



IT STARTS WITH ZERO

Three strategies to accelerate
your business transformation



Reimagining success in the digital age.

It's never been more imperative to digitally transform your business to...

- ✓ Build long-term competitive advantage
- ✓ Make the business more agile
- ✓ Deliver a superior customer experience

Whether you're a CIO, CISO, head of networking, head of security, or an IT infrastructure leader, helping the business accelerate its transformation confidently and securely is a top priority. Legacy network and security infrastructure worked well in the past, but now stands in the way of transformation.

As your company transforms, it's moving into a cloud-first world where your ecosystem of customers, partners, employees, applications, and data come together using the internet as the connective tissue. In this world, security must be delivered through the cloud, close to your business ecosystem, using the principles of zero trust to make the cloud safe.

That's why transformation starts with zero. Here's how. →

SIEMENS

CUSTOMER STORIES

“The cloud will be our new data center and the internet our new network. We drove down networking costs by 70%.”

— Frederik Janssen, VP of IT Strategy, Siemens



VISUALIZATION

Examining the future of work.

The internet is the
new connectivity layer:

4.6x

growth (2016–2021)¹

The cloud is the
new destination:

220x

growth (2016–2021)¹

Business happens
everywhere **on any device:**

1.4B

5G devices by 2023²

Server, IoT, OT traffic is
growing **exponentially:**

50%

of all connected devices by 2023²

Overcoming the barriers to transformation.

Transformation and cloud connectivity upend 30 years of IT networking and security approaches. Legacy infrastructure was centered on building private networks to connect branches and users to applications in the data center. All traffic flowed to the data center and business took place on the trusted private network. That model is no more.

Attempting to adapt out-of-date network and security architectures to the demands of modern, cloud-first business introduces barriers to transformation.

BARRIERS TO TRANSFORMATION

High Operational Cost

Traditional enterprise networks use a hub-and-spoke model, and offices and branches are often connected using expensive MPLS WAN links to central locations like the data center. Users outside the office typically use VPN to access the network. This method is expensive, slow, and adds operational complexity.



Risk

Moving business to the internet dramatically expands the attack surface and makes traditional network security irrelevant. Legacy security infrastructure such as site-to-site VPNs perpetuate lateral movement of threats, therefore creating an increased risk of infection.



Poor Experience

Current network and security architectures rely on backhauls to the data center, introducing latency issues that impact productivity and deliver poor cloud application experiences. It's also difficult to monitor user experience or troubleshoot performance issues in complex network architectures.



STRATEGIES TO OVERCOME THEM

Make the internet your new network by going direct-to-cloud
[page 6](#)

Embrace zero trust to make the cloud safe
[page 7](#)

Empower the anywhere business with faster access and a better user experience
[page 9](#)

STRATEGY

Make the internet your new network.

As applications move from the data center to the cloud, you need to begin transforming your network from hub-and-spoke to direct-to-cloud. With a secure, direct-to-cloud approach, you can dramatically reduce cost and complexity while improving IT agility and responsiveness to the business. No more friction. No more waiting on network connections for cloud application access.

Zscaler makes it possible. With **Zscaler Zero Trust Exchange**, you can:

- ✓ Reduce cost and complexity by shifting security to the cloud, eliminating the need for legacy perimeter based security
- ✓ Deliver a superior user experience by directly connecting to cloud applications
- ✓ Eliminate the internet attack surface with applications that sit behind the exchange, thus preventing discovery and targeted attacks
- ✓ Prevent the lateral movement of threats by connecting users to applications directly, without network access

You can accomplish this iteratively, over time, cutting MPLS costs and retiring infrastructure such as firewalls in branch offices as you transform your network.



Learn more about
how to modernize
your network



STRATEGY

Embrace zero trust.

To accelerate transformation with confidence, you also need to transform your approach to security by starting with zero ... zero trust. Instead of outdated, legacy network security, the zero trust approach — made possible with the **Zscaler Zero Trust Exchange** — securely connects applications and users over the internet based on business policies to:

- ✓ Eliminate the internet attack surface
- ✓ Minimize lateral movement across the network
- ✓ Stop hidden threats and data loss
- ✓ Prevent patient-zero infections

The Zscaler Zero Trust Exchange relies on three tenets to securely connect users, devices, and applications using business policies over any network:

- 1 Application access without network access:** Use identity to connect users and applications to resources, not the corporate network.
- 2 Zero attack surface:** Make applications invisible to the internet to eliminate the attack surface and achieve application isolation without the need for network segmentation.
- 3 Proxy architecture:** Use a proxy architecture, not a passthrough firewall, for all application connections to improve cyberthreat and data protection.

CORE CONCEPTS OF ZERO TRUST

Zero trust is based on the principles of least privilege access and that **no entity (user or application) should be inherently trusted.**

A zero trust strategy uses the identity of an entity and business policy to grant access to specific resources, instead of allowing access to a network. Policies include **four key elements (user, device, application, and content)**, and are enforced by the zero trust exchange.

Discover more
about the Zscaler
Zero Trust Exchange

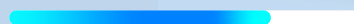


VISUALIZATION

Rising zero trust adoption.

Zero trust network access (ZTNA) and **cloud access security broker (CASB)** controls will be the top two zero trust technologies in which companies plan to invest in the next 12 to 18 months.

72%



Organizations with a zero trust strategy

76%



Organizations with new budget allocated to zero trust

82%



Organizations that will increase spending on technologies over the next 12 to 18 months



STRATEGY

Empower the anywhere business.

Beyond making the cloud a safe place to do business, you need to make it **enjoyable and productive** for users. Delivering secure, direct-to-cloud access to applications eliminates the latency inherent in backhaul, VPN, and VDI architectures, improving the user experience and optimizing productivity. Providing services and peering at the edge, near users, provides the fastest performance possible.

Yet, there's more to delivering a great user experience: you also need visibility into performance and a way to quickly identify and resolve issues that could impact the experience. Zscaler gives you **full visibility** from endpoint to application for all your users around the world. With Zscaler, you can **identify and resolve issues faster**, which means far fewer IT tickets to which your team needs to respond.



Explore more
Work-from-Anywhere
resources



PROVEN RESULTS

Security at the speed of cloud.

500

companies on the Forbes
Global 2000 rely on Zscaler

150B

global requests
processed daily

10+

years operating the largest
inline security cloud

175k

unique security updates
performed daily

150+

data centers across 6 continents,
with peering in internet exchanges,
bringing security close to the user
for a fast experience

7B

threats
blocked/policies
enforced daily

WHY ZSCALER?

Choose the right partner for your journey.

No matter where you are in your transformation journey, Zscaler can help you accelerate it with confidence. Zscaler offers the people, infrastructure, and tools to protect the modern enterprise while keeping business users productive.

- ✓ **Cloud native, zero trust architecture**, running at the edge across 150 data centers worldwide
- ✓ **Robust AI and analytics** provide visibility and control through cloud sandbox, DNS security, antivirus, advanced threat protection, IPS, and browser isolation
- ✓ **Users connected directly to the resources they need** via dynamic policy: no complex segmentation required, no unnecessary exposure, and no unrestricted movements in any direction to thwart attacks
- ✓ **Full inline SSL inspection at scale**, paired with Zscaler's complete security stack, provides improved protection without the inspection limitation of appliances
- ✓ **The world's premier cloud threat research team**: Our team of researchers is dedicated to identifying new vulnerabilities and making continuous improvements for all customers
- ✓ **Always-on, everywhere, no-hassle user experience** with better application speed/performance no matter where your users are
- ✓ **Robust dashboards and reporting**, and cloud-to-cloud log streaming that integrates with other SecOps tools and workflows

IT STARTS WITH ZERO

Accelerate your move to the cloud
with the Zscaler Zero Trust Exchange.

[Learn more](#)

Zscaler (NASDAQ: ZS) accelerates digital transformation so 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 in-line cloud security platform.

