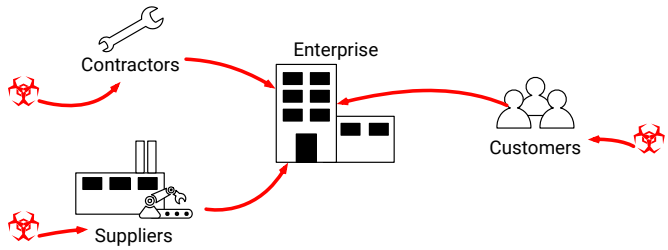
Zero Trust Network for Supply Chain Security

Secure Third-Party Access to Corporate Assets

The Supply Chain is the New Weakest Link

To stay ahead of hackers, companies have deployed and upgraded security tools, minimized and hardened attack surfaces, and driven best practices for operations, training, and incident response. Hackers have responded by turning their attention to softer targets in the supply chain. After all, companies still rely on credentialed network access to each other's business applications, networks, and resources.

The supply chain members have differing levels of resources and sophistication when it comes to protecting users, computers and networks. Small companies often lack the IT and cybersecurity resources necessary to manage complex questions of network and application infrastructure ownership and responsibility. Hackers know this. Phishing, social engineering and other hacks of supply chain partners quickly yield enterprise VPN credentials; the hacker, posing as a trusted partner, can then launch attacks from within the enterprise perimeter.



But what if you could create a secure zone around a supplier and control how they interact with assets in your IT environment? What if you could contain and segment applications as security conditions change? What if the security adapted to where and how your assets are deployed, and how the supplier interacts with your applications and your assets did not matter?

CoIP® Platform for Supply Chain Security

- Zero Trust Network eliminates dependence on network topology and supplier security posture
- Web-based, VDI-based, and network-level access options
- Enables 3rd party access rights to be defined by user, port, protocol and application
- Micro-segmentation locks access to specific resources and prevents lateral migration
- Advanced encryption with dynamic end-to-end tunnels
- Rich security events and alerts, integrated with monitoring tools (e.g. Splunk)
- LDAP and Active Directory integration streamlines onboarding and offboarding
- Multi-factor Authentication for additional user security
- Transparently deploys without touching existing network security

www.zentera.net
Copyright © 2019 Zentera Systems, Inc.
CoIP is a registered trademark of Zentera Systems, Inc.
All other trademarks herein are property of their respective owners.

zentera™

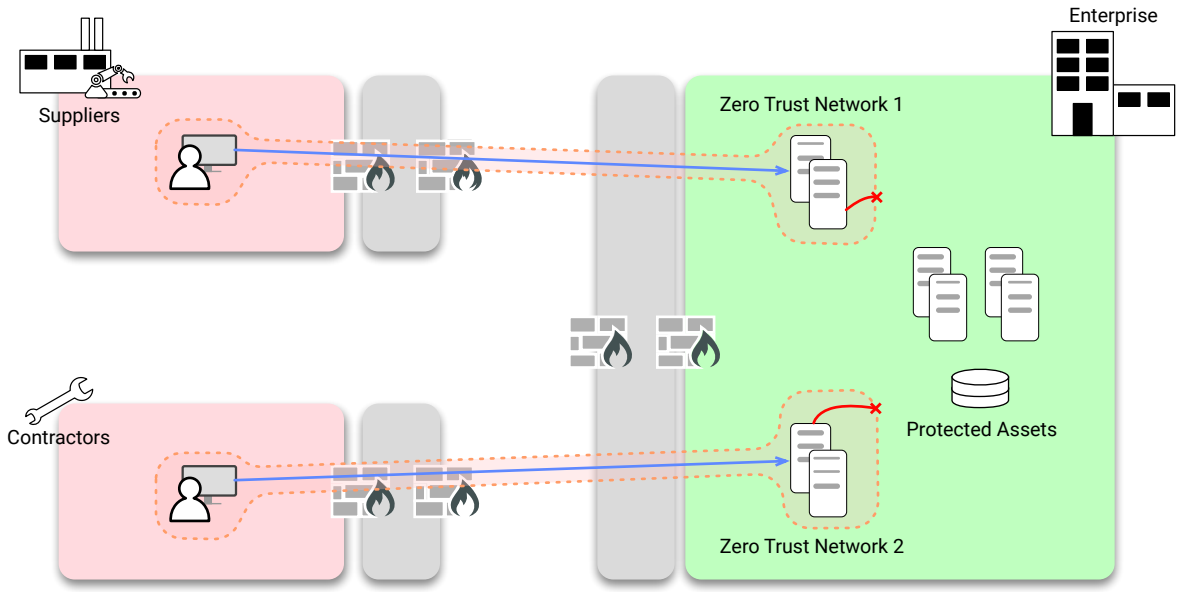
zentera™

Zentera Systems' CoIP® Platform for Zero Trust Networking

Zentera provides a Zero Trust Network (ZTN) solution that connects selected third parties to specific applications and resources inside the enterprise. At the same time, the Zero Trust Network effectively contains and segments that third party traffic away from all other enterprise operations and infrastructure. This is because all traffic inside the ZTN is escorted from end to end, with security policies that apply to each remote machine.

With Zentera's ZTN, third-party users can only access what they're authorized to access; everything else is blocked and beyond their reach. That is because Zentera's ZTNs are overlay networks with complete micro-segmentation – both east-west *and* north-south. They run on top of the existing network, decoupled from the underlying network infrastructure on a completely separate plane. As a result, corporate assets are protected, hidden from the third-party users.

Since the ZTN is overlay, it also saves enterprise IT from having to manually reconfigure firewalls, subnets, and routers. Zentera's approach is to decrease the risk of error-prone network heavy lifting by simply building an overlay network. A ZTN can be set up and configured within a day. Enterprises can build multiple Zero Trust Networks, each decoupled from the underlying infrastructure and segmented from each other, allowing different third-party users access to different resources.



For more information on how to implement Zero Trust Networks using the Zentera CoIP Platform, contact your local Zentera sales representative at sales@zentera.net.

Copyright © 2019 Zentera Systems, Inc.
CoIP is a registered trademark of Zentera Systems, Inc.
All other trademarks herein are property of their respective owners.