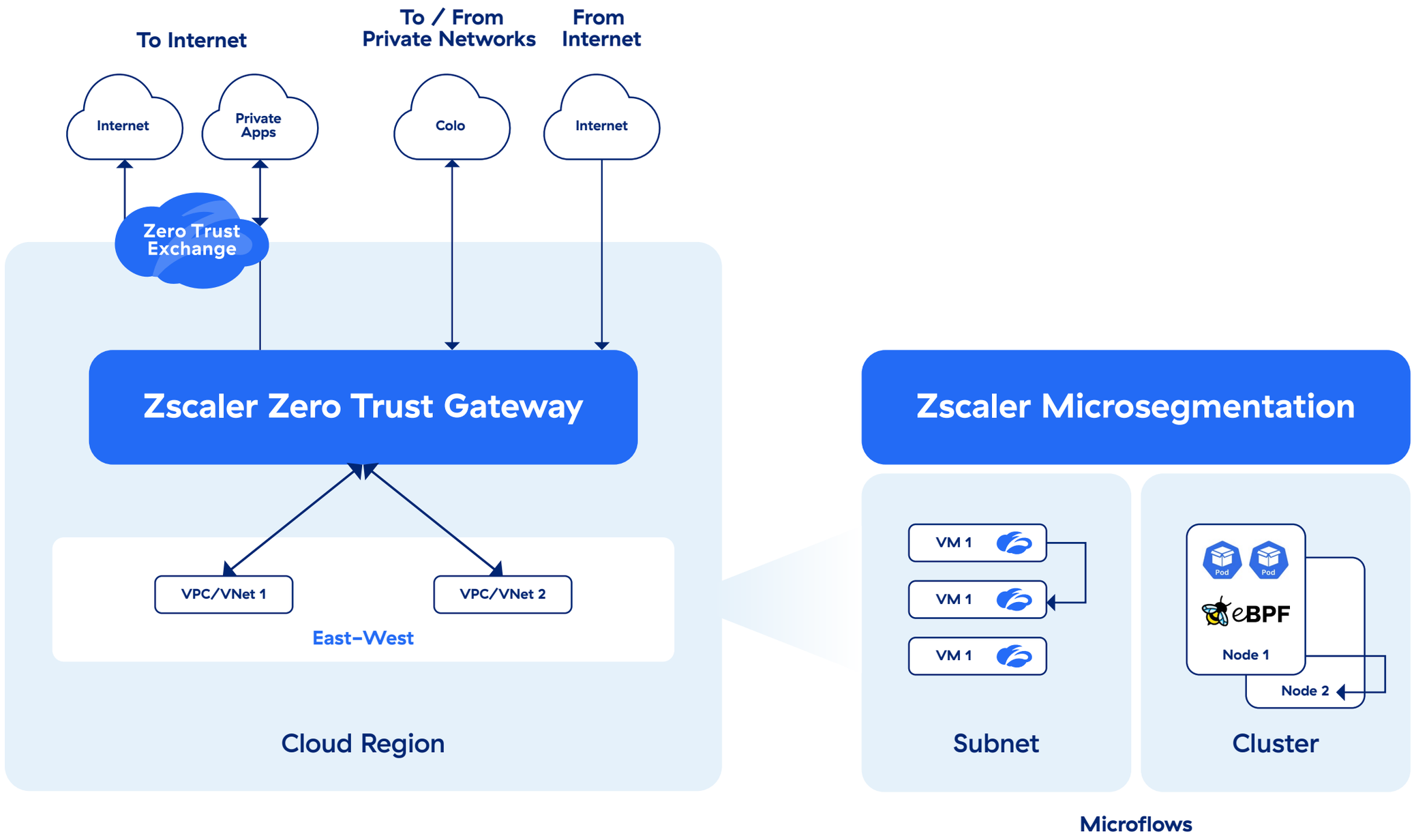
Zero Trust Cloud

The simplest way to connect and secure every workload across any cloud.

DATASHEET

The multicloud era, spurred by digital transformation, means an explosion of workloads. Your business must have visibility into these key resources and prevent cyberattacks and data loss to thrive.

Traditional security offerings such as network firewalls and IPSec VPNs are built on legacy architectures with inherent flaws. They lack real-time asset visibility, provide inconsistent protection, expand the attack surface, and enable lateral movement. This inevitably increases operational complexity and cost.



Secure all traffic paths using Zero Trust Gateway/Connectors and Zscaler Microsegmentation

Zero Trust Cloud extends comprehensive security to your multicloud environment. It provides real-time visibility with instant metadata and process-level insights, delivering an accurate asset inventory. Gain consistent threat and data protection across all traffic paths and clouds, reducing operational costs with a single platform. To address visibility and control for microflows from a VM or Container, the solution offers intelligent host-based microsegmentation.

Extend zero trust architecture to multicloud environment

With Zero Trust Cloud, you can:

REAL-TIME CLOUD RESOURCE VISIBILITY

Get real-time visibility into your cloud resources with Zero Trust Cloud

- **Instant Metadata Capture:** Seamlessly integrates with cloud infrastructure to automatically collect cloud metadata (tags, labels, attributes) upon resource creation, modification, or deletion.
- **Deep Process-Level Insights:** Zscaler Microsegmentation agents provide granular, process-level metadata from VM and container environments.
- **Accurate Asset Inventory:** Delivers a detailed and precise region-level inventory of VPCs/VNets, subnets, and VMs/EC2s without any manual intervention.

GAIN CONSISTENT, COMPREHENSIVE THREAT AND DATA PROTECTION

Enforce uniform security policies in a multicloud environment

- **Secure all traffic paths** including Ingress and Egress traffic, East-West traffic, Private Network traffic and Microflows.
- **Prevent zero day-attacks** with cloud-scale TLS inspection and threat protection.
- **Stop data leaks** with inline data protection.

REDUCE OPERATIONAL COST AND COMPLEXITY

Use one security platform to protect all workloads in your clouds

- **Secure workloads** across major cloud service providers including AWS, Azure, and GCP using one unified platform.
- **Automate security deployments** through programmable interfaces including Zscaler APIs, Hashicorp Terraform and AWS CloudFormation.
- **Support cloud to cloud**, cloud to data center, region to region, VPC/VNet to VPC/VNet, subnet to subnet, and between hosts or nodes.

SECURE MISSION CRITICAL APPLICATIONS

Achieve regulatory and compliance requirements and strengthen workload security with host-based microsegmentation

- **Process-Level Visibility:** Gain deep insight into cloud resources at the individual process level.
- **Automated Resource Grouping:** Leverage machine learning to automatically recommend and define optimal resource segments based on traffic flow analysis.
- **Strict Least Privilege Enforcement:** Apply granular security rules per segment, granting only essential access and limiting potential lateral movement.

Zero Trust Gateway / Connector Features

EDITION	DETAILS
Advanced	• TLS/SSL Inspection • Cloud Firewall (Standard) • Advanced Threat Protection • NSS Log feed (No Log Recovery) • Cloud to Cloud Streaming • DNS Essentials • File Control • Dynamic, Risk-Based Access & Security Policy • SaaS Security (CASB Standard) • Workload-to-Workload Segmentation (ZPA) • App Discovery (ZPA) • Data Protection (Monitor Mode) • Zscaler Source IP Anchoring
Advanced Plus	• Everything available in Workloads Advanced edition • Workload to Internet Protection • IPS, Data Protection • NSS Logfeed (With Log Recovery) • DNS Advanced • Cloud Sandbox (Advanced) • Custom Root Certificate • SaaS Security • Cloud Firewall (Advanced) • Data Protection(Inline) • Exact Data Match (EDM) • Index Document Match (IDM) • Optical Character Recognition (OCR)

Zscaler Microsegmentation Features

EDITION	DETAILS
Advanced	• Platform supported – Windows, Linux and Kubernetes (Amazon EKS) • Visibility into your cloud workloads (AWS, Azure, GCP) • Traffic flow visibility including application details • Application dependency maps • Policy enforcement • Appzones for advanced policy scopes • Built-in agent upgrades using version profiles • Advanced flow analytics • Integration with SIEM using Log Streaming Service(LSS) • Workload Discovery Service – Zero Trust Gateway /Connector integration for real-time visibility into multicloud metadata

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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

zscaler™

Zero Trust Everywhere