# CoIP® Access Platform
# Zero Trust Network Access
# Technology Backgrounder

## Introduction

The cybersecurity market is noisier than ever; the intent of this Technology Backgrounder is to help increase the signal-to-noise level by clearly explaining the terms and the context that makes them relevant, from Zentera's perspective, as well as Zentera's unique approach.

## What is Zero Trust?

Based on ideas first captured by the Jericho Forum in 2004, "Zero Trust" as a term was coined in 2010 by Forrester to describe a movement to replace implicit trust relationships with explicit authentication and policy-defined access control.

The core tenet of Zero Trust is "never trust, always verify."

For example, in existing enterprise networks, the network topology creates an implicit trust relationship. Just being connected to a particular subnet automatically grants an endpoint a certain set of access rights within the corporate network. Access from point A to point B is defined by the programming of IP addresses and all of the routers, and firewalls along the path, making it difficult to visualize and manage risk.

Replacing implicit trust with explicit trust surfaces any hidden security assumptions, making it easier to manage security and risk.

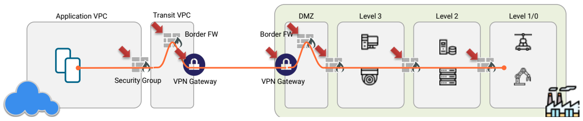
## Why do we need Zero Trust? What's wrong with today's security?

The traditional enterprise security model is based on a "hardened" perimeter. There were fewer applications, running in a few centralized datacenters, completely under the control of enterprise IT; in those days, securing the enterprise at the perimeter was good enough for the average company.

However, modern enterprise applications run in an increasingly complex environment. Applications and data have increasingly moved beyond the traditional corporate perimeter into the public cloud, already stressing the perimeter model. Add to that an increasingly mobile workforce, increasing requirements for ecosystem collaboration, and multi-cloud initiatives – the increased complexity is clear. At the same time, more of the business operations are digitized than before – companies are more susceptible to cyber threats than they used to be.

The tried-and-true tools in IT's arsenal – namely, firewalls, VPNs and VLANs – are now over twenty years old. With these tools, policy is defined by topology. They were defined to support static networks, and change management to support complex and dynamic requirements is a struggle.

Consider the connection shown below, between a cloud and resources in a factory environment.



Path connectivity is defined by as many as 6-12 different routers, switches, and firewalls along the path, each potentially managed by a different team. It's a difficult enough problem to analyze that the best way to validate connectivity is to try it – with a ping. It's even more difficult to prove that that's the *only* connectivity allowed.

## What is Zero Trust Network Access?

Zero Trust Network Access (ZTNA) is a secure method of delivering applications to users or other machines. Unlike traditional VPN + firewall solutions, which connect networks at Layer 3 and *then* attempt to filter, a ZTNA does not rely on the network topology at all, instead using trust factors such as certificates, geolocation, and application fingerprinting to establish the identity of applications.

By default, no connectivity exists. When an application sends a packet, the ZTNA automatically performs a policy check against a centralized database, to authenticate ("are you who you claim to be?") and authorize ("are you allowed to take this action?") the combination of user, endpoint, and application on both ends of the connection. Only when policy checks pass are packets allowed to be sent/received.

## What are the properties of an ideal Zero Trust solution for a modern network?

### *Simple Policy Definition*

Enterprises need tools to define and enforce simplicity. Security policies should be human-readable; they should be easily mapped to business requirements to streamline implementation and increase auditability for compliance.

### *Access That Follows Least Privilege*

Hybrid environments are complex, yet most corporate resources (VMs, containers, etc) are service-oriented and single-purpose – the in-house git server is not also hosting the Active Directory service. As a result, the ideal solution should have strong mechanisms to define whitelist policies to minimize the attack surface.

### *Portable to Any Environment*

Streamlining cloud adoption and enabling user mobility means companies need to be able to secure their applications and data wherever they happen to be. The ideal Zero Trust solution must shift the focus from network-level architecture to the application-level, operating in every environment and across traditional security boundaries. It should not be dependent on firewalls.

### *Co-Exists with Existing Networks and Applications*

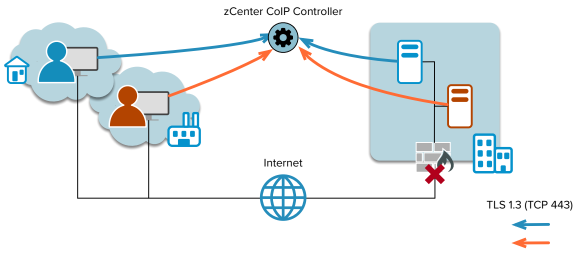
Enterprises cannot switch to this new paradigm overnight. It is important that a Zero Trust solution be deployable to protect critical applications without requiring a forklift upgrade, not only for cost reasons, but also to avoid disrupting the enterprise's existing infrastructure and operations.

## What is CoIP® Access Platform?

CoIP (Cloud over IP®) Access Platform is Zentera's Zero Trust Network Access solution. CoIP Access Platform creates a session-layer overlay network that connects applications with end-to-end security. CoIP runs on top of an unmodified Layer 3 IP network and creates a new network interface on machines it is deployed to; applications are unaware of the existence of the overlay network and need no modification take advantage of the additional security.

All traffic within the CoIP overlay is protected in transit with TLS 1.3 encryption and mutual authentication.

The overlay session network is completely decoupled from the traditional physical network. No physical connectivity exists between endpoints; application connectivity is built on-demand based on application traffic and whitelist connectivity policies. All connections (whether inbound or outbound) appear to be outbound TLS 1.3 tunnels, as shown in the figure below.



The zCenter CoIP Controller shown above is typically hosted by the enterprise (deployed in the corporate DMZ or in a cloud). Zentera also provides Zentera Air, a hosted version of CoIP served from a global network of points of presence.

The CoIP Access Platform provides strong Zero Trust security capabilities that enable consistent security policies in any infrastructure: on-prem, cloud, and hybrid.

## What can I do with CoIP Access Platform?

CoIP Access Platform supports many common applications, including:

- Providing employees and third parties with secure access, directed and locked to a specific resource within the enterprise

- Enabling cloud servers to access on-prem resources (e.g. code repositories) without creating inbound connections from the cloud

- Replacing risky always-on VPN connections for remote IoT devices with on-demand, point-to-point application tunnels that are locked to the IoT application

- Cloaking sensitive applications with micro-segmentation to reduce the attack surface

For more design concepts, please visit www.zentera.net.

## How does CoIP work?

A CoIP-enabled endpoint uses an overlay network for application traffic. The overlay network uses the existing physical IP network, but is decoupled from it – hosts are assigned a new overlay IP address which is not used for routing purposes and does not need to correspond to the network topology. As a result, the overlay IP address contains no useful information about the network or its location.

A CoIP-enabled endpoint can be programmed to block packets arriving through the normal physical interfaces ("default deny"). Packet traffic through the overlay network is allowed by whitelist policies ("whitelist allow"), removing the potential for unexpected network connectivity and holes in network security.

This combination of blocking the underlay and opening whitelisted access in the overlay creates a "chamber" which cloaks hosts within it from the physical network. Hosts outside of the chamber cannot communicate with hosts inside, unless allowed by policy. Approved traffic inside the chamber is transported through non-persistent and point-to-point encrypted tunnels.

The CoIP platform contains support to extend chambers across traditional perimeter firewalls, enabling admins to construct hybrid chambers that contain cloud and on-prem resources.

## What security capabilities does the CoIP Access Platform provide?

The CoIP platform supports numerous security controls, including:

*Identity*
Certificate-based mutual authentication for hosts; LDAP and SAML 2.0 for users; application fingerprinting for applications

*Policy Enforcement*
End-to-end application control ("application A on host B can talk to application C on host D using service E"); chamber micro-segmentation based on port, protocol, direction and application; geolocation

*Data*
LAN/WAN encryption (TLS 1.3); uni-directional and bi-directional communication; on-demand remote tap for packet capture

In addition, the CoIP platform can automatically quarantine hosts for policy violations. Coupled with external logic, the CoIP Platform's APIs enable automated flows for security event detection, quarantine, and remediation.

## Can hosts using CoIP communicate with non-CoIP hosts?

Yes: if the chamber is off, there's no change to the host's connectivity.

For higher security applications where the chamber function is desired, admins can define allowed connectivity to non-CoIP endpoints, allowing chambered hosts/applications to access existing corporate services such as LDAP servers, storage appliances, and DNS.

In addition to the host-based model, the CoIP Access Platform also supports a gateway proxy model to extend access across hybrid environments to machines that cannot directly run CoIP (e.g. IoT devices). The gateway proxy filters overlay traffic with a stateful L4 host-based firewall to enforce the defined security policies.

## How do I configure policies in CoIP Access Platform?

Policies are expressed in "Application Profiles," define the allowed connectivity into, out of, and within a CoIP chamber. An Application Profile can be defined in multiple ways:

- Through a simple web-based GUI
- Through scripting and APIs
- Automatically, based on learned normal application behavior

CoIP Access Platform supports "secure access as code", reducing the potential for error in policy implementation, and making the implemented policies auditable.

## How is CoIP Access Platform Zero Trust different from firewall- or router-based Zero Trust?

Zero Trust with CoIP Access Platform is completely software-based, can be implemented and changed easily and rapidly. The Zero Trust protections it provides work in any fragmented infrastructure with any combination of vendors.

In contrast, firewall- or router-based Zero Trust solutions often require special hardware that supports vendor-proprietary Zero Trust protocols. They require a homogeneous infrastructure. Customers may be required to upgrade their networks in order to be able to take advantage of these hardware-based Zero Trust solutions.

## How is CoIP different from SD-WAN and SDN?

CoIP Access Platform is completely compatible with, and can run on top of any SDN or SD-WAN.

SD-WAN is a solution for connecting sites together at Layer 3, terminating at the enterprise edge.  SD-WAN does not have the granularity or deployment model to connect individual subnets or endpoints — it handles the "last mile".  It provides no protection from the point of termination to the application server and must be coupled with traditional security tools (firewall, etc).

In contrast, CoIP Access Platform is designed to connect application endpoints and users, regardless of where they are.  CoIP addresses the end-to-end connection, including the "last 100 feet," all the way to the OS running on the application server inside the datacenter.

Software-defined Networks (SDN) are complex solutions that use software virtual routers– to implement a full virtualized network on top of a physical network.  As a result, SDN implementation and maintenance is of a similar degree of difficulty as the physical network.

In contrast, CoIP is an access solution.  No BGP is required to configure CoIP, and user, host, and application connectivity are defined by policy, rather than routing protocols.

## Is CoIP Access Platform a SASE?

CoIP Access Platform is one of the first implementations of the SASE model. Since the company's founding in 2012, our vision has been that connectivity and security must merge to satisfy the pace of change in infrastructure implementation and business requirements, and we developed CoIP Access  Platform as a result.

Our implementation differs from the Gartner SASE model in one key respect – we do not rely on SD-WAN as an onboarding mechanism. It is our belief that the security and networking disciplines must be *decoupled* to avoid bringing the I&O challenges into a new, agile world. For this reason, we call our technology SASE *overlay*, rather than SASE.

Unlike an SD-WAN-based SASE, which provides a service demarcation at a network topology edge, CoIP Access Platform's SASE overlay brings security filtering and connectivity control directly to the edge of the *application* – into the operating system of the endpoint – centralizing security policy definition with distributed security enforcement for scalability.

## How is CoIP different from SDP?

CoIP is related to the Software-Defined Perimeter concept defined by the Cloud Security Alliance, and many of the flows and use cases are related.  However, CoIP was developed independently of CSA and does not implement the CSA SDP Specification. CoIP uses different message formats and command sequences to register clients to the CoIP Controller, as well as our own packet encapsulations and network implementations to ensure high throughput and low latency.

Endpoints in a CoIP WAN network do not communicate directly with each other; instead, they communicate through a Zentera Network Switch (ZNS) node, which switches traffic between the pair of outbound TLS 1.3 tunnels. As a result, there is no need to expose the CoIP endpoint in the enterprise to the public Internet.

Many SDP solutions are focused on securing the "front door" access for web apps – how users access machines inside the corporate perimeter without opening the perimeter.

A more difficult question that arises once generic client/server applications are allowed is: once the access is provided, where can the user go next? SDP does not address this question, but it is important to consider, as access methods can become a path for malware or data leak/loss. SDP vendors typically do not combine their access solutions with micro-segmentation, and leave that question for other vendors to answer. However, the CoIP Chamber model can completely lock the back tiers of an application, reducing risks of theft of credentialed access.

## How do I get learn more and started with CoIP?

Contact us for a demo and a trial account on our servers. You can launch CoIP services in the cloud and follow our how-to documents to walk through a tutorial. Sign up for an account on our support site for more documentation and helpful resources.

## About Zentera

Zentera is the leader in secure and agile infrastructure solutions for the digitally-transformed enterprise. The company's CoIP Access Platform provides award-winning Zero Trust networking, security, and multi-cloud connectivity that overlays on top of any infrastructure in any fragmented environment, allowing customers to be up and running in less than a day. The CoIP Platform has been deployed by global enterprises to secure employee and third-party network access for compliance, protect sensitive data against leaks, and instantly connect hybrid applications and containers running in the cloud and on-premises. The Silicon Valley-based company has received numerous recognitions, including Cool Vendor for Cloud Security by Gartner.