

THE ZERO TRUST EDGE:

DELIVERING A MORE SECURE NETWORK FROM THE START

Remote work has accelerated the move to cloud. What's your plan to deliver the network performance improvements and close security gaps? How does your architecture need to change?



53% of newly remote workers want to stay remote



Cloud, Edge, and IoT are redefining the location of data and applications



A growing number of enterprise applications exist in the cloud



Users and devices have now left the traditional enterprise perimeter

Why historic security and networking approaches no longer work

Disjointed security and networking silos and a limiting hardware-centric approach mean:



Higher levels of complexity, less flexibility, lower efficiencies



Hampered resilience capabilities and disaster recovery



Missed opportunities and danger of falling behind competitors



Difficulties meeting requirements for using cloud and supporting home workers

Why you need a Zero Trust Edge (ZTE)

A Zero Trust Edge solution securely connects and transports traffic, using Zero Trust access principles, in and out of remote sites leveraging mostly cloud-based security and networking services.

A Secure Access Services Edge (SASE) Is A Zero Trust Edge (ZTE). A SASE network architecture integrates SD-WAN capabilities with security at the "services edge", where devices and networks are connected, using a cloud software model.

Forrester 2021

What are the benefits of ZTE and SASE?



Embedding security into the DNA of networking



Prioritizing business application traffic that dominates the branch WAN



Protecting businesses from customers, employees, contractors, and devices connecting through WAN fabrics to a higher-risk environment



Providing secure access to corporate services and applications to secure remote workers



Securing the internet of all the things, including IoT and edge devices and business partners



Enabling central management, monitoring, and analysis of the set of security and networking services that reside within ZTE solutions

Should you be on a ZTE journey? 3 questions to ask in your business

1

How segregated are security and networking?

2

Struggling to secure devices and users at the edge?

3

Are you ready for 53% of workers staying remote?

INTRODUCING THE ZERO TRUST EDGE MODEL FOR SECURITY AND NETWORK SERVICES:

A SECURE ACCESS SERVICES EDGE (SASE) IS A ZERO TRUST EDGE (ZTE)

Read the full Forrester Report to find out:

- Why siloed networking and security infrastructures and operations are disappearing fast
- Which type of ZTE method is right for your business
- How to assess multivendor and single-vendor choices



Read the report [→](#)