Zero Trust Branch Connectivity securely connects your branches, factories and data centers without the complexity of VPNs, ensuring zero trust access between users, IoT/OT devices and applications based on business policies. Combining the power of Zscaler’s industry leading Zero Trust Exchange platform, with seamless connectivity for locations, clouds and users, organizations can embrace a secure access service edge (SASE) framework and enable a cafe-like branch experience.

Overcoming Legacy WAN challenges

As applications migrate to the cloud, employees adopt hybrid work models, and security becomes increasingly crucial, organizations need to rethink their WAN infrastructure. Legacy WAN technologies like MPLS and SD-WAN introduce cost and complexity without adequately solving for security. Organizations are often forced to stack multiple appliances at the branch to meet security needs, or trombone traffic through a hub site leading to a degraded user experience.

Zero Trust Branch Connectivity

- Zero Trust Branch Connectivity provides branches and factories with fast and reliable access to the internet, SaaS and private applications with a direct-to-cloud architecture that provides high security and operational simplicity
- It eliminates lateral threat movement by connecting users and IoT/OT devices to applications through the Zero Trust Exchange.
- It dramatically simplifies branch communications by eliminating complex routing, VPNs, firewalls, while allowing for flexible forwarding and simple policy management by using the proven ZIA and ZPA framework.

Solution benefits:

- **Reduced complexity**
  Eliminate the complex mesh of site-to-site VPNs and overlay routing.

- **Improved user experience**
  Eliminate unnecessary traffic tromboning and improve performance for SaaS and cloud apps without compromising on security. Enforce security and bandwidth policies at over 150 Zscaler data centers globally.

- **Improved security**
  Minimize the attack surface and the risk of lateral threat movement inherent to SD-WAN devices without additional firewall/VPN appliances. Simplify user-to-app and app-to-app segmentation using the cloud-native Zero Trust Exchange platform.

Improved user experience
Eliminate unnecessary traffic tromboning and improve performance for SaaS and cloud apps without compromising on security.

Enforce security and bandwidth policies at over 150 Zscaler data centers globally.

Improved security
Minimize the attack surface and the risk of lateral threat movement inherent to SD-WAN devices without additional firewall/VPN appliances. Simplify user-to-app and app-to-app segmentation using the cloud-native Zero Trust Exchange platform.
Solution Use Cases

Replace site-to-site VPNs
Replace mesh of site-to-site VPNs connecting branches, factories, and data centers with simple plug and play connectivity that delivers operational simplicity with better security.

Secure access to IoT/OT resources
IoT/OT assets need to be regularly accessed by employees and third-party vendors to maximize production uptime and avoid disruptions from equipment and process failures. Zero Trust Branch Connectivity simplifies access to IoT/OT resources without the need for VPNs or exposed ports, providing fully isolated, clientless remote desktop access to internal RDP and SSH target systems for vendors/contractors.

Accelerate M&A integration
Be operational on day one by avoiding the need to merge routing domains or translate overlapping IP addresses. Connect new users to critical resources like Active Directory by simply adding plug & play appliances to new sites.

IoT device discovery and classification
IT teams face blindspots as unsanctioned, unknown IoT devices connect to branch office networks resulting in a greater risk of malware infestations across the organization. Zscaler identifies and classifies devices to give IT teams deeper visibility into behavior for better access control policies.

Figure 1: Zero Trust Branch Connectivity Solution
Zero Trust Branch Connectivity uses a Z-Connector (Branch Connector) plug & play appliance available in virtual or physical form factors.
Accelerate your SASE journey with Zscaler’s industry-leading Zero Trust Exchange

- Transform your branch
  By using Branch Connector behind a router or an SD-WAN appliance, enterprises can secure network edges and protect critical services with a complete end-to-end Zero Trust architecture.

- Get unlimited scale
  Cloud-native security services delivered from over 150 data center locations with no artificial chokepoints.

- Simplify and streamline operations
  By moving towards a single-vendor SASE, enterprises can manage connectivity and security through a common platform and be more secure and agile.

Business Analytics
Knowledge from trillions of daily telemetry signals

Cyber Threat Protection
Prevent compromise and lateral movement

Data Protection
Prevent data loss, inline and API

Zero Trust Connectivity
Users, Branches, Factories, Public Clouds, Data Centers

Globally Distributed Cloud: 150+ Data Centers, China Connectivity, Peering, BCP/DR