Analyst Brief

#224130

August 2024

Commissioned by
Broadcom, Inc.

VMware VeloCloud Secure Access Service Edge (SASE) Portfolio

Comparison to Industry Definition of SASE Architecture

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 at Gartner coined the term SASE, Secure Access Service Edge, and defined the key elements covered by the Gartner SASE framework which is broken down into two areas: WAN edge services and cloud-hosted security services which the industry calls the Security Services Edge (SSE).

Broadcom commissioned Tolly to examine its portfolio of SASE services that address the general industry definition and expand coverage use cased in edge modernization, data-centric security, digital experience management.

The Tolly analysis shows that the VMware VeloCloud SASE solution covers each of the industry's generally-accepted SASE categories and provides services beyond those main components. See Table 1 for a summary. The body of this paper will explore each area as well as some related features.

THE BOTTOM LINE

VeloCloud SASE provides:

1 Long-standing prominence in the network security space

2 All key requirements of a SASE architecture

3 Additional data awareness capabilities beyond the industry definition

4 Open solution that helps start the SASE journey at each customer's pace integrating with existing third-party solutions

VeloCloud SASE Solution Highlights

Industry Framework Component	Functional Area	VeloCloud SASE Solution
Secure Web Gateway	Secure Web Gateway	Symantec SSE for VeloCloud
	URL Threat Prevention & Classification	Symantec SSE for VeloCloud
	Advanced Content Analysis (Malware sandboxing)	Symantec SSE for VeloCloud
CASB	Cloud Application Security Broker (CASB)	Symantec SSE for VeloCloud
Zero Trust Remote Access	Path Optimzed access based on Zero Trust Principles	VeloCloud SD-Access
FWaaS	Cloud Firewall	Symantec SSE for VeloCloud
Remote Browser Isolation	High Risk Browser Isolation	Symantec SSE for VeloCloud
SSL Decryption	SSL Inspection	Symantec SSE for VeloCloud
Sensitive Data Awareness	Data Loss Prevention	Symantec SSE for VeloCloud
SD-WAN Connectivity	Dynamic Multi-Path Optimization	VeloCloud SD-WAN
	Application recognition and Traffic Steering	VeloCloud SD-WAN
Branch Firewall	IDS and IPS	VeloCloud SD-WAN
	URL Filtering and Malicious IP Filtering	VeloCloud SD-WAN
Simplified Management	Zero Touch Provisioning	VeloCloud SD-WAN
	Automated On-Ramp to Symantec SSE	VeloCloud SD-WAN
	AIOps for User Experience Management	VMware Edge Network Intelligence

Source: Tolly August 2024

Table 1

Report link: https://www.tolly.com/publications/detail/224130

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.

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." Symantec gathers threat intelligence from all managed endpoint and integrates it into Symantec's Global Information Network.

URL Threat Prevention & Classification

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 allows the system to be managed easily by security and IT admins. The very granular policy control allows organizations to implement web filtering policies that are most appropriate for their organizations.

Advanced Content Analysis

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 into the end user's device, thus providing enhanced security.

CASB

CASB is an essential tool for maintaining the security of cloud data. Symantec CASB can recognize over 45,000 different cloud apps and provides deep visibility across apps 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.

The solution integrates tightly with the DLP function, discussed below.

Zero Trust Remote Access

This function is provided by VeloCloud SD-Access.

VeloCloud SD-Access allows creation of private, secure, high performance path-optimized overlay networks. The cloud delivered solution connects remote users, devices, and services located anywhere. The solution uses principles of Zero Trust going beyond user credentials to include device posture (certificate, domain, registry, presence of AV/FW/MDM Agent, disk encryption), geo location, time of day, and device OS type for remote user access.

FWaaS

Firewall as a 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 Web Protection functions.

Remote Browser Isolation

Symantec SSE for VeloCloud supports High Risk Isolation (HRI).

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, based on a customer's policy.

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/TLS Inspection

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.

Sensitive Data Awareness (DLP)

Data Loss Prevention protects sensitive data in motion and prevents this data from leaving the enterprise perimeter. User behavior and application risk levels are used when determining data access rights and applying protection controls.

Importantly, Symantec DLP 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.

SD-WAN Connectivity

VeloCloud SD-WAN solution connects branch users to applications in the data center, cloud, or at the edge in an efficient, reliable, and optimal manner. The solution uses Dynamic Multi-Path Optimization (DMPO) to offer path optimization over all types of WAN links that include MPLS, broadband, satellite, or dedicated circuits. The solution can recognize over 4300 business applications for automatic traffic steering and better quality of experience under poor WAN link conditions like loss, latency, and jitter.

Branch Firewall/ Enhanced Firewall Services

The VeloCloud SD-WAN solution offers built-in Enhanced Firewall Services that includes IDS, IPS, URL Filtering, and Malicious IP filtering using the VeloCloud SD-WAN Edge. The solution eliminates the need for a separate security appliance at branch locations simplifying operations. Business and security policies are managed centrally by the VMware Edge Cloud Orchestrator.

Simplified Management

Zero Touch Provisioning simplifies deployment of VeloCloud SD-WAN to connect thousands of branches from months to weeks. The solution uses centralized orchestration using VeloCloud Edge Cloud Orchestrator (VECO) to manage Day0/Day1 operations. VECO also enables automatic tunnel setup from branch SD-WAN Edges to Symantec SSE removing human errors and management burden. The solution uses AI and ML to provide visibility into user and device experience accessing applications with fault isolation and proactive remedial insights.

Edge Modernization/ Transformation

In many industries there is a need for edge-native applications to improves efficiency of operations. VeloCloud SASE in combination with VMware Edge Compute Stack enable Operations Teams (OT) to deploy, connect, secure and manage edge-native workloads. With in-built automation for VeloCloud SD-WAN the solution detects these applications and provides the right level of treatment. In addition, VeloCloud SD-WAN's Enhanced Firewall Services and the Symantec SSE solution provide tighter security with layered defense.

Proactive Threat and Data Protection

Symantec uses the Global Intelligence Network (GIN) that gathers over a billion threat telemetry signals from 153 countries covering Symantec's End Point Security, Email Security, and Symantec SSE solution. Symantec Threat Researchers leverage AI and ML to analyze this data and detect evolving (mutating) threats, and incorporate the results into the Symantec security portfolio.

Tolly & VMware VeloCloud Performance Reports

See these Tolly Group test reports to learn more about the capabilities of VMware VeloCloud in single-link and dual-link SD-WAN environments:

Tolly Report #220138 - VMware Work From Home Performance, VoIP and Microsoft 365 User Experience Evaluation (Single-link SD-WAN), &

Tolly Report #221128 - User Experience with VMware SD-WAN Work-from-Anywhere with Dual WAN Links

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 sales@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-12-wt-2024-07-05—VerD