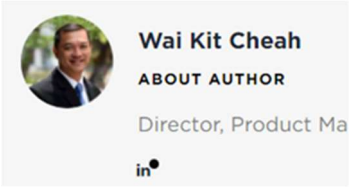
Lumen APAC Blog

5 signs your organisation needs SASE



In the post-COVID-19 world, hybrid and remote work have become the norm among organisations in the Asia Pacific region. Companies now use scores of SaaS applications and internal file-sharing systems that are accessed by employees who are working outside the office.

Unfortunately, centrally applied security policies and entitlements enforced in the organisation for employees who access enterprise systems through virtual private networks (VPN) have come up short in terms of user experience and performance.

VPNs and centrally applied security policies present choke points in traffic flow, forcing organisations to invest in larger and costlier security solutions and products. Meanwhile, the network perimeter has become amorphous and the potential attack surface unclear.

As the network perimeter expands, organisations are using software to define it. The key question is: How can you leverage the advantages of a software-defined wide area network (SD-WAN) while enforcing a consistent security policy when your employees are working from anywhere?

This is where Secure Access Service Edge (SASE) comes to the rescue of APAC enterprises that are either still in the infancy of adopting SD-WAN or starting to look for a better approach in securing their WAN.

SASE is a framework rather than a technology. It represents the convergence of several established technologies that merge SD-WAN capabilities and network security functions into a unified approach.

SASE comprises five security and networking technologies:

- SD-WAN
- Firewall as a Service (FWaaS)
- Cloud Access Security Broker (CASB)
- Secure Web Gateway
- Zero Trust Network Access (ZTNA)

The framework is designed to ensure that the applications and data that workers need to stay productive would remain optimised for performance, are always available, and are protected wherever they are accessed from. SASE distributes all checkpoints across various regions to improve the efficiency of network resources, and reduce the latency created by the hub-and-spoke model.

The advantage of SASE is that it is designed with the user in mind and begins with the idea of zero trust. To make things simple for you, here are five signs that proves your organisation can greatly benefit from SASE today:

1. Slow application response times

Your employees' productivity is marred by poor network and application performance. Furthermore, wherever users are accessing the network, response times to SaaS applications are slow. SASE solves this challenge by embedding security into the global or regional spread of your organisation’s network. This means your network and cloud applications are always available whenever your workforce needs them.

Regardless of where users are located and applications are accessed, or the nature of the technologies that connect the user and the systems, SASE can ensure the performance and user experience that your workforce expects. This is because SASE combines networking and security capabilities into a unified, built-for-cloud architecture that shifts the focus of security from traffic flow centred to identity-centred.

2. High capital investment and opex due to complexity

Using diverse point products to manage security causes IT sprawl, and typically the costs of managing such an infrastructure are also very high. The complexity creates an IT environment that is not conducive to hybrid work or optimal access to cloud applications.

The SASE framework ensures that all network and security capabilities are embedded in a single software stack. You can manage consolidated networking and security services from a "single pane of glass" to reduce the workload of your security staff, so that they can focus more time on high-value tasks.

In addition, a SASE architecture can greatly complement your investment in the cybersecurity, allowing you to enforce a unified security policy, lower operational costs, and make your infrastructure more accessible for remote cloud applications.

3. Fast-evolving cyber threats

Cyber criminals today are highly ingenious in the tactics they use to hack your network, and cyber threats – such as malware and ransomware – are becoming increasingly complex and rapidly evolving. Worse still, cloud architectures provide a lot of “openings” for malicious acts.

Cyber criminals who hack into VPN-based access can freely get into enterprise networks and corrupt data and assets with few, if any, barriers to stop them. In this regard, SASE provides better way to secure the network to protect your assets and data. This is done by enforcing identity and context-based authentication as well as continuous validation for security configuration and posture. SASE also enhances security by enabling least-privileged access.

4. Slow security deployment and incident response times

Traditional models like VPNs require centralised authentication with incident management routed through that central location. This invariably slows down the response to cybersecurity breaches and deployment of security services. A few seconds or minutes lost can make a huge difference to how your organisation salvages data and assets after an incident.

SASE aggregates threat intelligence across all cybersecurity solutions. It enables you to quickly implement identity-based security policies and cloud-based firewall (such as FWaaS), while improving incident response times through decentralising security services (on-premise or cloud-based) to save time and costs.

5. Unclear network perimeter and extent of attack surface

When most employees were working on-premises, securing network endpoints was a relatively trouble-free endeavour. However, with hybrid and remote work models gaining popularity in Asia Pacific, and the remote workforce accessing enterprise SaaS applications over the cloud, organisations became unsure where the edge of the network is, and the extent of the potential attack surface.

SASE ensures that security policies follow the user wherever they are, and whichever device they use to access applications and resources. It ensures that mission-critical business assets are well-protected when a user access a cloud service even beyond the perimeter. With a software-defined foundation, SASE give enterprises the flexibility to protect this expanding perimeter.

SASE helps deliver immersive digital experiences at reduced cost

Using SASE ensures that you can streamline the application of all security policies and processes to reduce complexity and cost and do more with less resources. Organisations can confidently deliver immersive digital experiences across distributed environments and geographies using an architecture strategy that combines Security Service Edge (SSE) and SD-WAN.

SASE keeps the end user in mind and its application begins with the idea of zero trust. This means that as long as the user can verify their identity and the connecting device, the location of the user is immaterial. By using a software-defined perimeter, SASE ensures that a trusted user can access only the required specific resources and nothing else.

What's next?

If you're ready to get started on your SASE journey, Lumen can help.

As a leader in the 2022 Gartner® Magic Quadrant for Network Services, Global and a diverse network across APAC including China with extended reach across four continents, Lumen has a robust record in supporting enterprises globally to achieve their SASE potential.

For a deep dive into adoption of SASE, watch our 6 steps to simplified SASE adoption webinar right now. Alternatively, you can contact us to arrange a SASE consultation with one of our technical experts.

SOLUTION

LUMEN CONNECTED SECURITY

Automated threat detection.
Built in protection.

See more. Stop more.

LEARN MORE