DATA SHEET

Zero Trust Branch

A simpler, safer, more cost-effective way to connect and secure your branches, campuses, and factories

Legacy Network and Security Architectures are Complex and Facilitate Ransomware Attacks

Traditional networks weren't built for today's distributed workforces and cloud-first apps. Using firewalls, VPNs, and legacy SD-WANs creates many security and operational challenges, including:

- **Expanded Attack Surface**

  Extending networks to remote sites amplifies your attack surface. Firewalls and VPN gateways become targets, and zero-day threats are prevalent

- **Lateral Threat Movement**

  Infected devices in branch offices can infect everything on your network — fast. Ransomware attacks can cause crippling outages in as little as 45 minutes

- **Cost and Complexity**

  The complex mix of firewalls, proxies, NAC agents, and IP-based policies adds significant operational complexity and cost, hindering business agility

- **Poor Performance and User Experience**

  Routing traffic through data centers and multiple security layers slows application performance and frustrates users

Zero Trust Branch

Delivers a café-like branch experience

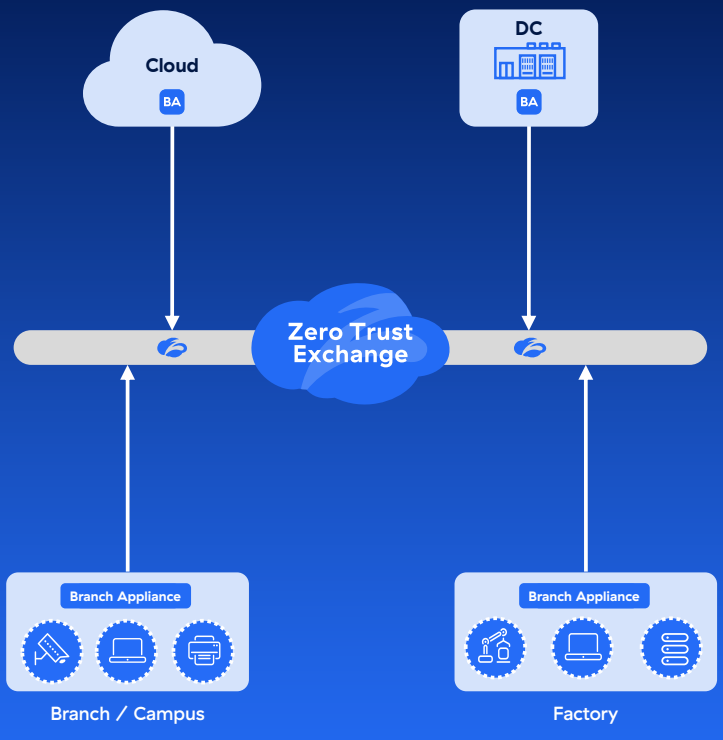
Connect users and devices to apps without extending your network to every branch

Stops lateral movement of ransomware

Segment users and OT/IoT devices in days—not months or years

Cuts firewall and infrastructure spend by 50%

Eliminate N/S and E/W firewalls, NAC, expensive proprietary switches and device agents.



How it works

Zscaler Zero Trust Branch securely connects and segments your branches, factories, and data centers without the complexity of VPNs or overlay routing. It enables zero trust access from users and IoT/OT devices to applications based on your organization's security policies. By combining the power of Zscaler's industry-leading Zero Trust Exchange platform with an integrated Branch Appliance deployed in branches, campuses and factories, organizations can embrace a secure access service edge (SASE) framework, segment critical OT/IoT devices and enable a café-like branch.

Zero Trust Branch appliances directly terminate ISP connections and manage traffic forwarding across multiple links for maximum availability and resiliency. Branch and factory traffic is securely forwarded to the Zero Trust Exchange where rich AI-powered cyber threat and data protection policies can be enforced.

With our industry-leading zero trust architecture, sites are automatically segmented from each other, preventing the lateral movement of malware. Within each site, our innovative "network-of-one" segmentation technology automatically classifies and isolates each IoT/OT device without the need for NAC, scanners or endpoint agents. Auto-grouping and threat-level based policies reduce the blast radius, simplify compliance and automate incident response, all without firewalls.

With automatic device discovery and classification, network administrators can simplify policy management by automatically grouping devices based on behavioral identity and avoid complex inventory management.

Zero Trust Branch appliances also feature an integrated AppConnector which facilitates third-party Privileged Remote Access to OT/IoT resources without the need for VPNs, jump boxes or VDI farms.

Zero Trust Branch Use Cases

VPN replacement: Eliminate the complexity of site-to-site VPNs and routed overlays with a simpler, more cost effective solution that reduces your attack surface and stops the lateral movement of threats.	**IT/OT Segmentation:** Secure factories, hospitals and critical infrastructure by eliminating lateral movement between IT and OT systems. Get segmentation done in days, not months or years
SD-WAN refresh: Adopt a cafe-like branch architecture and reduce ransomware risk. Enhance security with a Zero Trust Secure Access Service Edge (SASE) framework.	**AI-powered Device Discovery & Classification:** Discover, classify and inventory OT/IoT devices without the need for endpoint agents, scanners or traffic mirroring.

Zero Trust Branch Capabilities

Category	Features
Simplified Provisioning	• Single Touch provisioning with pre-defined templates • Activation URL or Code to securely provision appliance to tenant • Template and site-profile based deployment
Traffic Forwarding Policy	• Flexible traffic selection criteria: dynamic groups, user and machine identity, five tuple, FQDN or MAC • Traffic forwarding options: ZIA, ZPA, Routes Tunnel or Direct • Intelligent route priorities: static, dynamic, policy-based

DNS Policy Engine	• Explicit and Transparent DNS Proxy intercept all DNS queries* • Applies L7 policies based on requested FQDN or Domain • Policy Actions Accept/Reject/Override/Redirect
Unified Zero Trust Policies	• Full Integration with ZIA and ZPA • Privileged Remote Access (PRA) Support • Unified policies: user–to–app, IoT device–to–app, and server–to–server • Location and geo–based policies • Comprehensive security inspection including IPS, SSL/TLS decryption, proxy, URL filtering and data protection • Comprehensive protection for IoT/OT devices • Inbound connectivity with AppConnector
Incident Response	• Ransomware Kill Switch
Interfaces	• Multiple L3 LAN networks • Multiple L3 WAN networks • 802.1q/VLAN tagging • Link Aggregation (802.3ad) • Dedicated management interface
High Availability	• Two–node cluster with VRRP and session sync • Interface health monitoring • Config and state sync • Hitless software upgrades • In–service hardware replacement
Routing & Network Services	• Static Routing • Dynamic routing — BGP, OSPF • Network Address Translation (source NAT) • DHCP Server, Relay / Proxy • Equal Cost Multi–Path (ECMP)
Application Aware Path Selection	• Dynamic app–aware path selection • Built–in link monitoring and failover
Device Isolation	• Agentless device Isolation (“Network of ONE”) • Dynamic micro–subnets • MAC address–based filtering
Zero Trust Segmentation	• Autonomous grouping and policy • IntraVLAN and InterVLAN policy control • Flexible hierarchical policy framework based on devices, tags, users identity, time and, zones
Asset Discovery & Profiling	• Endpoint and network discovery • Device fingerprinting • Profile–based device categorization • ICS and Medical protocol decoding
Monitoring & Troubleshooting	• Remote debug console • Local CLI on Zero Trust Branch devices • SNMP v2/v3 support
Centralized Management	• Single sign–on (SSO) and MFA • Audit trails for login events, and configuration changes • Role–based access control • Multitenant cloud delivered platform with single UI • OneAPI for comprehensive automation • Dedicated Managed Service (MSSP) Portal

Visibility and Logging	• Comprehensive session and transaction logging for all ports and protocols • Traffic map with policy correlation • Integrated Elastic data lake • Session–init logs for all intra and inter segment communications
Integrations	• Microsoft Active Directory • EDR Vendors – Crowdstrike, SentinelOne • Asset Management – Armis, ServiceNOW, Ordr
Zscaler Data Centers / POPs	• Global cloud security platform delivered from more than 150 data centers • Built–in availability and redundancy with seamless PoP failover

Zero Trust Branch Appliances

Zscaler Zero Trust Branch appliances are available in a range of physical or virtual form factors for branch, campus and factory deployments.

	ZT 400	ZT 600	ZT 800	ZT 8010
Front View				
Ideal For	Small branch	Small to medium branches	Branches, Factories	Factories, Campuses
CPU	4C	4C	8C	16C
DRAM	32 GB	32 GB	64 GB	128 GB
Storage	256 GB	256 GB	512 GB	1 TB
TPM	2.0			
LAN/WAN RJ45 Ports	4 x 1GbE RJ45	6 x 1GbE RJ45	6 x 1GbE RJ45	10 x 1GbE RJ45
LAN/WAN Fiber Ports	NO	NO	2 x 1Gb SFP	8 x 10G SFP+
USB Port	1x USB 3.1	2x USB 2.0		2x USB 3.0
Console Port	1 x RJ45			

	ZT 400	ZT 600	ZT 800	ZT 8010*
Physical Specifications				
Factor Form	Desktop	Desktop	Desktop	Rackmount – 1U
Dimensions (W x H x D)	6.61 x 1.26 x 7.20 in (16.76 x 3.175 x 18.29 cm)	9.09 x 1.73 x 7.78 in (23.08 x 4.39 x 19.76 cm)		17.24 x 1.73 x 12.64 in (43.8 x 4.4 x 32.1 cm)
Weight	1.98 lbs (0.898 kg)	2.64 lbs (1.197 kg)		18.96 lbs (8.6 kg)
Mounting Brackets	Rackmount/ Wallmount (Optional Kit)	Rackmount included by default		
Power Specifications				
Power Supply	DC: External AC power adapter included			Internal: AC
Redundant Power Supply	No			Yes (1+1)
Typical Power Consumption	Idle Mode — 12W Full Load Mode — 20W	Idle Mode — 21W Full Load Mode — 29W	Idle Mode — 24W Full Load Mode — 43W	Idle Mode — 107.8W Full Load Mode — 225.5W
Maximum Power Consumption	40W		60W	Redundant PSU: 300W Single PSU: 350W
Power Cord Rating	C14 10A			
Input Range	AC 100~240V@50~60 Hz			Redundant PSU: AC 100~240V @50~60 Hz Single PSU: AC 100~240V @47~63 Hz
Input Current	1.7Amax		1.8Amax	5Amax
Output Rating	11.4 ~ 12.6V			
Cooling	Fanless	Fan		
Environmental Specifications				
Operating Temperature	32 ~ 104°F (0 ~ 40°C)			
Non-Operating Temperature	-4 ~ 150°F (-20 ~ 70°C)			
Relative Humidity	5% ~ 90%, Operating 5% ~ 95%, Non-operating			
Altitude	5,000 feet (1,524 m) Operating 50,000 feet (15,240 m) Non-operating			
MTBF	89,959 hrs	69,464 hrs	88,439 hrs	71,924 hrs

Zero Trust Branch Virtual Machine

Environmental Specifications	Option 1	Option 2
CPU	4 vCPU	8 vCPU
Memory	16 GB	32 GB
Storage	256 GB	256 GB
Ports	4 x vNICs	4 x vNICs
Throughput (64 KB HTTP)	10 Gbps	20 Gbps
Sessions	500K	1 Million
Number of Endpoints	500	1,000

Ordering Information

Zscaler Zero Trust Branch devices are sold as part of a subscription that includes the hardware and the cloud service. Please consult your Zscaler representative for subscription options and appliance selection based on bandwidth needs.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com