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?

- Users and devices have now left the traditional enterprise perimeter.
- Cloud, Edge, and IoT are redefining the location of data and applications.
- 53% of newly remote workers want to stay remote.
- A growing number of enterprise applications exist in the cloud.
- A siloed networking and security infrastructure is no longer sustainable.

Integrate security and networking to better protect your business

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.

Why historic security and networking approaches no longer work

- Higher levels of complexity, lower flexibility, lower performance, lower efficiency
- Struggling to secure devices and users at the edge
- Higher levels of cost, complexity, lower flexibility, lower performance, lower efficiency
- Upper levels of complexity, lower flexibility, lower performance, lower efficiency

Why you need a Zero Trust Edge (ZTE)

- Zero Trust Edge delivers security that connects and transports traffic, using Zero Trust access principles, in and out of remote sites leveraging mostly cloud-based security and networking services.
- Forrester 2021: 53% of workers want to stay remote.
- A Secure Access Services Edge (SASE) is a Zero Trust Edge (ZTE).
- A growing number of enterprise applications exist in the cloud.
- A siloed networking and security infrastructure is no longer sustainable.
- Disjointed security and networking silos and a limiting hardware-centric approach mean:
  - Why historic security and networking approaches no longer work.
  - Why you need a Zero Trust Edge (ZTE).

What are the benefits of ZTE and SASE?

- Embedding security into the DNA of networking.
- Providing secure access to corporate resources and applications to secure remote workers.
- Protecting businesses from customers, partners, and third parties contacting through WAN fabrics to a high-risk environment.
- Securing the internet of all the things, including IoT and edge devices used by business partners.
- Enabling central management, monitoring, and control of all on-premises and cloud-based security and networking services.

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

1. How segregated are security and networking?
2. Are you ready for 53% of workers staying remote?
3. Could service edge devices and users at the edge?