SASE: The cloud-native network security solution

Addressing the need for better remote working security

Many businesses have had no choice but to introduce remote working to their workforce over the past year. But it’s only now that those same businesses are beginning to see how their teams and processes have adapted and thrived. KPIs have been hit, communication has been upheld, and client relationships have survived all from the comfort of home.

So now, a lot of businesses are gravitating towards introducing working remotely as a permanent fixture. But with remote working comes greater risk of security threats, data breaches, and business risks, as the amount of data being generated outside the cloud rises.

Why the need for a new architecture?

In the past, architectures have verified and inspected all application traffic from branch locations by passing it over private MPLS services (Multiprotocol Label Switching) first, before reaching the corporate data centre. This architecture sufficed when the corporate data centre was the exclusive applications host. But now, with applications and services migrating to the cloud, and more remote workers connecting to the cloud, a new architecture is needed.

This comes down to internet-destined traffic having to get through the data centre and corporate firewall first before reaching its destination. And as a result, application performance and user experience take a hit, as well as network security. So, a more secure, reliable, cloud-based architecture is needed.

Introducing SASE: Secure Access Service Edge

SASE, or Secure Access Service Edge, is the cloud-native architecture solution that securely connects the Edge to the cloud, increases network security, and improves application performance for enterprises.

Bringing together advanced WAN edge functions like SD-WAN, routing, segmentation, zone-based firewall and WAN optimisation with cloud-delivered security services, all in all, SASE builds a new, cohesive architecture. No matter the location or device, SASE ensures direct, secure access to applications and services across multi-cloud environments, designed for the new decade. And more specifically, remote working.

Thanks to enhanced security and improved performance, SASE gives businesses peace of mind when capturing data at the Edge. With fewer risks, it helps to maintain brand image. And with improved performance, SASE increases productivity, customer satisfaction, and IT efficiency, even lowering overall WAN and security costs. Plus, it gives businesses the opportunity to evaluate and integrate new security technologies as they arise.

Working in harmony with Aruba ESP

Aruba ESP is an agile, resilient, and integrated services platform that businesses are turning to as a result of remote working, and more data being generated outside of the cloud. Reducing the need for troubleshooting with sixth sense, AI technology, and simplifying and improving IT operations with a Unified Infrastructure.

But as Aruba ESP captures data at the Edge, increased protection and security is needed, as old architectures just don’t cut it. Aruba ESP features a built-in foundation for the SASE framework, meaning businesses can effortlessly adopt the SASE architecture alongside the Aruba ESP platform, for enhanced security and improved productivity across their enterprise. Meaning Aruba ESP and SASE go hand in hand.

Capture data at the Edge, safely

In a nutshell, SASE is the cloud-native architecture that any enterprise migrating applications to the cloud, needs. Along with increasing network security, SASE helps businesses improve productivity and efficiency, letting people work from anywhere, at any time, with total peace of mind. For a new way of working, that feels just as safe and secure as before.

Want to find out more about selling SASE with TD SYNNEX? Get in touch today.