zscaler™

EBook

4 Requirements for a Zero Trust Branch

By implementing a zero trust approach at the branch, enterprises can not only fortify their networks against threats, but also streamline connectivity for users, devices, and applications across diverse locations.

In today's dynamic business landscape, many enterprises face challenges in ensuring the security of their users, devices, and applications. In the past, when applications resided within data centers and users primarily connected from office locations, the requirements for connectivity were relatively straightforward. Traditional hub-and-spoke and firewall-based architectures were effective in meeting those needs. However, as the modern work environment has evolved, these traditional approaches now struggle to provide adequate protection against threats and an optimal user experience.

Today, users no longer connect exclusively from their office spaces, but from a plethora of locations, including their homes, coffee shops, airports, and more. Additionally, the proliferation of the internet of things (IoT) further complicates the enterprise security landscape, as IoT/OT devices pose additional security risk.

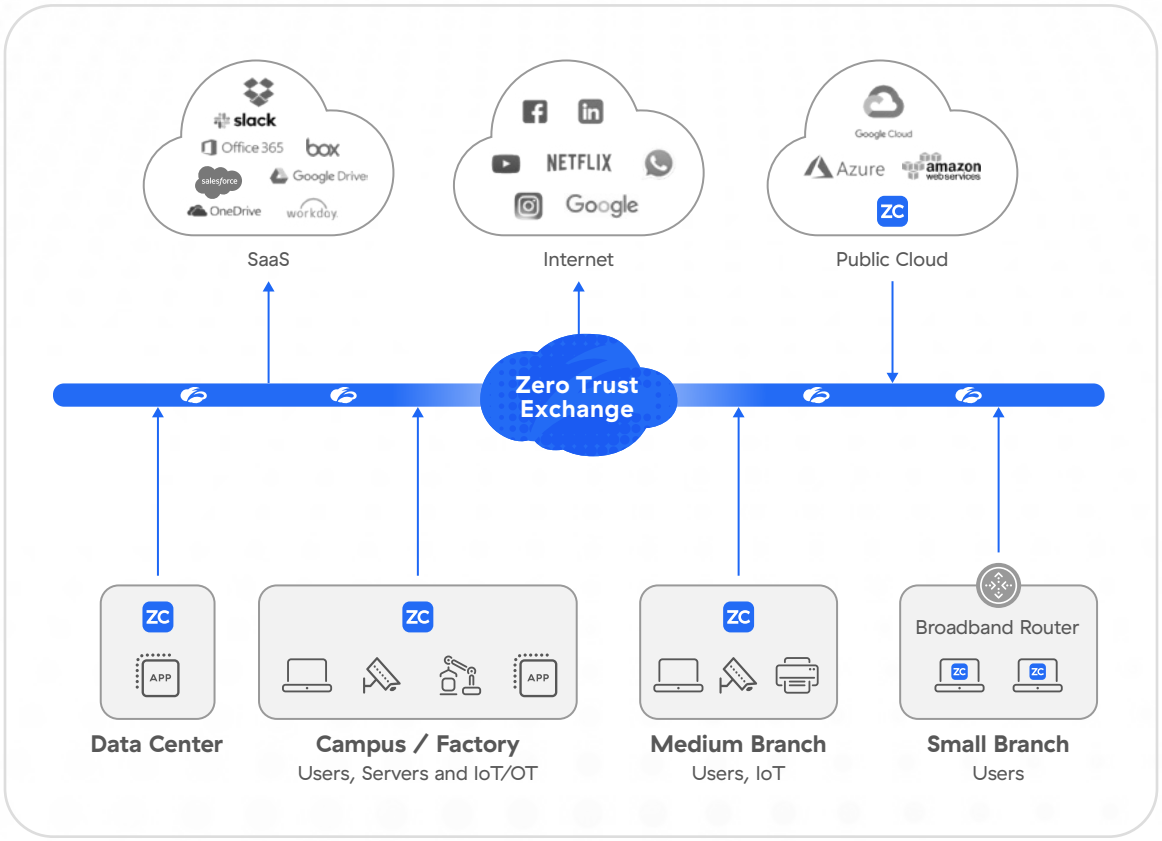

Figure 1: Zero Trust Branch offers a zero trust approach to network connectivity

The changing landscape is driving organizations toward a zero trust approach to security. The principles of zero trust—never trust, always verify, and enforce least privileged access—has enabled many enterprises to thwart sophisticated cyberattacks. With zero trust, users are granted access only to applications they need, unlike VPNs which put users on the network and give unrestricted access. By applying zero trust principles to network connectivity, organizations can better protect themselves against threats, especially ones originating in the locations. Implementing zero trust approach at the branch ensures secure connectivity and simplified operations, overcoming routing complexities or a degraded user experience while eliminating attack surface and preventing lateral threat movement.

A zero trust branch architecture ensures improved security for all locations, including branches, factories, kiosks, and data centers. Here are four key requirements for ensuring a zero trust branch:

Ensure zero trust principles for your network 1

Secure IoT/OT devices in your branch locations 2

Ensure direct-to-cloud paths for SaaS/internet traffic 3

Ensure consistent user experience for in-office & remote employees 4

Traditional SD-WAN is Not Zero Trust

Traditional SD-WAN appliances simply extend the corporate network out to remote branch locations, expanding the enterprise attack surface. They offer poor protection against lateral threat movement, enabling compromised devices in remote locations to easily communicate with business-critical apps in the data center or public cloud. Enterprises experience greater risk of lateral threats and internet-based attacks from using legacy SD-WAN. A patchwork of security appliances, tools, and non-standard policies lead to increased security risk due to known and unknown gaps in security coverage. Therefore, when architecting secure branch connectivity, it becomes imperative to focus on implementing zero trust to reduce the attack surface and prevent the lateral movement of threats.

A 2023 VPN Risk Report by Cybersecurity Insiders that surveyed 382 IT professionals and cybersecurity experts found that VPNs pose security risks, with 88% of organizations expressing a slight to extreme concern that VPNs may jeopardize the security of their organization.

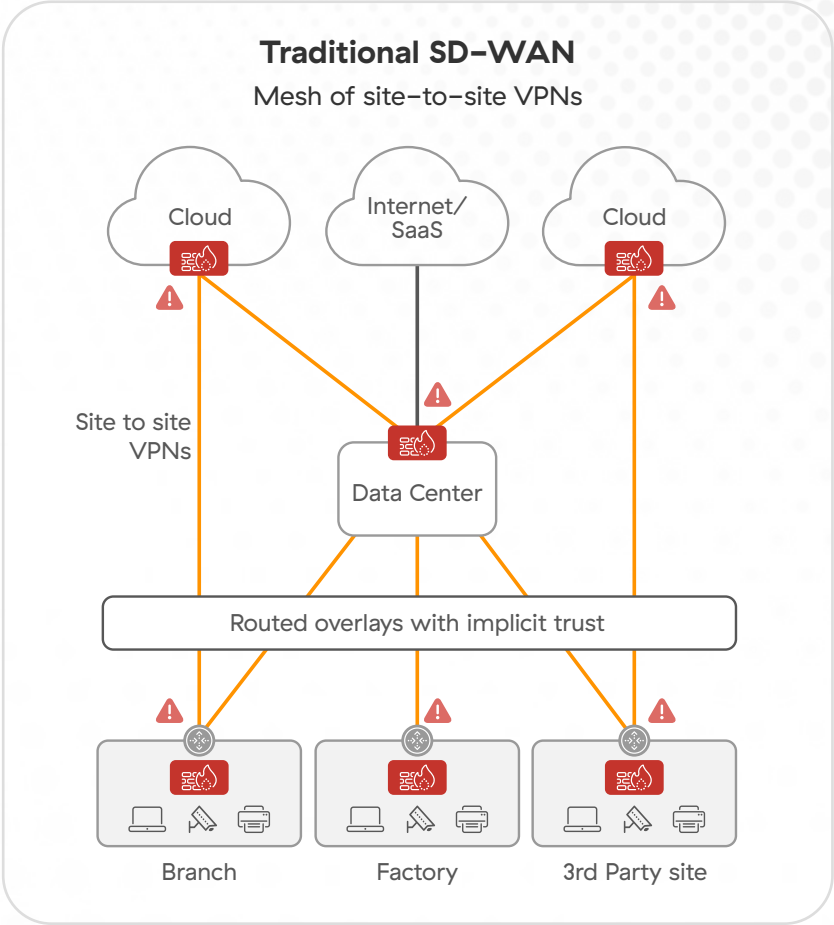

Figure 2: Traditional SD-WANs expand attack surface and do not protect against lateral threat movement.

Furthermore, 45% of organizations confirmed they'd experienced at least one attack that exploited VPN vulnerabilities in the last 12 months—one in three became victims of VPN-related ransomware attacks. The increasing threat of cyberattacks exploiting VPN related vulnerabilities underscores the urgent need to address the security of current architectures.

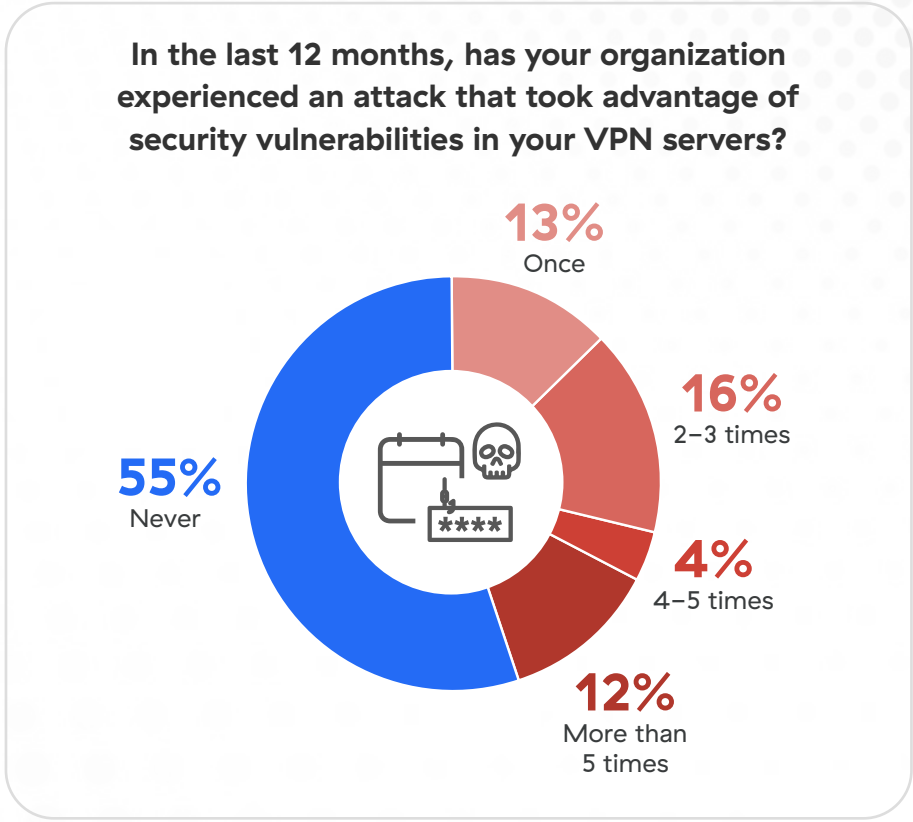

Figure 3: Organizations are experiencing increased cyberattacks due to vulnerabilities in VPN servers.

You Can't Build Zero Trust with Firewalls and VPNs

Traditionally, enterprises deployed site-to-site VPNs to ensure connectivity to critical applications hosted within the data center. However, as these applications migrate to the cloud, the conventional site-to-site VPN architecture becomes less viable since traffic is still backhauled to the data center, resulting in a degraded user experience and performance issues. It also introduces operational complexity, as VPN tunnels require site management and setup on an individual basis. Consequently, enterprise IT teams want to transition from a hub-and-spoke network to a direct-to-cloud architecture that sends application traffic to a cloud security provider, improving application performance.

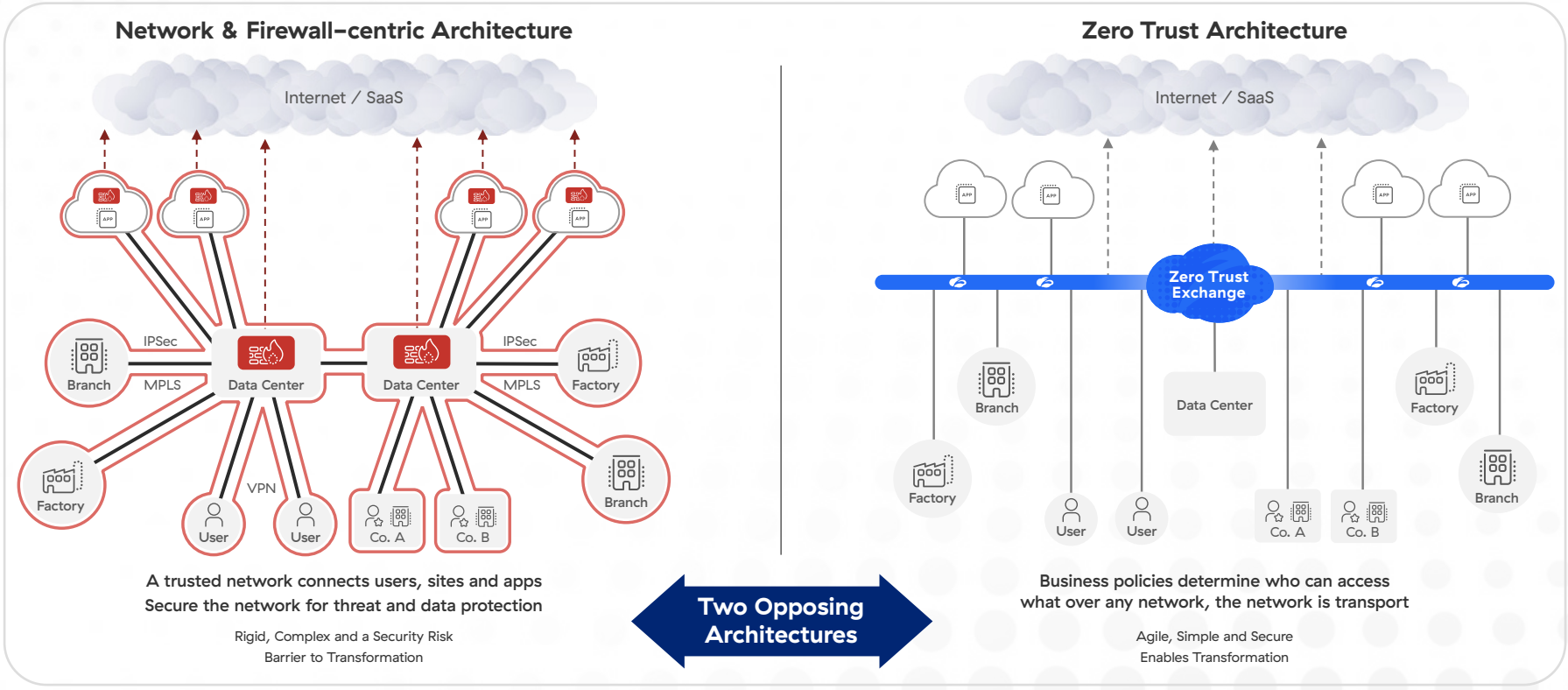

Figure 4: Organizations are experiencing increased cyberattacks due to vulnerabilities in VPN servers.

Four Key Requirements for Ensuring a Zero Trust Branch

1 Ensure Zero Trust Principles for Your Network

Site-to-site VPNs extend your corporate network to branches, data centers, cloud regions, and third parties. Traditional networks expand your attack surface to entities beyond your direct control and allow traffic flows implicitly, enabling lateral threat movement. Unlike traditional network segmentation, which splits the network into zones and is complex to manage, user-to-app and device-to-app segmentation provides granular, contextual access only when authorized. A network foundation grounded in zero trust principles eliminates the inherent risks in traditional flat networks and helps you avoid the complexity of layering on firewalls for security controls.experience and performance issues. It also introduces operational complexity, as VPN tunnels require site management and setup on an individual basis. Consequently, enterprise IT teams want to transition from a hub-and-spoke network to a direct-to-cloud architecture that sends application traffic to a cloud security provider, improving application performance.

2 Secure IoT/OT Devices In Your Branches, or Branch Locations

IoT/OT devices are proliferating in just about every organization with the rise of "smart" things such as printers, TVs, cameras, card readers, and sensors. These devices run a myriad of operating systems with varying security risks, and patch management remains a challenge as such. Many IT leaders have no visibility into these devices, let alone a detailed inventory, yet, these devices often have unrestricted access to your crown jewel applications in your data centers and cloud services. With IoT malware-based attacks increasing by 400%[1], this represents a significant threat vector for your organization. Organizations must secure IoT/OT devices in branches or factories to protect their business operations.

IoT and OT-based malware attacks have increased by 400% since 2022, representing a significant threat vector.

3 Ensure Direct-to-Cloud Paths for SaaS and Internet Traffic

Direct-to-cloud architecture quickly connects any user or IoT/OT device to any application, wherever that user or IoT/OT device is in the world. Implementing direct-to-cloud paths for SaaS and internet traffic is crucial for optimizing network performance and ensuring seamless connectivity. Hub-and-spoke architectures that backhaul traffic to a data center over expensive MPLS links degrade application performance and hinder business productivity. When applications lived in the data center, it made sense to backhaul application traffic to a regional hub. However, with the applications moving to the cloud, sending user or IoT/OT device traffic directly to its destination makes the most sense. A direct-to-cloud architecture allows SaaS applications and internet traffic to take the most efficient and direct routes to their destinations. This has many benefits, including cost savings, enhanced user experience, and network simplification.

Today, business leaders want a cafe-like experience for their users and IT teams that makes connecting to business apps as straightforward as possible while delivering superior application performance.

4 Ensure Consistent User Experiences for In-Office and Remote Employees

Many employees work remotely, or they divide their time between working from home and at the office. This shift in work dynamics has brought to light a significant challenge. Namely, users frequently express dissatisfaction with the quality of connectivity at the office compared to their home working environment. This situation introduces a fresh set of concerns for IT teams to address. VPN technologies that backhaul traffic to a data center result in poor and inconsistent user experience, which negatively impacts business and decreases productivity.

Today, business leaders want a café-like experience for their users and IT teams that makes connecting to business apps as straightforward as possible while delivering superior application performance. They want an experience where business users can access the apps they need with uniform consistency of experience between home and the office with the same ease of use, which is impossible when connecting to networks through VPNs. To stay relevant in today's competitive world, organizations must ensure consistent user experiences for in-office and remote employees to boost employee productivity and drive creativity.

Please provide callout text

Applying Zero Trust Principles to SASE

Secure Access Service Edge (SASE) integrates networking and security services into a unified, cloud-delivered solution, streamlining operations, reducing complexity, and enabling organizations to enforce consistent policies across their networks. SASE combines zero trust networking with essential cloud-delivered security services like SWG, CASB, FWaaS, and ZTNA. It's crucial to recognize that SASE solutions built on traditional SD-WAN offer inadequate protection, increasing the enterprise attack surface and exposing critical applications to diverse internet threats.

Moreover, the segmentation capability in traditional SD-WAN is fragmented and coarse, which allows threats to spread easily to other systems, posing a risk of bringing down entire sites or networks.

TechTarget's Enterprise Strategy Group (ESG) surveyed 390 IT and cybersecurity professionals at various organizations in North America (US and Canada) to understand the state of SASE. According to this study, top three use cases driving organizations towards SASE are:

1. Aligning network and security policies
2. Reducing or eliminating the internet attack surface
3. Improving remote user security

All three SASE use cases highlight the significance of providing secure connectivity for users, devices, and applications in establishing a resilient SASE framework. Organizations embarking on SASE implementation must prioritize solutions that adhere to zero trust principles. Traditional SD-WANs connect various sites through site-to-site VPNs or routed overlays, establishing an implicit trust that grants unrestricted access to critical business resources, even for compromised entities. On the other hand, SD-WANs built on zero trust principles effectively reduce the attack surface and safeguard against lateral threat movement while facilitating secure user-to-app, device-to-app, and app-to-app communication.

Figure 5: Organizations are experiencing increased cyberattacks due to vulnerabilities in VPN servers.

Conclusion

Traditional branch network architectures rely on implicit trust, expanding the attack surface to the furthest branch location and allowing cyberthreats to move laterally throughout the organization. By adopting a zero trust approach at the branch, enterprises can fortify their networks against threats and streamline connectivity for users, IoT/OT devices, and applications across diverse locations. Designing a branch network with zero trust principles improves enterprise security posture by eliminating the attack surface and preventing lateral threat movement while overcoming routing complexities. It's important for organizations to carefully consider the four requirements outlined here when implementing zero trust principles at the branch to effectively navigate the complex and ever-changing demands of security and network connectivity.

References:

1. zscaler.com/press/zscaler-threatlabz-finds-400-increase-iot-and-ot-malware-attacks-year-over-year-underscoring
2. info.zscaler.com/2023-vpn-risk-report
3. zscaler.com/resources/industry-reports/esg-sse-leads-the-way-to-sase.pdf

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 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**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com