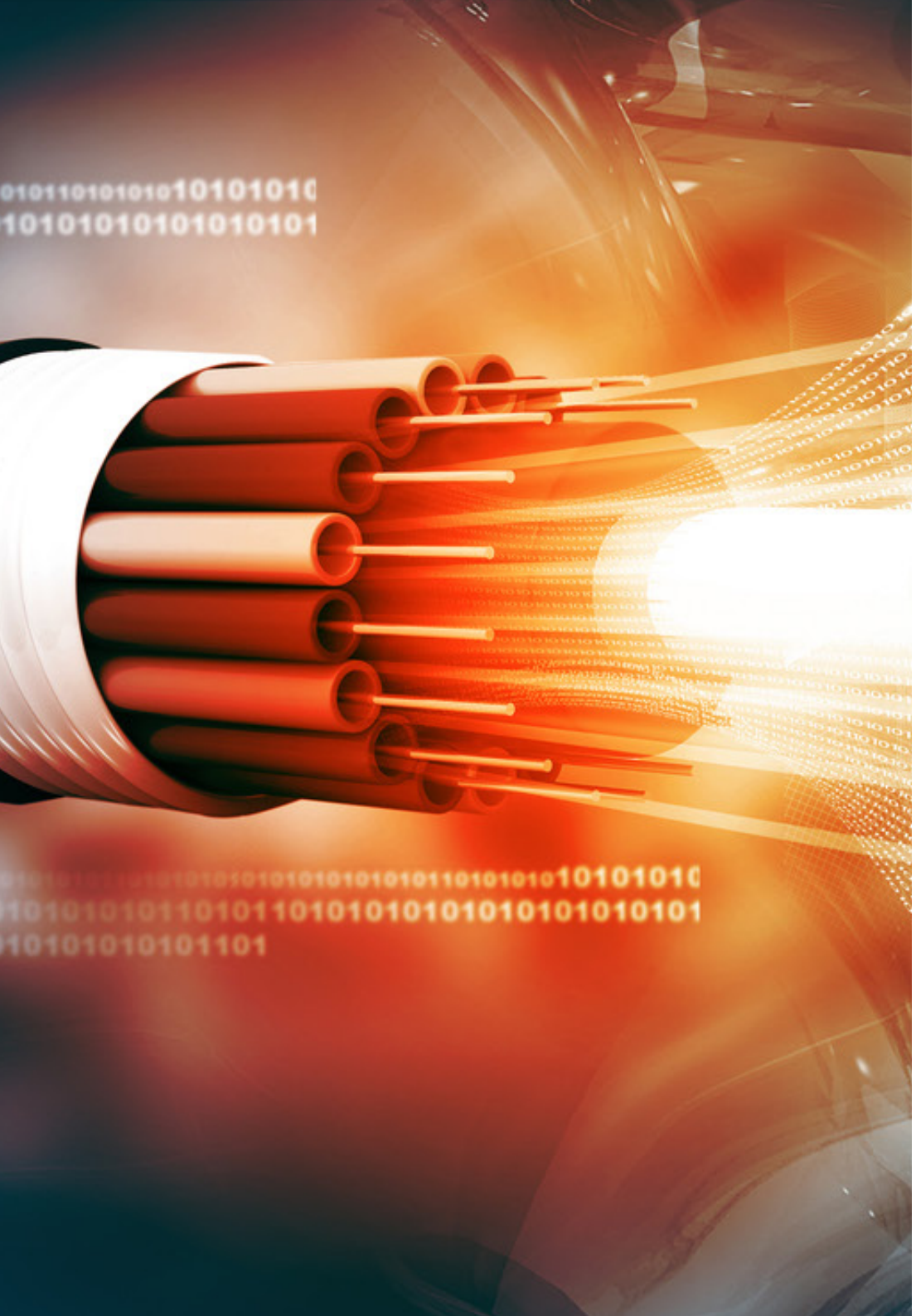


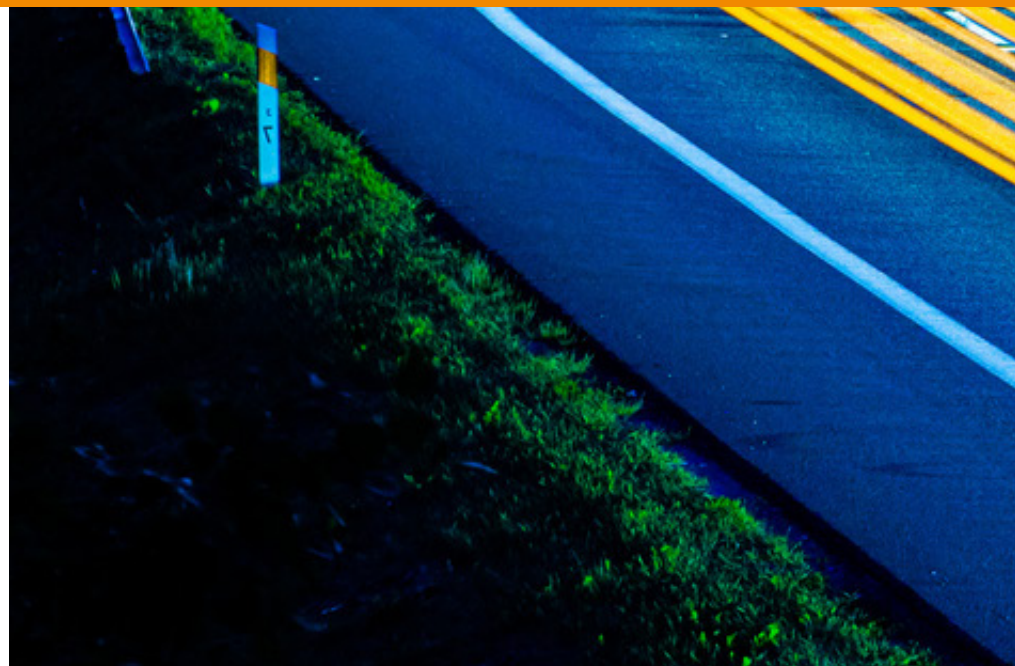
enablis | business nbn® accredited adviser

8 reasons SASE will help you get the most from business nbn® Enterprise Ethernet

Having a reliable, high-performance network is essential for all businesses today.

But with increased demands being placed on them to support remote working and ever more business critical cloud applications, along with a vastly more threatening and complex cyber security landscape, it's no longer enough to simply have a super-fast highway.

business **nbn®** Enterprise Ethernet is certainly one of the fastest highways in Australia.



And helping to keep it that way is secure access service edge (SASE) from Enablis, a business **nbn®** accredited adviser.

We know that SASE is not a technology per se, rather it's a number of critical technologies spanning networking and security, all working together within a cloud native framework.

As a new and evolving framework for security and data management, it's never standing still. But here are the eight core pillars that support successful deployment of SASE today.

Firewall as a Service

Firewall-as-a-Service ((FWaaS) shifts firewall protection to the cloud instead of the traditional network perimeter.

This allows organisations to securely connect a remote, mobile workforce to the corporate network, yet still enforce consistent security policies that extend beyond the organisation’s physical and geographic footprint.

2

SD-WAN

A software-defined wide area network (SD-WAN) is an overlay architecture that relies on routing or switching software to create virtual connections between endpoints—both logical and physical.

SD-WANs offer almost unlimited paths for user traffic, greatly enhancing user experiences, while affording powerful flexibility when it comes to encryption and policy management.

3

Intrusion Detection and Intrusion Prevention

An intrusion detection and prevention system (IDPS) is essentially a system that monitors a network and scans it for possible threats to alert the administrator and prevent potential attacks.

Often sitting right behind the firewall, what differentiates the IDPS is that while the former regulates what gets into a network, the IDPS regulates what flows through the system.

As well as providing the critical functions of monitoring, detecting, and alerting for CIOs, CISOs and others tasked with cyber security, the IDPS also boasts sophisticated - and increasingly automated - incident prevention capabilities.

4

Centralised Unified Management

A modern SASE platform allows tech administrators to manage SD-WAN, SWG, CASB, FWaaS, and ZTNA through centralised and unified management spanning security and networking.

Tech teams are then free to focus more time and energy on more important tasks, while more broadly the user experience for the organisation's hybrid workforce is greatly enhanced.

5

Secure Web Gateway

A secure web gateway (SWG) is a web security service that filters unauthorized traffic from accessing a particular network.

The goal of a SWG is to zero in on threats before they penetrate a virtual perimeter. A SWG accomplishes this by combining technologies like malicious code detection, malware elimination, and URL filtering.

6

Cloud Access Security Broker

A cloud access security broker (CASB) is a SaaS application that acts as a security checkpoint between on-premises networks and cloud-based applications, and enforces data security policies.

A CASB protects corporate data through a combination of prevention, monitoring, and mitigation techniques. It can also identify malicious behavior and warn administrators about compliance violations.

Zero Trust Network Access

Zero trust network access (ZTNA) describes a set of consolidated, cloud-based technologies operating within a framework in which trust is never implicit and access is granted on a need-to-know, least-privileged basis across all users, devices, and applications.

This model stipulates that all users must be authenticated, authorised, and continuously validated before being granted access to private company applications and data. ZTNA eliminates poor user experiences, operational complexities, costs, and the risks of traditional VPNs.

Data Loss Prevention in the cloud

Data loss prevention (DLP) is the practice of protecting a company's data against loss, theft or misuse - deliberate and accidental - regardless of where it is located and whether it's static, in use or in motion. It should also take account of intellectual property and regulatory compliance.

Today, companies collect and process massive amounts of information, ranging from confidential business and customer data to sensitive intellectual property, to everyday data. And they store it in more places than ever, be it data centres, public and private clouds, software-as-a-service (SaaS) applications, mobile devices and so on.

As a result, many organisations no longer know where all their data is or which applications their employees use, nor do they have any visibility into how or from which devices their data is being accessed, used, transferred or shared. Organisations also struggle with the configurations of tools they use to distinguish sensitive data from normal, shareable data, meaning many don't really know what's what.

Cloud DLP allows consistent discovery, monitoring, governance and security of an organisation's sensitive data regardless of its location, everywhere it resides and moves, both on-premises and in the cloud. By utilising the cloud, a next-generation DLP solution provides simplified implementation, unified data policies and quick remediation actions.

enablis | business nbn® accredited adviser

Enablis is a business **nbn®** accredited adviser. If you would like further information visit Enablis' high-performance network webpage here or for more information about SASE click here or get in contact with one of Enablis' SASE certified experts.