As businesses continue to adopt cloud and edge computing, traditional security models are being challenged. The history of security architecture in enterprises was built around the data center, with a well-defined perimeter and the firewall as the most important central security control point. But with the rise of cloud computing and the migration of workloads outside the data center, the role of the firewall has become less important. Enterprises are now subscribing to more than 800 software-as-a-service (SaaS) applications, and the COVID-19 pandemic has accelerated the trend of working from anywhere. As a result, more people, devices, applications, services, and data are leaving the confines of the enterprise data center.

In the pre-cloud era, securing the network was the most important aspect of enterprise security, and the data center was a single location where a company housed its valuable digital assets. However, in the cloud era, the data center is no longer the center of enterprise security, and the fastest growing threats are in the cloud, not in the data center.

In the pre-cloud era, securing the network was the most important aspect of enterprise security, and the data center was a single location where a company housed its valuable digital assets. However, in the cloud era, the data center is no longer the center of enterprise security, and the fastest growing threats are in the cloud, not in the data center.

The result is that enterprises need to shift their security focus from securing the network to securing the data and following it wherever it goes.

The limitations of point products are also becoming more apparent. In the traditional security model, businesses adopted security designed to thwart individual threats or categories of threats as they emerged. However, in the cloud era, there are too many threats of different types to keep up with using point products. Instead, security needs to be integrated and follow the data, and security tools need to work together to provide a cohesive security solution.

This is where Secure Access Service Edge (SASE) comes into play. SASE is a security architecture that provides services at the edge of the network—closer to where the data and users are located. SASE brings security closer to the data, which is critical in a cloud-first world where the data is no longer confined to the enterprise data center. With SASE, security services are delivered as a cloud-native service, which means that they are scalable, flexible, and easy to manage.
The capabilities of SASE are many and varied. The most important key components agreed upon by experts and are included in Hughes Managed SASE:

- Firewall-as-a-Service (FWaaS)
- Cloud Access Security Broker (CASB)
- Secure Web Gateways (SWG)
- Zero Trust Network Access (ZTNA)
- Software Defined Wide-Area Network (SD-WAN)

SASE aims to enable people and businesses to connect and work as quickly and securely as possible by functioning everywhere, which means that it can follow data, applications, and people that have moved to the cloud. SASE addresses cloud-enabled threats and data risks for personal instances of managed applications, thousands of shadow IT applications, and cloud services.

ZTNA is a key component of SASE that enforces the premise that no one is blindly trusted and allowed to access company assets until they’ve been validated as legitimate and authorized. It supports the implementation of least privilege access, which selectively grants access only to resources that people or groups of people require, nothing more. By giving ZTNA adaptive access capability, SASE boosts ZTNA and harmonizes policy administration and decision with other SSE components while still maintaining distributed policy enforcement.

SASE is a comprehensive approach to cloud-based security that offers many benefits to organizations. By using shared services to power high-level security functions and providing continuous monitoring, policy-based administration, and adaptive access capability, SASE can help organizations stay ahead of cloud-based threats and protect their sensitive data and applications.

Call for a free consultation: 888-440-7126 or learn more at www.Hughes.com/cybersecurity