



# Zscaler Zero Trust SD-WAN

Securely connect branches, factories and data centers and extend zero trust security to servers and IoT/OT devices in any location.

Hybrid work and cloud transformation have upended perimeter-based network and security models, with private applications moving to the cloud and users accessing applications over the public internet, on any device, from any location.

In today's landscape, many enterprises also leverage IoT/OT devices across various locations—including branches, factories, and data centers—to streamline their operations. Additionally, a considerable number of customers rely on server-to-client workload communication. Traditional approaches that depend on legacy WANs, mesh VPNs, and firewalls to manage application access have become ineffective in a world that prioritizes cloud and mobile technologies.

However, as organizational requirements have evolved, legacy WAN solutions struggle to keep pace. SD-WAN presents various challenges, such as limited security through network-based access, an expansive attack surface, extensive lateral movement privileges, and routing complexities. Layering on zero trust principles to this network often requires adding additional firewall appliances, adding cost and complexity.

## Zscaler Zero Trust SD-WAN:

- **Enables zero trust everywhere** for all users, devices, servers, and IoT/OT, regardless of location
- **Improves application performance** by sending branch traffic directly to the Zero Trust Exchange and trusted application traffic directly across the internet with direct internet breakout
- **Prevents lateral threat movement:** zero trust builds a foundation for secure connectivity that enables east-west segmentation
- **Eliminates the attack surface** by connecting branches and data centers through Zero Trust Exchange independent of the underlying transport
- **Enables shadow IoT device discovery and classification** with automatic device classification based on traffic profiles
- **Simplifies secure access to OT resources** with clientless browser-based access to SSH/RDP/VNC ports on OT assets
- **Enforces finely-grained forwarding policies** for internet and non-internet traffic using ZIA or ZPA
- **Introduces plug-and-play deployment:** zero touch provisioning (ZTP) simplifies deployment and reduces time to integration

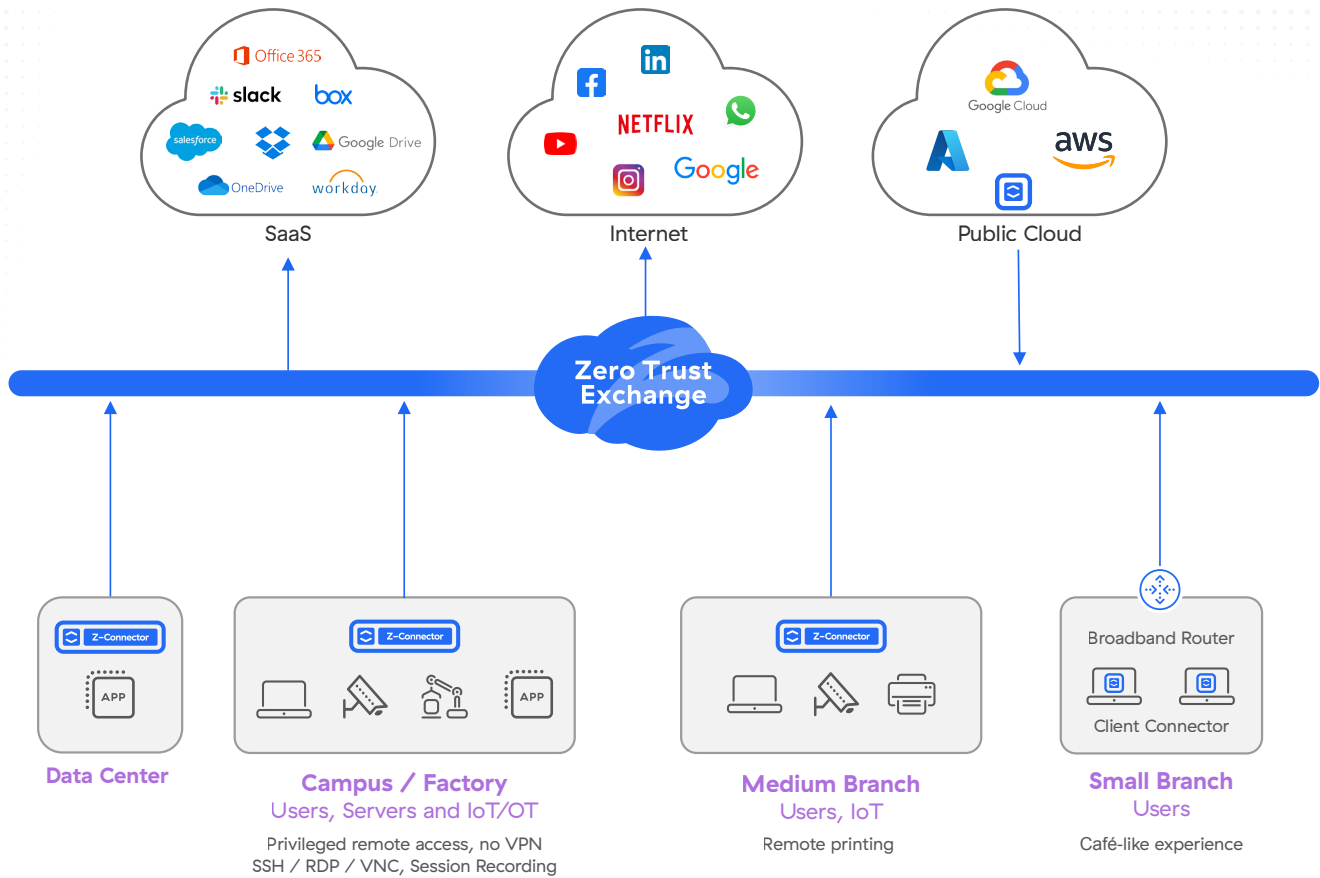


Figure 1: Zero Trust SD-WAN

Zero Trust SD-WAN 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 organizational policies.

## Traditional SD-WAN is not Zero Trust

Organizations face several challenges when using legacy network and security architectures to connect a branch to the internet or to their other applications in a public cloud or data center environment, including:

- **Greater risk of lateral threats and internet-based attacks** from using legacy, network-centric connectivity solutions such as site-to-site VPNs, firewalls, or traditional SD-WANs. These solutions overextend a customer's trusted network across the internet to other clouds and on-premises environments, increasing the attack surface. A patchwork of security appliances, tools, and non-standard policies lead to increased security risk due to known and unknown gaps in security coverage.

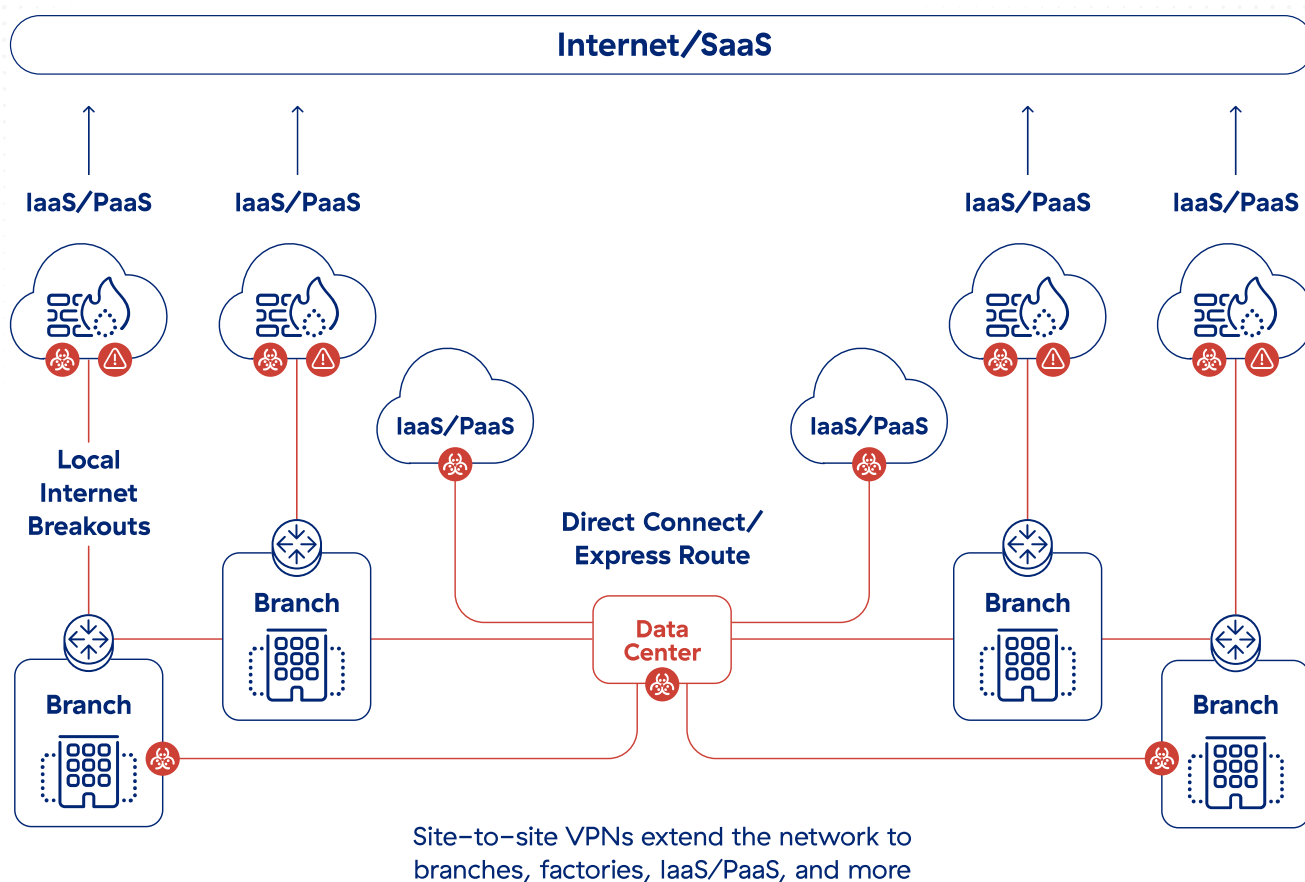


Figure 2: Greater risk of lateral threats and internet-based attacks with traditional SD-WANs

- **Increased complexity** due to complicated routing, multiple network hops and appliances, and fragmented policy management from introducing legacy models to the cloud. Managing this complexity is a difficult task for networking and security teams as they struggle to standardize connectivity and enforce security policy across branch, cloud, and data centers.
- **Lack of visibility** across branch, data center, and cloud connectivity paths, which creates network and security blind spots.
- **Poor performance and scalability** due to the increasing number of network and security services within branch and data center environments, traffic hairpinning and chokepoints for centralized security inspection and control.
- **High costs** due to legacy network and security appliances (e.g., firewalls, IPS, routers, and other point products), overprovisioning of network services to compensate for lack of scalability, and increased use of cloud native services.

## How Zero Trust SD-WAN works

Zero Trust SD-WAN enables organizations to build a thin branch by eliminating multiple products such as routers, firewalls and VPNs with a simple plug-and-play device that can be deployed quickly using only an internet connection. This allows organizations to reduce the complexity associated with managing multiple devices and optimize the overall functionality of the branch. Zero Trust SD-WAN dramatically simplifies branch communications with zero trust network overlay that allows for flexible forwarding and simple policy management by using the proven ZIA and ZPA policy framework.

Branch traffic can be securely forwarded directly to the Zero Trust Exchange, where ZIA or ZPA policies can be applied for full security inspection and access identity-based control of branch and data center communications. Trusted application traffic can be sent directly across the internet with direct internet breakout. This unique approach provides three key advantages:

- You move away from network-based site-to-site VPN connectivity to identity and application-based communication for true, zero trust security
- You eliminate a legacy castle-and-moat architecture without compromising security;
- no need for legacy products such as Squid proxies, NAT gateways, IPSs and so on
- You provide distributed, scalable connectivity wherever it's needed, with centralized, automated policy management to simplify branch and data center communications

## Zero Trust SD-WAN use cases

### Site-to-site VPN replacement

Connect branches directly to private applications without extending your WAN or relying on VPNs, both of which increase a network's attack surface. Applications are hidden from discovery behind the branches, and access is restricted via the Zero Trust Exchange to a set of named entities. Identity, context, and policy adherence of the specified participants are all verified before access is allowed, prohibiting lateral movement elsewhere in the network.

### Mergers and acquisitions

Merging two separate networks is challenging and time-consuming. Problems range from IP overlaps and routing issues to increased security risk from an enlarged network attack surface. With Zero Trust SD-WAN, networks can remain separate and branch locations in one environment can

quickly connect to private applications in another, without disruption.

### Direct internet access enablement for branches

On-premises networking and security models become less effective as organizations migrate their apps to the cloud and build cloud native apps. Zscaler Zero Trust SD-WAN is a purpose-built solution for branch transformation, ushering in a new model that enables branches to communicate with any destination securely and independently from the underlying network.

### Zero trust for server, IoT/OT connectivity

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 SD-WAN for IoT/OT provides fully isolated, clientless remote desktop access to RDP and SSH target systems—without having to install a client on their device using jump hosts and legacy VPNs.

### Shadow IoT/OT discovery and visibility

IT teams face blind spots as unsanctioned, undiscoverable devices connect to branch office

networks, and the result is an increase in device vulnerability and a broader attack surface. Zscaler identifies and classifies devices to give IT teams deeper visibility into behavior for better access control policies.

## Z-Connector Plug & Play Appliances

FEATURE	ZT 400	ZT 600	ZT 800	ZT VM
				
Type	Small-Medium branches	Small-Medium branch	Medium-Large branch	Branch and Data Center
Throughput/hypervisor	200 Mbps	500 Mbps	1 Gbps	KVM, ESXi
Physical ports	4 x GbE	6 x GbE	8 x GbE	N/A
Zero touch provisioning	✓	✓	✓	✓
Granular forwarding policy for internet, private applications, and direct WAN traffic	✓	✓	✓	✓
Leverage URL filtering, file type control & cloud firewall policies for internet bound traffic	✓	✓	✓	✓
Zero Trust ZPA policies for IoT devices, servers	✓	✓	✓	✓
Centralized visibility and logging	✓	✓	✓	✓

ZSCALER ZERO TRUST SD-WAN CAPABILITIES	
FEATURE	DETAILS
<b>Capabilities</b>	
Zero touch provisioning and automated deployment	<ul style="list-style-type: none"> <li>Zero touch provisioning with pre-defined templates</li> <li>Fully automated deployment</li> <li>Dynamic discovery of branch office geo-location</li> </ul>
Granular forwarding policy for internet and private application traffic	<ul style="list-style-type: none"> <li>Options to send the traffic to ZIA, ZPA, or Direct across the internet</li> <li>Flexible traffic selection criteria location, sublocation, location group, 5 tuple, or FQDN</li> </ul>
Unified zero trust policies	<ul style="list-style-type: none"> <li>Unified policy for user-to-application, IoT device-to-application, and server-to-server through ZPA's enhanced policy to include new client types</li> <li>Location and geo-based policies</li> <li>Security policy enablement that includes IPS, SSL proxy, URL filtering, and data protection</li> <li>Full security stack with posture configured for IoT/OT and servers</li> </ul>
High availability	<ul style="list-style-type: none"> <li>Two instances of Zero Trust SD-WAN operating in HA mode provide additional support for traffic bursts and redundancy in case of a hardware failure</li> <li>Active-passive fault tolerance using a virtual IP address (VIP) based on common address redundancy protocol (CARP)</li> <li>Active-active circuits (single appliance)</li> <li>Active-active circuits (dual appliance when balancing FHRP)</li> </ul>
Centralized visibility and granular logging	<ul style="list-style-type: none"> <li>Centralized dashboard for device health and traffic monitoring</li> <li>Available filtering for cloud, data center, and branch deployments</li> <li>Detailed logging of every session and transaction for all ports and protocols—including all public and private DNS transactions</li> <li>Full integration with Nanolog Streaming Service infrastructure with option to stream logs to customer owned SIEM</li> </ul>
WAN interface termination	<ul style="list-style-type: none"> <li>Dual ISP connectivity (Ethernet)</li> <li>Multi-homing with a single appliance</li> </ul>
LAN interface management	<ul style="list-style-type: none"> <li>Multiple L3 LAN Networks</li> <li>802.1q/VLAN tagging support</li> <li>DHCP Server</li> <li>DNS gateway</li> </ul>
On-device firewall policies	<ul style="list-style-type: none"> <li>Granular access control for local LAN to LAN (east-west) traffic</li> <li>L3/L4 Access Control Lists (ACLs)</li> </ul>
Application aware path selection	<ul style="list-style-type: none"> <li>Dynamic path selection for mission-critical SaaS or private applications</li> <li>Intelligent Zscaler POP connectivity</li> <li>Built-in SLA monitoring and failover</li> </ul>
Routing	<ul style="list-style-type: none"> <li>Static routing</li> </ul>
Zscaler Data Centers/POPs	<ul style="list-style-type: none"> <li>Zscaler has built its cloud security platform in more than 150 data centers across the world — strategically placed where customers are located</li> <li>Built-in availability with seamless failover to next available service PoP</li> </ul>



Experience your world, secured.™

#### About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](https://www.zscaler.com) or follow us on Twitter @zscaler.

© 2023 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/](https://www.zscaler.com/legal/) trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.