

SD-WAN Provider		SD-WAN Plattform		SD-WAN Backbone	SD-WAN Anbieter Anforderung	SD-WAN Topologien	SD-WAN Kunden Zielgruppe	SD-WAN Internationale Verfügbarkeit	SD-WAN-Bereitstellung	SD-WAN Einsatzunterscheidungsmerkmal	SD-WAN Anschlussoptionen	SD-WAN Ausfallsicherheit und Failover	SD-WAN Routing-Funktionen	SD-WAN Verschlüsselung	SD-WAN Firewall	SD-WAN Cloud Connect	Anmerkungen
	aryaka		aryaka	Ja	Managed Service	Multi-site	Internationale Enterprise, und Large Enterprise Kunden, die Cloud-Anbieter nutzen	ja	Physisch oder Virtuell	MPLS alternative, Global Private network CDN provider	Ethernet, Broadband, 3G/4G/LTE, Satellite	26 Gateways auf der ganzen Welt	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	Ja (IP Sec)	nicht verfügbar	O365, Azure, AWS, Salesforce, Box, SAP, Autodesk AutoCAD Application Acceleration Site-to-site/Site-to-cloud	Fully Managed Service mit Support, wenn der Kunde das Aryaka Edge Device (ANAP) nutzt. Last-Mile-Management und Beschaffung.
	Expereo		aryaka	über Aryaka	Managed Service	Multi-site	Internationale Kunden Kunden, die Cloud-Anbieter nutzen	ja	Physisch oder Virtuell	MPLS alternative, Global Private network. CDN provider.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	26 Gateways auf der ganzen Welt	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	Ja (IP Sec)	nicht verfügbar	O365, Azure, AWS, Salesforce, Box, SAP, Autodesk AutoCAD Application Acceleration Site-to-site/Site-to-cloud	Fully Managed Service mit Support, wenn der Kunde das Aryaka Edge Device (ANAP) nutzt. Last-Mile-Management und Beschaffung.
	BigLeaf		BigLeaf	nicht bekannt	Anbieter unabhängig	None	Cloud-App-Kunden, Kunden, die die bestehende Firewall / Sicherheit beibehalten und die Konfiguration nicht ändern möchten	keine	Physisch	Jeder Kundenstandort ist aus Redundanzgründen mit zwei BigLeaf-Gateways verbunden.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Hot Spare und HA Option verfügbar, Im selbstem IP failover, Hochverfügbarkeitsoption	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	nicht verfügbar	nicht verfügbar		Der Kunde muss über eine Firewall oder einen Router verfügen, um VPN-Verbindungen herzustellen. Support-Team rund um die Uhr verfügbar. Bietet Switches für hohe Verfügbarkeit Bereitstellungen, um Fehlkonfigurationen zu vermeiden.
	BT		CISCO IWAN	Ja	Managed Service	Multi-site	Cisco Bestandskunden, Mittelständische- und Enterprise Kunden	ja	Physisch oder Virtuell	Cisco-Router, entweder vorhandene oder neue Bereitstellungen.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Performance-Routing, um den Ausfall von HSRP zu vermeiden, um redundante Geräte zu ermöglichen	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	ja	Cisco-Firewall integriert in SD-WAN-Edge-Gerät	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	Der Kunde kann vorhandene Cisco-Router verwenden, sofern diese kompatibel sind. Kein allumfassender zentraler Orchestrator Nur ISR 4300 und ISR 4400 Router unterstützen vollständige IWAN-Funktionen. Manuelle Konfiguration Das zentrale Management ist nicht so robust wie die Konkurrenz
	Expereo		CISCO IWAN	nicht bekannt	Managed Service	Multi-site	Cisco Bestandskunden, Mittelständische- und Enterprise Kunden	ja	Physisch oder Virtuell	Cisco-Router, entweder vorhandene oder neue Bereitstellungen.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Performance-Routing, um den Ausfall von HSRP zu vermeiden, um redundante Geräte zu ermöglichen	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	ja	Cisco-Firewall in SD-WAN-Edge-Gerät integriert	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	Der Kunde kann vorhandene Cisco-Router verwenden, sofern diese kompatibel sind. Kein allumfassender zentraler Orchestrator Nur ISR 4300 und ISR 4400 Router unterstützen vollständige IWAN-Funktionen. Manuelle Konfiguration Das zentrale Management ist nicht so robust wie die Konkurrenz
	Netwolves		CISCO IWAN	nicht bekannt	Managed Service, optional auch Unmanaged Service für Multi-Service-Provider	Multi-site	Cisco Bestandskunden, Mittelständische- und Enterprise Kunden	ja	Physisch oder Virtuell	Anbieter / Schaltung agnostisch unter Netwolves.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Performance-Routing, um den Ausfall von HSRP zu vermeiden, um redundante Geräte zu ermöglichen	WAN, Anwendung, QoS, Traffic Shaping	ja	Cisco-Firewall integriert in SD-WAN-Edge-Gerät; Palo Alto Option verfügbar	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	Der Kunde kann vorhandene Cisco-Router verwenden, sofern diese kompatibel sind. Kein allumfassender zentraler Orchestrator Nur ISR 4300 und ISR 4400 Router unterstützen vollständige IWAN-Funktionen. Manuelle Konfiguration Das zentrale Management ist nicht so robust wie die Konkurrenz
	Telstra		CISCO IWAN	Ja	Managed Service	Multi-site	Cisco Bestandskunden, Mittelständische- und Enterprise Kunden	ja	Physisch oder Virtuell	Cisco-Router, entweder vorhandene oder neue Bereitstellungen.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Performance-Routing, um den Ausfall von HSRP zu vermeiden, um redundante Geräte zu ermöglichen	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	ja	Cisco-Firewall integriert in SD-WAN-Edge-Gerät	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	Der Kunde kann vorhandene Cisco-Router verwenden, sofern diese kompatibel sind. Kein allumfassender zentraler Orchestrator Nur ISR 4300 und ISR 4400 Router unterstützen vollständige IWAN-Funktionen. Manuelle Konfiguration Das zentrale Management ist nicht so robust wie die Konkurrenz
	Verizon		CISCO IWAN	Ja	Managed Service	Multi-site	Cisco Bestandskunden, Mittelständische-, Enterprise-, und Large Enterprise Kunden die einen bedeutenden Teil der Standorte im Verizon Gebiet (USA) haben	ja	Physisch oder Virtuell	Cisco-Router, entweder vorhandene oder neue Bereitstellungen.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Performance-Routing, um den Ausfall von HSRP zu vermeiden, um redundante Geräte zu ermöglichen	WAN, Anwendung, QoS, Traffic Shaping	ja	Cisco-Firewall integriert in SD-WAN-Edge-Gerät	AWS, Azure, Google HPE, IBM, Oracle, Salesforce	Der Kunde kann vorhandene Cisco-Router verwenden, sofern diese kompatibel sind. Kein allumfassender zentraler Orchestrator Nur ISR 4300 und ISR 4400 Router unterstützen vollständige IWAN-Funktionen. Manuelle Konfiguration Das zentrale Management ist nicht so robust wie die Konkurrenz
	Expereo		Citrix NetScaler	nicht bekannt	Managed Service	Multi-site	Citrix Bestandskunden die XenDesktop/XenApp verwenden	ja	Physisch oder Virtuell	Unterstützt BGP- und OSPF-Routing.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Paketüberwachung zum Erkennen von Fehlern und Schaltkreise, Packet Duplication für VoIP und andere missionskritische Anwendungen, Paketbasierte Pfadauswahl	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	Ja (AES-128, AES-256, IPsec, GRE, und Citrix Virtual Path)	Stateful firewall	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	Kann im Edge- oder Overlay-Modus bereitgestellt werden. Optimiert den HDX-Datenverkehr auf Quellcodeebene. Liefert die bestmögliche XenApp und XenDesktop-Erfahrung. Drei Optionen - Standard, WANOP und Enterprise
	CLOUDGENIX		CLOUDGENIX	nicht bekannt	Anbieter unabhängig	Multi-site	Cloud-App-Kunden, Kunden, die eine Hybrid-Cloud-Strategie für bestehende und neue Apps verfolgen.	ja	Physisch oder Virtuell	Aktive / aktive Pfadauswahl per Sitzung für die gleiche Anwendung. Kann im reinen Überwachungsmodus für umfassende Netzwerk- / Anwendungsanalysen bereitgestellt werden, ohne den Datenverkehr zu unterbrechen.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Branch- und DataCenter-HA-Modelle für Skalierung und Redundanz, anwendungsspezifische Brownout-Erkennung auf Layer 7, nahtloses Failover für Netzwerkpfad-Down-Szenarien	WAN, Anwendung, QoS, Traffic Shaping	Ja (AES-256 und AES-128 für ausgewählte Länder)	Zonenbasierte Firewall	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	Nutzt anwendungsspezifische Leistungsmetriken und Erreichbarkeit in die Pfadauswahllogik. Weltweit auf 6 Kontinenten eingesetzt. Cloud-basierter Controller, hoch skalierbar. Ermöglicht den Zugriff auf die zurende liegenden Netzwerke, wodurch Integration und Migration einfacher und robuster
	ECESSA		ECESSA	nicht bekannt	Der Kunde muss SLA bereitstellen, damit Ecessa Updates bereitstellen kann	Multi-site	Mittelständische Unternehmen mit bis zu 20 Standorte	ja	Physisch oder Virtuell	Pure over-the-Top, muss der Kunde Bandbreite bereitstellen; 24/7 Support, um Kunden bei der Implementierung zu unterstützen.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Packet Duplication Link Aggregation Ports werden basierend auf der Konfiguration nicht geöffnet / geschlossen	WAN, Anwendung, QoS, Traffic Shaping	ja	Basic-Firewall integriert in das SD-WAN-Edge-Gerät; Advanced Security erfordert entweder On-Premise oder Cloud-basierte Firewall	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	Unterstützt bis zu 25 WAN-Verbindungen. Drei Upgrade-Optionen.
	Netwolves		MERAKI	nicht bekannt	Managed Service, optional auch Unmanaged Service für Multi-Service-Provider	Multi-site	Meraki Bestandskunden, kleine-, mittelständische- und Enterprise Kunden	ja	Physisch	Anbieter / Schaltung agnostisch unter Netwolves.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Performance-Routing, um den Ausfall von HSRP zu vermeiden, um redundante Geräte zu ermöglichen	WAN, QoS, Traffic Shaping	ja	Meraki MX Firewall integriert in SD-WAN Edge Device; Palo Alto Option verfügbar	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	Nutzt bestehenden Meraki-Orchestrator. Enthält keine Anwendungsoptimierung.
	T-Systems		ngena	Ja (ngena global Backbone)	Managed Service	Multi-site	Internationale Enterprise, und Large Enterprise Kunden	ja	Physisch	Mandantenfähige, verwaltete Implementierung	MPLS, Ethernet, Broadband, 3G/4G/LTE	Weltweit stehen fünf standardisierte Access Designs zur Auswahl	WAN, Anwendung, QoS, Traffic Shaping	ja	auf Anfrage	auf Anfrage	Mit einer Präsenz in mehr als 20 Ländern, 37.900 Mitarbeitern und einem Außenumsatz von 6,9 Milliarden Euro (2017) ist T-Systems einer der weltweit führenden herstellereigenen Anbieter digitaler Dienstleistungen mit Sitz in Europa
	AT&T		VELOCLOUD	Ja	Managed Service	Multi-site	National und Internationale Kunden, die einen bedeutenden Teil der Standorte im AT & T Gebiet (USA) haben	ja	Physisch oder Virtuell	Aktiv / Aktiv in den USA, mit Cold Spare-Gerät in 51 Ländern.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Internet-Paket-Duplizierung Link-Aggregation	WAN, Anwendung, QoS, Traffic Shaping	ja	Müssen ein separates AT & T Firewall-Lösung nutzen, entweder on-premise oder Cloud-basiert	AWS, Azure, Blue Jeans, Box, Cisco, Google, HP Helion, IBM, Salesforce, Sungard, VMware	Verfügbar in 52 Ländern. Benötigt kein Netzwerk von AT & T.
	Becom		VELOCLOUD	Ja	Managed Service	Multi-site	National und Internationale Kunden	ja	Physisch oder Virtuell	Internet Gateways, Packet Duplication.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Internet-Paket-Duplizierung Link-Aggregation	WAN, Anwendung, QoS, Traffic Shaping	ja	Müssen ein separates Firewall-Lösung nutzen, entweder on-premise oder Cloud-basiert	AWS, Azure	
	MetTel		VELOCLOUD	nicht bekannt	Managed Service	Single site +	kleine-, Mittelständische- und Enterprise Kunden	ja	Physisch oder Virtuell	Mehrere NNIs bieten hybride MPLS / Breitband-Bereitstellungen an; 4 SD-WAN-Gateways in Nordamerika.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Internet-Gateways, Paketduplikation, Link-Aggregation	WAN, Anwendung, QoS, Traffic Shaping	ja	Müssen ein separates MetTel Firewall-Lösung nutzen, entweder on-premise oder Cloud-basiert	AWS, Azure, Google über Megaport	
	Mitel		VELOCLOUD	nicht bekannt	Managed Service	Single site +	Mitel Phone Kunden	ja	Physisch oder Virtuell	Internet Gateways, Packet Duplication.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Internet-Gateways, Paketduplikation, Link-Aggregation	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	ja	Müssen ein separates Firewall-Lösung nutzen, entweder on-premise oder Cloud-basiert	AWS, Azure, Google	
	Sprint		VELOCLOUD	Ja	Managed Service	Multi-site	National und Internationale Kunden, die einen bedeutenden Teil der Standorte im Sprint Gebiet (USA) haben	ja	Physisch oder Virtuell	Internet Gateways, Packet Duplication.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Internet-Paket-Duplizierung Link-Aggregation	WAN, Anwendung, QoS, Traffic Shaping	ja	Müssen ein separates Sprint Firewall-Lösung nutzen, entweder on-premise oder Cloud-basiert	AWS, Azure	
	TPX		VELOCLOUD	Ja	Managed Service	Single site +	Wiederverkäufer (Resale), Mittelständische- und Enterprise Kunden	ja	Physisch oder Virtuell	Internet Gateways, Packet Duplication.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Internet-Gateways, Paketduplikation, Link-Aggregation	WAN, Anwendung, QoS, Traffic Shaping	ja	Müssen eine separate Sicherheitslösung nutzen, entweder eine Cloud-basierte Firewall oder eine Managed Security-Lösung	AWS, Azure, Google	
	Windstream/ Earthlink		VELOCLOUD	Ja	Managed Service	Multi-site	Wiederverkäufer (Resale), Mittelständische- und Enterprise Kunden	ja	Physisch oder Virtuell	Vollständig verwaltete Implementierung (White-Glove). Fähigkeit zur Bereitstellung eines hybriden SD-WAN- und MPLS-Netzwerkdiseigns.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Internet-Gateways, Paketduplikation, Link-Aggregation	WAN, Application, QoS, Traffic Shaping	ja	Müssen eine separate Sicherheitslösung von Windstream/ EarthLink nutzen, entweder eine Cloud-basierte Firewall oder eine Managed Security-Lösung	AWS, Azure	
	CenturyLink		VERSA	Ja	Managed Service	Multi-site	National und Internationale Kunden, die einen bedeutenden Teil der Standorte im CenturyLink Gebiet haben	ja	Physisch oder Virtuell	Mandantenfähige, verwaltete Implementierung mit umfangreichen Arbeiten zum Erstellen von Profilen nach Kundenanforderungen.	MPLS, Ethernet, Broadband, 3G/4G/LTE	Link Aggregation, redundante Geräte sind bis zu 50% rabattiert	WAN, Anwendung, QoS, Traffic Shaping	ja	Basic - muss eine separate CTL-Firewall-Lösung entweder on-premise oder Cloud-basiert nutzen, Premium - Firewall in das SD-WAN-Edge-Gerät integriert, umfasst Content-Filterung, Intrusion Prävention und Virenschutz	AWS, Azure	100% SLA nur mit CenturyLink WiFi Backup verfügbar. Cisco IWAN auf Roadmap.
	China Telecom		VERSA	Ja (eigenes SD-WAN AS)	Managed Service	Multi-site	mittelständische-, Enterprise- und Large Enterprise Kunden mit Standorten in China	ja	Physisch oder Virtuell	Mandantenfähige, verwaltete Implementierung	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Link Aggregation, Hochverfügbarkeitsoption	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	ja	Stateful Firewall, IPS, AV, IP-Filterung, Dateifilterung, DNS-Sicherheit, DNS-Filterung	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	aktuell 15 SD-WAN Gateways weltweit. Davon 4 in China Festland
	Colt		VERSA	Ja	Managed Service	Multi-site	mittelständische- und Enterprise Kunden mit HQ in Europe od. Japan	ja	Physisch oder Virtuell	Mandantenfähige, verwaltete Implementierung	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Link Aggregation, Hochverfügbarkeitsoption	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	ja	Stateful Firewall, IPS, AV, IP-Filterung, Dateifilterung, DNS-Sicherheit, DNS-Filterung	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	51 Metropolitan Area Networks (MANs), 206 Verwaltete Rechenzentren weltweit
	GTT		VERSA	Ja	Managed Service	Multi-site	Internationale Enterprise, und Large Enterprise Kunden	ja	Physisch oder Virtuell	Mandantenfähige, verwaltete Implementierung	MPLS, Ethernet, Broadband, 3G/4G/LTE	Beim Kunden vor Ort, basierend auf Design, das bei POP ausgewählt oder eingebaut wurde	WAN, Anwendung, QoS, Traffic Shaping	ja	Müssen eine separate Sicherheitslösung von GTT nutzen, entweder eine Cloud-basierte Firewall oder eine Managed Security-Lösung	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	GTT betreibt ein Top-Five, Tier-1-IP-Netzwerk und das transatlantische Fiber-Netzwerk mit der niedrigsten Latenzrate der Branche
	Nitel		VERSA	Ja	Managed Service	Multi-site	mittelständische- und Enterprise Kunden mit HQ in USA	ja	Physisch oder Virtuell	Mandantenfähige, verwaltete Implementierung	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Link Aggregation, Hochverfügbarkeitsoption	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	ja	Stateful Firewall, IPS, AV, IP-Filterung, Dateifilterung, DNS-Sicherheit, DNS-Filterung	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	IPv6 Support Flexible Bereitstellung - Appliance, Bare-Metal, Virtuelle, Cloud. Sehr robuste Firewall-Funktionen umfassen Malware-Schutz, DoS-Prävention, IPS, AV, DNS-Sicherheit und URL-Filterung
	Tata		VERSA	Ja	Managed Service	Multi-site	Internationale Enterprise, und Large Enterprise Kunden	ja	Physisch oder Virtuell	Mandantenfähige, verwaltete Implementierung	MPLS, Ethernet, Broadband, 3G/4G/LTE	Beim Kunden vor Ort, basierend auf Design, das bei POP ausgewählt oder eingebaut wurde	WAN, Anwendung, QoS, Traffic Shaping	ja	Müssen eine separate Sicherheitslösung von Tata nutzen, entweder eine Cloud-basierte Firewall oder eine Managed Security-Lösung	AWS, Azure, Google	Gartner Magic Quadrant Leader 4 Jahre in Folge
	Verizon		VERSA	Ja	Managed Service	Multi-site	Mittelständische- und Enterprise Kunden die einen bedeutenden Teil der Standorte im Verizon Gebiet (USA) haben	ja	Physisch oder Virtuell	Mandantenfähige, verwaltete Implementierung	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Link Aggregation, Hochverfügbarkeitsoption	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	ja	Stateful Firewall, IPS, AV, IP-Filterung, Dateifilterung, DNS-Sicherheit, DNS-Filterung	Verizon SDI	IPv6 Support Flexible Bereitstellung - Appliance, Bare-Metal, Virtuelle, Cloud. Sehr robuste Firewall-Funktionen umfassen Malware-Schutz, DoS-Prävention, IPS, AV, DNS-Sicherheit und URL-Filterung
	Expereo		VIPIELA	nicht bekannt	Managed Service	Multi-site	Mittelständische- und Enterprise Kunden	ja	Physisch oder Virtuell	10G SD-WAN-Box verfügbar	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Überwachung jeder Schaltung basierend auf Anwendungsprofil	WAN, Anwendung, QoS, Lastverteilung (Load Balancing)	Ja (SSL und IPsec)	nicht verfügbar	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	
	Verizon		VIPIELA	Ja	Managed Service	Multi-site	Mittelständische- und Enterprise Kunden die einen bedeutenden Teil der Standorte im Verizon Gebiet (USA) haben	ja	Physisch oder Virtuell	10G SD-WAN-Box verfügbar	MPLS, Ethernet, Broadband, 3G/4G/LTE	Aktiv / Aktiv zur Leistungsüberwachung basierend auf dem Anwendungsprofil, Aktiver Leistungstest pro Anwendungsklasse, pro Pfad	WAN, Anwendung, QoS, Traffic Shaping	ja	Müssen eine separate Sicherheitslösung von Verizon nutzen, entweder eine Cloud-basierte Firewall oder eine Managed Security-Lösung	AWS, Azure, Google HPE, IBM, Oracle, Salesforce	
	Hypercore		ZERO OUTAGES	nicht bekannt	Anbieter unabhängig	None	Wiederverkäufer (Resale), Mittelständische- und Enterprise Kunden	keine	Physisch	Flexibilität mit optionalen Funktionen zur Bereitstellung einer benutzerdefinierten Lösung. Nur Bereitstellung von VoIP-Failover, Inbound-Load-Balancing und Active / Failover SSL-Bonding bei Bedarf als optionale Funktionen.	Alle Transport technologien (MPLS, Ethernet, Broadband, 3G/4G/LTE, Satellite, etc.)	Benachrichtigt Dienstanbieter automatisch im Falle eines Netzwerkausfalls Hardware-Ersatz über Nacht, Hochverfügbarkeitsoption	WAN, Anwendung, QoS, Traffic Shaping	ja	Stateful Inspection Firewall. Umfasst Intrusion Detection / Prevention, cloudbasierte Infiltration und anwendungsspezifische Funktionen	Nein, Sie können jedoch alle Cloud-Verbindungsdienste nutzen, die von Netzbetreibern bereitgestellt werden	