

Granite's SD-WAN Technology Matrix





SD-WAN Technology Matrix

Technology		VeloCloud	Cisco Meraki	Fortinet	Cisco Viptela	Juniper Networks	Oracle Talari
Carrier Requirements		Granite Guardian: Monitoring and Management options available	Granite Guardian: Monitoring and Management options available	Granite Guardian: Monitoring and Management options available	Granite Guardian: Monitoring and Management options available	Granite Guardian: Monitoring and Management options available	Agnostic
Minimum Site Requirement		1+ Site	1+ Site	Multi-Site	Multi-Site	Multi-Site	Multi-Site
Geographical Deployment	Domestic	Yes	Yes	Yes	Yes	Yes	Yes
	S. America	ICB	ICB	ICB	ICB	ICB	ICB
	Europe	ICB	ICB	ICB	ICB	ICB	ICB
	APAC	ICB	ICB	ICB	ICB	ICB	ICB
	Global	ICB	ICB	ICB	ICB	ICB	ICB
	Mixed	ICB	ICB	ICB	ICB	ICB	ICB
Deployment		Physical or Virtual	Physical or Virtual	Physical or Virtual	Physical or Virtual	Physical or Virtual	Physical or Virtual
Deployment Differentiator		Create customer domains within controller using profiles	Built networks within organization using templates	Shared or Customer VDOMs used to build customer networks	Leverage existing or new Cisco infrastructure to deliver SD-WAN.	Uniform global tenant and service policies, hyper-segmentation based on tenants and services	Hybrid WAN, WAN Failover, Circuit Agnostic, MPLS/ Private IP underlay, Point to Point/WAVE, etc. Service built on a true SDN orchestration and neutral platform all with zero touch provisioning
Access Options		Any transport (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc)	Any transport (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc)	Any transport (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc)	Any transport (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc)	Any transport (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc)	MPLS, Ethernet, Broadband, DIA, 3G/4G/LTE, Wave or Point to Point
Resiliency & Failover		Internet Gateways, Packet duplication, Link Aggregation, Cloud Management, Active/Active and Active/Passive, Sub-second failover between circuits. High Availability pairs option on any device	Link Aggregation, Cloud management, Failover between circuits, High Availability pairs option on any device	Link Aggregation, Sub-second failover between circuits, High Availability pairs available on all models	Link aggregation, failover between circuits, High Availability pairs option on devices	Link aggregation, Stateful failover (sub-second failover)	Seamless path transition, packet duplication, automated No threshold configuration, Link aggregation
Routing Capabilities		Dynamic routing (multicast, OSPF, BGP), dynamic mesh VPN, hub clustering, customizable business policy, WAN Optimization, Application acceleration, QoS, Traffic Shaping	Dual VPN, Dynamic path selection, QoS, Traffic Shaping, Policy-based routing	Full routing capabilities (BGP, OSPF, etc), customizable SLA targets for application control, WAN Optimization, Application Identification and Steering, QoS, Traffic Shaping	Supports traditional routing protocols (BGP, OSPF) and First-hop redundancy (VRRP), Overlay Management Protocol (OMP) establishes and maintains Viptela control plane (enabled by default)	"Secure Vector Routing (SVR), Application Steering via Metadata rather than tunnels, Service Route (Defines fabric egress policy, Full 5-tuple plus Tenant/Service, Propagated using STEP, Directional and Symmetric), BGP over SVR (Enables BGP end-to-end, Legacy destination prefix-based propagation /redistribution), QoS, Load Balancing, WAN Optimization"	OSPF, BGP, WAN, Application, Traffic Shaping, QoS
Encryption		Yes	Yes	Yes	Yes	Yes, AES 256 or 128	Yes Aes128/256
Security	Zone Based firewall	Yes	Yes	Yes	No	Yes	Yes
	Next Gen. Firewall including IPd/ IPS	Need to leverage a separate premise or cloud-based firewall solution	Premise-based Advanced Security features integrated into SD-WAN device	Device bundle includes Unified Threat Management service	Need to leverage a separate premise or cloud-based firewall solution	FIPS 140-2, ICSA Firewall, deny-by-default, prevent eavesdropping	Need to leverage a separate premise or cloud-based firewall solution
Cloud Connect		AWS, Azure, Google	Can leverage any cloud connect services supplied by carriers	AWS, Azure, Google, O365; all major Cloud providers are supported	Tunnel or cloud connect possible depending on location of PoP and client data center	AWS, Azure, Google	Yes
Customer Sweet Spot		SMB to Large Enterprise with US-Based HQ. Ideal for businesses with critical applications like voice and video	SMB to Large Enterprise with US-Based HQ. Smaller IT Staff.	SMB to Mid-Enterprise with US-Based HQ. Businesses that have security as a top concern.	SMB to Large Enterprise with US-Based HQ. Businesses that already have Cisco infrastructure (ISR/ASR)	SMB to Large Enterprise with US-Based HQ. Businesses with bandwidth issues due to overhead.	Anywhere there are critical applications, multi-cloud connectivity
Notes		Includes Layer 7 stateful firewall, recommended to be paired with cloud or premise-based firewall solution	Does not include application optimization. Failover events typically take 30 seconds	Great for utilizing existing Fortinet equipment in order to deliver SD-WAN	Can use existing ISR/ASR Cisco devices in order to deliver SD-WAN capabilities	Tunnel-free SD-WAN via Secure Vector routing	