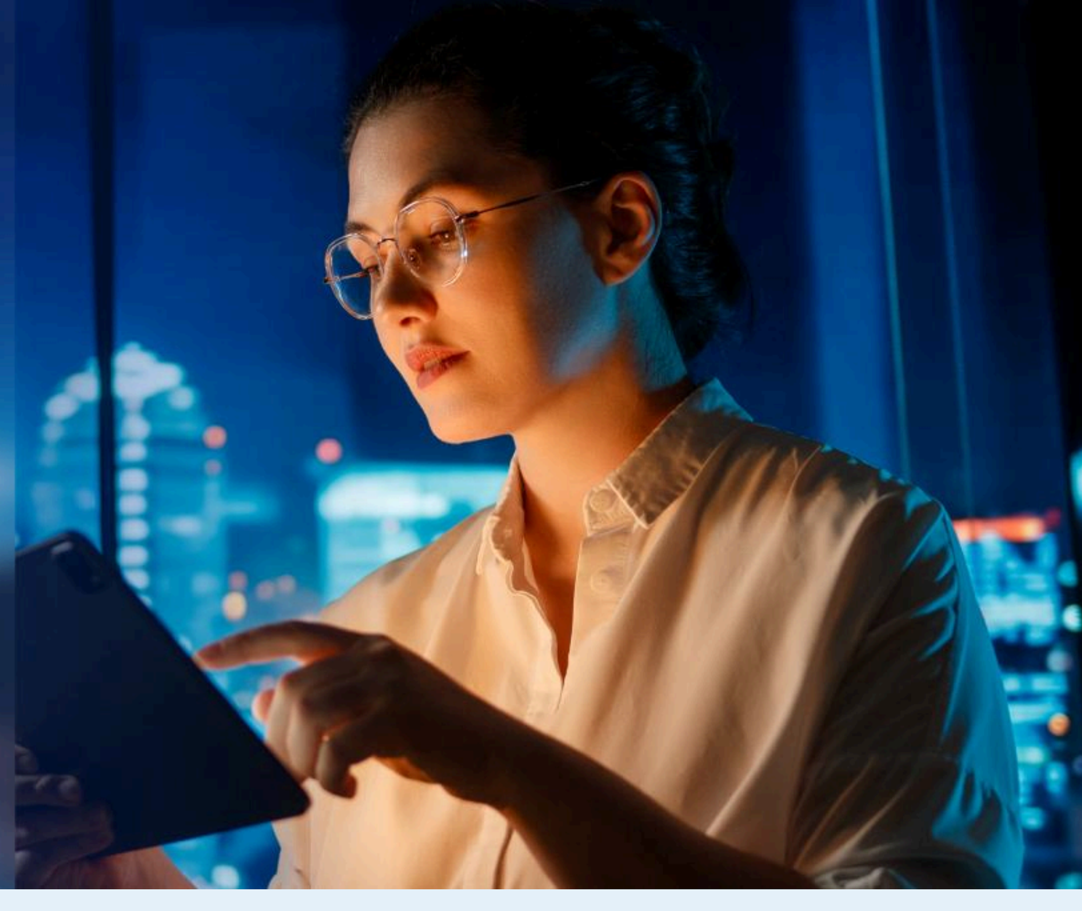
zscaler

Zero Trust 101: From siloes to security everywhere

As employees and apps go remote, traditional security is no longer enough.

Here's what's replacing it.



Work has changed

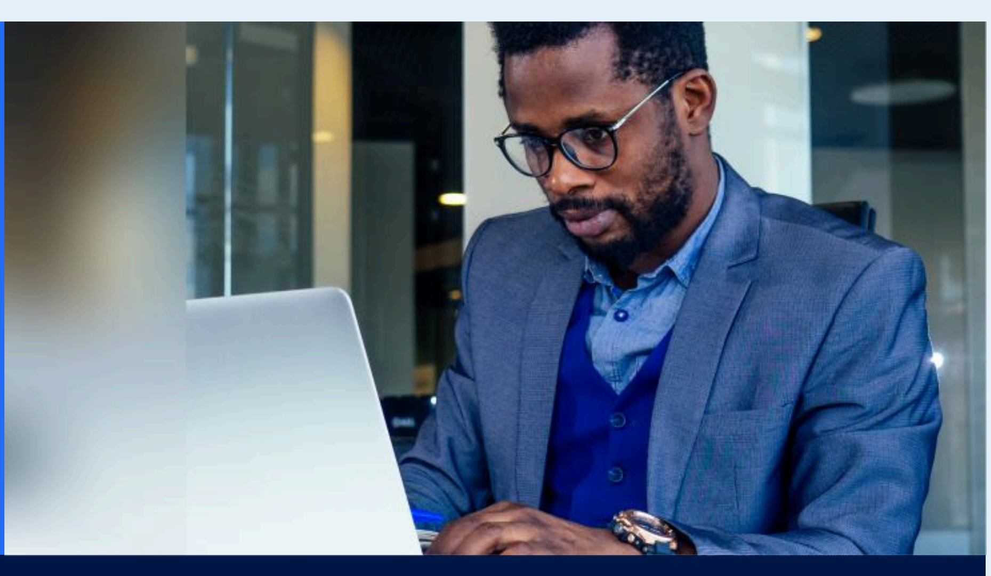
Today, users, devices and apps are connecting from everywhere, not just the corporate network.

80%
of employees are hybrid or remote[1]

90%
of apps reside in the cloud[2]

Traditional security can't keep up

Conventional network–centric architectures create fundamental weaknesses.



Expanded attack surface
Public IPs expose firewalls and VPNs

Lateral movement
Once inside, attackers can move freely

Encrypted blind spots
95% of traffic is encrypted and difficult to inspect

Poor user experience
Backhauling traffic causes delays

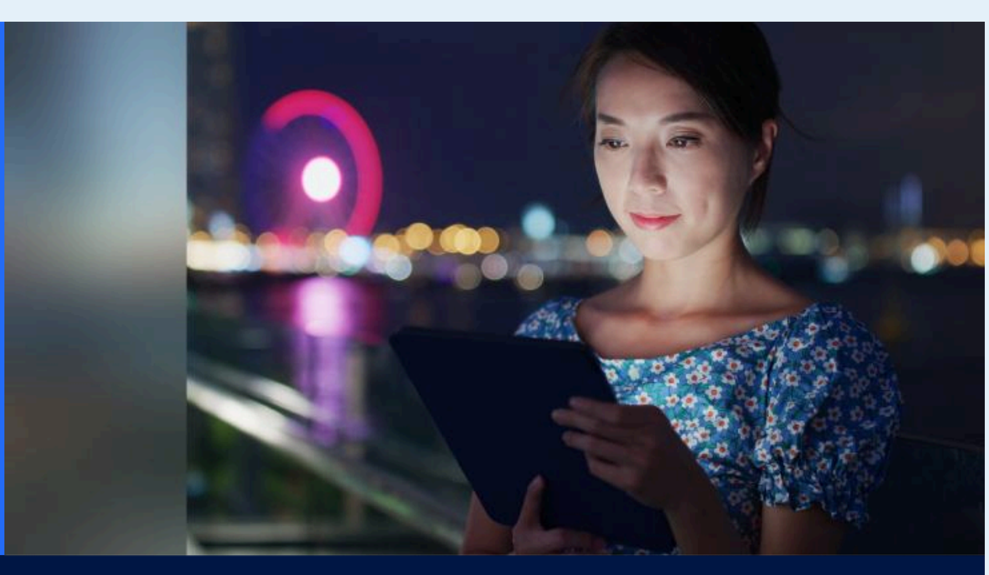
The 'trusted network' is no longer trustworthy

Once an attacker is inside your network, they can unleash serious damage — deploying ransomware, stealing sensitive data, and disrupting critical systems.

200%
increase in ransomware attacks between 2021-24

Enter a new approach: zero trust

Zero trust is a security framework that treats every connection as untrusted until proven safe.



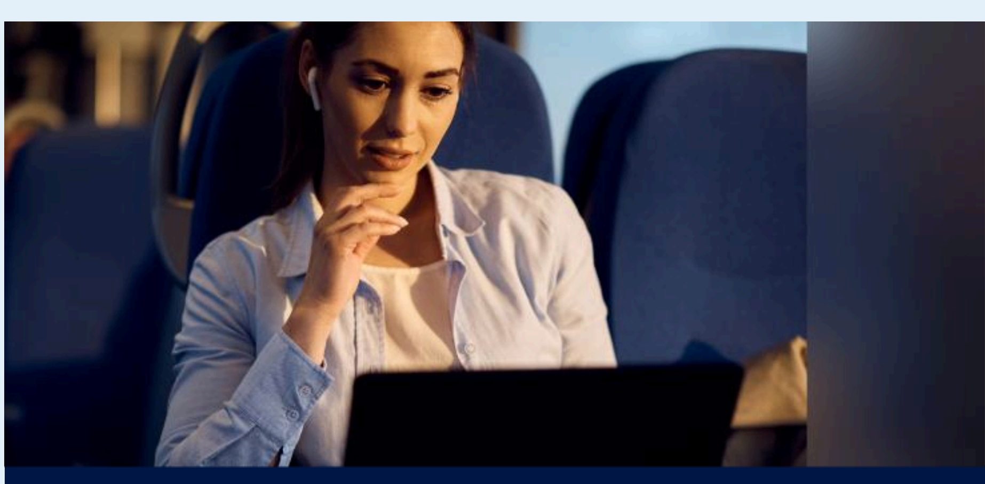
PRINCIPLES OF ZERO TRUST

No implicit trust
Assume no user, device or connection is safe

Continuous verification
Check every identity, device and context

Minimal exposure
Grant access only to the resources users need

Direct–to–app connectivity
Connect direct to apps, not the network



How it works

In a zero trust architecture, every access request is evaluated before access is granted.

Verify identity
Who are you?

Identify destination
Where are you going?

Assess risk
What's the risk?

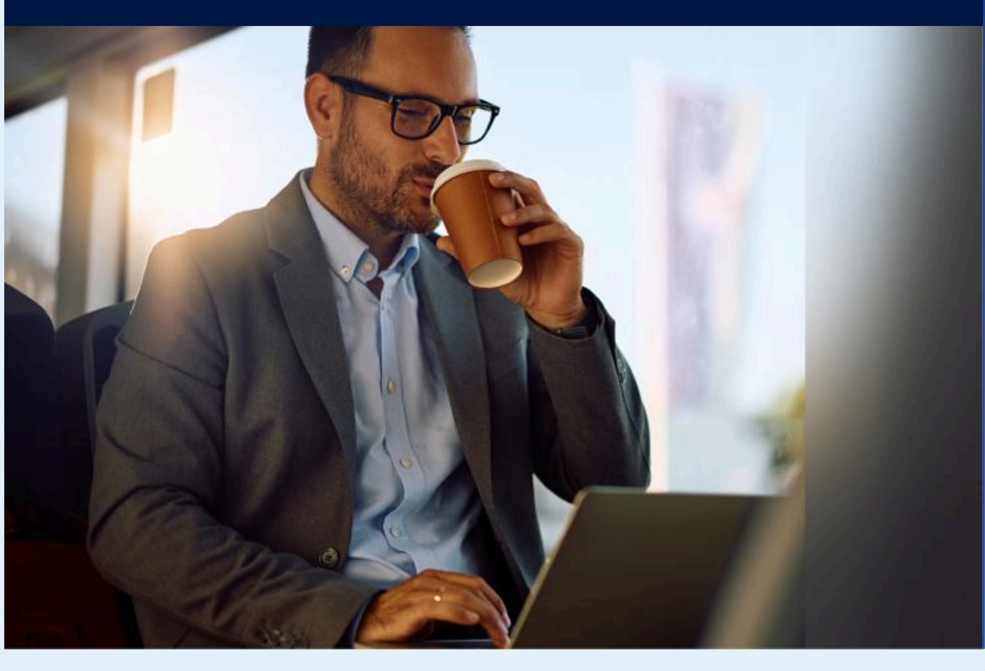
Enforce policy
Block, allow, caution?

"Think of zero trust as an intelligent switchboard that provides secure any–to–any connectivity in a one–to–one fashion, without extending the network to anyone or anything. Basically, you're decoupling security and connectivity from the network."

Jacob Serpa, Zscaler

Zscaler: powering zero trust everywhere

Zscaler's Zero Trust Exchange enforces zero trust at scale, securely connecting users to apps, services and data, without exposing your network.



160+
points of presence

500B+
requests processed every day

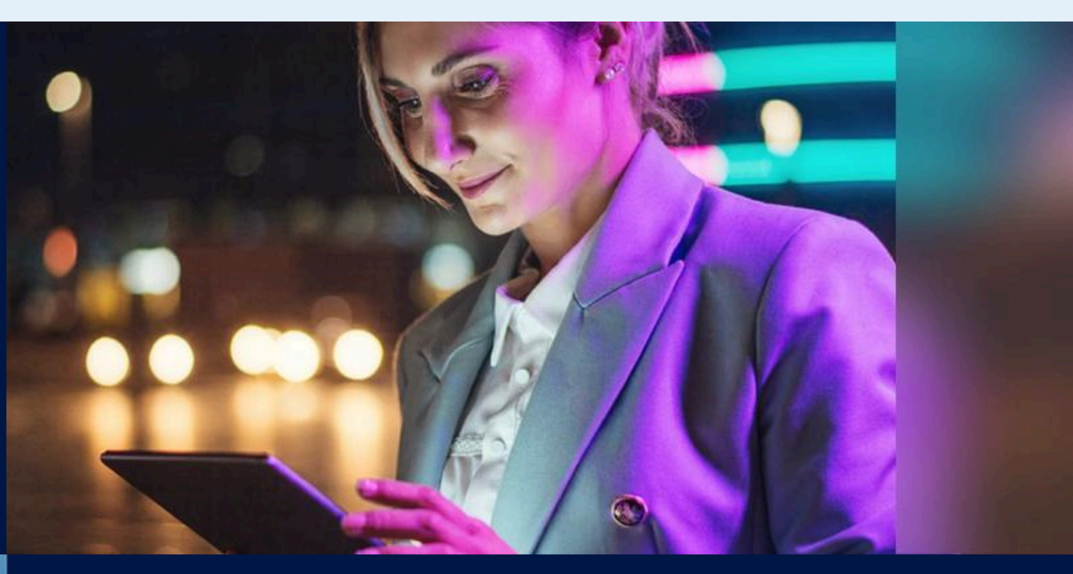
4000
threats blocked every second

Ready to take the next step?

Master the fundamentals of zero trust and start applying it in your organisation with our 3–part video series.

To understand the essentials of zero trust:

Watch Zero Trust 101



To learn how it secures your hybrid workforce:

Watch the masterclass

1. Source: Gallup
2. Source: O'Reilly

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 centres globally, the SSE–based Zero Trust Exchange™ is the world's largest in–line cloud security platform. Learn more at **zscaler.com** or follow us on X (Twitter) **@zscaler.**