VeloCloud™ SD-WAN Edge Threat Management

Enterprise WAN Simplicity, Performance, and Security

At a Glance

VeloCloud SD-WAN brings cloud-delivered networking, security, and AIOps to support ubiquitous access for branch and remote workers as well as digital transformation at the edge.

VeloCloud SD-WAN enables enterprises to support application growth, network agility, and simplified branch implementations while delivering high performance, reliable branch access to cloud services, private data centers, SaaS-based and edge-native enterprise applications.

Cloud-native by design, VeloCloud SD-WAN is delivered via a global network of Edge PoPs, either self-managed or as a managed service.

Secure SD-WAN

VeloCloud SD-WAN Edge Threat Management delivers comprehensive, enterprise-grade network security at the network edge.

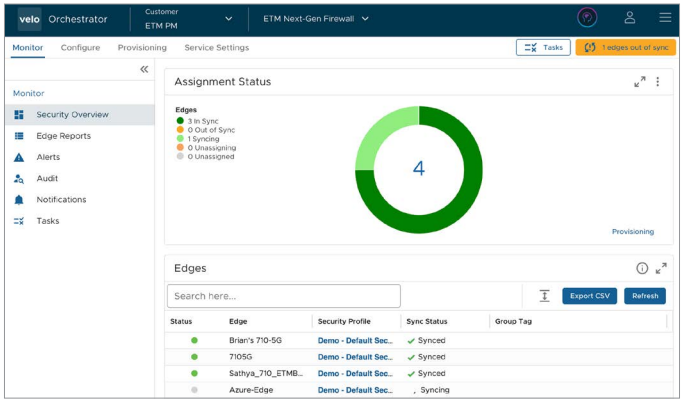
- Stateful Firewall
- Time based policies
- Zone based segmentation
- Denial of Service Protection
- Network Address Translation
- Application Identification
- Intrusion Prevention
- URL Filtering
- Geo-IP Filtering
- DNS Filtering
- External dynamic IP / URL lists
- IP / URL Reputation

Overview

Organizations with distributed branch locations face increasing operational complexity, security risk, and network costs. Traditional, site-by-site network and security architectures are no longer scalable, resilient, or cost-effective. A centrally managed branch firewall enables consistent security enforcement, improved application performance, simplified operations, and measurable cost savings while supporting business growth and digital transformation.

Unified SD-WAN and Security Policy Management

ETM is integrated into VeloCloud Orchestrator as a dedicated enterprise application. This enables security operators to configure policies that build on the same source of shared network configuration while maintaining a dedicated management console for security policy configuration, provisioning, and reporting. Bridging NetOps and SecOps breaks down organizational silos by reducing finger pointing, lowering licensing costs, and minimizing the overhead of training staff on disparate systems.



Consistent Security Policies for Branch Networks

For geographically dispersed organizations, advanced network security layers at remote branch locations are the frontline defense against an expanded attack surface. At branch sites that incorporate business policies to steer various types of traffic directly to the Internet, each remote site becomes a potential gateway for sophisticated cyber threats. Modern threats often target remote offices because they are perceived as weaker links. Branch sites are often composed of diverse devices from corporate laptops to unmanaged IoT hardware (smart cameras, printers, badge scanners).

Policy Orchestration

VeloCloud Orchestrator is a cloud-hosted or on-premises central management tool for VeloCloud SD-WAN. Its web-based user interface provides simplified configuration, provisioning, monitoring, fault management, logging, and reporting functions. Orchestrator enables flexible implementation of business-based policies for application delivery and traffic management.

VeloCloud SD-WAN Edge

Edges are available as easy-to-install appliances for remote branches with a range of throughput, ports for WAN and LAN connectivity, integrated wireless LAN, and security firewall services. Dynamic routing enables policy-based overlay insertion for both inline and out-of-path deployments. High Availability (HA) setup provides redundancy and failover.

Advanced security layers provide the granular visibility needed to automatically segment, identify, and enforce uniform security policies across every location, regardless of local IT footprint.

By embedding advanced security layers at the remote edge, organizations can confidently scale their footprint, improve user experience, and maintain a seamless, hardened security posture across the entire global enterprise.

Threat Protection at the Edge

VeloCloud SD-WAN Edge Threat Management combines multiple Next-Generation firewall technologies including IP reputation, external blocklists, Intrusion Prevention, URL filtering, Application classification, Geo-IP filtering, Network Address Translation, Deep Packet Inspection (DPI), and stateful firewalling to provide a comprehensive security layer at the network edge.

Centrally Managed Firewall Policies

Edge Threat Management security policies are managed in VeloCloud Orchestrator, enabling security admins to focus on security specific operations. Admins can build and assign reusable policies consisting of predefined objects and templates. This design makes updating security policies possible by a few simple clicks, while the associated changes are propagated throughout the network within minutes.

AI Powered Insights and Deep Analysis

Gain valuable insights from database-driven reports without the need for a separate appliance. See the network status at a glance on the dashboard, ensure compliance with full event logs, and get notifications of threats, anomalies or unusual user behavior with alerts. An integrated AI assistant provides interactive guidance on a variety of inputs, such as the effects of a policy on a given object.

Cloud-based Threat Intelligence

VeloCloud edge routers collect threat intelligence data from a variety of dynamic sources to determine in real-time the trustworthiness and identity of hosts inside and outside the network.

With integration to Arista NDR and other web based dynamic lists, administrators can identify suspicious hosts and build policies to block potentially harmful activities.

Network-wide Segmentation Policies

The flexible security policy configuration within the Edge Threat Management policy management extends the security coverage from the data center to the branch. Security operations administrators can build access policies that are enforced across a distributed network. The centralized design enables admins to configure and deploy consistent zone based policies across the entire distributed network.

By extending the enforcement to the access layer, filtering happens at the earliest opportunity, reducing the potential for internal threats and preserving network bandwidth by blocking threats and other undesirable traffic at the origination point.

Deploy in Minutes

Using a zero-touch provisioning capability, VeloCloud Edge installs quickly. The Edge is shipped to the branch office where it is connected to power and a network cable. Activation, configuration, and ongoing management are all handled from the cloud.

Flexible Deployment

VeloCloud Edges are available in various form factors: hardware, software (VMs), downloadable from cloud marketplaces, or virtual network functions (VNF), with hardware appliances most widely deployed at customer branch sites.

Secure Branch Connectivity

VeloCloud Edges aggregate multiple links and steer traffic over the optimal links based on Dynamic Multipath Optimization (DMPO) and deep application recognition (DAR). Edges support high-availability (HA) deployment models and can easily integrate into an existing network.

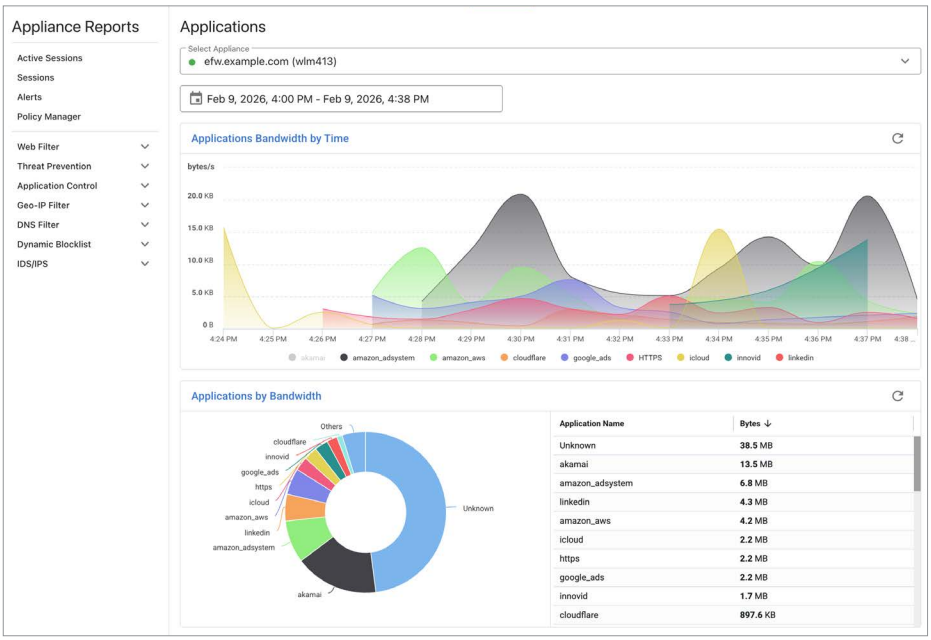
Data Plane Security

VeloCloud edge routers include a variety of essential data layer security features. In addition to the stateful firewall, the edge routers provide zone based traffic segmentation, Intrusion Detection and Prevention (IDS/IPS), URL & malicious IP filtering, a security monitoring dashboard, hosted firewall logging, DoS and flood protection, and more.

The Edge Threat Management services running on the device improves overall branch network security by detecting unauthorized access to corporate network assets, mitigating threats, and defending against cyber attacks. Today's distributed branch networks greatly benefit from the security services for user traffic protection, consolidated hardware, simple and unified management, reduced operational overhead, and overall cost savings.

Real-time Monitoring, Reporting, and Event Notifications

Timely alerts and notifications enable administrators to swiftly detect and respond to attacks or suspicious activity such as intrusions, malware, policy violations, and unauthorized access requests before they escalate. Edge Threat Management in VeloCloud Orchestrator provides cloud based access to historical reporting data and real-time notifications so admins can receive critical events on their mobile device or other systems that enable them to immediately address critical issues.



SIEM Integration for Better Security at the Edge

VeloCloud SD-WAN integrates with major security information and event management (SIEM) providers to better protect customers with improved security posture, timely detection of threats, proactive protection, and compliance with industry regulations. SIEM collects, analyzes, and correlates security data from various sources, such as logs, network traffic, and security alerts. Organizations gain visibility into user traffic, detect threats or malicious activity in a timely manner, and take responsive actions accordingly.

Simplified VPN connectivity

VeloCloud SD-WAN provides unified, secure communications, regardless of the underlying transport type. The VeloCloud Orchestrator platform provides automatic IPsec VPN tunnel provisioning from branches to Gateway aggregation points for interoperable access to your cloud infrastructure, eliminating manual, two-sided tunnel setup from 1XN branches to 1XN cloud data centers.

Public Key Infrastructure

The VeloCloud Orchestrator platform includes a Public Key Infrastructure (PKI) providing scalability and robust security around device identification and encryption services. The consolidated management of the built-in certificate server enables secure onboarding of devices and revocation management. Risk is minimized by pinning certificates to specific devices and using unique pairwise encryption keys.

Firewall Feature Matrix

Feature	Integrated Firewall	Edge Threat Management
Stateful Firewall	✓	✓
Denial of Service Protection	✓	✓
Network Address Translation	✓	✓
Application Classification	✓	✓
Access Control List	✓	✓
Policy Objects	✓	✓
Security Services Policy Manager		✓
AI Powered Policy Insights		✓
Intrusion Detection and Prevention		✓
URL Categorization & Filtering		✓
Geo-IP Filtering		✓
DNS Filtering		✓
Security Zones		✓
Dynamic External IP / URL Lists		✓
IP / URL Reputation Service		✓
Time Based Policies		✓

VeloCloud Edge Threat Management Add-on SKUs

SKU	Description
SDEX-ETM-10M-1M	Edge Threat Management Add-On; 10 Mbps; Requires Purchase of a SD-WAN 10 Mbps
SDEX-ETM-30M-1M	Edge Threat Management Add-On; 30M Mbps; Requires Purchase of a SD-WAN 30M Mbps
SDEX-ETM-50M-1M	Edge Threat Management Add-On; 50M Mbps; Requires Purchase of a SD-WAN 50M Mbps
SDEX-ETM-100M-1M	Edge Threat Management Add-On; 100M Mbps; Requires Purchase of a SD-WAN 100M Mbps
SDEX-ETM-200M-1M	Edge Threat Management Add-On; 200M Mbps; Requires Purchase of a SD-WAN 200M Mbps
SDEX-ETM-500M-1M	Edge Threat Management Add-On; 500M Mbps; Requires Purchase of a SD-WAN 500M Mbps
SDEX-ETM-1G-1M	Edge Threat Management Add-On; 1G Gbps; Requires Purchase of a SD-WAN 1G Gbps
SDEX-ETM-2G-1M	Edge Threat Management Add-On; 2G Gbps; Requires Purchase of a SD-WAN 2G Gbps
SDEX-ETM-10G-1M	Edge Threat Management Add-On; 10G Gbps; Requires Purchase of a SD-WAN 10G Gbps
SDEX-ETM-40G-1M	Edge Threat Management Add-On; 40G Gbps; Requires Purchase of a SD-WAN 40G Gbps
SDEX-ETM-100G-1M	Edge Threat Management Add-On; 100G Gbps; Requires Purchase of a SD-WAN 100G Gbps

Platform Compatibility

710-W	710-5G	720	740	4100	5100	Virtual	AWS	Azure	GCP
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note: Edge Threat Management requires minimum software release version **7.0.1F**

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 © 2026 Arista Networks, Inc. All rights reserved. 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. July 16, 2026