Zscaler Zero Trust Cloud: Modern Security for Multi-Cloud Workloads

The Simplest Way to Secure Every Workload, Everywhere

SOLUTION BRIEF

Navigating Multi-Cloud Security

Securing workloads across multiple clouds, regions, and availability zones is a critical challenge for enterprises. Workloads require diverse traffic paths to connect seamlessly with the internet, Saas applications and private applications. At the same time, mission-critical workloads running in these environments must remain isolated from evolving threats. Traditional security and networking models are ill-suited for this complexity, leaving organizations struggling to protect their cloud environments in a scalable, cost-efficient way.

Pitfalls of Traditional Security

Legacy security frameworks consisting of firewalls, VPNs, and private networks fail to meet the requirements of cloud-driven architectures.

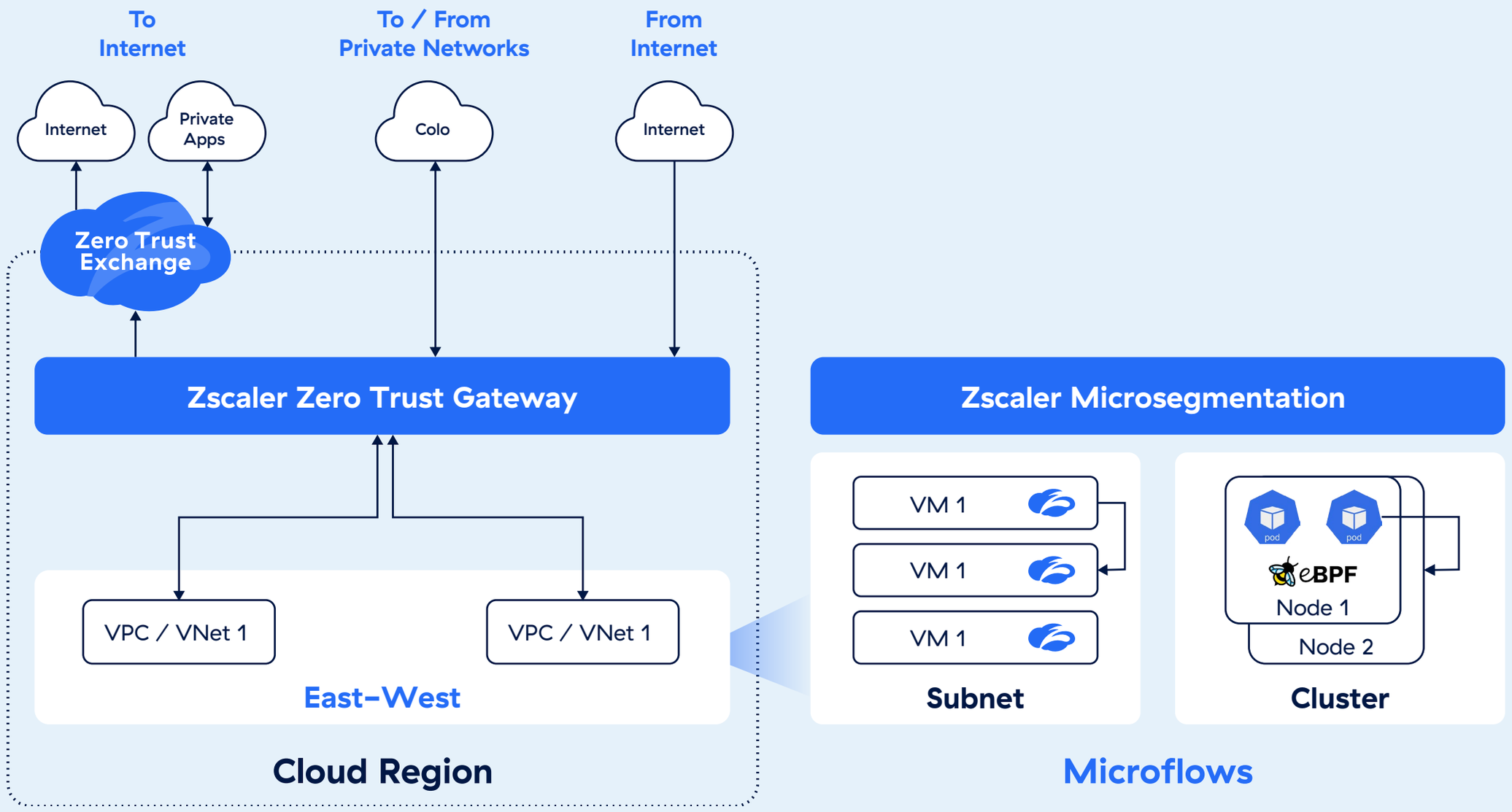
These tools introduce several risks and inefficiencies:

- **Expanded attack surface:** Every exposed firewall is a potential entry point for attackers.
- **Lateral movement of threats:** VPNs lack segmentation, allowing threats to spread internally once they gain access.
- **Operational complexity:** Managing security across multiple cloud service providers is inconsistent, inefficient, and expensive.

As a result, organizations face inconsistent threat and data protection across multi-clouds.

Zscaler Zero Trust Cloud

Zscaler Zero Trust Cloud revolutionizes workload security by eliminating dependency on traditional firewalls, VPNs, and private networks. Organizations gain standardized, cloud-native zero trust controls that extend across multi-cloud environments.



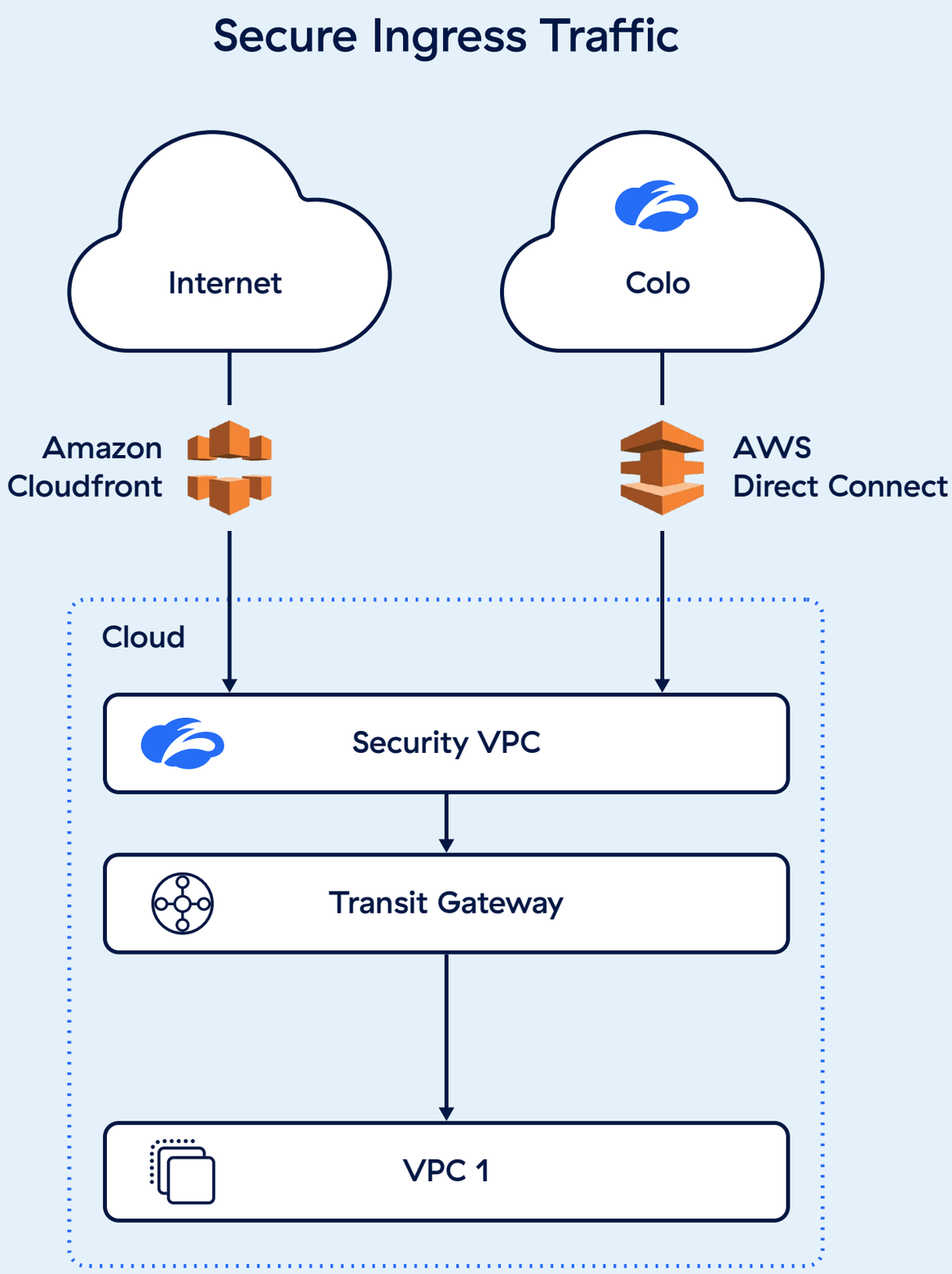
Essential Capabilities

Zero Trust Cloud provides consistent threat and data protection for workloads. It reduces attack surface and eliminates lateral threat movement. It reduces operational complexity and costs. You can deploy in less than 10 minutes using Zero Trust Gateway that allows customers to consume the features of Zero Trust Cloud as a cloud native service that is fully managed by Zscaler. Now let us dive into the key capabilities of Zero Trust Cloud.

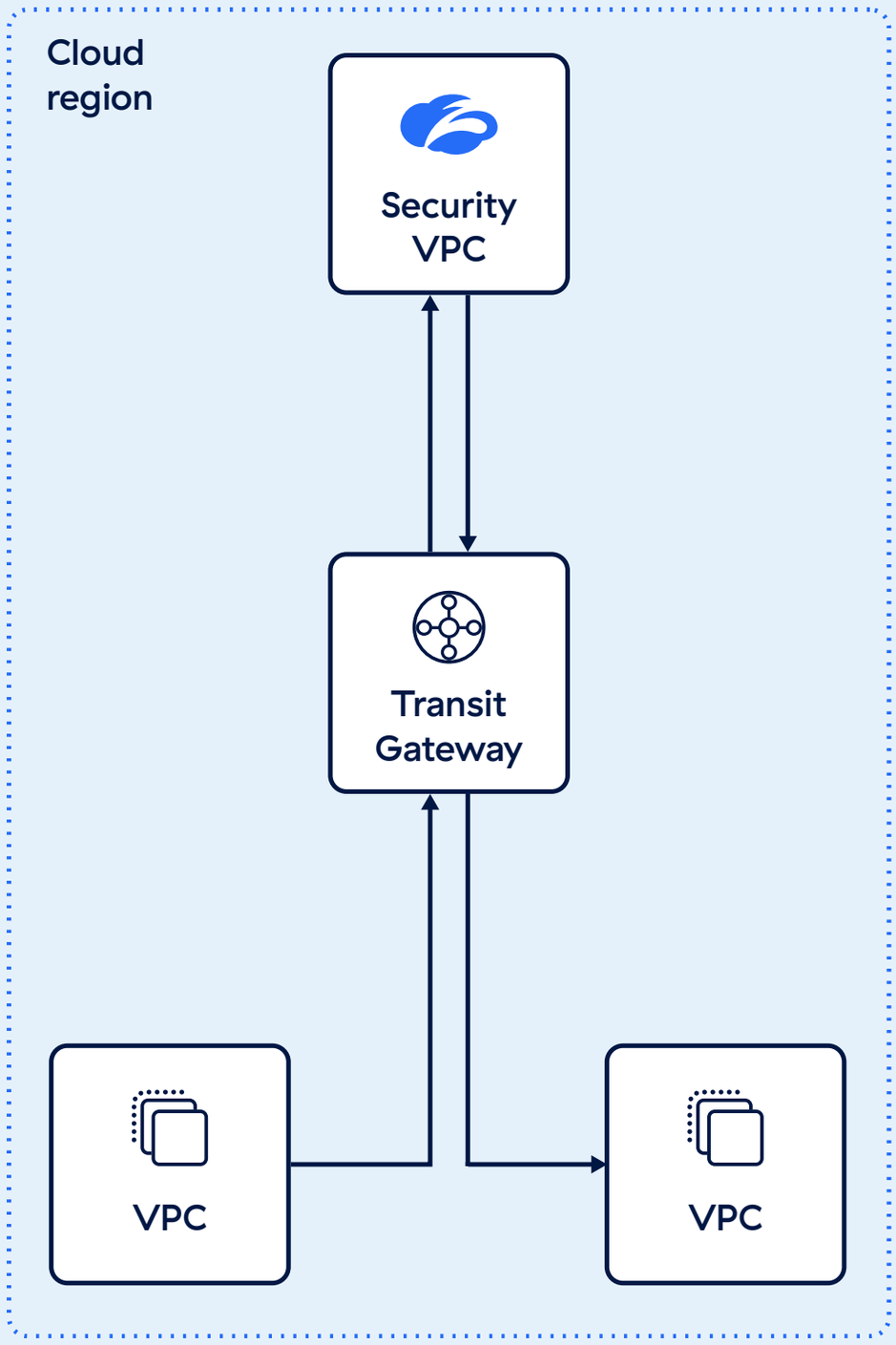
Secure Ingress and Egress Traffic

Enable secure connectivity between workloads and internet or SaaS apps.

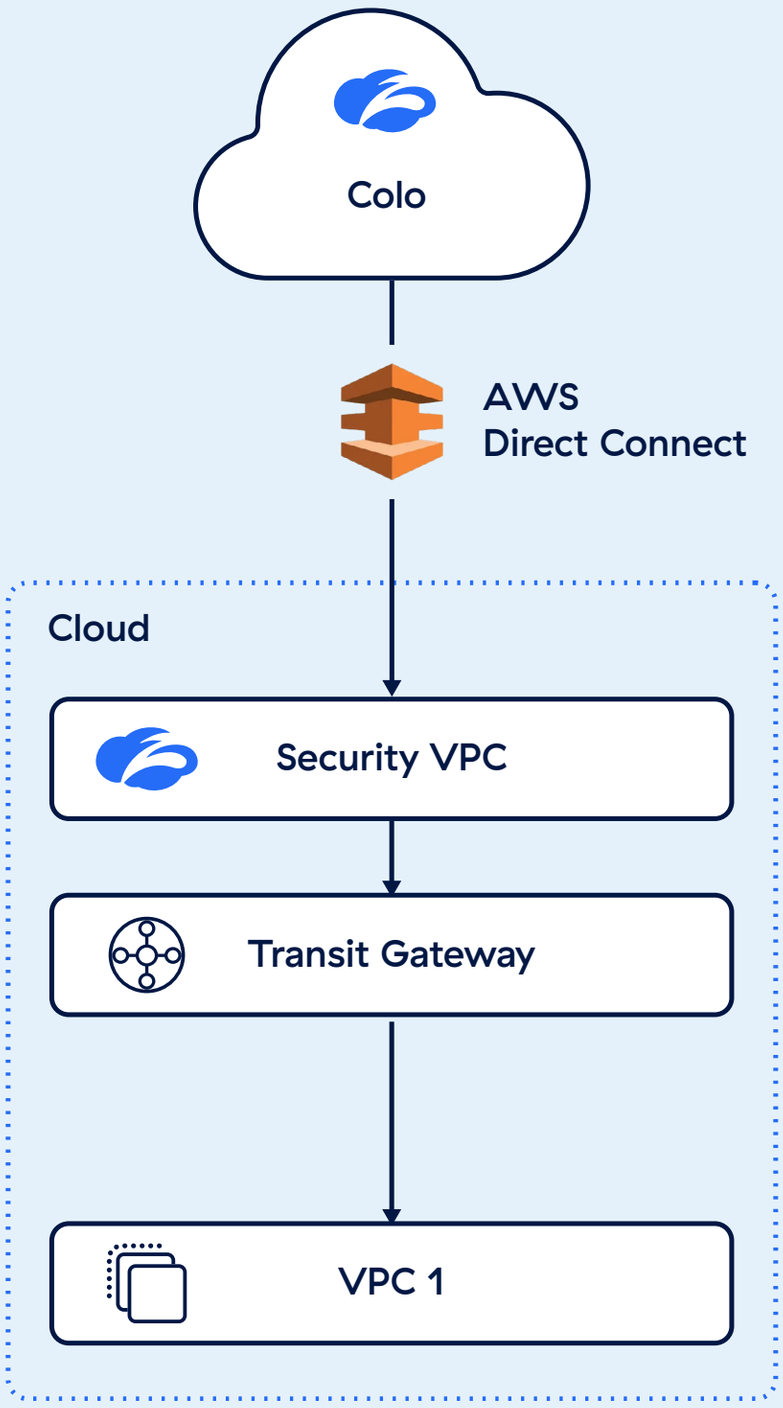
- Secure egress traffic with advanced threat protection and cloud scale TLS inspection.
- Stop data leaks in outbound traffic with inline data loss prevention.
- Enforce strict controls on outbound and inbound connections.



Secure traffic between VPC / VNet in the same Cloud region



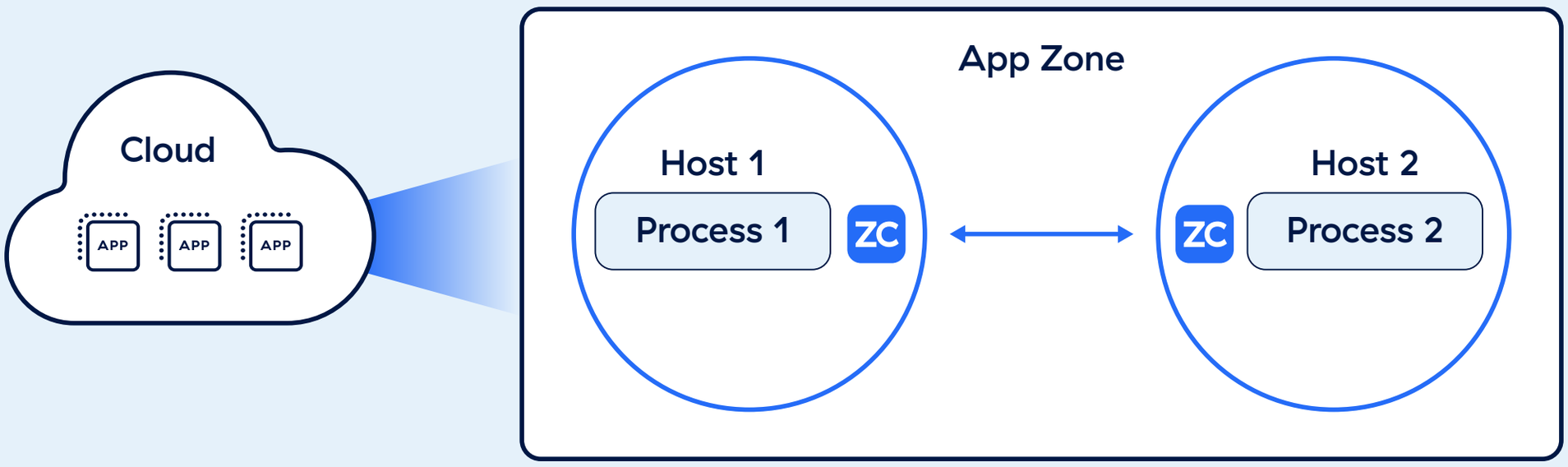
Secure traffic between Colo and Cloud



Secure East–West Traffic

Secure your workloads communicating with each other.

- Protect bi–directional traffic between your Colo and Cloud using local inspection.
- Secure VPC to VPC/VNet to VNet connections in the same region.



Microsegment Workloads

Isolate and protect high risk applications.

- Gain real-time visibility into resources.
- Streamline policy management with real-time, AI-suggested rules
- Reduce the attack surface with granular segmentation policies at application level.

These capabilities help organizations to effectively address 5 key use cases:

- Protect AI powered software development like Devin or Cursor without slowing down innovation.
- Eliminate security silos across AWS, Azure, and GCP with a single policy framework.
- Reduce cloud / virtual firewall sprawl. Minimize cost and complexity.
- Use identity-based microsegmentation to isolate critical apps (like Oracle) and contain breaches instantly.
- De-risk “lift and shift” projects (like SAP migration to cloud) by decoupling security from the network.

Next Steps

Standardize your workload security across multi-cloud with Zero Trust Cloud. Achieve unified protection for your workloads across any environment, eliminating lateral threat movement and reducing operational complexity. To know more visit **Zero Trust Cloud webpage**.

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**.

zscaler™

Zero Trust Everywhere