WHITE PAPER

The Role of a Secure SD-WAN in Multi-Cloud Transformation

Table of Contents

The problem with legacy WANs

Legacy WAN architectures are not up to the task of supporting the digital transformation to cloud-first and mobility-first architectures for the simple reason that the data center is increasingly neither the source nor the destination for transactions. The traditional focal point of the network has morphed into a performance bottleneck and single point of failure, with traffic being shuttled through for the sole purpose of anchoring security enforcement. To achieve usable application performance in a cloud environment, branch office and road warrior traffic must be routed in a more direct—but still secure—way.

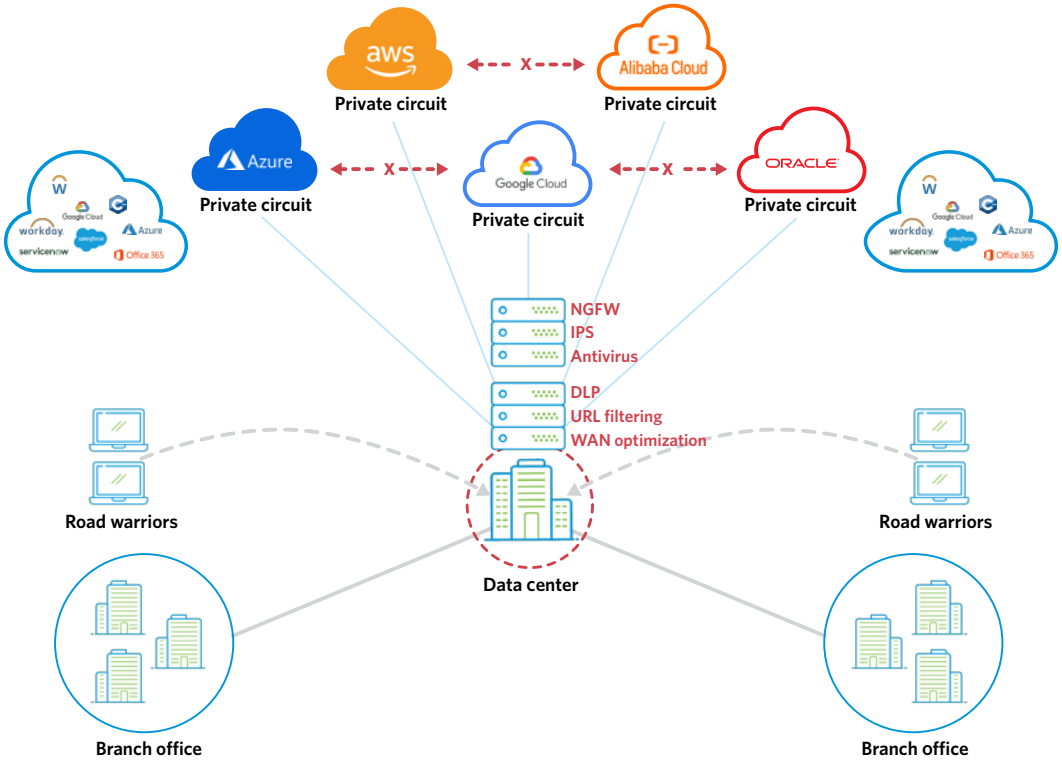

Fig. 1 – In today's world, the data center is a bottleneck in a legacy WAN architecture.

However, keep in mind that purely focusing on the problem of traffic routing efficiency to the cloud from branch offices, as well as for work-from-home and on-the-road users, is necessary but not sufficient to address the new reality of enterprise networking, because organizations today typically leverage multiple cloud providers. Interconnecting these cloud environments is anything but simple. The high-bandwidth private connections utilized—like Azure Express Route or AWS Direct Connect—are not automated, can take days or weeks to deploy, and any traffic between any (for example) Azure and AWS deployments may have to bounce through a company's already overtaxed data center.

Troubleshooting in a legacy architecture also presents challenges. If the IT team receives a call regarding poor video quality, the problem could be anywhere: the WAN optimizer, the QoS devices, deficient WAN circuit bandwidth, network delays. With myriad devices in the network, sourced from a variety of vendors, and faced with complex traffic patterns, the tools and visibility necessary to pinpoint problems at speed are lacking.

In the face of the declining centrality of the data center, adding more hardware to a legacy WAN, even if bigger and better, will only compound the complexity that is itself a core problem. What is needed to improve security and rationalize traffic flows in today's cloud-first and mobility-first world is a paradigm shift to a secure SD-WAN solution that offers a globally flexible cloud-native architecture, allowing deployment of cloud instances with a simple point and click, irrespective of whether they are a public, hybrid or on-premises cloud.

Designing a SaaS-ready architecture

A SaaS-ready architecture, as shown in Figure 2 below, is achieved with an SD-WAN device at each site, ubiquitous internet access, and strategically located SD-WAN gateways to provide efficient routing from any site or mobile location to the cloud. Of course, an internet break-out in theory increases your attack surface. But a secure SD-WAN architecture brings integrated full-function security policy and enforcement—malware protection, sandboxing, intrusion prevention, NGFW, data loss prevention and more—at each location and network access point.

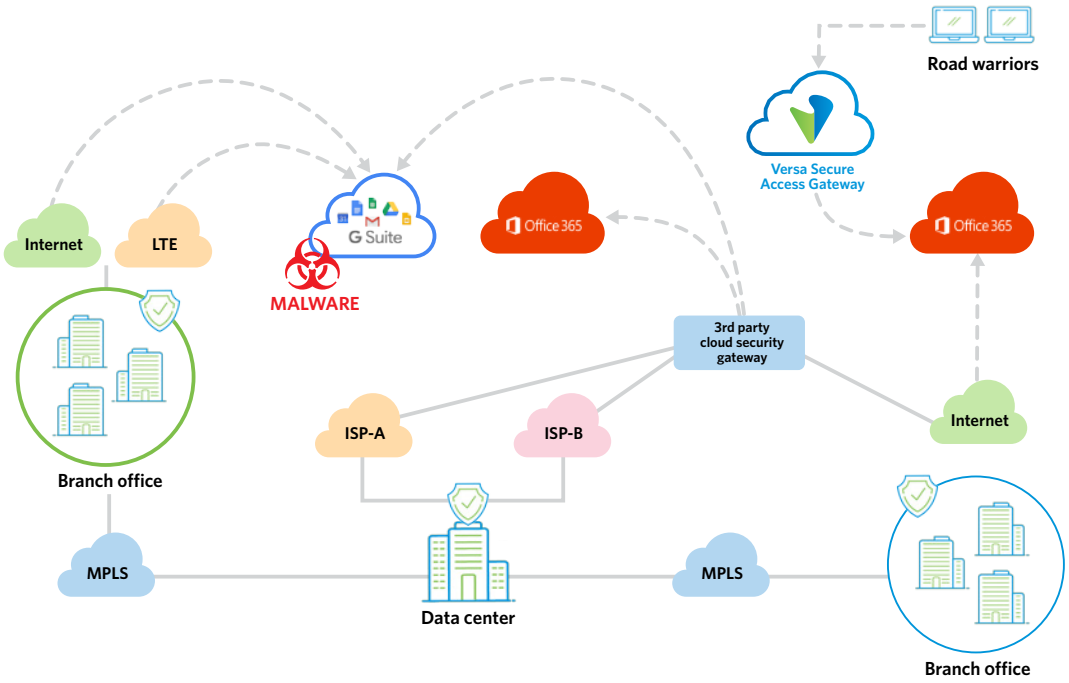

Fig. 2 - In a SaaS-ready architecture, a secure SD-WAN provides security at each location and network access point.

With SD-WAN devices at sites and gateways, traffic can now securely use any transport available to it for the most direct access to the cloud. The secure SD-WAN software instantly identifies traffic flows to SaaS applications such as Office 365, Salesforce, or Gmail, and locally breaks out that traffic. It applies optimal multi-dimensional policies—for best path selection, QoS, and security—and guarantees consistent security posture and application performance. Security and application performance go hand-in-hand: one cannot be compromised in favor of the other.

A secure SD-WAN solution also delivers extensive automation to ensure unified security policy is enforced across all devices, all locations, all sites, and all users. It eliminates repeated, tedious and error-prone site-specific configurations: no more accidental security loopholes due to misconfiguration.

This SaaS-ready architecture suffices for enterprises using a single cloud service, but often a multi-cloud architecture is more suitable to most effectively address business needs. A secure SD-WAN solution also provides the flexibility for quick and easy integration with third-party cloud services, resulting in a hybrid architecture that shares a single security model between the secure SD-WAN and the third-party service providers

Solving multi-cloud connectivity challenges

Cloud environments are renowned for being agile, elastic, and fault-tolerant. While this is indeed true for cloud-based computer storage services, it's not quite as true for networking services. Cloud environments lack many familiar and indispensable routing capabilities, such as multicast support, fast reroute, and equal cost multi-path routing. In reality, routing within the cloud is extremely static in nature: every prefix, mask, and next-hop must be explicitly programmed. Maintaining a static routing table for a large network is extremely cumbersome and vulnerable to errors that can cause application disruptions and routing outages. It also makes designing an architecture for high availability very complex.

A secure SD-WAN that includes a cloud high availability (HA) engine keeps track of the health of the network virtual appliances (NVAs) where your workloads are running as well as the connectivity between them. The SD-WAN cloud HA engine instantly detects failures in NVAs or their routing path, and automatically reconfigures cloud routing and workload distribution to ensure operational continuity.

To add further complexity, multi-cloud environment may encompass various IaaS and SaaS public clouds, often in addition to a dedicated on-premises cloud. Generally, this network model avoids vendor lock-in, minimizes costs and enhances disaster recovery options, but it does not come without challenges.

Let's consider a typical application such as a Customer Relationship Management (CRM) solution—enterprises today may deploy the web services aspects on Azure, the application portion on AWS, and the database and storage on Google Cloud. The interconnection of these three clouds to render the entire application usable immediately poses several complications:

- How to quickly and securely connect the on-premises resources to the clouds
- How to route traffic optimally between the Azure, AWS and Google environments
- How to ensure that precious customer data are not exfiltrated or leaked from any of the clouds

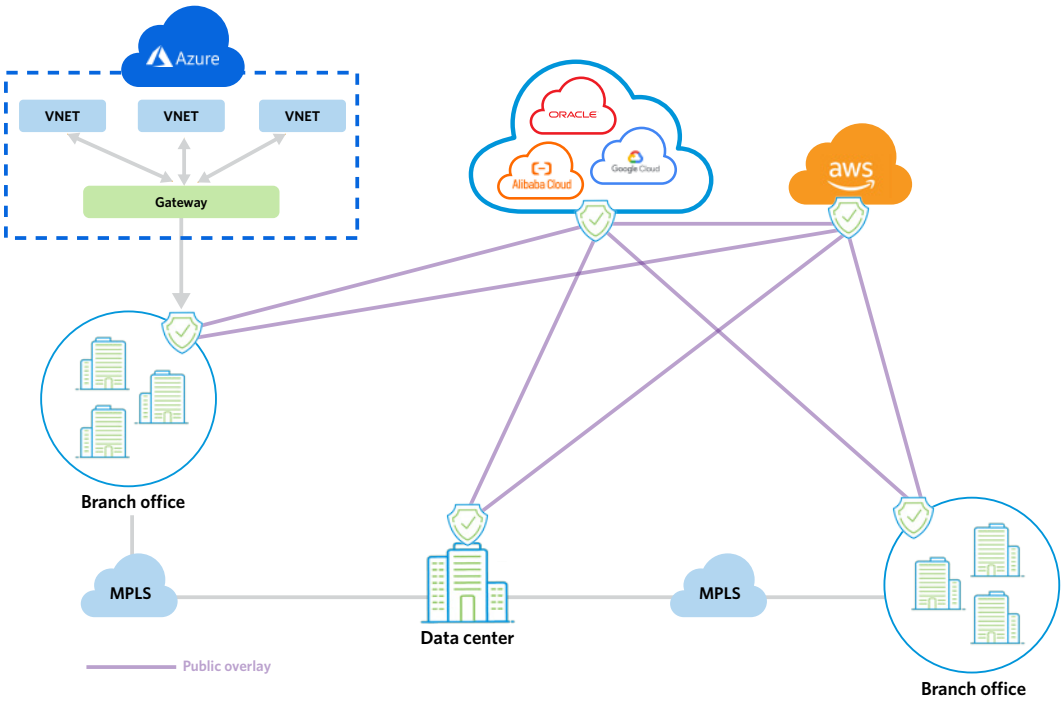

Fig. 3 – A secure SD-WAN seamlessly establishes dynamic overlay IPSec connectivity across disparate clouds for both the data and control planes.

The SD-WAN infrastructure eliminates the multi-cloud interconnectivity challenges by automatically discovering, and seamlessly establishing, dynamic overlay IPSec connectivity to each cloud for both the data and control planes to each cloud. The connectivity topology is ready in minutes—fully secured with encryption—and the control plane across the disparate clouds is normalized by the IPSec tunnel mesh to provide complete global visibility of your network.

If a user or business activity needs to use a gateway service, such as Azure Virtual WAN or AWS Transit Service, the secure SD-WAN brokers this ability by automatically discovering the nearest gateway available and creating an integration between it and other cloud and on-premises environments without requiring the user to log into the cloud subscription.

Simplifying operations through multi-cloud automation

A key benefit of a multi-cloud transformed architecture is that it significantly simplifies operations. IT staff no longer has to understand the intricacies of each cloud environment nor retain experts trained in each of the multiple user interfaces of the various providers and pieces of equipment. Instead the SD-WAN software provides you with a single-pane-of-glass view that shows where each workload is deployed, who is accessing them, and all the active users. Additionally, it can deliver real-time analytics on end-to-end application and performance trends as well as cross-network tools to aid troubleshooting.

The intelligence source in the secure SD-WAN multi-cloud architecture is the orchestrator, or director, in charge of automating centralized provisioning and management—providing true zero-touch administration that requires absolutely no intervention by the cloud administrator.

At the same time, it orchestrates configurations and settings into the different cloud environments, including the cloud gateway services, significantly reducing deployment time. The complete lifecycle, from creation to termination, is orchestrated from the SD-WAN director using a single pane of glass.

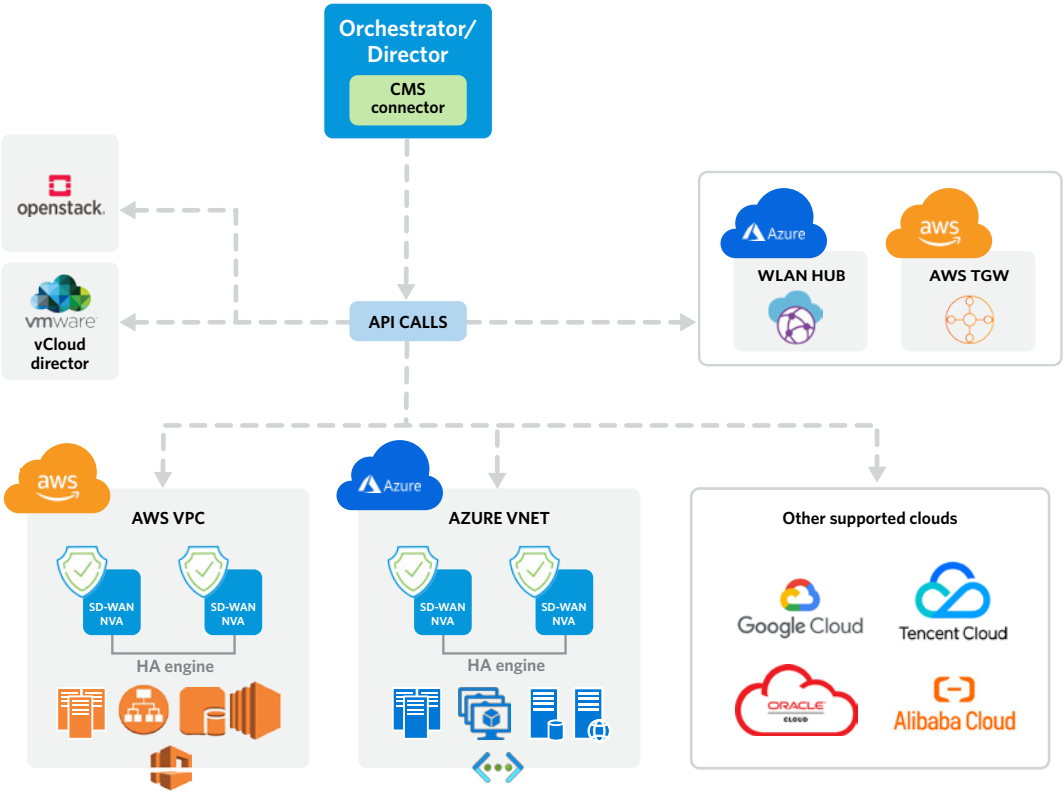

Fig. 4 – A secure SD-WAN supports integration with third-party cloud environments.

The secure SD-WAN also provides the flexibility to integrate other third-party cloud environments—non-native clouds such as OpenStack as well as other clouds like Google Cloud Platform (GCP), Oracle, Alibaba and TenCent—in a completely distributed environment that can be leveraged for enhanced performance or disaster recovery.

Keep in mind that your security policy is also normalized across your entire environment, including all the clouds, as the secure SD-WAN director can ensure that a consistent security language is spoken across all these different environments, hiding and automating the complexities of each cloud provider's unique APIs, protocols, and configurations.

Achieving full operational visibility

The automated, centralized orchestration provided by a secure SD-WAN enables cohesive visibility of applications, users, workloads, databases, web servers, and security policy violations without requiring anyone on staff to understand the intricacies of the specific clouds and their unique tools.

With the secure SD-WAN single-pane-of-glass orchestration you can view a global map and pinpoint the exact geolocation of any particular workload, and which users are accessing that workload.

If a workload is being attacked by an external actor, you can block it with a single click, as well as access deep analytics to give more insight into the attack: who is trying to bring down your service, what kind of attack are they using, and how can it be mitigated. With full visibility comes complete data, and comprehensive trend analysis allows you to adjust your baseline security posture across all environments.

A pane that shows device utilization can help you manage performance. If the CPU use of any specific device exceeds a given threshold, you can create an auto-scaling policy to instantiate more devices and increase aggregate performance. You can also see exactly which users, in which regions, are using your service.

These displays help you to architect high availability or prepare a design for future business expansion requirements. And it is all done from an applications perspective and presented on a single analytics dashboard.

Comparing multi-cloud services: Azure, AWS and Google Cloud

Let's take a closer look at three of the popular cloud services—Azure, AWS, and Google Cloud—and see how they stack up in terms of networking services, operations and security.

Networking services

Each cloud service has different throughput limitations between them, and each has its own individual way of connecting to them from your on-premises cloud. While there are features like availability sets and availability zones that can be leveraged to increase resilience, you are still unprotected if a networking convergence takes place due to a connectivity failure, or if an external third-party service-chaining service becomes unavailable.

Networking	Azure	aws	Google Cloud
Virtual networks	Azure VNet	Amazon VPC	Google VPC
Load balancer	Azure Load Balancer	Elastic Load Balancer	Cloud Load Balancer
Dynamic routing	No (UDR/static within VNET)	No (Custom route/static within VPC)	No (Custom route/static w/in VPC)
Interconnect	Azure ExpressRoute	AWS Direct Connect	Cloud Interconnect
Gateway service	Azure Virtual WAN	AWS Transit Gateway	Preview
VPN service	Azure VPN Gateway	AWS VPN	Cloud VPN
Tunnel limits	30 per VPN GW	10 per VPN GW and 30 per region	10 per project
Max throughput	1.25 Gbps per tunnel	1.25 Gbps per tunnel	1.5 Gbps per tunnel
VM high-availability	Not supported natively	Not supported natively	Not supported natively

Fig. 5 - Networking features comparison

Operations

Each cloud provider offers its own interface and tools—Azure Network Watcher, AWS X-ray, Google Cloud monitoring and logging—and enterprise network design teams are expected to sift through all the nuances of these tools to attempt to build a cohesive picture of business metrics like end-to-end application performance. Besides not being a scalable strategy, there is also always a gap in understanding about how an application actually works across these clouds, how a user flow truly works, or how to determine if a workload is being attacked anywhere in this environment, and if so, how and by whom.

Operations	Azure	aws	Google Cloud
Monitoring	Application Insights	Amazon CloudWatch	Cloud Monitoring
Logging	Log Analytics	Amazon CloudWatch Logs	Cloud Logging
Audit logging	Log Analytics	AWS CloudTrail	Cloud Monitoring
Debugging	Network Watcher	AWS X-Ray	Cloud Debugger
Performance tracing	Network Watcher	AWS X-Ray	Cloud Trace
Deployment	Resource Manager	AWS CloudFormation	Cloud Deployment Manager

Fig. 6 - Operations features summary table

Security

Security today is a shared experience with the cloud service providers, which means that it is as much the responsibility of the cloud provider as the enterprise to secure workloads from unauthorized access, prevent data breaches, and ensure that quality is consistent.

Security	Azure	aws	Google Cloud
IAM	Azure Active Directory, ADDS	Amazon Identity Management	Cloud Identity Access Management
Threat detection	Advanced Threat Protection	Amazon Guard Duty	Event Threat Detection
Vulnerability scanner	Security Center	Amazon Inspector	Web Security Scanner

Fig. 7 - Security services summary table

An SD-WAN bridge

A Secure SD-WAN can help bridge all these disparities and complexities among the various cloud implementations. It speaks a "common language" across the environments, automates setup, coordinates configurations, and helps with routing and rerouting to aid in HA designs.

Multi-cloud challenges and solutions summarized

Considering first and foremost security challenges like exposure to data exfiltration and malware in the cloud, a secure SD-WAN architecture—with security built into the very fabric from the ground up—allows enterprises to deploy multi-dimensional L2-L7 policies including all the security measures the organization requires: data loss prevention, unified threat management, IPS filtering, extraction of malware, et al. And all of these are provided with the flexibility to turn each one on or off for different environments, as needed.

Compliance and visibility concerns are addressed by a secure SD-WAN analytics dashboard capable of unifying the entire visibility plane across on-premises, hybrid and public clouds, and usually compatible with existing licenses you may already have in your network. The SD-WAN solution can provide historical analysis to aid in investigations and the forensics of user flows and data to determine if a possible breach may have happened in your network, and if so, from where and how they gained access.

The table below summarizes the major challenges that inhibit multi-cloud deployment and how a secure SD-WAN can address them.

Challenges	Secure SD-WAN Solutions		
Data Security, Data Leakage, Malware, Ransomware	✔ Integrated full security stack	✔ Complete application visibility	✔ Multi-dimensional policy control
	✔ Thousands of pre-defined applications	✔ Millions of pre-defined IP reputation DB	✔ Thousands of pre-defined IPS signatures
	✔ DPI with NGFW + NGIPS	✔ File filtering, DNS filtering, IP filtering	✔ URL filtering with SSL inspection
Compliance and lack of visibility	✔ Historical SD-WAN, WAN underlay analytics	✔ Big data security analytics	✔ Compatible with existing SIEM
Misconfigurations and lack of automation	✔ Powerful CMS cloud orchestration	✔ Templatized 3rd party integration	✔ Consistent enterprise security posture
	✔ True zero touch provisioning	✔ Full support for REST API's	
Need for multi-cloud, hybrid cloud deployment strategy	✔ Deploy on any public / on-premises cloud	✔ Seamless integration with gateway services	✔ Cloud-based TCP optimization
	✔ Dynamic multi-cloud IPSec connectivity	✔ Comprehensive cloud security	✔ Purpose built cloud high availability
SaaS breakout challenges	✔ Active, passive, hybrid SaaS monitoring	✔ First packet SaaS endpoint identification	✔ Powerful 3rd party SaaS integration
	✔ Vera Link Score technology	✔ SaaS gateway with low latency peering	
Staff expertise and training	✔ Single pane for public, private, SaaS clouds	✔ Remove barriers to multi-vendor expertise	✔ Simplifies cloud operations

Fig. 8 - Challenges and solutions for multi-cloud deployments.

Leveraging automation in an SD-WAN solution is paramount, taking advantage of a rich set of pre-built applications and predefined signatures to help users migrate to these services quickly.

Misconfigurations are one of the leading causes of outages. A high degree of automation in a secure SD-WAN solution eliminates the error-prone and repetitive site-specific tasks that give rise to misconfigurations. Instead, IT staff can use a single point-and-click to deploy consistent and complete configurations across the entire network.

Deploying in multi-cloud environments relies on SD-WAN features such as TCP optimization. The SD-WAN software stack is effectively a proxy to ensure network capabilities such as compression caching is done appropriately. By leveraging these types of built-in features, the SD-WAN can establish a highly optimized end-to-end service flow across interconnectivity between different clouds.

The SD-WAN stack is able to breaks out applications that move to the cloud by identifying the very first packet. It is also key to ensuring that traffic truly destined for the data center is not broken out unnecessarily, causing routing delays. Several internal SD-WAN technologies track gateways and links across the geography so that optimal access is always guaranteed to every user—whether at home, on the move, or at an office.

Many enterprises are also hindered by the barrier to staff expertise and training in the nuances of management and provisioning across several different cloud environments. All of this complexity is completely simplified with automated workflows from the SD-WAN orchestrator service.

Conclusion

A secure SD-WAN with top-of-class networking, security, visibility, automation and performance capabilities all built ground-up into the architecture can help you overcome the challenges and complexities of multi-cloud environments—while at the same time allowing you to reap the benefits that these cloud deployments can bring to your networking environment, application environment, and cost of ownership. The principle advantages over legacy WAN architectures include:

- A single-click true zero-touch SD-WAN enables a high-speed, low-latency fabric with all the familiar routing capabilities and HA characteristics extended into the cloud(s).
- The SD-WAN orchestrator simplifies multi-cloud operations through automation and normalization—allowing you to gain application insights and end-to-end visibility through a cloud-agnostic single-pane-of-glass.
- The SD-WAN stack facilitates compliance enforcement through integrated reporting and a consistent security posture across the entire environment: public cloud, hybrid cloud, and on-premises.
- Multi-dimensional security is enforced with an advanced security stack comprised of a full set of unified threat management features.
- The SD-WAN dramatically enhances application performance by ensuring SaaS optimization.
- Real-time capacity demands are met by leveraging elastic auto-scaling and network intelligence.
- A secure SD-WAN offers a global, flexible deployment model: consume applications on-premises or as-a-service with zero upfront costs.

About Versa Networks

Versa Networks, the leader in single-vendor Unified SASE platforms, delivers AI/ML-powered SSE and SD-WAN solutions. The platform provides networking and security with true multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and Service Providers.

Thousands of customers globally with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, BlackRock Inc., Liberty Global Ventures, Princeville Capital, RPS Ventures and Triangle Peak Partners. For more information, visit www.versa-networks.com or follow Versa Networks on X (Twitter) @versanetworks.

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com