SOLUTION BRIEF

Secure Contractor and Vendor Access

A VPN-Free Way to Deliver Applications

June 2022

zentera™

Contractor and Vendor Access Need Strong Security Controls

Enterprises have traditionally turned to contractors to rapidly scale their workforce to meet demand and to 3rd party vendors to acquire products and services to avoid having to develop them in-house.

Both contractors and vendors require access to enterprise applications, but each case brings unique security considerations.

Contractors and employees often do similar types of work, but the role of a contractor often implies a different level of trust compared to an employee. The contractual nature of the relationship means enterprises must take care when allowing contractors access to core intellectual property, such as source code.

Compared to contractors, vendors need access for a very specific purpose – for example, servicing tools deployed in the enterprise. They require access to a very small subset of the enterprise's applications. However, enterprises typically have little to no visibility over who the vendor hires – or subcontracts work to. In these cases, enterprises must be careful to restrict the access to only those applications that are needed for service.

The Problems With Traditional Contractor and Vendor Access

The traditional tool for remote access, the VPN, provides no security beyond basic user authentication, and is commonly paired with a firewall to filter all user traffic destined for the corporate network.

This access pattern is far from perfect; some of the major challenges include:

Filtering isn't based on user identity or role
Network packets don't carry information about the user identity or role, making it hard to limit 3rd party access contained to authorized applications and data

Difficult to administer and enforce security policies
VPN, firewalls, and user identities and roles are provisioned and configured separately, making it hard to coordinate the implementation and enforce an end-to-end access policy

Creates paths for malware injection and data theft
Allowing access to the corporate network creates a potential vector for cyber attacks for anyone with access to the credentials

Costly and slow to onboard users
Typical IT practices involve provisioning a managed corporate laptop, which is expensive and slow, and encourages users to find "workarounds" like sharing devices or account credentials that reduce security

Difficult for users to understand
3rd party users must be trained how to get to their applications once logging in to the VPN, leading to increased load on helpdesk and support

The security-related challenges alone have made VPNs a favorite target for hackers.

Attacks against VPNs up nearly
2,000% in 2021![1]

[1]https://www.helpnetsecurity.com/2021/06/15/vpn-attacks-up/

How Zentera CoIP® Platform Upgrades Access Security

Zentera Systems' CoIP Platform is an advanced cybersecurity solution capable of layering NIST 800-207 Zero Trust security controls over complex modern infrastructure.

Once onboarded to CoIP Platform, corporate applications can be mapped for access by authenticated user access, with authorization based on roles and responsibility. Applications can also be assigned to logical zones called Application Chambers; traffic flow into, out of, and between Chambers is controlled by identity-based policies that are easy to program and change.

All policies are defined in a centralized orchestrator and enforced at the user and application for tight security control. The Zero Trust implementation completely overlays existing networking and firewall architectures without disruption.

Strong Zero Trust Security

Chamber and Access policies implement NIST 800-207 Zero Trust Security based on user, server, and application identity – not on IP address – and are applied properly even as users move and servers migrate across network environments

Workload Micro-Segmentation

Application Chambers provide granular segmentation, cloaking, and isolation of individual applications, preventing access from being abused

Zero Trust Network Access

VPN-free access that uses your existing identity providers and multi-factor authentication to identify users and connects them to applications securely

Application-Specific Access

From VNC, RDP and ssh that are hardened to prevent data leaks, to web apps, or to generic TCP/UDP applications, you have full control over how much access to provide your users

Zero Touch Deployment

Agent-based and agentless onboarding options to fit any use case and application deployment scenario, without changing or disrupting existing applications or networks

Simple Operations and Change Management

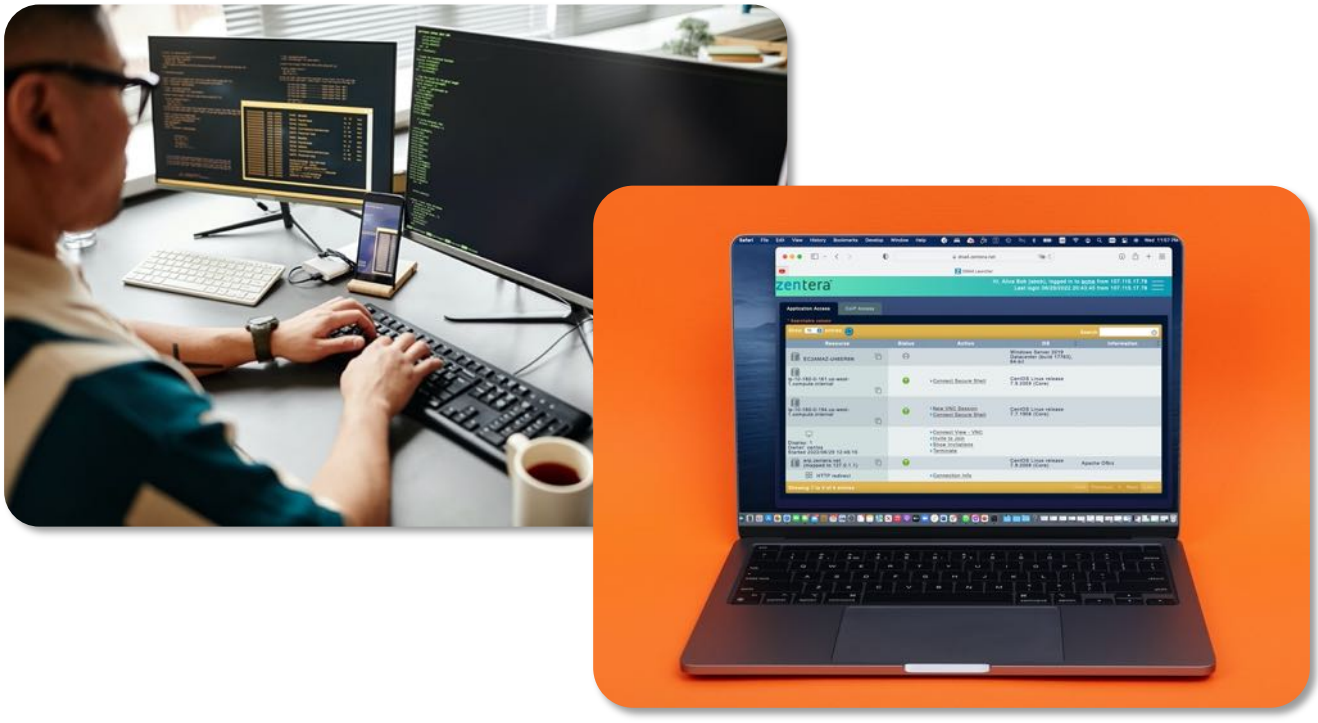
Moving access and segmentation policies to CoIP Platform makes it simple and easy to onboard new users and devices or change policies without impacting already enforced policies

CoIP Platform Elegantly Solves the Challenges of Secure Contractor and Vendor Access

CoIP Platform's powerful ZTNA capabilities makes it easy to create project specific, end-to-end access policies that give contractors or vendors access to specific applications or servers based on roles and responsibilities. Users are authenticated against your existing identity provider and MFA setup; user devices are identified and fingerprinted, with optional geolocation.

CoIP Platform offers both agent-based and agentless models for delivering access, and you're covered whether your users need access to web apps, interactive sessions (remote desktop or ssh), or custom TCP/UDP clients. And with CoIP Platform's Application Interlock™ feature, you can apply policies with full application awareness to enable limited access from an unmanaged laptop while simultaneously blocking ransomware propagation and data leaks.

With CoIP Platform, contractors and vendors can be provisioned in minutes – simply configure their account, and then send them a bookmarkable URL to access their user portal to view and launch their available applications.

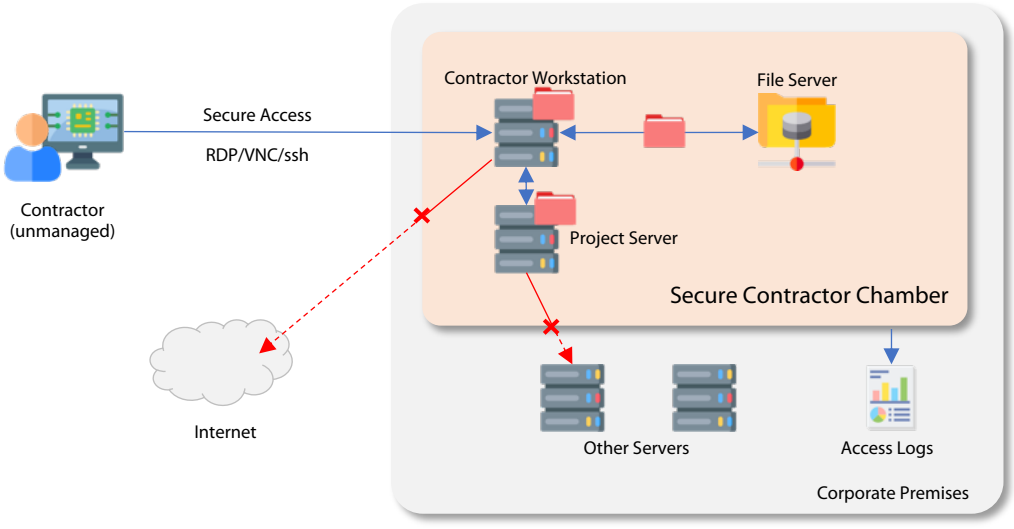


Establishing a High-Security Environment with CoIP Platform

One common enterprise need is to enable contractors to access corporate intellectual property, such as source code, design files, or financial documents. It can be difficult to create specially-segmented networks (secure zones) due to the difficulty of setting up and managing the necessary infrastructure – particularly when contractor access is project oriented and ad-hoc.

A common deployment model for this access requirement uses CoIP Platform to create a secure virtual chamber to contain the sensitive IP the contractor will need to handle. All engagement takes place within the chamber; contractors authenticate using CoIP Platform, and are given pixel-only views (e.g. VNC or RDP) to keep IP in the chamber and block the potential for malware injection.

CoIP Platform's Application Chamber capabilities also prevent data exfiltration, either to servers within the corporate network or to the Internet. All accesses and attempted policy violations are logged, making IP security auditable.



CoIP Platform Creates a Complete, High-Security Environment for Handling Sensitive IP

SOLUTION BRIEF

Secure Contractor and Vendor Access
A VPN-Free Way to Deliver Applications

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™