ac.jp/

筑波大学
情報環境機構学術情報メディアセンター
ネットワーク研究開発部門 准教授
佐藤 聡 氏



「脅威防御を複合的に運用できるファイアウォールであることを考えていましたので、様々な セキュリティ機能を稼動しても十分なスループットが得られ、かつ安定的に運用できることが最大要件でした。」（佐藤氏）。

ネットワーク構成概要図



 © 2018, Palo Alto Networks. All Rights Reserved.

エンタープラズグレードのファイアウォールをそのままクラウドへ

 © 2018, Palo Alto Networks. All Rights Reserved.

あらゆる規模に対応するVM-Seriesラインナップ

Extra small (200M)

ブランチオフィス,マルチテナント用小規模リソース

Small, Medium (2-4G)

ハイブリッドクラウド、セグメンテーション、インターネットゲートウェイ

Large, Extra Large (8-16G)

NFVコンポーネント; 仮想化された100%のデータセンターでワークロードを防御

VM-50

VM-100

VM-200

VM-300

VM-1000-HV

VM-500

VM-700

アプリ識別 200M,脅威防御 100MB, 50K セッション

アプリ識別 2G, 脅威防御 1G, 250K セッション

アプリ識別 4G, 脅威防御2G, 800K セッション

アプリ識別 8G, 脅威防御 4G, 2M セッション

アプリ識別 16G, 8G 脅威防御 8G, 10M セッション

 © 2015, Palo Alto Networks. Confidential and Proprietary.

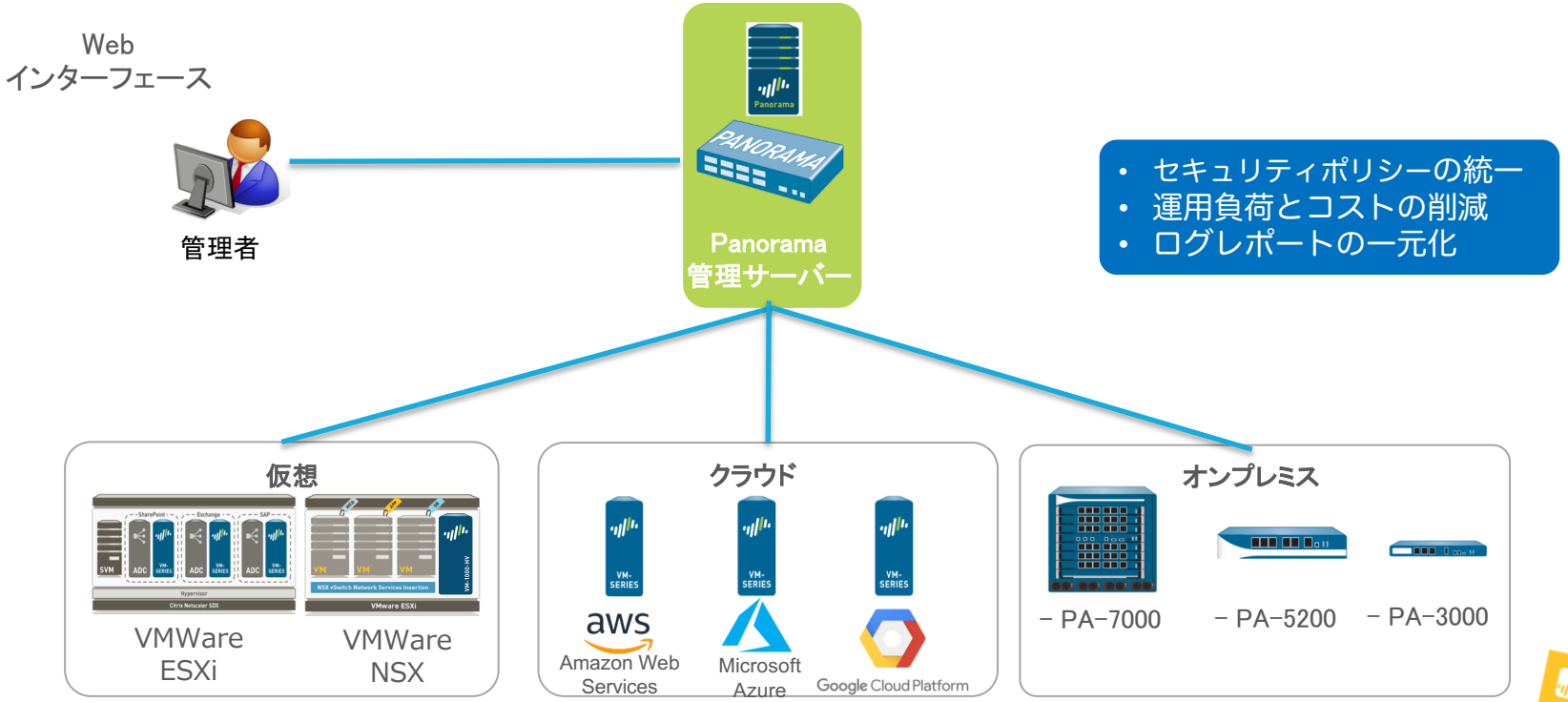
マーケットプレイスから数ステップでVM-Seriesをデプロイ

アニメーションGIFのためオフラインPowerPointのスライドモードで御覧ください。

The contents of this course are only intended for authorized employees & partners of Palo Alto Networks & cannot be shared with anyone who is not entitled under any condition.

Panoramaによるハイブリッド環境を一括監視、管理

複数のパロアルトネットワークス 次世代ファイアウォール（PA）の中央管理と可視化を実現する管理ツール



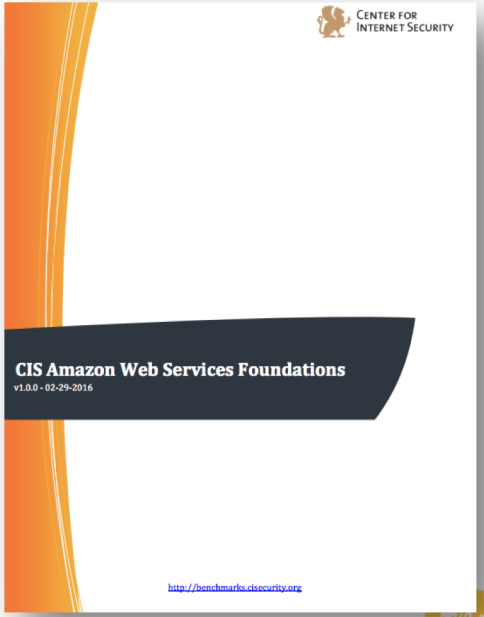
- セキュリティポリシーの統一
- 運用負荷とコストの削減
- ログレポートの一元化

パブリッククラウドセキュリティのガイドライン

CISとは？ベンチマークとは？

“米国のNSA(National Security Agency/国家安全保障局)、DISA(Difense Informaton Systems Agency/国防情報システム局)、NIST(National Institute of Standards and Technology/米国立標準技術研究所)などの米国政府機関と、企業、学術機関などが協力して、インターネット・セキュリティ標準化に取り組む団体の名称”

CIS(Center for Internet Security) - マルチメディア／インターネット事典



 © 2018, Palo Alto Networks. All Rights Reserved.

AWS CIS Foundations Benchmarkチェック項目：IAM

- rootアカウントが利用されていないこと(Level1,Scored)
- コンソールログイン用のパスワードが設定されたIAMユーザにMFAが有効化されていること(Level1,Scored)
- 90日以上利用されていない認証情報は無効化されていること(Level1,Scored)
- アクセスキーが90日以内にローテーションされていること(Level1,Scored)
- rootアカウントのアクセスキーが設定されていないこと(Level1,Scored)
- 秘密の質問が設定されていること(Level1,NotScored)
- IAMポリシーがグループまたはロールにのみ適用されていること(Level1,Scored)
- IAM管理者の権限を、"作成のみ"の担当者(IAMマスター)と"割り当てのみ"の担当者(IAMマネージャー)に分離していること(Level1,Scored)
- 契約者情報が最新化されており、特定の個人のみに紐付いていないこと(Level1,Scored)
- EC2からのAWSリソースアクセスにIAMロールが利用されていること(Level2,NotScored)
- フルコントロール(全リソースおよび全アクション)権限を持つポリシーが作成されていないこと(Level1,Scored)

 © 2018, Palo Alto Networks. All Rights Reserved.

AWS CIS Foundations Benchmarkチェック項目：Logging

- 全RegionでCloudTrailが有効であること(Level1,Scored)
- CloudTrailログファイルの検証が有効化されていること(Level2,Scored)
- CloudTrailログの格納バケットが公開設定となっていないこと(Level1,Scored)
- CloudTrailログがCloudWatch Logsに配信設定されていること(Level1,Scored)
- 全RegionでAWS Configが有効であること(Level1,Scored)
- CloudTrailログの格納バケットがログ有効化されていること(Level1,Scored)
- CloudTrailログがSSE-KMSで暗号化設定されていること(Level2,Scored)
- KMSマスタキーがローテーション設定されていること(Level2,Scored)

 © 2018, Palo Alto Networks. All Rights Reserved.

AWS CIS Foundations Benchmarkチェック項目：Monitoring

- 許可されていないAPIコールに対して、アラーム通知設定されていること(Level1,Scored)
- MFAなしでのAWSマネージメントコンソールログインに対して、アラーム通知設定されていること(Level1,Scored)
- rootアカウントの利用に対して、アラーム通知設定されていること(Level1,Scored)
- IAMポリシーの変更に対して、アラーム通知設定されていること(Level1,Scored)
- CloudTrail設定の変更に対して、アラーム通知設定されていること(Level1,Scored)
- AWSマネージメントコンソールのログイン失敗に対して、アラーム通知設定されていること(Level2,Scored)
- KMSマスターキーの無効化またはスケジュール削除に対して、アラーム通知設定されていること(Level2,Scored)
- S3バケットポリシー、 Security Group、 Network ACL、 Internet Gateway変更に対して、アラーム通知設定されていること(Level1,Scored)
- VPC設定(新規作成、削除やVPC Peering, Classi Link等)の変更に対して、アラーム通知設定されていること(Level1,Scored)

 © 2018, Palo Alto Networks. All Rights Reserved.

AWS CIS Foundations Benchmarkチェック項目：Networking

- Security Groupにて、0.0.0.0/0からport 22(SSH)への接続が許可されていないこと(Level1,Scored)
- Security Groupにて、0.0.0.0/0からport 3389(RDP)への接続が許可されていないこと(Level1,Scored)
- 利用可能な全てのRegionにおいて、VPC Flow Logsが有効化されていること(Level2,Scored)
- Default Security Groupが全ての通信を許可していないこと(Level2,Scored)
- VPC Peering越しのルーティングは必要最低限に絞られていること(Level2,NotScored)

 © 2018, Palo Alto Networks. All Rights Reserved.

ベンチマークとは？

AWS CIS Foundations Benchmark

- ベストプラクティスに従った適切なセキュリティ設定をAWSより提示
- 標準化されたシステム設定により、リスクを低減し、システム監査を行うことができる
- PCIDSSやFedRAMP等の各種セキュリティ監査エコシステムにも適用できる
- ただしすべてを理解し正しく実施するにはAWSの各種サービスに精通し、かつセキュリティ・コンプライアンスを理解し監査、レポートするのは事情に難しい

 © 2018, Palo Alto Networks. All Rights Reserved.

APIベースのセキュリティ、コンプライアンス Evident.ioとは

APIベースのセキュリティ、コンプライアンスソリューション マーケットリーダー、EVIDENT.IOを買収

継続的かつリアルタイム

マルチクラウド対応

ワンクリックでレポート作成

カスタマイゼーションによる柔軟な企業ポリシーへの対応

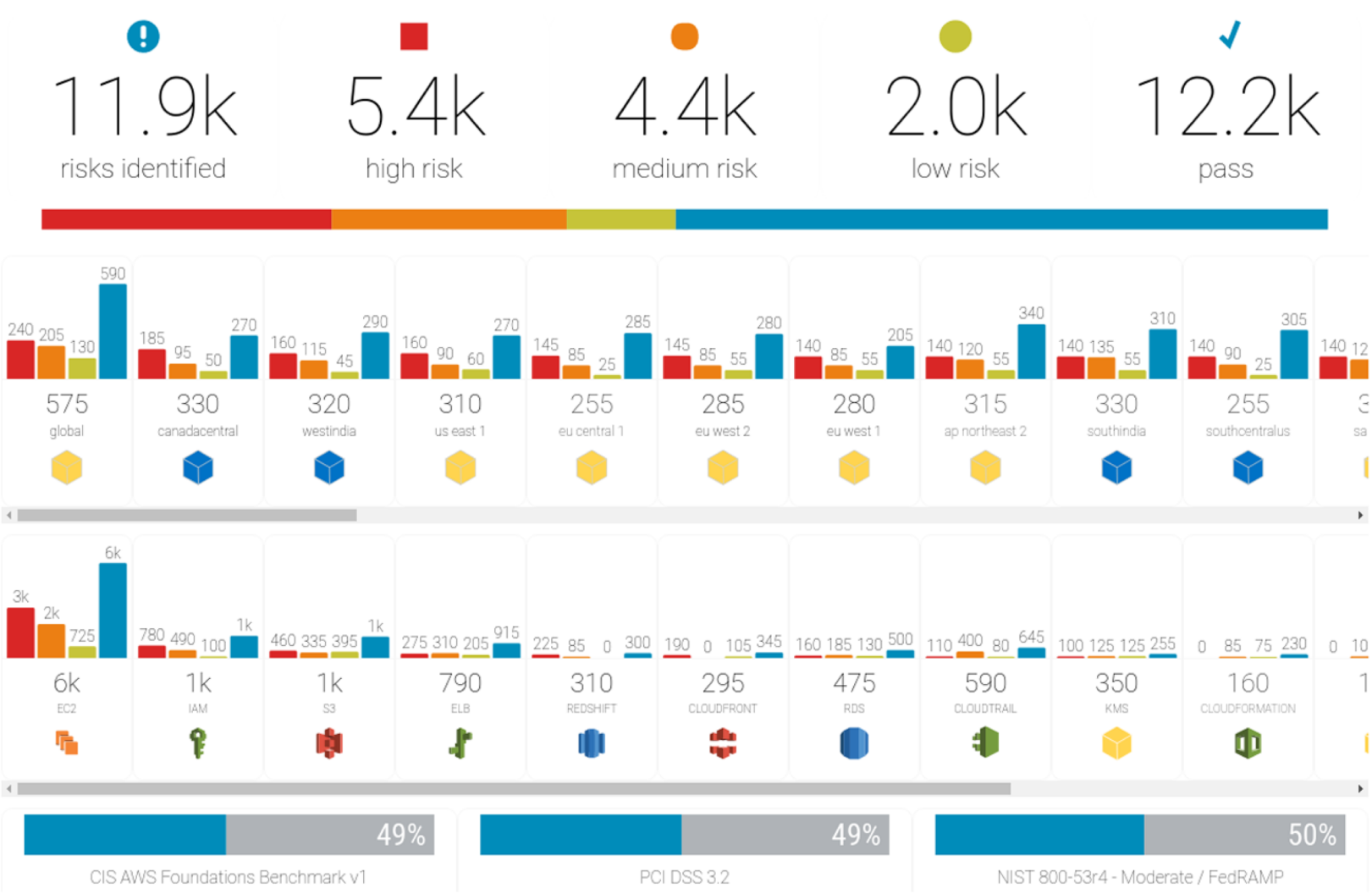
エージェントは不要

コンプライアンス、DevOps、SecOps対応

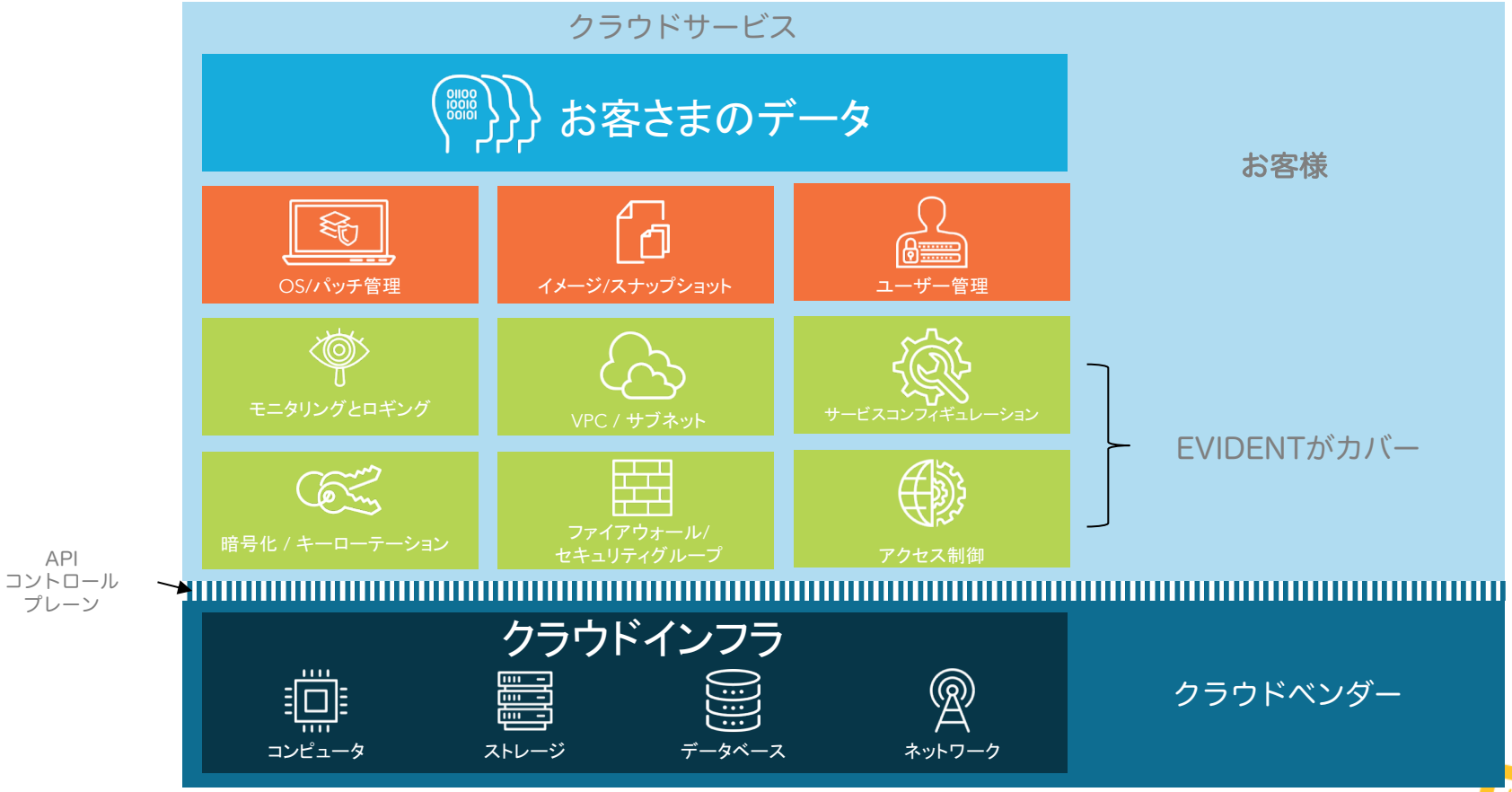
既存パロアルトネットワークス製品との完全統合

We expect to complete the acquisition of Evident.io, Inc. in our third fiscal quarter, upon satisfaction of customary closing conditions contained in the definitive agreement.

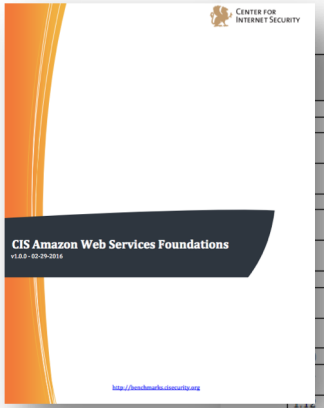
 © 2018, Palo Alto Networks. All Rights Reserved.


11.9k
risks identified
5.4k
high risk
4.4k
medium risk
2.0k
low risk
12.2k
pass
240 205 130 590
575
global
185 95 50 270
330
canadacentral
160 115 45 290
320
westindia
160 90 60 270
310
us east 1
145 85 25 285
255
eu central 1
145 85 55 280
285
eu west 2
140 85 55 205
280
eu west 1
140 120 55 340
315
ap northeast 2
140 135 55 310
330
southindia
140 90 25 305
255
southcentralus
3k 2k 725 6k
6k
EC2
780 490 100 1k
1k
IAM
460 335 395 1k
1k
S3
275 310 205 915
790
ELB
225 85 0 300
310
REDSHIFT
190 0 105 345
295
CLOUDFRONT
160 185 130 500
475
RDS
110 400 80 645
590
CLOUDTRAIL
100 125 125 255
350
KMS
0 85 75 230
160
CLOUDFORMATION
49%
CIS AWS Foundations Benchmark v1
49%
PCI DSS 3.2
50%
NIST 800-53r4 - Moderate / FedRAMP

クラウドセキュリティの責任範囲

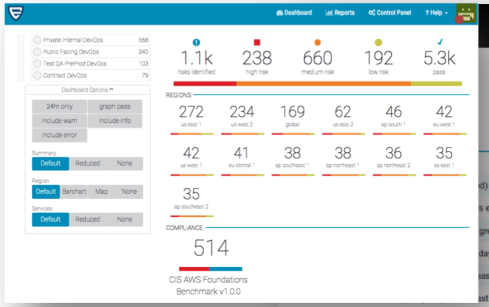


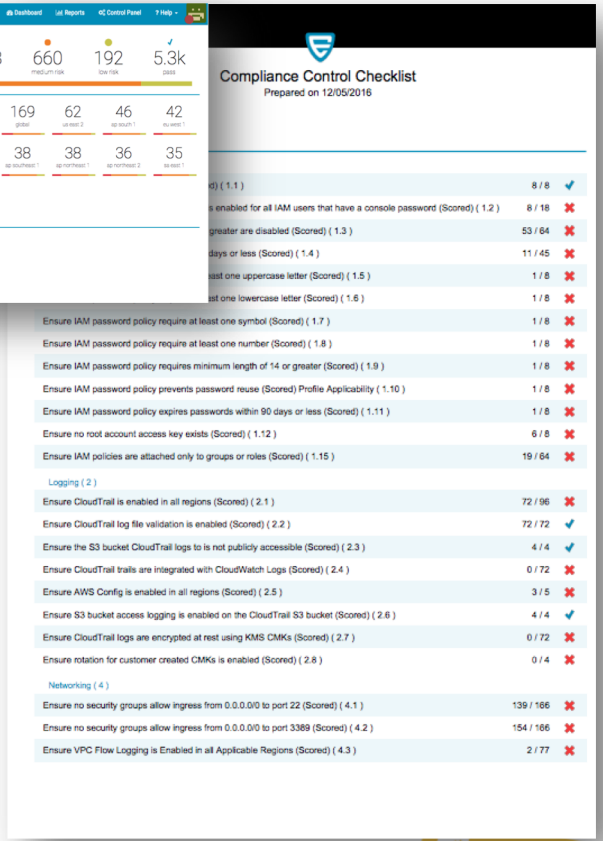
1クリックでCIS AWS FOUNDATIONS BENCHMARKを作成



	Control	Set Correctly Yes	Set Correctly No
	Identity and Access Management		
	Avoid the use of the "root" account (Not Scored)	☐	☐
	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a password (Scored)	☐	☐
	Ensure credentials unused for 90 days or greater are disabled (Scored)	☐	☐
	Ensure access keys are rotated every 90 days or less (Scored)	☐	☐
	Ensure IAM password policy requires at least one uppercase letter (Scored)	☐	☐
	Ensure IAM password policy require at least one lowercase letter (Scored)	☐	☐
	Ensure IAM password policy require at least one symbol (Scored)	☐	☐
	Ensure IAM password policy require at least one number (Scored)	☐	☐
	Ensure IAM password policy requires minimum length of 14 or greater (Scored)	☐	☐
	Ensure IAM password policy prevents password reuse (Scored)	☐	☐
	Ensure IAM password policy expires passwords within 90 days or less (Scored)	☐	☐
	Ensure no root account access key exists (Scored)	☐	☐
1.13	Ensure hardware MFA is enabled for the "root" account (Scored)	☐	☐
1.14	Ensure security questions are registered in the AWS account (Not Scored)	☐	☐
1.15	Ensure IAM policies are attached only to groups or roles (Scored)	☐	☐
2	**Logging**		
2.1	Ensure CloudTrail is enabled in all regions (Scored)	☐	☐
2.2	Ensure CloudTrail log file validation is enabled (Scored)	☐	☐
2.3	Ensure the S3 bucket CloudTrail logs to is not publicly accessible (Scored)	☐	☐
2.4	Ensure CloudTrail trails are integrated with CloudWatch Logs (Scored)	☐	☐
2.5	Ensure AWS Config is enabled in all regions (Scored)	☐	☐
2.6	Ensure S3 Bucket Access Logging is enabled for all buckets (Scored)	☐	☐
2.7	Ensure CloudTrail logs are encrypted at rest using KMS CMKs (Scored)	☐	☐
2.8	Ensure rotation for customer created CMKs is enabled (Scored)	☐	☐
3	**Monitoring**		
3.1	Ensure a log metric filter and alarm exist for unauthorized API calls (Scored)	☐	☐
3.2	Ensure a log metric filter and alarm exist for Management Console sign-in without MFA (Scored)	☐	☐

86 | Page





paloalto NETWORKS

Dashboard | Reports | Control Panel | ? Help

COMPLIANCE CONTROL CHECKLIST

CIS AWS Foundations Benchmark v1.0.0

Identity and Access Management (1)

1.1	Avoid the use of the "root" account (Scored)	8/8	✓
1.2	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)	8/18	✗
1.3	Ensure credentials unused for 90 days or greater are disabled (Scored)	53/64	✗
1.4	Ensure access keys are rotated every 90 days or less (Scored)	11/45	✗
1.5	Ensure IAM password policy requires at least one uppercase letter (Scored)	1/8	✗
1.6	Ensure IAM password policy require at least one lowercase letter (Scored)	1/8	✗
1.7	Ensure IAM password policy require at least one symbol (Scored)	1/8	✗
1.8	Ensure IAM password policy require at least one number (Scored)	1/8	✗
1.9	Ensure IAM password policy requires minimum length of 14 or greater (Scored)	1/8	✗
1.10	Ensure IAM password policy prevents password reuse (Scored) Profile Applicability	1/8	✗
1.11	Ensure IAM password policy expires passwords within 90 days or less (Scored)	1/8	✗
1.12	Ensure no root account access key exists (Scored)	6/8	✗
1.15	Ensure IAM policies are attached only to groups or roles (Scored)	19/64	✗

Logging (2)

2.1	Ensure CloudTrail is enabled in all regions (Scored)	72/96	✗
2.2	Ensure CloudTrail log file validation is enabled (Scored)	72/72	✓
2.3	Ensure the S3 bucket CloudTrail logs to is not publicly accessible (Scored)	4/4	✓
2.4	Ensure CloudTrail trails are integrated with CloudWatch Logs (Scored)	0/72	✗
2.5	Ensure AWS Config is enabled in all regions (Scored)	3/5	✗
2.6	Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket (Scored)	4/4	✓
2.7	Ensure CloudTrail logs are encrypted at rest using KMS CMKs (Scored)	0/72	✗
2.8	Ensure rotation for customer created CMKs is enabled (Scored)	0/4	✗

Networking (4)

paloalto NETWORKS

継続的なコンプライアンスレポート

クラウド環境は常に変わるため、常にコンプライアンス監査できる環境が必要です

監査の自動化、ワンクリックでレポート作成

クリック一つで、幾つものクラウド上のサービスからデータを取得し、コンプライアンスチェック項目とマッピングします。

クラウドアカウントによるコンプライアンス

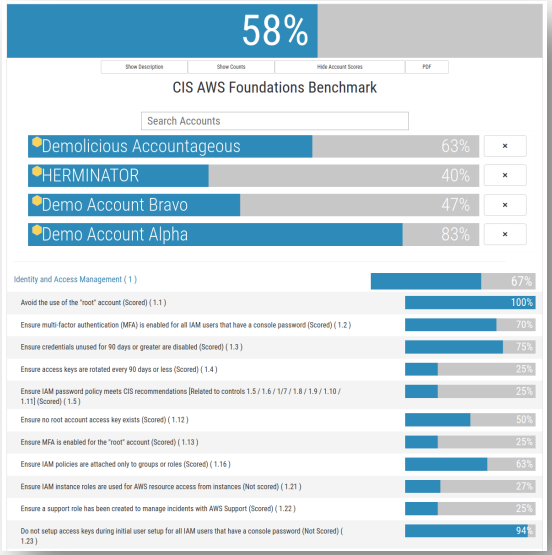
組織内全てのAWSもしくはAzureアカウントの行動を把握し、現在の状況を把握できます

クリック一つで問題を修正

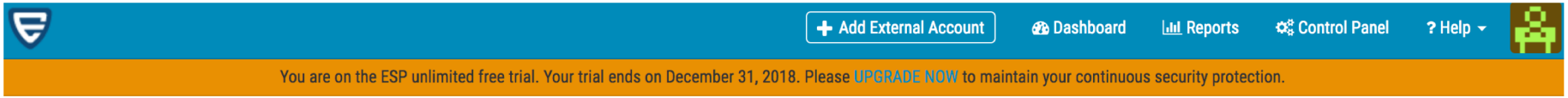
チームメンバーはコンプライアンスに違反する行動を把握し、それを素早く修正することができます

カスタムコンプライアンスレポート作成

ESP内で作成された、メンバーにより作成された組織、社内コンプライアンス標準、カスタムコンプライアンスレポートなど、どれが一番自分たちにとって重要なのかをチェックし判断することができます



GDPRシグネイチャーによりチェックを自動化



General Data Protection Regulation - GDPR

Expand Accounts

This report helps to define recommended AWS services to be correctly configured to protect personal data against accidental or unlawful destruction; or accidental loss, alteration, unauthorized use, unauthorized modification, disclosure or access; and against all other illegal forms of processing.

This report uses the framework based on the AWS recommended best practices for processing GDPR workloads; reference below. Each organization that falls under GDPR must define controls and monitoring for audit.

Reference links used in this report and for additional information:

Navigating GDPR Compliance on AWS

AWS General Data Protection Regulation (GDPR) Center

Art. 25 GDPR Data protection by design and by default

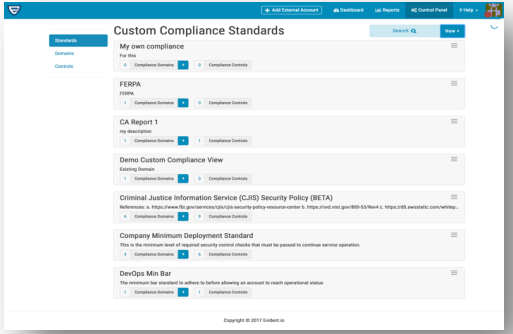
Art. 32 GDPR Security of processing

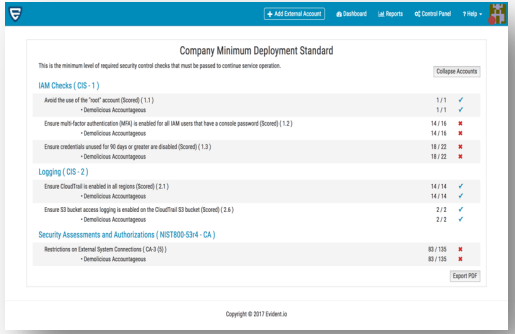
Art. 35 GDPR Data protection impact assessment

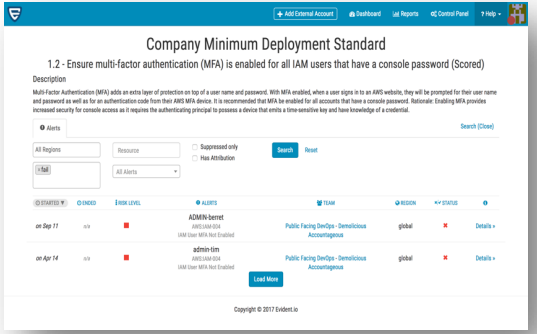
Access Control (GDPR-AC)

Limit Access (GDPR-AC-001)	3 / 5	✖
Multi-Factor-Authentication (MFA) (GDPR-AC-002)	0 / 3	✖
Fine granular access to objects in Amazon S3 Buckets (GDPR-AC-003)	154 / 154	✓
Fine granular access to objects in Amazon SQS (GDPR-AC-004)	0 / 0	✓
Fine granular access to objects in Amazon SNS (GDPR-AC-005)	1 / 1	✓

カスタムコンプライアンスレポート



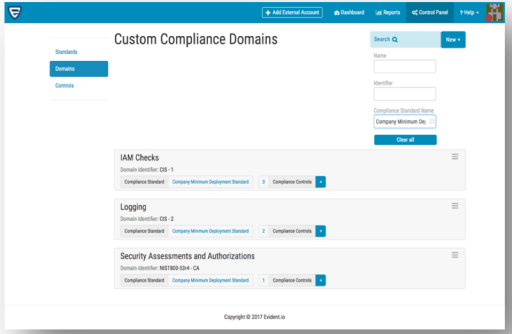


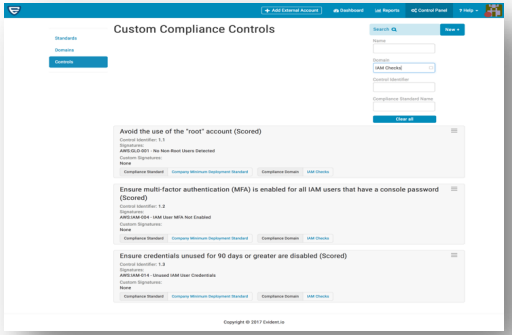


管理フレームワークをカスタマイズ可能

PCIやNISTなどからコピーして、それを元に新しいフレームワークを作成

GUIベースウィザードで簡単にセットアップ、コンフィギュレーション





製品概要

Evident.ioが提供する2つの機能:

Evident セキュリティ プラットフォーム

パブリッククラウド環境の継続的なモニターによるパブリッククラウドインフラのセキュリティ確保

- モニタリング
- 警告
- 可視化
- 修復手順の提示
- ユーザー属性(Attribution)

コンプライアンス

パブリッククラウド上のアカウントが規制フレームワークに準拠しているかを解析、レポート

関連する法規に準拠しているかを訴訟、規範に基いたガイダンスを提供

クラウドセキュリティの継続的な監視

多種多様なサービスや常に拡張するクラウド環境に対し、統合的な管理インターフェース提供により管理リスクを軽減

APIベースのアーキテクチャ

IPベースのソリューションでは常にIPが変わるクラウド環境には対応できません。ESPはAWS、AzureのAPI経由でデータにアクセスし、継続的なセキュリティ維持、管理を提供します。

エージェント不要=デプロイメントの整合性を確保

クラウド環境に簡単にアクセス可能 – AWSとマイクロソフト Azureの全てのサービス、リージョン、アカウントをカバー

すべての情報を包括的に可視化

全てのクラウドの状況とユーザー行動を把握 – セキュリティポリシーに対する監視ルールをカスタマイズ可能

リアルタイムかつストリーミングベースで情報を取得

ESP for Azureでは設定が変更されると同時にその情報がESPに送信されます。ESP for AWSは2018年前半に対応を予定しています。APIへのプッシュは最短5分間隔で実施されます。

セキュリティの脅威に対して対応を完全自動化

クラウドにより、人による解析よりも多くのデータを提供可能

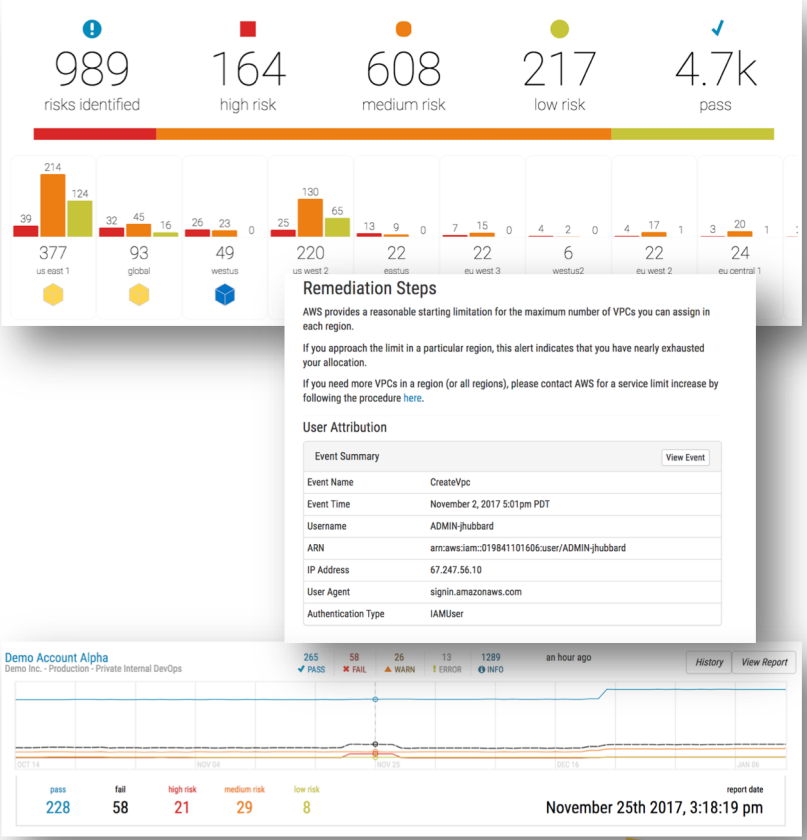
優先度を提示
予め設定(お客様自身でカスタマイズ可能)された値によりリスクを判定し、チーム内で何を最初に対処すべきかを判断できます

チェックしたいリスクをカスタマイズして表示
チーム別、地域別、サービス別、コンプライアンス、時系列などステータスを自由にカスタマイズしてコンソールを作成することが可能

ワンクリックでセキュリティとコンプライアンスレポートを作成
対応手順や詳細情報をクリックひとつでレポートとして提供可能

脅威トレンドを把握
継続的に状況をチェックすることにより、何がリスクなのかを把握し、常にコンプライアンスプロファイルを変更します。またクリック一つでそれらの履歴をレポートとして受け取ることができます。

迅速な解決
モニタリング、アセスメント、修復手順の開示を自動化することにより、リスクを大幅に軽減し、チームは他のプロジェクトに専念することができます。



Devopsチームにセキュリティを

サイロ化されたセキュリティはDevOpsでの開発-運用反復プロセスの妨げになります

ライフサイクル全般に継続的なセキュリティを

開発 – QA – 本番 というプロセスに対し、 ESPによるセキュリティ監視、管理を提供により、イノベーションのペースを落とすことなくセキュリティを担保することができます

カスタマイズ可能なアラート

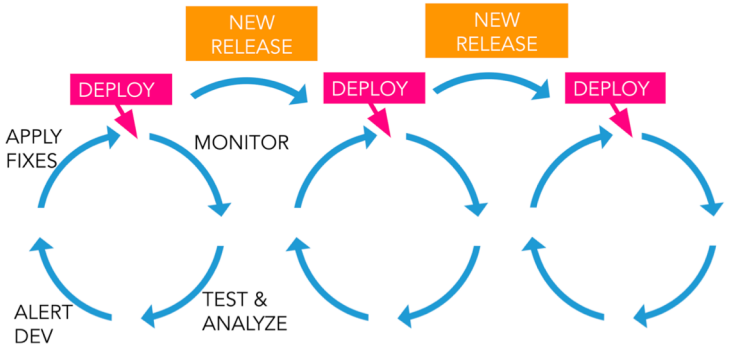
ユーザーもしくはシステムに対して、ツールにより簡単かつ直感的にアラート内容をカスタマイズできます

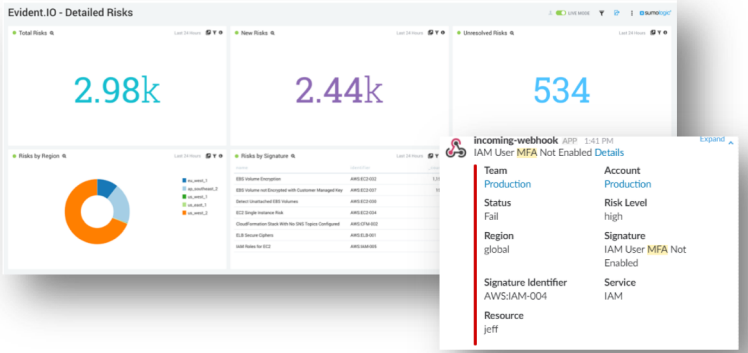
運用状況を詳細に把握

誰が、何を、いつ、どのように操作したかを「危険なユーザー行動」として把握することができます

復旧手順を自動化

AWS LambdaもしくはAzureの機能を利用したワークフローをキックし、エクスプロイト攻撃に対して自動的に修復を行います



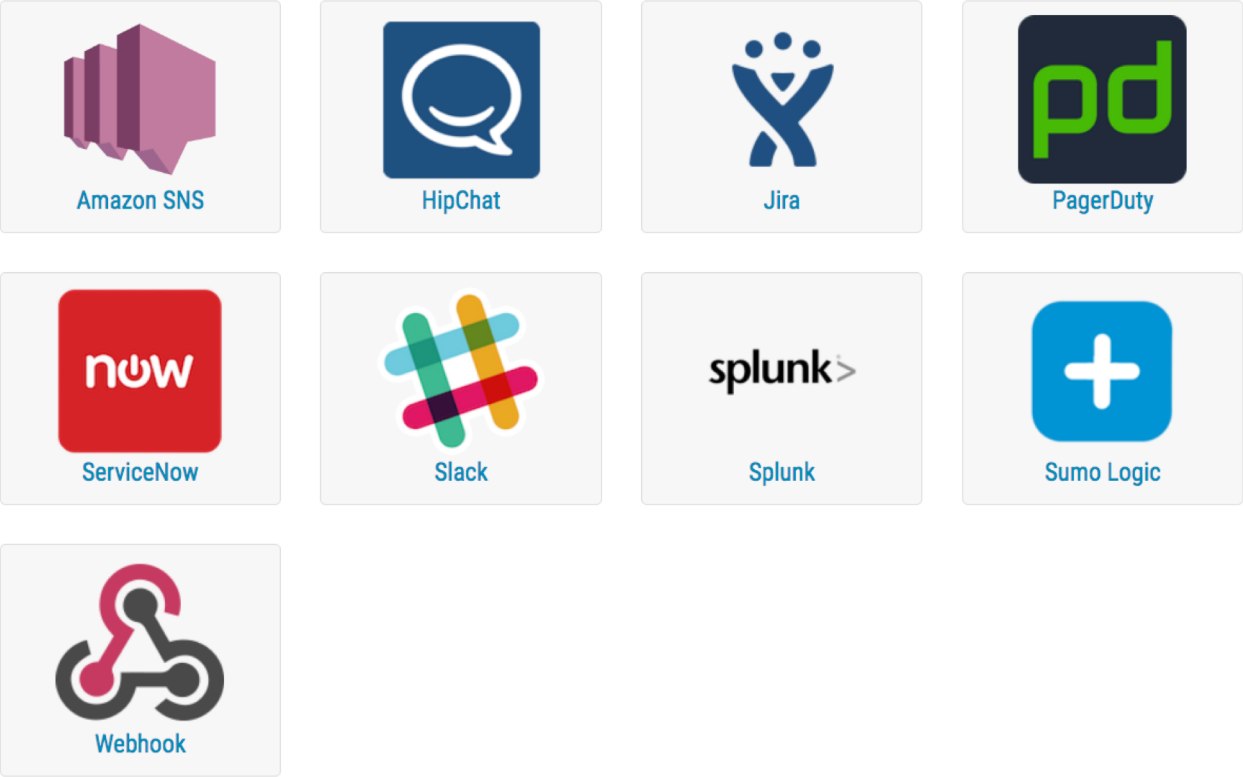


sumologic splunk> servicenow JIRA slack HipChat pagerduty OpsGenie

現在利用中のグループツールと統合

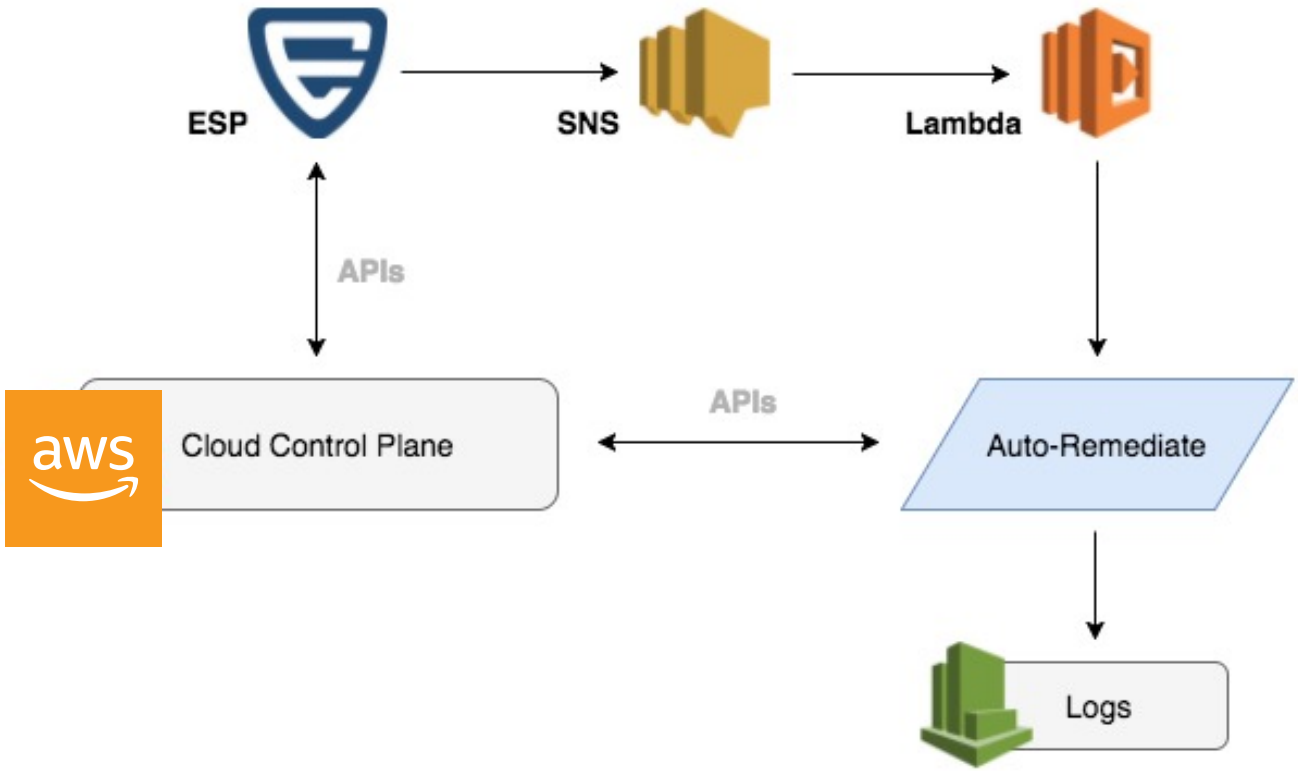
paloalto NETWORKS

今利用中のツールと統合可能



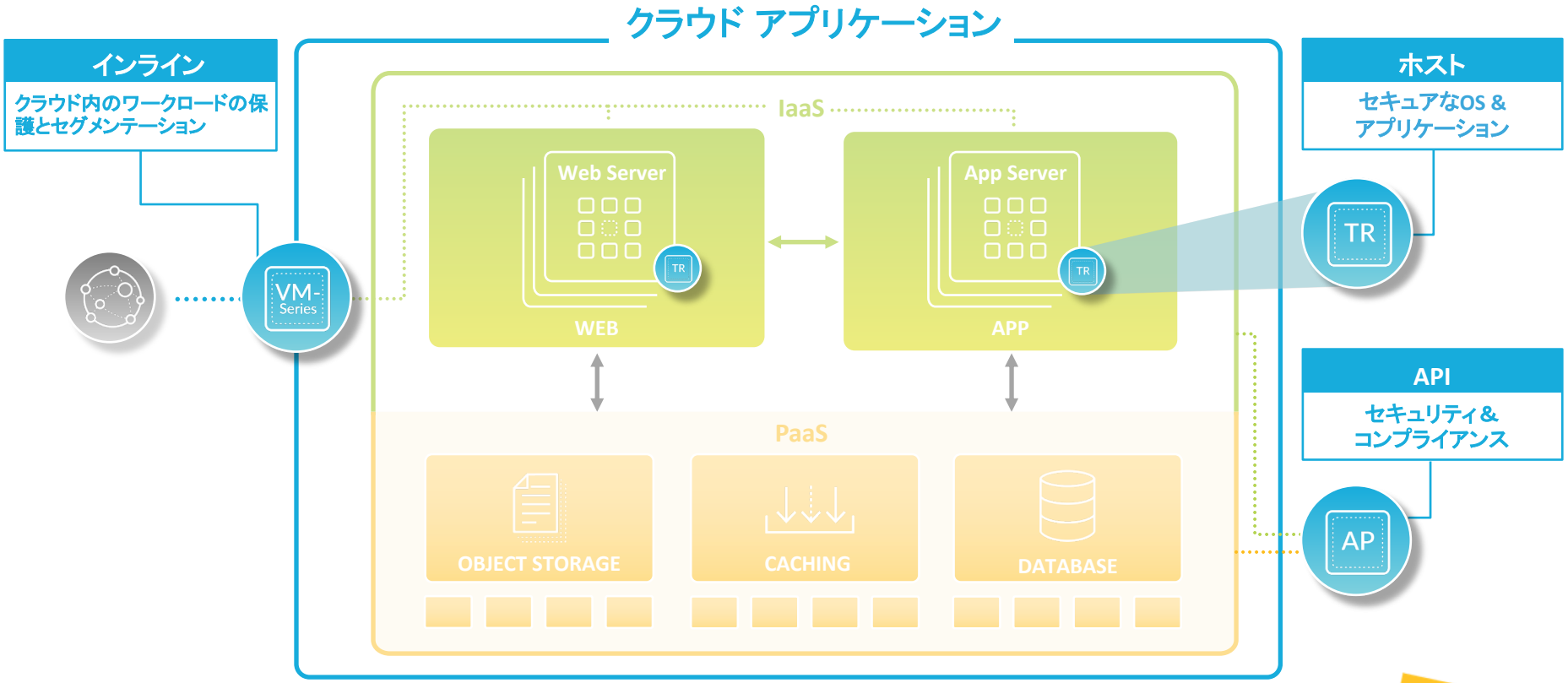
 © 2018, Palo Alto Networks. All Rights Reserved.

AWS LAMBDAによる問題解決フローの自動化例



パロアルトネットワークスのクラウド戦略

パロアルトネットワークスクラウド戦略とは

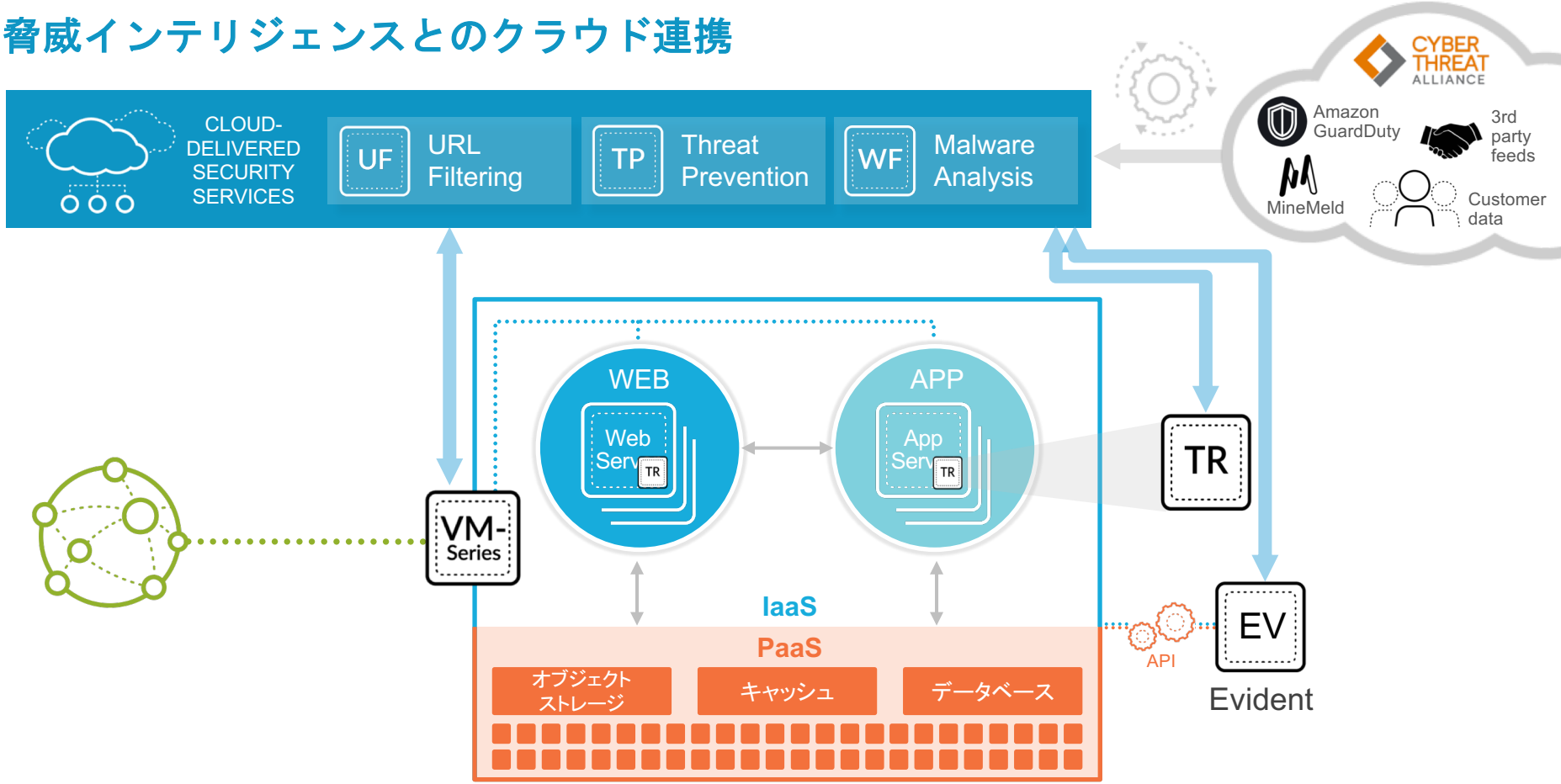


ハイブリッドクラウド

	Amazon Web Services	Microsoft Azure	Google Cloud Platform	
VM-Series	ENHANCED	ENHANCED	NEW	マイクロセグメンテーションによるセキュリティ強化
EV Evident	ENHANCED	NEW		継続性のあるセキュリティ対策とコンプライアンス
TR Traps "End point Security"	ENHANCED	ENHANCED	NEW	セキュアなOSとアプリケーション利用の安全性向上

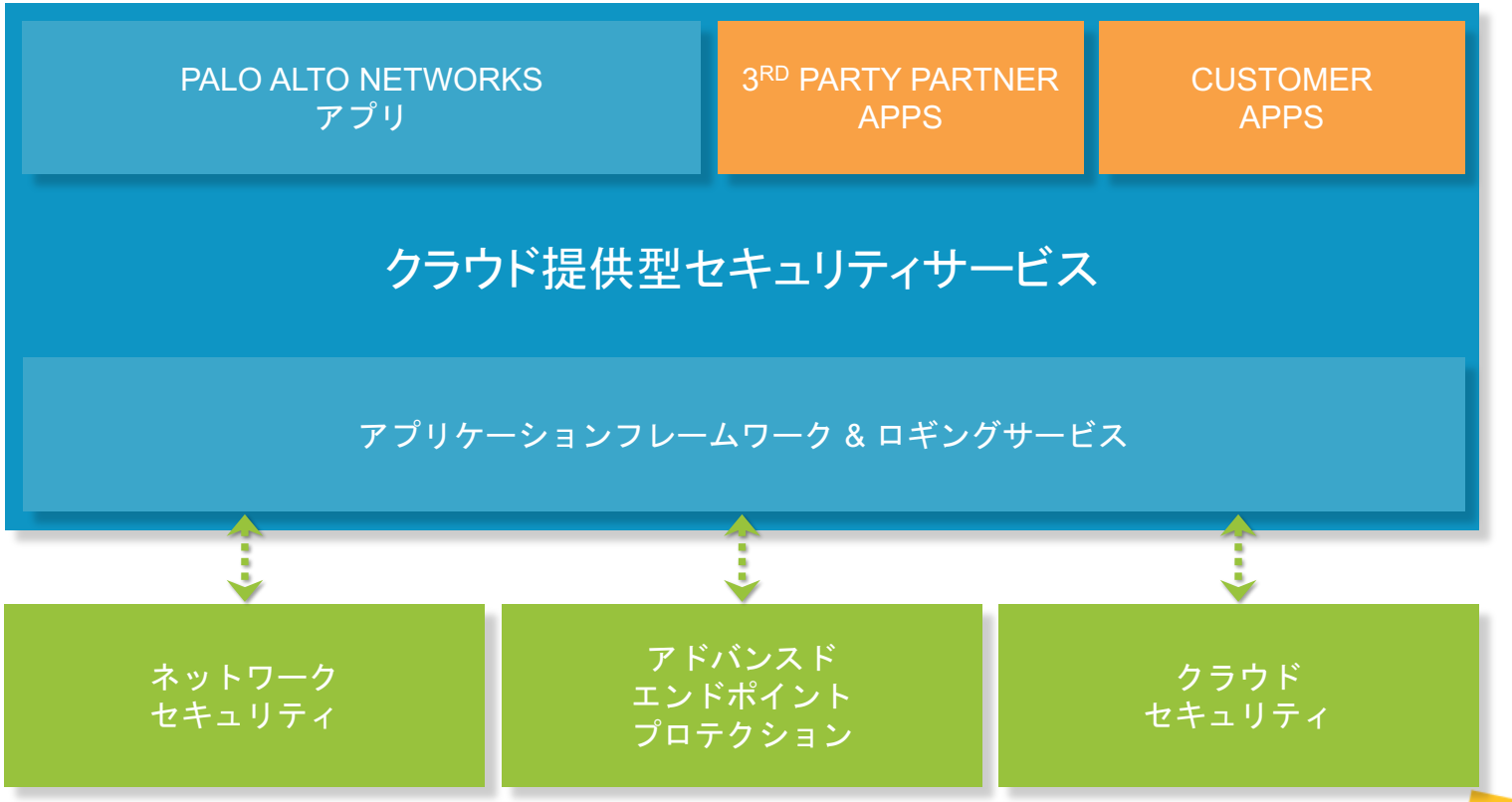
 © 2017, Palo Alto Networks. All Rights Reserved.

脅威インテリジェンスとのクラウド連携



 © 2018, Palo Alto Networks. Confidential and Proprietary.

脅威インテリジェンスをプラットフォームとして提供

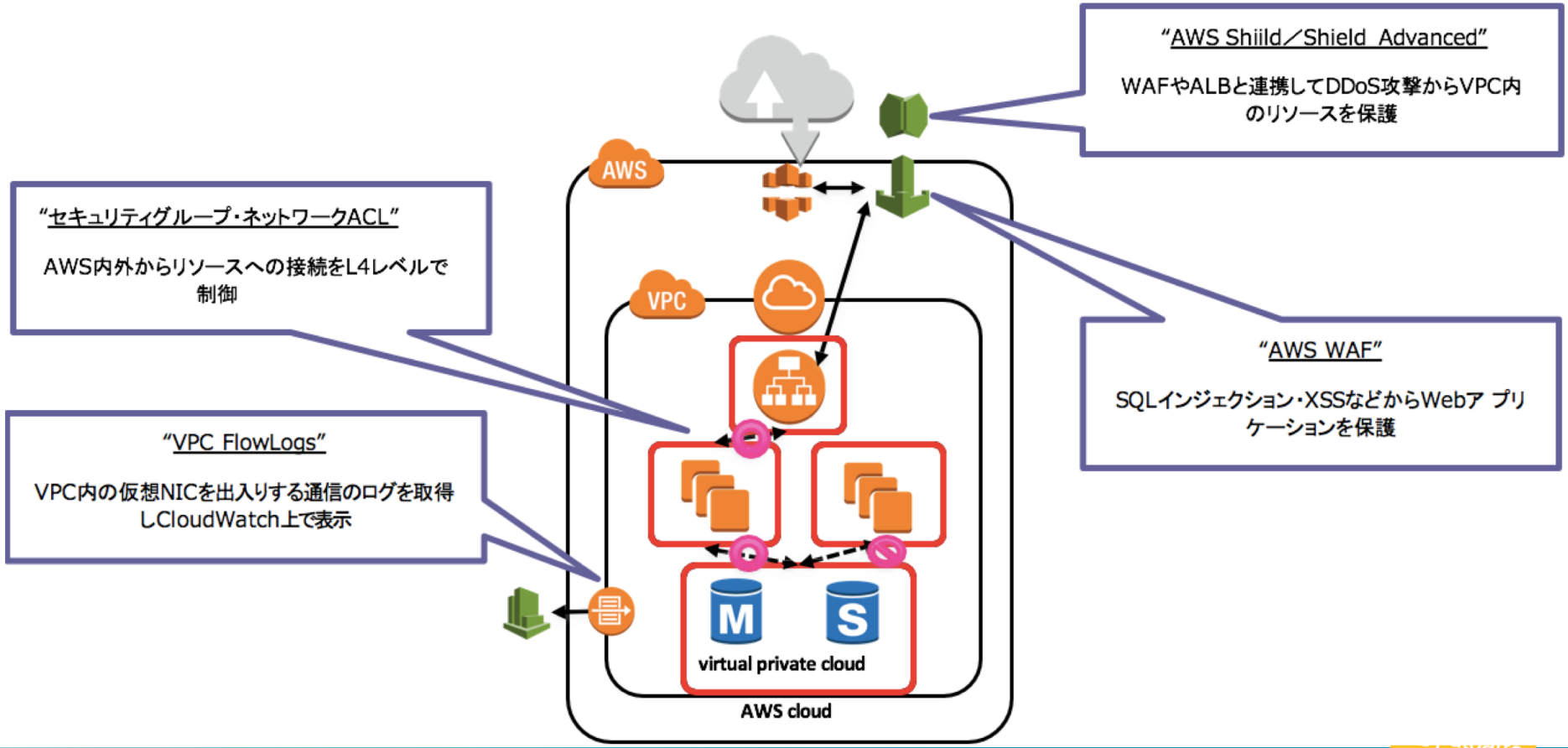


 © 2018, Palo Alto Networks. All Rights Reserved.

paloalto
NETWORKS®

AWSネイティブセキュリティ

AWSのネットワークセキュリティ関連サービス



 © 2018, Palo Alto Networks. All Rights Reserved.

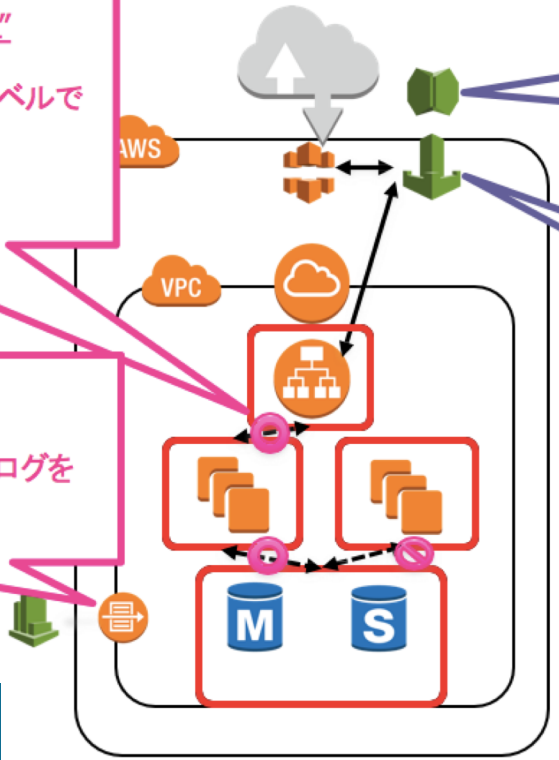
AWSのネットワークセキュリティ関連サービス

"セキュリティグループ・ネットワークACL"

AWS内外からリソースへの接続をL4レベルで制御

"AWS Shiild／Shield Advanced"

WAFやALBと連携してDDoS攻撃からVPC内のリソースを保護



"VPC FlowLogs"

VPC内の仮想NICを出入りする通信のログを取得しCloudWatch上で表示

"AWS WAF"

SQLインジェクション・XSSなどからWebアプリケーションを保護

VPCのセキュリティ対策に必要なもの

インフラストラクチャの高いセキュリティ

 © 2017, Palo Alto Networks. All Rights Reserved.

セキュリティグループ・ネットワークACL

sg-[redacted]

要約 | インバウンドルール | アウトバウンドルール | タグ

編集

タイプ	プロトコル	ポート範囲	送信元
SSH (22)	TCP (6)	22	0.0.0.0/0
SSH (22)	TCP (6)	22	::/0
SMTP (25)	TCP (6)	25	0.0.0.0/0
SMTP (25)	TCP (6)	25	::/0
IMAPS (993)	TCP (6)	993	10.20.30.40/30
MySQL/Aurora (3306)	TCP (6)	3306	sg-[redacted]
HTTP* (8080)	TCP (6)	8080	200.100.10.1/32

acl-[redacted]

要約 | インバウンドルール | アウトバウンドルール | サブネットの関連付け | タグ

インバウンドトラフィックを許可します。ネットワーク ACL はステートレスであるため、インバウンドおよびアウトバウンドルールを作成する必要があります。

編集

View: All rules

ルール #	タイプ	プロトコル	ポート範囲	送信元	許可/拒否
100	すべての トラフィック	すべて	すべて	0.0.0.0/0	許可
*	すべての トラフィック	すべて	すべて	0.0.0.0/0	拒否

- 宛先ポート・接続元IPアドレスによるポリシー定義
- セキュリティグループはインスタンスごと、ネットワークACLはサブネット毎 にルールを関連付けて適用
- 接続元アドレスはグループ化して管理することは不可

VPC FlowLogs

イベントのフィルター

	時間 (UTC +00:00)	メッセージ
	2016-08-20	
▸	06:52:15	2 483162472715 eni-89c1e4c2 117.21.191.2 192.168.1.59 6000 8080 6 1 40 1471675935 1471675986 ACCEPT OK
▸	06:53:11	2 483162472715 eni-89c1e4c2 130.193.122.52 192.168.1.59 42725 23 6 1 40 1471675991 1471676046 ACCEPT OK
▾	06:58:14	2 483162472715 eni-89c1e4c2 190.52.165.194 192.168.1.59 45412 23 6 4 208 1471676294 1471676346 ACCEPT OK
2 483162472715 eni-89c1e4c2 190.52.165.194 192.168.1.59 45412 23 6 4 208 1471676294 1471676346 ACCEPT OK		
▸	06:58:14	2 483162472715 eni-89c1e4c2 117.212.100.95 192.168.1.59 65322 23 6 1 40 1471676294 1471676346 ACCEPT OK
▸	06:59:06	2 483162472715 eni-89c1e4c2 185.40.4.123 192.168.1.59 5068 5060 17 1 432 1471676346 1471676406 ACCEPT OK
▸	06:59:06	2 483162472715 eni-89c1e4c2 184.105.247.235 192.168.1.59 18485 5351 17 1 30 1471676346 1471676406 ACCEPT OK
▸	06:59:06	2 483162472715 eni-89c1e4c2 187.36.41.57 192.168.1.59 48583 23 6 3 156 1471676346 1471676466 ACCEPT OK
▸	07:00:07	2 483162472715 eni-89c1e4c2 67.220.57.85 192.168.1.59 3977 23 6 2 120 1471676407 1471676466 ACCEPT OK
▸	07:02:07	2 483162472715 eni-89c1e4c2 219.71.212.96 192.168.1.59 47255 23 6 2 120 1471676527 1471676586 ACCEPT OK
▸	07:03:11	2 483162472715 eni-89c1e4c2 125.105.214.128 192.168.1.59 13571 3306 6 1 40 1471676591 1471676646 ACCEPT OK
▸	07:07:15	2 483162472715 eni-89c1e4c2 94.102.49.174 192.168.1.59 40894 808 6 1 40 1471676835 1471676886 ACCEPT OK
▸	07:09:11	2 483162472715 eni-89c1e4c2 117.222.109.108 192.168.1.59 23239 23 6 1 40 1471676951 1471677007 ACCEPT OK
▸	07:10:11	2 483162472715 eni-89c1e4c2 179.232.249.66 192.168.1.59 49621 23 6 4 208 1471677011 1471677067 ACCEPT OK
▸	07:10:11	2 483162472715 eni-89c1e4c2 103.213.251.95 192.168.1.59 38964 3306 6 1 52 1471677011 1471677067 ACCEPT OK
▸	07:11:19	2 483162472715 eni-89c1e4c2 94.102.49.174 192.168.1.59 40894 9797 6 1 40 1471677079 1471677127 ACCEPT OK
▸	07:14:57	2 483162472715 eni-89c1e4c2 222.186.34.223 192.168.1.59 6000 3306 6 1 40 1471677297 1471677307 ACCEPT OK

- ポート番号／送信元先IPアドレス／転送パケット数・バイト数／アクション などが時系列で記載
- パケットの中は記録されない
- ENI（仮想NIC）の入出力分のみが記録される
- 脅威の可視化は不可能

paloalto NETWORKS

VPCのネットワークセキュリティ関連機能のまとめ

通信の制御

- 制御できるヘッダはレイヤ4まで
- アプリケーションやユーザの識別は不可能

通信の可視化

- インタフェースからのIN/OUTのみが記録される
- プロトコル／アプリケーション／ユーザまでは識別不可能
- 可視化は不可能

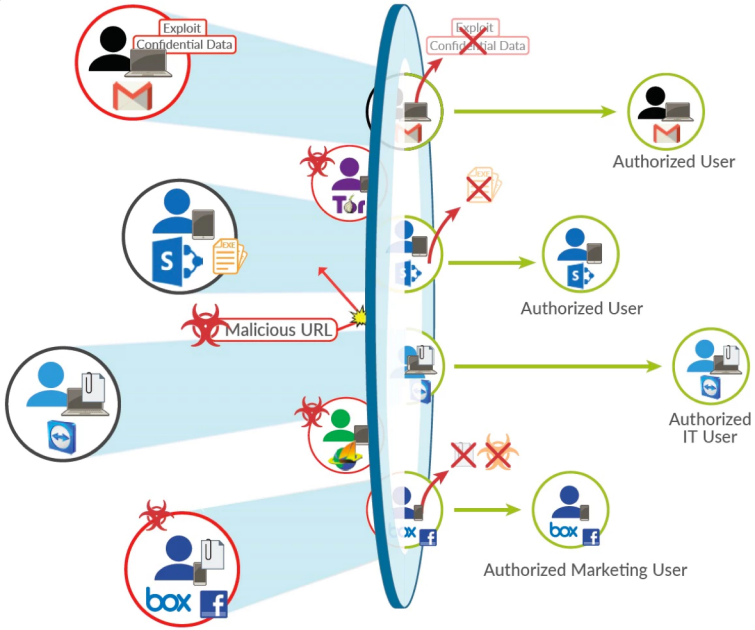
脅威への備え

- マルウェア等悪意のあるコンテンツに対する可視化・防御機能はない（ユーザ側の責任範囲）

次世代ファイアウォールとは

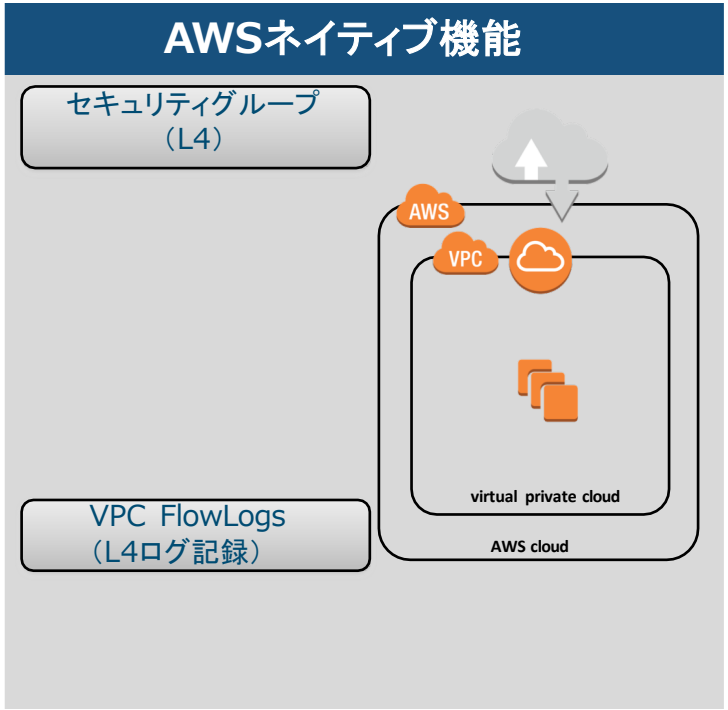
これまでのIP・ポートベースの防御ではなくアプリケーション、ユーザー、コンテンツの3つを組み合わせることにより次世代のファイアウォールとして機能します

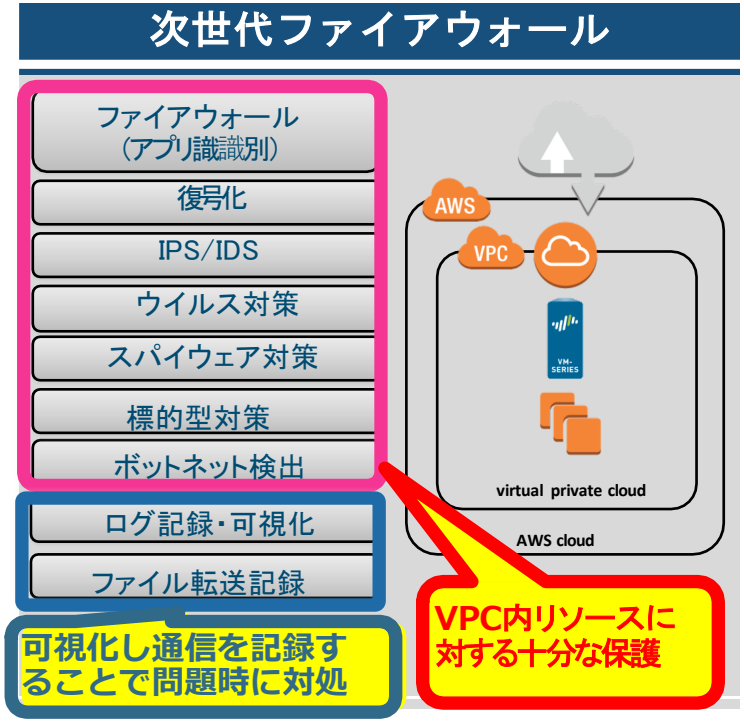
- App-ID
- User-ID
- Content-ID



 © 2018, Palo Alto Networks. All Rights Reserved.

セキュリティの考え方：”共有責任モデル”と“VPC内リソースに対する保護”





セキュリティの考え方：”共有責任モデル”
- AWS VPCのセキュリティ機能に必要不可欠な要素 -

通信の制御

- 制御できるヘッダはレイヤ4まで
- アプリケーションやユーザの識識別は不可能

通信の可視化

- インタフェースからのIN/ OUTのみが記録される
- プロトコル/アプリケーション/ユーザまでは識別不可能
- 通信の列挙のみで可視化は不可能

脅威への備え

- マルウェア等悪意のあるコンテンツに対する可視化・防御機能はない（これらは利用者側責任範囲）

通信の制御

- 「誰（ユーザ）」の識別と制御
- 「何をしたか（アプリケーションやアクション）」の 識別と制御

通信の可視化

- VPC内のSubnet間を流れる通信を記録
- プロトコルは通信元先は当たり前
- アプリケーションやユーザまで遡って把握する仕組み

脅威への備え

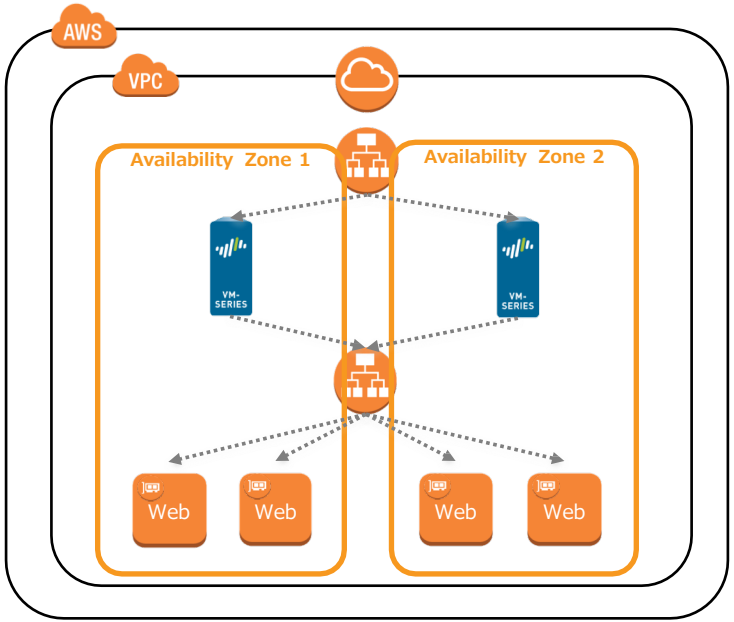
- クラウドサービス基盤以上のレイヤについては構築する必要がある
- 脅威自体も可視化することで攻撃のフェーズ進行を阻止

次世代ファイアウォールの特長

- 従来のステートフル型ファイアウォールでは検知できなかったアプリケーションを識別することで、高レベルでの通信可視化とトラフィック管理を実現
- クラウド型マルウェア検知(WildFire)やユーザ可視化(User-ID)等との組み合わせによりAWS環境の出口/入口対策が可能

ポイント1	ポイント2	ポイント3
アプリケーションとユーザの可視化＆制御	高度な防御機能が実装されたゲートウェイセキュリティ	Site-to-Site & Site-to-Client　VPN
App-ID/Content-ID/User-IDの組合せで、ユーザとコンテンツに基づいた通信の可視化と制御が可能	未知のマルウェア対策(WildFire)／URLフィルタ／DDoS対策／IPS／ファイルブロッキング等の出口・入口対策を実現可能	リモートアクセス／拠点間VPNのアクセスサーバとして展開可能 Host Information Profile(HIP)を利用した端末制御も実現

ユースケース：公開Webサーバの保護



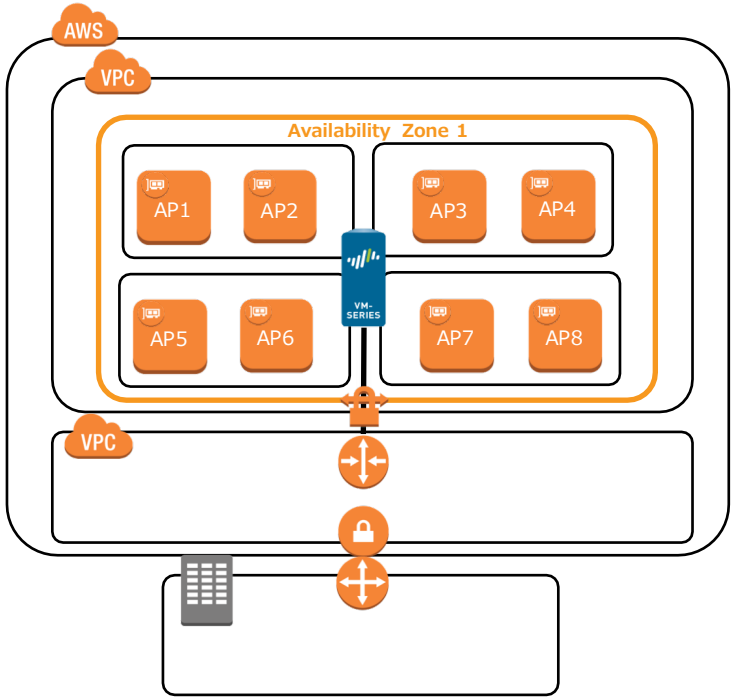
【 構成 】

- Internet向けの公開Serverの手前にFWを設置
- ELB（Elastic Load Balancer）を利用し、Trafficを複数FWに分散 ※ **PAN--OS7.1からの新機能**
- S3ブートストラップとの併用用でAutoScalingに対応した弾性的な構成を組むことも可能

提案のポイント

- North<->Southのトラフィックを検査
- IPS機能を用いたServerの保護
- アクセス/攻撃元の国情報の把握
- アプリ/ 宛先ごとのアクセス量量の把握
- Serverへの接続トラブルの際のログ確認 （トラブルシュート）
- DoS対策
- AutoScalingによる大規模アクセス対応

ユースケース：社内基幹系システムの保護



【 構成 】

- 社内サーバを用途等に応じてサブネットに配置、 サブネット間をVM-Seriesで橋渡し
- 社内とはDirect ConnectやハードウェアVPNで接続用VPC経由でプライベート接続

提案のポイント

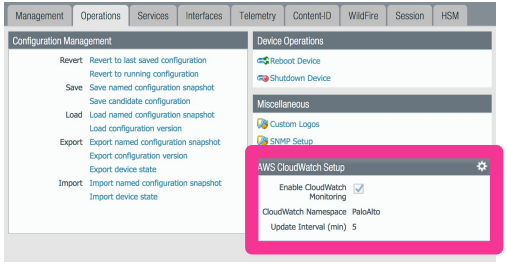
- East<->Westのトラフィックを検査
- 社内からのマルウェア混入入等の脅威からEC2インスタンスを保護
- IPS機能を用いたServerの保護
- User-IDにより社内からのアクセスをAD構成情報に基づいて制御／可視化

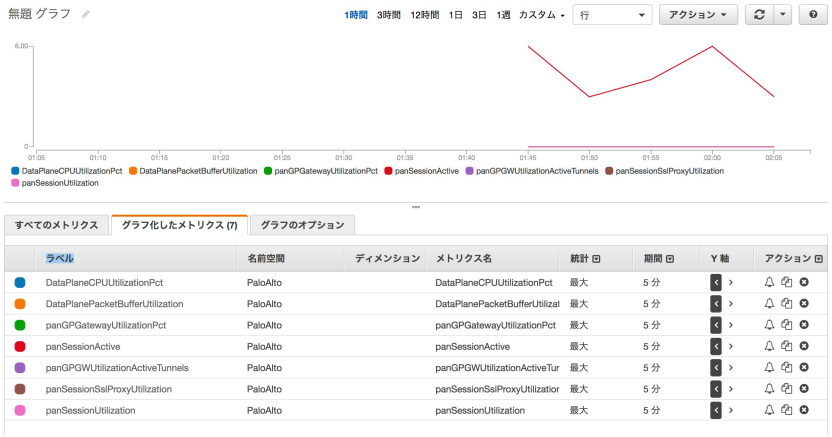
Palo Alto NetworksとAWSの連携メリット

- VM-SeriesではAWSのネイティブ機能と連携するための機能が豊富に提供されている
- 次世代ファイアウォールのPAシリーズと同じエンタープライズグレード仮想ファイアウォールによる大規模構成での管理を簡略化したり、トラフィック変動に応じた柔軟な構成を組むことが可能

Amazon CloudWatch Integration（ PAN-OS8.0～ ）

- CloudWatchに対してカスタムメトリクスのPUTが可能
- CloudWatchでは収集できないアクティブセッション数を始め、内部の様々なメトリクスがCloudWatch上で確認できるように実装

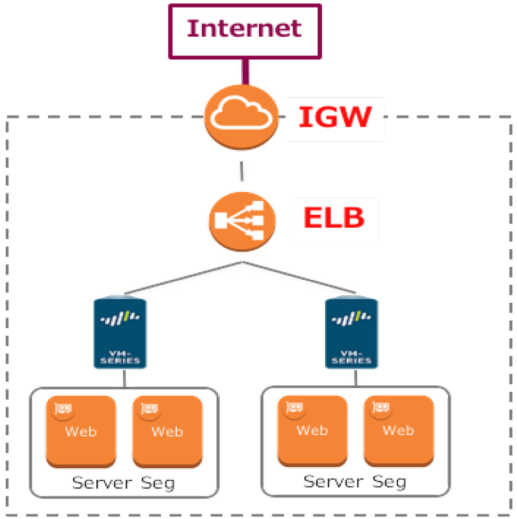




Amazon ELB対応

- 従来は高トラフィックなWebサイトを構築する際に、フロントに配置した“ファイアウォール”がボトルネックになるケースがあった

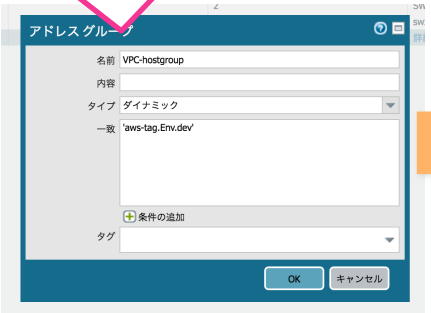
- ELB（ロードバランサー）に部分対応したことで、ELB -> VM-Series ->バックエンドサーバというトラフィックルーティングが可能となり、 VM-Series自体の高負荷の際にはAutoScalingによって負荷を分散することも可能



VPCと連携したダイナミックアドレスグループ

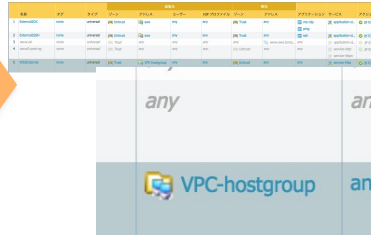
- AWS提供のAPIからEC2インスタンスの管理理情報を取得することで、配下ノードの動的な変化に自動追従するアドレスグループを作成可能
- インスタンス構成の動的な変化に対して、自動的にファイアウォールによる保護ポリシーが適用

キー"Env"に値"dev"が設定されたインスタンスをリストアップ

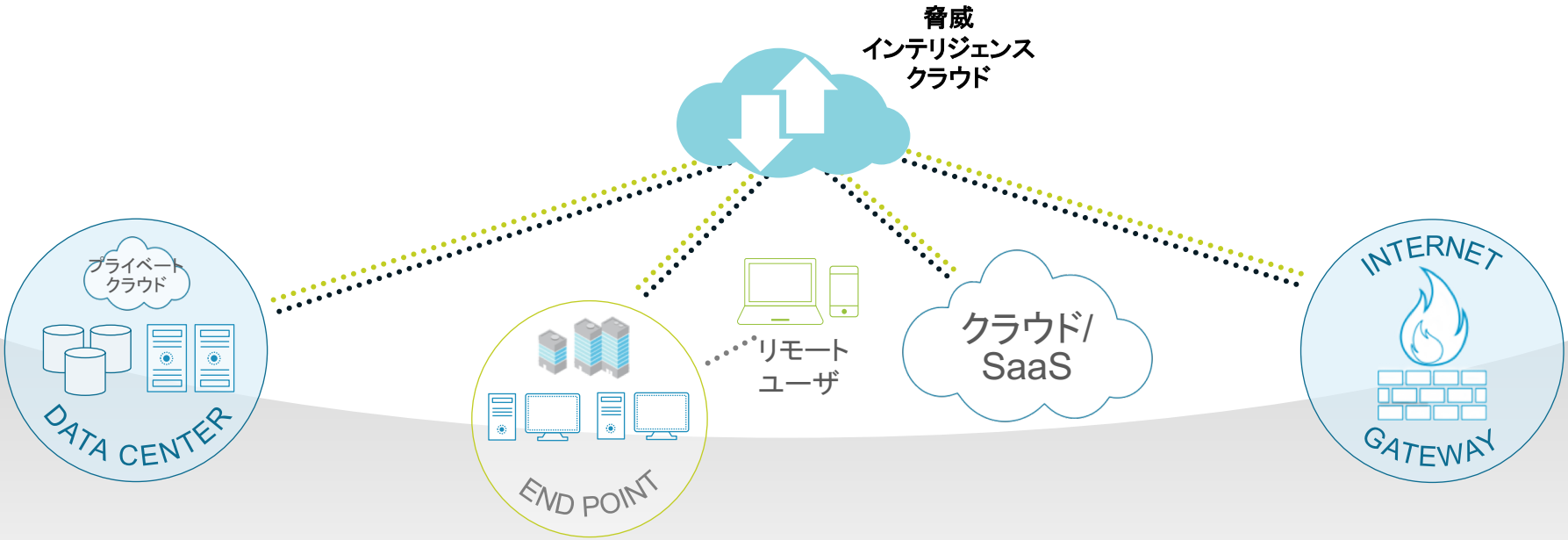


設定した検索条件に該当するIPアドレスが自自動登録される

ポリシー自体はそのまま。動的に登録されたアドレスに同じポリシーが自動的に適用される。



一貫したセキュリティをクラウドから配信

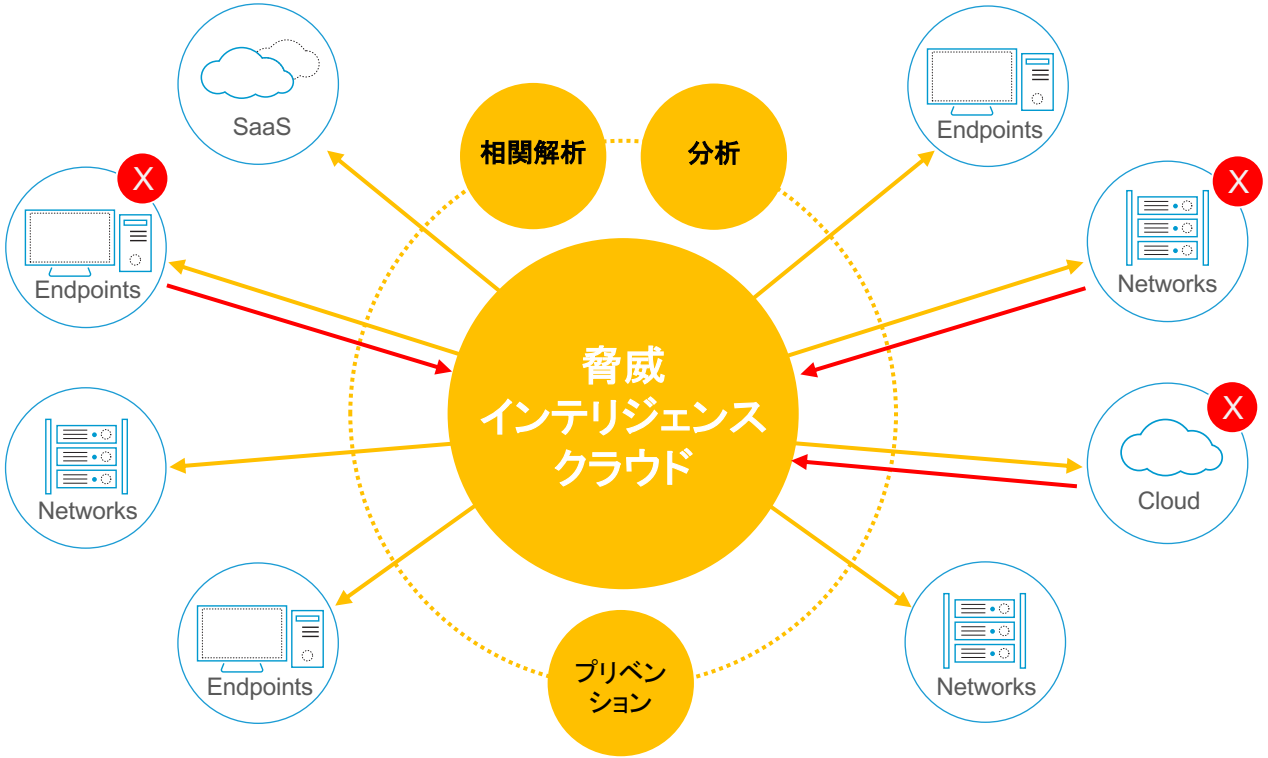


エンタープライズネットワーク

 © 2017, Palo Alto Networks. All Rights Reserved.

自動化された脅威プリベンション

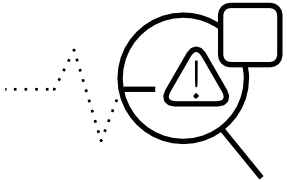
防御策を最短5分で自動配信



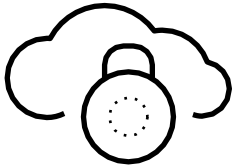
 © 2017, Palo Alto Networks. All Rights Reserved.

CASB提案

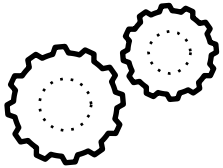
Aperture の基本機能



コンテンツ検査
と可視化



ポリシーに基づく
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

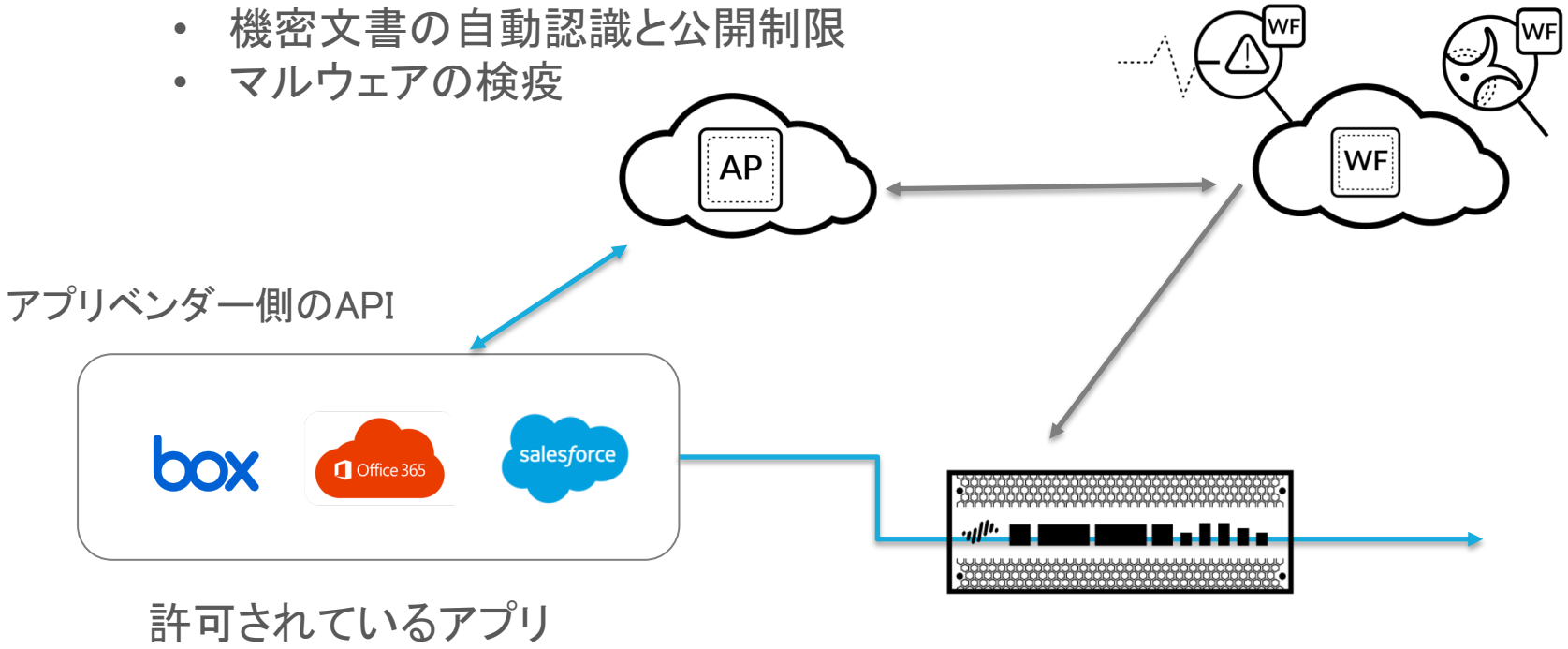
情報漏えい対策

マルウェア
対策

 © 2018, Palo Alto Networks. Confidential and Proprietary.

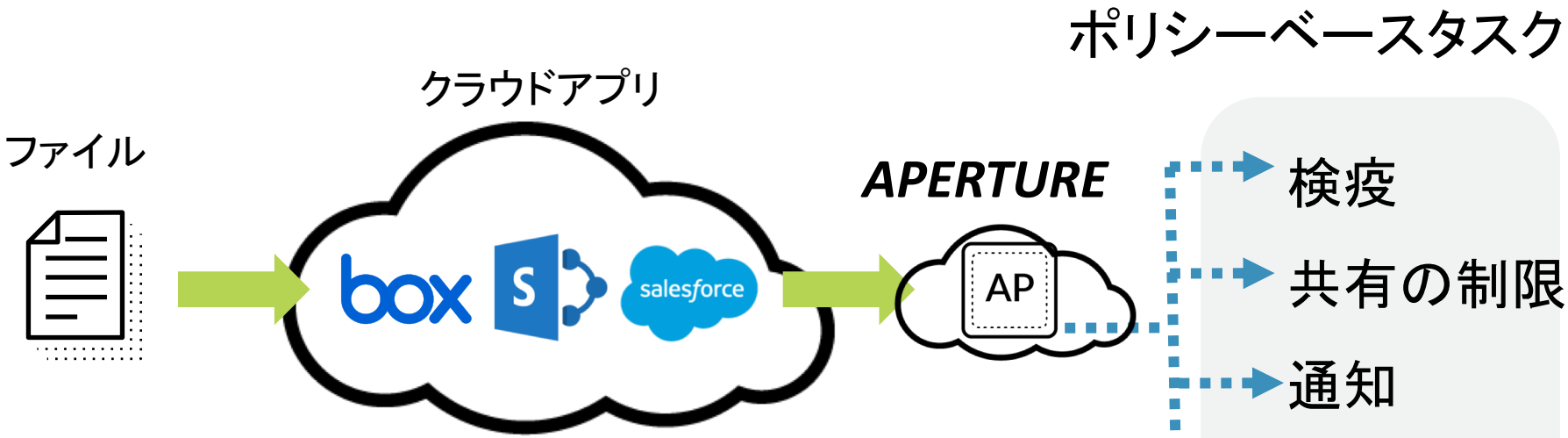
Aperture SaaSアプリ向けデータ保護ソリューション

- 機密文書の自動認識と公開制限
- マルウェアの検疫



 © 2018, Palo Alto Networks. All Rights Reserved.

Aperture　ポリシーに基づく自動的なデータ公開制御

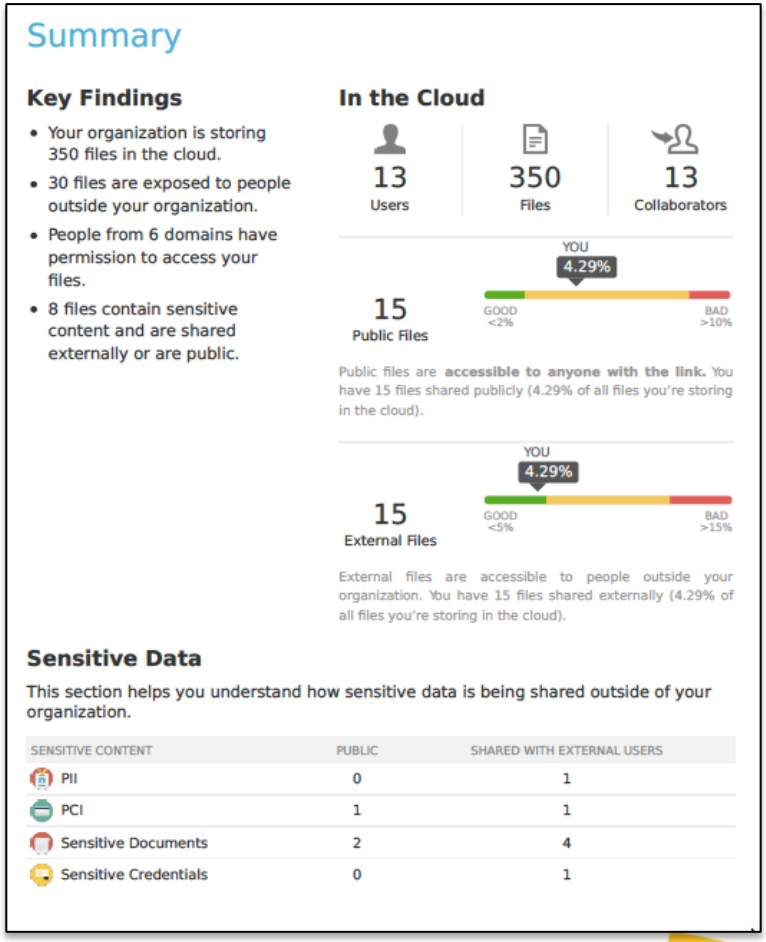


ファイルが保存されると、中身をスキャンし
ポリシーの条件に一致したファイルに対して
自動的に処理を行う。

 © 2018, Palo Alto Networks. All Rights Reserved.

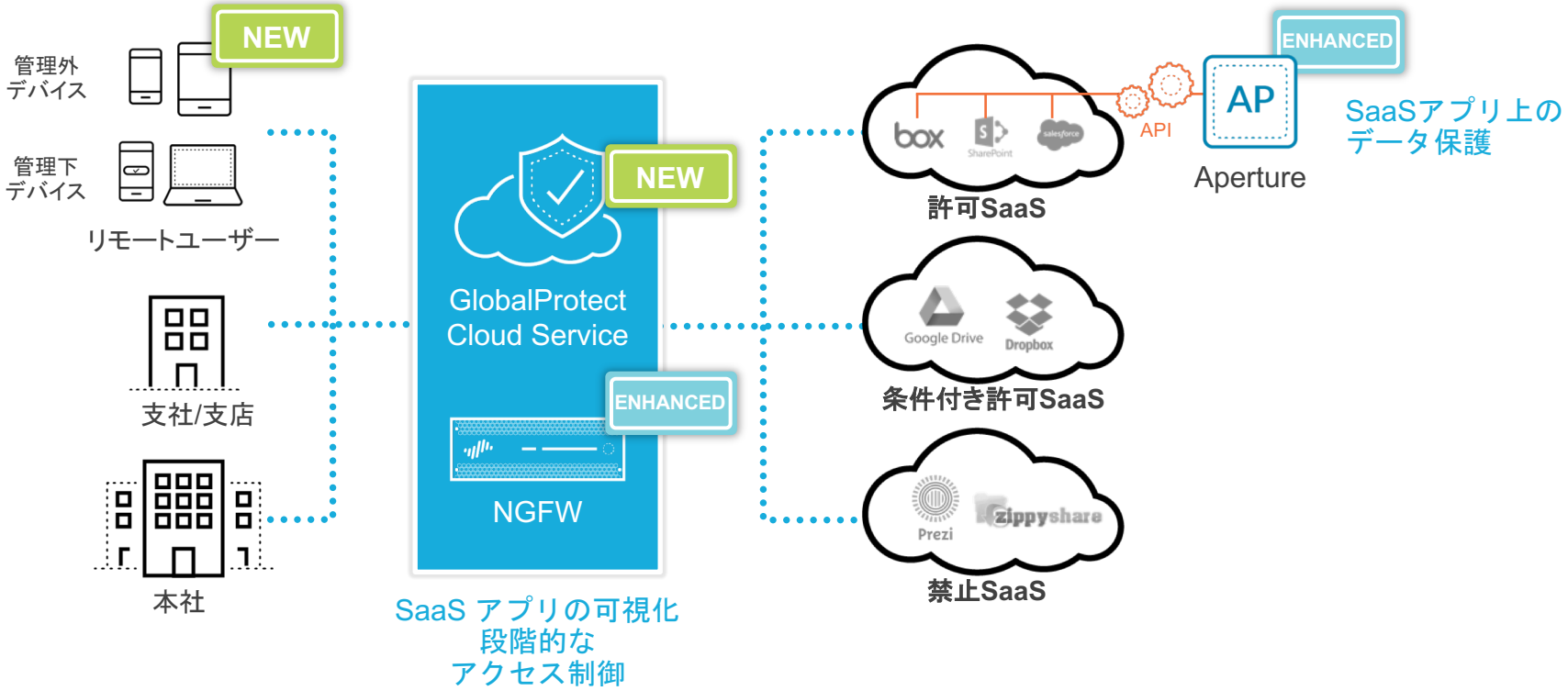
Aperture リスクの可視化

複数のSaaSアプリを横断し、
活動の内容、リスクにつながる行為に
関するレポート作成



 © 2018, Palo Alto Networks. All Rights Reserved.

SaaSアプリに対する保護



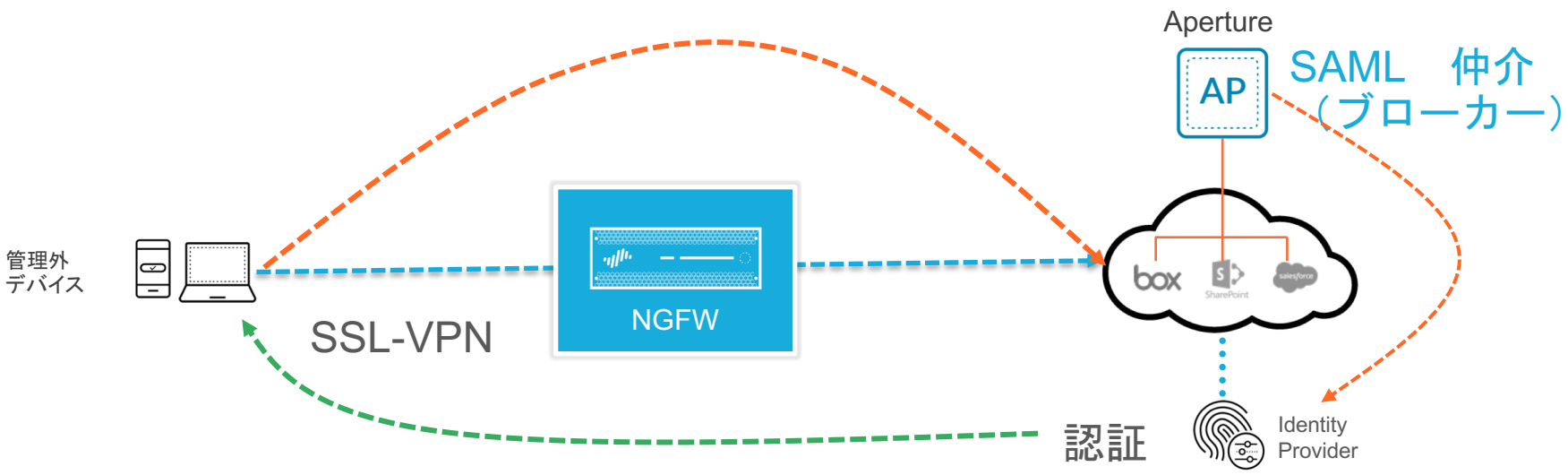
 © 2018, Palo Alto Networks. Confidential and Proprietary.

エージェントレスのセキュアSaaSアクセスと可視化

管理外のデバイスに対しても正しいアクセス制御とデータ保護を実現	SaaSアプリの制御は次世代ファイアウォール	エンドポイントエージェント不要のデータ保護

 © 2018, Palo Alto Networks. All Rights Reserved.

エージェントレスのセキュアSaaSアクセスと可視化



①管理外のデバイスアクセスが SaaSアプリにアクセス	②ApertureがSAML仲介	③認証後にNGFWと SSL-VPN接続

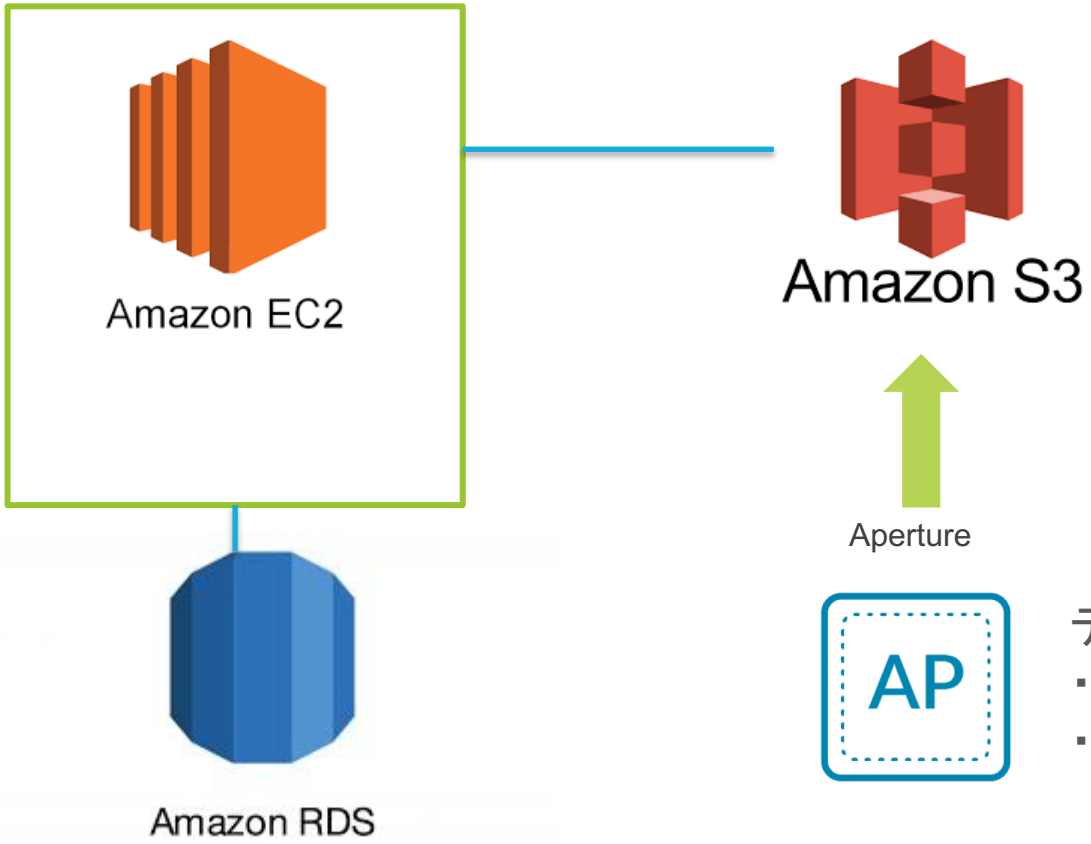
 © 2018, Palo Alto Networks. All Rights Reserved.

対応アプリの拡張

Box	Citrix ShareFile	Confluence	Dropbox	GitHub	Gmail	Google
Jive	Microsoft Exchange	Office 365 OneDrive & SharePoint	Salesforce	Secure Data Space	ServiceNow	Slack Enterprise Grid
Azure Storage	Yammer	Amazon Web Services	G Suite	Amazon S3	Workplace	Google Cloud Storage

 © 2018, Palo Alto Networks. All Rights Reserved.

Public Cloud で利用するストレージ上のデータ保護

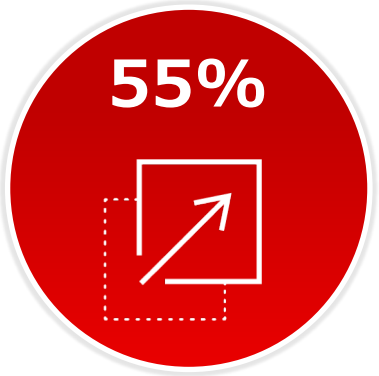


AP

データ保護
・機密情報保護
・マルウェア対策

 © 2018, Palo Alto Networks. All Rights Reserved.

脅威のランドスケープ　進化を続けるサイバー攻撃



攻撃量

新種マルウェアの数の
増加率

攻撃の深刻度

35% ファイルレスアタックの
増加率

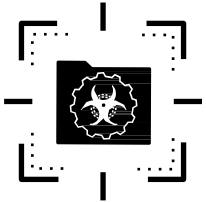
さらに高度に

標的型がさらに
多様化

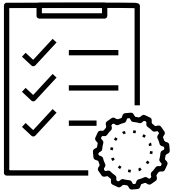
 © 2018, Palo Alto Networks. All Rights Reserved.

外部フィードの処理と自動化

AutoFocus



脅威フィード

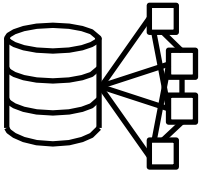


ホワイトリスト
（Microsoft等）

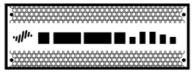
フォーマットの
異なるデータ

MineMeld

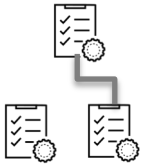
収集と処理
アウトプット
の自動化



SIEM



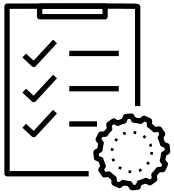
Gateway



ワークフロー

 © 2018, Palo Alto Networks. All Rights Reserved.

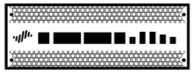
Office 365を次世代ファイアウォールで管理



ホワイトリスト
（Microsoft等）

MineMeld

EBLとしてアウトプット



次世代
ファイアウォール

 © 2018, Palo Alto Networks. All Rights Reserved.