



■ EBOOK

How Traditional SD-WANs Enable Ransomware Attacks—and How to Stop Them



Introduction

As security challenges continue to escalate, network architectures have not evolved to keep pace. According to the Zscaler ThreatLabz [2024 Ransomware Report](#), we saw larger ransom payouts than ever and a 58% year-over-year increase in the number of extorted companies. Ransomware spreads quickly through organizations for one simple reason: legacy networks implicitly trust everything connected to them, allowing ransomware to move freely from infected devices in remote branch offices to crown jewel applications.

In the past, organizations relied on a “castle and moat” security model, where all traffic within the network was considered safe by default, and security controls were enforced only at the perimeter. As they became more distributed and cloud-centric, organizations simply extended their private networks into branches and clouds using software-defined wide area networks (SD-WAN) and site-to-site VPNs. This created large, flat trusted networks where attackers can move laterally, despite the multitude of firewalls deployed everywhere.

Meanwhile, networks include an ever-growing number of IoT devices. It is estimated that 55.7 billion of these devices will be connected to enterprise networks by 2025, generating 80 billion zettabytes of data each year.¹ This expansion of the edge creates a larger and larger attack surface, making organizations more vulnerable. All these trends make perimeter-based approaches to security increasingly untenable. As a result, year after year, the number—and cost—of data breaches continues to increase and ransomware activity continues to escalate.

To protect their infrastructure against these mounting threats, organizations across industries are increasingly turning to a zero trust approach to cybersecurity.



17.8% increase in ransomware attacks from 2023 to 2024.²



\$75 million record-breaking ransomware attack payout reported in 2024.²



104% increase in the number of data breach victims from 2023 to 2024.³



The global average cost of a data breach reached an all-time high of **\$4.88 million** in 2024.⁴

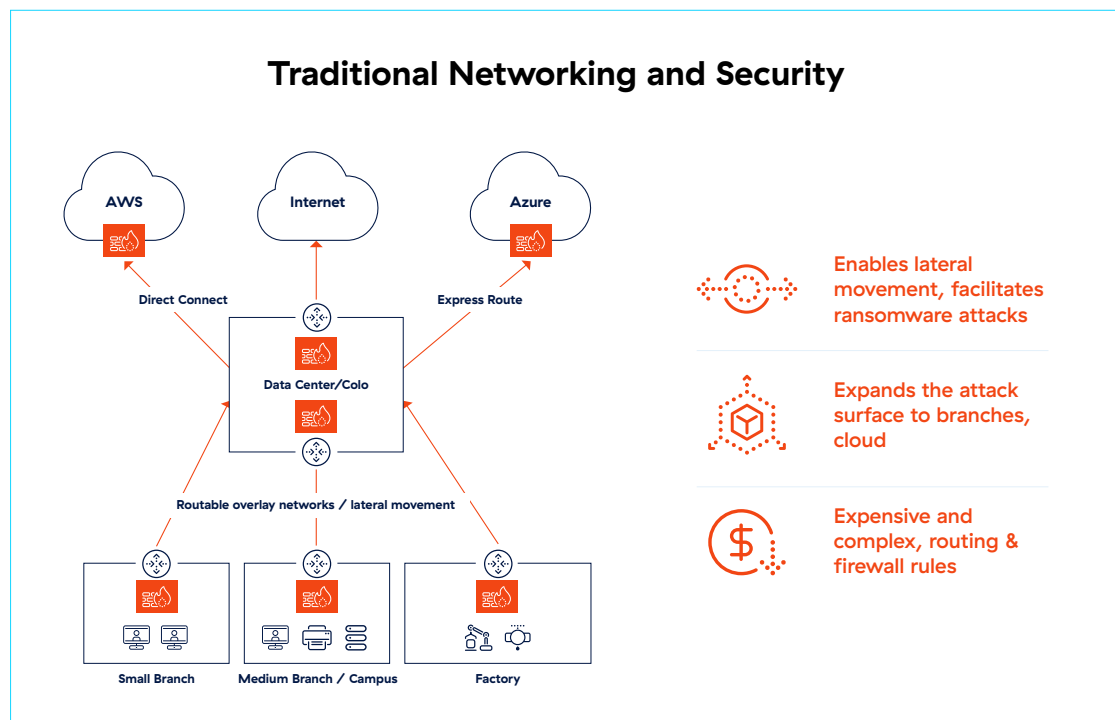
1: IDC Research, [Future of Industry Ecosystems: Shared Data and Insights](#), 2021.
2: Zscaler ThreatLabz [2024 Ransomware Report](#).

3: Identity Theft Resource Center, [H1 2024 Data Breach Analysis](#).
4: IBM, [Cost of a Data Breach Report 2024](#).

What Traditional SD-WAN Is and Isn't?

SD-WAN leverages automation to steer network traffic to the most efficient path across various network transport services and infrastructures. Application-aware routing protocols improve application performance by prioritizing traffic between critical apps.

Traditional SD-WAN solutions simply extend the organization network to branch locations and data centers. Designed to simplify connectivity, SD-WAN enables devices everywhere—including branches, factories, and third-party sites—to communicate with apps in the data center or public cloud. Comprising a mesh of appliances and site-to-site VPNs, these architectures offer little to no protection against lateral threat movement and ransomware.





SD-WAN was designed to improve connectivity, making it faster and easier for users to access resources. But connectivity does not equal security. In fact, when connectivity is achieved through trust-by-default, it's at odds with the zero trust model. Zero trust instead requires that identity and security posture be verified before connectivity is allowed. The implicit trust built into legacy networks only makes them harder to secure and facilitates the quick spread of ransomware.

What Is Zero Trust?

Zero trust is a security strategy that asserts that no entity—user, app, service, or device—should be trusted by default. Following the principle of least-privileged access, before any connection is allowed, trust is established based on the entity's context and security posture, and then continually reassessed for every new connection, even if the entity was authenticated before.

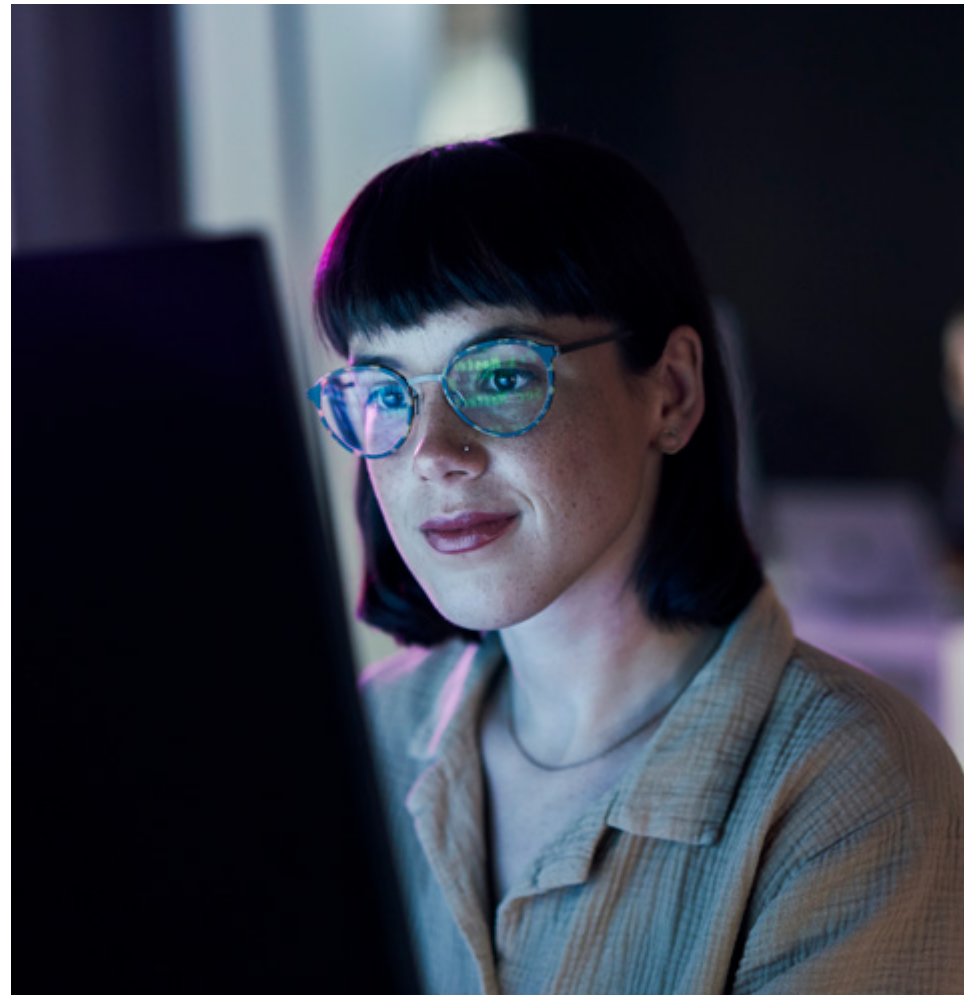
To achieve zero trust across a traditional SD-WAN, an organization needs to layer on additional security appliances, tools, and policy enforcement points. The result is a patchwork of firewalls, mesh VPNs, and other tools such as network access control (NAC), DNS security solutions, etc. This architecture is complex, consuming excessive budget and personnel resources to manage.

Starting with Zero Trust

Starting with an open, flat network and adding enforcement points and security controls to achieve zero trust is operationally complex and expensive. Network segmentation projects often run into months or even years, and requirements often change before these projects finish. What if you could start the other way around? What if your branches could be like cafés, with no routable network connecting them to organization applications in the cloud?

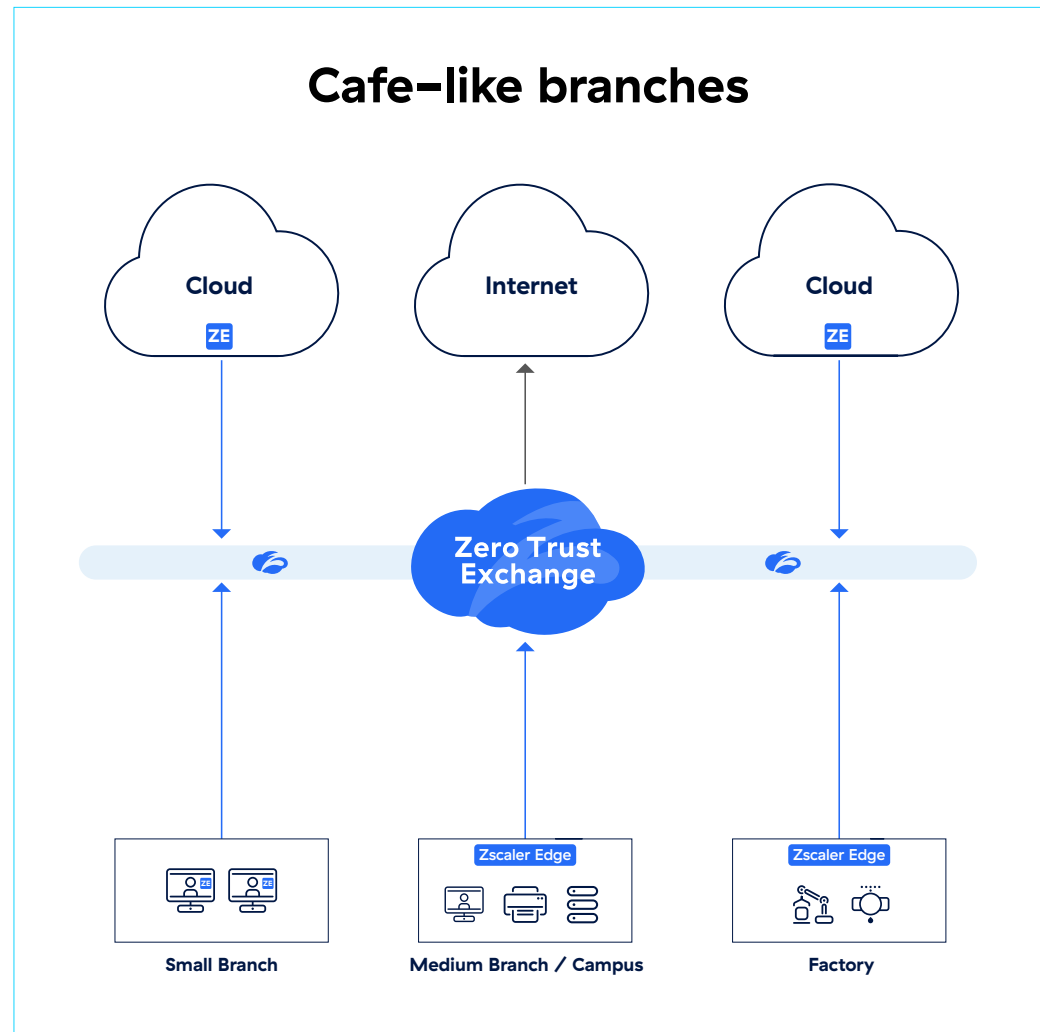
Zero Trust SD-WAN is a new way to provide branches and data centers with fast, reliable access to the internet, private applications, and cloud services without extending the network everywhere. It connects users and devices to applications based on policy, not network presence, providing both robust security and operational simplicity.

This is native zero trust approach it makes lateral movement impossible, since users and devices (including internet of things (IoT) and operational technology (OT) devices) are never directly connected to applications. Instead, they communicate via the Zscaler Zero Trust Exchange™ platform, which facilitates full cyberthreat and data protection with robust identity and context-based access controls.



This zero trust approach:

- **Improves application performance.** Enterprises can replace complex site-to-site VPNs with a simple direct-to-cloud architecture that delivers fast, consistent performance to support productivity.
- **Minimizes the internet attack surface.** Legacy WAN solutions expose VPN ports to the public internet, leaving the network vulnerable to attacks. With Zero Trust SD-WAN, private applications sit behind the Zero Trust Exchange, where they can't be discovered or attacked from the internet.
- **Prevents lateral threat movement.** Site-to-site VPNs create a large routable network where a malware infection can be transmitted from a single device to everything on the network. With Zero Trust SD-WAN, connections are made directly to applications, not the network. This makes lateral movement impossible.
- **Reduces cost and complexity.** This approach eliminates the need for multiple firewalls, VPNs, NAC, and other layered solutions. The result is an architecture that's simpler, less expensive, and far easier to configure and maintain.



Zscaler Solves Traditional SD-WAN's Challenges

By relying on the Zero Trust Exchange to securely connect branches, factories, and data centers, Zscaler ensures uniform, consistent zero trust access for all users, IoT/OT devices, and applications.

	Zero Trust SD-WAN	Traditional SD-WAN
Reduces attack surface and stops lateral threat movement	Yes	No
Reduces firewall and ACL rule complexity	Yes	No
Eliminates tradeoffs between security and performance	Yes	No
Eliminates the need for firewalls at the branch	Yes	No

Zscaler Zero Trust SD-WAN is flexible enough to support multiple deployment options that do not require a full replacement. It can work alongside your existing branch SD-WAN infrastructure and build zero trust overlays to the Zero Trust Exchange. This will ensure secure, performant access from your branch devices to private applications at other sites and in the cloud without allowing lateral threat movement.

If you are taking a fresh approach to your organization's connectivity needs, start with a native zero trust architecture that reduces complexity and eliminates the need for additional firewalls everywhere. Zscaler Zero Trust SD-WAN can manage your ISP connections and intelligently steer application traffic to deliver a secure, café-like branch experience to your users while keeping your organization safe from ransomware attacks.

Stop ransomware attacks with zero trust

Zero trust is critical for meeting today's security challenges—and reducing your risk from ransomware attacks. With Zscaler Zero Trust SD-WAN, your organization can secure all communications and eliminate the possibility of lateral threat movement without the cost and operational complexity of legacy approaches. Plus, exceptional digital experiences will keep customers, employees, and other end users productive and satisfied.



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. To learn more, visit www.zscaler.com.

© 2024 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/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.