zscaler™

EBook

Architecting Enterprise Networks for the Next Decade

EBook

Contents

Introduction

Enterprise network design is currently at a crossroads: should architects continue to follow the well-worn path that they've taken for years, providing connectivity via routable networks? Or should they reimagine what's needed for fast, secure communication between users, devices, and workloads, especially given that everything is distributed, and more data is being generated and exchanged, faster than ever before? Is it time to move beyond the costs and complexities associated with yesterday's infrastructure solutions, and instead find a better approach to secure connectivity—one that supports productivity in a fast-paced world?

Within the past few years, the fundamental requirements for networking have changed. Network teams are now challenged to provide hybrid workers with access to Software-as-a-Service (SaaS) applications as well as private apps. They're also tasked with maintaining workload-to-workload communications between the cloud and private applications as well as from cloud to cloud. And they must secure communications among ever-growing fleets of Internet of Things (IoT) and operational technology (OT) devices. When organizations try to meet these new requirements using outdated infrastructures, costs and operational complexities mount. Add the fact that reliability and security are paramount, and you've got a delicate balancing act on your hands.

Even though this revolution is now well underway, far too many organizations still rely on legacy architectures to try to keep their employees productive, their networks performant, and their technology assets protected. Many invested in tools like virtual private networks (VPNs) and wide-area networks (WANs) more than two decades ago, but they've since become outdated and obsolete. In today's world of smart devices, always-on communications, and borderless IT ecosystems, it's essential to adopt a new approach.

Greater efficiencies are also a must-have. Networking teams need to do more with less, given the persistence of skills shortages across this industry, as well as the present-day reality of budget constraints. Rearchitected networks should incorporate time- and labor-saving innovations like artificial intelligence (AI) that will empower network engineering and operations teams to achieve success faster by reducing manual effort and allowing professionals to focus on the highest-value tasks.

The result is that organizations are experiencing new challenges.

52%

of Americans with remote-capable jobs are now working on a hybrid basis.[1]

56%

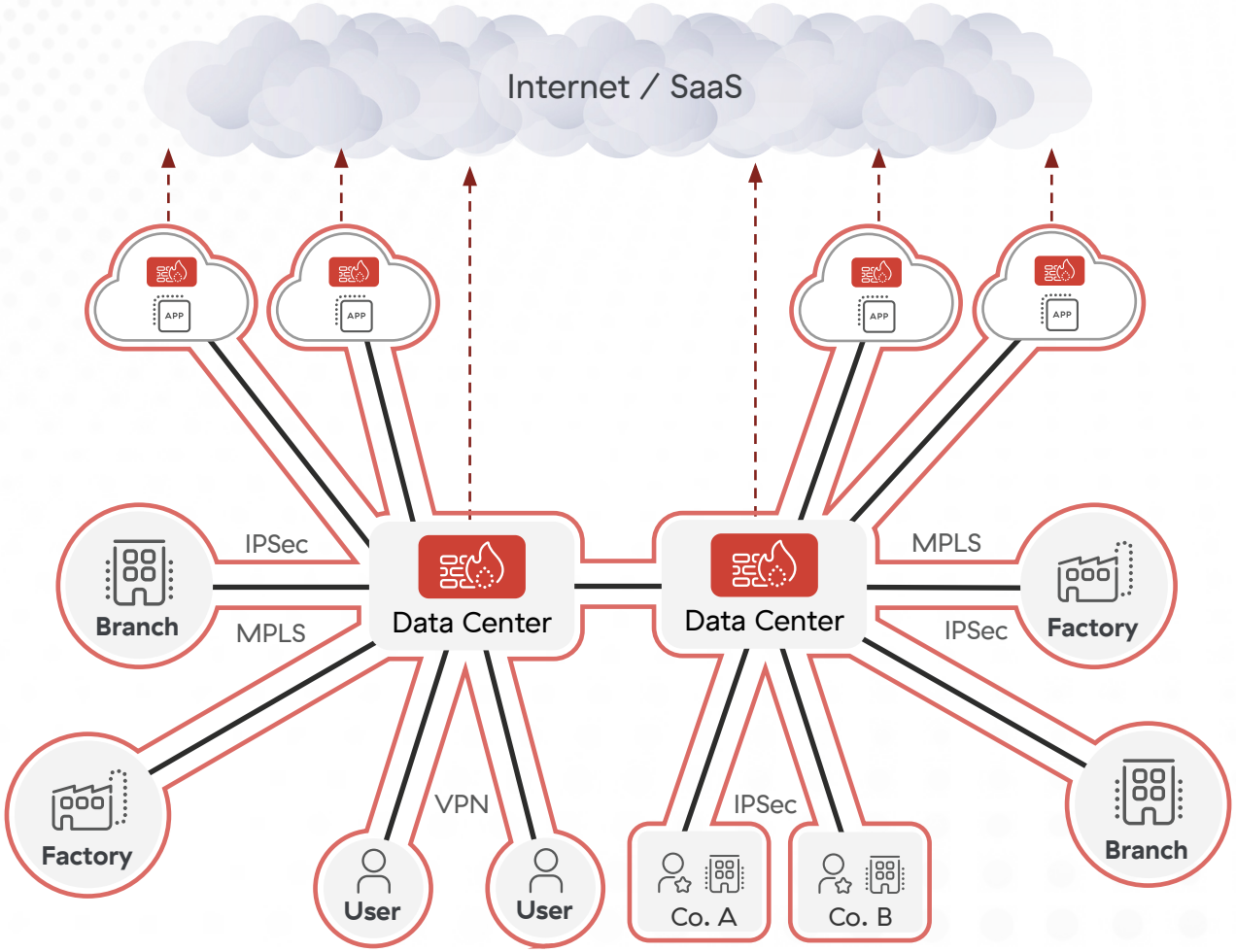
of employees would prefer hybrid or remote options for their future work.[2]

70%

of organizations are bringing cloud workloads back on premises due to security concerns.[3]

1. "Global Indicator: Hybrid Work," *Gallup*, October 2023.
2. *Connected Consumer Survey 2023*, Deloitte, 2023.
3. *Cloud Computing Study 2023: The balancing act of cloud expansion*, IDG Research, 2023.

Network & Firewall–centric Architecture



Legacy Architectures Pose Growing Challenges

#1: Increases in threat actor activity and cyber risk

The number of cyberthreats reaching enterprise networks from the open internet has grown since the start of the pandemic, when organizations began relying heavily on traditional remote access solutions such as VPNs to provide application access to their newly-remote workforces. Within the past year, nearly half of organizations (45%) have experienced one or more attacks on their VPN servers that exploited vulnerabilities in their VPN software.[4] Threat researchers have also observed a surge in IoT malware attacks, which are up 400% since last year.[5]

#2: Rising costs associated with management complexity

WAN infrastructures typically have hub-and-spoke architectures that were not designed to support modern cloud-centric enterprises with hybrid workforces. This is an inflexible approach, involving multi-year contracts and long lead times. It's not compatible with business agility. While adopting SD-WAN can lower bandwidth costs and reduce management overhead, it fails to provide adequate security, and requires additional firewall infrastructure at branch locations. As a result, today's decision-makers often find their organizations' networking and security needs are growing faster than their budgets.

#3: Performance issues

Legacy firewall- and VPN-based network designs require that all traffic be backhauled to a central choke point for inspection. This is inherently inefficient, forcing end users' traffic to travel an indirect, lengthy path between their devices and the cloud apps they're connecting to. It leads to excessive bandwidth consumption, elevated costs, and poor user experience. This often manifests itself as growth in the number of support tickets. In fact, service desk teams have seen a 35% increase in support ticket volumes since 2020,[6] when the pandemic forced organizations to adopt remote work on the fly, without making investments in remote-ready security and networking solutions beforehand.

In the past year 45% of organizations have experienced cyberattacks exploiting vulnerabilities in their VPN software.[4]

4. *2023 VPN Risk Report*, Cybersecurity Insiders, 2023.
5. *Zscaler ThreatLabz 2023 Enterprise IoT and OT Threat Report*, Zscaler, 2023.
6. Helpdesk meltdown due to absenteeism, low morale and increased workload," *Computer Weekly*, February 2021.

#4: Out-of-the-box solutions aren't scalable

Organizations continue to move to the public cloud. They are migrating existing workloads and building new mission-critical workloads there. Scalability is one of the main reasons for this shift, but legacy network architectures fall far short when it comes to supporting scalability. Cloud-based workloads are in constant communication with the internet, SaaS applications, and other workloads hosted in other cloud regions or in other public clouds. Businesses' operations depend on these workloads. If they run slowly—or go down—so does the business. Thus, preventing cyberattacks and lateral threat movement is imperative.

Additionally, out-of-box solutions are a poor match for today's cloud environments. Whether organizations rely on native tools supplied by their public cloud provider or another vendor's solution, their network teams will need to create unique deployments specific to every cloud environment. This approach is largely untenable in a multi-cloud world. With 98% of today's enterprises using at least two cloud providers' infrastructure, and 31% using four or more, very few organizations can take advantage of this approach efficiently.[7] And, of course, it cannot scale as the business's cloud footprint grows.

#5: Labyrinthian network paths make troubleshooting cumbersome

With employee productivity dependent upon reliable access to SaaS apps, it's critical that network operations teams be able to diagnose issues' root causes quickly and reliably. This is all but impossible in a world where visibility into home WiFi networks, last-mile internet service providers (ISPs), applications in the cloud, and private applications is lacking. As a result, support ticket volumes are skyrocketing, with excessive escalations increasing the burden on network engineering teams.

Today's network architects and engineering teams find themselves under immense pressure to optimize network paths for both security and performance. On the one hand, they need to optimize connectivity between users and applications distributed across SaaS ecosystems, public clouds, and on-premises environments. On the other, they need to protect high-value data and intellectual property to keep the enterprise's crown jewels safe from attackers. This can feel like walking on a razor's edge—a task made all the more difficult by the fact that network operations teams have difficulty troubleshooting issues when essential IT resources live outside the corporate network, in places where they have no visibility or control.

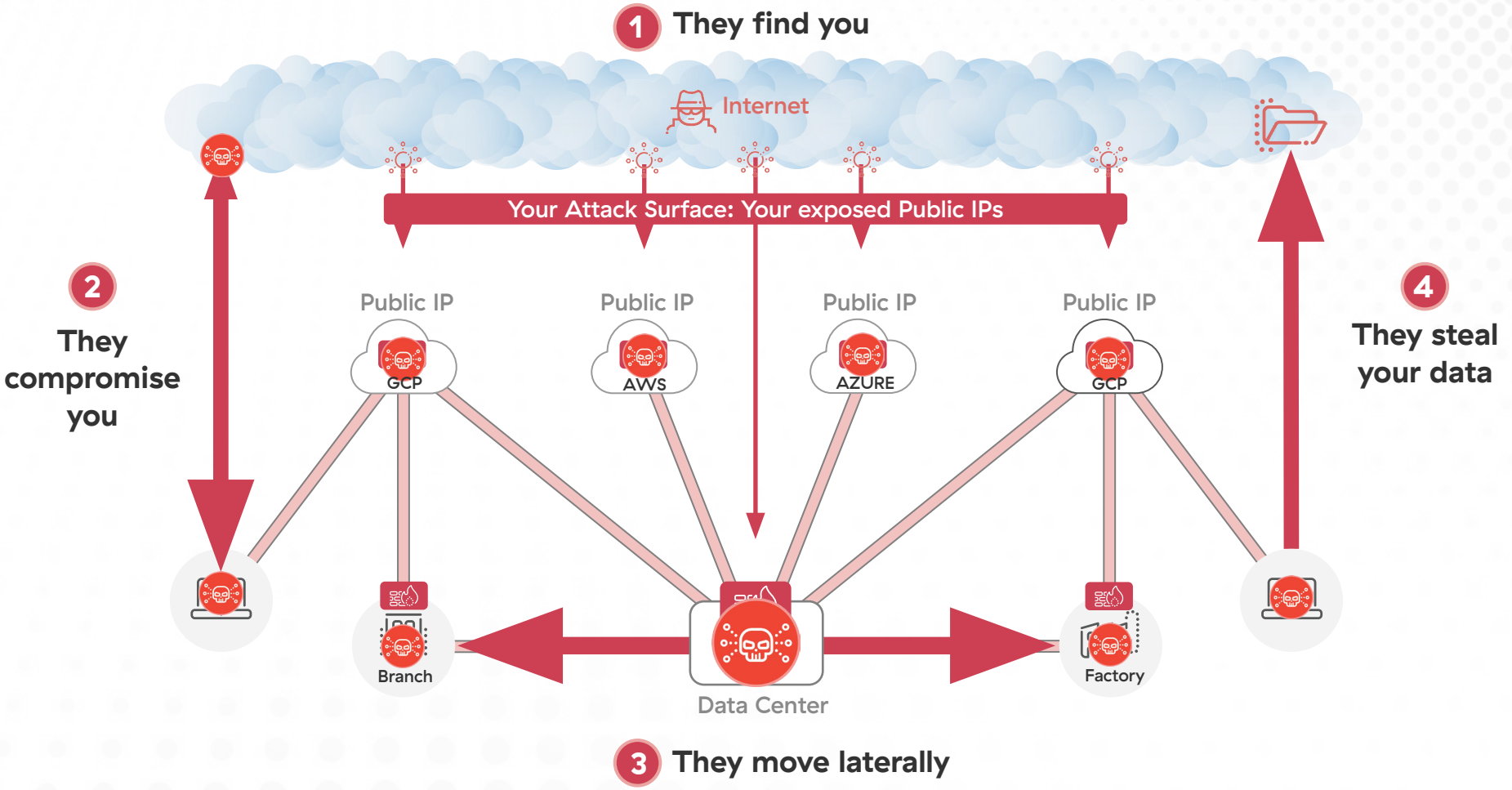
7. *Multicloud in the Mainstream*, 451 Research, February 2023.

Challenges Create Opportunities for Cybercriminals

As network architectures become increasingly complex, the jobs of network, security, engineering, and operations teams become more difficult—and life becomes easier for attackers.

- **Expanded attack surface:** When technology ecosystems are more complex, it's harder for vulnerability management teams to apply software updates in a timely fashion. Plus, it's more difficult to keep cloud assets properly configured to prevent inadvertent exposure. This makes it easier for attackers to conduct reconnaissance and take advantage of zero-day exploits.
- **Ease of initial compromise:** Ransomware remains prevalent, with bad actors continuing to leverage tried-and-true strategies (such as phishing attacks and zero-day vulnerabilities) to deliver exploit kits or malicious attachments. Attackers are increasingly concealing malicious communications within encrypted traffic to cover their tracks.
- **Few mechanisms to block lateral movement:** Legacy network architecture designs were flat, making it so that a single compromised user account could enable ready access to additional resources. With this access, attackers can explore the environment, escalate privileges, and prepare to exfiltrate high-value data.
- **No way to prevent extortion or data loss:** Once they've gained access to legacy-architected networks, attackers have the keys to the kingdom. There's little to nothing stopping them from stealing data, deploying ransomware, setting scams in motion, or sabotaging business-critical information assets.

How Legacy Architectures Create Opportunities for Cybercriminals



Answering These Challenges: A New Paradigm in Network Architecture

Today's network architects face a critical decision point: Should they continue to build out existing designs that have been in place for years, if not decades, by purchasing more physical and virtual firewalls, expanding their reliance on VPNs and siloed monitoring solutions, or extending their WAN infrastructures? Or should they embrace a new paradigm and seek out a solution that's expressly designed for modern networks that incorporate hybrid and remote users, cloud workloads, IoT/OT devices, and smart connectivity? To be fast, reliable, and cost-effective, such a solution must leverage an intelligent platform approach, one driven by advanced machine learning (ML) and AI.

Modern enterprise networks demand flexibility. Because users can be anywhere and everywhere, it must be possible to deliver secure cloud access from any location, at any time. Because most enterprises rely on more than one cloud provider, they need to be able to standardize their approach to securing cloud workloads in a way that's consistent across all of their different cloud environments. And because nearly all enterprises rely on at least a few private applications, they need to make sure end users can securely and efficiently access resources in the data center as well as the cloud.

As hybrid becomes the working model of choice for a growing number of employees and employers alike, business leaders are looking to redesign corporate and branch offices so that they can offer on-site workers amenities that can compete with the comforts of home. Increasingly, this means delivering seamless in-office connectivity that resembles what a customer would experience when visiting the local coffee shop.

High-Performance Network Connectivity: What's Needed for Success

Today's users need reliable connectivity that keeps them productive whenever they want to work. But architects and engineers must also redesign networks in order to:

- Reduce operational costs by decreasing complexity
- Improve performance
- Safeguard business-critical workloads by enhancing security
- Proactively identify issues before users are impacted

The advantages of this kind of seamless connectivity are many:

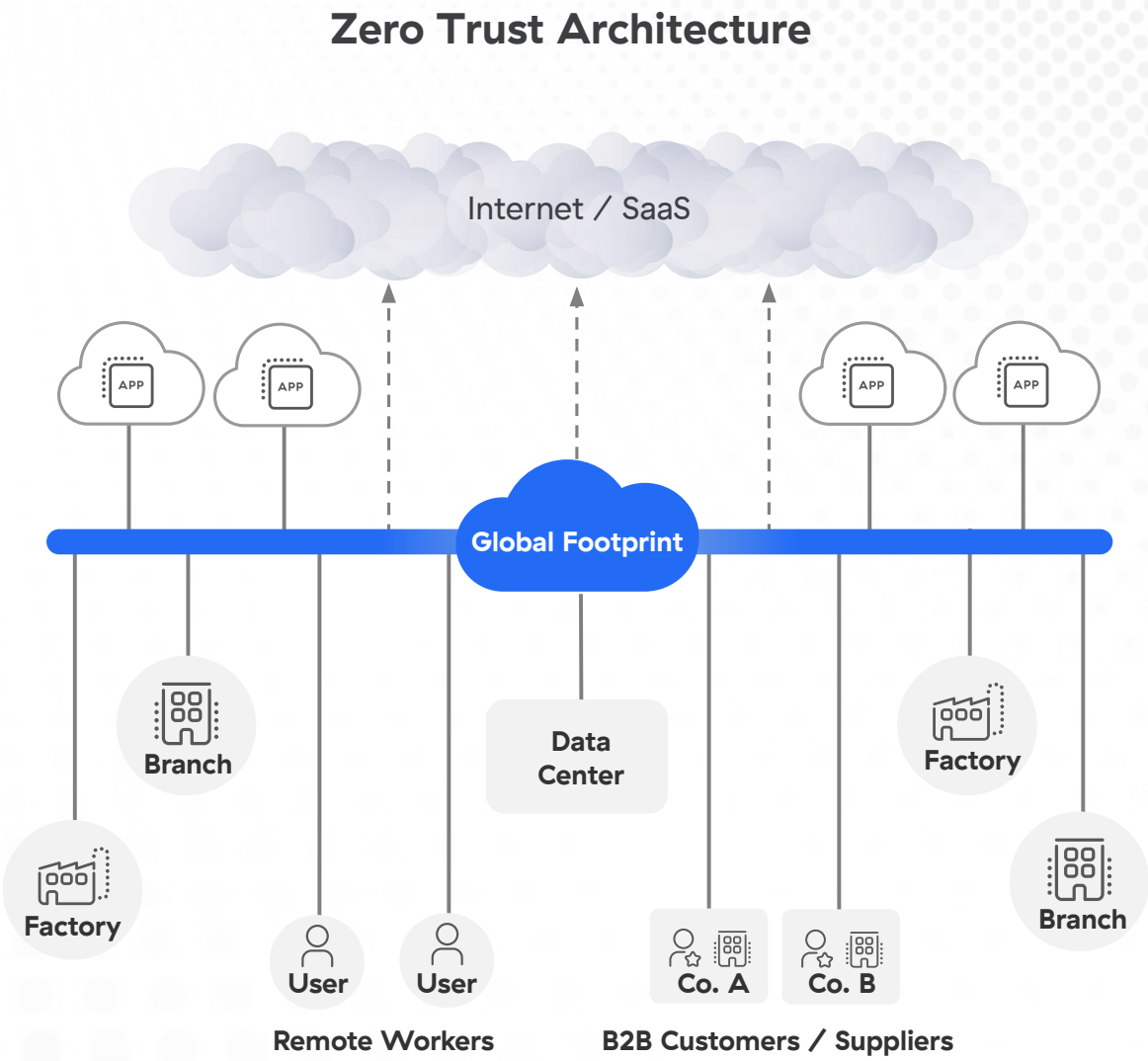
- **It's simple for end users.** There's no need to install VPN software or troubleshoot VPN connectivity. There's no need to backhaul traffic, resulting in poor performance. Instead, users experience the same reliable connectivity that they'd get at home, in a café, or elsewhere.
- **It's simpler for administrators.** Setting up a new branch office can be as simple as plugging in a laptop. Just connect a single appliance to an internet connection, and all of the connectivity and security needed to operate the branch location can be automatically provisioned from the cloud in less than ten minutes. With fewer boxes to manage and reduced deployment times, network administrators can lower cost and complexity and be more agile, making it faster to deploy new locations or integrate acquisitions.
- **It makes it possible to build zero trust into your connectivity architecture.** To enforce robust security policies that truly mitigate real-world risks, organizations must adopt the zero trust approach to connecting and securing users, devices and app traffic. Zero trust implies segmentation at the user and app level, ensuring that no user or device can communicate with anything unless this is explicitly allowed by business policies, and only after verifying identity and device posture. This way, users have access to the apps they need, whenever they need it, while cyberthreats such as ransomware are contained.

A Zero Trust Architecture Is the Way Forward

Zero Trust Architecture is a security architecture built to reduce network attack surface, prevent lateral movement of threats, and lower the risk of a data breach. It's based on the zero trust security model, which rejects the traditional "network perimeter"—inside which all traffic between workloads is trusted and given broad permissions—in favor of least-privileged access controls, granular microsegmentation, and multi-factor authentication (MFA). Zero trust architectures make it possible to provide secure connectivity and access to devices that weren't designed with security in mind. This includes many of today's IoT and OT devices.

A Zero Trust Architecture

- Protects against sophisticated cyberthreats
- Prevents data loss
- Prevents lateral movement of threats
- Delivers a great user experience
- Reduces cost and complexity



Conclusion

Present-day trends won't reverse themselves in the foreseeable future. More and more employees will seek out employers willing to support the agile and flexible ways of working that they prefer. Growing numbers of enterprises will continue to take ever-greater advantage of cloud infrastructure and services. Organizations' network environments will only become more complex, with increasing adoption of smart technologies and connected devices, as the number of communications between workloads continues its exponential growth.

Enterprises need to ready themselves for this future by building fast, reliable, and cost-effective network architectures. But they can't achieve this using yesterday's network designs or the last decade's technologies. Instead of firewalls, VPNs, and MPLS/WAN infrastructures, they need a comprehensive new approach, one that delivers fast and secure application access from anywhere, that simplifies branch and cloud connectivity, and that supports the transition to zero trust.

Adopting this approach won't happen overnight. Instead, it's a journey—one that begins by adapting connectivity to a few of your key applications so that users and workloads can access them securely and reliably. Once you've seen the value of this approach for yourself, you'll be well positioned to expand upon it, having already developed a recipe for success.

Be Ready

Tomorrow's network architectures will be built on a foundation of secure connectivity.

Learn more

Is Your Network Architecture Ready to Face Tomorrow's Challenges?

- ☐ Are network operations teams able to keep up with current ticket volumes?
- ☐ Are ticket volumes growing faster than what your team can keep pace with?
- ☐ Does your organization struggle to provide consistent, reliable connectivity to remote users when too many people work outside the office at the same time?
- ☐ Are you challenged to enforce security policies in ways that are consistent for remote and in-office users?
- ☐ Are network teams struggling to handle ever-increasing network complexity?
- ☐ Are you seeing evidence that cyber threats are increasing or that greater numbers of incidents are occurring?
- ☐ Have you been impacted by a ransomware attack or data breach?
- ☐ Are network teams struggling to manage growing fleets of physical or virtual appliances?
- ☐ Are the costs associated with maintaining a secure and high-performing network spiraling out of control?

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