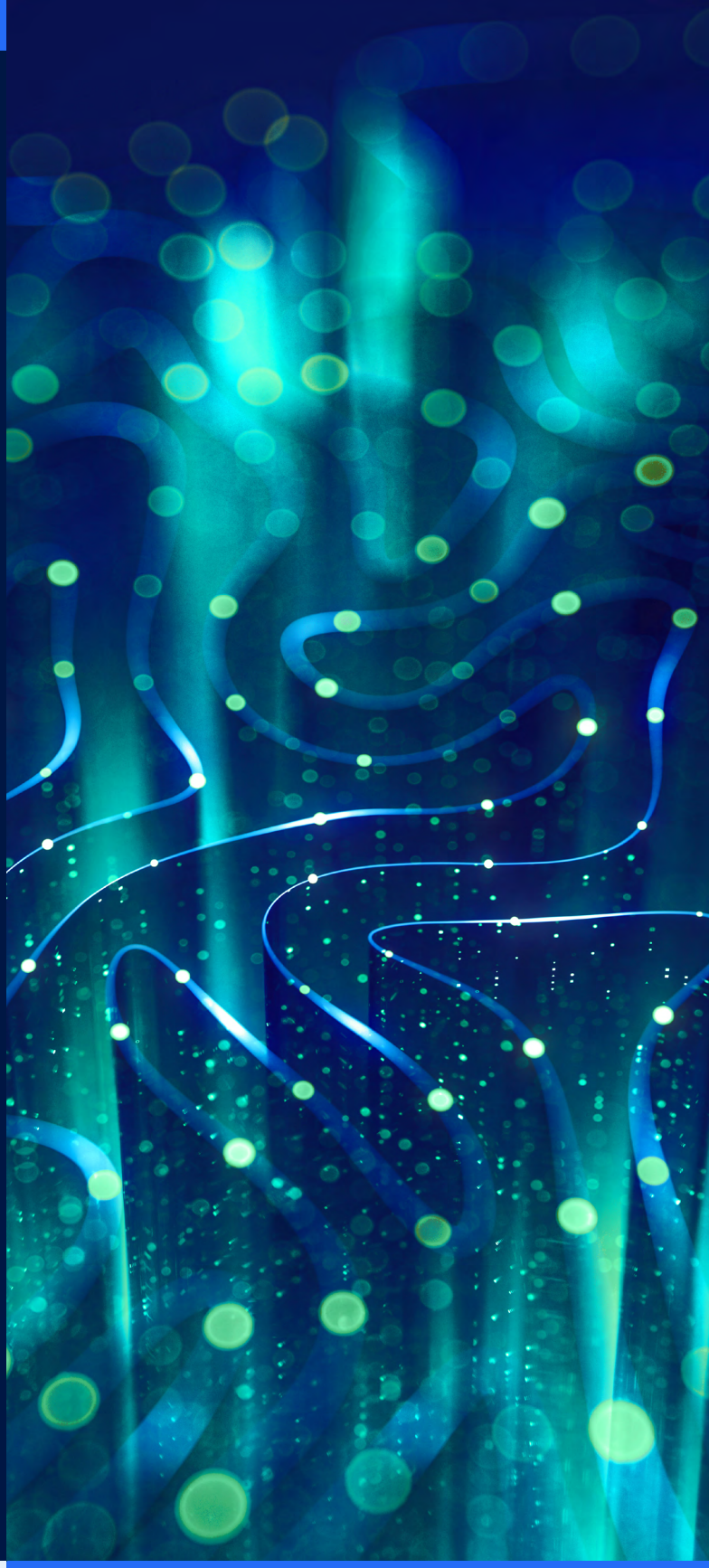
zscaler™

FedRAMP™

Extending zero trust to the branch, IoT and OT for TIC 3.0



©2026 Zscaler, Inc. All rights reserved.

WHITEPAPER

Executive Overview

Federal agencies are working to replace implicit trust with continuously verified access across the enterprise, consistent with the Federal Zero Trust strategy set out in OMB Memorandum M-22-09.[1] Many agencies, particularly those already using the Zscaler platform, have made significant progress securing user access to applications based on identity, security policy, and device posture rather than network location. The branch network, including the OT, IoT, and unmanaged devices connected to it, often remains an exception, relying on legacy constructs such as VLANs, VRFs, site-to-site VPNs, and per-site security infrastructure that continue to grant trust based on network location.

Zero Trust Branch (ZTB) extends zero trust principles to this remaining layer by removing direct site-to-site connectivity, isolating devices within the branch, and centralizing security policy through the Zero Trust Exchange. Rather than treating WAN modernization, branch segmentation, and security as separate initiatives, ZTB addresses them through a common architecture in which the network provides transport while access and security policy are centrally enforced. The sections below examine how this model secures communication between sites and within individual sites, supports OT and IoT environments, aligns with federal zero trust and TIC 3.0 guidance, and simplifies the infrastructure and operations required at each branch.

©2026 Zscaler, Inc. All rights reserved.

Current State

Agencies that have adopted Zscaler for user access have already retired the assumption that network location should determine trust. Application access is granted based on verified identity and device posture, not on which network segment a user happens to be connected to.

The branch network has generally not gone through the same transition. Connectivity between sites is typically still built on a mesh of site-to-site VPNs or an SD-WAN overlay, and segmentation within a site relies on VLANs and / or VRFs configured on a per site basis. OT systems, IoT devices, and unmanaged endpoints, including contractor laptops and guest devices, sit on this same infrastructure and inherit whatever trust is granted to the network segment they are plugged into.

The Problem

This gap creates risk in two directions at once. The first is lateral movement: a device on a shared VLAN can generally reach any other device on that VLAN without further verification. OMB Memorandum M-22-09 directs agencies to "meaningfully isolate environments"[1] so that a compromise of one system cannot spread to others, which is precisely the scenario this architecture leaves open.

The second is operational: every new site requires its own VLAN design, routing configuration, and firewall rule set, every policy change has to be replicated site by site, and the resulting rule sets become more brittle as exceptions accumulate over time.

These issues are frequently misdiagnosed as an SD-WAN problem, since the visible symptom is usually cost, performance, or reliability of the existing WAN. Framing it that way leads to a like-for-like SD-WAN replacement that resolves the visible symptom without touching the underlying architecture. The lateral movement risk and the operational overhead both remain exactly as they were.

The risk is also compounding faster than patch cycles can keep pace with. Verizon's 2026 Data Breach Investigations Report found that vulnerability exploitation has overtaken stolen credentials as the leading initial access vector for breaches, and that only 26 percent of CISA's known exploited vulnerabilities were fully remediated in 2025.[2] Removing a site's exposure to the public internet closes this path regardless of patch status, which is a more durable defense than attempting to patch faster than vulnerabilities are discovered.

©2026 Zscaler, Inc. All rights reserved.

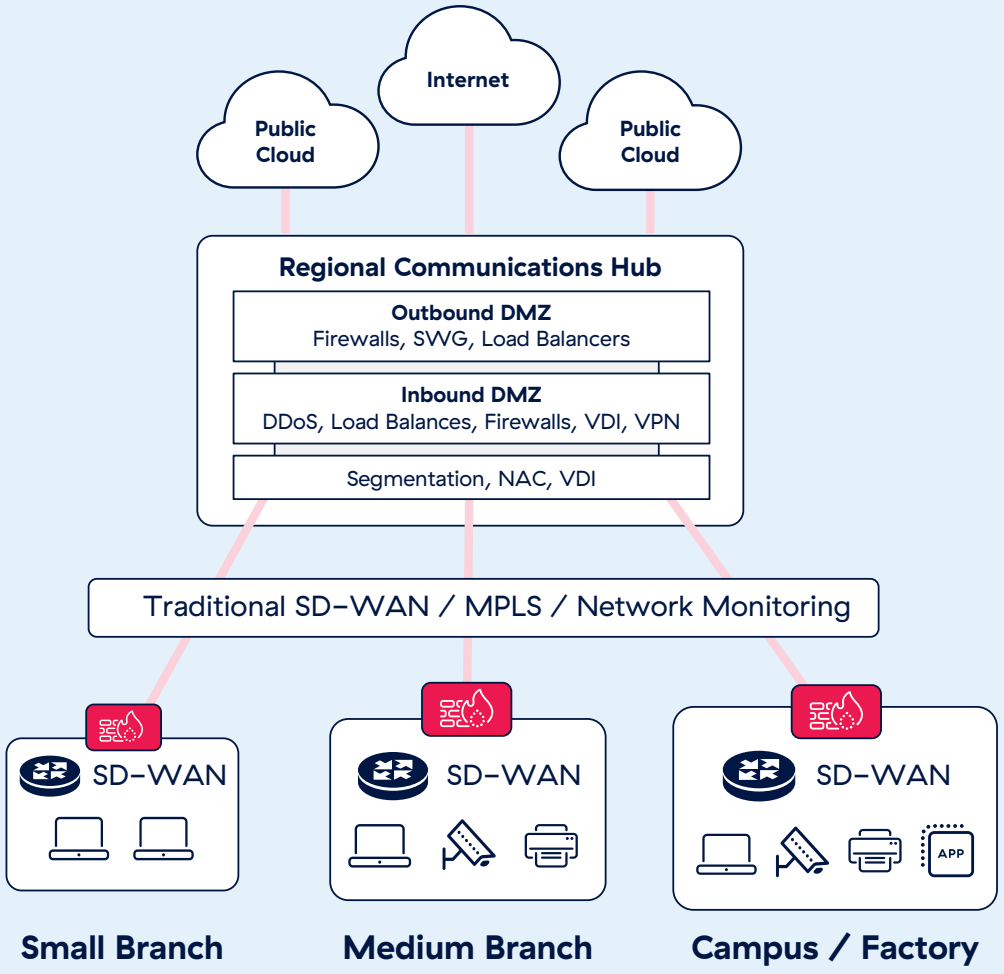


Figure 1. Legacy Branch Architecture *Shared SD-WAN / MPLS overlay and per-site firewall stacks grant implicit trust by network location, enabling lateral movement across sites and creating an attack surface that grows with every connected branch.*

The Zscaler Solution

Zero Trust Branch addresses this by changing what the network itself is responsible for. The physical network, whether broadband, 5G, or existing WAN links, becomes transport only. It moves packets, but it makes no decisions about trust. Every decision about who or what can reach a given resource is made and enforced by the Zero Trust Exchange, independent of the physical path the traffic happens to take. That separation, between the network as plumbing and the Zero Trust Exchange as the decision layer, is the basis for how ZTB handles external communication between sites, internal communication within a site, and how the platform differs from combining separate networking and security products under one vendor.

©2026 Zscaler, Inc. All rights reserved.

Securing External Communication: Replacing the WAN, Not Upgrading It

A traditional SD-WAN is still built around the same assumption as the architecture it replaced: that a defined set of sites should be able to reach each other, and that the WAN's job is to find the best path between them. Every site still needs to know about, and often route to, every other site's address space, and a site-to-site VPN mesh or overlay is doing the same job a private WAN link used to do, just over the internet. If one site is compromised, the overlay connecting it to every other site is exactly the path an attacker uses to reach them.

Zero Trust Branch does not attempt to make that overlay more secure. It removes the need for it. Each site connects only to the Zero Trust Exchange, not to other sites directly, so there is no mesh to compromise and no shared routing table for one site's addressing scheme to conflict with another's, which also removes the overlapping IP address problems that complicate mergers, acquisitions, and site consolidations. A user or device requesting something at another site, or in the cloud, is authenticated and authorized by the Zero Trust Exchange and connected only to that specific resource. Sites have no listener waiting for inbound connections and are not reachable from the public internet at all, which closes off the reconnaissance step that most external attacks depend on before an exploit can even be attempted.

Alignment with TIC 3.0

This architecture maps directly to the TIC 3.0 Branch Office Use Case. TIC 3.0 moves beyond the original requirement to route all traffic through a centralized TIC Access Point, introducing a trust zone model in which agencies position Policy Enforcement Points closer to the data and distributed across the environment rather than concentrated at a single chokepoint.[6] The Zero Trust Exchange serves this function: each branch's outbound traffic is inspected and policy-enforced at the cloud edge before reaching any destination, implementing the security capabilities TIC 3.0 requires at trust zone boundaries without requiring a physical TICAP at every location. Zero Trust Branch is authorized at FedRAMP Moderate and High. CISA's 2026 guidance on using SASE in a modern TIC 3.0 solution describes this architecture pattern explicitly, stating that it "aligns with TIC 3.0 and zero trust principles by moving away from perimeter-based security models toward distributed enforcement of access control and security policies across the enterprise."[7] Because ZTB eliminates direct site-to-site connectivity entirely, each branch operates as a cleanly bounded trust zone with no lateral path to adjacent sites — consistent with TIC 3.0's principle that the trust of a zone is designated independently of adjacent zones.

©2026 Zscaler, Inc. All rights reserved.

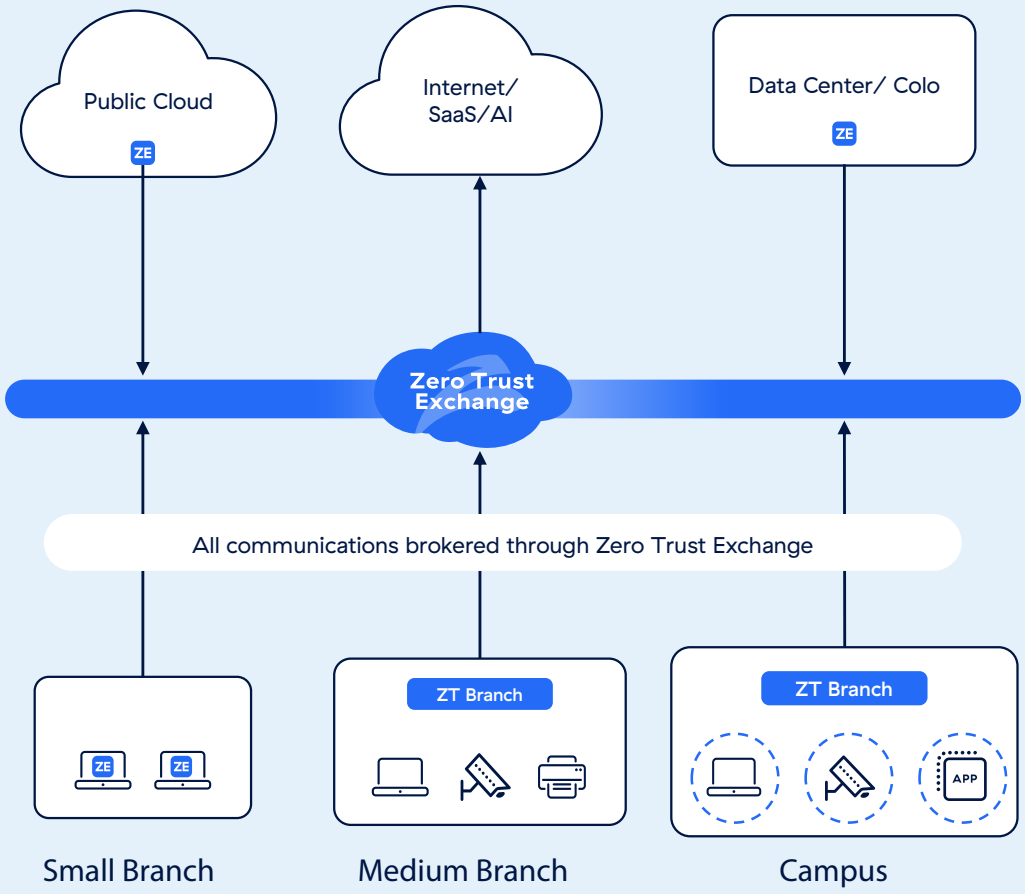


Figure 2 Zero Trust Branch: All Traffic Brokeredt *Instead of connecting sites to each other, every branch connects only to the Zero Trust Exchange, removing the shared overlay that lateral movement and ransomware depend on to spread between locations*

Securing Internal Communication: The Site Itself

Removing site–to–site exposure addresses one half of the problem. The other half is what happens once something is already inside a site, since a compromised badge reader or an unpatched sensor is still a threat even if it can no longer reach another location. Traditional LAN segmentation is what CISA's guidance on microsegmentation terms macrosegmentation: large, coarse grained zones that group devices for convenience of management rather than security.[3] Everything inside one of these zones can generally reach everything else inside it unless a separate layer of access control has been added on top, and those rules tend to degrade as exceptions accumulate.

©2026 Zscaler, Inc. All rights reserved.

ZTB's Network of ONE segmentation is a direct implementation of what that same guidance defines as microsegmentation: dividing a network down to the level of individual devices and enforcing policy based on identity and behavior rather than location.3 Every device connected to a site, including OT and IoT devices that cannot support an agent, is discovered automatically and placed into its own isolated segment. The same guidance notes that agent based approaches are typically unavailable for OT, IoT, and legacy devices, which is why network based segmentation is the necessary approach for this class of asset rather than simply the preferred one.3 Two devices on the same physical switch cannot communicate with each other unless that specific connection has been explicitly authorized.

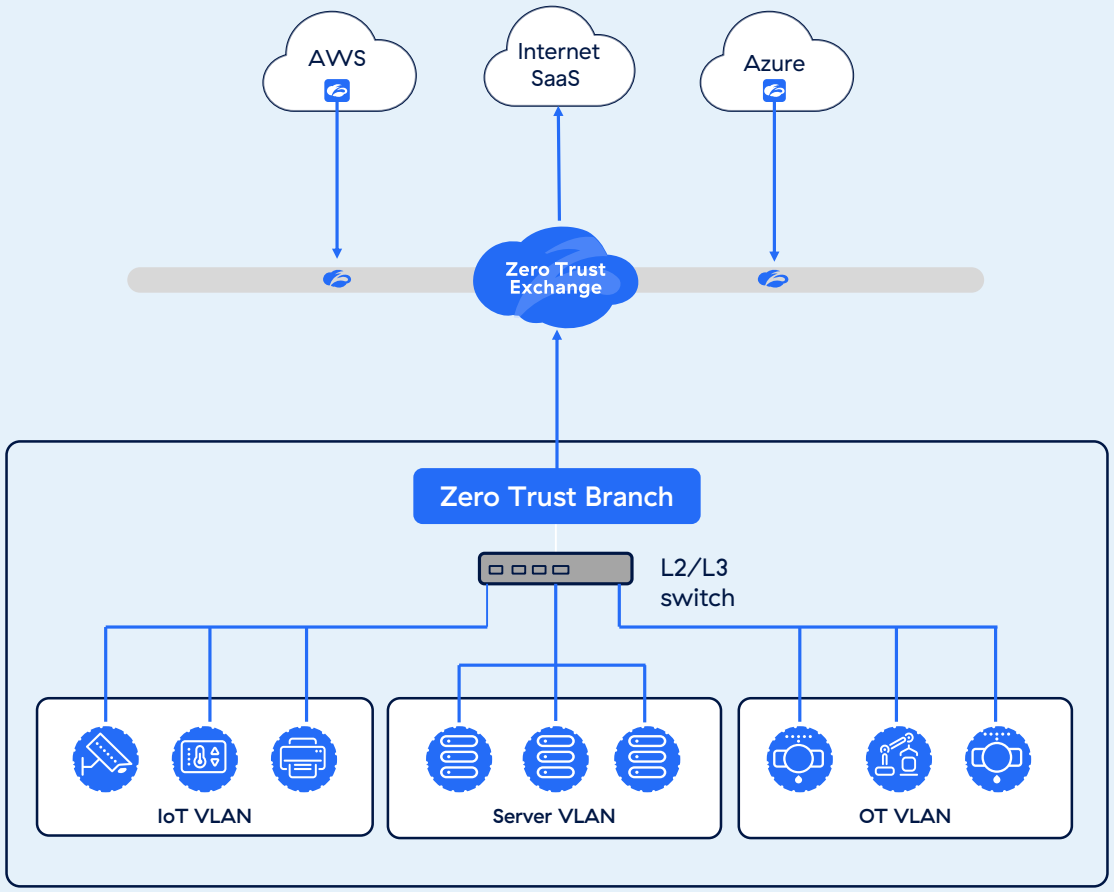


Figure 3. Network of ONE: Agentless Microsegmentation *Every device, including OT and IoT endpoints that cannot run an agent, is automatically discovered and isolated into its own segment via intelligent DHCP proxy, so that two devices on the same physical switch cannot communicate unless that connection has been explicitly authorized.*

©2026 Zscaler, Inc. All rights reserved.

This same architecture allows a site's security posture to be adjusted without taking the site offline, a capability Zscaler refers to as its Ransomware Kill Switch. Devices and users can be grouped and tagged by threat level, green, orange, yellow, or red, with policy defined for each level in advance. Federal guidance on applying zero trust to OT environments recommends treating segmentation this way, as a "dynamic, enforceable security policy"[4] rather than a one time architectural decision, so that posture can change as conditions change instead of being fixed at deployment. If a breach is suspected, the response is not limited to a choice between doing nothing and shutting the entire site down.

Ransomware Kill Switch Threat Level	Typical Policy Effect
Green (Normal)	All classified devices and verified users operate under standard policy.
Yellow (Elevated)	Guest Wi-Fi and unmanaged devices restricted to a minimal set of resources; verified users unaffected.
Orange (High)	Contractor and third party access suspended pending review; only verified, managed devices retain access.
Red (Critical)	Access limited to a defined set of mission critical users and systems until the incident is resolved.

A Single Vendor Architecture, Not SD-WAN Plus a Security Add-On

Zero Trust Branch is frequently compared to a SASE deployment, and it is worth being precise about the term. Gartner defines single-vendor SASE as networking and security capabilities, including SD-WAN, secure web gateway, cloud access security broker, and firewall as a service, delivered by one vendor as a unified platform rather than assembled from separate products connected through APIs. Most vendors presenting themselves as unified do not meet that bar in practice.

The distinction is not academic. In a multi-vendor deployment, traffic is often decrypted and inspected separately at each vendor's boundary, which adds latency and creates gaps where policy is inconsistent between the networking layer and the security layer. Zero Trust Branch avoids this by design: the branch appliance and the Zero Trust Exchange share the same policy engine already used for user traffic, so a device or site is not evaluated by one set of rules for connectivity and a different set of rules for security.

Typically in Place Today	Effect of Zero Trust Branch
SD-WAN edge appliance / site-to-site VPN mesh	Replaced; each site connects to resources brokered by the Zscaler Zero Trust Exchange
Internal segmentation firewall	Responsibility moves to Network of ONE — segmentation is enforced per-device without requiring dedicated hardware.
NAC appliance	Functionality absorbed into identity and device-based segmentation — NAC may be retained for visibility during transition
Next generation firewall at the branch	Inspection moves to the Zero Trust Exchange; branch hardware complexity is reduced

©2026 Zscaler, Inc. All rights reserved.

Zscaler IT's Results – Zero Trust Branch Deployment

Zscaler's own internal deployment of Zero Trust Branch decommissioned 20 firewalls across 10 sites, reduced its legacy security footprint by 99 percent, and realized cost savings of up to 43 percent.[5] The specific figures will vary in a larger or more legacy OT environment, but the underlying mechanism, isolating every device by default and removing site-to-site exposure, does not depend on scale.

Summary

Zero Trust Branch extends the zero trust model from users and applications to the branch network and the OT, IoT, and unmanaged devices connected to it. By removing direct site-to-site connectivity, isolating devices by default, and moving access and security decisions from the underlying network to centrally defined policy, ZTB addresses both external and internal lateral movement while reducing reliance on per-site routing, segmentation, and security infrastructure.

The result is a common architecture for security and network modernization rather than separate solutions for WAN connectivity, branch segmentation, and security. Security teams gain stronger isolation and reduced attack surface; network teams gain a simpler, centrally managed branch architecture; and agencies gain a more repeatable model for deploying, operating, and securing new, existing, temporary, or acquired locations. For executive leadership, these outcomes can be evaluated as a single modernization initiative: extending zero trust consistently across the enterprise while reducing the complexity required to operate and secure each site.

©2026 Zscaler, Inc. All rights reserved.

References

[1] Office of Management and Budget, M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[2] Verizon, 2026 Data Breach Investigations Report, May 2026. https://www.verizon.com/business/resources/reports/dbir/

[3] Cybersecurity and Infrastructure Security Agency, The Journey to Zero Trust: Microsegmentation in Zero Trust, Part One: Introduction and Planning, July 29, 2025. https://www.cisa.gov/sites/default/files/2025-07/ZT-Microsegmentation-Guidance-Part-One_508c.pdf

[4] Cybersecurity and Infrastructure Security Agency, Department of War, Department of Energy, Federal Bureau of Investigation, and Department of State, Adapting Zero Trust Principles to Operational Technology, April 29, 2026. https://www.cisa.gov/sites/default/files/2026-04/joint-guide-adapting-zero-trust-principles-to-operational-technology_508c.pdf

[5] Zscaler, Zscaler on Zscaler customer story. https://www.zscaler.com/customers/zscaler

[6] Cybersecurity and Infrastructure Security Agency, Trusted Internet Connections 3.0: Branch Office Use Case, Version 1.0, April 2021. https://www.cisa.gov/sites/default/files/2023-05/TIC%203.0%20Branch%20Office%20Use%20Case_508c_0.pdf

[7] Cybersecurity and Infrastructure Security Agency, The Journey to Zero Trust: Using Secure Access Service Edge in a Modern TIC 3.0 Solution, June 2026. https://www.cisa.gov/sites/default/files/2026-06/The_Journey_to_Zero_Trust_Using_SASE_in_a_Modern_TIC-3.0_Solution_CB_Approved_508c.pdf

zscaler™ | Act Fast. Stay Secure.

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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, Zscaler Digital Experience, and ZDX™, and other trademarks listed at **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.

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