

VeloCloud SASE Secured Service Edge (SSE)

Unleash Secure Enterprise Edge and Cloud Transformation

A COMPLETE SOLUTION FOR FASTER TIME-TO-VALUE

VeloCloud SSE includes everything organizations need to transform their networking and security infrastructure:

- VeloCloud™ SD-WAN: Optimize application performance over any WAN link, with zero-touch provisioning that accelerates connectivity at scale.
- SSE: Deliver a dependable, high-performance cloud security service that enforces security between employees, wherever they are located, and the Internet.
- VeloCloud SD-Access: Enables easy, secure remote access for workers and IoT devices anywhere, with connectivity optimized for speed and reliability.
- VeloCloud Orchestrator: Cloud-hosted centralized orchestration software that provides a single management pane for networking, branch security, and remote access, providing visibility into the user experience, traffic flow, and other insights.

Overview

Digital transformation is changing the way IT thinks about the network and security infrastructure. Applications are now spread across data centers, cloud, SaaS, and the edge, and the devices that access them are everywhere. Traditional network and security architectures can't keep up with evolving hybrid work environments, evolving security threats, more IoT devices, and an expanding attack surface. The pressure is growing for IT to protect applications, users, and sensitive data, while controlling costs and helping users be more productive.

Power Transformative Use Cases

VeloCloud SSE supports a wide variety of use cases that can help enterprises accelerate digital transformation and strategic initiatives.



Cloud Migration

81% of enterprises are expected to have workloads in multiple clouds, and it's up to IT to connect users across the enterprise to cloud destinations.

The SSE for VeloCloud overlay network automatically delivers user traffic to cloud services like Azure, GCP, AWS, and Alibaba on the best path, prioritizing the most critical applications.



SaaS Adoption

As organizations use more SaaS applications, they expose the perimeter to potentially risky websites. With the SSE, they can give users reliable, efficient access to SaaS applications while maintaining a robust security perimeter.



Edge Transformation

New edge-native applications are being deployed at branch locations or in mobile edge destinations like police cars or ambulances. The SSE securely connects these sites over MPLS, satellite, LTE/5G or any other transport mechanism at scale using centralized orchestration.

It detects edge applications that need to prioritize and steer traffic to cloud destinations.



Hybrid Work

Workspaces are evolving, and surveys show approximately 50% of employees are expected to work remotely or in a hybrid environment.

The SSE uses Zero Trust Network Access (ZTNA) to provide access only to resources a user needs, while continuously validating trust based on context.



Stop a New Generation of Attacks

The SSE prevents targeted ransomware attacks and other evolving threats by analyzing over a billion telemetry data points daily using advanced machine learning techniques.



Ensuring Compliance

Achieving compliance is challenging when enterprise data is spread across data centers, the public cloud, SaaS clouds, and the edge. The SSE helps organizations assess risk and deploy the controls they need in a centralized, consistent way using pre-built templates.



Protecting Data

A substantial amount of enterprise data gets generated and consumed in the cloud or at the enterprise edge. The SSE prevents sensitive data from leaving the enterprise perimeter with multi-layered detection. Its high accuracy helps reduce false positives, while speeding response times if data loss occurs.



WAN Upgrades

A substantial amount of enterprise data gets generated and consumed in the cloud or at the enterprise edge. The SSE prevents sensitive data from leaving the enterprise perimeter with multi-layered detection. Its high accuracy helps reduce false positives, while speeding response times if data loss occurs.

Benefits of VeloCloud SASE SSE

What happens when organizations reimagine network and security architecture for the software-defined edge? They set the stage for powerful business outcomes.



Proactive Threat Detection and Response

As their attack surface continually expands, enterprises need a multi-layered defense with faster threat detection and response. The SSE lets organizations take advantage of the latest analysis from over 200 million control points.



Simplified Management

The SSE manages all networking connectivity and operations using VeloCloud Orchestrator, giving administrators insights into path visibility and quality of experience, as well as proactive remediation. VeloCloud Orchestrator communicates with the SSE management console to automatically secure traffic between users and their applications.



Global Reach at Scale

The SSE delivers networking and security using robust public cloud infrastructure in more than 200 countries and territories. The cloud native infrastructure offers stronger resilience, with less dependence on congested public internet routes. It automatically scales to support new demand and heals more quickly.



Easy Cloud Security On-Ramp

When security moves to the cloud, it's challenging for IT to get user traffic to the security enforcement points distributed across the globe. The SSE removes the burden by automatically connecting all VeloCloud SD-WAN Edges with a policy configuration on VeloCloud Orchestrator. It automatically directs agentless device traffic over the right path, minimizing human errors.

VeloCloud SSE: Transform at Your Pace, Your Way

No matter where organizations are in their transformation journey, VeloCloud SASE SSE enables them to connect and secure users, devices, applications, and data wherever they reside. A complete SASE solution, it provides protection for the distributed enterprise edge, improved user experience, simplified management, and better performance and scale with an agile security posture. Providing a powerful combination of connectivity and security, the solution helps organizations unlock new levels of productivity and achieve their most important business outcomes.

Santa Clara—Corporate Headquarters

5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500

Fax: +1-408-538-8920

Email: info@arista.com

Ireland—International Headquarters

3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office

9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office

Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office

9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Copyright © 2025 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. June 30, 2025 05-0055-01

