zscaler™

Why SD-WAN Requires a New Approach to Security

Survey shows that **88% of companies are concerned about traditional security** limiting SD-WAN's advantages

NETWORKWORLD FROM IDG

SPONSORED CONTENT / IDG COMMUNICATIONS, INC.

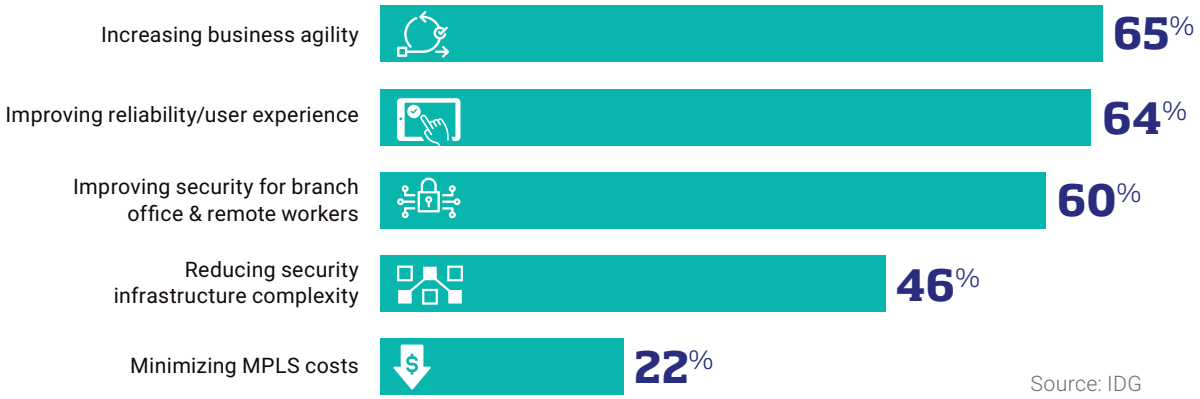
It is no longer a question whether an organization will deploy cloud applications, but *when*.

According to a new survey from IDG and Zscaler, many enterprises (49%) are leveraging hybrid cloud and on-premises approaches and more than one-third (37%) plan to shift or deploy all their workloads to the cloud.

The top reasons for adopting the cloud include increased business agility (65%) and better user experience (64%) (Figure 1).

FIGURE 1

Top Reasons for Adopting Cloud



Source: IDG

But although migrating to the cloud promises clear advantages, traditional wide-area networks (WANs) based on conventional routers are far from cloud-friendly. That's because traditional WANs require backhauling all traffic, including traffic destined for the cloud, over Multiprotocol Label Switching (MPLS) to a centralized Internet gateway—a costly and complex approach that can cause latency and performance issues and increase security risks.

Backhauling traffic—routing it through the data center—has been common for companies with multiple branch locations, especially because most applications have traditionally resided on-premises. But as applications move to the cloud, backhauling to a centralized data center to egress to the Internet can prove slow and expensive—and can negatively impact user experience.

47%

OF RESPONDERS STILL BACKHAUL ALL BRANCH OFFICE TRAFFIC OVER MPLS.

So why not send branch traffic direct-to-cloud? The performance, cost, and efficiency gains can easily be offset by increased security risks. Because many apps no longer sit in the data center behind a security stack, they become exposed, creating one more attack surface for network intruders.

SD-WAN for Your Consideration

Achieving cloud benefits requires a different approach to networking: breaking out Internet traffic locally. It's no surprise, then, that many organizations, especially those with a cloud-first mandate, are increasingly turning to SD-WAN.

In fact, more than half (55%) of the respondents to the IDG/ Zscaler survey are either piloting or upgrading SD-WAN or have installed it but not yet upgraded (Figure 2).

A variety of factors is driving interest in SD-WAN among survey respondents, including improved user experience (61%) and reduced MPLS costs (47%) (Figure 3).

FIGURE 2

Current Adoption of SD-WAN

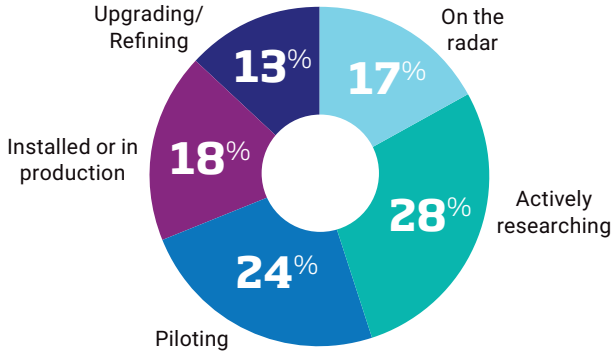


FIGURE 3

What's Driving Interest in SD-WAN

Source: IDG

32%

OF RESPONDENTS ARE GOING DIRECT-TO-CLOUD TO CONNECT USERS TO THEIR APPLICATIONS.

Central to SD-WAN's appeal is that it allows for seamless migration from yesteryear's hub-and-spoke architecture, which requires routing traffic from a remote branch through a data center before reaching the Internet and then routing it back again—an inefficient path not unlike flying from Miami to New York City via Los Angeles.

Instead, SD-WAN provides a new approach to routing Internet traffic that enables organizations to leverage multiple branch connection types, including fixed broadband, VPN over broadband, 4G, LTE, and MPLS for data-center-bound traffic.

These prioritization capabilities offer two key advantages:

1. Policies can be defined in a single cloud management console, thereby simplifying IT operations.
2. Organizations can optimize MPLS costs by eliminating backhauling and reserving MPLS for traffic that's being routed to in the data center.

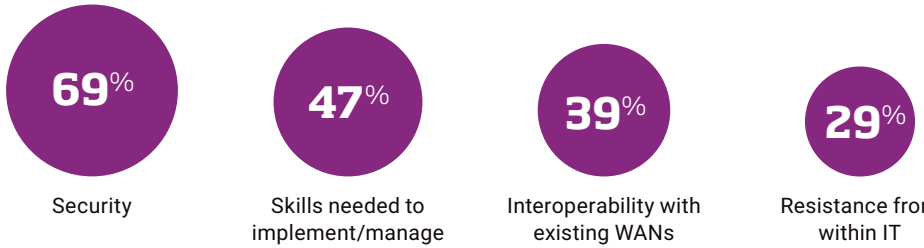
SD-WAN has another upside: Establishing local Internet breakouts is easier. These days, employees expect the same high-quality user experience from their enterprise apps that they do from their at-home consumer apps. Fortunately, SD-WAN improves user experience by providing direct access to the Internet for cloud-based apps. IT teams can also deploy new applications and services easily and quickly—a competitive differentiator in today's fast-paced environment.

The Security Conundrum

But for all of SD-WAN's advantages, local Internet connections must be secure to protect organizations from bad actors. In fact, 69% of the survey respondents cited security as a top concern—more than management skills and IT adoption (Figures 4 and 5).

FIGURE 4

Security Tops the List of SD-WAN Concerns

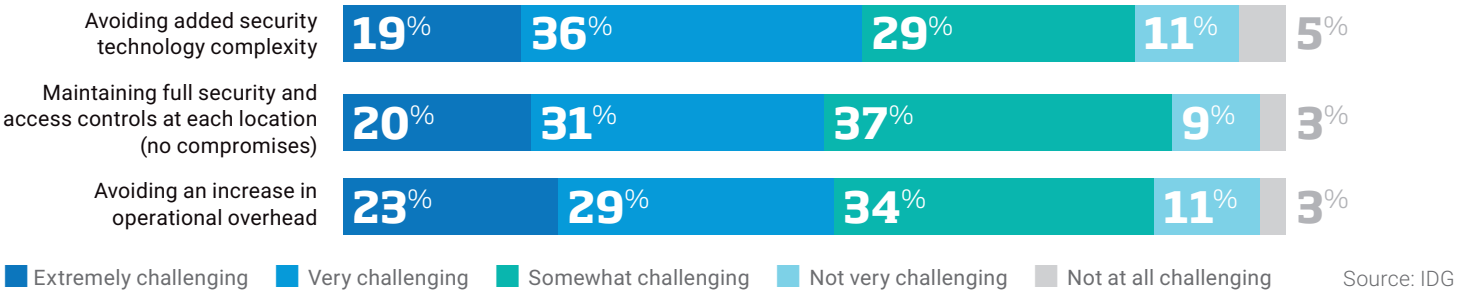


Source: IDG

Unlike traditional architectures that rely on complex access control lists to direct traffic across the WAN, SD-WAN relies on software-defined policies to automatically steer traffic along the best path, intelligently connecting branches to the Internet, cloud applications, and the data center.

FIGURE 5

Challenges of Securing Direct-to-Internet Connections Across Locations



Source: IDG

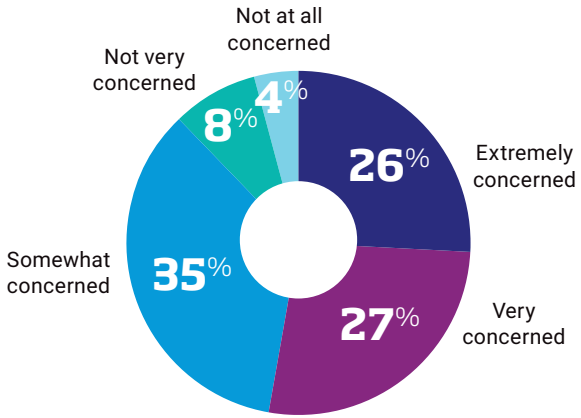
Organizations have long resorted to traditional solutions to minimize these security risks. For some, that entails replicating the stack of security appliances at every branch office, and security stacks are costly to buy, deploy, and manage. It's also counterproductive: SD-WAN allows for remote provisioning and central management. Having to replicate security stacks cancels out this key advantage.

These age-old approaches to SD-WAN security often only compound IT headaches and impede the ability of an organization to achieve a return on its SD-WAN investments (Figure 6).

Among their concerns about securing local Internet connections are increased technology complexity (54%) and potential security blind spots (46%) (Figure 7, next page).

FIGURE 6

Traditional Security Approaches Hamper SD-WAN Benefits



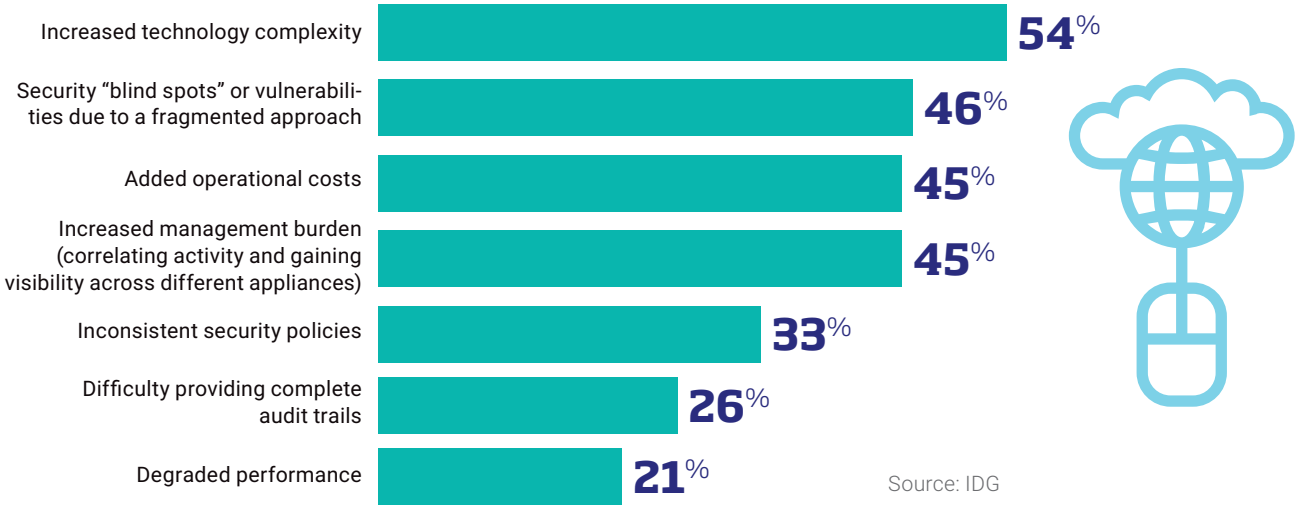
Source: IDG

53%

OF RESPONDENTS ARE HIGHLY CONCERNED ABOUT THEIR ABILITY TO REAP FULL BENEFITS FROM THEIR SD-WAN DEPLOYMENTS WITH TRADITIONAL SECURITY APPROACHES.

FIGURE 7

Concerns About Current Approach to Securing Local Internet Connections



Source: IDG

The Cloud Way to Secure SD-WAN

So how can organizations secure direct-to-cloud connections without sacrificing performance or burdening IT? The answer lies in a cloud-based security solution that doesn't require legacy security hardware.

Together, Zscaler and SD-WAN enable secure, high-performance routing of traffic directly to the Internet from your branch sites—without the cost and complexity of traditional on-premises security or VNFs. Zscaler's cloud-based approach to securing SD-WAN offers three key advantages:

1. REDUCES COSTS AND COMPLEXITY

Unlike traditional approaches that place firewalls, UTMs, or stacks of security appliances at every branch, Zscaler secures local Internet breakouts by delivering the entire security stack as a cloud service. This not only simplifies security but also reduces the costs associated with MPLS backhauling and managing stacks of security appliances at all branch locations.

2. SIMPLIFIES OPERATIONS

Zscaler eliminates the complexity, time, and resources required to deploy and manage stacks of security appliances across all branch locations, in several ways. First, it enables central definition of security and access policies in a single console and immediately enforces any policy changes across all locations, which significantly reduces the burden on busy IT teams. It also enables deployment of new security services across all locations in minutes with just a few clicks. Internet traffic is securely routed locally for a faster user experience. And by providing security and access controls for outbound Internet traffic on all ports, not just 80 and 443, Zscaler solutions protect against today's most advanced threats.

3. SECURES AND SCALES

By delivering security and access controls as a purpose-built, cloud-based service, Zscaler offers the scalability needed for rapid deployment of new features without impacting performance or requiring application refreshes. It also brings the entire security stack closer to the user, ensuring the same protection for users wherever they connect. Full inline content inspection—including native SSL inspection, plus access controls for all ports and protocols, with full logging capabilities—give security a boost and enable Zscaler solutions to quickly identify and block threats.

The Route to Cloud Rewards

Organizations are increasingly moving some of their applications or computing infrastructure to the cloud. With average cloud spend rising, there's no sign that adoption rates are slowing. Although SD-WAN can facilitate this journey, it's often fraught with security fears.

That doesn't have to be the case: Enterprises can leverage cloud-based security capabilities and access controls. This not only eliminates the need for costly MPLS backhauling for traffic egressing to the Internet but it also saves IT teams from having to deploy and manage security appliances in each branch office. Cost savings, performance enhancements, operational efficiencies—there are plenty of reasons to move security to the cloud when deploying SD-WAN.

Beyond SD-WAN

The emergence of new platform offerings combining multiple WAN security services can provide several benefits for securing SD-WAN deployments. Often referred to as Secure Access Service Edge (SASE), these offerings provide a single service that secures connections between users in any location and any application. This platform approach offers reduced cost, a better user experience, and greater security for all user connections, including ones coming from SD-WAN connections.

To learn more, go to Zscaler's webinar "SD-WAN: Why Traditional Security Doesn't Cut It."

ABOUT THE SURVEY

Company Size (Number of Employees)

7%	100,000 or more
9%	50,000 - 99,999
17%	30,000 - 49,999
17%	20,000 - 29,999
21%	10,000 - 19,999
29%	5,000 - 9,999

Job Title

16%	CIO (Chief Information Officer) or top IT executive
12%	Chief Technology Officer (CTO) or equivalent
1%	CSO, CISO
2%	Head of Networking
14%	IT Infrastructure Architect/Engineer
12%	IT Network Architect/Engineer
3%	Security Architect/Engineer
11%	Executive VP, Senior VP IT
6%	VP IT
23%	IT Director

Vertical Industry

17%	Technology
14%	Healthcare
13%	Banking & Financial Services
11%	Manufacturing (Industrial)
8%	Wholesale/Retail trade
4%	Aerospace/Defense
4%	Insurance
4%	Life Sciences, Pharmaceuticals, Biotechnology
4%	Hardware/Software
3%	Business/Professional Services
2%	Automotive
2%	Chemicals/Energy/Utilities
2%	Food & Beverage
2%	Information, Media & Entertainment
2%	Transportation & Logistics
1%	Communications
1%	Distribution
1%	Food and Beverage
5%	Other

To learn more, go to Zscaler's webinar
"SD-WAN: Why Traditional Security Doesn't Cut It."

zscaler™

NETWORKWORLD FROM IDG