Symantec SSE for VMware VeloCloud

Enterprises are undergoing cloud transformation, app modernization, edge modernization, and workforce transformation. While these changes may vary in pace, roadblocks appear in the form of legacy security solutions and sub-optimal network design. Cloud-native security service edge (SSE) helps organizations respond to increasing threats and address multiple use cases across a distributed business landscape.

Enterprises are either moving applications to public cloud infrastructure or directly consuming apps from SaaS vendors. A survey of IT leaders and decision makers shows 81% of enterprises expect to use multi-cloud applications in 2024[1]. About 54% use SaaS applications and tools to reduce the operational burden of managing software on-premises and to improve productivity.

Enterprise edge is also experiencing major changes, with edge-native applications deployed in increasing numbers for better productivity. There is also a significant increase in the number of user devices, including bring-your-own-device (BYoD), and IoT devices that connect over the enterprise network. Approximately 50% of enterprises have adopted some form of hybrid work environment to reduce costs, improve productivity, and retain talent.

From a security perspective, these changes imply a wider attack surface and a very active threat landscape. According to a Verizon report[2] about 68% of breaches involve a non-malicious human element. Industry data shows that approximately 45-50% of data is created and consumed outside the data center.

Legacy security design with the data center as the center of the security universe is no longer valid. Also, legacy security solutions cannot provide a dynamic response to the mutating threats that enterprises routinely encounter. According to the Symantec Ransomware Threat Landscape report[3] there was a 66% increase in the number of organizations affected by ransomware in 2023 compared to the previous year.

Introducing Symantec SSE for VMware VeloCloud

Symantec SSE for VMware VeloCloud is a cloud-hosted solution that offers threat and data protection when users access applications in the cloud or at the

[1] VMware Digital Momentum Study
[2] Verizon 2024 Data Breach Investigations Report
[3] The 2024 Ransomware Threat Landscape, Symantec by Broadcom

edge. As the SSE component of VMware VeloCloud SASE™, the service is delivered closer to users and their applications using Symantec Enterprise Cloud (SEC), a global network of security enforcement points of presence (POPs),

VMware VeloCloud SD-WAN™ uses automation to steer user and IoT device traffic at branch locations to the nearest Edge PoP in an optimal manner. Remote users in a hybrid work environment are connected to their applications based on zero trust principles using VMware VeloCloud SD-Access™. Networking policies for automatic traffic steering can be configured centrally and managed by VMware Edge Cloud Orchestrator.

Symantec SSE for VeloCloud enables customers to set their own pace for digital transformation while delivering robust security, reducing risks, and simplifying operations. The solution is sold as an add-on license to VeloCloud SD-WAN or VeloCloud SD-Access. Customers have the choice of buying this solution as a bandwidth-based license or Per User Per Year (PUPY) license.

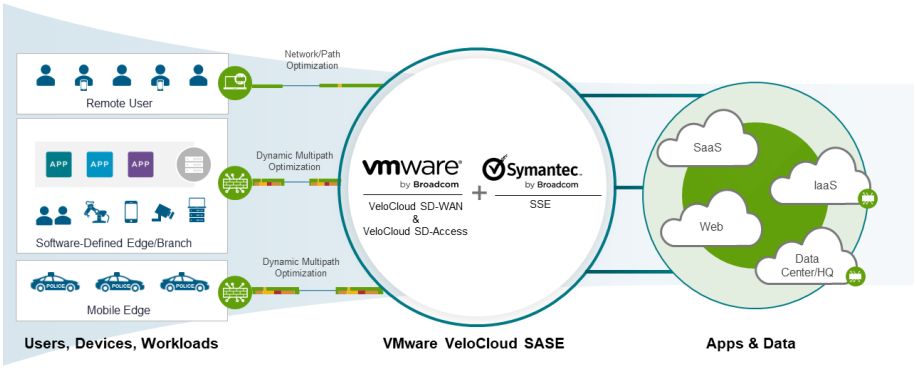

Figure 1: Proactive threat and data protection with simplified operations

Solution benefits

Enterprise-grade network and information security

Deployed by the most stringent security conscious enterprises, Symantec offers a comprehensive security solution that protects approximately 60% of Fortune 500 companies. The solution is delivered at scale using a global network of over 200 PoPs offering improved stability, performance, and reach. Security enforcement is done in the cloud, closer to users and their applications.

Proactive threat mitigation and data protection

Symantec SSE for VeloCloud delivers improved threat efficacy and response to manage continuous exposure to threats. The solution ~~stops~~ reduces the risk from a new generation of attacks or mutating threats using the largest civilian threat intelligence platform, Global Intelligence Network (GIN). GIN collects over a billion security telemetry data per day from 157 countries. This data is analyzed by a team of over 300 threat researchers using AI and ML for proactive threat detection and prevention. Symantec SSE helps reduce exposure to the most sophisticated and completely new generation of threats.

Tighter security with high-risk isolation

Every day over 250,000 web sites are introduced worldwide. The risk and reputation of these sites are not known to security vendors at the time of launch. About 50% of intrusion incidents involve credentials stolen when users interact with web applications, according to the Verizon 2024 Data Breach Investigations Report. Instead of blocking users from accessing these sites, Symantec SSE for VeloCloud creates an air gap between the users and the application to prevent users from being tricked into sharing credentials. It adds another layer of defense, at no extra cost, when users access websites that are uncategorized or categorized to be a higher risk. This approach strikes a balance between employee productivity and infrastructure security.

Reducing number of SOC investigations

Symantec SSE for VeloCloud provides layered defense to reduce alerts and threats that SOC teams need to investigate. Over a 30-day period, typical Symantec SSE customers experienced about 90% reduction in the number of incidents the SOC team had to investigate. SOC teams can now focus on the most important cyber threats without being subjected to alert fatigue.

Automated access with VeloCloud SD-WAN

VeloCloud SD-WAN provides connectivity and automation to direct user and IoT device traffic from enterprise edge locations to the nearest SEC security enforcement point. This automation takes away months of configuration changes needed on WAN edge routers to steer cloud application traffic away from the data center to cloud security. It helps reduce human errors that can leave classes of applications exposed to security risks or result in unwanted hair-pinning through the data center.

Consistent security for hybrid workforce

Policy configuration, management, and enforcement is consistent across the enterprise. A user blocked from accessing a website deemed malicious will have the same experience working at the office or from home. The solution uses principles of zero trust to provide access only to those applications the user is authorized for.

Use cases

Accelerating public or private cloud migration

Migrating workloads while relying on on-prem data center security solutions exposes several issues. User traffic gets sent to the data center for security enforcement before getting routed to the destination. This creates unwanted latency, poor user experience, wasted bandwidth on the WAN, and the operational burden of managing firewall capacity. These issues slow down cloud adoption. Symantec SSE for VeloCloud provides security enforcement on an optimal path between users and their applications. VeloCloud SASE also offers branch security using VeloCloud SD-WAN Enhanced Firewall Service. Users get the same consistent and secure experience from the cloud native application as they do with their data center applications.

Seamless SaaS adoption and controlling shadow IT

Many enterprises are using SaaS applications directly from SaaS vendors. This approach reduces the operational burden on IT, but they still need visibility into these applications. With support for over 45,000 SaaS applications using Cloud Access Security Broker (CASB), Symantec SSE for VeloCloud provides visibility and control into most of the applications commonly used by enterprises.

The ease of purchasing and using SaaS applications without the need for long-term contracts has enabled many enterprise divisions to use productivity apps outside the purview of IT, giving rise to shadow IT. With visibility and control Symantec SSE for VeloCloud helps rein in shadow IT,-improving user security without affecting their productivity.

Securing OT/ edge-native applications and accelerating branch modernization

In many industries like retail, manufacturing, utilities, and public safety, there is an increasing use of edge-native apps that directly affect productivity. With many locations, the scale and magnitude of operations to manage connectivity and security can become complex. VeloCloud SASE offers application-aware traffic steering and security to connect these applications to users and services located elsewhere on an optimal path. Using the automated access of VeloCloud SD-WAN along with an added layer of protection using Enhanced Firewall Services, Symantec SSE for VeloCloud uses in-depth defense to protect edge-native applications.

Enabling secure Internet access/guest access

In branch sites there may be contractors or partners working on a project for the enterprise. These users may need direct access to the internet without backhauling their traffic to the data center. They are subject to the same Acceptable Use Policy (AUP) as the employees. Without a proper security posture these users can expose the branch to security risks. As a cloud-hosted solution sitting on an optimal path, Symantec SSE for VeloCloud provides the security needed for direct internet access. In addition, VeloCloud SD-WAN Enhanced Firewall Service offers options to add another layer of security and helps prevent attacks propagating from a branch site.

Stopping a new generation of attacks

Ransomware is the top threat among 92% of the industries according to Verizon's 2024 DBIR2. The combination of increasing threats, decreasing resources, and a complex environment that places a heavy burden on SOC investigation can expose the infrastructure to targeted ransomware attacks (attacks that emerge through the software supply chain). Attackers are sometimes able to dwell in an environment for months before extracting valuable information.

Symantec SSE for VeloCloud uses layered security with sandboxing to detect zero-day threats while blocking known threats using anti-malware and deep file inspection. The solution provides better detection and response along with prevention taking advantage of the analysis done on the telemetry data

Learn more

VMware VeloCloud SASE,
vmware.com/products/secure-access-service-edge-SASE

VMware VeloCloud SD-WAN,
vmware.com/products/sd-wan

gathered from GIN. Symantec SSE for VeloCloud unifies security and telemetry to help stop emerging threats at the security enforcement points.

Protecting data and mitigating compliance risks

Adhering to compliance requirements is a key concern for enterprise customers. With Symantec SSE for VeloCloud, users experience safer browsing with URLs filtered by 90 categories and threats identified by 10 levels of risks—all while the solution gets continuous updates from Symantec Threat Research. Using CASB, enterprises gain visibility into user activity across a broad range of sanctioned and unsanctioned cloud apps and services, such as Office 365, Google Workspace, Box, and GitHub. The solution helps prevent data breaches in the cloud by identifying sensitive data, monitoring data in motion, and enforcing policy controls that align with corporate compliance policies using Data Loss Prevention (DLP). The solution helps identify and classify critical compliance-related data such as GDPR, HIPAA, PHI, PCI, and PII, and continuously monitors data movement to help prevent this data from leaving the enterprise perimeter.

Secure access for the hybrid workforce

With the hybrid work environment here to stay, enterprises can no longer rely on legacy VPN solutions that are less secure and prone to scale challenges. It is imperative that security follows the user no matter where they work. VeloCloud SD-Access is the remote access solution of VeloCloud SASE that is scalable, path optimized, easy to deploy and based on principles of zero trust. Using centralized orchestration, the solution enables IT to set policies for remote access and security. Remote user traffic is subject to security enforcement at the nearest security enforcement point based on policy.

Reducing the load on data center firewalls

Enterprises can reduce their investment in data center firewalls as they move applications to the cloud. VeloCloud SASE places user traffic destined for cloud applications on the most optimal path for security enforcement. These enforcement points are in the cloud, so the dependence on data center firewalls to protect this user traffic continues to go down. In addition, customers who need branch security can leverage VeloCloud SD-WAN Enhanced Firewall Service. The combination of branch security and cloud security options helps IT deliver security closer to the users and reduce investments in data center firewalls.

Conclusion

Symantec SSE for VMware VeloCloud helps customers set the pace of transformation with a robust threat and data protection solution. As the security component of VeloCloud SASE the solution reduces risks, mitigates compliance needs, and simplifies operations. With threat research and intelligence deeply integrated into the solution, customers can safely address the risks posed by a changing threat landscape.

vmware by Broadcom

Item No: sase-2009-VeloCloud-SSE-so-0524