



# Zentera Secure Access

Secure Remote Access Solution

Simple Zero Trust Security

Infrastructure-Free Deployment

zentera™

## Remote Work Creates New Cybersecurity Risk

In today's environment, companies are embracing remote workforces for business continuity and to maintain competitiveness. However, expanding remote access brings new cybersecurity risks; remote workers' unmanaged devices can expose the company to threats, and even the most sensitive applications and data now need to be remotely accessed.

Current solutions are built on a patchwork of technologies: mobile device management to establish trust, VPNs to encrypt traffic, and UTM firewalls to filter out any unauthorized or malicious traffic. Deploying and managing user access requires wrangling a tangled web of distributed policies, controlled and operated by separate teams. Such approach may be secure, but frequently it requires constant customization efforts and fails to scale effectively to cope with the ever-increasing cybersecurity threats.

There's a better solution.

## Zentera Secure Access

Zentera Secure Access (ZSA) is a centralized access management platform that connects and protects distributed applications, endpoints, workloads, services, and users across complex hybrid environments. Its central policy engine with single pane of glass management portal streamlines access policy configuration and distributed enforcement.

Built on the principles of Zero Trust, ZSA identifies and authenticates users, endpoints, and applications to establish endpoint and user trust. Access is blocked by default; ZSA grants whitelisted, "least-privilege" access to data and services based on administrator-defined application-aware and time-based policies.

ZSA deploys as a SaaS or as an on-prem appliance; its overlay transport tunnels avoid touching infrastructure-based VPNs, routers, or firewalls. Not only does this speed up implementation of new remote access policies, it also means that the policy enforcement is decoupled from underlay infrastructure, eliminating the need to file tickets to open or close firewall ports or re-engineer network topologies.

## Use Cases



Provide secure access from untrusted user laptops and devices



Protect the corporate resources from threats on employee and 3<sup>rd</sup> party networks with Zero Trust security



Secure cloud application access to on-prem services and databases with Zero Trust



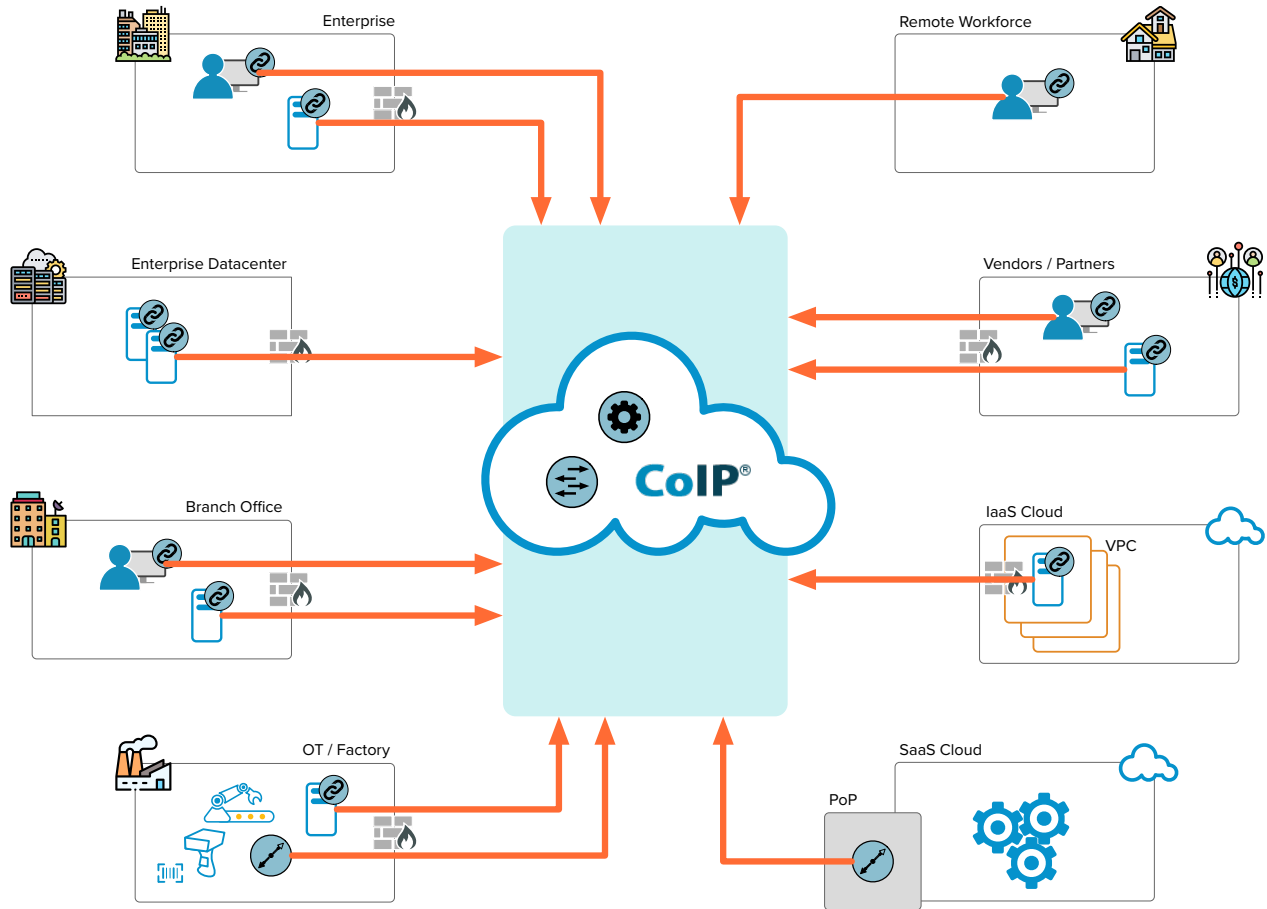
Increase cloud access security by blocking inbound TCP/UDP and eliminating the need for jump hosts



Protect IoT devices from threats by limiting the applications, users, and endpoints who can access them

## ZSA Benefits

- Whitelist-based and cost-effective solution to protect against un-trusted remote user devices
- Single pane of glass policy management for end-to-end access
- One solution for a wide a range of secure access requirements, including data leak prevention
- Works on top of any existing enterprise network and security infrastructures
- Enterprise-grade logging, monitoring, and audit-trails for compliance



## Directed Access

Zentera Secure Access directs authenticated user accesses to land on specific resources deployed deep inside enterprise environments. Unlike a VPN, which provides users the ability to connect to the entire network, our patented application proxy network, micro-segmentation, and centralized policy engine prevent users from connecting to any system beyond their privileges.

For higher security, Zentera Secure Access can be coupled with Zentera's CoIP Platform to lock down backend servers – for example, to allow ssh access to a server, but control what a user can do once logged in.

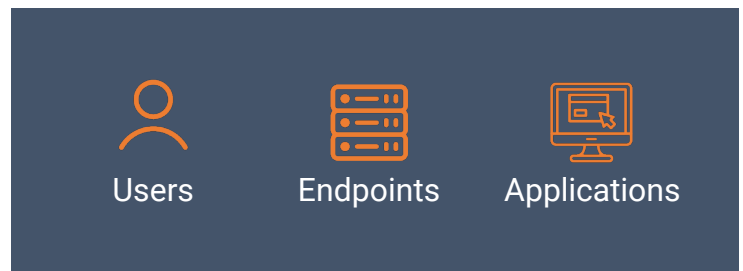
## Zero Trust Security

Following the Zero Trust model, Zentera Secure Access assumes that all users, devices, and applications

are untrusted. Instead, a series of challenges establish the necessary trust and grant access.

Users are authenticated against your existing corporate LDAP or Active Directory service, with multi-factor authentication.

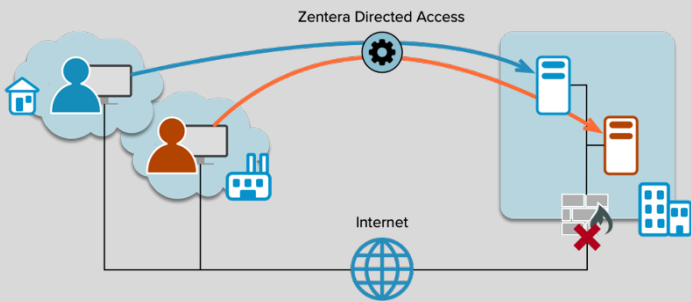
User authentication is then combined with endpoint and application authentication information and other policy factors (for example, application flow control) to make an informed access decision.



## Deploys Without Infrastructure

Zentera Secure Access can deploy either on-premises as an application, or as a SaaS hosted in Zentera's global datacenters. No VPN, router, or firewall changes are needed to quickly support a variety of different secure remote access scenarios.

A standard Windows or Linux machine can be converted into a landing target for Zentera Secure Access by deploying a lightweight software agent. For agentless installs, users connect directly to the target device via a gateway proxy.



## Overlay Security Decoupled from Firewalls and the Global Network

Zentera Secure Access' unique application proxy network technology connects any TCP/IP-based application *without* opening firewall ports or deploying a new VPN. This approach has multiple key benefits:

### *Physical Network Port Blocking*

Zentera Secure Access' application proxy network enables arbitrary proprietary applications to communicate through a firewall without opening the physical port. This allows remote access protocols, such as Microsoft RDP, to connect without opening port 3389 to inbound traffic at the firewall, which significantly minimizes the attack surface.

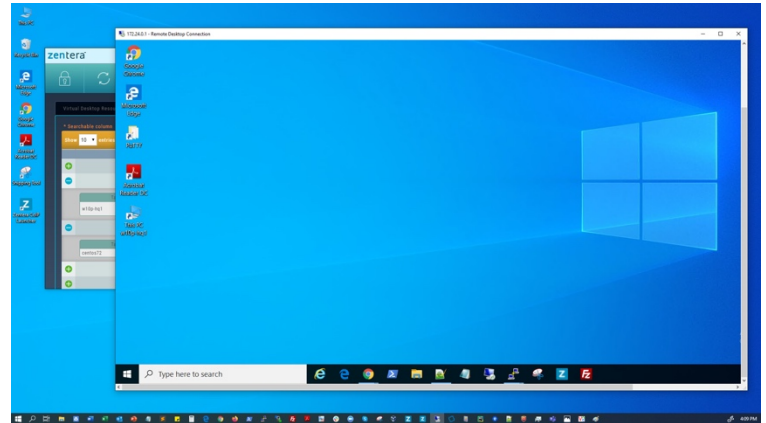
### *Centralized Management*

End-to-end access control policies can be configured, managed and enforced centrally. Reducing the number of control knobs in the infrastructure significantly streamlines setup, reduces error-prone change requests, and minimizes the troubleshooting effort.

### Secure RDP/VNC

Using the CoIP Launcher client software, an authenticated user can land directly on a remote Windows or Linux host for RDP and VNC. RDP/VNC access is guided directly to the landing server in a secure zone.

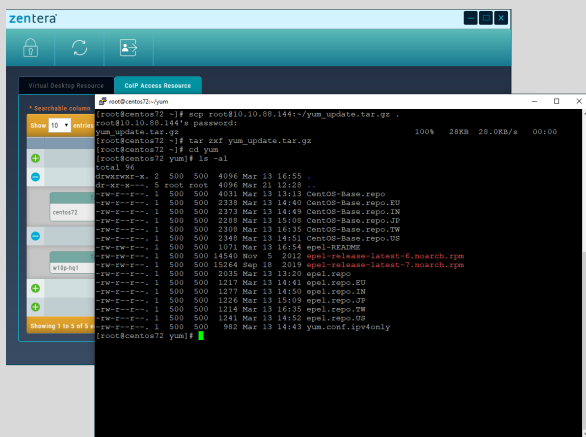
The application proxy network creates an end-to-end encrypted tunnel that locks access to the VDI client, with administrator control over copy/paste behavior.



### Secure Application, SSH, and Network Access

With Zentera Secure Access, administrators can grant remote users restricted network-level access to specific hosts in the secure zone through a Gateway Proxy or an Endpoint Proxy.

Access can be restricted to specific applications, such as proprietary client/server application protocols; standard services such as ssh or scp; or even specific web portals in the on-premises Intranet.

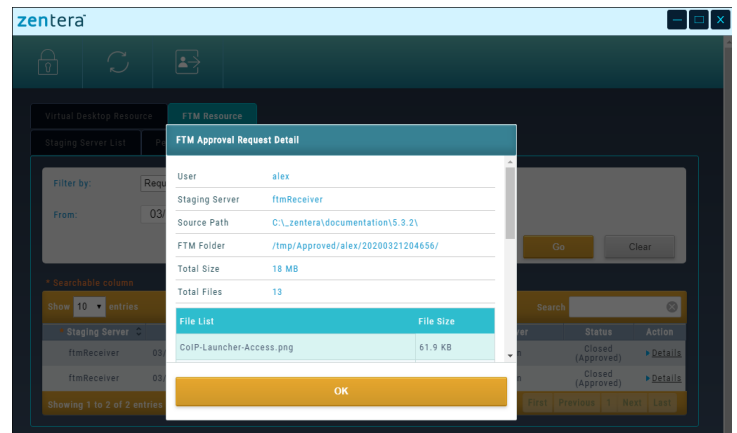


### Secure File Transfer

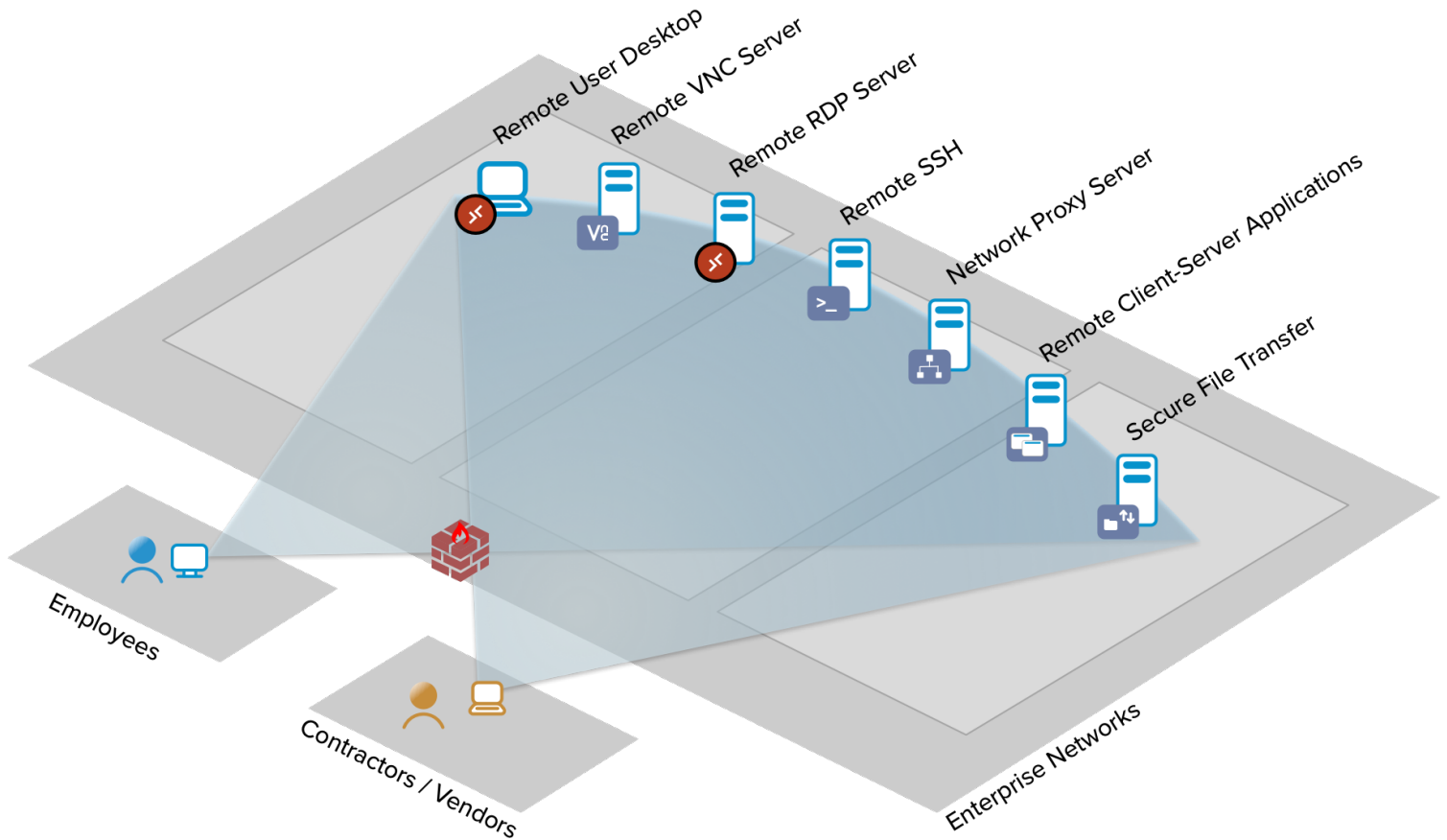
Zentera Secure Access' File Transfer Manager enables secure, policy-based file transfers into or out of a secure zone, or periodic file mirroring to a remote fileserver. Enabling the File Transfer Manager discourages shadow IT and enhances Data Leak Prevention.

Using File Transfer Manager, employees and 3rd parties can securely monitor or update files in the secure zone, without logging in or opening network access.

Administrators can define workflows enabling approvers to review and approve or reject the requested file transfer.



## Wide Range of Access Capabilities



Zentera Secure Access is deployed either as an appliance (physical or virtual) in the corporate DMZ or as a SaaS from Zentera's worldwide datacenters.

Corporate administrators can easily configure the access policy and connect remote users through Zentera Secure Access to specific resources in the on-premises environment without opening the network infrastructure. All access traffic is directed and secured with TLS 1.3 encryption, eliminating the need for a separate VPN or any network re-engineering effort.

Remote users can land on servers in the IT or OT environment with an endpoint proxy installed for virtual desktop, ssh, or proprietary application protocol access. A gateway proxy delivers secure and directed remote access to dedicated services – for example, ERP access, or access to specific manufacturer tools.

Copyright© 2020 Zentera Systems, Inc. All rights reserved. Zentera®, Zentera CoIP®, CoIP®, Cloud over IP®, and certain other marks are registered trademarks of Zentera Systems, Inc., in the U.S. and other jurisdictions, and other Zentera names herein may also be registered and/or common law trademarks of Zentera. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Zentera, and Zentera disclaims all warranties, whether express or implied, except to the extent Zentera enters a binding written contract with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Zentera. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Zentera's internal lab tests. In no event does Zentera make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Zentera disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Zentera reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.