Solution Brief

Symantec
A Division of Broadcom

SASE: New Architecture for a New Era

Challenge

What is the expected life of a cyber-security architecture? No architecture comes with a warranty; but a decade or more is a long run. Nothing digital is set in stone. The classic paradigm of guarding data centers and network perimeters has run its course, a victim of too many costly intrusions and a perceived inability to meet the requirements of digital transformation, mobile access, and cloud-native applications.

Opportunity

In the place of that old paradigm, our industry is rapidly coalescing around Secure Access Service Edge (SASE), a cloud-based security architecture that prioritizes data protection over hardware or even company networks. SASE combines networking and security-as-a-service capabilities.

Benefits

In this solution brief, we describe how to get started with SASE and discuss where SASE fits into a broader set of solutions. Of course, with a new architecture, the focus shifts from fixing legacy problems to solving for the challenges of where computing is headed: to the cloud and the edge.

Symantec Enterprise looks toward the future.

Implications

In the 5G-powered, edge processing world of the near future, applications are latency-sensitive and data flies around at speeds 100x greater than today. This speed requires a lot of computing resources and bandwidth, all while being fully secured. Information must be instantaneously encrypted and decrypted as it shifts from edge to data lake, and again when it is replicated in a cloud-based data set for an entirely different purpose, such as training or business analytics.

Protecting data in flight between endpoint and service is one of the primary objectives of SASE. If you make a strategic shift from protecting data centers to controlling centers of data, it is worth asking, what is the difference?

According to Gartner, "Network security architectures that place the enterprise data center at the center of connectivity requirements are an inhibitor to the dynamic access requirements of digital business."[1] To our view, the alternative that Gartner advocate is consolidating networking and security-as-a-service capabilities into SASE. Secure access cloud services must not be landlocked by company networks or hamstrung by backhaul connections through corporate data centers.

In SASE, security policies are tied to validating identities rather than the protection of IP addresses; and identities are no longer based on location. Establishing control over whom and what accesses cloud-based services becomes your first mission, particularly when it is key to enforcing security in another infrastructure.

First Comes the Proxy

You cannot protect a digital business without first establishing both visibility and control over all web traffic. To achieve this, you need a single termination layer to process this traffic.

Since the majority of all web traffic is encrypted, your termination layer must also support the ability to handle encrypted traffic to preserve visibility and control. Once web traffic has been decrypted, you can block malware and other malicious threats, apply security policies, and enforce data compliance requirements.

[1] Gartner "The Future of Network Security Is in the Cloud," Neil MacDonald, Lawrence Orans, Joe Skorupa, 30 August 2019.

Features

Secure Web Gateways take a giant first step toward SASE because it provides the following features:

- Cyber-attack prevention and detection:
  - Implements white lists and black lists .
  - Works with DLP and sandboxing tools; considers file reputation analysis.
- Visibility into all web traffic:
  - Monitors and logs transactions.
  - Supports cloud apps to ensure compliance.
- Lower total cost of ownership (TCO) for security.
  - Improves the overall performance and availability of your business apps and media, with bandwidth management, content caching, traffic optimization, and streaming media splitting and caching features.

First Comes the Proxy (cont.)

We know this because we have literally decades of experience with proxy protection. Our Secure Web Gateway (SWG) enables in-depth inspection of web and encrypted web traffic required to uncover and protect against the web threats that may target your organization.

If SWG detects a potential issue, it may send the payload to a data loss prevention (DLP) solution, or to a sandbox for behavioral analysis, detection and remediation. A proxy is perfectly positioned to handle encrypted traffic. Decrypting SSL requires negotiating and completing a full SSL/TLS handshake, which can create issues for non-proxy solutions. With the advent of TLS1.3, managing encrypted traffic is further complicated for non-proxy architectures, such as next-generation firewalls (NGFW), since there is no way to fully inspect the initial TLS handshake.

Next Steps

Will every organization adopt SASE? Gartner projects, "By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018."[2]

While adoption is gaining momentum, it might take half a decade or more for SASE to become the predominant cyber-security architecture. Some of the pieces, such as SWG, are more mature than others. The Symantec portfolio of SASE solutions will act in harmony to provide industry-leading architecture that meets or exceeds your security KPIs.

For more information, please visit our site at broadcom.com/products/cyber-security.

[2] Gartner "The Future of Network Security Is in the Cloud," Neil MacDonald, Lawrence Orans, Joe Skorupa, 30 August 2019.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com