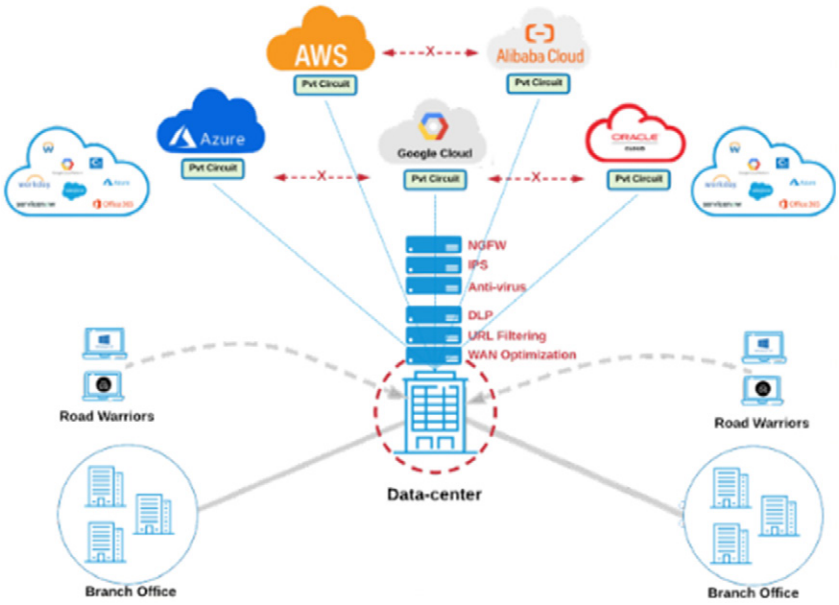
WHITE PAPER

Secure SD-WAN and Multi-Cloud Transformation

Every CIO is frustrated to hear from users that the network is so slow that productive work just cannot be done. This despite regular upgrades to bigger and better hardware, and constant additions of new devices: higher capacity and increasingly capable NGFWs, WAN optimizers, proxies, sandboxes. Legacy WAN architectures are simply not up to the task of supporting digital transformation trends such as cloud-first and mobility-first architectures—email is no longer an on-premises application but is instead hosted as a SaaS Office-365 service; corporate file sharing has moved into the cloud, including Microsoft Azure, Amazon Web Services (AWS), Google Cloud, Oracle and Alibaba.



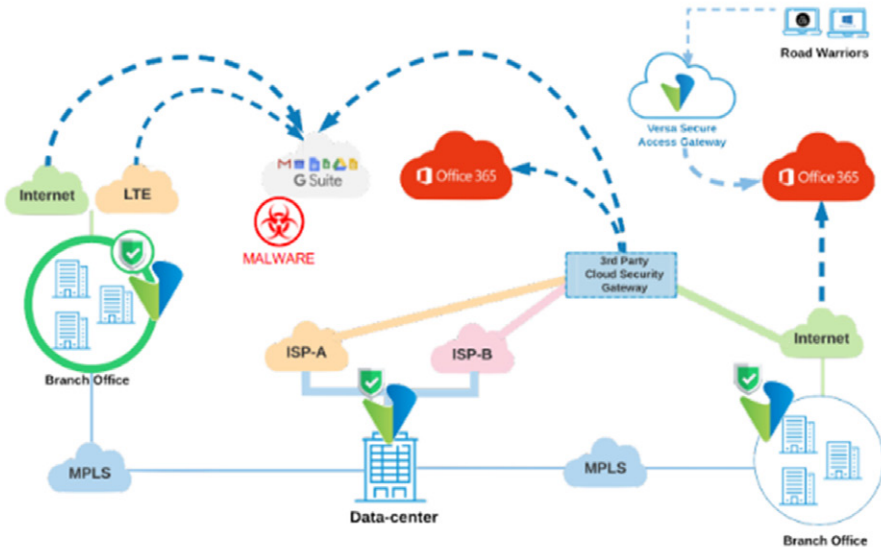
The data center is increasingly neither the source nor sink of transactions. The erstwhile focal point of the network has morphed into a performance bottleneck and single-point-of-failure merely shuttling traffic through for the sole purpose of anchoring security enforcement. To achieve usable application performance in a cloud environment, branch office and road warrior traffic must be routed in a more direct—but still secure—way.

Troubleshooting in a legacy architecture is equally challenging. 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 different devices, sourced a plethora of vendors, in the network and complex traffic patterns, the tools and visibility to pinpoint problems are meagre.

Solving traffic routing efficiency from branch offices, as well as work-from-home or on-the-road users, to the cloud is necessary but not sufficient. Organizations typically leverage multiple cloud providers or services. Interconnecting these cloud environments is anything but simple. Typical organizations utilize high bandwidth private connections—Azure Express Route, AWS Direct Connect—but these are not automated and can take days or weeks to deploy. They are also isolated islands so that traffic from Azure to AWS may have to bounce through your already over-taxed data center.

SaaS Transformed Architecture

A SaaS-ready architecture is achieved with an SD-WAN device at each site, ubiquitous Internet access, and using strategically located SD-WAN gateways to provide efficient routing from any site or mobile location to the cloud. Of course, an Internet break-out immediately increases your attack surface. But a Secure SD-WAN architecture circumvents this exposure by bringing integrated full-function security policy and enforcement—malware protection, sandboxing, intrusion prevention, NGFW, data loss prevention and more—to 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, security—and guarantees consistent security posture and application performance. Security and application performance go hand-in-hand: one cannot be compromised for 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.

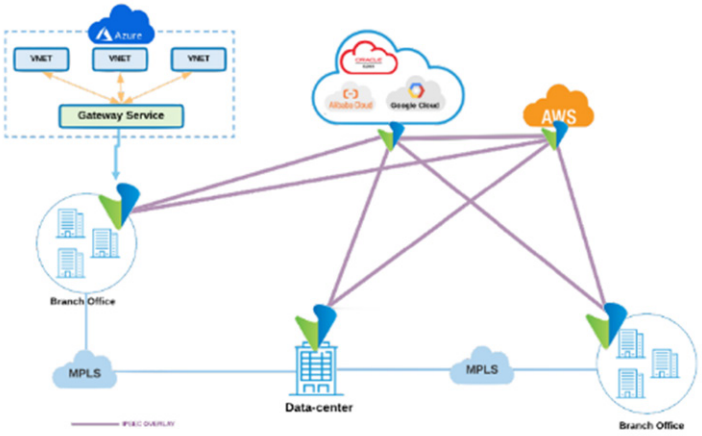
This SaaS-ready architecture suffices for enterprises using a single cloud service, but often a multi-cloud architecture is more suitable to most effectively address business needs. A Secure SD-WAN solution also provides the flexibility for quick and easy integration with 3rd party cloud services, resulting in a hybrid architecture that shares a single security model between the Secure SD-WAN and the 3rd party service provider(s).

Multi-Cloud Transformed Architecture

A 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 Customer Relationship Management (CRM)—enterprises today have the flexibility to choose a cloud provider based on a best fit of price and feature set. For example, you 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.

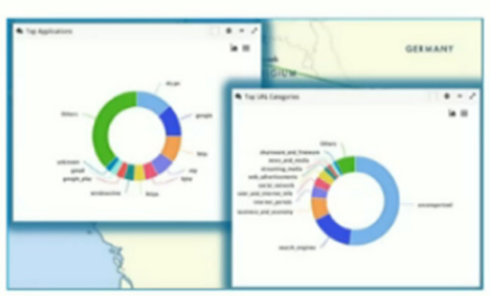
- How to quickly and securely connect the on-prem resources to the clouds
- How to route traffic optimally between the Azure, AWS and Google environments
- How to ensure that precious customer data are not exfiltrated or leaked from any of the clouds



A Secure SD-WAN solution offers a global flexible cloud-native architecture, deploying cloud instances with a simple point and click, irrespective of whether it is a public, hybrid or on-prem cloud, or multiples thereof. The SD-WAN infrastructure eliminates the multi-cloud interconnectivity challenges by automatically discovering, and seamlessly establishing, dynamic overlay IPSec connectivity 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.

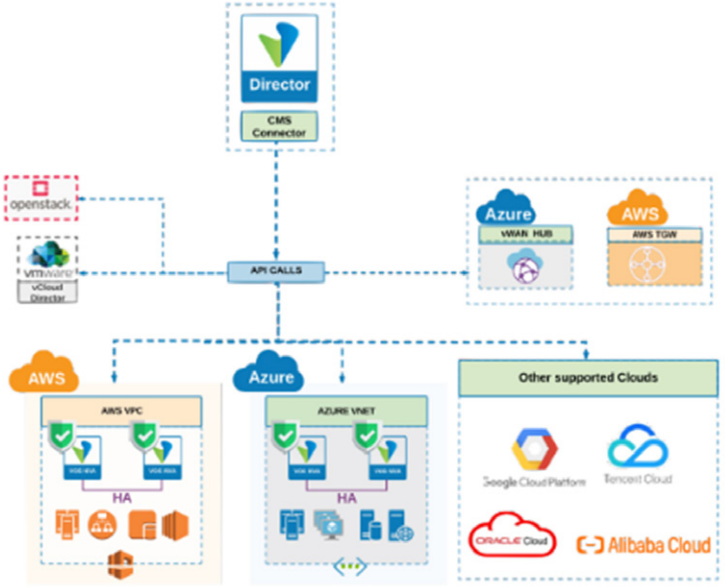
If a user or business activity needs to use a gateway service, such as Azure Virtual WAN or AWS Transit Service, the Secure SD-WAN brokers this ability by automatically discovering the nearest gateway available in a subscription and creating an integration between your on-premises or other cloud environments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

Multi-Cloud Automation



A key benefit of a multi-cloud transformed architecture is that it significantly simplifies operations. Your IT staff no longer has to understand the intricacies of each cloud environment, or 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 delivers 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 one single-pane-of-glass.



The Secure SD-WAN also provides the flexibility to integrate other 3rd party cloud environments—non-native clouds such as Openstack as well as other clouds such as Google Cloud Platform (GCP), Oracle, Alibaba and TenCent—in a completely distributed environment that can be leveraged for enhanced performance or disaster recovery.

Your security policy is also normalized across your entire environment, including all the clouds, as the Secure SD-WAN director ensures 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.

Cloud environments are renowned for being agile, elastic, and fault-tolerant. While this is indeed true for 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. In reality, routing within the cloud is extremely static in nature: every prefix, mask, and next-hop must be explicitly programmed. As you already know, maintaining a static routing table for a large network is extremely cumbersome. Not to mention vulnerable to errors that cause application disruptions and routing outages. It also makes architecting for high availability very complex.

A key benefit therefore is a Secure SD-WAN that includes a Cloud HA Engine that keeps track of the health of the NVAs (Network Virtual Appliances) where your workloads are running as well as the connectivity between them. The SD-WAN Cloud HA Engine instantly detects failures in either NVAs or their reachability, and automatically reconfigures cloud routing and workload distribution to continue your business operation regardless of the outage.

Multi-Cloud Service Comparison

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

Dynamic routing and resilient networking do not feature strongly anywhere. There are also 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 3rd party service-chaining service becomes unavailable.

Networking	Azure	aws	Google Cloud Platform
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 within VPC)
Inter-connect	Express Route	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

Operations

Each cloud provider offers its own interface and tools—Azure Network Watcher, AWS X-ray, Google Cloud monitoring and logging—and enterprise design teams are expected to sift through all the nuances across these respective 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 or by whom.

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

Security

Security today is also a shared experience with the cloud(s), which means that it is as much the responsibility of the cloud provider as the enterprise to secure workloads from unauthorized access, preventing data breaches, and ensuring that quality is consistent.

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

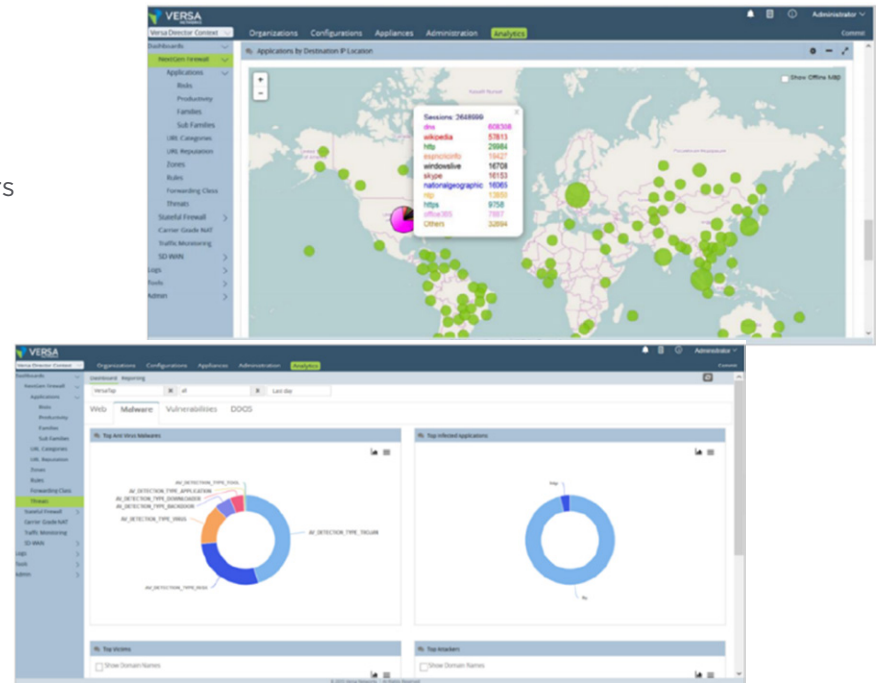
An SD-WAN Bridge

A Secure SD-WAN can help bridge all these disparities and complexities between 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.

Full Operational Visibility

The Secure SD-WAN centralized orchestration provides a portal for 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 exactly pinpoint the 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.

Comprehensive trend analysis allows you to adjust your baseline security posture across all environments.

A pane that shows device utilization helps you manage performance. If, perhaps, 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 application perspective and presented on a single analytics dashboard.

Cloud Adoption

The table below summarizes the major challenges that inhibit multi-cloud deployment.

Challenges	Solutions		
Data Security, Data Leakage, Malware, Ransomware	✔ Comprehensive full security stack	✔ Complete application visibility	✔ Multi dimensional policy control
	✔ 3600+ pre-defined applications	✔ 12+ million pre-defined IP repudiation DB	✔ 30000+ 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 supports 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 for multi vendor expertise	✔ Simplifies cloud operations

One of top-most considerations is always security: anguish about 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, and more. 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 the Secure SD-WAN analytics dashboard that unifies the entire visibility plane across on-premises, hybrid and public clouds. It is also compatible with existing licenses you may already have in your network. The SD-WAN solution provides historical analysis to aid in investigations and 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.

Automation in the SD-WAN solution is paramount, offering a rich set of pre-built applications, and a set of predefined signatures, to help users to migrate into these services very 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 establishes 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 ensure that traffic truly destined to the data center is not broken out unnecessarily, causing routing delays. Several internal SD-WAN technologies track gateways and links across the geography such that optimal access is always guaranteed to every user—whether at home, on the move, or in 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.

Next Steps

Multi-cloud environments are a reality for most enterprises, especially the larger ones. Different cloud providers have different strengths, features, pricing and geographic presence. Most enterprises also still have a large investment in on-premises resources and many run their own private clouds.

A Secure SD-WAN with top-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.

- **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.

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