zscaler™

eBook

# The CIO's Guide to Accelerating Secure Digital Transformation

Five imperatives to get you where you need to go, quickly and securely

# The new IT reality

Your organization is adopting cloud applications, your internet traffic volume has exploded, and mobile-first computing has become a strategic initiative for your company.

Digital transformation may be both nerve-wracking and exhilarating for your IT organization. It might even be keeping you up at night, but it doesn't have to.

## These five imperatives will help your secure digital transformation

1. Modernize aging infrastructure ›
2. Enable secure internet connectivity at branch locations ›
3. Securely connect your distributed mobile workforce ›
4. Improve the Microsoft 365 experience for users ›
5. Simplify IT integration during M&As ›

# Modernize aging infrastructure

Organizations have been building complex networks to connect users to applications in the data center for 30 years, and to secure it all, they've invested in a multitude of network security appliances. In the ever-evolving threat landscape, the need to update or replace aging infrastructure and add new security controls has increased—and so have the costs and complexity of your network.

With users and applications moving off the network and more traffic destined for the cloud, the traditional network model has become irrelevant.

It's time for a modern, purpose-built approach that meets your security needs and cuts costs by connecting users directly to their destinations. It's time to move security to the cloud.

## How to get started:

- **Use a secure access service edge (SASE) architecture** as referenced in the Gartner report, **"The Future of Network Security is in the Cloud,"** and refer to the **"Gartner Magic Quadrant for Secure Web Gateways."**
- **Transform your network** from hub-and-spoke to direct-to-cloud, leveraging cloud security as a service.
- **Phase out hardware and software over time** to free up technical talent and reduce day-to-day management and maintenance.

**SUCCESS STORY**

## SIEMENS

The cloud is becoming the new data center and the internet the new corporate network for 350,000 Siemens users across 192 countries. Siemens significantly reduced costs with a modern network architecture that's built for the cloud and provides secure, high-performance access to apps—anytime, anywhere.

"By not backhauling our traffic, but directly using the internet, we expect we can drive down costs by 70%."

Frederik Janssen
VP of IT Strategy & Governance
Siemens

# Enable secure internet connectivity at branch locations

How long does it take your organization to get a new branch office or retail store online? Integrating new sites with a hub-and-spoke network is time-consuming and resource-intensive. Even after your locations are online, you may face traffic bottlenecks and latency, especially as rising bandwidth demands overwhelm your firewalls, drive up WAN costs, and clog your gateways. Legacy networks simply can't scale rapidly enough.

As you plan to move to SD-WAN to simplify branch operations and enable local internet breakouts, you'll need to move security from your data center to your network edge to fully realize the value of SD-WAN.

## How to get started:

- **Move security to the cloud** to inspect all traffic, whether it's bound for the data center, cloud services, or the open internet.
- **Make branches "asset free"** by deploying local internet connections at every location and removing MPLS where possible.
- **Refocus your local IT talent** to get closer to the business and enable transformation initiatives.

## SUCCESS STORY

AutoNation

The largest auto retailer in the US, AutoNation established local breakouts that provide users with fast and secure internet access at its 360 locations. With Zscaler, AutoNation is reducing costs, bringing new locations online more easily, and improving its security posture with inline SSL inspection, sandboxing, and other capabilities.

"With Zscaler, we were able to bring down our footprint to basically just a router and endpoints for 360 branches."

Ken Athanasiou
CISO and Vice President
AutoNation

# Securely connect your distributed mobile workforce

With users working and connecting to their applications from everywhere, you've had to rely on VPN technology that extends your network to users' locations. For security, you've had to backhaul traffic to your data center, making a bad user experience worse and often leading remote users to bypass the VPN and security, increasing your business risk. For these reasons and others, Gartner estimates that 60% of organizations will phase out VPNs in favor of zero trust network access (ZTNA) solutions by 2023.[1]

Endpoint security alone isn't enough to keep up with sophisticated threats. How can you leverage a service edge security cloud to protect your users and give them a great experience?

## How to get started:

- **Adopt a ZTNA architecture** to provide users with access to apps without giving them access to the network.
- **Move security to the edge** to provide identical security wherever users connect while guaranteeing a fast user experience.
- **Grant or deny application access** via centrally managed identity that reduces administration complexity.

**SUCCESS STORY**

nab

National Australia Bank (NAB), Australia's largest business bank, began its cloud migration to provide a better, more secure banking experience for customers and to streamline operations. Today, NAB is embracing zero trust and delivering a future-proof networking infrastructure that enables all staff to work from anywhere.

**"People go home, turn on their PC, and it operates in exactly the same way as it does in the office. They don't have to worry about extra login steps or deal with security tokens—it just works."**

Steve Day
EGM Infrastructure, Cloud and Workplace
National Australia Bank

# Improve the Microsoft 365 experience for users

With just about everyone relying on Microsoft 365, user experience is an important measurement of your deployment's success. However, because user traffic to Microsoft 365 increases network utilization, it quickly overwhelms firewalls and creates a poor user experience. This often results in the need for expensive hardware upgrades that add complexity, and constant firewall updates, which are difficult to keep up with.

You need a fast and consistent Microsoft 365 experience. To achieve it, here's what Microsoft recommends:

- Identify and differentiate Microsoft 365 traffic
- Egress network connections locally
- Assess bypassing proxies
- Avoid network hairpins

## How to get started:

- **Route Microsoft 365 traffic** over your local internet breakouts, as recommended by Microsoft.
- **Leverage Microsoft's only recommended cloud security vendor** to achieve the fastest user experience.
- **Streamline bandwidth usage** to prioritize Microsoft 365 traffic over recreational traffic.

## SUCCESS STORY

KELLY SERVICES

Kelly Services transformed its network to enable fast, secure, and direct internet connections across 900 locations worldwide, providing fast access to Microsoft 365 and other cloud apps. The company shaved 60% from its MPLS budget, improved its inspection capabilities, and vastly simplified network and policy management.

"With Zscaler, Office 365 could be guaranteed 30% of all bandwidth, but also be limited to no more than 50%, so that OneDrive file transfers wouldn't bog everything down."

Darryl Staskowski
SVP & CIO
Kelly Services

# Simplify IT integration during M&As

The complexity of IT integrations slows M&As and disrupts business activities. You need to manage risk as you on– or off–board users while providing them access to the applications they need. Adding to this complexity is the need to standardize on security while you integrate new parts of a company with lower or different security standards, which can elevate risk and always demands special attention.

You can accelerate M&As and related activities from years to weeks by providing users with access to applications without the need to converge network infrastructures, minimizing business risk.

## How to get started:

- **Leverage ZTNA technology** and give users immediate access to applications without bringing them onto the network.
- **Use a phased approach based on identity.** Start with users at both entities working on M&A–related activities and determine which applications they need to access.
- **Expand the list of users and applications** as the business integration evolves.

## SUCCESS STORY

A Fortune 500 US healthcare organization shaved nine months off its integration timeline by providing application access without network access, enabling secure onboarding for newly acquired or merged organizations. This helped simplify the organization's M&A infrastructure and reduce complexity for IT.

# About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.

# CIO Library

For more essential resources by and for CIOs, visit:

**revolutionaries.zscaler.com**

Or contact your sales representative for peer references.

zscaler™ | 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