SOLUTION BRIEF

Secure Digital Collaboration

Delivering Agility Without Security Compromise

September 2022

zentera™

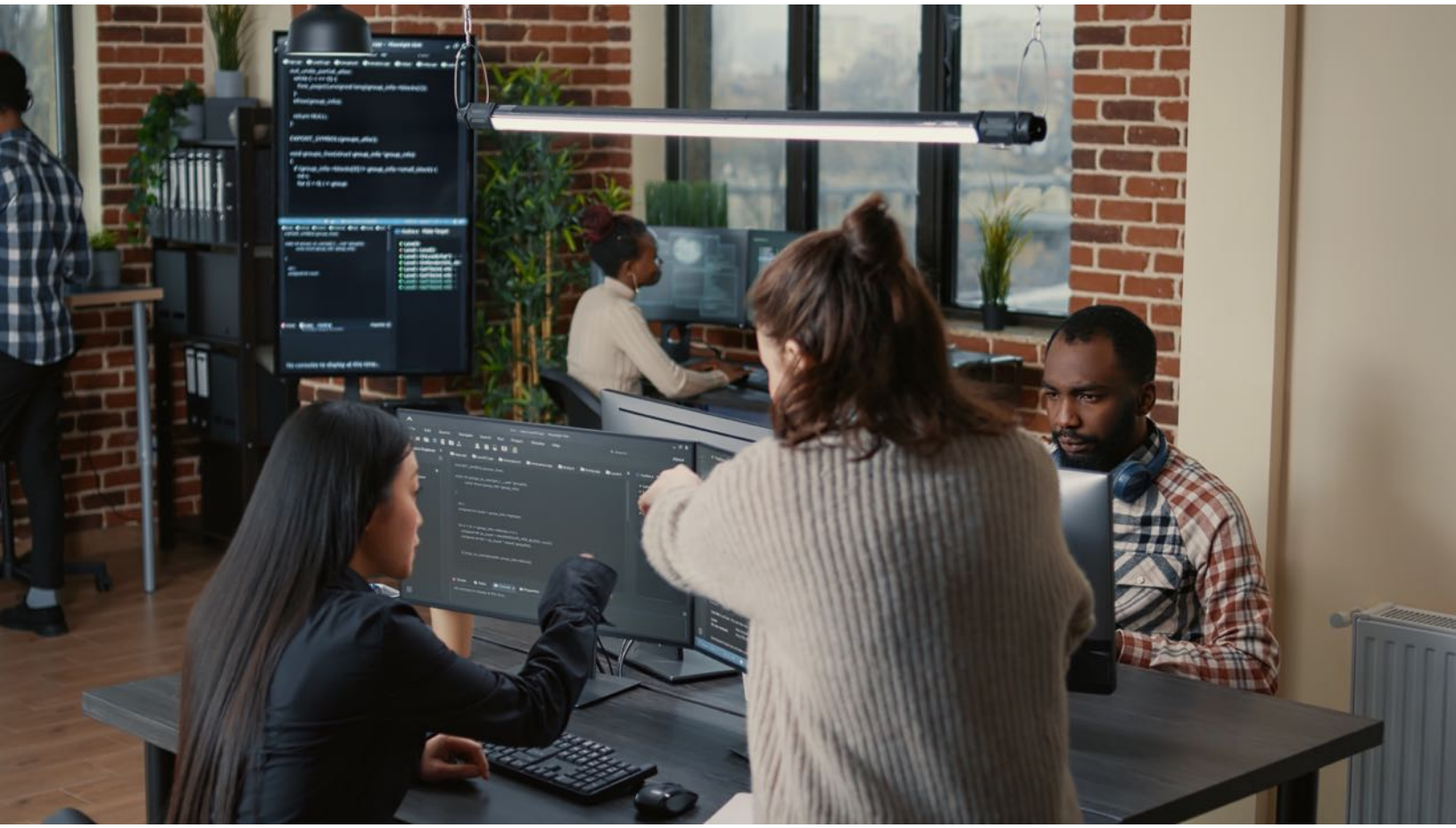
Secure Information Sharing is Essential for Modern Business

Economies are all about interaction and exchange. We typically think of goods and capital, of course, but in today's digital world, *information itself* is increasingly the "coin of the realm" that holds real value.

The more advanced or large-scale an enterprise is, the more critical it is to share this information securely. Advanced hardware, like nanometer-scale semiconductors, must be reduced to bits of information (design files) so teams of thousands of experts can work on them in parallel. Sharing this information with the wrong people, however, can cause severe economic losses, including a loss of time-to-market advantage and long-term competitiveness.

The key to securely sharing information is to always maintain control over the information. Information should be shared only with authorized individuals and organizations. The sharing method should ensure it is being used for authorized purposes and must minimize the risk of exposure.

As the pace of innovation continues to accelerate, it's more critical than ever to ensure cross-organization digital collaboration is effective and secure.



What Makes Secure Digital Collaboration Difficult?

Securely sharing information for digital collaboration is a difficult task for many companies. That's because the traditional tools for remote access, virtual private networks (VPN), are simply not up to the task. At this point, VPN technology is now over 3 decades old, and was designed for an earlier point in our digital evolution, before security emerged as a major concern for digital collaboration.

So what exactly is the problem with VPNs?

VPNs are connectivity, not security tools.
The core function of a VPN is to "short" two networks together, creating one larger, united network. They keep communications private, but don't filter traffic and must be paired with a firewall for security.

This property creates significant headaches when connecting across organizational boundaries that typically take months for networking, security, and legal teams to resolve.

It's difficult to limit connectivity based on user identity or role.
While VPNs do authenticate users, filtering is performed in the network as a separate step – and network packets don't carry any information about user identity. This makes coordinating the filtering with the user role an extremely challenging network design task that can take a long time to implement and even longer to change.

VPNs create a path for malware injection and data theft.
As VPNs do not filter traffic that flows through them, it's common for them to be used to inject malware such as ransomware, as well as to exfiltrate data. Implementing Layer 7 deep packet inspection and DLP on the firewall is expensive and can slow performance by a factor of 10 or more.

Costly and slow to onboard users.
Typical IT practices involve provisioning a managed corporate laptop, which is expensive and cannot often be done with 3rd party users in a collaboration project. Slow IT setup and response to business needs tends to encourage users to find "workarounds" like sharing information insecurely – through email or file sharing services, or by sharing account credentials.

Attacks against VPNs in 2021 up nearly

2,000%

Difficult for users to understand.
Users must be trained in using the VPN, leading to increased load on helpdesk and support personnel.

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

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

How Zentera Solves Digital Collaboration Challenges

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

CoIP Platform allows enterprises to instantly create a collaboration environment in software. It's easy to onboard servers and assign them 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.

Users are authenticated against the corporate identity provider and its multi-factor authentication, and access is provided by ZTNA, a much more secure connectivity method that allows access to be restricted to secure access methods based on application identity.

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.

Zero Trust Network Access

Limits user connectivity to secure access methods that enable productivity while managing the risk of data leaks

Application Chambers

Keeps information secure by preventing unauthorized access into/out of the collaboration environment

Zero Touch Deployment

Create and modify cross-company connectivity, without changing or disrupting existing applications or networks

Simple Operations and Change Management

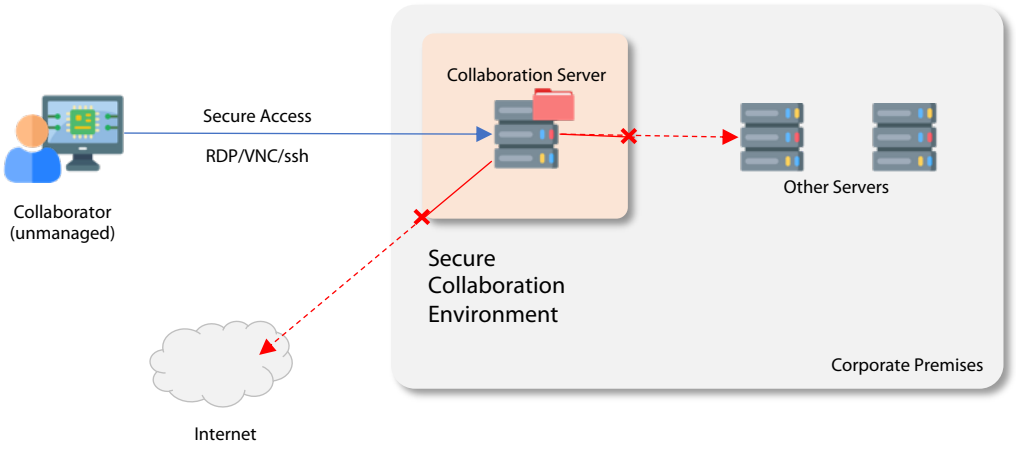
Moving access and segmentation policies to CoIP Platform makes it simple and easy to onboard new users and devices or change policies without impacting already enforced policies

CoIP Platform Enables Agility in Secure Digital Collaboration

CoIP Platform's powerful software-defined capabilities makes it easy to create a secure collaboration environment to contain information, then give collaborators access to the environment 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.

With CoIP Platform, collaborators can be provisioned in minutes – simply configure their account, and then send them a bookmarkable URL to access their user portal to view and get access to the collaboration environment.

Whether your collaboration requires web access, interactive sessions (remote desktop or ssh), or any other software client, CoIP Platform has you covered with data leak prevention features such as watermarking and copy/paste controls that keep information secure. 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.



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

SOLUTION BRIEF

Secure Digital Collaboration
Delivering Agility Without Security Compromise

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™