Simplifying Cloud Security with Zero Trust and SASE as a Service

January 2021

zentera™

Cloud Computing - Simple to Adopt, Complex to Scale

The cloud computing market has witnessed robust growth in recent years, thanks to enterprises looking to modernize operations with new service models and reduce capital expenditures. Cloud vendors offer their customers instant access to global scale, with a suite of tools to rapidly build and maintain applications.

Typically, enterprises start the cloud journey by treating the cloud as just another corporate datacenter (just one offered via services), applying existing best practices to connect and secure a remote site. But as companies scale their cloud usage, they discover a whole new set of pain points associated with securing this newfound flexibility using conventional infrastructure security practices. These pain points, which can put corporate agility and security at risk, often come as a hidden surprise.

New Problems Need New Solutions

These unwelcome surprises can be now easily avoided with next-generation security tools that streamline the scalability of cloud security before it gets out of hand.

Zentera's CoIP Access Platform enables customers to leverage advanced Zero Trust security, delivered as services in the cloud, to implement strong controls for corporate applications and data that are deployed in the cloud or on premises. At the same time, SASE and overlay technologies reduce operational complexity, enabling smooth transition of all kinds of applications to a cloud, multi-cloud, or hybrid environment.

Storm Clouds Ahead!

Companies that start off with one cloud may soon find themselves with two or three, and hundreds of projects in different VPCs, interconnected with resources back on premises. This complexity creates new operational challenges.

Some common pitfalls enterprises encounter as they scale cloud adoption include:

- **Legacy network gateway-based security (firewalls, VPN) cannot gracefully scale the enforcement of security policies as the number of sites/VPCs/VMs increases**
- **Lack of a unified security technology stack across cloud, edge, and on-prem environments makes security management difficult at scale**
- **Traditional, ticket-based management of security policies and tools negates the agility benefits of cloud**
- **Existing network and access security bottlenecks create a poor user experience for users, who need secure access to any resource from anywhere**
- **Proliferation of sites and privileged accounts creates more opportunities for misconfiguration and configuration drift**

What are Zero Trust and SASE?

Zero Trust and SASE share one thing in common: they are two of the hottest trends in cybersecurity. They are, however, independent concepts: Zero Trust is an approach to security based on trust factors, while SASE is an architecture that defines where security is implemented and enforced.

Zero Trust

The Zero Trust security philosophy replaces implicit trust relationships based on network topologies with explicit authentication and policy-defined access control. It can be summed up in Forrester's tenet: "never trust, always verify."

In traditional networks, the network topology defines the "trust relationship" – to access a resource, users must first "get on the network." The job of a VPN is to connect users to that network, while the job of a firewall is to filter/block un-authorized traffic from reaching certain networks. Once on a network, a packet is effectively trusted to access every resource on that network.

In a hybrid cloud environment, remote access policy is defined by the programming of IP addresses, VPN/NAT gateways, routers, and firewalls along the access path. As the number of sites scales, the complexity increases exponentially, and it becomes increasingly difficult to manage changes – let alone answer questions like, "are you sure the contractor can't access that VPC?", and "exactly where is the policy setting broken?"

Zero Trust changes the security model, so every access is authenticated and authorized and enforced end to end. Ideal solutions can centralize the identity and security policies, so that they are are consistent in every environment – on-prem, cloud, and hybrid, greatly reducing complexity.

We encounter Zero Trust principles routinely in the physical world.

In an airport, access to the terminal is granted only after authentication (your passport), authorization (your ticket), and threat detection and mitigation (security screening). As you board the plane, you must reauthenticate and reauthorize for additional security.

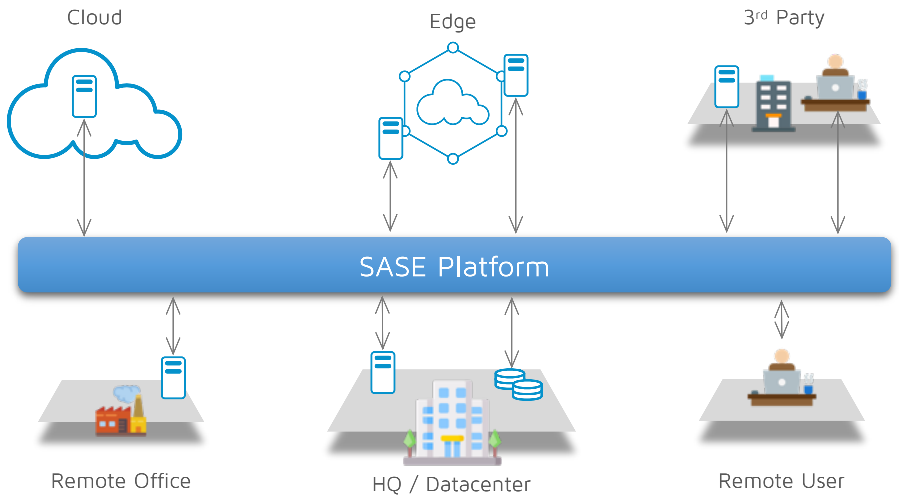
Secure Access Service Edge (SASE)

The concept of Secure Access Service Edge (SASE) was formalized by Gartner in 2019. Recognizing that corporate users and resources have moved out of the traditional corporate perimeter, Gartner observed that enterprises have an increasingly difficult time ensuring that the traffic between these users and resources passes through traditional network security appliances deployed in fixed locations. Instead, security functions can be delivered from the cloud, thereby enabling the flexibility needed to handle mobility.

The operational benefits of SASE are clear; instead of having to manage disparate security appliances and enforcement points spread across many environments, companies enjoy a centralized management layer with consistent security services.

Many current SASE offerings are advertised as a hosted SaaS model. One of the major challenges with this approach is that it forces all enterprise traffic to transit a service that under the operational control of the hosting party, leaving the enterprise without visibility or tools to manage quality of service. This can also create compliance issues for sensitive traffic that must be escorted securely from end to end. Many companies have already invested significant effort to optimize applications for performance or governance reasons. The choice to deploy a hosted SaaS offering must therefore be balanced against the enterprise's need to retain control of mission-critical apps. While a hosted SaaS model does provide ease of use and flexibility, non-hosted SaaS is an architecture option to avoid the above concerns.

The SASE model simplifies enterprise security by concentrating security features into a unified stack of security services that can be inserted between users and resources, wherever they are.



Introducing CoIP® Access Platform – Zero Trust as a Service

Zentera Systems' flagship CoIP Access Platform is an advanced SASE platform that provides unparalleled security to support enterprise Digital Transformation. Following the Zero Trust model, it identifies and authenticates users, endpoints, and applications, and authorizes every access with a centralized policy engine to ensure consistent behavior across the entire complex computing landscape end to end.

Using CoIP Access Platform, customers can deploy their own services for:

- instantly provisioning and managing Zero Trust Network Access (ZTNA) for least-privilege remote user access to corporate resources and applications
- segmenting and cloaking distributed application servers and endpoints with micro-segmentation
- securing connectivity for remote services without a VPN
- inserting threat prevention or other 3rd party security services
- automating security with APIs that support infrastructure-as-code initiatives

At the heart of CoIP Access Platform is the CoIP Overlay, a patented Zero Touch session-based overlay technology that decouples application connectivity and relieves IT and DevOps from the operational drudgery of building and maintaining network connectivity. With the CoIP Overlay, hybrid applications can be set up to run across sites in minutes, without tickets to open brownfield firewalls or configure VPNs, and even without public IP addresses.

Unlike hosted SaaS SASE implementations, customers may instantiate CoIP Access Platform as needed from cloud marketplaces with ownership for full architectural control, for a single application or the entire company. This prevents corporate traffic from having to transit a 3rd party service provider, incurring additional latency and data charges and potentially creating compliance concerns. It also gives customers full control over quality of service, allowing them to leverage existing private lines and peering setups. And finally, it leverages existing cloud provider platforms, relationships, and SLAs.

A VoIP telephone uses a familiar session-based overlay; when you dial a VoIP number, the call goes through. Unlike the PSTN network, when you move the phone, you don't need to re-provision the circuit.

In the same way, the CoIP Overlay connects arbitrary TCP/IP applications, without having to first provisioning IP network infrastructure.

How Zero Trust as a Service Simplifies Cloud Security

CoIP Access Platform's native integration of Zero Trust and SASE enables enterprises to confidently embrace Digital Transformation without worrying about "hitting the wall" created by legacy infrastructure silos from the operational and agility perspective. Key benefits include:

- Zero Trust that authenticates users against corporate directories and uniquely identifies endpoints and applications, decoupling security policies from the network topology and gateway security devices
- Unified security policy controls across all environments, with onboarding options that support the full range of enterprise devices, including cloud/datacenter VMs, containers, user machines, and IoT devices
- Zero Touch deployment that eliminates the need to manage and maintain interconnected network silos at the IP level
- Composable SASE model that enables security services to be optimized with the application
- API-driven security-as-code that can enable self-service deployment of approved security patterns, with auditability

And delivered in the same cloud providers that customers are already using, CoIP Access Platform removes reliance on 3rd party data transport and backhaul. Compared to hosted SaaS SASE platforms, CoIP Access Platform allows enterprises to instantly apply Zero Trust Security to existing enterprise environments and applications on the fly, while retaining control over application performance and compliance.

Make Security Invisible

Move security management away from individual technology silos

Use policies that express the security *intent*, not implementation details

Apply policy end-to-end, with visibility across all environments

360° Authentication

Authenticate every user, endpoint, and application before allowing access

Leverage existing corporate identity and access management tools

Authorize Every Access

Eliminate implicit trust granted by having network access

Base trust on authentication and authorization

Continuously validate authorization during the session

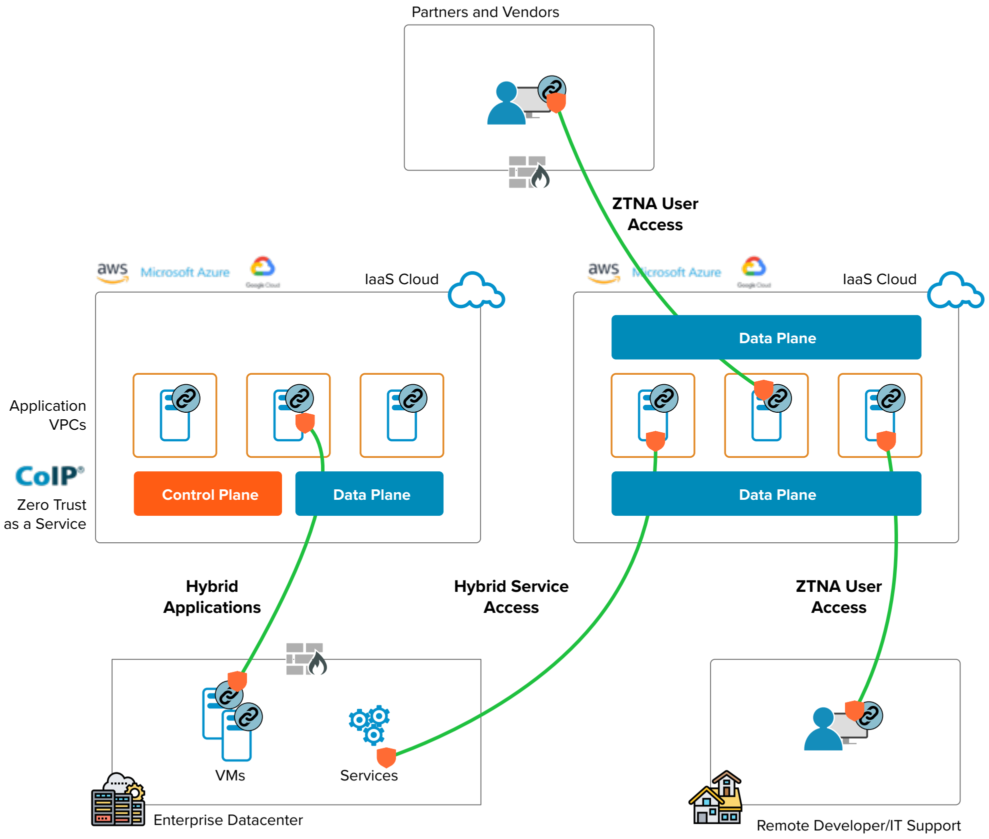
Using CoIP Access Platform for Seamless Protection of Cloud Migration

CoIP Access Platform solves many of the major operational and infrastructure challenges associated with scaling the use of cloud and edge platforms.

Once onboarded to CoIP Access Platform, either through a lightweight software agent or an endpoint gateway, applications are instantly secured and connected to remote applications through the CoIP Overlay, without the need to change the IP network or configure a VPN, and without public IP addresses. This allows applications to be rapidly brought up in new sites or clouds while avoiding the painful network building and provisioning steps normally required to connect a remote site.

Because CoIP Access Platform connects applications, rather than networks, the hybrid connectivity naturally follows principles of least privilege. CoIP Access Platform's micro-segmentation capabilities can even be used to authorize further connections to other machines within the VPC or datacenter environments.

As shown in the diagram below, customers can instantiate the service near resources – in the cloud, or at the edge – ensuring optimal performance for access to those resources. And with CoIP Overlay's single flow performance of up to 6Gbps, the solution works well for even the most demanding applications, such as high-performance database replication to the cloud.



- Secure access from the cloud to on-prem services
- Micro-segmentation in VPCs and on-prem
- High-performance database replication to the cloud
- Privileged access for users to cloud VMs for development and support
- No public IP addresses or inbound VPC security rules

Using CoIP Access Platform for Secure Cloud-based Application Delivery

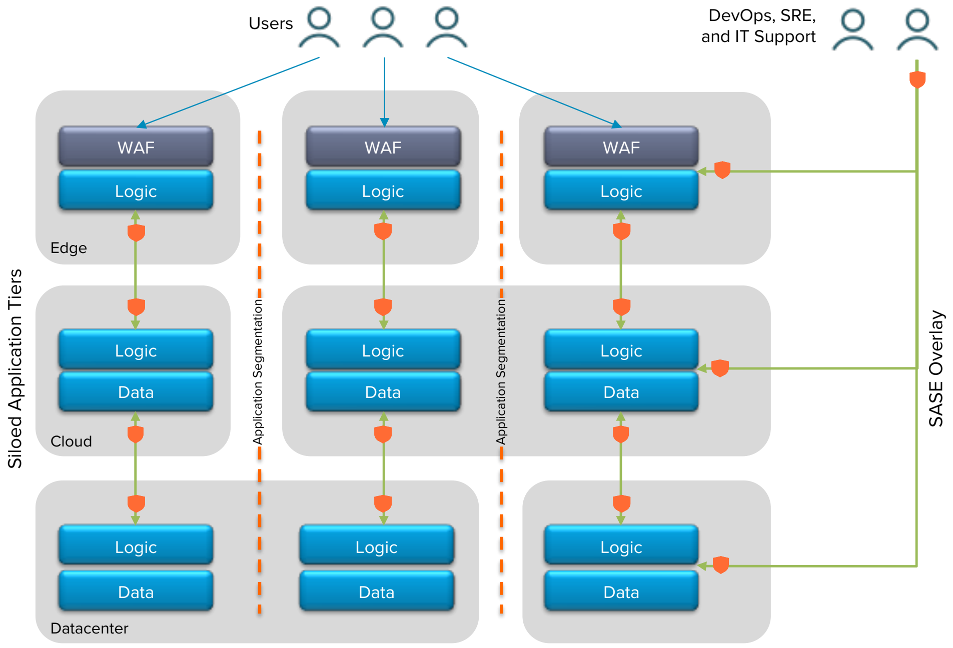
CoIP Access Platform's Zero Trust SASE capabilities also support advanced security protection for application delivery from cloud or edge computing. The Internet-facing first tier is typically secured by web application firewalls and DDoS protection, while CoIP Access Platform's micro-segmentation cloaks the applications and blocks lateral attacks within and across tiers. As a result, none of the application servers need have a public IP address. Zentera's policy engine makes it simple to define users, resources, and the access policies that connect them.

Connections between tiers are secured with Zero Trust controls that enforce directionality, while Application Interlock™ is used to prevent unauthorized applications and processes on the endpoints from abusing the network. Each tier can be deployed in a separate VPC, or even in a separate cloud or co-location environment. Here again, Zentera's deployment model allows the performance of the application to be optimized and controlled by SRE and DevOps personnel in place, avoiding routing traffic to third party SaaS hosting locations.

CoIP Access Platform continually monitors the application behavior and can flag anomalous behavior, such as a network access by an unauthorized application or port scan. Once detected, CoIP Access Platform can optionally quarantine the suspicious server for inspection and remediation.

DevOps and IT support personnel can leverage CoIP Access Platform's ZTNA functions for privileged access to backend servers for maintenance from any location in the world, with server access types (ssh, VNC, RDP, etc) that match roles and responsibilities. Directed access to authorized endpoints throughout the is secured in TLS 1.3 tunnels.

- Platform-based overlay SASE avoid stitching underlay silos
- Instant ZTNA access for maintenance and support
- Micro-segmentation protects against lateral migration of attacks, both north-south and east-west
- Enforces application data flows and directionality



Conclusion

Zentera's CoIP Access Platform can address many of the technical and operational challenges from scaling the use of cloud, multi-cloud, and hybrid applications. Its advanced Zero Trust security and SASE deployment models meet customer expectations for high performance, security, and streamlined controls across all environments.

For more information on CoIP Access Platform, please visit our website at https://www.zentera.net.
To speak with an architect, please contact us at support@zentera.net.