SOLUTION OVERVIEW

Zero Trust Cloud Networks

The New Standard in Cloud Security for Hybrid and Multi-Cloud

Hybrid Applications Present New Security Challenges

The public cloud is quickly becoming the next-generation datacenter for enterprises, but it has brought new complexities few enterprises are prepared for. Public cloud infrastructure is owned and operated by the cloud service provider (CSP). Under the shared responsibility model for security and compliance, everything at the endpoint operating system level and up (applications, networking and security) is left to the enterprises to figure out.

While applications are migrating to the cloud, key corporate services such as LDAP and critical databases have stayed on-prem. Any hybrid connection from the cloud to those resources could expose the corporate network to new vulnerabilities. Traditional tools, such as VPNs and private lines, were designed for IT/InfoSec to connect trusted remote sites. Since the public cloud is multi-tenant, the conventional trust model is disrupted. Traditional tools are no longer sufficient to contain and segment hybrid workloads.

Traditional tools were also deployed by specialists following a careful and methodical design and review process as part of the corporate always-on infrastructure. This is because routing or firewall misconfigurations could expose the corporate network or even bring it down for other applications. In the cloud, IT and InfoSec teams now share implementation responsibilities with DevOps teams, who don't have the same expertise. The truth is cloud projects simply can't afford to get bogged down in weeks or months of review – cloud migration has the attention of the C-suite and the board with high priority for business.

CoIP® Platform for the Hybrid and Multi-Cloud

- Industry best-practice Zero Trust Networking for cloud application segmentation
- Works on any public or private cloud, and on any on-premises environment
- Mutual authentication and end-to-end encryption
- Micro-segmentation blocks north-south and east-west threat movements
- Overlay fabric deploys without touching existing network and security infrastructure
- Granular protection down to the app and container level

Companies need new tools to create new cloud security best practices. The InfoSec and corporate IT teams need to maintain visibility and control, while the business operation team (e.g. DevOps) needs design patterns that can be implemented at cloud speed. They need tools to create unified hybrid networks and security, allowing the enterprise to enforce consistent security policies for cloud migration.

zentera™

zentera™

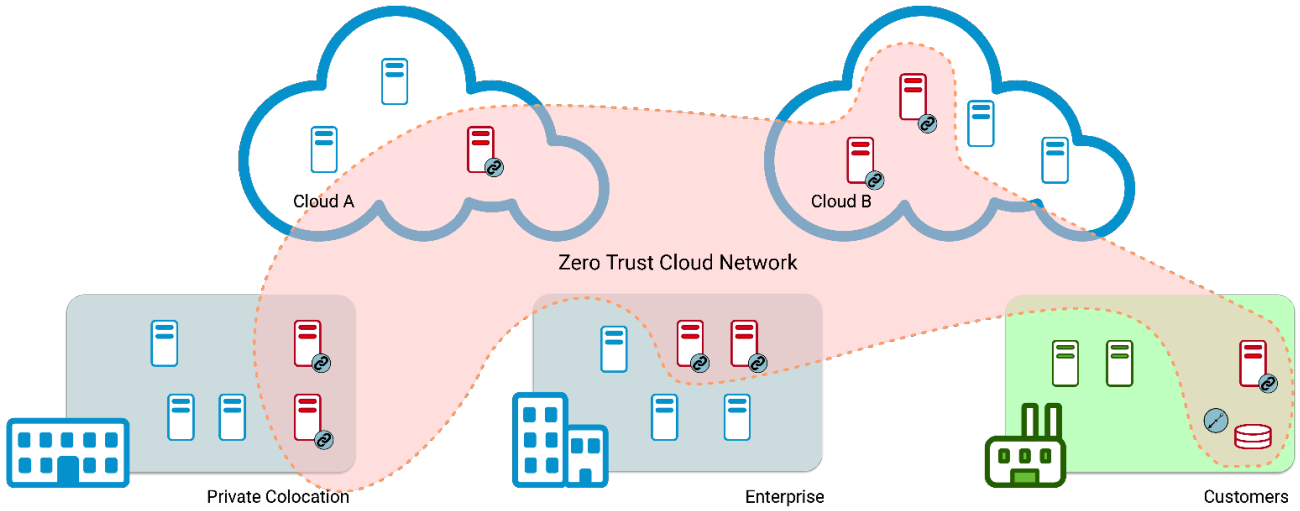
SOLUTION OVERVIEW
Zero Trust Cloud Networks

Enter Zentera's CoIP® Platform: Zero Trust Networking

Zero Trust is one of the most promising solutions to address cybersecurity challenges in the cloud today. The principal idea of Zero Trust is that the cloud network is fragmented and not to be trusted – access is granted, not based on hybrid network topology, but on authentication that is checked at *all* points of use, in the cloud or on-prem. Today's enterprise networks are like an airport security checkpoint; once you show your ticket and ID (WiFi password or VPN credentials), you are "trusted" to roam freely inside the secure area. However, unlike the airport (where your boarding pass is checked to make sure you board the correct plane), there is no further check before you access the other computers, file servers, or printers once you are inside the enterprise networks. Zero Trust Networking upgrades the enterprise network with security protocols proven in the real world, requiring all points of use to prove that it is authorized to access a machine before it can even make a network connection.

Zentera's CoIP Platform protects individual VMs, applications, and even containerized micro-services with a micro-network that cloaks machines, rendering them invisible to the physical network, with mutually-authenticated and encrypted TLS tunnels to protect application traffic against snooping. Its powerful policy engine enables access permissions and micro-segmentation rules to be defined based on a combination of certificate-based identity and network and application meta-data. Finally, its monitoring and logging provides complete visibility and observability over all applications. This micro-network runs as the unified security connection, overlay fabric across hybrid cloud and multi-cloud, without requiring VPN or opening the corporate boundary.

CoIP Platform contains and protects hybrid and multi-cloud application workloads by creating connectivity and restricting access only to defined applications and services. Access granted to one app can't be abused by another app, even if they run on the same host; this significantly minimizes the attack surface in the multi-tenant cloud environment and dramatically reduces the risk when connecting back to the corporate network, compared to legacy network security tools. Finally, CoIP Platform deploys without touching existing network and security. Security policies defined by InfoSec and IT can be implemented by business operation teams with self-service APIs to reduce IT tickets, restoring agility to cloud operations.



www.zentera.net