



Data Sheet:

Zentera Systems

CoIP Cloud-Ready Enclave

HIGHLIGHTS

Software-Defined Perimeter

Build an enclave (CoIP Enclave) on demand across multicloud and enterprise datacenters.

Defense-in-Depth

Deploy advanced security capabilities as standalone or together to protect application workloads.

Workload Shield

Shield workloads with CoIP Enclave on demand across multicloud and enterprise datacenters.

Security Policy Migration

Migrate security policies to any cloud by leveraging CoIP Enclaves.

Security Compliance

Achieve security compliance through CoIP capabilities.

Enterprise applications are typically coupled with their underlying network and security infrastructures. Both network and security infrastructures are static in nature and unable to move with an application when it moves from an enterprise datacenter to the cloud. Additionally, the cloud does not support the conventional enterprise security model, which is based on perimeter and network infrastructure. Therefore, finding a good solution that allows enterprises to be cloud-ready while maintaining security and compliance can be challenging.

The CoIP Cloud-Ready Enclave™ solution enables enterprise workload migration into the cloud by decoupling enterprise workloads from their existing network and security infrastructures and makes the workloads dynamic and ready for cloud migration.

Cloud-Ready Enclave uses the CoIP® (Cloud over IP®) Platform, which secures workloads in the multicloud ecosystem by connecting them through a unified virtual overlay network. In addition to enabling enterprise workload migration, the Cloud-Ready Enclave also migrates the enterprises' existing security policies, and offers micro-segmentation, encryption and application interlock, a feature that permits only specific applications to access the CoIP overlay network.

Lastly, the Cloud-Ready Enclave offers adaptive discovery, a feature that identifies applications on compute endpoints to automate the application interlock capability. CoIP's security is deeply integrated with its virtual network overlay, shielding production workloads and cloud endpoints.

CoIP Cloud-Ready Enclave

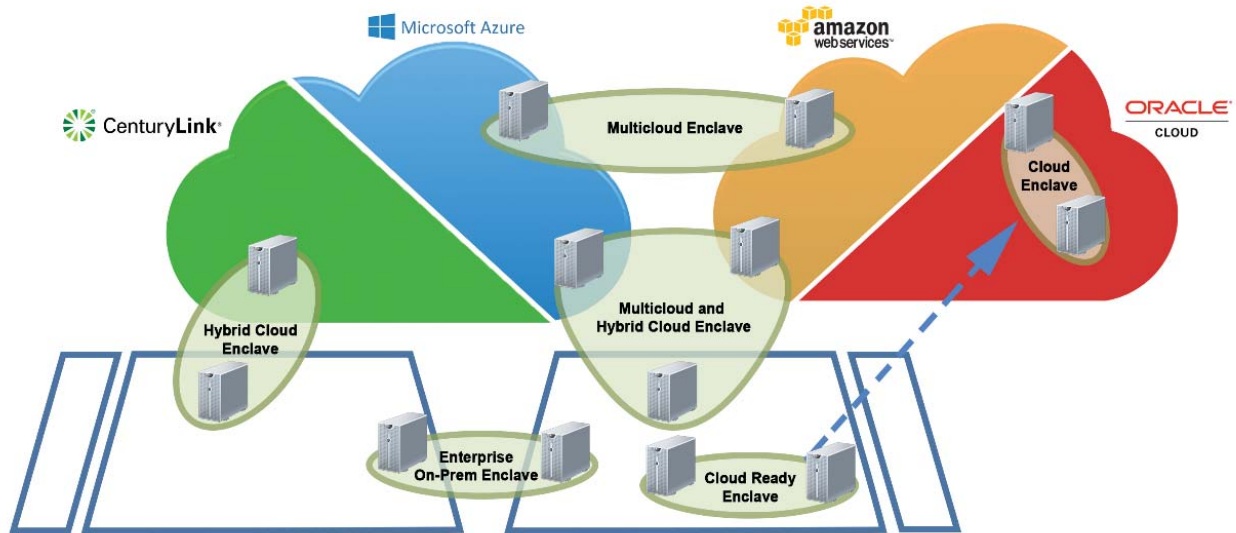


Figure 1: CoIP Cloud Enclaves

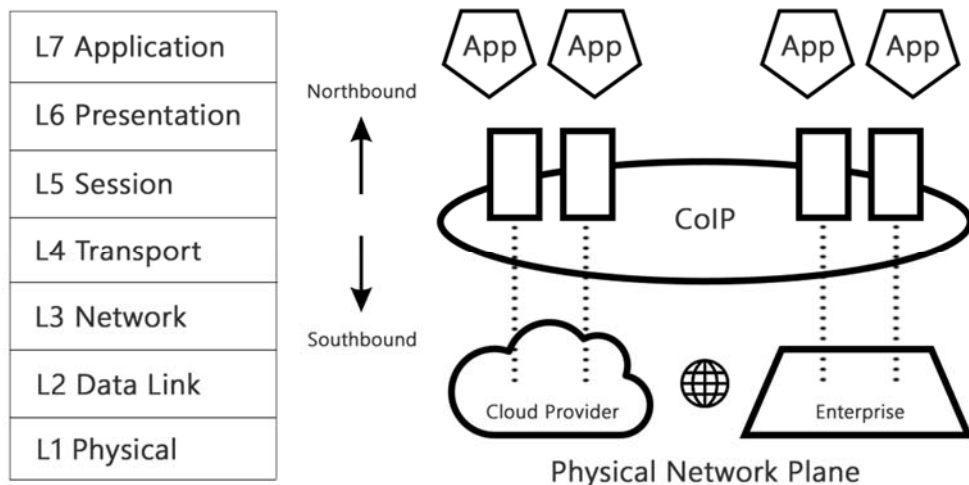
The CoIP Cloud-Ready Enclave (CCRE) solution allows enterprises to easily prepare workloads and make them ready to move to the public cloud. CCRE decouples applications from the underlying on-premise physical network and security infrastructures. Using the CoIP Network-in-Motion™ and CoIP Security-in-Motion™ capabilities, workloads can be simply moved between clouds or datacenters while maintaining and extending secure connectivity between the enterprise and the hybrid cloud.

BENEFITS

- | | | | |
|--|---|--|---|
| | Ease of management with unified network console across enterprise and cloud | | Unified security for cloud endpoints across cloud ecosystem |
| | Full enterprise control in any cloud datacenter | | Virtual network segregation for cloud applications on top of shared corporate networks |
| | Enterprise protection without altering corporate perimeter security & compliance | | Extremely rapid deployment— within days, not months or years |
| | Remote shielding of hybrid cloud workloads in any cloud | | |

CoIP Cloud-Ready Enclave Architecture

CCRE consists of a CoIP Controller™, CoIP Endpoints™, CoIP Edge Gateway and Zentera Network Switch (ZNS). Endpoints can be VMs, servers, and containers.



CoIP Controller

The CoIP Controller is the management portal for the CoIP platform. All policies and configurations are implemented centrally in the controller and pushed to the endpoints for enforcement. The CoIP controller enables and manages Application Profiles – which provision virtual infrastructures and security policies across the multicloud – to define the cloud-ready enclave using mouse clicks and programmable cloud APIs. The Controller can be a physical appliance or VM running in public and private clouds, or running in the enterprise datacenter.

Table 1: CoIP Controller Specifications and Performance for Physical Appliance

Hardware Appliance	Specifications	Performance
ZCA-1000	x86 Server with 4-core, 2.1GHz and 8G RAM, 2 1G NIC and 500G Storage	1G throughput and 10k endpoints
ZCA-5000	x86 Server with 12-core, 2.4GHz and 16G RAM, 4 1G NIC and 500G Storage	5G throughput and 15k endpoints
ZCA-10000	x86 Server with 12-core, 2.4GHz, 16G RAM, 2 10G NIC and 500G storage	10G throughput and 30k endpoints

Table 2: CoIP Controller Specifications and Performance for Virtual Appliance

VM Configuration	Cloud Platform	VM Details	CoIP Endpoint Support
C3.xlarge	AWS	4 cores, 7.5G RAM, 2 x 40G SSD	Up to 5,000
C3.2xlarge	AWS	8 cores, 15G RAM, 2x 80G SSD	Up to 10,000
C3.4xlarge	AWS	16 cores, 30G RAM, 2 x 160G SSD	Up to 20,000
Basic A3	Azure	4 cores, 7G RAM, 120G Storage	Up to 5,000
Basic A4	Azure	8 cores, 14G RAM, 240G Storage	Up to 10,000
D14	Azure	16 cores, 112G RAM, 800G Storage	Up to 20,000

FEATURES



Virtual hybrid network across multiple cloud domains



Private routing plane and chamber firewall for application shield across outsourcing ecosystem



CoIP endpoint security via OS environment protection and application interlock along with network setting monitoring and enforcement



Cloud Connectors convert cloud APIs to mouse clicks



Data encryption and automated synchronization across domains



Secure remote terminal access without IP leakage

Supported OS Versions

- Windows
 - Windows 7, 8, 10
 - Windows Servers 2008, 2012, 2016
- Canonical Linux
 - Ubuntu Servers 16.04, 14.04, 12.04
- Red Hat Enterprise Linux
 - RHEL 4, 5, 6, 7
- CentOS
 - CentOS 6, 7
- SUSE Enterprise Linux
 - SELS 10.3, 10.4, 11.2
- Open SUSE Linux
 - Open SUSE 10.3, 12.2
- Amazon Linux
 - Amazon Linux AMI 2016.09, 2017.03

CoIP Endpoints

CoIP endpoints are the computing resources that sit on the cloud enclave and are part of a common network plane and security policy. Endpoints can be VMs, physical servers or containers. zLink is an agent that runs on endpoints and registers with the CoIP controller to be part of a CoIP enclave.

CoIP Edge Gateway

The CoIP Edge Gateway acts as a gateway to non-CoIP networks. It is a Layer 5 device that performs NAT and forwarding functions. The gateway does not provide routing functionality. An Edge Gateway can be a physical appliance or a VM.

Table 3: CoIP Edge Gateway Specifications and Performance

Form Factor	Specifications	Performance
Physical	x86 Server with 6-core, 2.4GHz and 12G RAM, 2 1G NIC and 200G Storage	Unlimited connections with 1G throughput
VM	Linux VM(CentOS/Red Hat recommended) with 2 vCPU, 4G RAM and 10G Storage	10 concurrent connection
VM	Linux VM(CentOS/Red Hat recommended) with 4 vCPU, 6G RAM and 20G Storage	30 concurrent connection
VM	Linux VM(CentOS/Red Hat recommended) with 6 vCPU, 8G RAM and 30G Storage	100 concurrent connection

Zentera Network Switch

The CoIP Switch Node performs switching functionality for CoIP packets when CoIP is used for WANs. ZNS supports clustering for scale, performance and high availability. ZNS can be a physical appliance or a VM, running in public and private clouds or in an enterprise datacenter.

Table 4: CoIP ZNS Specifications and Performance

Form Factor	Specifications	Performance
Physical	x86 Server with 6-core, 2.4GHz and 12G RAM, 2 1G NIC and 200G Storage	Up to 10k endpoints and 1G throughput
Physical	x86 Server with 12-core, 2.4GHz and 16G RAM, 4 1G NIC and 500G Storage	Up to 10k endpoints and 5G throughput
VM	Linux VM (CentOS/Red Hat recommended), with 6 vCPU, 8G RAM and 30G Storage	Up to 100 endpoints
VM	Linux VM (CentOS/Red Hat recommended), with 12 vCPU, 16G RAM and 50G Storage	Up to 500 endpoints
VM	Linux VM (CentOS/Red Hat recommended), with 24 vCPU, 32G RAM and 60G Storage	Up to 1k endpoints

About Zentera

Zentera Systems, named a Cool Vendor in Cloud Security 2017 by Gartner, Inc., secures workloads in the multicloud ecosystem by connecting them through a unified virtual overlay network. The CoIP® (Cloud over IP®) suite of infrastructure security and networking solutions works with any transport in any environment, does not interfere with existing infrastructure, and can be up and running in less than a day. It provides defense-in-depth for enterprise applications in the cloud, moving to the cloud or on-premise. CoIP is deployed for worldwide operations by global corporations. The company has received multiple honors, including Red Herring Top 100 2016 and 2017, and is based in Silicon Valley.

More Information

To learn more about Zentera CoIP platform, please contact your local account representative, or visit www.zentera.net