zscaler™

THE CIO'S GUIDE TO:

Accelerating secure digital transformation

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

The new CIO 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.

The process of 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. Modernizing aging infrastructure ›
2. Enabling secure internet connectivity at branch locations ›
3. Securely connecting a distributed mobile workforce ›
4. Improving the Office 365 experience for users ›
5. Simplifying IT integration during M&As ›

Keep reading to learn how to get started.

Modernizing an aging infrastructure

For 30 years, you have been building complex networks to connect users to applications in the data center and, to secure it all, you've invested in a multitude of network security appliances. With an ever-evolving threat landscape, the need for updating or replacing your aging infrastructure and adding new security controls has increased, which has, in turn, increased the complexity of your network and the cost.

But with users and applications moving off the network, and more and more traffic destined for the cloud, the network model is becoming increasingly 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

Enabling 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 your hub-and-spoke network is a time-consuming and resource-intensive endeavor. And 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 cannot scale rapidly enough.

As you plan to move to SD-WAN to simplify branch operations and to enable local internet breakouts, you will need to move security from the data center to the edge of your network 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 U.S., 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 connecting a 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 the user's location. But for security, you've had to backhaul traffic to the data center, making a bad user experience worse and often causing remote users to bypass the VPN and security, increasing your business risk. For these reasons and others, Gartner estimates that 60 percent of organizations will phase out VPNs in favor of ZTNA by 2023.[1]

Relying on endpoint security alone is not enough to keep up with sophisticated threats. How can you leverage a service edge security cloud to protect your users and provide them a great experience?

How to get started:

- **Adopt a zero trust network access (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 regardless of where users connect, while guaranteeing a fast user experience.
- **Grant or deny application access** via centrally managed identity that reduces administration complexity.

SUCCESS STORY:

GE's vision of the future didn't include a "network." So, GE eliminated the notion of being on- or off-network and, instead, simply has 425,000 users who are secure wherever they are.

"We've ended up with a security posture that's better than we had with a complex network and a user experience that is 80% faster."

Chris Drumgoole
CTO
GE

Improving the Office 365 experience for users

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

There is an alternative: a fast and consistent Office 365 experience. To achieve it, Microsoft recommends the following:

1. Identify and differentiate Office 365 traffic
2. Egress network connections locally
3. Assess bypassing proxies
4. Avoid network hairpins

How to get started:

- **Route Office 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 O365 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 Office 365 and other cloud apps. The company shaved 60 percent 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

Simplifying 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.

But 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 zero trust network access (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 U.S. healthcare organization shaved 9 months off their integration timeline by providing application access without network access enabling secure on-boarding for newly acquired or merged organizations. This helped simplify the organization's M&A infrastructure and reduced 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:

www.zscaler.com/cio-insights

Or contact your sales representative for peer references.

zscaler™

[1] Steve Riley, Neil MacDonald, Lawrence Orans, Market Guide for Zero Trust Network Access, Gartner, April 2019