Z解体真書

Chapter 3

ゼットスケーラー株式会社

エバンジェリスト＆アーキテクト

髙岡 隆佳

Zアーキテクチャを6つの切り口から紹介

Z通信処理

Zキャパシティ

Z構成要素

Z冗長性

Zセキュリティ

Zデータセンター

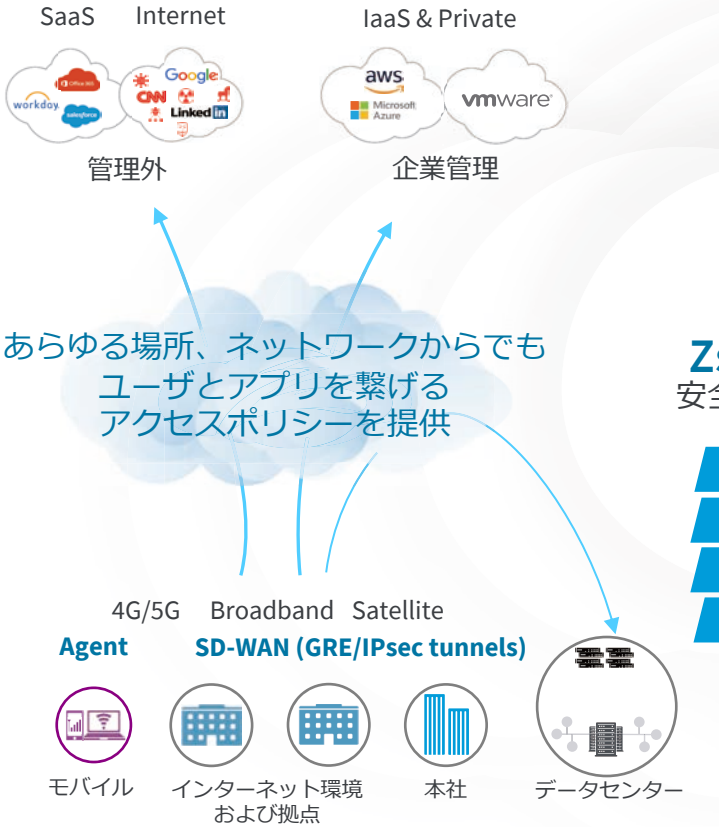
3. Zセキュリティ

Zscalerのプラットフォームサービス(OLD)

ZIA

Zscaler Internet Access
インラインですべての通信を保護

- リアルタイムURLフィルタ
- ホワイトリスト/無害化
- サンドボックス（静的・動的）
- NGFW/IPS
- SSL フルプロキシ
- CASB（GW/API）
- 帯域制御・QoS
- EDM対応DLP



ZPA

Zscaler Private Access
安全なユーザを内部アプリへ接続

- SDP/ZTNA
- ブラウザアクセス対応
- 接続端末の体勢管理
- マルチIdP対応

Zscalerのプラットフォームサービス(2020)

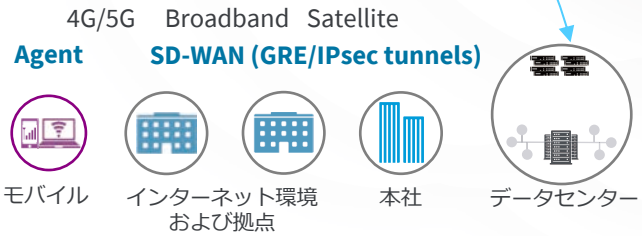
ZIA

Zscaler Internet Access
インラインですべての通信を保護

- 無害化/ウェブ分離
- リアルタイムURLフィルタ
- ホワイトリスティング
- サンドボックス（静的・動的）
- NGFW/IPS
- SSL フルプロキシ
- CASB API/Gateway
- 帯域制御・QoS
- EDM対応DLP
- Source IP Anchoring

ZDX

Zscaler Digital Experience
End-to-Endでユーザ体感を監視



ZPA

Zscaler Private Access
安全なユーザを内部アプリへ接続

- SDP/ZTNA
- ブラウザアクセス対応
- 接続端末の体勢管理
- マルチIdP対応

Securing your cloud transformation

セキュリティポリシー設定

Web

Security
- マルウェア対策
- Sandbox
- ブラウザ制限
- ATP対策

Access Control
- URLフィルタ
- アプリ制御
- 拡張子制限
- 帯域制御
- SSL

DLP
- 情報流出対策ポリシー

Mobile

Z-app configuration
- Appプロファイル
- デバイス管理
- 通信転送ポリシー

Security
- モバイルセキュリティ設定

Access Control
- アプリストア関連設定

FireWall

Access Control
- NGFWポリシー
- DNSポリシー
- FTPポリシー

Zscalerのインテリジェンス

通信処理ボリューム（日）

15M　接続ユーザ
5000　企業
650G　通信量（ピーク時）
2.4PB　分析されたデータ

検出した脅威の実績（日）

65B　分析された通信
3.1B　ブロック（3.7%）
100M　検出した脅威（0.3%）

120K セキュリティ情報/日・毎15分&オンデマンド

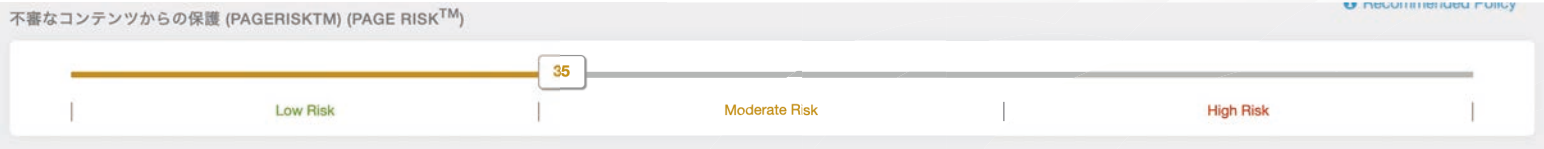
zscaler | ThreatLabZ

60以上の外部セキュリティフィード連携

CYBER THREAT ALLIANCE
OPEN THREAT EXCHANGE
Google Safe Browsing
VirusTotal
Microsoft (MAPP)

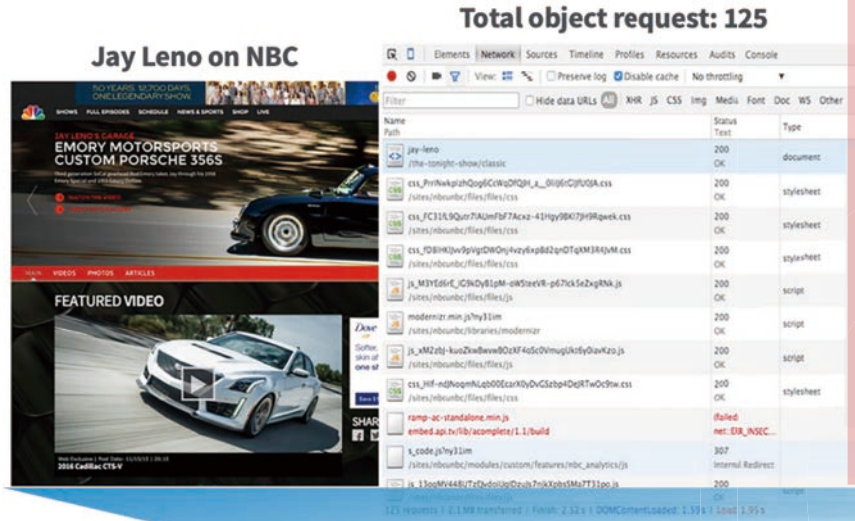
リアルタイムのリスクに対応する

Page Risk Index™



Zscalerサービスは、ページ内の悪意のあるコンテンツ（スクリプトの挿入、脆弱性のあるActiveX、ゼロピクセルのiFrameなど）を識別して、リアルタイムでリスクインデックスを計算し、リスクスコア（ページリスクインデックス）を作成します。同時に、ホスティングしている国、ドメインの古さ、過去の結果、および高リスクのトップレベルドメインへのリンクなどのデータを使用して、ドメインリスクインデックスが作成されます。ページリスクとドメインリスクは結合され、単一のリスクインデックススコアが作成されます。このスコアは、このポリシーで設定した不審なコンテンツからの保護（PageRiskTM）値と照合して評価されます。低リスク領域とは、わずかでも疑わしければ何でもブロックすることを示しています。リスクは許容されません。高リスク領域では、リスクへの許容度が高く、ユーザーは非常に危険なサイトでもアクセスできます。バーをクリックして所属組織のページリスク許容値を設定します。

全パケットの検査実行



検出できる脅威

Potential threats: 98

Personalized content from different sources (CDN)

Traffic: SSL

Page objects loaded: JavaScript, CSS, images

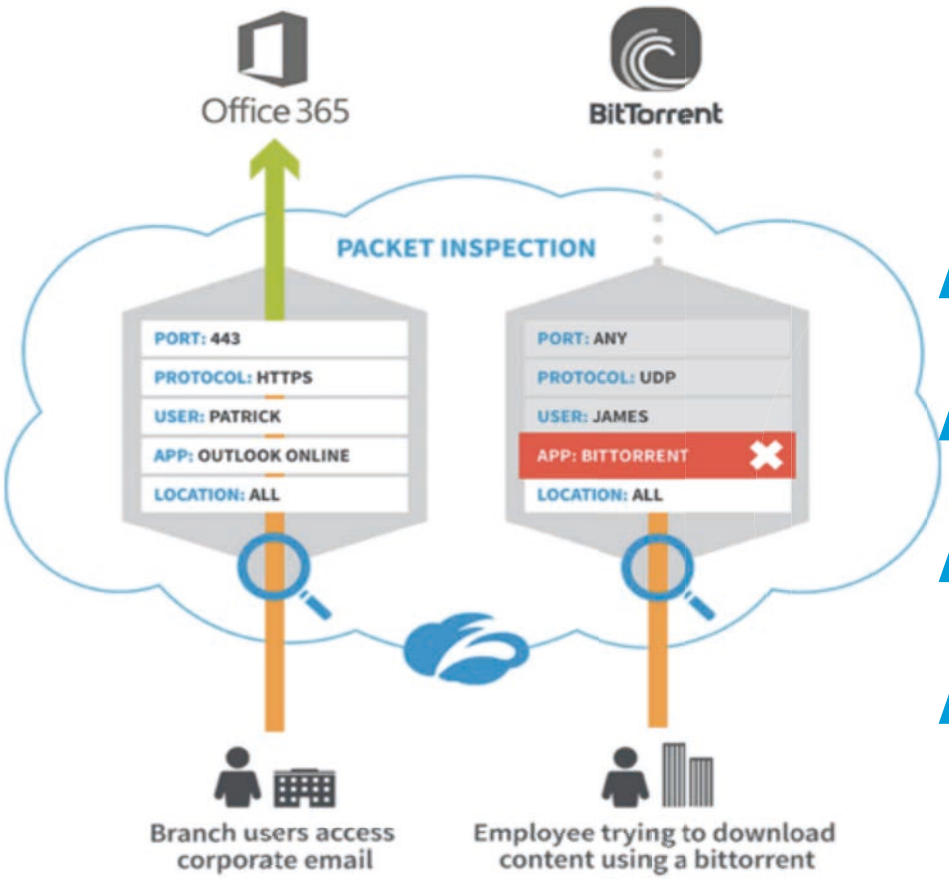
- ✓ 隠されたiFrame
- ✓ クロスサイトスクリプト（css）
- ✓ フィッシング
- ✓ クッキー搾取
- ✓ C&C通信

隠された脅威を全ての通信についてあぶり出す

ByteScan™

Securing your cloud transformation / zscaler™

Cloud Firewall



“ばらまき型”ではない
クラウド時代のFWaaS

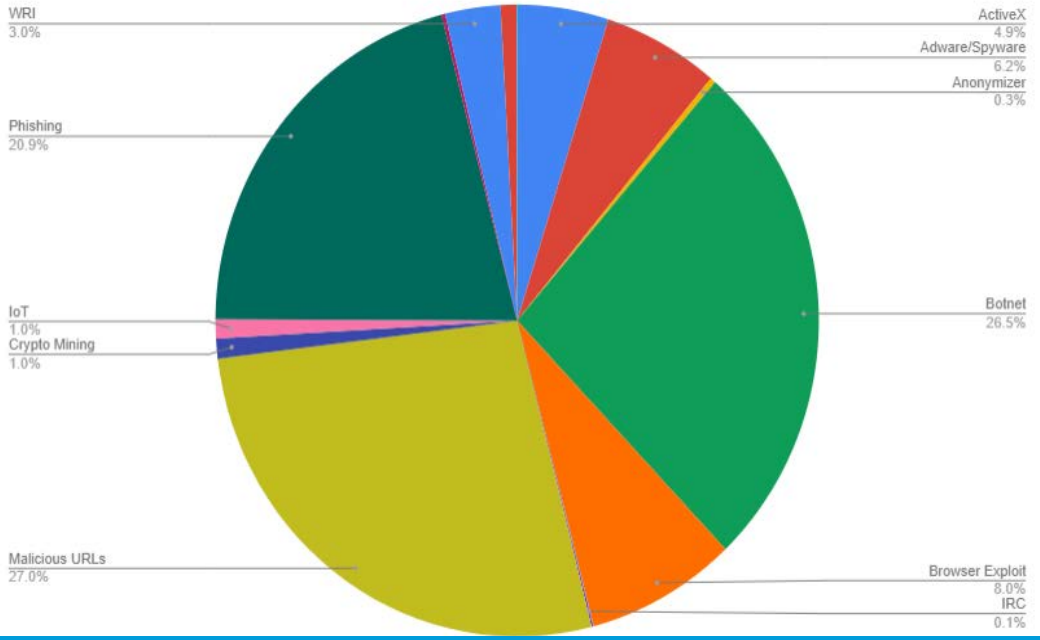
Deep Packet Inspectionの実行
非ウェブ通信（FTP, DNS, TDS等）も分析

全ロケーションのログ集中管理
6ヶ月分までオンラインで証跡確保

DNS通信に対するセキュリティ
不審なドメイン、DNSトンネリングをブロック

”Always-On” Cloud IPS
SSLを含む全ての通信を分析しExploitsを検出

ウェブ通信に対するIPSの効果

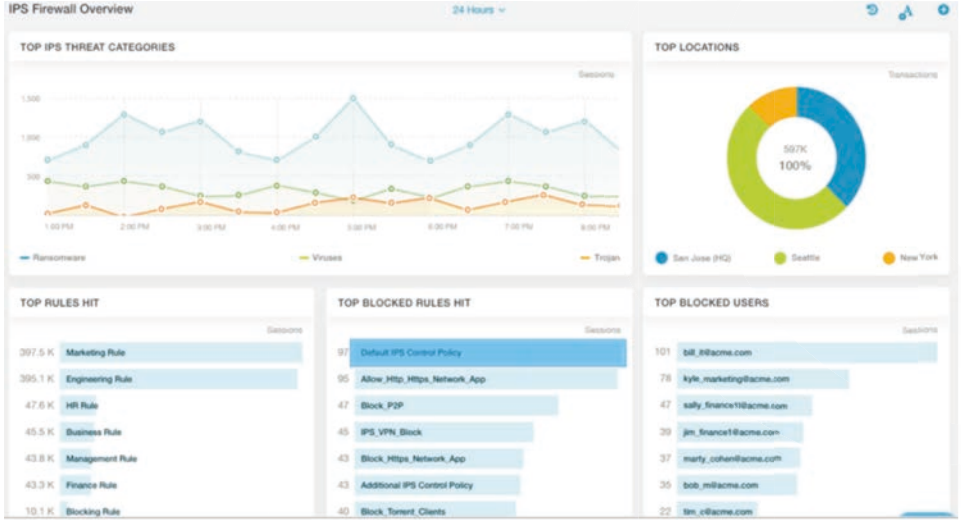


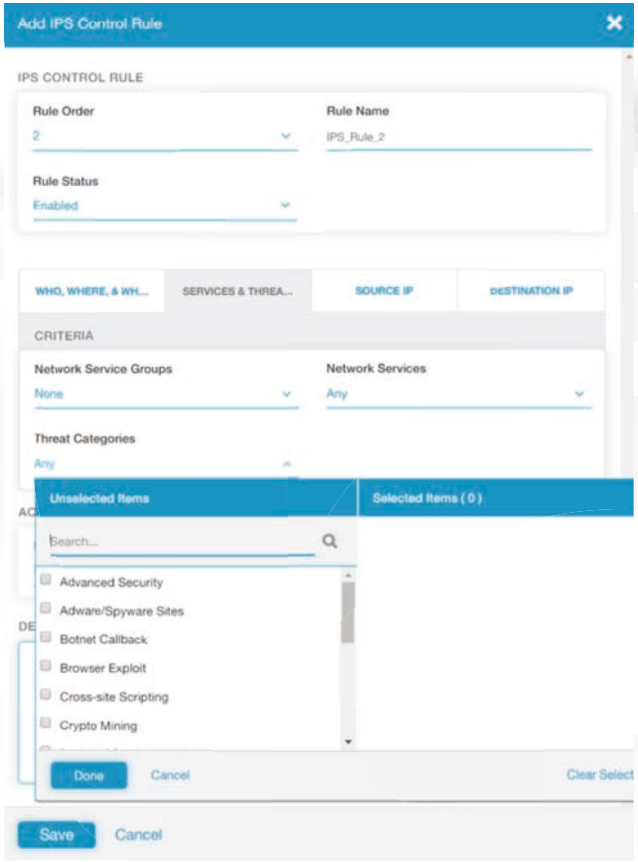
- **14,000+ IPSシグニチャ**
  - 3699 active Botnet C&C protocolシグニチャ
  - 2918 content based phishing シグニチャ
  - 4000超の malicious contentシグニチャ
  - 143 Crypto Mining シグニチャ
- **Zscaler流命名規則**
  Platform.Category.Family.Variant
  - e.g. Win32.Trojan.Dyre.AA
- https://threatlibrary.Zscaler.com

92%のIPSシグニチャがSSL通信に潜む怪しい挙動を検出

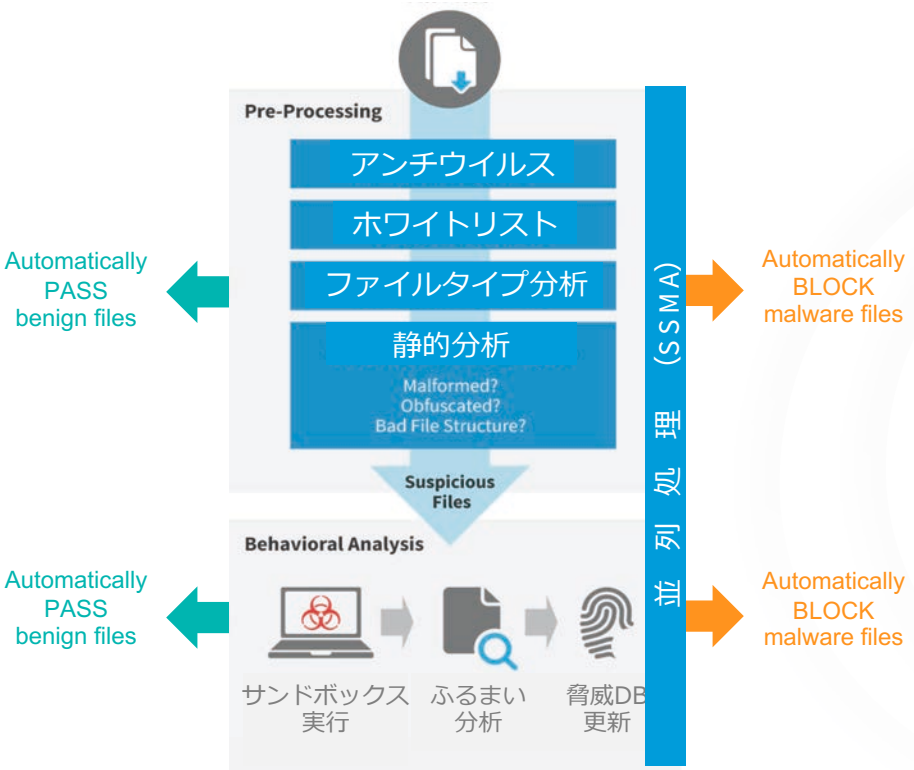
非ウェブ通信に対するIPS

- **IPS non-web signatures** (600以上)
  - Backdoors / RATs / Trojans
  - Botnet Callbacks, IRC
  - Denial of Service
  - SMB, DNS exploits..





Cloud Sandbox



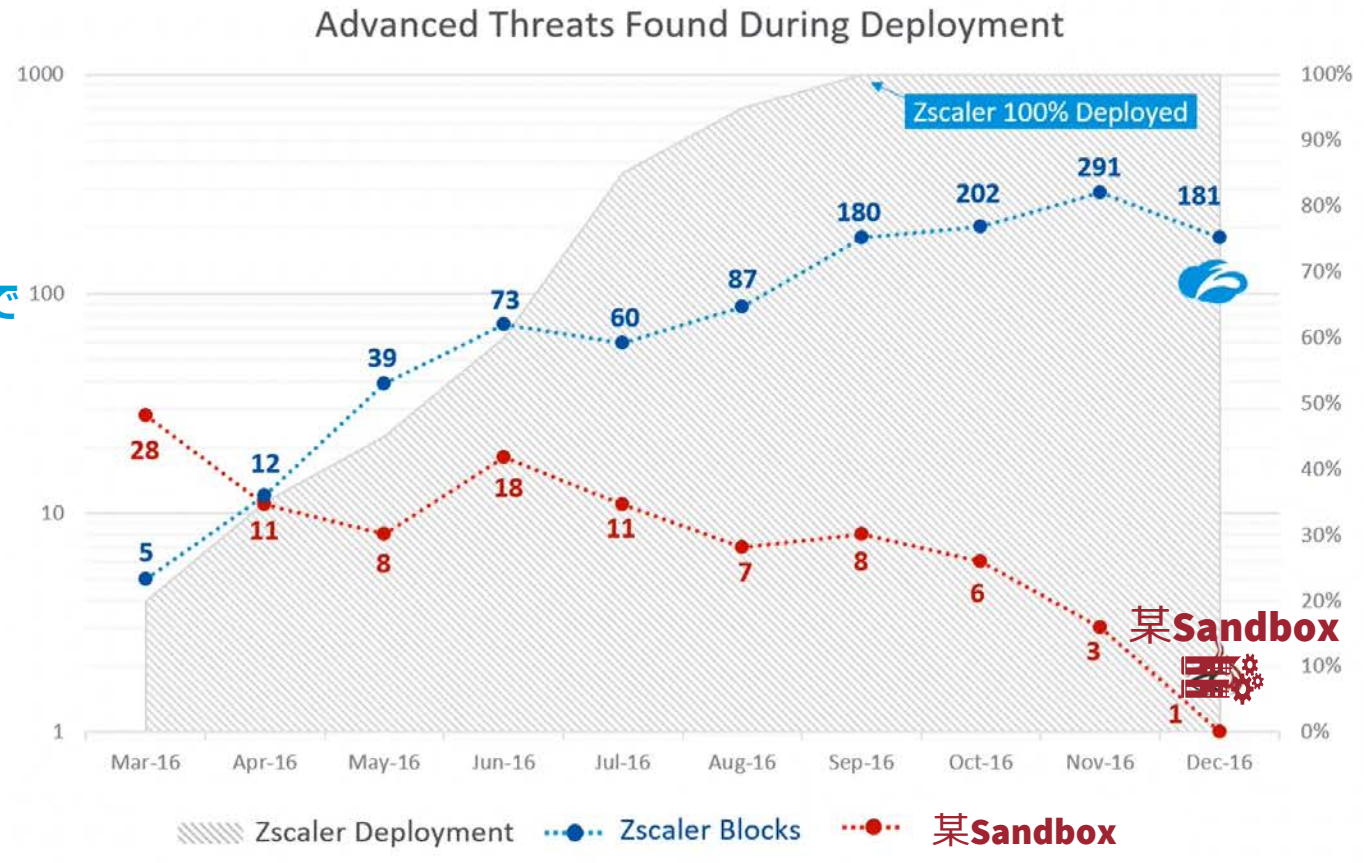
サンドボックスも オンプレミスに持つ理由なし

- インライン型サンドボックス
  分析完了まで完全隔離可能
- “Cloud Effect”インテリジェンス
  世界中のどこかで検出されたマルウェアは即時対応
- SSL通信対応で標的型対策
  信頼できるサイト通信に含まれる脅威を炙り出す

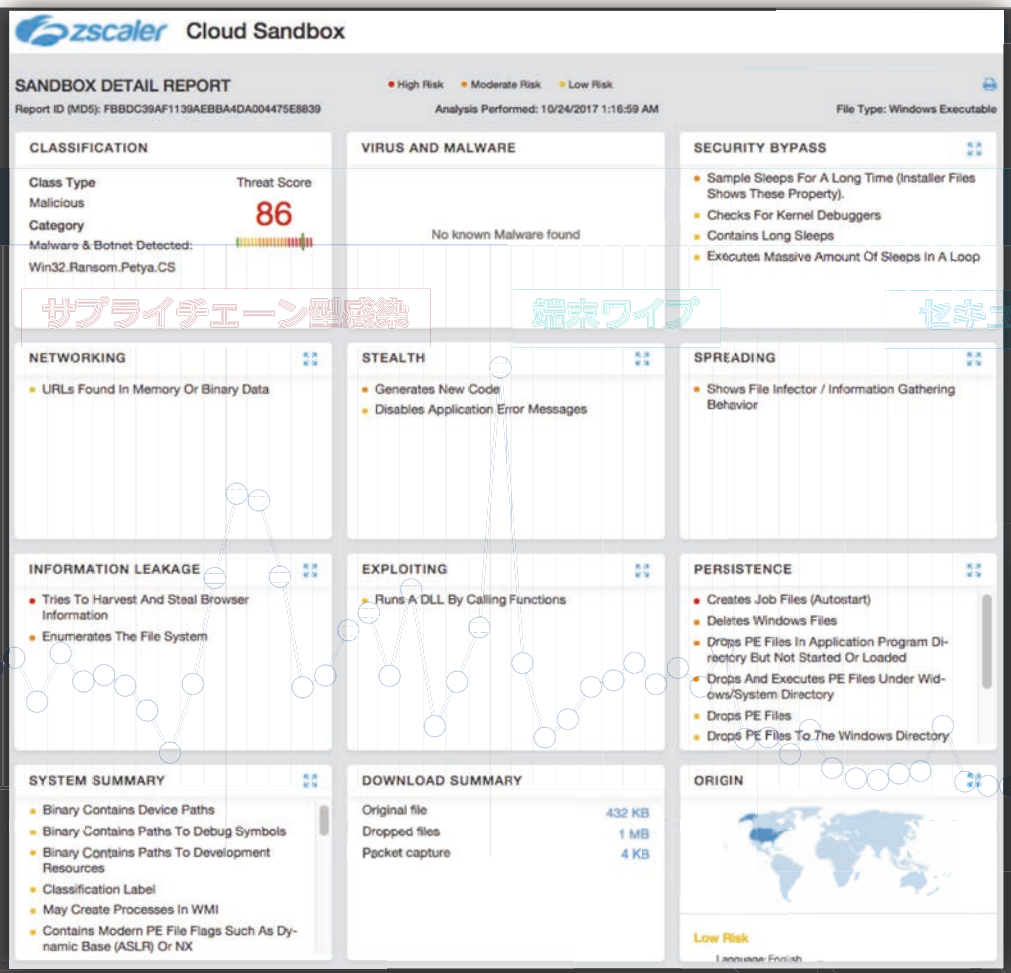
分析精度も凄い

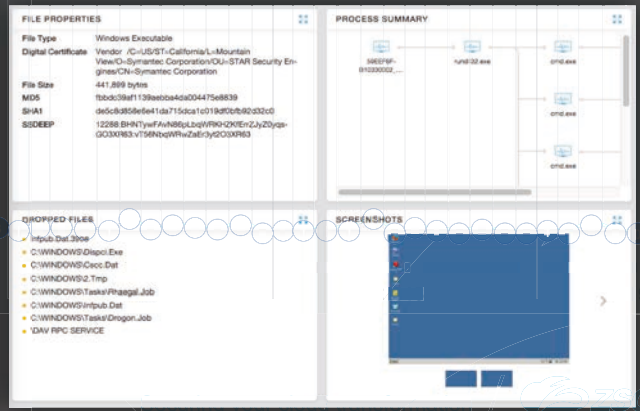
クラウド上の
SSL復号
＋サンドボックス機能で

オンプレサンドボックス
不要に

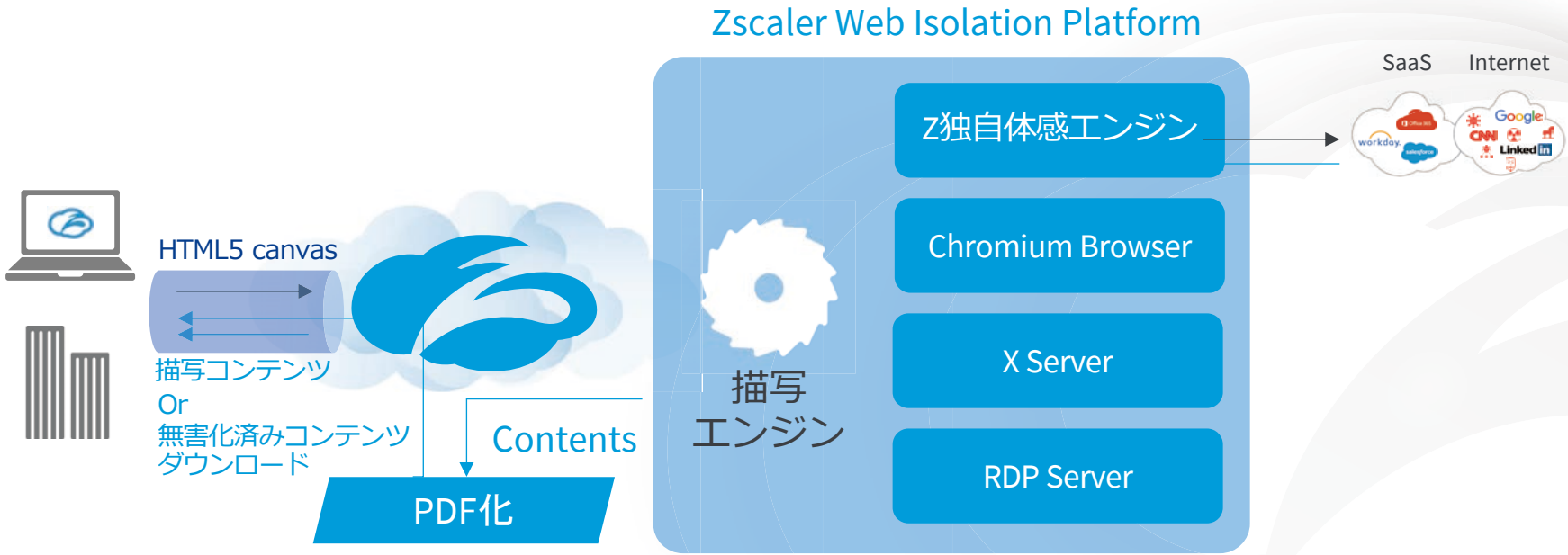


お客様事例：感染端末の削減を実現





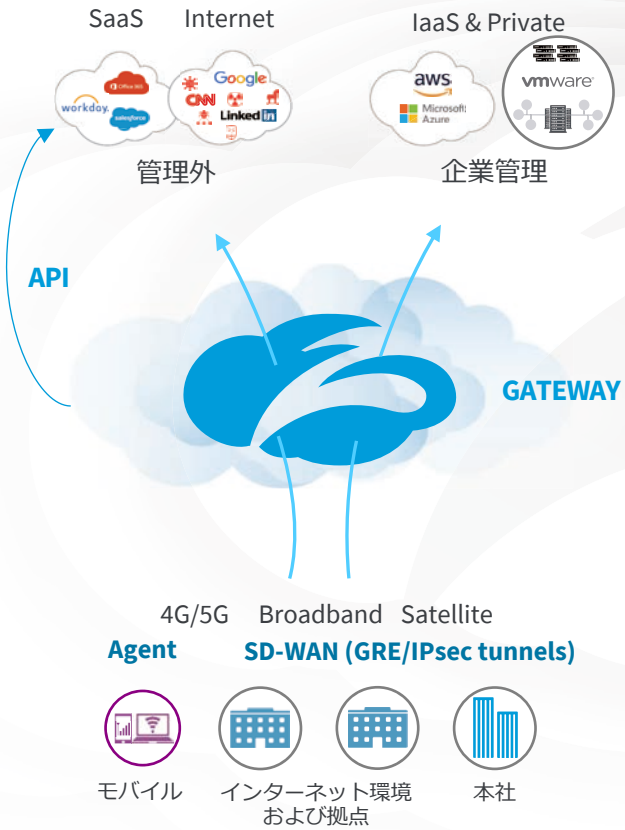
Web Isolation（無害化）



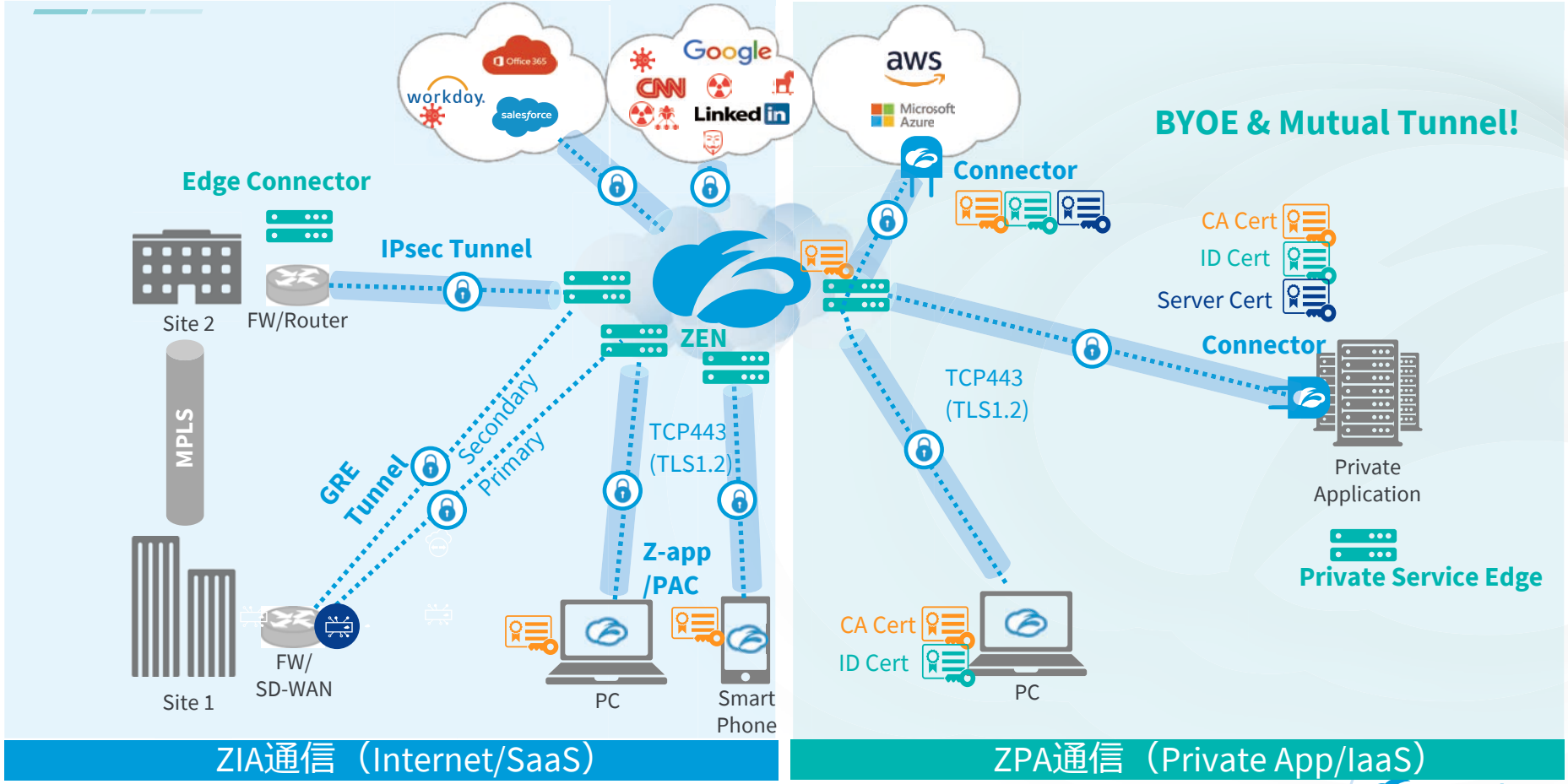
ポリシーに基づきリスクあるコンテンツ
を無害化してアクセス可能

CASB（Gateway/ API）

- **API(NEW!)**
  - 管理者権限を使用して企業アカウントについて制御
  - クラウドに上がったデータの制御
    - 公開リンクの削除、権限の変更、隔離など
  - 対応予定アプリ（OneDrive, SharePoints, BOX, Exchange SFDC, TEAMS, GDRIVE, GMAIL, Slack, GitHub, servicenow, dropbox）**→ サブスクリプション（ユーザ単位）で全アプリ対応**
- **GATEWAY**
  - 利用アプリの検出
  - リスクスコアの表示
  - 個人アカウント＆企業アカウントの把握
  - テナント制御
  - サンドボックス
  - ウェブ分離（無害化）
  - デバイス制御
  - 帯域制御

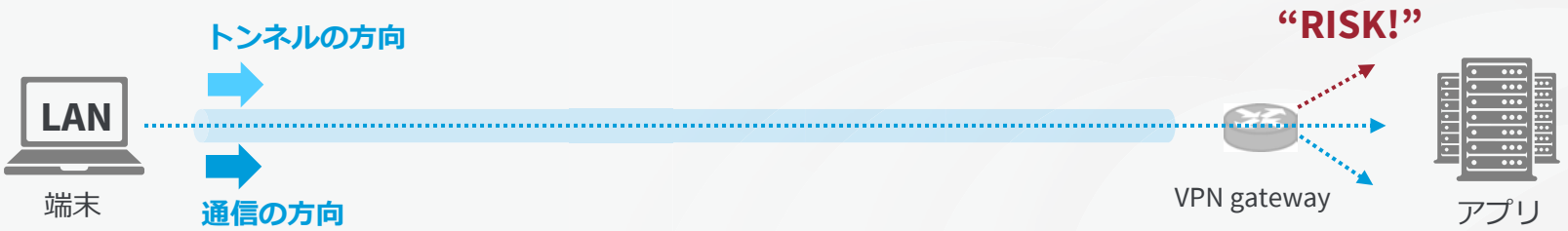


ZIA/ZPA通信イメージ図

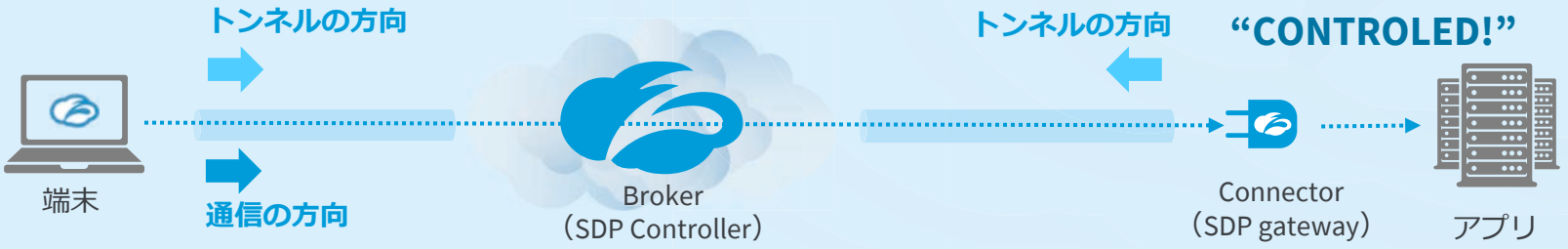


VPNとSDP（ZTNA）の違い

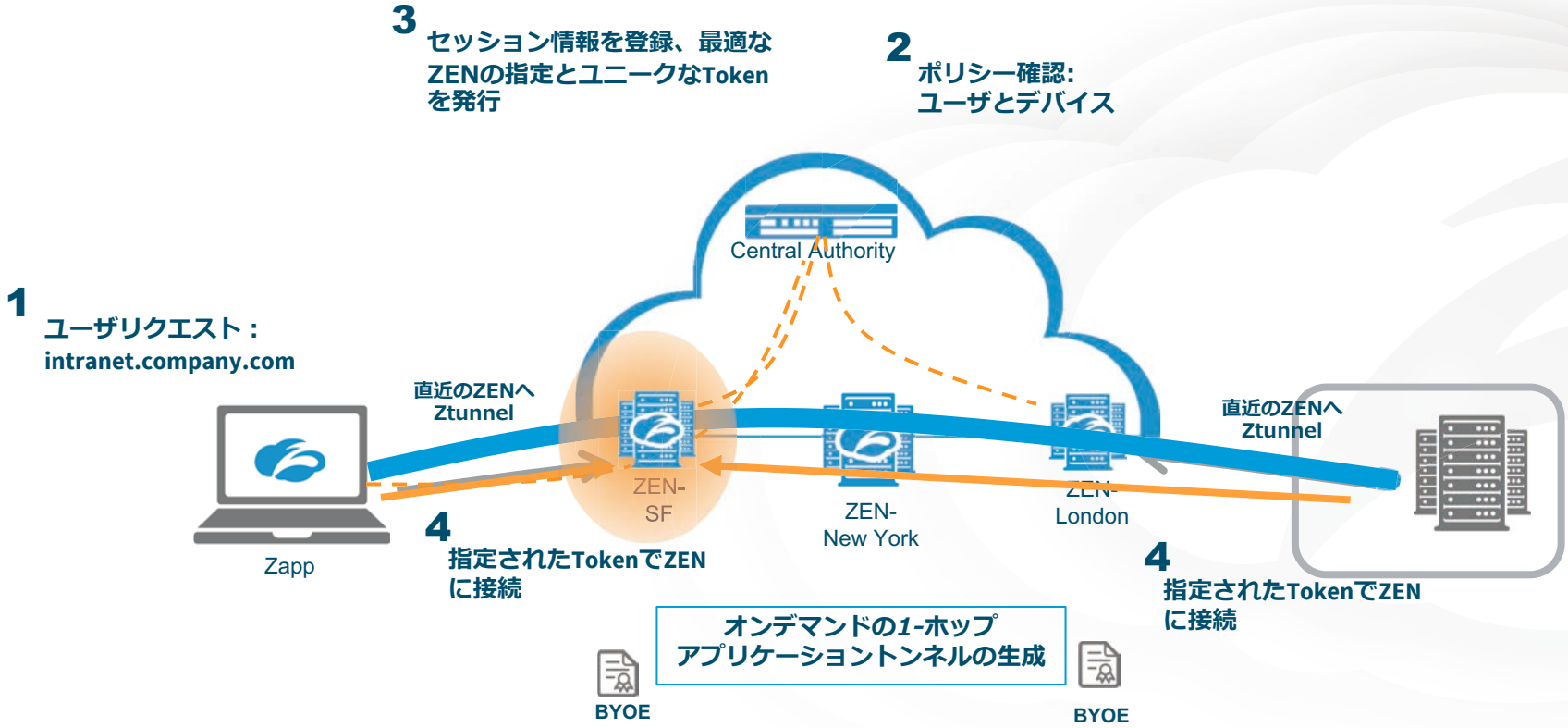
VPN　**認証後はLANのアドレスで社内にアクセス**（二次感染リスク、情報流出リスクあり）



SDP/ZTNA　**認証後もセキュリティ施行＆不要なアクセス不可**（アプリをネットワークから隔離）



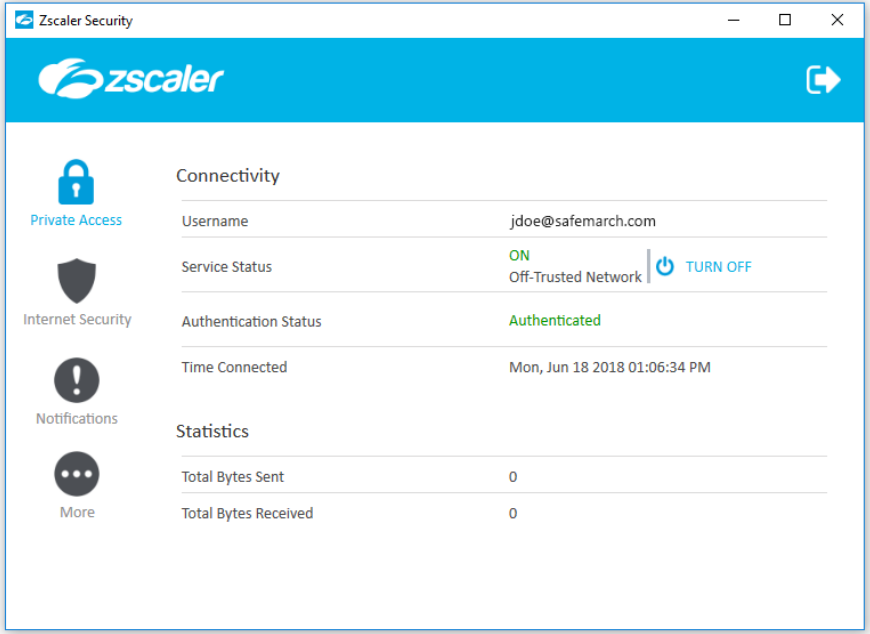
ZPAトンネル確立までのフロー



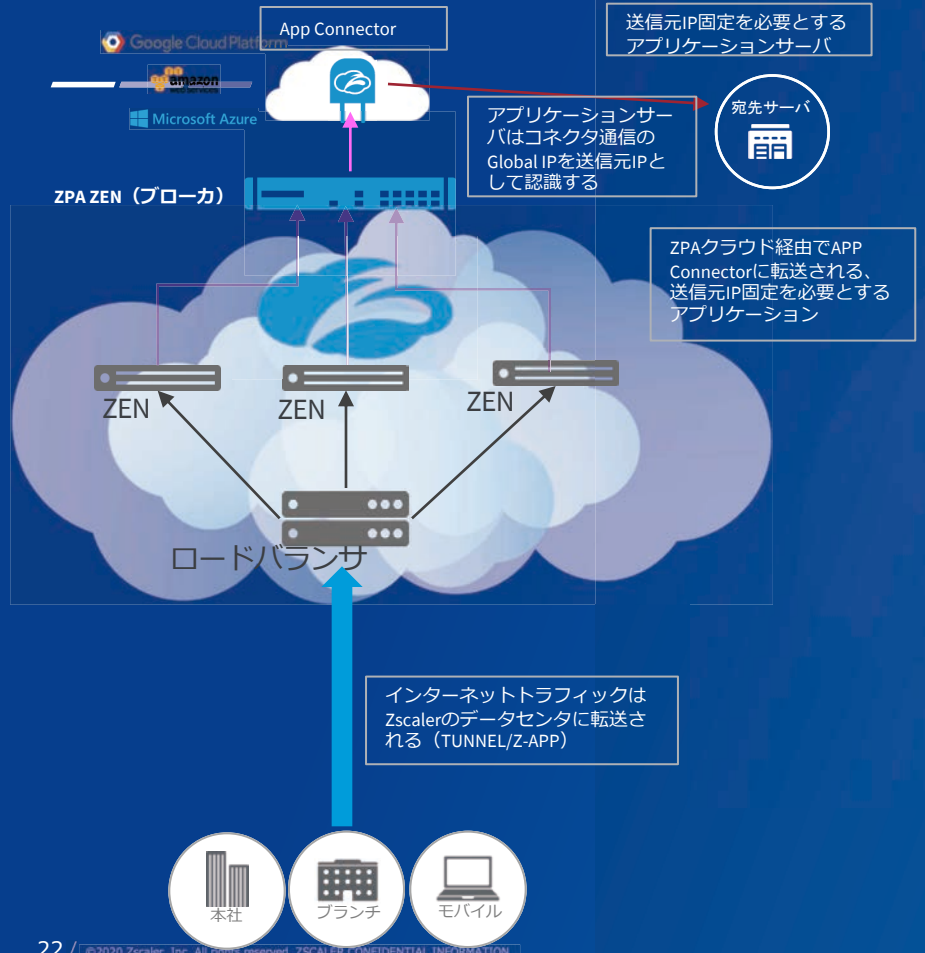
Zscaler Client Connector

モバイル・外部ユーザの端末からのセキュアなアクセスを実現

- ZIAとZPAの通信を自動切り替え
- iOS, Android, Windows,macOSに対応
- 機能概要
  - プラットフォーム共通の操作感
  - ポリシー強制オプション（OFFれない）
  - 社内ネットワークの自動検出
  - ユーザアトリビュート指定
  - ユーザに透過的な認証
  - SSL復号のための証明書を内包



ZPA App Connectorを利用した送信元IP固定化



- 送信元IP固定を必要とするトラフィックを選択してZPAクラウドに転送する機能を顧客に提供する
- ZscalerのZENとZPAの間のZ-Tunnel 2,0
- 定義されたポリシーに基づき、トラフィックがZPAクラウドに転送され、ZPAコネクタ経由で外に出る
- Webと非Webのトラフィックを処理できる
- ZIA UIのコネクタのプロビジョニング、監視、ZPA関連のレポート。SSOを利用してアクセスできる
- ZIA UIで定義するポリシー。ZPAクラウドに転送する必要があるトラフィックを定義する。APIコールによるZPAでのポリシーの自動化
- Application Connectorライセンスが必要

ZCSPM(Cloudneeti)

1 設定情報の収集

APIによるクラウドサービスとの連携

amazon web services　Microsoft Azure　Office 365

2 検出内容のまとめ

1,700以上のセキュリティポリシーと14のコンプライアンスフレームワーク参照

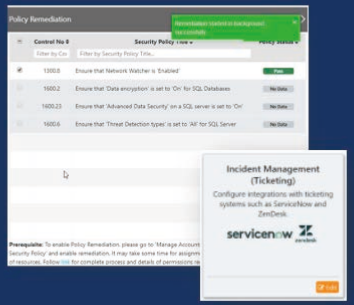
CIS, CSA, NIST 800-53, NIST CSF, ISO 27001, PCI-DSS, HIPAA, GxP, NCSC (UK), FFIEC, RBI (India), GDPR, SOC 2

3 優先順位とリスク対応整理

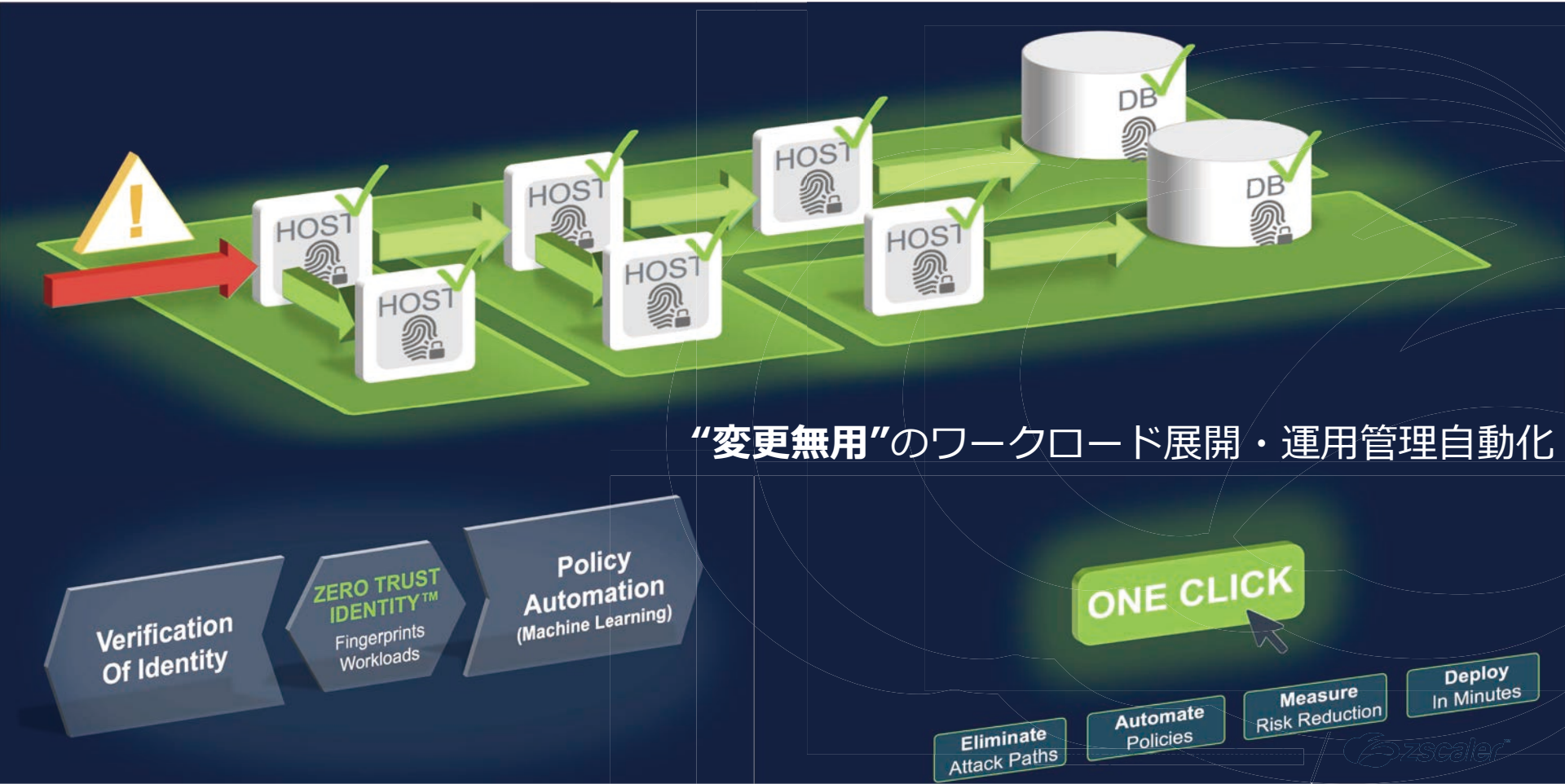
リスク分析に基づく機械学習を活用しセキュリティ上のリスクを取りまとめ

4 問題の解決

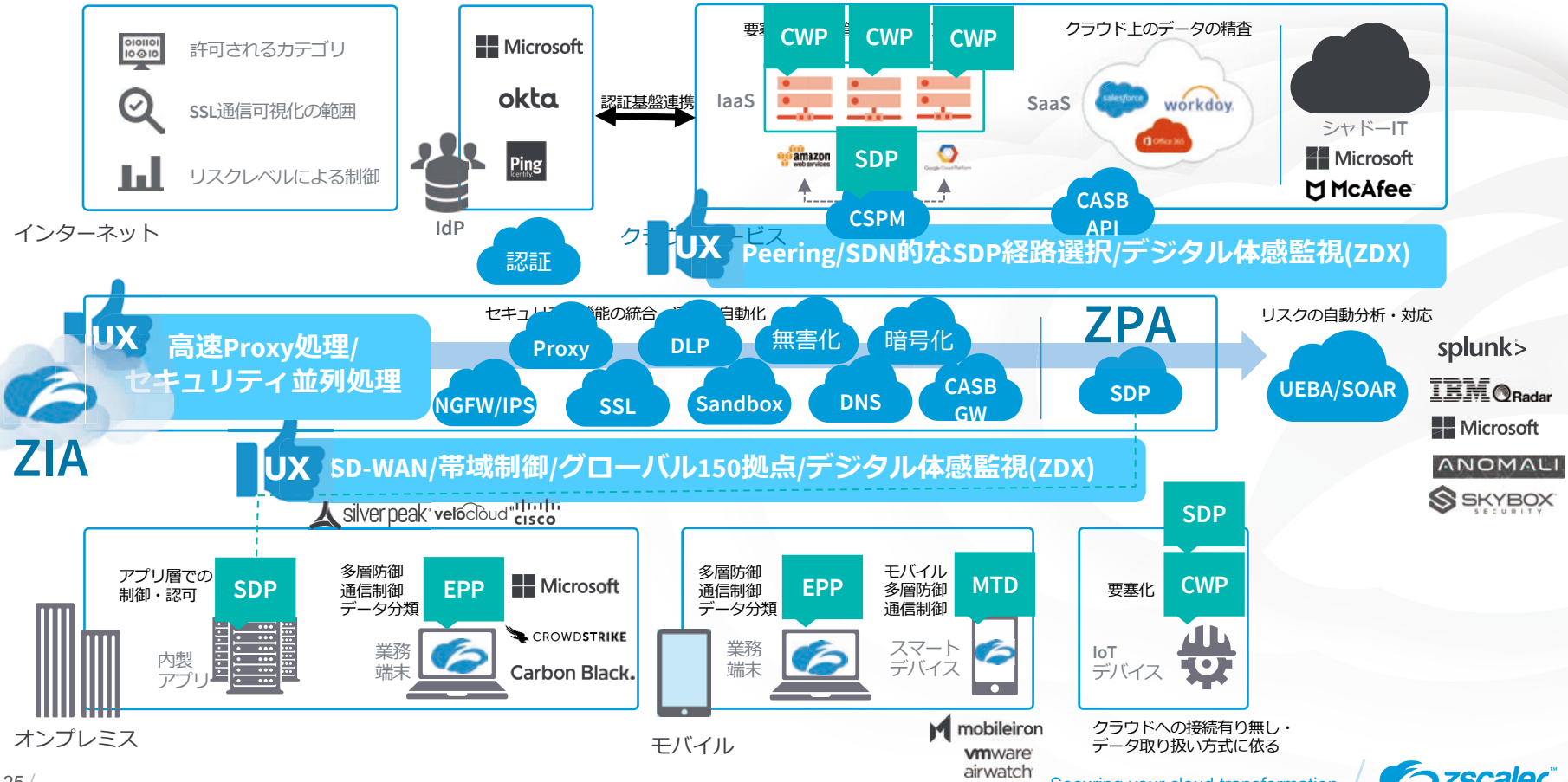
修正の提案と自動修正の提供



CWP (Edgewise)



SASE –Zscaler eco-system



Securing your cloud transformation

zscaler

Thank You

NEXT STEPS