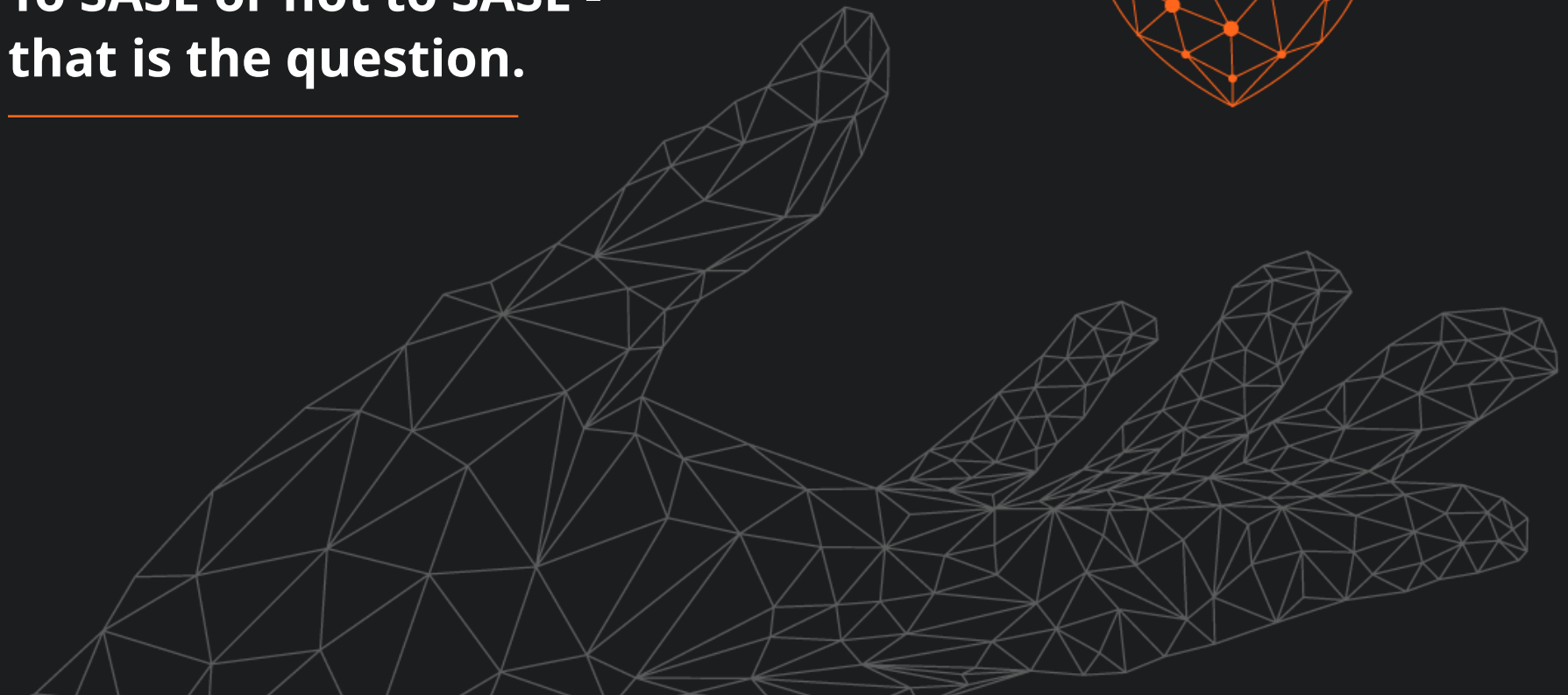
BESTPATH

To SASE or not to SASE - that is the question.

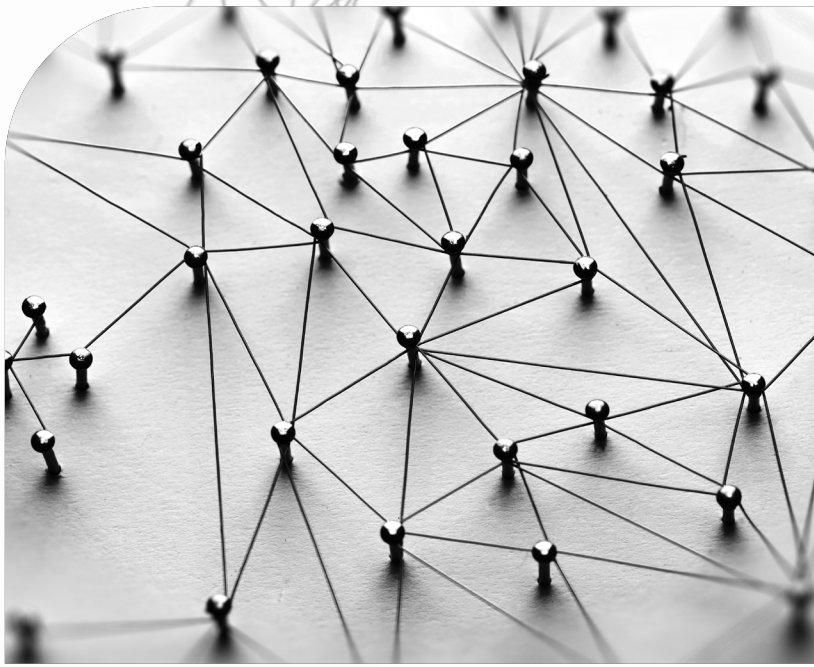


Introduction

SD-WAN (Software-Defined Wide Area Network) and SASE (Secure Access Service Edge) are two related technologies that are transforming the way organisations connect and secure their networks.

SD-WAN is a technology that uses software to simplify the management and operation of a wide area network (WAN). It allows organisations to use different transport types (such as broadband, cellular, Direct Internet Access (DIA) or MPLS to connect their sites and applications, while providing centralised control and management of network traffic.

SASE, on the other hand, is an emerging security architecture that combines SD-WAN with cloud-based security services to provide a more comprehensive and flexible solution for secure access to applications and data. SASE delivers security functions such as firewall, secure web gateway, zero-trust network access, and cloud access security broker as a service from the cloud, and provides these services at the edge of the network, closer to the users and applications.



Why SD-WAN and SASE?

SD-WAN combined with the appropriate SASE (Secure Access Service Edge) components provides a more comprehensive and secure networking solution for modern businesses. Here are some reasons why:

1. Traditional security solutions are no longer sufficient:

Traditional security solutions in isolation, such as firewalls and VPNs, were designed for a perimeter-based network where applications and data were housed within a corporate data centre. However, with the increasing adoption of cloud-based applications and remote work, the network perimeter has expanded, and traditional security solutions might not scale efficiently to keep you protected against modern threats.

2. SD-WAN alone cannot provide complete security:

While SD-WAN provides a simplified and more efficient way to manage network traffic, it does not include all the security functions necessary to protect against advanced threats. For example, SD-WAN does not provide advanced threat protection, data loss prevention, or secure web gateway functions.

3. SASE provides cloud-based security services:

SASE integrates a comprehensive set of cloud-based security services, such as next-generation firewalls, secure web gateways, zero-trust network access, and cloud access security brokers. By leveraging SASE, organisations can secure their network traffic, irrespective of where the traffic originates, where it traverses or where it ends up.

4. SASE enables secure access for users and applications:

With a rise in hybrid working SASE provides secure access for users to cloud-based applications, regardless of their location or device. With SASE, organisations can ensure that users are accessing applications securely, and that their data is protected.

How do you align SD-WAN as a SASE foundation?

1. Implement centralised policy management:

SD-WAN allows for centralised policy management, which can be used to enforce security policies across the network. SASE can further enhance this by providing a centralised policy management platform that covers both networking and security policies.

2. Consolidate services:

With SD-WAN, organisations can adopt a network focused approach and simply consolidate services and functions, from simplifying contracts with regional ISPs, to reducing the hardware footprint by adopting wires-only services all wrapped with security, onto a single platform. This consolidation simplifies network management and reduces costs.

3. Integrate security features:

SD-WAN can either be integrated with existing on-premise security solutions for a more traditional approach or with cloud-based security services to provide a more comprehensive security solution. This integration can include functions such as next-generation firewalls, intrusion prevention systems, and anti-malware protection.

4. Adopt zero-trust network access:

Zero-trust network access (ZTNA) is a security model that requires all users, devices, and applications to be authenticated and authorised before they are granted access to the network. ZTNA can be integrated into a SASE solution to provide secure remote access to applications and data.

In summary, SASE provides a more comprehensive and secure network solution for modern businesses. From a network-first approach, SD-WAN is the starting component or building block for many organisations looking towards SASE instead of a security-first or converged approach when talking about SASE. That is because SD-WAN provides so much value by itself, providing operational efficiencies and reduced costs. By leveraging SASE, organisations can further protect their environments against modern threats, provide secure access to cloud-based applications, and ensure that data is protected in flight before being protected at rest.

In closing, ensuring that you get the right SD-WAN solution for your organisation is essential. The solution should provide a seamless transition to a full SASE implementation, evaluating how these solutions will integrate and whether a multi-vendor or fully converged approach is what you desire for your business. Most importantly, get the migration strategy right.

BESTPATH

We're BestPath. The unsung heroes, working quietly and competently behind the scenes to inspire and empower our clients. Combining curiosity with innovation we deliver agile, secure and trusted network infrastructures that enable businesses to deliver exceptional services and outstanding customer experiences. Let's chat about how we can do just that, for you.

To learn how BestPath can help you identify and manage your network vulnerabilities to avoid costly outages, contact us today *info@bestpath.io*

linkedin.com/company/bestpath/

info@bestpath.io

+44 (0)203 879 4826