WHITE PAPER

Symantec® Data-Centric SASE

Cost-Effective, Hybrid-Capable Security Built Upon Zero Trust Principles

TABLE OF CONTENTS

Enterprise Digital Transformation Demands a Modern Security Architecture

Many enterprises are undergoing a digital transformation: serving more customers online, migrating applications to cloud platforms, and integrating suppliers into digital supply chains. They are also giving employees more options to work at home, in remote offices, and at customer locations.

Part of the transformation is moving away from outdated network security models in which the entire security stack is housed in corporate data centers and accessed by workers in large corporate offices. These models were not designed to provide mobile and remote workers with convenient, secure, high-performance access to applications and data in the cloud—or to ensure secure access to existing on-premises infrastructure.

A cloud-delivered security stack is the preferred path for digital transformation, but enterprises find challenges here too. They fear that managing a disparate patchwork of cloud services can ultimately increase the cost and complexity of network security. Today, IT organizations seek a new model for delivering low-latency network and security services for employees in distributed, cloud-oriented, digital businesses. One of the leading contenders is the Secure Access Service Edge (SASE) architecture, but the security footprint of a large enterprise is often quite complex. Implementing SASE the right way should not be done in haste. More importantly, an enterprise must not abandon the principles of Zero Trust in the pursuit of operational efficiency. In this white paper we offer an overview of SASE and a discussion of how Symantec® by Broadcom operationalizes the concepts behind SASE.

What is SASE?

The most complete articulation of SASE comes from the industry analyst firm Gartner, in the research note *The Future of Network Security Is in the Cloud*. The note was written by Neil MacDonald, Lawrence Orans, and Joe Skorupa and published in August 2019. They, and other industry analysts and vendors after them, describe SASE as a combination of concepts, principles, and technologies designed to improve network performance and security in a world where users are remote and mobile and where they access applications and data spread across corporate data centers and multiple cloud platforms.

CONVERGENCE REDUCES THE NUMBER OF SEPARATE PRODUCTS, VENDORS, AND ENDPOINT AGENTS THAT MUST BE MANAGED, AND OPTIMIZES THE USE OF NETWORK RESOURCES TO IMPROVE APPLICATION PERFORMANCE FOR USERS.

SASE has several core concepts:

- Convergence of cloud-hosted network services and network security solutions
- Support for key principles of a Zero Trust security model
- Extensive Points of Presence (POPs) and peering for optimal performance
- Simplified management and monitoring

Convergence of Cloud-Hosted Network and Network Security Services

One of the fundamental concepts of SASE is the convergence of network services, such as software-defined wide area networks (SD-WAN), with cloud-hosted security technologies, such as secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), browser isolation, Zero Trust network access (ZTNA), and SSL inspection.

Convergence in this context means a high degree of integration, so that network services and network security services can share information, use each other's work, and apply network and security policies consistently, in real time, on a high-performance cloud architecture. For example, convergence might allow for a smooth process where network traffic for a mission-critical application could be decrypted, inspected for malware, identified as latency sensitive, and routed to a cloud platform using the fastest and most reliable path available.

Another benefit of convergence is that it can improve performance and reduce latency by enabling single-pass inspection of network traffic. For example, instead of having multiple security services decrypt and re-encrypt SSL/TLS traffic from a web application in a chain, the service could decrypt the traffic once, feed it to multiple security services for inspection and analysis in parallel, and then re-encrypt the traffic once for forwarding to users.

Convergence also reduces the number of separate products, vendors, and endpoint agents that must be managed, and optimizes the use of network resources to improve application performance for users.

Support for Zero Trust Security Model

Zero Trust principles complement the SASE framework in three ways:

- Every request for access to a corporate resource must be assessed (if possible, transparently to the user) based on multiple factors such as the identity and role of the user, the profile and location of the device, and the sensitivity of the application and data being requested.
- A user's access to resources should be limited by the level of confidence established during the assessment.
- The level of confidence and access to resources should be continuously reassessed during the session based on the user's behaviors.

The implementation of the SASE Framework should support Zero Trust security to ensure that employees and other users can have convenient access to corporate resources from anywhere, on any device, while minimizing the risk of data breaches by threat actors.

A SASE SOLUTION MUST INCLUDE A GLOBAL FABRIC OF POPS TO THE INTERNET, AS WELL AS PEERING RELATIONSHIPS WITH MAJOR CLOUD PLATFORM AND APPLICATION PROVIDERS TO REDUCE LATENCY AND DELIVER HIGH PERFORMANCE.

Extensive Points of Presence and Peering for Optimal Latency

Gartner analysts also point out that, to provide employees with a positive user experience and unrestrained access to cloud-based resources, a SASE solution must include a global fabric of POPs to the Internet, as well as peering relationships with major cloud platform and application providers to reduce latency and deliver high performance.

Simplified Management and Monitoring

Finally, a SASE infrastructure offers simplified management and monitoring in order to handle the growing number of remote and mobile users and devices and the expanding level of services that need to be provided to them locally and in the cloud. For example, it should be possible to offer more services on endpoints and edge devices with fewer agents. A single management console should be able to log and present information from multiple network and network security services.

The Advantages of Data-Centric SASE

Traditional data center-centric network and security models are becoming increasingly complex and costly in a cloud-centric world, while complicating the end-user experience and reducing productivity. They also constrain scalability and flexibility. A data-centric SASE architecture is designed to address those issues while providing several concrete benefits, and ultimately, the most secure form of data protection.

Improving Network and Application Performance

Application intelligence and policy enforcement at the network edge improve network and application performance by enabling employees and devices to connect directly to the Internet. This minimizes the number of hops to applications and services by leveraging service provider backbones instead of the public Internet, and by using traffic management features to provide high quality of service for latency-sensitive applications.

Providing Stronger, More Consistent Security

The convergence of network and network security services means security policies can be applied consistently across multiple security technologies and all parts of the business, regardless of where data is hosted, on-premises, in the cloud, or in hybrid environments. Single pass decryption and inspection reduces network latency and can ensure that all traffic is inspected by all security tools (subject to policy).

WITH SASE, ORGANIZATIONS CAN MANAGE NETWORK AND SECURITY SERVICES CENTRALLY, IN A UNIFIED FASHION, WITH FEWER ENDPOINT AGENTS.

Enabling Zero Trust Network Access

A key capability within a SASE Framework is the ability to allow remote and mobile employees and devices to access cloud-based, hybrid and on-premises resources from anywhere, based on permissions appropriate to their identities, devices, and the context of their requests and data being requested, without the use of costly VPNs.

Decreasing Complexity and Simplifying Management

With SASE, organizations can manage network and security services centrally, in a unified fashion, with fewer endpoint agents. They may also be able to consolidate the number of network and security tool vendors to simplify administration and coordination.

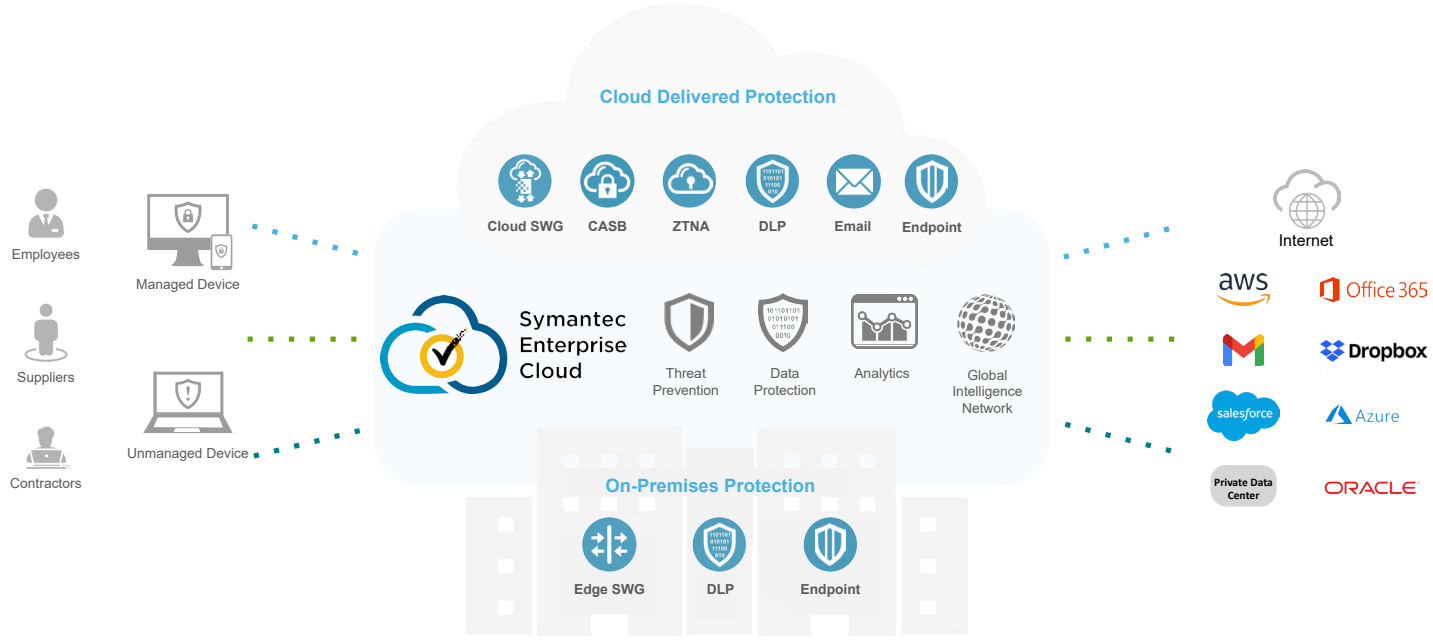
Reducing Costs and Increasing Productivity

SASE offers multiple avenues to cost savings, including reducing reliance on expensive MPLS connections to backhaul network traffic from branch offices to data centers. It also allows organizations to consolidate many security and network edge devices into fewer physical and virtual appliances. The productivity of network and security teams improves because management and configuration are simplified. Making network access for end users simpler and more uniform increases employee productivity and satisfaction.

Symantec Data-Centric SASE: Convergence

One of the core characteristics of SASE is the convergence of network services and network security technologies. The following figure shows how Symantec integrates a wide range of these technologies.

Figure 1: Symantec SASE Enforces Zero Trust Policies for Applications on Cloud Platforms and in Data Centers



Secure Web Gateway: A Comprehensive Selection of Integrated Security Technologies

Symantec Cloud Secure Web Gateway (SWG) is the foundation of the Symantec SASE solution. It integrates multiple advanced security technologies and makes them available from the cloud. Cloud SWG, along with the entire Symantec security stack, runs on the Google high-performance, global cloud platform. Google Cloud provides one of the largest and best-connected compute platforms in the world, that is edge-optimized for remote employees. Symantec Cloud SWG running on Google infrastructure scales rapidly to meet the demands of new customer workloads, for example reducing onboarding lead times to mere hours instead of days or weeks. The software-defined infrastructure heals much quicker than the previous generations of dedicated PoP infrastructure used by other vendors, which rely on physical network components to scale. Finally, being a truly cloud-native application means that Symantec engineers can focus on delivering security while Google delivers best-in-class performance and scale to optimize the Symantec security stack.

Secure Web Gateway and SSL/TLS Decryption

Symantec Cloud SWG is built around an industry-leading security platform that filters unwanted Internet traffic, detects malware and malicious code, and decrypts SSL/TLS-encrypted traffic for sharing with other security tools. It also extracts and inspects files, identifies traffic from individual applications, and applies appropriate security, compliance, and QoS policies to each application stream.

Cloud SWG is built on a forward proxy architecture that guarantees that 100% of web traffic can be authenticated, decrypted, scanned, and analyzed before it is released to employees. It also provides much better performance than next-generation firewalls at a lower cost, when features like decryption and file extraction are turned on[1].

[1] For a detailed discussion of the importance of a proxy architecture, see the white paper: Next Generation Secure Web Gateway: The Cornerstone of Your Security Architecture.

SYMANTEC CLOUD FIREWALL SERVICE (CFS) IS BASED ON INDUSTRY-LEADING NGFW TECHNOLOGY.

Cloud Access Security Broker

Cloud SWG is integrated with Symantec CloudSOC® technology, which allows organizations to control access to data hosted on SaaS workloads. Administrators can also detect and block access to cloud and other unauthorized (shadow IT) applications and enforce controls such as malware scanning on file downloads.

Cloud Firewall Service

Symantec Cloud Firewall Service (CFS) is based on industry-leading NGFW technology. CFS performs deep inspection and gives organizations control of network traffic over all ports and protocols, not just selected protocols on a few ports. It identifies traffic from different applications and can apply policies based on applications, user groups (through tight integration with user identity management features in Cloud SWG), and factors such as whether users are roaming or are at specific locations. CFS can apply firewall rules based on user behavior, permissions, and geolocation. It also provides single-pane-of-glass firewall management and centralized reporting through the Cloud SWG portal.

Web Isolation

Symantec Web Isolation defends against ransomware, malware, and phishing attacks that target browsers. Users are allowed to access uncategorized and potentially risky websites, but pages from those sites are executed and rendered in a remote, secure, disposable container. Only a safe rendering of information is sent to users' browsers, so ransomware and malware can not be installed or executed on employee endpoints. To reduce the chance of credential compromise, web pages can be rendered in read-only mode, to prevent users from submitting corporate credentials and other sensitive information. Also, links in emails to malicious websites are rendered harmless so they cannot deliver malware or ransomware to email recipients' machines.

SYMANTEC WEB ISOLATION DEFENDS AGAINST RANSOMWARE, MALWARE, AND PHISHING ATTACKS THAT TARGET BROWSERS.

Data Loss Prevention

Symantec Data Loss Protection (DLP) solutions monitor and analyze web, application, and email traffic to prevent sensitive content from leaving the organization or being accessed by risky users or devices. This behavior enforces centrally managed security and compliance policies and reduces the chance of a data breach. Also, the Symantec DLP solution can detect information being sent to shadow IT cloud applications, and scan cloud-based applications to detect sensitive files uploaded by employees through non-corporate links (out-of-band access).

Content and Malware Analysis with Sandboxing

Sandboxing allows the actions of suspicious files and malware to be observed and analyzed in an isolated space in our cloud platform. It reveals malicious behaviors and exposes zero-day threats without risk to your endpoints and systems. Symantec Content Analysis provides advanced features such as the use of multiple analysis techniques (including static, behavioral, and YARA rule analysis), memory exploit detection, sandbox avoidance detection (including delayed delivery), and the use of custom sandbox images. It also takes advantage of the extensive Symantec threat intelligence database to more quickly identify and classify threats.

Zero Trust Network Access

Symantec Zero Trust Network Access (ZTNA) provides point-to-point connectivity at the application level, cloaking all resources from the end-user devices and the Internet. The network-level attack surface is entirely removed, leaving no room for lateral movement and network-based threats. Symantec ZTNA makes it easy to apply fine-grained access and activity policies to prevent unauthorized access to corporate resources. Organizations can secure employee, partner, and BYOD access by implementing continuous, contextual authorization for the enterprise, leveraging user, device, and resource-based context.

SD-WAN Partner Ecosystem

Symantec is integrated with industry-leading SD-WAN products and network services that are tested to ensure technologies interoperate with Symantec web security solutions.

Advantages of Convergence and Integration

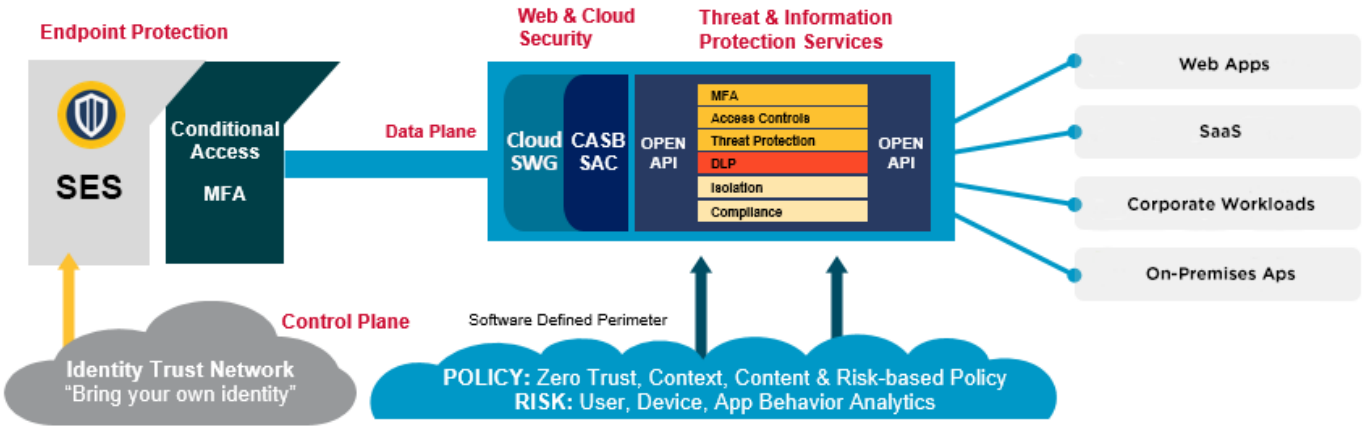
The integration of security and network technologies in the Symantec Cloud Platform, based on the SASE principles, allows the components of the platform to share information, strengthen each other's capabilities, and enforce security policies consistently. This also reduces complexity and simplifies management, because administrators can monitor activities and set policies in one place, for users, applications, and data across all locations. In addition, security and network features can work together to improve performance and lower cost, for example by routing security-related traffic efficiently using the fastest and most reliable networking platform through Google Cloud.

Symantec Data-Centric SASE: Enabling Zero Trust and Continuous Monitoring

Another key capability of SASE is support for Zero Trust security. The key principles include assessing every request for access to a corporate resource to determine how much the request can be trusted, limiting access based on that level of trust, and continually reassessing the level of trust based on the user's behavior.

Our approach to using SASE for Zero Trust security is shown in the following figure.

Figure 2: The Symantec Approach to Zero Trust Network Access



Symantec Endpoint Security (SES) provides a single endpoint agent for attack surface reduction, attack prevention, breach prevention, and Endpoint Detection and Response (EDR). It can also act as a Zero Trust agent, collecting information about the user and the device, supporting multi-factor authentication, and providing secure routing and conditional access capabilities.

Both Symantec ZTNA and CloudSOC CASB are cloud-based services that provide granular access management and enforce Zero Trust policies for applications on cloud platforms and in on-premises data center environments. When Symantec ZTNA receives requests from endpoints to access corporate resources, it analyzes user, device, location, and authentication information from the endpoints and connects to identity platforms to obtain the roles assigned to the users. It also assesses the sensitivity of the applications and data being accessed and the operations requested. Symantec ZTNA then allows the users to connect to only the specific resources they are authorized to access. Finally, it continuously uses analytics to monitor user behaviors and reassess trust. Symantec CloudSOC Mirror Gateway allows similar protection to be extended to unmanaged devices (for example, BYOD) without the need for an agent.

Advantages of Support for ZTNA

Our approach to supporting Zero Trust security offers several valuable benefits:

- A simple, consistent, experience for users in all locations when they request access to corporate resources and the ability to eliminate costly VPNs that weren't designed for broad use by the entire user population.
- A reduction in data breaches, because organizations can apply fine-grained policies for controlling access to corporate resources based on user identities and permissions, device state and location, the sensitivity of resources, and other factors that determine trust.
- Assurance that all network traffic, including traffic originating on office networks, will be monitored, inspected, and routed based on policies.

Symantec Data-Centric SASE: Network Support for Security at the Network Edge and in the Cloud

As mentioned earlier, when employees working at home and in remote offices want to connect to cloud applications, it does not make sense to backhaul their network traffic to central corporate data centers for inspection and policy enforcement. That approach complicates the user experience by requiring users to create a VPN connection for every action. It also increases the latency of the requests by routing them using the VPN to the on-premises data center before sending them to the Internet.

THE SYMANTEC SASE SOLUTION HAD 144% GREATER THROUGHPUT AND 62% LOWER LATENCY THAN TRAFFIC GOING OVER THE PUBLIC INTERNET.

To improve the experience and productivity of home and branch office employees, they should be able to connect directly to the cloud. That requires placing security services somewhere on the direct path between the endpoints and the applications without rerouting traffic to a central site.

In addition, latency-sensitive applications such as collaboration, VoIP, media streaming, and video conferencing demand even more: a high-performance, low-jitter network backbone that is reliable and scalable. Performance and scalability will become even more important as IoT applications start to go into production.

Preceding sections of this white paper discussed Symantec solutions that provide security on the network edge: delivered from the cloud, through the closest edge location to each user's location, home or branch office. We also highlighted some Symantec offerings that provide security services on the endpoint itself.

Symantec offers a high-performance, highly scalable cloud infrastructure built on Google Cloud, with a global presence and industry-leading peering relationships with Content Delivery Network (CDN) providers. In fact, the Tolly Group tested the Symantec SASE security stack running on Google Cloud against direct traffic to the Internet that didn't receive any security inspection. The Symantec SASE solution had 144% greater throughput and 62% lower latency than traffic going over the public Internet. This means that Symantec customers not only get the expected benefit of full inspection and threat protection, they also experienced a significant improvement in performance.

Advantages of Symantec Security Intelligence at the Edge and in the Cloud

The Symantec high-performance cloud infrastructure provides many advantages:

- Avoid the performance hit and extra cost of backhauling network traffic to the data center for inspection and policy enforcement.
- Improve application performance for any user—in central corporate offices, branch offices, or any remote location.
- Deliver dramatically faster performance for global applications by leveraging the Google backbone network and ubiquitous POP coverage from extensive ISP and CDN peering partnerships.
- Best-in-class visibility into threats, provided by the world's largest civilian threat intelligence network.
- The most complete SASE portfolio from a single vendor, built on the market-leading Secure Web Gateway architecture.
- Flexible options allow on-premises, full cloud or customized hybrid deployments that will scale as business needs change, utilizing simple user-based licensing.

ONE OF THE KEY GOALS OF SASE IS TO REDUCE COMPLEXITY AND DRAMATICALLY SIMPLIFY THE MANAGEMENT AND MONITORING OF NETWORK AND SECURITY SERVICES.

Symantec and SASE: Simplified Management and Monitoring

One of the key goals of SASE is to reduce complexity and dramatically simplify the management and monitoring of network and security services.

One well-known source of aggravation for IT administrators is the task of deploying and managing multiple agents on each endpoint. On many endpoints Symantec Enterprise Agent can reduce the number of agents to one. Other Symantec solutions, such as ZTNA, can leverage that agent but can also operate with no endpoint agents at all, providing support for unmanaged devices as well as significantly reducing deployment and maintenance costs.

Symantec has a centralized management console for our SASE solution that allows security and operations teams to monitor and manage policy and administration for SWG, endpoint, and other key security components, easing the administrative burden and ensuring consistent protection. In a similar way, Symantec Unified Policy Enforcement (UPE) and integration between Cloud SWG and CloudSOC lets administrators manage a common set of web and data security policies that are applied to both on-prem and cloud security solutions, simplifying security administrator's workloads.

Symantec also gives organizations the opportunity to work with a single vendor with unmatched capability to develop their SASE architecture, a partner with the resources and experience to deliver effective security and network products today and to deliver on innovative concepts like SASE going forward.

Advantages of Simplified Monitoring and Management

With simplified monitoring and management, organizations can respond faster to threats and free network and security staff from routine tasks so they can focus on important issues.

THE TOLLY GROUP VALIDATED THAT SYMANTEC HAS ALL THE NECESSARY COMPONENTS FOR A COMPLETE SASE SOLUTION.

Summary

SASE has gained wide acceptance among leading-edge IT organizations as well as industry analysts and independent network and security experts. It promises to improve network and application performance, strengthen security, reduce complexity, and reduce IT and network costs, as well as fostering business agility.

Symantec has long been a leader in cloud and network security across SWG, CASB, and DLP with an integrated network and security platform. This foundation of core security technologies along with other critical components such as, full SSL/TLS decryption, Web Isolation, ZTNA, Content Inspection, and Sandboxing explain why the Tolly Group validated that Symantec has all the necessary components for a complete SASE solution. We lead the way in operationalizing the core concepts of SASE, including:

- Convergence of network and network security services
- Support for Zero Trust security principles
- Network support for security at the network edge and in the cloud
- Simplified management and monitoring

If you are interested in learning more about how Symantec solutions can help you evolve to a SASE architecture while improving security and compliance, increasing productivity, and reducing costs, please contact your Symantec representative or visit www.broadcom.com/SASE

SED-SASE-WP102 October 4, 2023