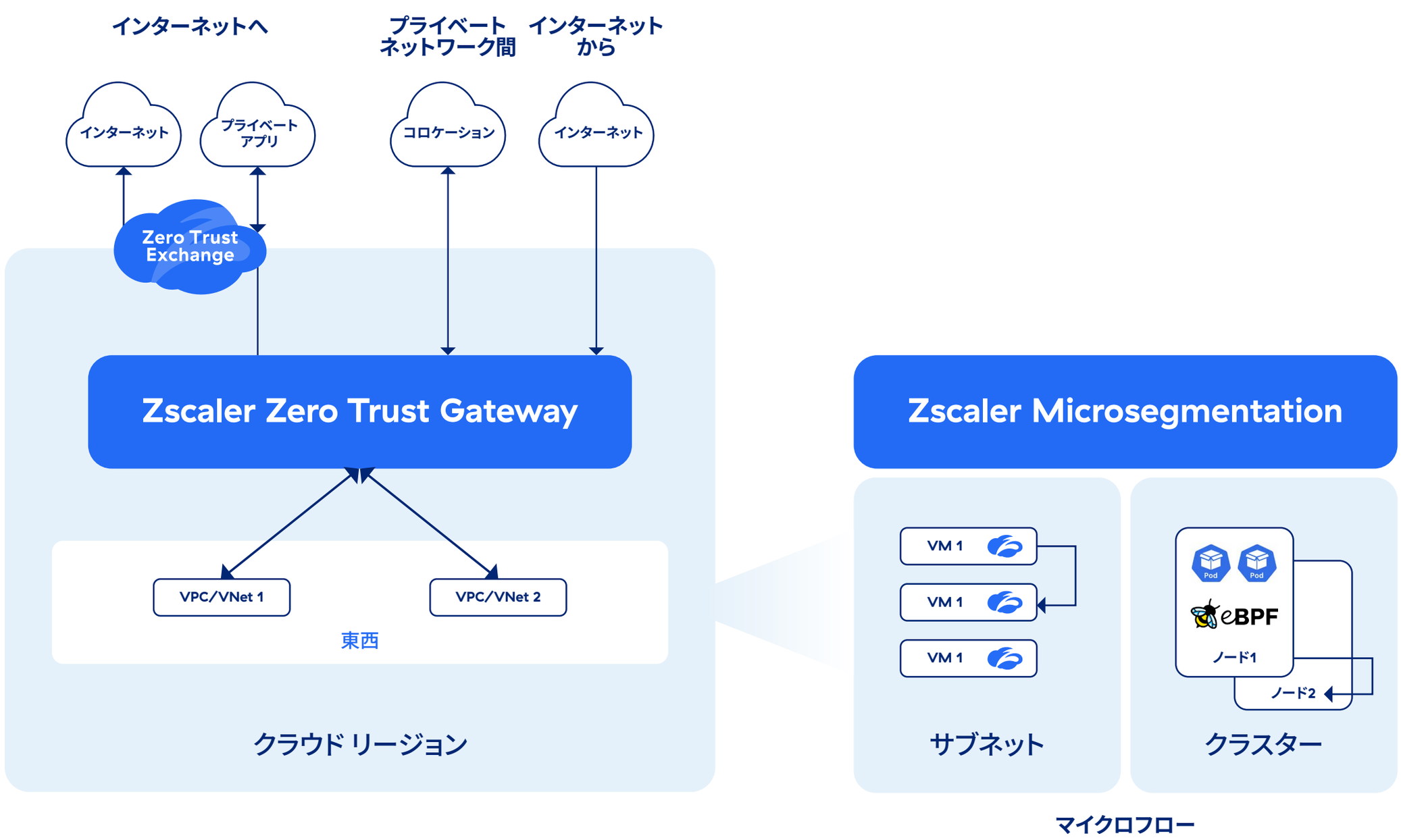
Zero Trust Cloud

あらゆるクラウドのすべてのワークロードを接続、保護する最もシンプルな方法

データシート

デジタル トランスフォーメーションの拡大を背景にマルチクラウド時代となった現在、ワークロードは爆発的に増加しています。企業が成功を収めるには、この重要なリソースを可視化し、サイバー攻撃やデータ流出を防止する必要があります。

ネットワーク ファイアウォールや IPSec VPN といった従来のセキュリティ製品は、古いアーキテクチャーに基づいて構築されており、特有の欠陥を抱えています。こうした製品は、資産に関するリアルタイムの可視性や一貫した保護に欠けるうえ、攻撃対象領域の拡大やラテラル ムーブメントを招きます。結果として、運用の複雑さやコストの増大は避けられません。



Zero Trust Gateway/ConnectorとZscaler Microsegmentationによるすべてのトラフィック経路の保護

Zero Trust Cloud は、マルチクラウド環境に包括的なセキュリティを拡張します。即時のメタデータやプロセスレベルのインサイトによってリアルタイムの可視性を提供し、正確な資産インベントリーを実現します。すべてのトラフィック経路とクラウドにわたって一貫した脅威対策とデータ保護を提供し、単一のプラットフォームで運用コストを削減します。VM やコンテナーからのマイクロフローの可視性と制御に対応するために、インテリジェントなホストベースのマイクロセグメンテーションも提供します。

マルチクラウド環境へのゼロトラスト アーキテクチャーの拡張

Zero Trust Cloudでは、次のことが可能です。

クラウド リソースのリアルタイムでの可視化

Zero Trust Cloud は、クラウド リソースをリアルタイムで可視化します。

- **即時のメタデータ収集：**クラウド インフラとシームレスに統合し、リソースの作成、変更、削除時にクラウド メタデータ (タグ、ラベル、属性) を自動的に収集します。
- **プロセスレベルの詳細なインサイト：**Zscaler Microsegmentation エージェントは、VM やコンテナー環境からプロセスレベルのきめ細かなメタデータを提供します。
- **正確な資産インベントリー：**手動による介入なく VPC/VNet、サブネット、VM/EC2 の詳細かつ正確なリージョンレベルのインベントリーを提供します。

一貫性のある包括的な脅威対策とデータ保護

マルチクラウド環境において統一されたセキュリティ ポリシーを施行します。

- **すべてのトラフィック経路の保護：**送受信トラフィック、東西トラフィック、プライベート ネットワーク トラフィック、マイクロフローなどを保護します。
- **ゼロデイ攻撃の防止：**TLS インスペクションと脅威対策をクラウドならではの規模で行います。
- **情報漏洩の阻止：**インラインのデータ保護を適用します。

運用コストと複雑さの軽減

クラウド内のすべてのワークロードを保護する単一のセキュリティ プラットフォームを使用します。

- **ワークロードの保護：**AWS、Azure、GCP などの主要なクラウド サービス プロバイダーのワークロードを 1 つの統合プラットフォームで保護します。
- **セキュリティの展開の自動化：**Zscaler の API、Hashicorp Terraform、AWS CloudFormation などのプログラム可能なインターフェイスを通じて自動化します。
- **クラウド間のサポート：**クラウドとデータ センター間、リージョン間、VPC/VNet 間、サブネット間、ホストやノード間もサポートします。

ミッションクリティカルなアプリケーションの保護

ホストベースのマイクロセグメンテーションにより、規制やコンプライアンス要件を順守し、ワークロード セキュリティを強化します。

- **プロセスレベルの可視性：**クラウド リソースを個々のプロセスレベルで詳細に把握できます。
- **リソースの自動グループ化：**機械学習を活用し、トラフィック フロー分析に基づいて最適なリソース セグメントを自動的に推奨、定義します。
- **厳格な最小特権の施行：**セグメントごとにきめ細かなセキュリティ ルールを適用して、必要最低限のアクセスのみを許可し、ラテラル ムーブメントを制限します。

Zero Trust Gateway/Connector の機能

エディション	詳細
Advanced	• TLS/SSL インスペクション • Cloud Firewall (Standard) • 高度な脅威対策 • NSS ログ フィード (ログの復旧なし) • クラウド間のストリーミング • DNS Essentials • ファイル制御 • 動的なリスクベースのアクセスとセキュリティ ポリシー • SaaS セキュリティ (CASB Standard) • ワークロード間のセグメンテーション (ZPA) • アプリ検出 (ZPA) • データ保護 (監視モード) • Zscaler Source IP Anchoring
Advanced Plus	• Workloads Advanced エディションで利用可能なすべての機能 • ワークロードとインターネット間の保護 • IPS、データ保護 • NSS ログ フィード (ログの復旧あり) • DNS Advanced • Cloud Sandbox (Advanced) • カスタム ルート証明書 • SaaS セキュリティ • Cloud Firewall (Advanced) • データ保護 (インライン) • 完全データー致 (EDM) • インデックス文書一致 (IDM) • 光学式文字認識 (OCR)

Zscaler Microsegmentation の機能

エディション	詳細
Advanced	• サポートされているプラットフォーム – Windows、Linux、Kubernetes (Amazon EKS) • クラウド ワークロード (AWS、Azure、GCP) の可視化 • アプリケーションの詳細を含むトラフィック フローの可視化 • アプリケーションの依存関係マップ • ポリシーの施行 • 高度なポリシー範囲設定のためのアプリゾーン • バージョン プロファイルを使用した組み込みエージェントのアップグレード • 高度なフロー分析 • ログ ストリーミング サービス (LSS) を使用した SIEM との統合 • ワークロード検出サービス – マルチクラウドのメタデータをリアルタイムで可視化するための Zero Trust Gateway/Connector の統合

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange™ は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/jp**

Zero Trust Everywhere