Analyst Brief

Tolly.

#224138

August 2024

Commissioned by Broadcom, Inc.

Symantec Security Service Edge (SSE) Portfolio

Comparison to Industry SSE Framework

EXECUTIVE SUMMARY

The growing reliance of businesses large and small on cloud infrastructure has, naturally, focused attention on the security of that infrastructure. To reflect this new focus, industry analysts coined the term SASE, Secure Access Service Edge, and defined the key elements covered in the framework which is broken down into two areas: WAN edge services and cloud-hosted security services which analysts call the Security Service Edge (SSE).

Broadcom commissioned Tolly to examine its portfolio of Symantec network security solutions and document how they encompass the SSE elements as defined by analysts. Broadcom's security components can work with any SD-WAN solution.

The Tolly analysis shows that the Symantec network security portfolio provides solutions within each of the SSE categories and provides services beyond the main components. See Table 1 for a summary. The body of this paper will explore each area in turn.

THE BOTTOM LINE

Symantec SSE provides:

1. Long-standing prominence in the network security space
2. All elements outlined in the Industry framework
3. Additional data awareness capabilities beyond the industry framework
4. Open solution that works with any SD-WAN vendor

SSE Analysis
Symantec Solutions Compared with Industry Framework

Gartner Framework Component	Functional Area	Symantec Solution
Secure Web Gateway	Secure Web Gateway	Symantec Network Protection
	URL Threat Prevention & Classification	Symantec Network Protection
	Advanced Content Analysis (Malware sandboxing)	Symantec Network Protection
CASB	Cloud Application Security Broker (CASB)	Symantec Network Protection (Advanced capabilities though Symantec DLP Cloud)
ZTNA/VPN	Zero Trust Network Access	Symantec Network Protection
FWaaS	Cloud Firewall	Symantec Network Protection
Remote Browser Isolation	Remote Browser Isolation	Symantec Network Protection
Decryption	SSL Inspection	Symantec Network Protection
Sensitive Data Awareness	Data Loss Prevention (DLP)	Symantec DLP Cloud

Source: Tolly, August 2024

Table 1

Secure Web Gateway

The Secure Web Gateway (SWG, pronounced "swig") is the core element of SSE and consists of multiple sub-components. As the name implies, it is the primary point where internal, corporate users' traffic transits to the internet. The SWG is the proxy between end-users and internet resources.

Analysts define two additional categories within SWG - URL Threat Prevention, and Advanced Content Analysis (Malware sandboxing). Symantec Network Protection[1] implements all of the industry-defined elements and more. The first is the primary SWG function that acts as an intercept point for all inbound and outbound traffic.

The Symantec SWG solution provides the core web proxy as well as additional functionality. Broadly stated, Broadcom notes the solution's role is to "identify malicious websites and payloads and to control access to sensitive content. … a broad feature-set to authenticate users, filter web traffic, identify cloud application usage, provide data loss prevention, deliver threat prevention, and ensure visibility into encrypted traffic." To provide flexibility to customers, it can be deployed in a traditional, on-prem installation or be accessed via the cloud. Symantec Universal Policy Enforcement provides support for both on-prem and cloud, enabling seamless management or migrations. Symantec gathers threat intelligence from all managed endpoints and integrates it into Symantec's Global Information Network.

URL Threat Prevention & Classification

This feature is provided by the Symantec Network Protection solution. Protection is provided in real time. Symantec web filtering categorizes URLs into some 80 categories that include 12 different security categories. Symantec notes that this categorization makes the system easily managed by security and IT admins. The very granular policy control allows

Symantec SSE Solution Highlights

Functional Area	Symantec Solution	Summary/Key Features
Secure Web Gateway	Symantec Network Protection	Core SSE security element. Proxy between users and internet, filter web traffic.
URL Threat Prevention & Classification	Symantec Network Protection	Leverages Symantec Global Intelligence Network to classify URLs and block malicious traffic.
Advanced Content Analysis	Symantec Network Protection	Provides multi-layer file analysis and isolated sandbox analysis of potentially malicious attachments to provide full protection for end user devices.
Cloud Application Security Broker (CASB)	Symantec Network Protection	Network Protection recognizes over 45,000 different applications and provides basic application access through the Proxy. More granular CASB controls are available through Symantec DLP cloud.
Zero Trust Network Access	Symantec Network Protection	Secure access to private applications and resources, without the need of a VPN. Integrated with multi-factor authentication.
Cloud Firewall	Symantec Network Protection	Full traditional firewall services integrated into cloud platform to inspect non-standard traffic.
Remote Browser Isolation	Symantec Network Protection	Full protection for end-user devices by executing web pages in a remote browser instance, sending only a safe, visual rendering of the site to the end user.
Decryption	SSL Inspection	Enhance security by inspecting encrypted traffic. Tap support can feed decrypted traffic to multiple tools.
Data Loss Prevention (DLP)	Symantec DLP Cloud	Symantec DLP enables a consistent data protection policy across SWG, ZTNA, CASB, eMail and endpoint control points.

Source: Tolly, August 2024

Table 2

[1] Table 3 contains web links to each Symantec product referenced in this report where more information can be found.

organizations to implement web filtering policies that are most appropriate for their organizations.

Advanced Content Analysis

This feature is provided by the Symantec Network Protection solution. Not every threat can be identified via a "fingerprint" or by referencing a list of malware files. Advanced detection often requires that files be subjected to a more detailed, multi-layer analysis.

Symantec provides content analysis and cloud-based sandboxing. This is important because this protects end-users from potentially malicious content. By "sandboxing" the content - isolating the content outside the user's environment - there is no possibility that malware can penetrate or infect the end-user's device. File attachments, for example, can be opened and examined before being allowed in to the end user's device, thus providing enhanced security.

CASB

Symantec Network Protection provides essential visibility and control for maintaining security when users access cloud-based applications. Symantec Network Protection can recognize over 45,000 different cloud apps and provides deep visibility across apps, email, and web traffic. It provides for logging access to cloud resources which is a mandatory function for environments where access needs to be audited. The solution also provides for automated alerts and policy-defined responses for administrator and system-defined situations.

Additional, fine-grained controls of cloud applications is also available through CloudSOC CASB found in Symantec DLP Cloud.

ZTNA

This function is included in Symantec Network Protection.

ZTNA provides secure access to private applications and resources, without the need of a VPN. It does not require agents or appliances and can be easily deployed to individual users, groups, sites or even outside partners.

It can integrate easily with multi-factor authentication and corporate identity provider (IdP) components. Furthermore, Symantec ZTNA can demonstrate compliance with a globally distributed and certified service, such as ISO 27001 or SOC 2 Type II, among others.

FWaaS

Cloud firewall is delivered as part of Symantec Network Protection. The service can be used to define firewall policies to control all TCP or UDP traffic based on IP addresses, destination ports, locations, users and groups.

The service provides traditional firewall services such as enforcing acceptable network use policy on roaming endpoints or restricting use of administrative tools that use protocols such as SSH.

The configuration of policies and the reporting on usage and site blocking are integrated into a single administration control panel along with the other Symantec Network Protection functions.

Remote Browser Isolation

Symantec offers full Remote Browser Isolation (RBI) in Symantec Network Protection, but also includes High Risk Isolation (HRI) as a component of Symantec Web Protection.

Certain websites might be in the gray area between "allow" and "block." The user might need to see the content but there can still be a risk that it is a malicious site and/or will try to load unwanted code into the user's browser or operating system environment.

When Symantec evaluates a website, it sets a risk level of 1 to 10 for each URL. Any sites evaluated to be a risk level 5 or higher are processed by HRI.

In such cases, the web content is executed remotely (i.e., not in the user's machine) and only safe, rendered content is sent to be displayed on the user's device. For additional protection, security administrators can mark certain sites as "read-only" - thus prohibiting any data entry into potentially harmful sites.

Decryption/SSL Inspection

Symantec provides encryption/decryption (encrypted traffic management) via Symantec Network Protection.

Within the bounds of privacy regulations, this feature allows the security admin to identify SSL/TLS (i.e., encrypted) traffic no matter what IP port it is using and no matter the application.

Selective decryption can be used for situations where privacy regulations prohibit global decryption.

Administrators determine decryption policies and the decrypted traffic to be fed to multiple third-party monitoring and/or logging systems for further analysis and/or archival.

Sensitive Data Awareness (DLP)

This function is provided by Symantec and is deployed in conjunction with Symantec CloudSOC CASB.

Symantec DLP Cloud is integrated with CloudSOC CASB to find sensitive data at rest or in motion. User behavior and application risk levels are used when determining data access rights and applying protection controls.

Importantly, Symantec DLP Cloud can enforce access policies and provides ready-made templates and policies that cover PII, PCI, and HIPAA. In addition, security admins can build custom policies for requirements unique to the organization.

Symantec SSE Solutions Web Links

Category	Functional Area	Symantec Solution	URL Reference
Secure Web Gateway	Secure Web Gateway	Symantec Network Protection	https://www.broadcom.com/products/cyber-security/network/web-protection/cloud-secure-web-gateway
	URL Threat Prevention & Classification	Symantec Network Protection	https://www.broadcom.com/products/cybersecurity/network/web-protection/intelligence-services
	Advanced Content Analysis	Symantec Network Protection	https://www.broadcom.com/products/cybersecurity/network/web-protection/atp-content-malware-analysis
CASB	Cloud Application Security Broker (CASB)	Symantec DLP Cloud	https://www.broadcom.com/products/cybersecurity/information-protection/cloud-application-security-cloudsoc
ZTNA/VPN	Zero Trust Network Access	Symantec Network Protection	https://www.broadcom.com/products/cybersecurity/network/network-protection/zero-trust-network-access
FWaaS	Cloud Firewall	Symantec Network Protection	https://docs.broadcom.com/docs/web-protection-cloud-firewall-service
Remote Browser Isolation	Remote Browser Isolation	Symantec Network Protection	https://www.broadcom.com/products/cyber-security/network/web-protection/web-isolation
Encryption/ Decryption	Encryption/Decryption	Symantec Network Protection	https://www.broadcom.com/products/cyber-security/network/encrypted-traffic-management
Sensitive Data Awareness	Data Loss Prevention (DLP)	Symantec DLP Cloud	https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention

Source: Tolly August 2024

Table 3

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 35 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at info@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

cz-12b-wt-2024-10-02-VerE