zentera™
Connect · Protect · Shield

*CoIP® Customer Success Story*

QUALCOMM®

# Qualcomm® Deploys CoIP Enclave™ Solution for Secure Clean Rooms and Vendor Remote Access

Qualcomm is a world leader in next-generation wireless technologies. For more than 25 years, Qualcomm innovation has driven the intense revolution of digital communications, linking people everywhere more closely to information, entertainment and each other. Qualcomm produces a wide variety of semiconductors, including Snapdragon™ processors and modems, which are found in over a billion smart devices worldwide.

## Key Objectives

- Allow secure remote access for design partners and EDA vendors with minimal changes to existing IT infrastructure
- Prevent data leakage in distributed development environments and avoid intellectual property loss
- Enable "single pane of glass" control over network and security for secure collaborations

## The Challenge

Qualcomm's semiconductor products are designed with the help of design partners worldwide, along with the Electronic Design Automation (EDA) software vendors who provide semiconductor design software. These collaborations require that Qualcomm have a secure compute environment where it can share product design and data.

However, creating and maintaining such a secure shared environment across dozens of companies presents multiple challenges. First, while sharing the necessary design tools and data, Qualcomm has to guard against intellectual property loss (also known as Data Loss Prevention (DLP)). The company must restrict the possible flow of any data out from the design platforms, including data transfer via the application tool level. Second, establishing connectivity between the design platform and Qualcomm's partners should not warrant changes to the existing network and security infrastructure—given Qualcomm's extensive IT organization, this would require IT intervention and security reviews, leading to substantial delays in onboarding partners. Finally, a key requirement is that these network and security changes be managed with minimal effort from a centralized management interface.

Qualcomm's original approach to creating a secure shared environment with VPNs proved unsatisfactory. Setting up VPNs requires that firewalls be opened on both ends and that internal routing tables be modified. These measures ensure that VPN access is restricted to only the design platform and keeps other Qualcomm servers inaccessible. However, opening firewalls and changing routing tables affect existing security implementations, triggering internal security concerns and leading to lengthy InfoSec (Information security) reviews. The resulting delays hurt Qualcomm's agility and efficiency each time an external partner was onboarded, creating an untenable situation.

## The Solution

- Secure remote access with micro-segmentation for enhanced DLP
- Interlock design applications with virtual network for defense-in-depth
- No changes to existing IT infrastructure
- Centralized management console

## Business Benefits

- Stringent security for intellectual property protection and data loss prevention
- Fast onboarding of design partners & EDA vendors
- Centralized network and security management
- Agile product development

*CoIP Success Story*

> *"With CoIP, we are able to onboard our design partners and EDA vendors in a matter of days instead of weeks or months, which provides us with a great advantage in our product design and development agility. That is critical in our fast-moving industry."*
>
> Qualcomm VP Engineering

## CoIP Products

- CoIP Enclave

## About Zentera

Zentera secures application workloads in hybrid environments with a type of software-defined perimeter called an enclave. The CoIP Enclave™ solution provides security and connectivity. It works with any infrastructure in any environment, does not interfere with existing environments or security, and can be up and running in less than a day. CoIP Enclave provides comprehensive network security for enterprise applications in the cloud, moving to the cloud or on-premise, and is deployed for worldwide operations by global corporations. The company has received numerous honors, including consecutive Red Herring Top 100 Awards, and is based in Silicon Valley. For more information, see www.zentera.net.

zentera™
Connect · Protect · Shield

## The Solution

Qualcomm chose to deploy the CoIP platform as a secure, virtual overlay network, or *enclave*, on top of the company's design datacenter, replacing the unsatisfactory VPN-based solution. The CoIP Enclave solution successfully addresses Qualcomm's initial challenges in creating a secure collaboration environment for its dozens of partners. First, CoIP provides DLP and protects against data leakage through multiple mechanisms. Qualcomm set up its CoIP network to isolate the secure collaboration environment via east-west traffic filtering (i.e., micro-segmentation). The company then established secure remote access for Qualcomm's partners and vendors using zAccess™, CoIP's version of a Virtual Desktop Infrastructure (VDI) tool. With zAccess, all parties can access the collaboration platform but cannot move data out of the platform. Unlike a conventional VPN, zAccess will not allow any unauthorized network protocols to operate within the secure network, thus providing strong security.

With respect to minimizing the effort of onboarding partners, CoIP, as an overlay network solution, does not require changes to Qualcomm, partner or vendor network and security infrastructures. Existing IT infrastructures remain untouched and the security policies unaltered, leading to limited or no need for enterprise InfoSec reviews. As a result, the time to onboard a partner or vendor is cut down from months to days or hours.

Finally, CoIP's centralized, GUI-based management interface allows for straightforward provisioning, managing and monitoring of the complete CoIP solution—the virtual overlay network, micro-segmentation, protocol authorization, partner onboarding and zAccess. Reconfiguring collaborations is similarly straightforward, when partner access is no longer needed.

## Business Benefits

Intellectual property protection and DLP are crucial to Qualcomm's success. With CoIP, Qualcomm can securely onboard design partners and EDA vendors to its secure collaboration platform in hours, and the partner access can be torn down very quickly once a project is completed. The CoIP virtual network for access control and security can be put in place without changing the existing IT infrastructure, which is a critical benefit to Qualcomm IT along with its EDA vendors and design partners, since their respective existing security policies remain intact. CoIP's centralized security and network management console enables policies and configurations to be readily established, monitored and modified. The end result is greater security and agility for secure collaboration environments, a crucial aspect of Qualcomm's operations.


2099 Gateway Place, Suit 420, San Jose, CA 95110
www.zentera.net Tel. 408-436-4811