zscaler™ | FedRAMP

Zero Trust Branch for FedRAMP Environments

Secure and simplify distributed public sector sites with Zero Trust Branch. Stop lateral movement, accelerate site onboarding, and modernize connectivity for field offices, campuses, and mission locations.

FedRAMP Moderate and High Authorized

Solution Brief

The Issue at Hand

Public sector operations are increasingly distributed. Civilian field offices, regional service centers, research campuses, transportation facilities, border stations, and operational sites all need reliable, secure connectivity to centralized mission applications and cloud services. But most site networks were not designed for today's threat model, compliance requirements, or operating tempo.

Traditional architectures at distributed public sector sites typically combine SD-WAN routing overlays, site-based firewalls, VPNs, and hub-and-spoke backhaul into regional hubs and agency data centers. That design creates four persistent problems:

- **Expanded blast radius.** Routed overlays and site-to-site connectivity can unintentionally make lateral movement easier once any site is compromised, turning a local incident at a regional office into an agency-wide incident that reaches mission-critical systems and data center resources.
- **Fragmented security operations.** Location-based security policies (per-site firewalls, ACLs, and NAC configurations) are managed separately from user and device security posture, creating multiple panes of glass, inconsistent controls, and slow change management. This fragmentation is compounded by the need to demonstrate compliance across dozens or hundreds of diverse environments.
- **High cost and slow provisioning.** Private lines and MPLS are expensive and slow to provision. Adding sites frequently means weeks or months of network buildout, firewall rule engineering, and troubleshooting—a burden that scales directly with the number of locations an agency or organization operates.
- **Reorganization friction and IP overlap.** Agency consolidations, facility realignments, and newly acquired or partner-connected sites commonly arrive with overlapping RFC1918 addressing, which can stall integration and delay access to critical mission applications, shared services, and identity infrastructure.

These sites are operationally intensive with badge readers, security cameras, HVAC systems, screening equipment, and specialized sensors operating alongside standard IT every day. As a result, network complexity becomes a mission productivity issue, not just an IT issue. A common example is cross-site application access, where field personnel reaching centralized case management, logistics, or operational systems must traverse multiple network hops, NAT domains, and firewall zones, creating fragile dependencies that get worse with scale.

Legacy security architectures are the bottleneck to modernizing distributed government operations.

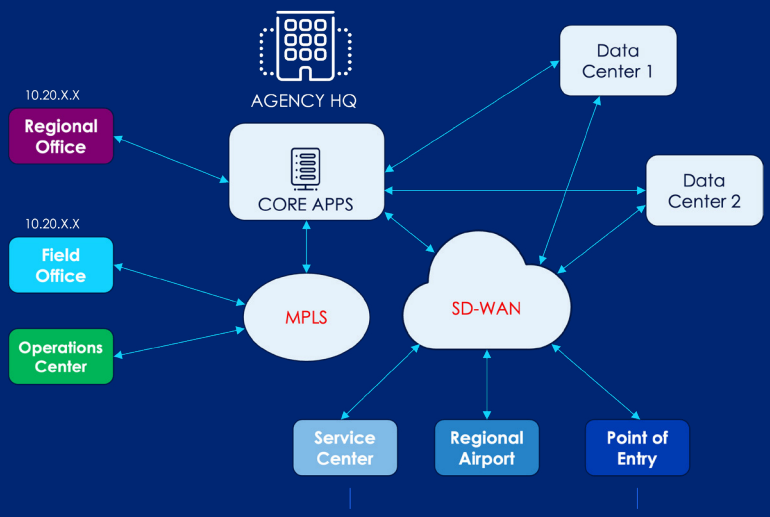
How This Impacts Agencies

Complexity
Location-based firewalls are slow to change, and complex routing overlays share routes across entire agency network

Risk
A breach in any field site can directly spread to mission-critical systems and data centers

Cost
Reliance on expensive MPLS circuits and hardware firewalls drives endless refreshes

Slow Provisioning
Onboarding new sites, resolving overlapping IPs, and adding services takes weeks or months



Legacy security architectures are the bottleneck to modernizing distributed government operations

Recommended Approach

A site security strategy that scales across a distributed public sector footprint should aim to:

- **Stop lateral movement by default** between sites, and from field sites to data centers and mission-critical services.
- **Reduce the branch security footprint** between sites, and from field sites to data centers and mission-critical services.
- **Segment and protect IoT, OT, and unmanaged devices** that cannot run agents or EDR, including sensors, cameras, HVAC controllers, badge readers, screening equipment, and legacy systems with end-of-life operating systems.
- **Enable safe third-party access** for contractors, vendors, and maintainers without exposing inbound ports or granting broad network access.
- **Accelerate site onboarding and reorganization**, even when IP overlap exists, so new or consolidated sites reach operational status in days, not months.
- **Apply policy consistently** across dozens or hundreds of sites without per-site firewall rule engineering.

Zero Trust Branch

Zero Trust Branch for FedRAMP Environments is a public-sector-focused approach built on **Zero Trust Branch** capabilities: modern connectivity plus integrated, policy-driven controls for users, devices, and applications without relying on implicit trust in the network.

Architecture Overview

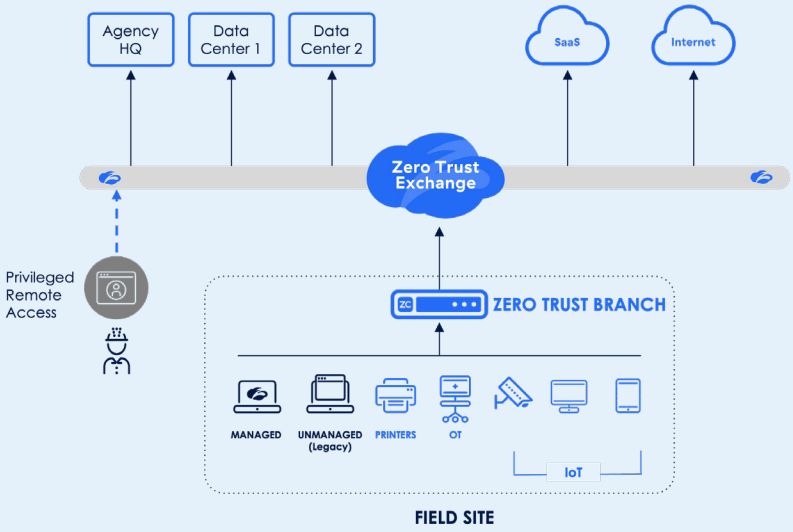
At each site, a **Zero Trust Branch appliance** becomes the standard unit of deployment, and:

- **Provides Zero Trust SD-WAN** to simplify and modernize site connectivity, replacing complex hub-and-spoke designs and routed overlays.
- **Enables agentless device segmentation** for IoT, OT, and unmanaged endpoints, enforcing segmentation even inside the site LAN without requiring agents, scanners, or VLAN restructuring.
- **Extends private access** patterns beyond users to headless devices so they can securely reach approved services in data centers and cloud environments.
- **Supports inside-out connectivity models** for privileged remote access so there is no inbound exposure to the internet.

This produces a site design where connectivity and security are **policy-driven and identity/context-aware,** rather than dependent on IP adjacency, flat VLANs, and sprawling firewall rules.

Zero Trust Branch

Simplify Distributed Sites and End Lateral Threat Movement



One platform. Secure communications between agency users, devices, and mission applications

Zero Trust SD-WAN: Replace complex hub-and-spoke networks and complex routing overlays while eliminating lateral threat movement and attack surface

Device Segmentation: Automatically discover, visualize and isolate every device-IoT, managed, and unmanaged systems – without agents

Privileged Remote Access: Give third-party contractors controlled access only to specific apps, never the network

What Gets Eliminated

✕ MPLS ✕ VPN ✕ Firewalls ✕ Complex Routing

Core capabilities

1) Secure Internet and SaaS Access from the Site

Legacy designs tie internet security to branch firewalls and backhaul through regional hubs, creating bottlenecks and expanding the attack surface at every location. When internet-bound traffic must traverse MPLS or VPN tunnels back to a centralized inspection point, the architecture becomes fragile, expensive, and slow to change.

Zero Trust Branch secures internet and SaaS traffic from each site by forwarding it to the Zero Trust Exchange for cloud-delivered inspection and policy enforcement. This replaces north-south firewalls at the branch edge and eliminates dependence on hub backhaul.

- Protect internet and SaaS access for users, managed endpoints, guest devices, printers, servers, and IoT/OT systems at each site.
- Replace branch internet firewalls and reduce costly backhaul through regional hubs.
- Apply consistent, cloud-delivered inspection and policy enforcement, including IPS, SSL/TLS decryption, URL filtering, and data protection, regardless of site location.
- Improve user and mission experience while shrinking the exposed attack surface.

2) Secure Communications Between Sites

Branch-to-branch and branch-to-application connectivity in legacy architectures depends on routed overlays and site-to-site VPNs. These designs extend the network to every location, creating broad lateral movement pathways. A compromise at one field office can traverse the overlay to reach mission-critical systems at any other connected site or data center.

Zero Trust Branch replaces these patterns with policy-brokered, non-routable connectivity through the Zero Trust Exchange. Sites communicate through the cloud, not through network adjacency. The result is no shared routing domain, no site-to-site VPN mesh, and no implicit trust between locations.

- Secure communication between field sites and between field sites and private mission applications without extending routing domains.
- Replace site-to-site VPNs, MPLS dependency, and traditional SD-WAN overlays.
- Prevent malware and ransomware from spreading across locations; each site is isolated by default.
- Simplify rapid onboarding of new offices, labs, field sites, and temporary or emergency locations, even when overlapping IP ranges exist.

3) Secure Devices Within Each Site

Distributed public sector sites are full of devices that cannot support agents such as security cameras, badge readers, HVAC controllers, screening systems, environmental sensors, legacy endpoints, and specialized OT equipment. Device security inside these sites still depends on VLANs, ACLs, NAC, and east-west firewalls—designs that are complex, incomplete, and rarely finished.

Zero Trust Branch applies an agentless segmentation model that can:

- **Discover and profile devices** in-line using passive signals—DHCP fingerprinting, protocol observation, and other network-visible telemetry—without requiring scanners, span ports, or endpoint agents.
- **Enforce "network-of-one" isolation** (per-device, /32-style segmentation) so each device is treated as a distinct security entity, not as a member of a broadly trusted subnet.

- **Control east–west traffic inside the site** by routing device communications through the enforcement point, so “same VLAN” does not mean “implicitly trusted.”
- **Apply policy based on device identity and context** (device type, role, observed behavior) not just IP address.

This approach contains ransomware–style lateral movement and reduce the probability that a compromised endpoint at any site can pivot to other systems or upstream mission services.

Privileged Remote Access for Contractors and Vendors

Contractors and third–party vendors routinely need access to systems and devices at distributed sites for maintenance, support, and operational tasks. Traditional methods such as VPNs, jump boxes, exposed inbound services and expand the attack surface and increase the likelihood of credential abuse.

Zero Trust Branch supports privileged access patterns that:

- Provide inside–out connectivity with no inbound exposure to the internet.
- Enable access to specific targets using common protocols (RDP, SSH, VNC) without granting broad network reachability.
- Support granular, auditable access policies aligned to least privilege.

Site Workflow Spotlight: Cross–Site Mission Application Access

Cross–site application access is a high–friction example of how legacy site networking shows up in day–to–day operations.

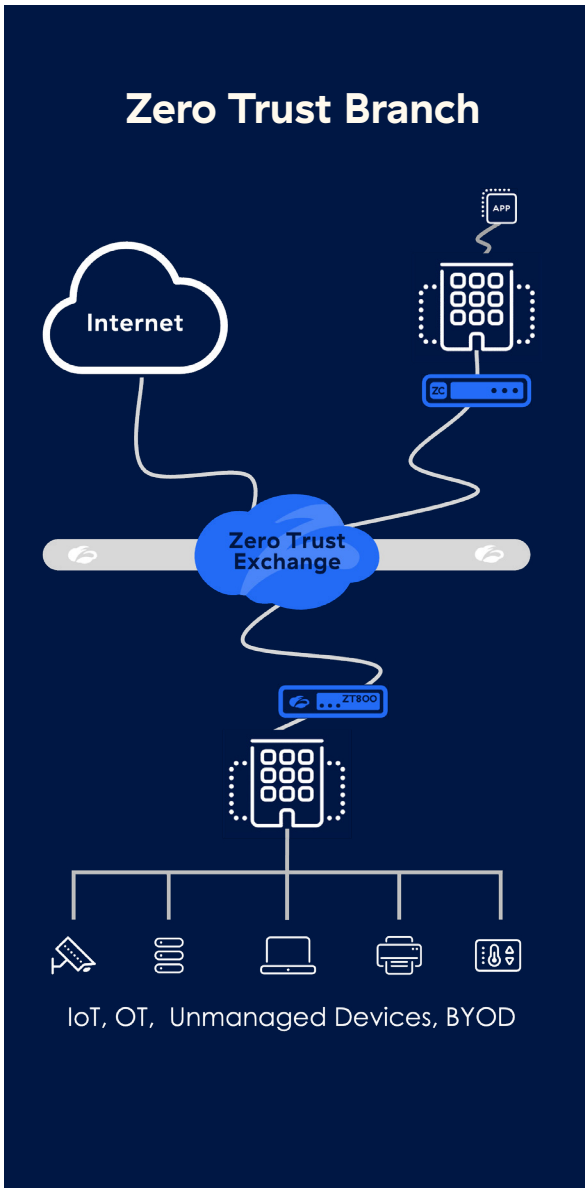
In a typical legacy architecture, field personnel at a regional office access a centralized mission system for case management, logistics, screening databases, or operational platforms through a chain of network hops: branch firewall, MPLS or VPN tunnel, hub router, core firewall, NAT translation, data center firewall, and finally the application. That path can involve six or seven hops each way, with IP address conflicts between sites slowing integration and making troubleshooting difficult. A compromise at any point in this chain can move laterally across the shared network to other sites and data center resources.

With Zero Trust Branch, the same access pattern is reduced to two hops: the Zero Trust Branch appliance at the field site forwards traffic to the Zero Trust Exchange, which brokers a direct, policy–governed connection to the application. Each site is isolated. Overlapping IP ranges are irrelevant. New sites gain immediate access to mission applications on day one.

This pattern applies to any distributed application access scenario:

- Field agents accessing centralized case management or screening systems.
- Regional office staff reaching shared services, HR, or financial platforms.
- Technicians at remote facilities connecting to operational management systems.
- Personnel at temporary or emergency sites needing immediate, secure access to agency resources.

For agencies operating dozens or hundreds of distributed locations, this workflow is frequently the first operational pain point that reveals whether site security architecture will scale.



1 Secure Location Access to the Internet

Leverages ZIA and Branch Connector

- Secure a site's internet access for PCs, servers, printers, IoT/OT, badge systems, etc.
- Start with secure internet access and expand to device segmentation and inter-site connectivity as needed

Top Use Cases	Eliminates
Securing field sites, guest Wi-Fi, and on-premise server/workloads access to internet	North/South Firewalls, Routers

2 Secure Communications Within Locations

Leverages Device Segmentation (Airgap)

- Identify all devices within your site and place them in a "network of one" (i.e., "/32")
- Build policy for devices discovered using modern constructs and intuitive workflows

Top Use Cases	Eliminates
IoT/OT classification & segmentation	East/West Firewalls, NAC

3 Secure Communications Between Locations

Leverages ZPA and Branch Connector

- Replace site-to-site VPNs and routed overlays with zero trust connectivity
- Hosts an App Connector for Zero Trust access to the site's private apps & resources

Top Use Cases	Eliminates
Secure site-to-site and site-to-Data Center communications	MPLS, VPNs, Traditional SD-WAN, routing complexity, local compute

Key Use Cases for FedRAMP Environments

- **Rapid onboarding of new sites** including facility realignments, consolidations, and emergency standup even with overlapping IP ranges, using policy-brokered access rather than network adjacency.
- **IoT/OT segmentation and containment** for devices that cannot run agents, including legacy operating systems, sensors, cameras, and embedded platforms.
- **Site-to-data-center blast-radius reduction** by removing implicit trust and enforcing least-privilege communications between every field site and centralized resources.
- **Third-party and contractor remote access** without VPN sprawl or inbound exposure.
- **Secure internal and external communications**—users and headless devices accessing approved internet services and private mission applications through a single, unified policy framework.

Benefits

Reduced cyber risk. Reduce ransomware propagation pathways by limiting east–west movement inside sites and blocking site–to–core lateral pivots by default. Each site operates as an isolated security domain; a compromise at one location cannot traverse the network to reach others.

Lower cost and fewer boxes. Retire or reduce dependency on MPLS and private lines where appropriate. Reduce branch firewall and VPN sprawl. Avoid perpetual refresh cycles for hardware stacks that do not scale. Organizations can achieve up to 50% reduction in branch infrastructure costs.

Faster operations with a repeatable site blueprint. Define policy once and apply it consistently across all sites using template–driven deployment, rather than engineering and maintaining hundreds of site–specific firewall rules. Bring new sites online in days with only a high quality broadband connection.

Better mission performance. Remove avoidable network friction from mission–critical application workflows and site operations. Simplify access patterns for field personnel, improve reliability, and reduce the troubleshooting time caused by complex routing, NAT conflicts, and fragmented firewall ACLs.

Deployment and Operational Model

- **Physical or virtual form factors** to fit site constraints, including hypervisor–based edge deployments for environments where additional hardware is impractical.
- **High availability options** including active/standby configurations with VRRP and session synchronization for sites that require additional resiliency, plus WAN link failover and hitless software upgrades.
- **In–line enforcement plus passive discovery** so device identification and segmentation are practical at scale, even when agents are not possible and devices cannot be taken offline.
- **East–west control inside the site** using enforcement–point policy rather than assuming VLAN boundaries equal trust boundaries.
- **FedRAMP Moderate and High Authorized,** enabling deployment across the broadest range of public sector environments, including those handling controlled unclassified information and high–impact workloads.

Where Zero Trust Branch Applies

Zero Trust Branch for FedRAMP Environments is designed for any distributed public sector organization that needs to secure site connectivity, segment devices, and standardize security operations across many locations:

- Civilian agency field offices and regional centers
- FAA facilities and operational sites
- HS, CBP, and USCIS field locations
- Public health clinics and laboratories
- Higher education and research campuses
- Transportation and critical infrastructure operations centers
- Contractor and partner–connected environments

zscaler™ | **Act Fast. Stay Secure.**

About Zscaler

Zscaler enables organizations to move faster and be more secure by replacing network-based security with a true zero trust architecture. The Zscaler Zero Trust Exchange platform secures users, workloads, and devices by connecting them directly to approved applications and services based on identity, context, and policy — reducing attack surface and limiting lateral movement.

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.

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

zscaler.com