Zero Trust for Supply Chain Collaboration

Enabling Secure Information and Data Exchange

SOLUTION BRIEF

zentera™

Cybersecurity Risk Can't Be Outsourced

Every company is part of an ecosystem of partners (suppliers and vendors) providing goods and services the company uses to create value. Successful businesses have leveraged digital technologies to integrate with partners to optimize business performance. For example, a manufacturing company may integrate its ERP systems with its vendors and customers to enable real-time demand forecasts to drive production schedules. A high-tech company may share its design data with selected partners, leveraging their domain experience to accelerate time to market for very advanced technologies.

Digital integration grants a high level of access and visibility into corporate processes and performance and may even expose core intellectual property; leaks of this sensitive data and injection of malicious data have severe consequences.

The current environment of rising East-West geopolitical tensions increases the risk for enterprises as well as the reward for industrial cyberattacks, including espionage and attacks on the supply chain. Yet it is not always possible to expect a small vendor to have the skill or resources to defend the natural attack points – the points of digital integration between companies.

Companies must find ways to secure collaboration and data exchange with partners that are independent of the partner's capability to secure that data – for example, with a trusted environment for collaboration that ensures partner access, limits it to the intended business purpose, and defends against abuse of access privileges.

This can be achieved with new Zero Trust security. Governments worldwide, including the United States, Japan, and Taiwan, have recognized that Zero Trust can help secure complex supply chains, and are adopting it themselves and promoting adoption within their respective partner bases.

What Is Zero Trust Security, and How Does it Help?

Zero Trust is a new security paradigm that minimizes the exposure of applications and data to cyber attacks. Where traditional network security promises to keep corporate networks free of cyber attacks, Zero Trust acknowledges that we just haven't been able to deliver on this promise – as evidenced by the parade of breaches reported in the news on a near-daily basis.

Instead, Zero Trust starts with the assumption that the corporate network is already compromised – it's no cleaner than the Internet. If we cannot trust the servers and devices on the network to be clean, we must require users, devices, and software to prove their identity and verify that they are authorized before we allow access to an asset. These checks must be done for every network access to that asset, effectively creating a new defensive perimeter around a protected asset that enforces such checks.

Traditional network security devices, such as firewalls, choose to allow or deny traffic based on information in each packet's header – the so-called 5-tuple, which includes the source and destination IP addresses, source and destination ports, and communication protocol. Zero Trust combines the traditional 5-tuple with identity and authorization of users, devices, and software that are involved in the communication to make policy decisions.

The approach is simple, but extremely effective, if it is executed correctly with right technology. Using the Zero Trust approach, companies can contain IP and data that are part of supply chain collaboration securely. As every access to the data is identified down to the software level, unauthorized access to and leaks of corporate data are effectively blocked.

Manufacturing companies can use Zero Trust to protect its ERP and EDI gateways, positively verifying that accesses come from valid suppliers and customer servers to block malicious actors. It also closes off access to everything except the authorized data interchange with authorized software, protecting the company against malware that may be present in partners' networks. Zero Trust authenticates users, devices, and software used in a remote and untrusted environment.

High-tech companies can use Zero Trust collaboration for fine-grained control over partner access to sensitive network environments and data – down to the level of authorized actions the partner can take with the data. For example, Zero Trust can enable the partner to access and manipulate the data through a remote desktop, while preventing the partner from downloading the data to a local machine or uploading it to Internet sharing sites. Zero Trust can also effectively control east-west lateral access, allowing users and software only limited access to the backend environment.

Why Secure Collaboration is a Challenge for Legacy Network Security

Companies have long recognized the importance of protecting partner collaboration projects and cross-organization integrations. However, collaboration projects have been difficult to implement with traditional network security, often requiring months to design and implement. Some of the steps include:

- Building isolated network zones using VLAN
- Updating edge firewalls and routing with rules for the new zone
- Moving compute resources, data, and dependencies into the new zone
- Create external user and service accounts for VPN
- Testing and validation

It's not uncommon for customers to spend 6 months building and validating a bespoke collaboration environment – and this doesn't even factor in time needed to set up and configure security monitoring that may be needed for compliance. Once the project is over, the team will have to tear down the environment and delete any project-specific rules from the edge firewall. Clearly, legacy network security is not a very practical solution for urgent business collaboration.

Furthermore, even after all of the infrastructure implementation effort, this security isn't even Zero Trust. Traditional network security appliances work on the 5-tuple, and aren't aware of the user, device, or application identity – telemetry which may come from 3rd party devices in 3rd party networks. This is a heavy lift, just to achieve conventional levels of security, which have already proven ineffective.

How Zentera Zero Trust Solves the Secure Collaboration Challenge

Zentera Systems' advanced Zero Trust security solution, CoIP® Platform, elegantly solves the challenges that legacy network security struggles with. CoIP Platform implements *software-defined network security* – completely software-based, it can be installed as an overlay on existing IP network and security infrastructure and reconfigured as needed to meet project requirements.

CoIP Platform makes Zero Trust simple, with the following core capabilities:

Implements a virtual network zone around assets in-place

CoIP's zLink sensor software enables administrators to create new zones around groups of hosts using software-defined perimeters (SDP) or micro-segmentation. This allows logical zones to be created around existing assets, and avoids having to create a zone with VLANs or physical networks and move applications and data into it.

Identifies users, devices, and software

Users are identified against existing corporate identity providers with MFA, while the zLink sensor fingerprints devices and software with cryptographic identity, augmenting the 5-tuple used in access control with rich identity and blocking malicious access.

Policy-based user access controls for asset protection

CoIP Platform supports fine-grained and identity-based policies that trust specific users to access assets for a specific purpose – unlocking the core benefits of Zero Trust. An integrated, end-to-end overlay transport enables users to access specific applications and assets without VPN and without disrupting or exposing physical networks.

Overlay application network

CoIP Platform offers a session layer transport for application connections across network domains, eliminating the need for site-to-site VPNs. After installing the zLink sensor, the overlay transport is governed by policies programmed in CoIP Platform without touching the edge firewall or routing.

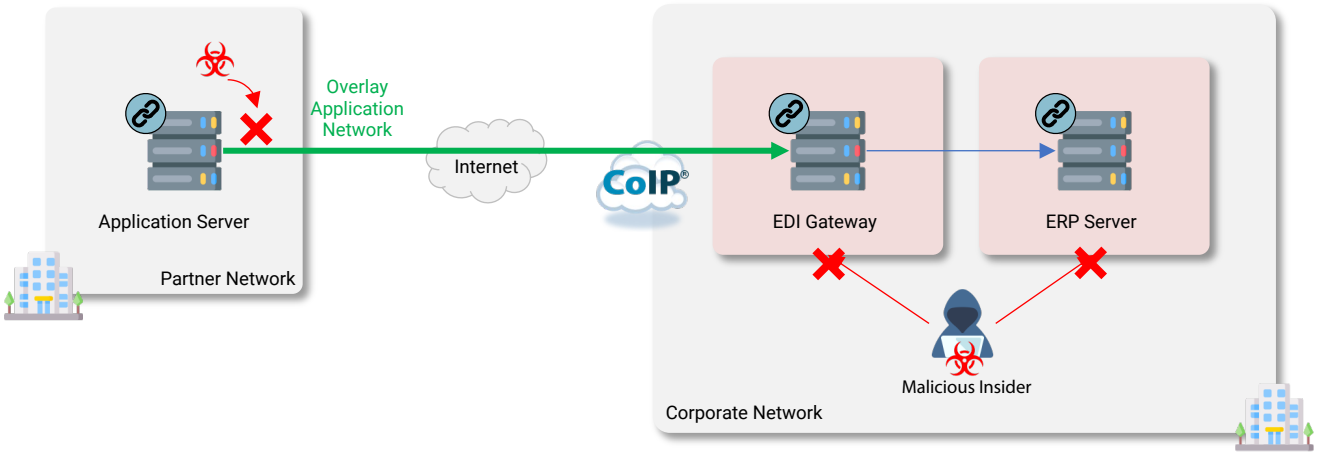
Examples of Securing Supply Chain Collaboration

Electronic Data Interchange

CoIP Platform can secure Electronic Data Interchange (EDI) as shown below using a private network for application isolation across domains. Also using a virtual network zone to segment the ERP server and the EDI gateway renders them inaccessible to unauthorized parties, such as malicious insiders in the corporate network.

Partners install the zLink sensor on the Application Server, creating an overlay and private network connection to the EDI Gateway. This avoids having to assign the EDI Gateway a public IP address and avoids giving the partner Application Server any access to the corporate network.

Zero Trust policies enable the partner application to access the EDI Gateway, while automatically blocking rootkits, ransomware, and other malware that may be on the Application Server from accessing the EDI Gateway or the corporate network.



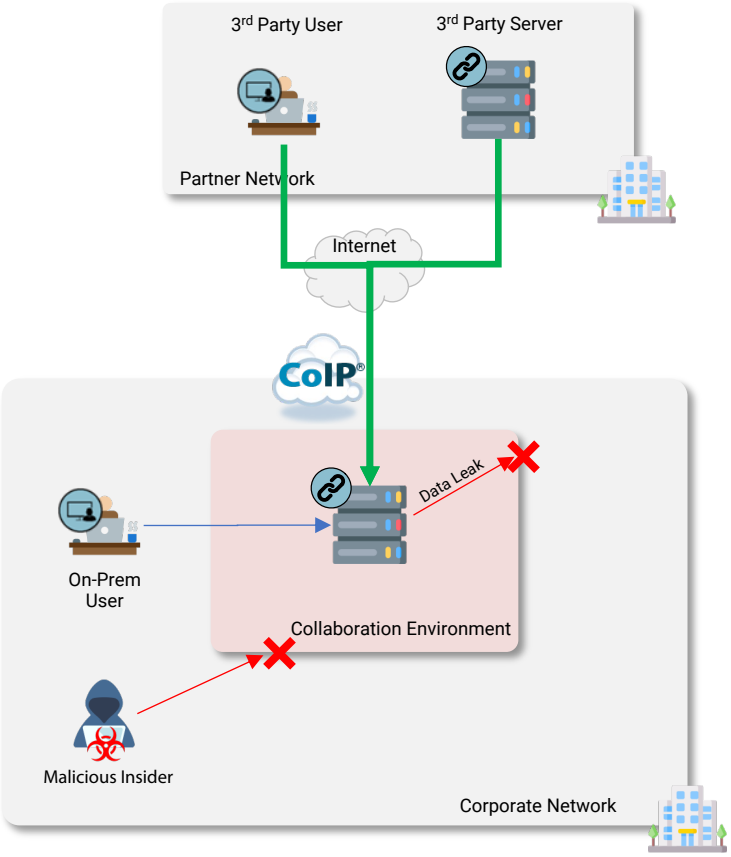
Examples of Securing Supply Chain Collaboration

Secure Collaboration Environment

CoIP Platform can also be used to create a Secure Collaboration Environment, as shown below. Instead of building a full network zone, a software-defined perimeter is used to isolate specific machines dynamically within the datacenter that hosts the collaboration environment. The machines do not need to be isolated on any specific physical network; CoIP Platform's control create a logical zone around them.

On-prem and remote users are authenticated and authorized by CoIP Platform and granted a secure method of access via CoIP overlay transport – for example, secure shell with data transfer blocked, or remote desktop with copy/paste protections. The virtual network zone is configured to block access to the internal network and Internet, preventing leaks of sensitive collaboration data.

The Collaboration Environment can be created or terminated in under an hour, enabling domain experts with quick, direct access to specific machines in the corporate network to assist in resolving issues, contributing data to a project, or participating in collaborative design. This same method applies for remote vendor access and support as well.



Zero Trust for Supply Chain Collaboration
Enabling Secure Information and Data Exchange

About Zentera

Zentera Systems is the leader in Zero Trust Security solutions for the digitally-transformed enterprise. Founded by experts in networking, security, and remote access, we offer award-winning Zero Trust networking, security, and multi-cloud connectivity that overlays any fragmented infrastructure and deploys rapidly on premises or as a service.

Our global enterprise customers and network of partners use our products to secure employee and third-party access, protect against data leaks, and instantly defend applications in complex hybrid and IT/OT environments. Based in Silicon Valley, we have received numerous recognitions, including Cool Vendor for Cloud Security by Gartner.

More Resources

On the web:
www.zentera.net

Email:
sales@zentera.net

Phone:
+1 (408) 436-4811

zentera™