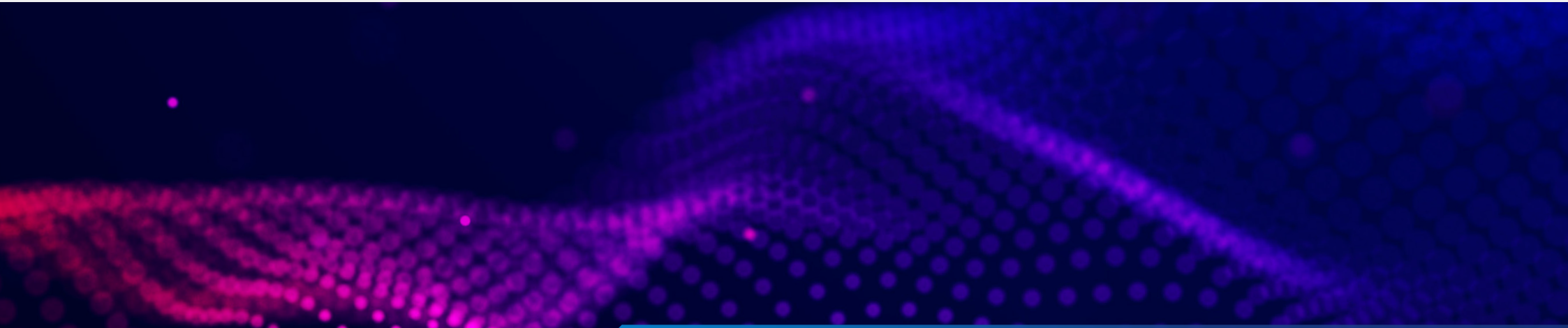

vmware
GET STARTED
Cloud Networking and Security with VMware
Network Elasticity, Resiliency, and Comprehensive Security at Your Fingertips.



Welcome

By the end of 2020, the volume of global ecommerce grew in one year by as much as experts had expected it to grow over the next five years [1]. This experience has shaken existing loyalties, with up to 75% of consumers saying they have tried new brands during lockdown [2].

To win in this accelerated, hyper-competitive and hyperconnected market, your company must offer the best possible user experience. But you must also be capable of re-orienting your operations and infrastructure at speed, to meet rapidly changing consumer demands and market conditions.

With VMware Cloud Networking, you can do both. VMware Cloud Networking includes a set of modular, interoperable cloud and virtualization technologies that provide the network elasticity, performance, and operational agility required to bring new computing resources online, including extra VMs and containers, network connectivity, load-balancers, security policies and so on.

1. https://techcrunch.com/2020/08/24/covid-19-pandemic-accelerated-shift-to-e-commerce-by-5-years-new-report-says
2. https://www.retaildive.com/news/what-covid-19-did-to-customer-loyalty/583377

In this way, your network scales with user demand to maintain a consistently high level of user experience. With a streamlined and intuitive suite of administration tools, you always have complete oversight of network performance. So, you're always in control.

For application owners and developers, this provides the perfect balance of agility, performance and simplicity. They know that no matter what the load, the architecture which underpins their application will flex and scale to maintain exactly the standard of user experience they're aiming for.

System reliability engineers (SREs) benefit from having service level objectives (SLOs) woven into the fabric of the network. Multi-site and -platform tools allow for centralized monitoring, management and troubleshooting. Together, these tools simplify the job of administration and make it easier to hit service-level agreements and minimize downtime.

Infrastructure administrators can use the built-in autoscaling, load balancing and secure cloud connectivity to ensure that storage, computer and networking resources are always available to the required standards. Using these administration tools, they can apply unified SLO-thresholds and other policies to the whole network, regardless of underlying infrastructure. The architecture is zero-trust by design and uses built-in encryption which allows resources that are spun-up dynamically, without manual configuration, to be secured to the highest standards.

In this briefing, we explain how businesses can use VMware Cloud Networking to deliver peak performance while still being as agile as the market demands. We look at different components and explain how they can improve your company's performance in a way that has a direct and positive impact on the top and bottom line.

The use cases in this document are based on real-world case studies. But they often include details from more than one deployment. For this reason, we have used fictional rather than real company names.

Contents

VMware Cloud Networking: An Overview

VMware Cloud Networking is a set of intelligent, integrated but modular technologies and services that extend virtual networking and security capabilities from edge to core to cloud for any workload running in VMs, containers, or bare metal.

A recent study on VMware Cloud Networking solutions by Forrester showed a 110% return on investment in just the first 12 months [3].

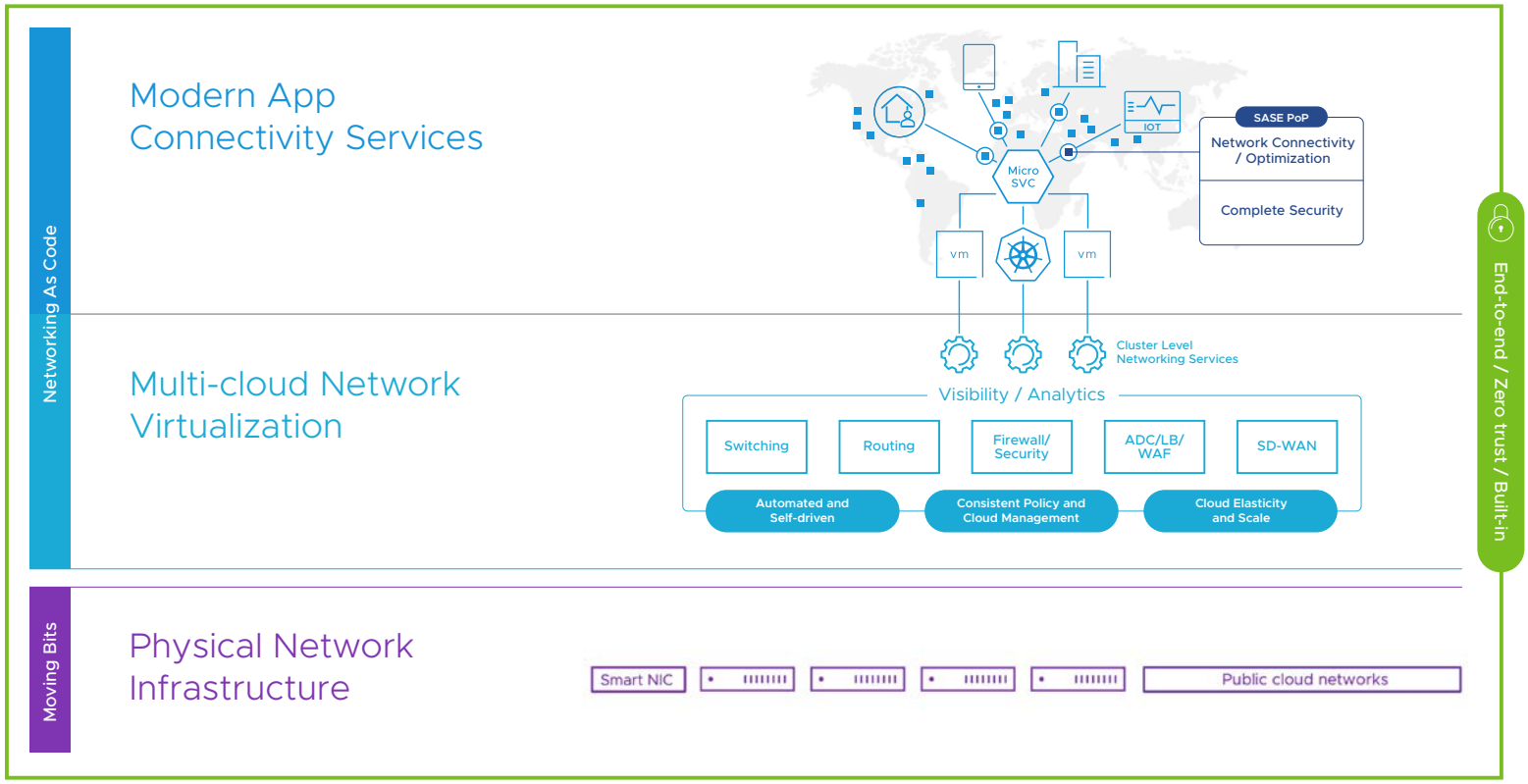


Figure 1 - VMware Cloud Networking

3. https://www.vmware.com/learn/939400_REG.html?cid=7012H0000018OY

The solution includes, among other things:

Modern Apps Connectivity Services

A service mesh with end-to-end connectivity, continuity, resiliency, security, compliance and observability for modern applications in single and multi-cloud environments.

Superior user experience through service level objectives (SLOs) enforcement allowing applications to function with no disruption.

A global load balancer, integrated to the containers, which dynamically scales to provide connectivity services. Regardless of what cluster a container is deployed.

Multi-Cloud Networking and Security

A complete Layer 2-to-Layer 7 networking and security solution with VMware NSX-T providing multi-compute platform, multi-cloud networking.

Policy-based security, elastic load balancing, and web application firewalling (WAF) with the NSX Advanced Load Balancer.

Optimized secure transport over WANs for delivering high-performance, reliable access to cloud services, private data centers and SaaS applications.

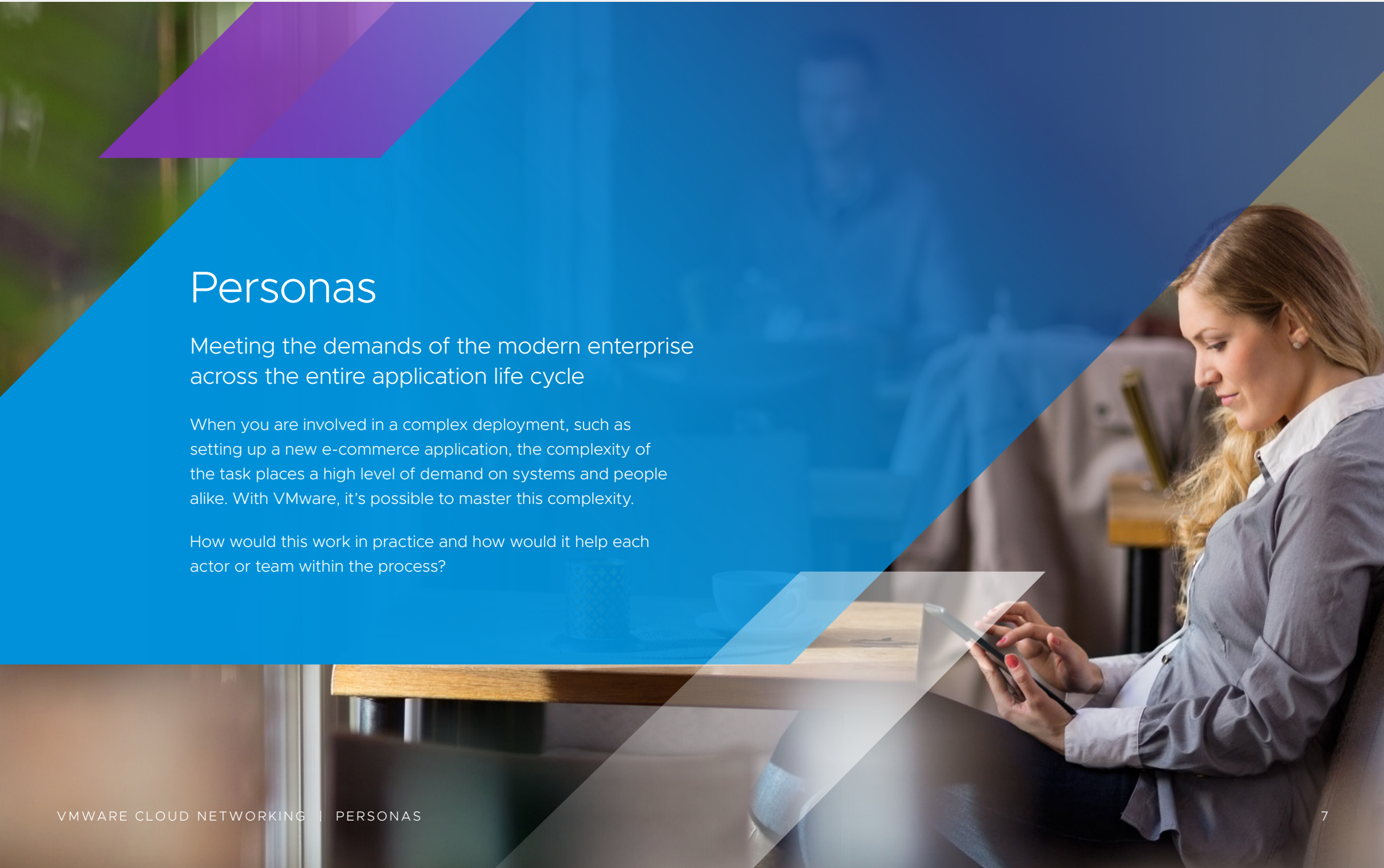
Unified edge and cloud service models with a single place to manage business policy, configuration and monitoring.

Network management tools that provide unified visibility and control across hybrid and multi-cloud environments with a single place to manage business policy, configuration and monitoring.

An open-source container network interface (CNI) that integrates with virtual machines (through NSX) and containers in hybrid cloud environments.

VMware Cloud Networking helps enterprises provide an unmatched public cloud experience on-premises. Not only does this provide an efficient and cost-effective cloud infrastructure, but it also removes the need for inefficient IT ticket requests and long waits for networking and security changes. Whether you're building a new hybrid cloud infrastructure or moving existing applications onto the cloud, VMware helps you manage your cloud environment in the smoothest and most cost-effective way possible to achieve the greatest benefit to the business and the highest return on investment (ROI). A recent study by Forrester found that VMware Cloud Networking showed a 110% return on investment in just the first 12 months [3].

3. https://www.vmware.com/learn/939400_REG.html?cid=7012H0000011I8OY



Personas

Meeting the demands of the modern enterprise across the entire application life cycle

When you are involved in a complex deployment, such as setting up a new e-commerce application, the complexity of the task places a high level of demand on systems and people alike. With VMware, it's possible to master this complexity.

How would this work in practice and how would it help each actor or team within the process?

Application owners

Application owners and developers shorten the time it takes to get their product to market.

In an accelerating marketplace, app owners and developers need to be able to respond to changing customer requirements quickly and securely. The modern application is dynamic and highly adaptive to changes in demand. It lives across multiple clusters and clouds. And it is highly distributed with hundreds of microservices servicing the requirements of rapid feature releases, high resiliency, and on-demand scalability.

This requires an environment which supports heterogenous development standards, languages and distributed application infrastructures that spans public and private architectures.

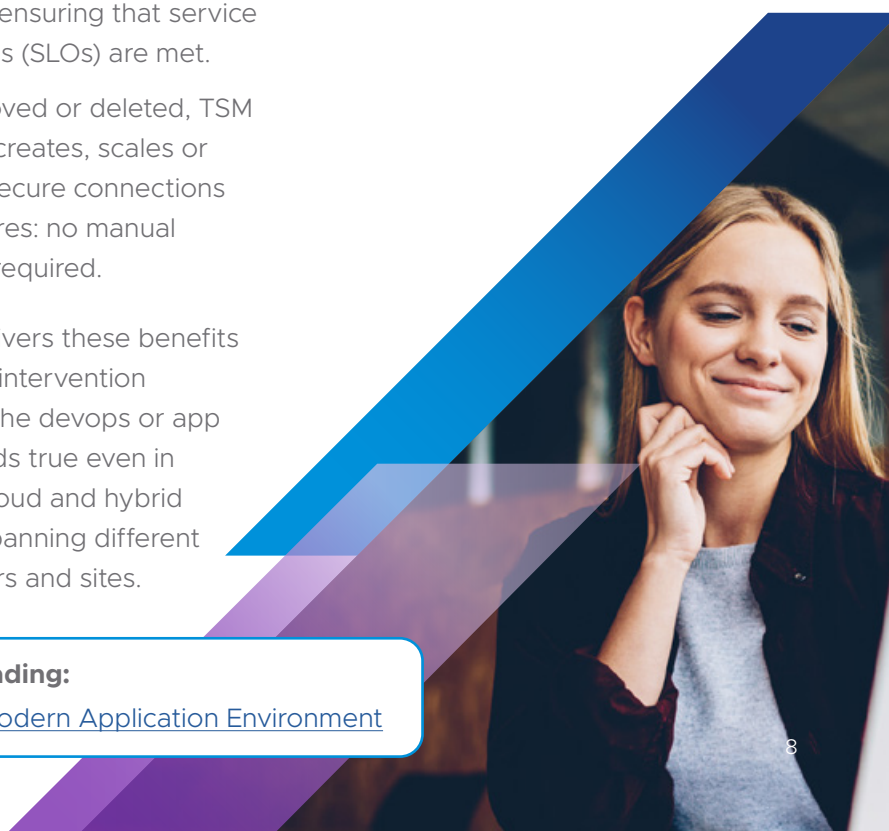
Tanzu Service Mesh simplifies the connection, observability, and protection of these applications across any runtime or cloud, providing a consistent way to connect and protect thousands or tens of thousands of individual microservices. It also makes it easier to operate and integrate your workloads through a new level of abstraction in the form of a global namespace that allows you to connect, manage, and secure applications across clouds and workloads. This provides full services and application mobility, giving you the freedom to choose tenancy and placement architecture based on the services and organization requirements rather than on cluster and vendor boundaries.

- When an app is deployed on Tanzu Mesh Services (TSM), it's easy to create the secure, monitored connections that app needs to run.
- With advanced load balancing (ALB), if the traffic increases, the resources available to the application are also scaled automatically, ensuring that service level objections (SLOs) are met.
- If an app is moved or deleted, TSM automatically creates, scales or removes the secure connections that app requires: no manual configuration required.

The platform delivers these benefits invisibly, with no intervention necessary from the devops or app owners. This holds true even in complex multi-cloud and hybrid environments, spanning different platforms, clusters and sites.

Suggested reading:

> Building a Modern Application Environment



Application owners

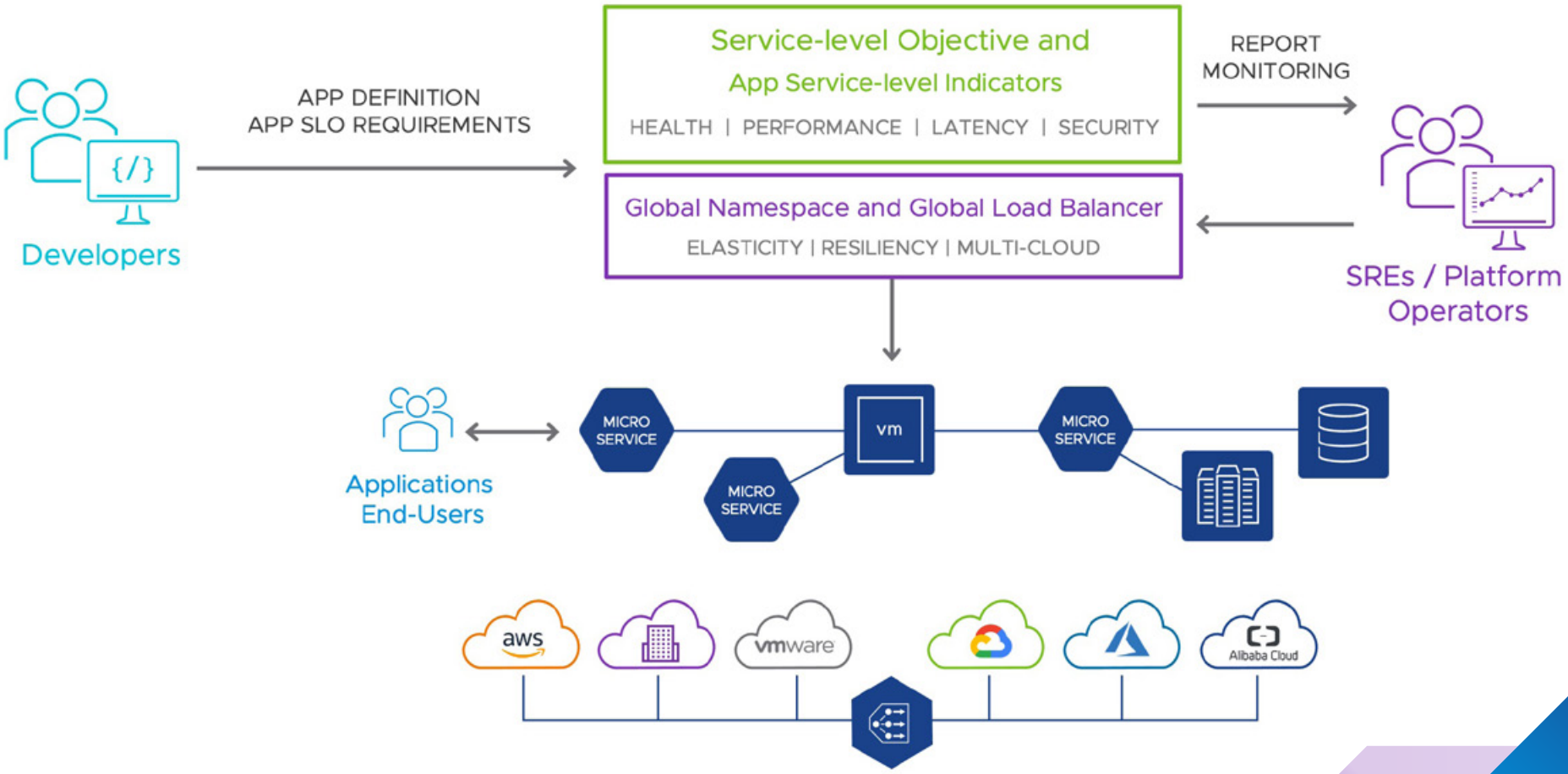


Figure 24 - Modern App Persona

Site Reliability Engineer

Site Reliability Engineers (SREs) and platform administrators are under pressure to ensure that developers and owners are able to build and deploy their app as fast as possible, with the minimum disruption. This means delivering the best possible network performance, with minimum downtime and the highest standards of reliability.

VMware Cloud Networking can help meet these needs in the following ways:

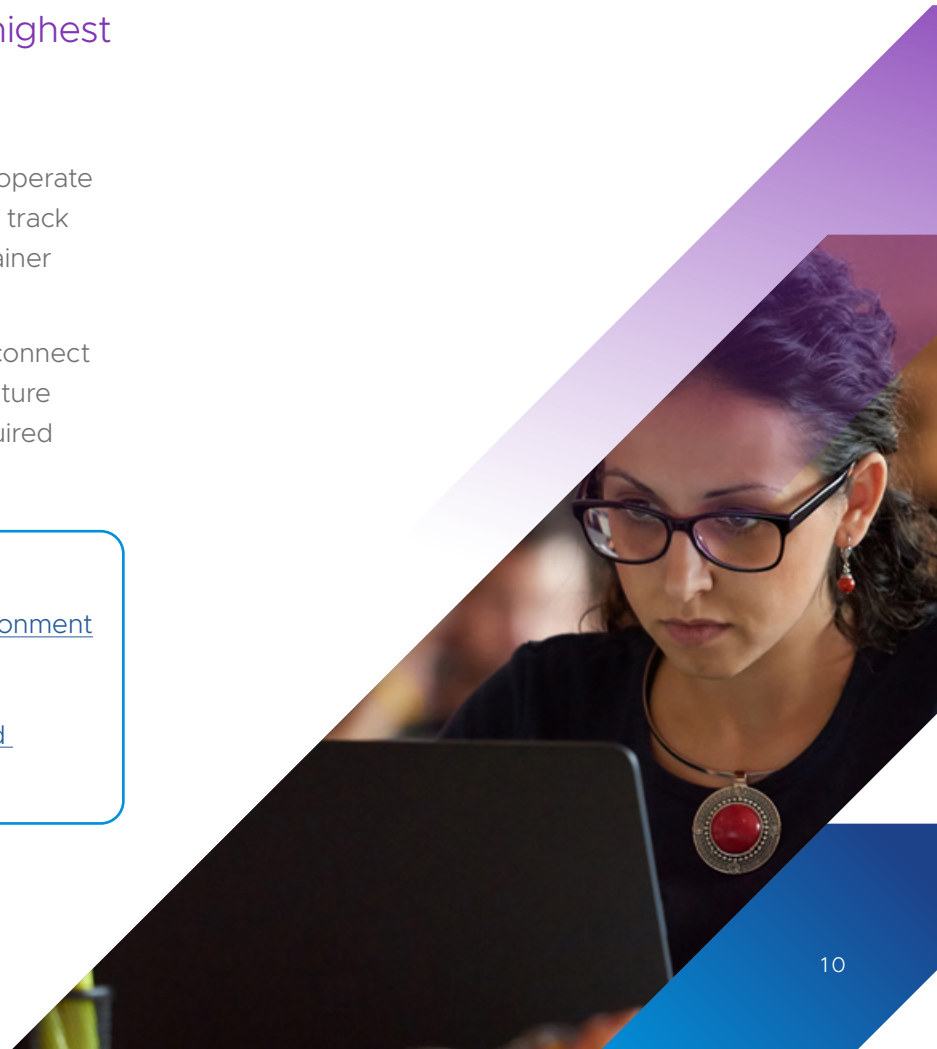
- Using ALB, pre-defined service level objectives are built into the network. TSM continually monitors performance and spins up new resources when required, to ensure SLOs are met.
- NSX provides an easy-to-use framework within which the deployment, provisioning and configuration of virtual machines and apps is quick and easy.
- TSM centralizes management to easily operate apps across a multi-cloud environment, track SLOs and automatically configure container ingress, API gateways and more.
- With Antrea, administrators can easily connect to workloads, no matter what infrastructure they're running on, and deploy the required policies and configurations.

Suggested reading:

> Building a Modern Application Environment

> Seamless Multi-Cloud Connectivity

> Elastic Scale with Modern Advanced Load Balancing



Infrastructure Platform Owner

Network administrators need to provide developers and other functions with the storage, computing power, secure connections to cloud resources and mission-critical functions such as load balancing. ITOps, meanwhile, is responsible for maintaining the network state, no matter what the demands placed upon the system.

To achieve these goals, both functions require the ability to apply network and security policies to entire multi-cloud network, regardless of the underlying infrastructure. They also need a single pane that provides the visibility and tools for monitoring and troubleshooting.

Here are some key elements that help meet these objectives:

- Using advanced load balancing ensures that applications have the resources they need, rerouting traffic and spinning up new resources whenever demand requires it.
- Advanced app discovery and dynamically adapting secure app connections ensure that SLOs are always met.
- Centralized enterprise-wide installation, configuration and real-time monitoring simplifies and accelerates the provision of the resources that app devs need to hit their targets.

Suggested reading:

> Building a Modern Application Environment

> Seamless Multi-Cloud Connectivity

> Intelligent Cloud Management

> Optimized Secure Transport over WAN

Network Security Owner

Network security professionals must ensure that only authorized users and applications have access to any given data set. This means deploying role-based access control (RBAC), encryption, identity-based access and a range of other security techniques. It also requires a system robust enough for these ways of securing data to operate in a rapidly evolving environment without breaking.

VMware Cloud Networking can help meet these needs in the following ways:

- Secure traffic within the data center with VMware NSX Firewall, with security deployed to the workload and distributed across the network to where it's needed.
- Manage configure and restore multiple data centers through a single interface, with NSX Federation.
- With advanced intrusion detection and prevention, secure wide-area networking and secure end-user computing, you can protect the entire network.

Suggested reading:

> Optimized Secure Transport over WAN

> Secure User-to-Application Communications

Building a Modern Application Environment

To deliver a modern application environment — one which enables rapid and cost-effective development to meet quickly evolving customer needs — the functions and capabilities outlined on page six must work seamlessly together. It must also allow the micro-services which these different functions support, to communicate and cooperate, across different clouds, platforms, and locations. A configurable and adaptable infrastructure layer i.e. service mesh allows seamless routing for modern applications.

Networking and Security for a Modern Application Environment

An industry-leading service mesh will not only route traffic to the right destination but also facilitate the kind of background work micro-services require to execute their allotted tasks and run at peak performance. For instance, this may include service discovery on the mesh or the creation of secure, authenticated channels of communication between micro-services.

VMware industry-leading Tanzu Service Mesh (TSM) provides advanced, end-to-end connectivity and security – across application end-users, microservices, APIs, and data – enabling compliance with service level objective (SLOs) and data protection and privacy regulations.

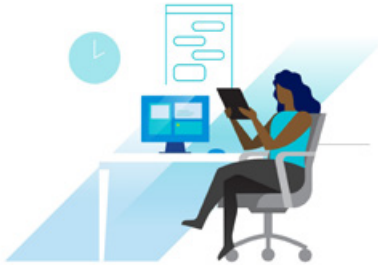
Elements of a successful modern consolidated application services include:

- **Intelligent routing:** the service mesh will route data and traffic between micro-services to the right destination in each instance, depending on the task at hand.
- **Policies:** a global namespace allowing through policy multi-cluster multi-cloud connectivity and mobility of micro-services.
- **Latency management:** the platform will scale resources to avoid unacceptably high latency that will impact the customer experience or even system stability.
- **Automatic failover:** with redundancy built in, should one instance of a service fail, traffic is instantly re-routed to another instance of the same application.
- **Automatic autoscaling:** once a particular metric, such as latency, hits a pre-defined threshold, the system brings extra resources online automatically.
- **Global server load balancing with ingress controller:** load balancing across locations, cloud platforms and data centers, for deployments that work seamlessly, regardless of underlying infrastructure, while in addition providing traffic management and flow optimization between containers and external applications with a single point of management.
- **API security:** APIs are front and center in today's infrastructure environments as automation has taken the lead in operations. Securing the APIs with authentication, authorization and encryption is very important to consider in any modern application framework.
- **Comprehensive Application Security:** Application encryption and AAA (authentication, authorization, accounting) is provided by many components: zero trust, certificates, micro-segmentation, FW/IPS/IDS, WAF (web application firewall).
- **Visibility:** it makes the operational status of each micro-service, including key performance metrics, available to users, facilitating both insight and action.

Enabling Efficient Containerization

Three use cases emerge in building a solution for modern app connectivity and security:

1. Seamless services connectivity across clusters and clouds, and with traditional apps running in VMs.



2. Fully secure environment including zero-trust end-to-end access to all services.

3. Elastic scalability, high availability, and self-healing/disaster recovery to assure app continuity and performance within service level objectives (SLOs).

Modern applications are made up of services. VMware helps connect and secure these services seamlessly as depicted in the following figures.

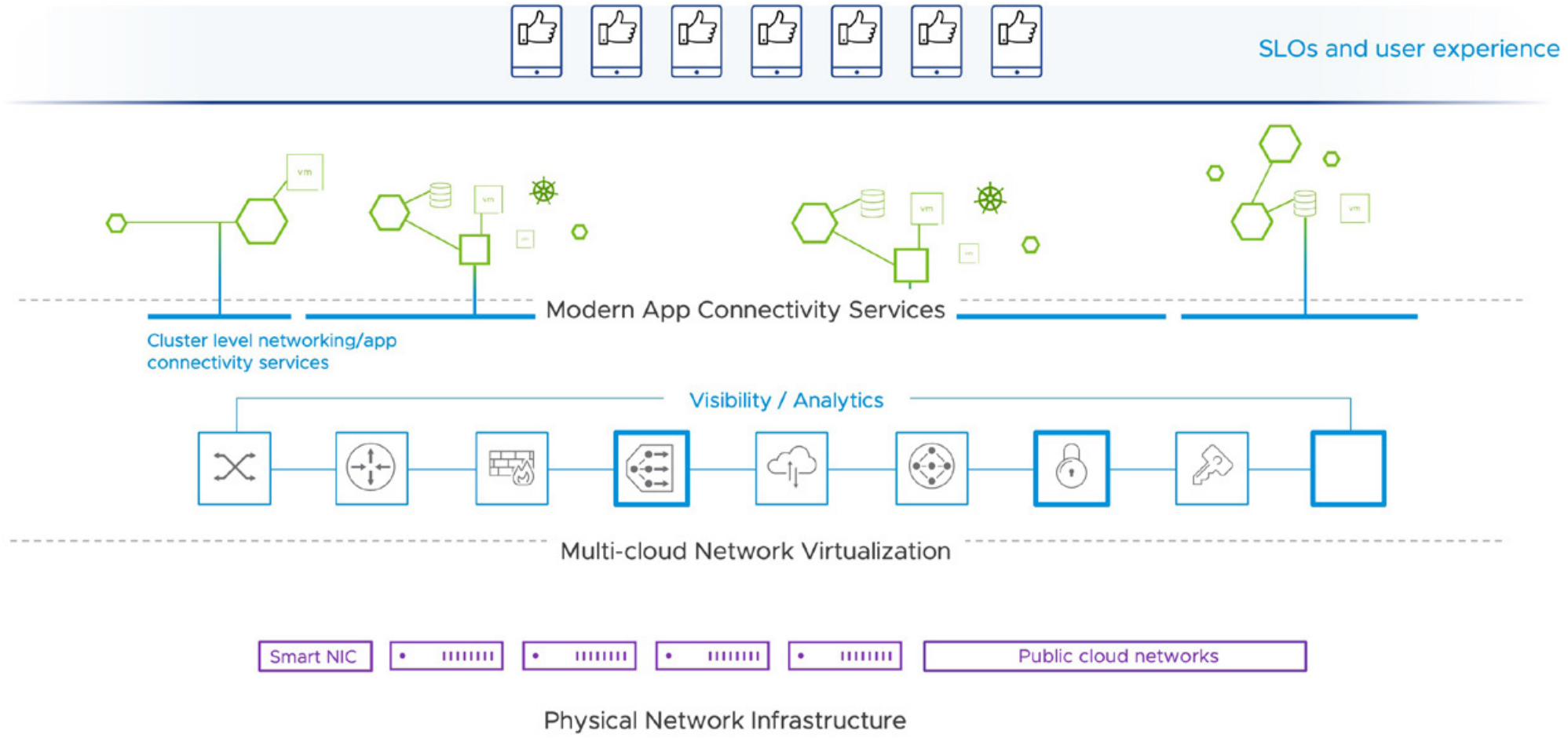


Figure 2 - Modern App Networking

Tanzu Service Mesh, NSX Advanced Load Balancer and Antrea

With TSM you can solve the common issues in cloud native networking and security in one powerful platform. This ensures application continuity, resilience, and security, even in the most demanding environments.

TSM enables an operator to deploy single and multi-cluster multi-cloud environments from one place. It allows to enforce consistent load balancing among many other network and security features across multi-clusters and multi-region.

These and other elements of traffic management and service discovery make an efficient state-of-the-art service mesh, with container ingress management built in, a crucial part of the modern application environment.

NSX Advanced Load Balancer provides multi-cloud load balancing, web application firewall, application analytics, and container ingress services across the data center and cloud. Benefits include consistent administration across multiple clouds, full-lifecycle automation, and actionable insights from real-time performance monitoring and closed-loop analytics.

VMware Modern App Connectivity Portfolio

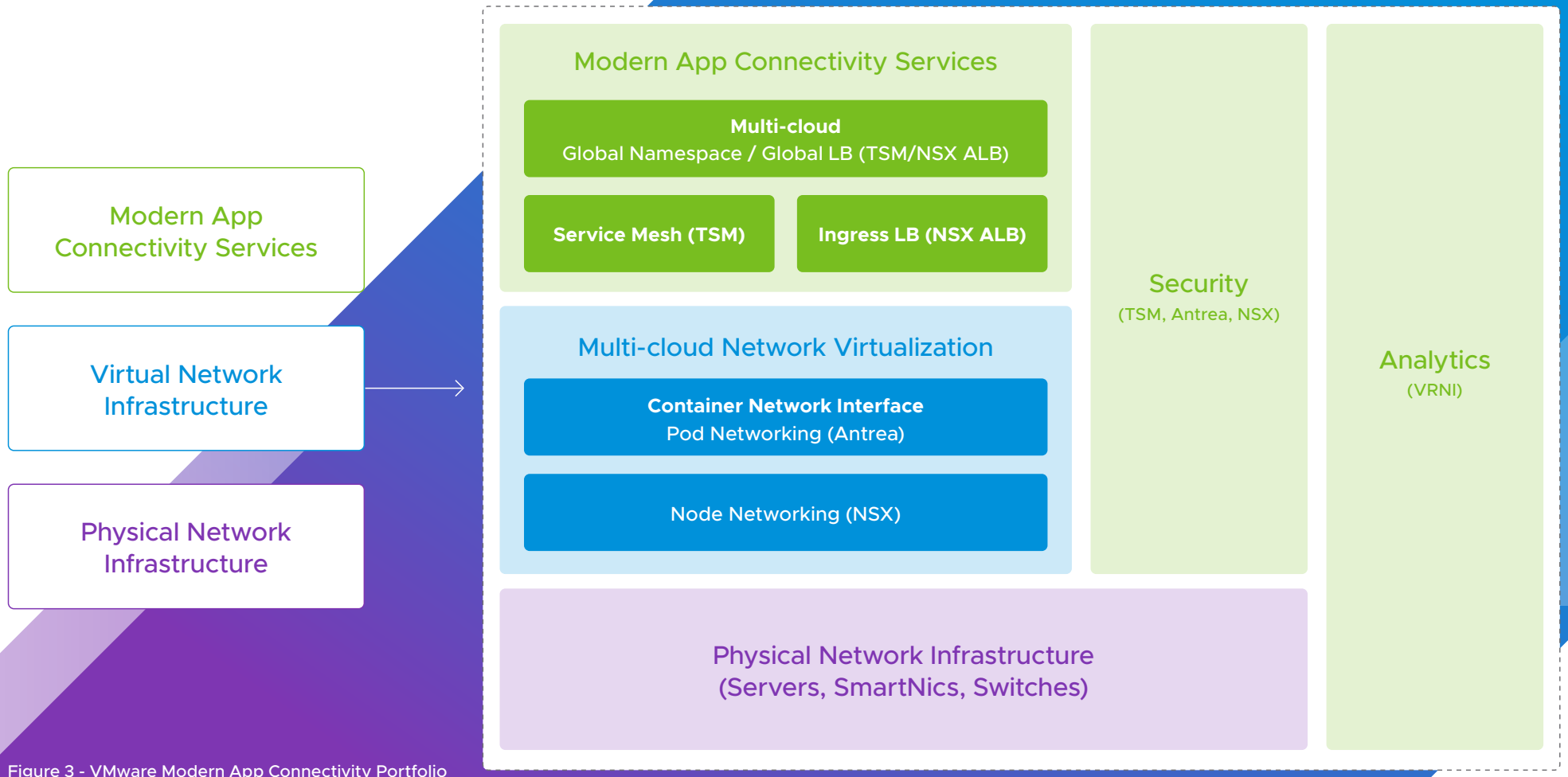


Figure 3 - VMware Modern App Connectivity Portfolio

Networking, Security and Analytics Built Into the Infrastructure

Antrea is a Cloud Native Computing Foundation (CNCF) project that implements the Container Network Interface (CNI). It allows developers to deploy their own network solution to enable container connectivity, including network connectivity and security services.

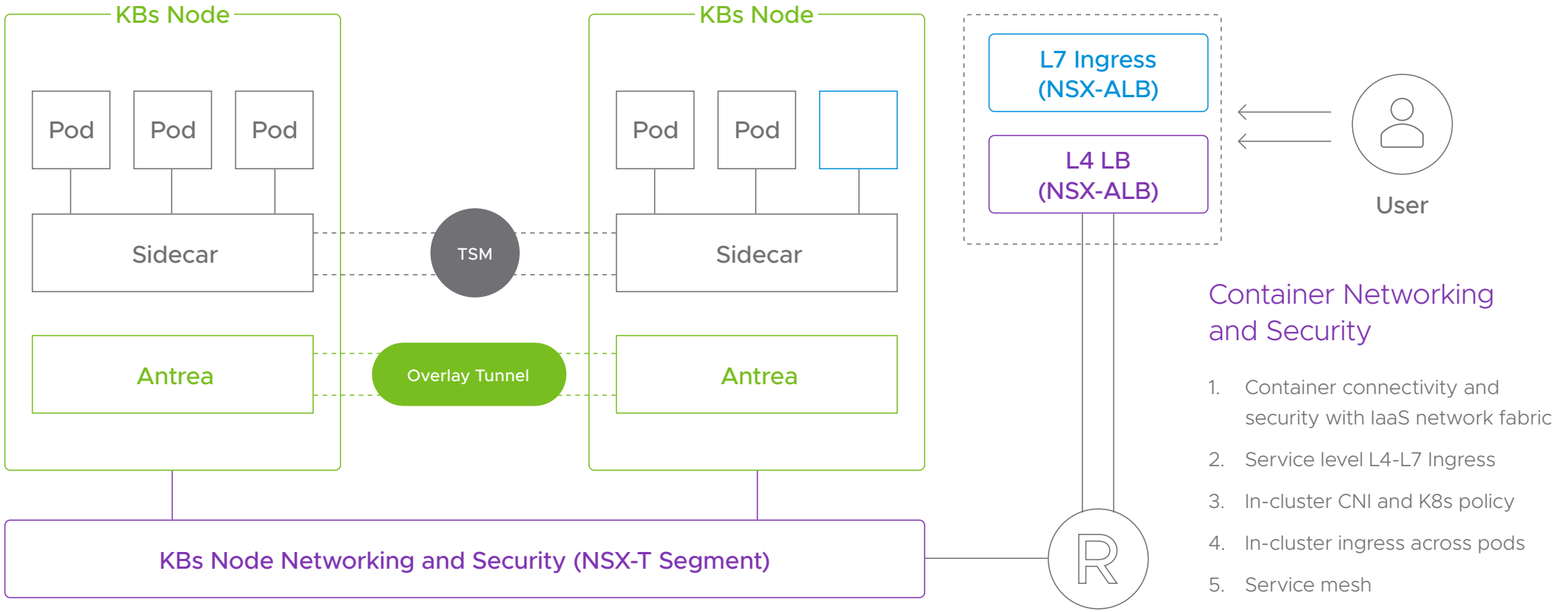


Figure 4 - Networking, Security and Analytics

Use Case: Auto-Scaling

Whether you're running a customer-facing e-commerce business, a B2B service provider or something else, demand can often fluctuate rapidly and widely. That's why VMware NSX Advanced Load Balancer comes with intelligent autoscaling as standard.

To prevent systems becoming overloaded, administrators — sometimes working with VMware consultants — set robust SLOs, designed to ensure a consistent and excellent experience for those using the system.

During peak traffic, rather than the app and the backend slowing down, or becoming unreliable, the peak in demand triggers the SLO threshold. VMware NSX Advanced Load Balancer scales the app up and down, by dynamically adding or subtracting resources such as virtual machines, and then load balancing traffic between them.

The system continues in this mode, ensuring a smooth service for all users, until the peak has passed. At this point, to conserve resources and cut costs, it powers down the extra resources and the load balancer routes all traffic back to its default destination. Being able to operate in this manner makes it easy to build, deploy and auto scale almost any modern application.

VMware's Modern App Connectivity Solution

Platform and workload agnostic

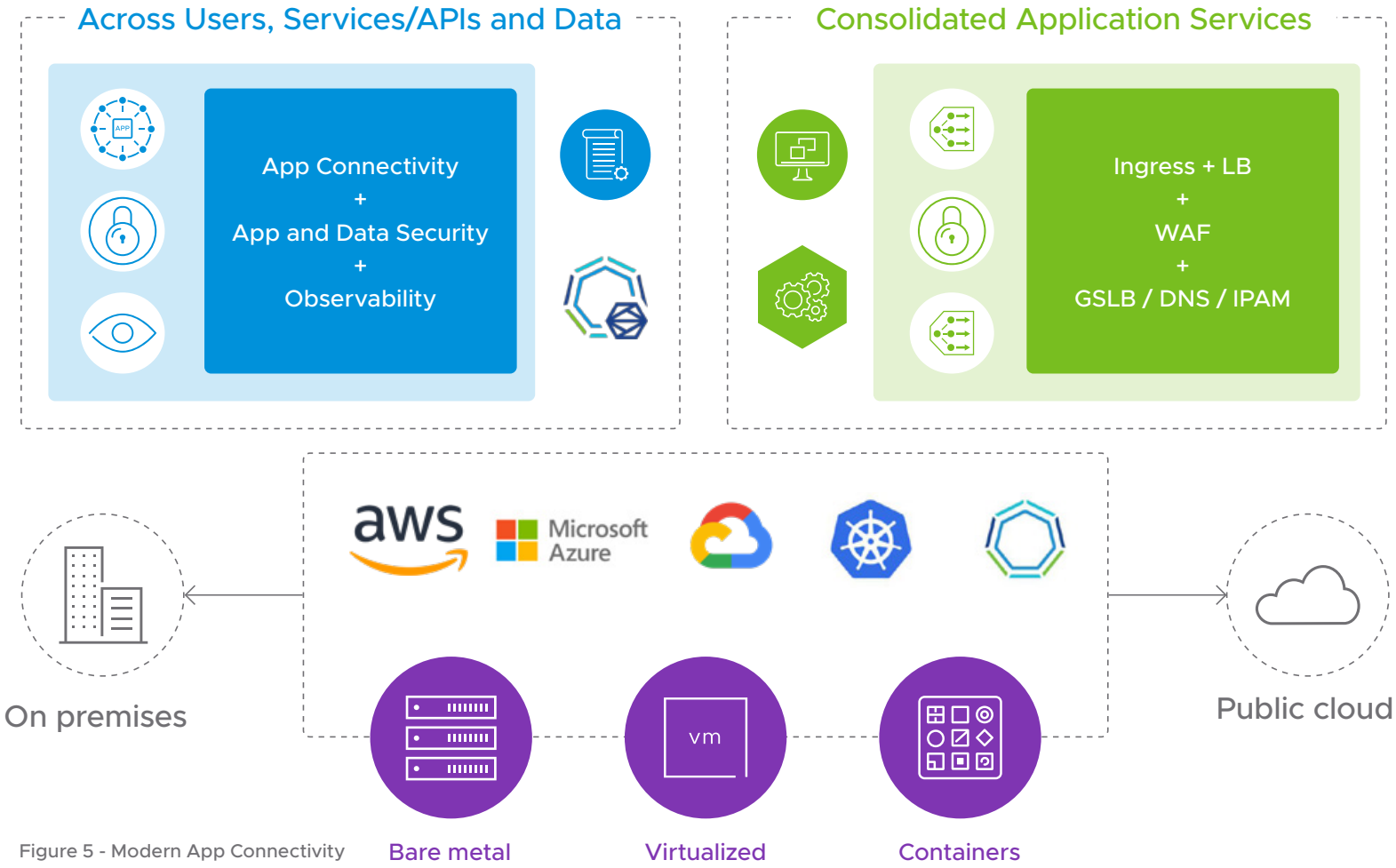


Figure 5 - Modern App Connectivity

Tanzu Service Mesh, Antrea CNI and NSX-T provide discovery, identity, policy control and traffic management across end-to-end communications from application end users to microservices and data. This enables compliance with service level objectives (SLOs) and data protection and privacy regulations.

This makes it easy to create a modern app with built-in auto-scaling and with end-to-end connectivity, continuity, resiliency, security, and observability, in single and multi-cloud environments with Tanzu Service Mesh.

Use Case: Modern App Security

No matter what type of business you are in, security is a priority. If you lose customer data, the damage to your reputation can be significant and you may face substantial fines levied by regulators.

For policy enforcement across environments, administrators can use Tanzu Service Mesh (TSM). TSM allows for the creation and enforcement of a common policy model across multiple Kubernetes clusters, different platforms and different clouds, either private or public. And Tanzu Service Mesh Global Namespaces (GNS) enables secure multi-cluster service discovery and connectivity in a seamless manner, without developers needing to worry about where app services are deployed.

With this power of abstraction, discovering and securely connecting these distributed services (using mutual TLS) across multiple clusters becomes very simple and easy to build and manage entire workload across multiple Kubernetes cluster either running on premise or any cloud.

Modern App Security Use Case

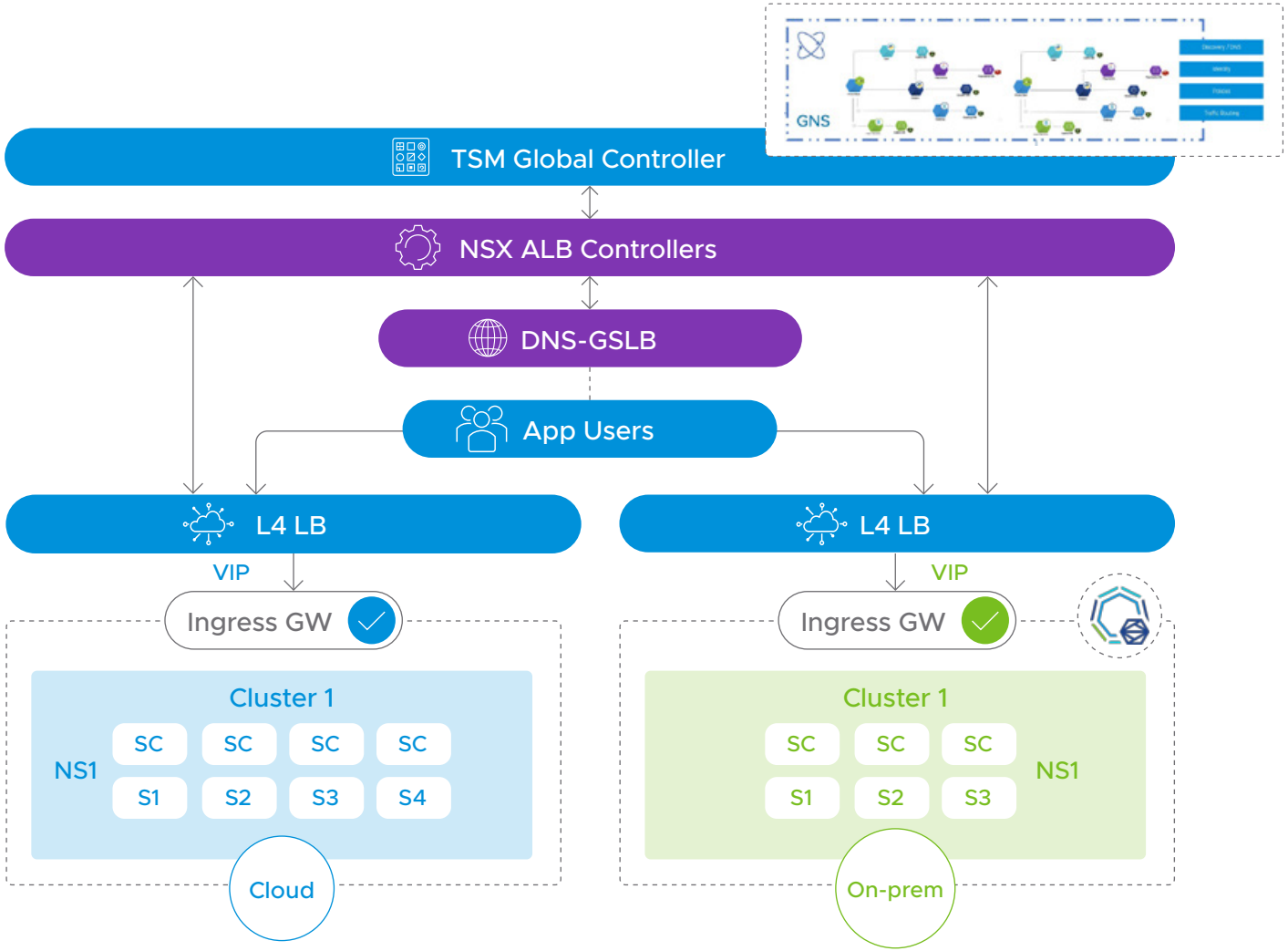
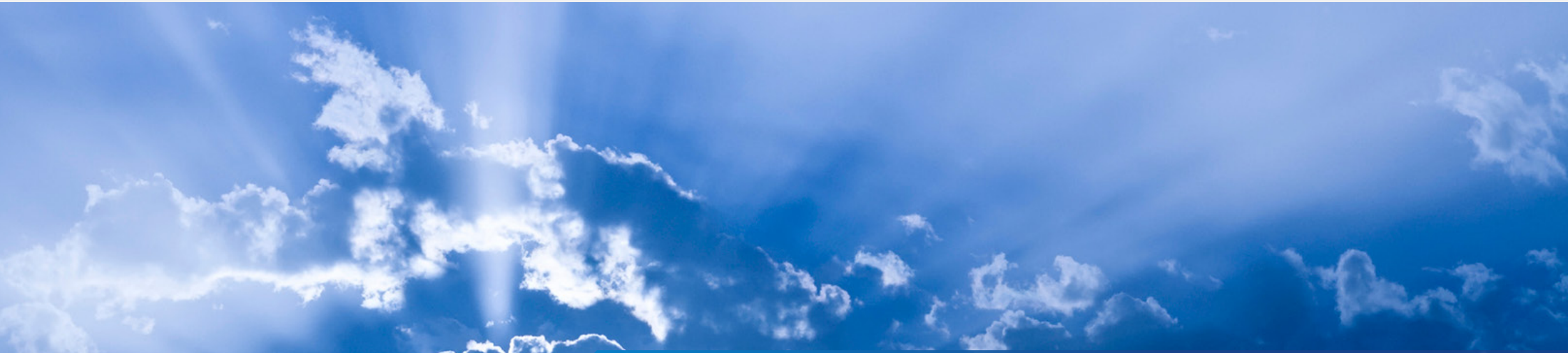


Figure 6 – Modern App Security use case

With VMware Tanzu Service Mesh, Advanced Load Balancer and Antrea automatically run across Layer 2 to Layer 7, connecting application services without having to specify any underlying infrastructure. With the power of this abstraction, your application micro-services can "live" anywhere, in any cloud, allowing you to make placement decisions based on application and organizational requirement.

To ensure the modern application environment is secure by design, VMware Cloud Networking comes with a range of tools and features. It includes The web application firewall (WAF). enforces policy-based security rules for traffic from within and without the network to secure every web application on the network. With container networking CNI plugins, open-source Antrea allows administrators to easily apply network-tagging workload and security policies at vNIC of Pod level or the service level.



Seamless Multi-Cloud Connectivity

By 2021, 92% of organisations have at least some of their data or computing power in the public cloud [4]. At the same time, the market for private cloud solutions is growing at a rate of 25% a year [5]. And despite the rapid growth of public and private cloud, 60% of enterprise software is still installed on-premises [6].

4. https://www.accenture.com/nl-en/blogs/insights/cloud-trends
5. https://www.businesswire.com/news/home/20200806005494/en/COVID-19-Impacts-Private-Cloud-Services-Market-Will-Accelerate-at-a-CAGR-of-over-25-through-2020-2024-Growing-Adoption-of-Cloud-Among-SMEs-to-Boost-Growth-Technavio
6. https://www.grandviewresearch.com/industry-analysis/business-software-services-market

Increasingly businesses need a way to manage this heterogenous infrastructure seamlessly, providing connectivity between private and public clouds, while protecting the user and application wherever they are deployed.

Multi-cloud connectivity services help address:

- Network connectivity and network services across multi-cloud environments.
- Consistent policy across all workloads, regions and platforms, whether on-premises private cloud or in the public cloud.
- Single interface to view and manage all workloads across clouds, accounts, subscriptions, regions, and VPCs — visible through a single interface.
- Real-time analytics including oversight of all traffic as it flows within and across virtual private clouds and other sites — including complete and comprehensible access to firewall logs.
- Secure access service edge (SASE) capabilities that secure the whole of the network — at the edge, in the data center and in the cloud.
- A built-in site-to-site virtual private network (VPN) that encrypts traffic between private and public sites to the highest standards.

Multi-cloud with VMware NSX

Its core components include:

VMware NSX Cloud delivers consistent networking and security for applications running natively in the public cloud. NSX Cloud uses the same management plane and control plane as VMware NSX Data Center, enabling a single networking and security solution from the private data center to the public cloud. It can help extend your security policies from on-prem to native AWS and Azure, which are defined based on application requirements and are agnostic to the cloud in which they are running.

VMware also offers managed multi-cloud solution with VMware Cloud on AWS (VMC), Azure VMware Service (AVS), Google Cloud VMware Engine (GCVE), Oracle Cloud VMware Solution, and VMware Solution on other leading Cloud Providers through the VMware Cloud Partner Program (VCPP). This delivers VMware's managed enterprise-class software-defined data center software on all major cloud providers, enabling customers to run production applications across VMware public, private, and hybrid cloud environments, with optimized access to native cloud services.

VMware Cloud Solution provides network connectivity options (VPN, DX, TGW), and key advanced Firewall features like: IDS/IPS, L7 firewall, IDFW and FQDN filtering features for Workloads running either on premise or in the public clouds.

Use Case: Consistent Network and Security Policies Across Cloud and On-Prem

One of the most common challenges of hybrid public-private and on-premises environments is the difficulty of applying consistent networking and security across environments and cloud platforms. Without the ability to do this, management overheads rise, and configuration drift and gaps are harder to manage.

With VMware NSX Cloud, you can extend your existing VMware NSX Networking and Security services across datacenters and public clouds.

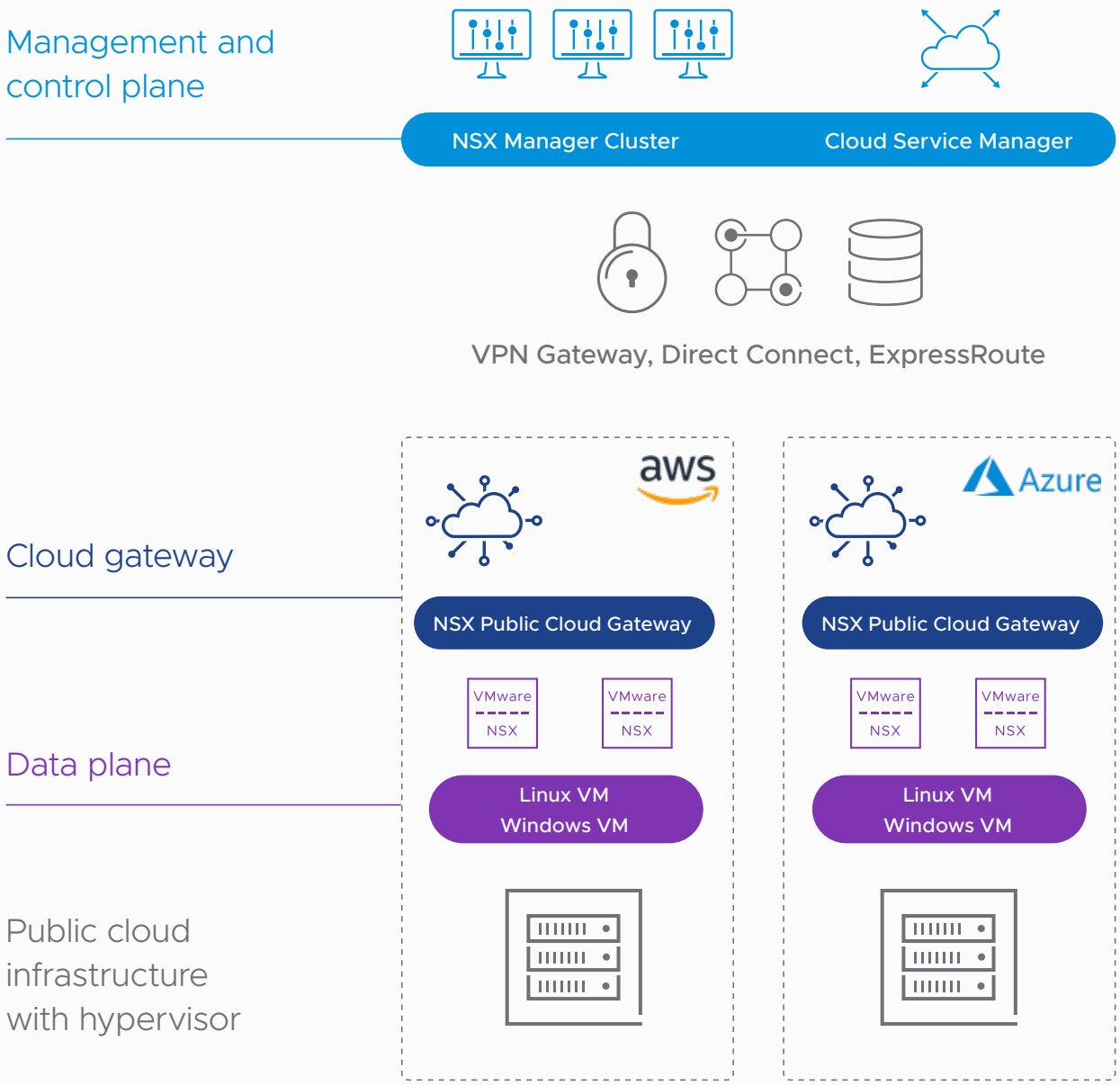


Figure 7 - NSX Cloud Architecture

Imagine a set-up with two public clouds, each with two regions — the fundamental security concepts differ between each cloud provider, and each region within a platform requires its own set of networking and security policies. NSX Cloud helps you eliminate this overhead. You identify the desired network outcome and NSX translates that intent into networking and security polices across the public cloud (for example, native cloud workloads such as AWS EC2 or Azure VMs and cloud services such as lambda function or S3 storage) and your on-premises workloads. Networking and security policies are created and enforced based on the needs of your applications – whether they are deployed in the data center or in public cloud.

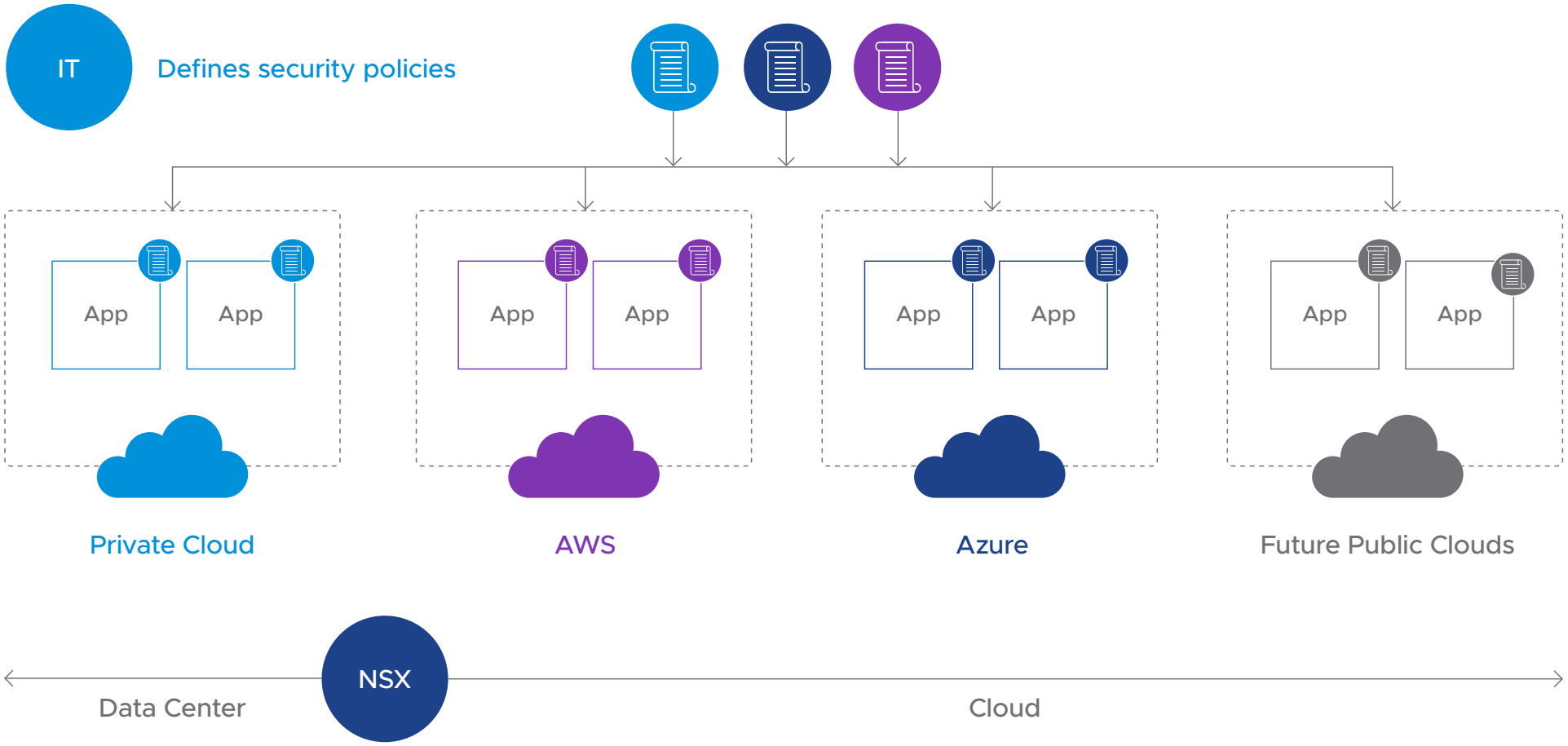


Figure 8: Consistent Security across Cloud with NSX Cloud

Use Case: Data Center Extension with VMware Cloud on AWS

VMware Cloud on AWS brings VMware's enterprise-class solutions to Amazon Web Services (AWS). The solution allows you to manage VMC on AWS resources through the VMware vCenter interface. You can manage, monitor, and configure your on-prem and AWS resources centrally with a single point of control.

VMC on AWS makes it easy to leverage cloud-based resources to extend your existing data center capacity. Administrators simply subscribe to a VMware-managed software defined data center (SDDC) in AWS on-demand and add this new environment to their existing data center private cloud. This process of bringing new cloud resources online and adding them to existing infrastructure is extremely streamlined.

Using multi-cloud distributed firewall and advanced threat prevention solutions, administrators can then secure all communications between on-site and off-site true hybrid applications, load balance between them and apply unified policies across all assets. This allows the on-demand data center extension in public cloud to proceed quickly and smoothly.

VMC VMware Cloud AWS

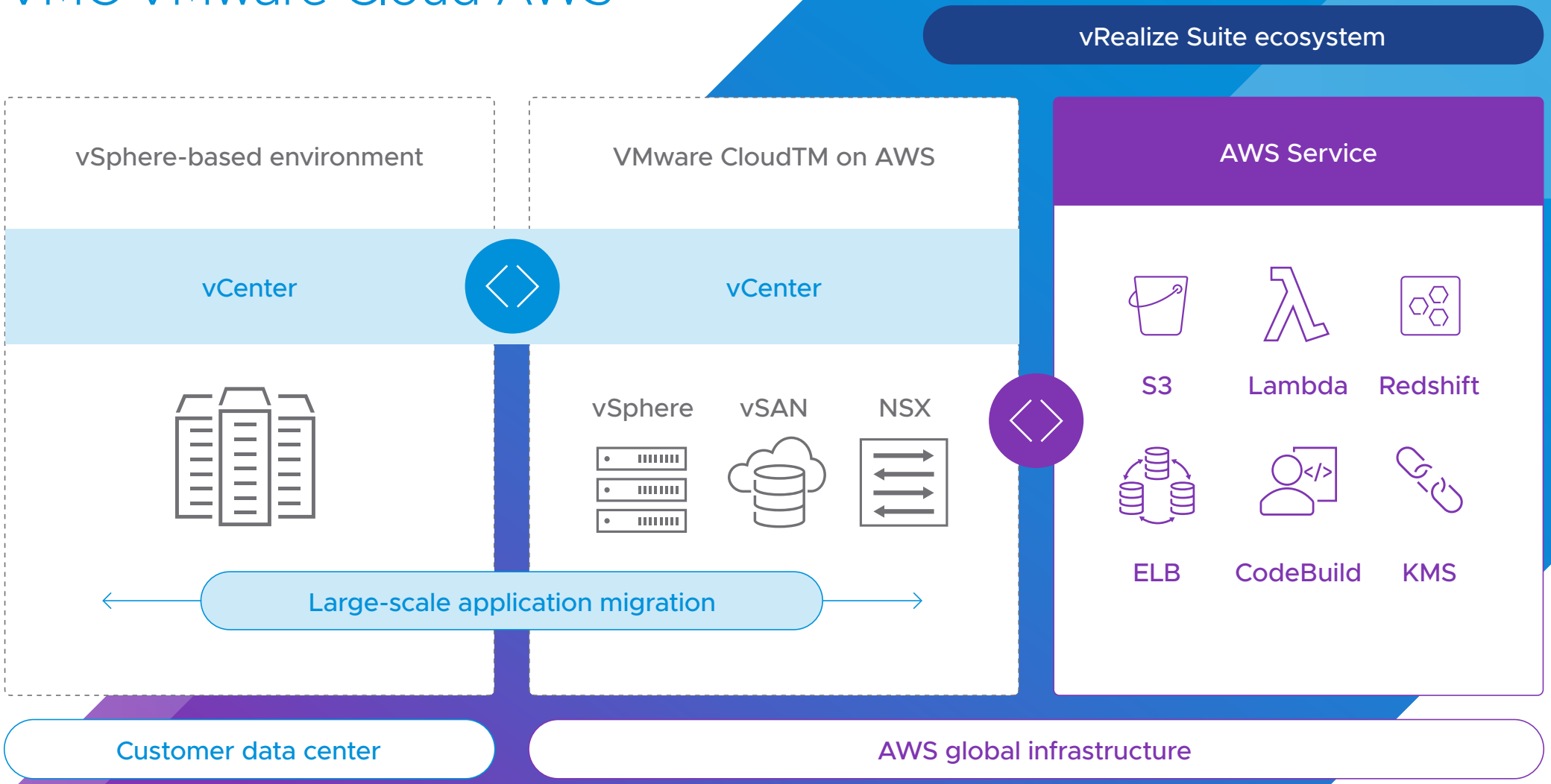


Figure 9 - VMC VMware Cloud on AWS

Elastic Scale with Modern Advanced Load Balancing

Modern enterprises need an on-demand, fast-to-deploy, easy-to-use, multi-cloud application delivery solution that facilitates consistent policies across on-premises and cloud environments. To guarantee continuity and quality of service in this type of hybrid environment requires hyper-efficient load balancing, able to route requests to the resource best able to service them in that instant — and to spin up new resources when demand requires it.

A modern advanced load-balancing system should have:

- Elastic load balancing and autoscaling, to prevent bottlenecks, latency and other problems which impact performance and stability.
- Easy, point-and-click simplicity for security policies, available from a single, central point of control.
- Granular analytics, logs and security insights on traffic flows, to allow administrators to spot problems and potential issues instantly.
- Protection against DDoS and other attacks with real-time security insights so the enterprise responds instantly when it's under attack.
- Traffic management and service discovery, to ensure that load balancing decisions keep the entire multi-cloud environment secure and running at peak performance.

VMware NSX Advanced Load Balancer

VMware NSX Advanced Load Balancer (Avi Networks) is a full-featured, enterprise-grade application services platform including a load balancer, a web application firewall (WAF), and a container ingress that provides traffic management and application security while collecting real-time analytics from the traffic flows.

Benefits include:

- 97% faster provisioning with automated per-app load balancing services [7].
- 30% lower total cost of ownership (TCO) thanks to intelligent rightsizing [8].
- 41% less time spent troubleshooting compared to last-gen load balancing [9].

7. IDC Study of Enterprises Using Next-Generation Application Delivery
8. VMware Data Integrated Customer Engagement (DICE) Tool
9. Load Balancing Benchmark Report by Principled Technologies.

Elastic Scale with Modern Advanced Load Balancing

Integrated cloud-native platform that delivers the path to app modernization

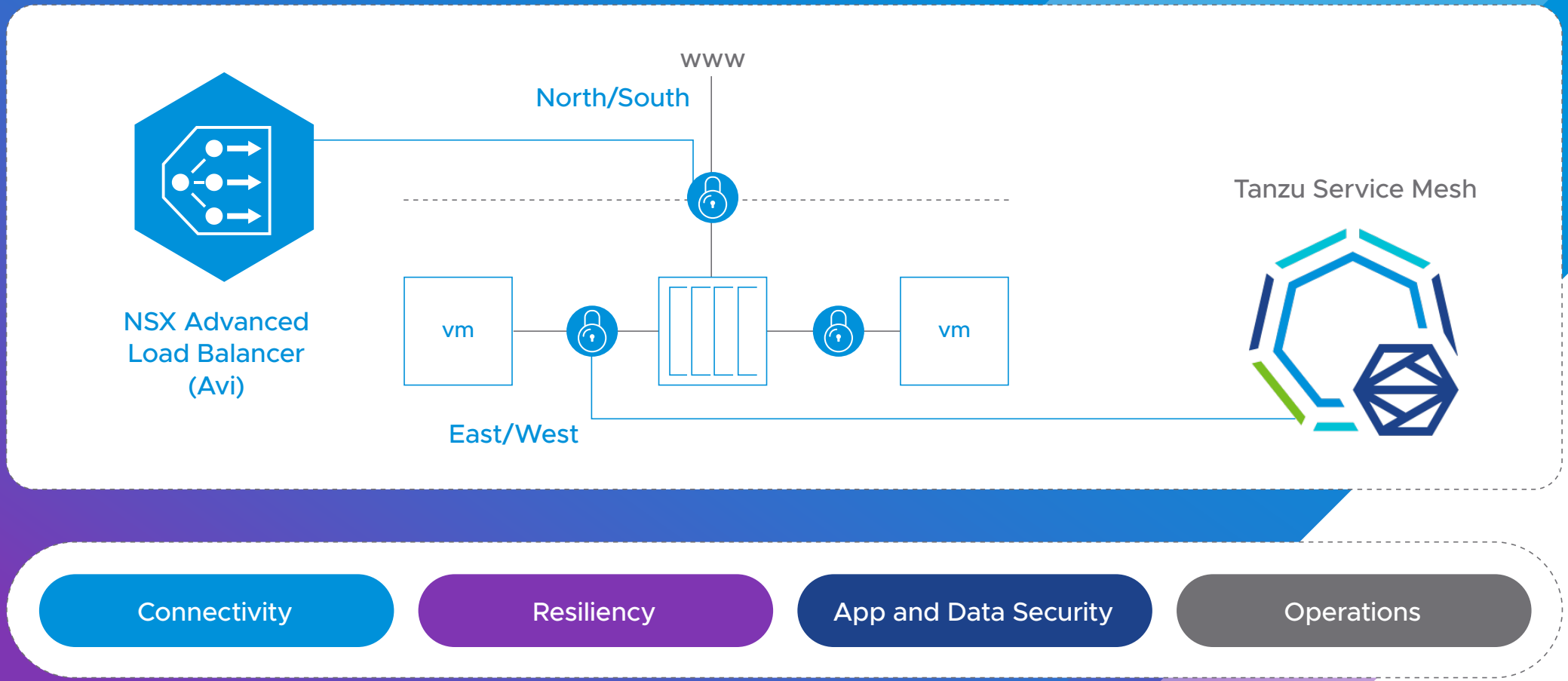
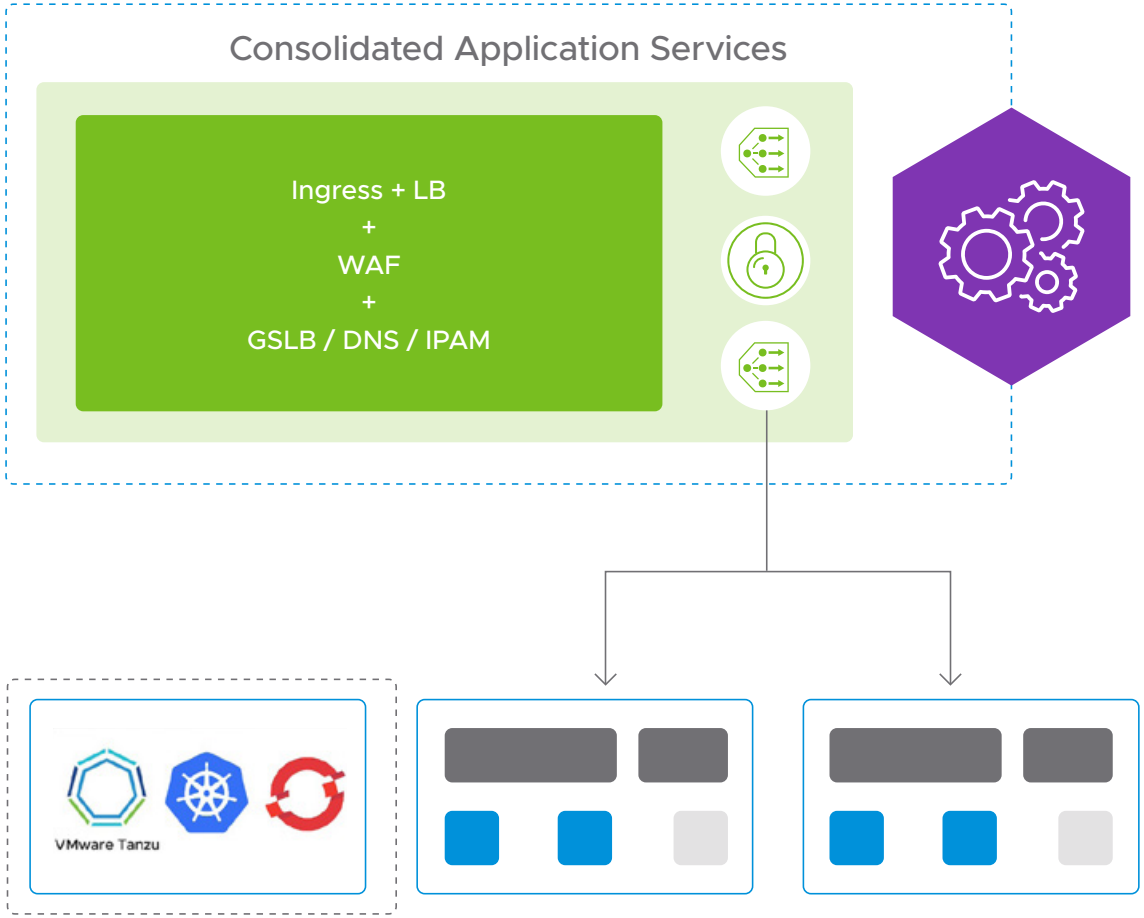


Figure 10 - VMware complete Modern App Connectivity

Converged Kubernetes Load Balancing/Ingress Services

A single L4 and L7 platform for holistic app operation



Integrated solution
Comprehensive LB, Ingress, intrinsic security, WAF, GSLB, DNS, and IPAM

Operational simplicity
A single solution with central control and ease of troubleshooting

Rich observability
Real-time telemetry with application insights across all components

Cloud-native automation with elasticity
Elastic autoscaling based on closed-loop analytics and decision automation

Figure 11 - Load Balancing / Ingress Services

Use Case: Ensuring Continuity of Service

NSX Advanced Load Balancer is a highly elastic application service platform which gives administrators a whole range of tools to ensure resilience, continuity, and quality of service. For instance, let's consider the case of an e-commerce platform which is dealing with unexpected peaks of demand, leading to increased latency and a poor customer experience.

Options available to administrators at the e-commerce site include using SSL offloading, allowing a separate app to handle the encryption for the e-commerce site, freeing resources on the main server to deal with merchant operations.

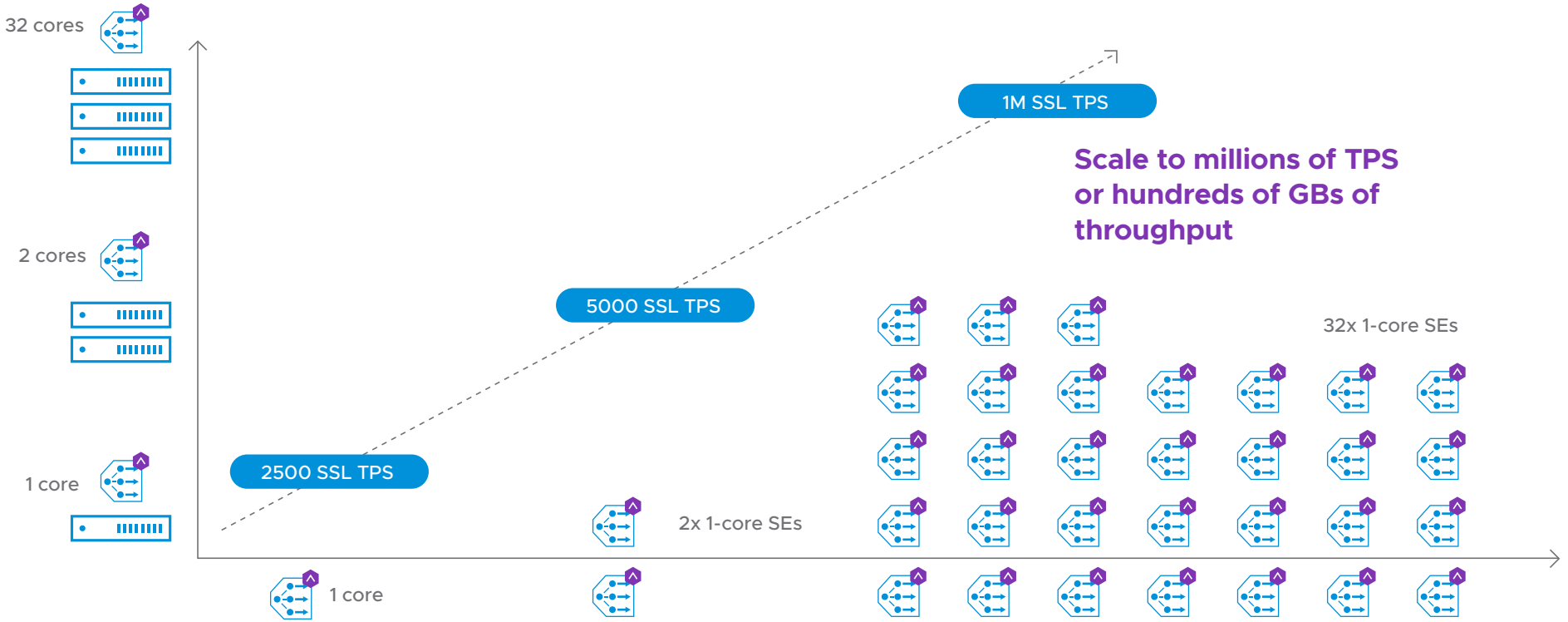
At the same time, administrators can configure the platform to act as an inline load balancer, dynamically distributing incoming e-commerce requests to different virtual machines, each running a clone of the merchant backend.

In this scenario, the load balancer provides autoscaling, self-healing of the load balancing fabric and app security, to ensure that key SLO metrics, such as latency, never hit unacceptable levels, maintaining a high standard of customer experience.

Elastic Autoscaling

Scale vertically with more CPUs or horizontally with more Load Balancers

Compared to hardware-based load-balances, VMware unlocks huge flexibility, cost savings and scalability benefits including massive scalability of up to x86 servers [10], a move from CapEx to a subscription-based OpEx model, deep application analytics and single point of control.



10. https://www.vmware.com/content/dam/learn/en/amer/fy21/pdf/603256-Load-balancer-buyers-guide-2020-ebook.pdf

Use Case: Cloud-Native Automation and Self-Service

One of the problems of multi-cloud environments without advanced load balancing, is the amount of manual troubleshooting and reconfiguration required to stay within acceptable performance parameters. Fault isolation alone can be difficult, involving much manual checking of logs. And that's before you even start with fault resolution.

With Tanzu Service Mesh, users can define an end-to-end latency policy, based on pre-defined SLOs. This enables the service mesh to automatically optimize and self-heal any application, even when loads increase suddenly and without warning, to ensure that the SLO is met. The platform monitors traffic and performance levels. When it detects a sudden increase in demand, and a metric hits the level defined in the SLO, it triggers auto-scaling capabilities, along with the associated component such as the NSX Advanced Load Balancer, allowing the platform to spin up and down resources based on dynamic demand.

Additionally, all the information administrators need — across the whole environment with all its different sites, platforms and web applications — is available through one controller. This central orchestrator gives fast access to policies, transactional logs and insights that enable rapid-resolution troubleshooting and automate lifecycle management of application delivery.

Automation / Self-Service with Advanced Load Balancer

Built-in ecosystem integration/cloud connectors

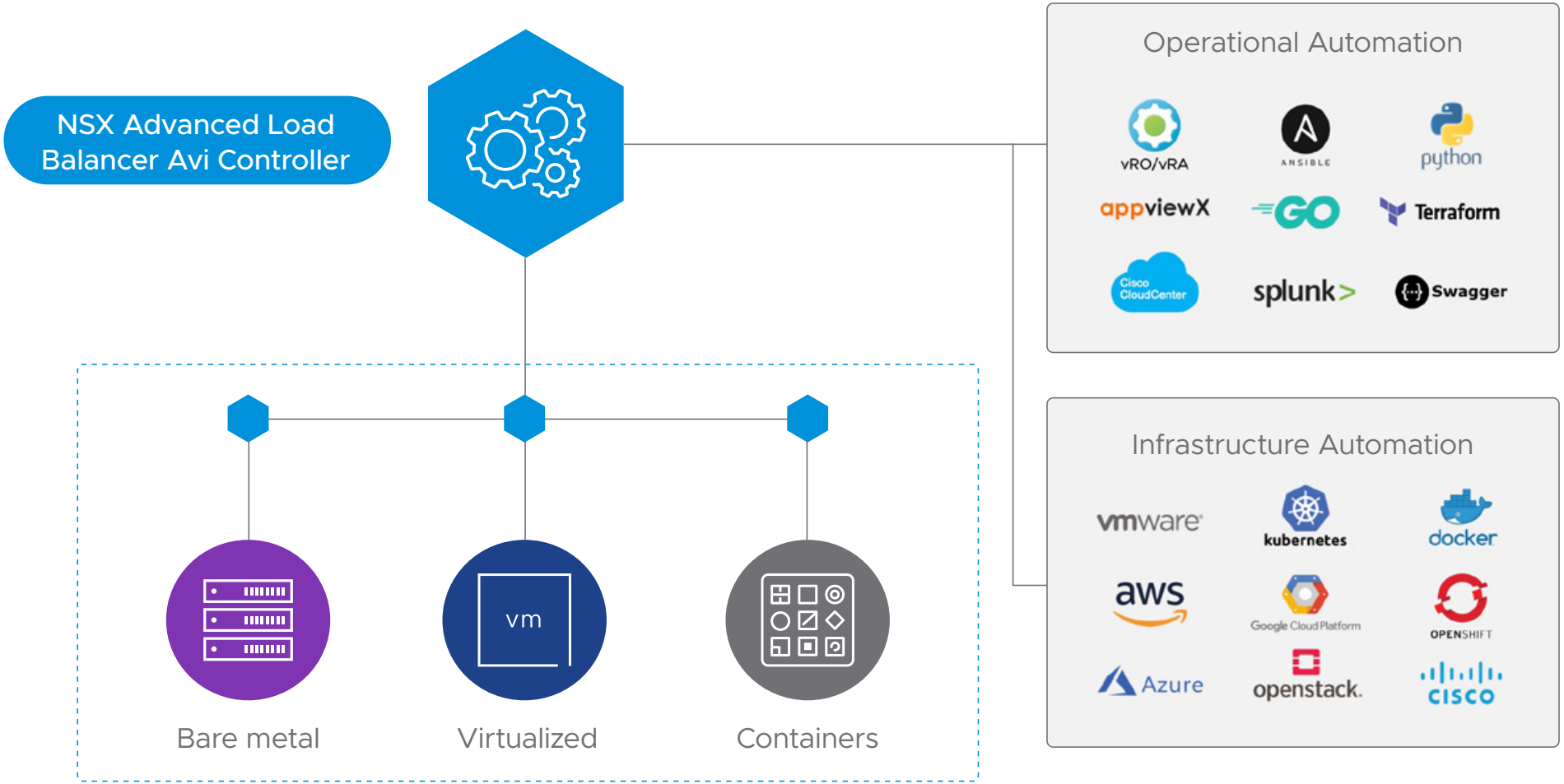


Figure 13 - Automation with Advanced Load Balancer

Optimize and Secure Transport Over WAN

To ensure service levels are met, traffic in a multi-cloud environment must be secured as it passes traffic between different sites and different web apps. Your system must, as far as possible, be self-healing. It must be easy to scale, as demand flexes. And it should be secured with industry-leading standards and technologies.

To meet this need, administrators require a platform which delivers secure transport over wide area networks, such as the public Internet, and which is highly configurable. Such as a solution should:

- Dynamically prioritize applications to ensure business-critical applications have higher priority than non-business critical applications like YouTube and Netflix.
- Detect and mitigate network issues as they arise, anywhere in the hybrid environment, to keep apps performing well.
- Easy set-up and provisioning of new resources through a central management platform that allows configuration, visibility and troubleshooting of all WAN edges.
- Secure and encrypt connections between different sites, clusters and apps on the network.

The secure-transport solution should securely support application growth, network agility, and simplified branch implementations while delivering high-performance, reliable access to cloud services.

It should also integrate with your multi-cloud management platform, to provide visibility, streamlined resource management and simplified troubleshooting across the hybrid network. A modern multi-cloud management platform will do this through a single pane of glass, and an interface which simplifies and streamlines operations for network administrators.

VMware SD-WAN

An SD-WAN is a software-defined wide area network. VMware SD-WAN delivers reliable, and resilient data transport over the wide area network (WAN). As well as securing data in transit, it can mitigate network degradations that would affect application performance and improve user experience.

Benefits of VMware SD-WAN include:

- Cloud VPN provides automated VPNC-compliant IPsec VPN for dynamic branch-to-branch and branch-to-data-center connectivity while delivering real-time status and health updates to administrators.
- Dynamic multipath optimization, with automatic link aggregation, per-packet load balancing, and automatic link remediation that mitigates underlying link issues such as packet drop, latency and jitter, enabling better application performance over consumer-grade broadband connections.
- Zero-touch provisioning: new VMware Edges can be deployed at scale and securely, without the need to send out expensive technicians to the site.
- Intelligent segmentation to ensure that network structures are secure and compliant, even for industries with high regulatory overheads.
- VMware Cloud Gateways provide optimized data paths to all applications, branches, and data centers along with the ability to deliver network services from the cloud.

SD-WAN for Modern App Connectivity with Tanzu

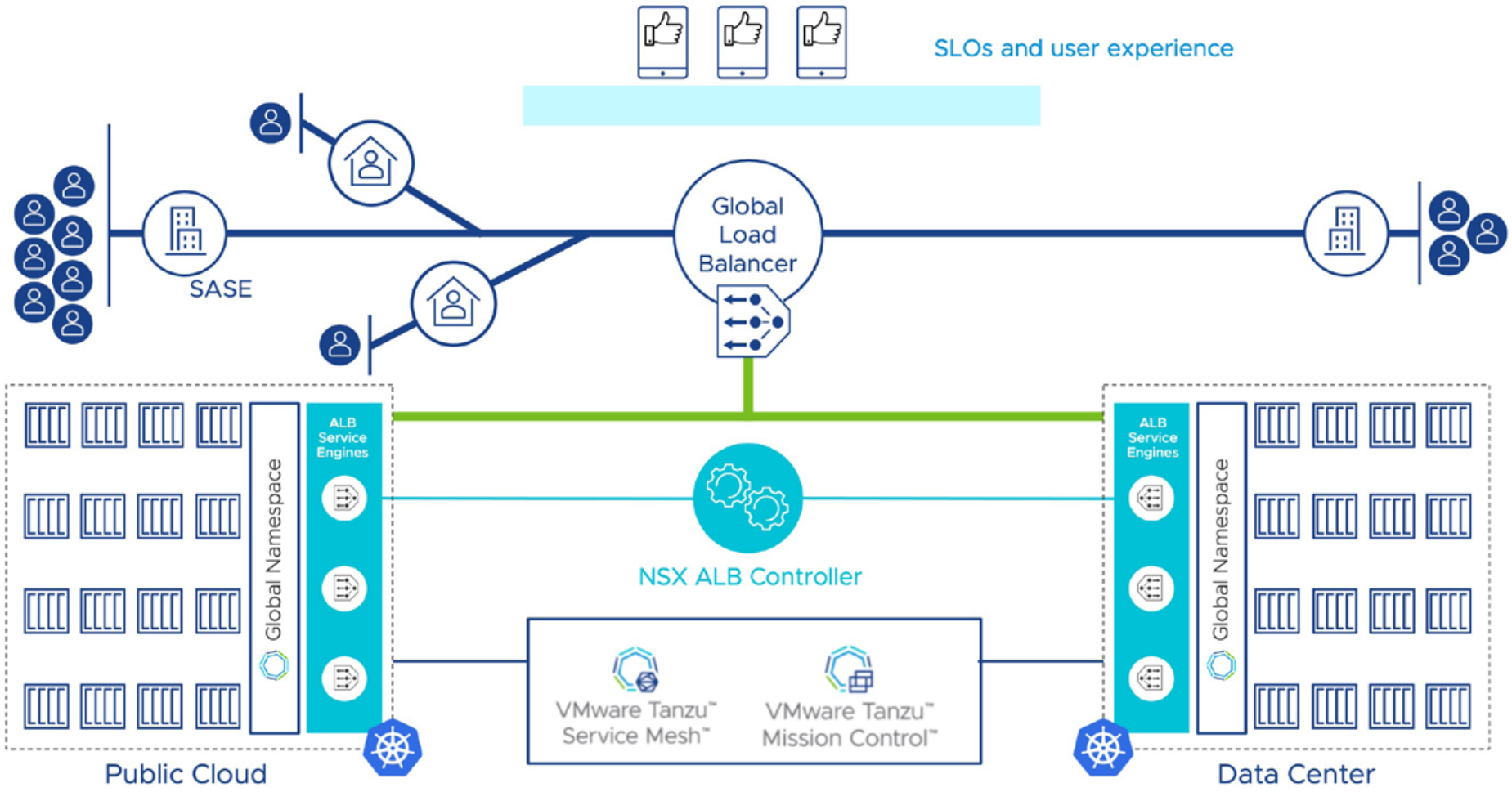


Figure 14 - SD-WAN for Modern App Connectivity with Tanzu

Use Case: PCI Compliance

The Payment Card Industry (PCI) Data Security Standards (DSS) are the leading standard in payment protection. Any entity which accepts card payments online, or in any digital medium, is expected to adhere to the PCI standards. That's why PCI DSS compliance is built into VMware's cloud networking solutions.

Having PCI DSS compliance built into the solutions on which your modern network is built can drastically simplify the tasks required to achieve and maintain PCI DSS compliance. By being certified as a PCI DSS service provider, VMware has demonstrated that the VMware Cloud on AWS service operates PCI DSS compliant security measures and controls, thereby serving the needs for a broader range of customers and workloads.

VMware's Cloud-Delivered SD-WAN solution meets PCI requirements by providing all the features for customers to become PCI DSS compliant. Customers can rely on VMware's network and security technologies and leverage VMware PCI Attestation of Compliance (AOC) to accelerate and save cost towards their PCI audit.

Use Case: Merging Enterprise Infrastructures

After a merger or an acquisition, the new company that's been formed often has to find a way to merge hundreds, or even thousands, of different sites and cloud services into one infrastructure. To work, the solution must be platform agnostic. And it must be secure.

With VMware SD-WAN, administrators can rely on technologies that are designed to work from the ground up with a wide range of cloud applications and underlying infrastructure.

With automatic provider-configuration detection, the platform interrogates each cloud provider and automatically uses the right configuration and protocols. Thanks to Cloud VPN, connections between sites and apps are secured with industry-standard encryption. And intelligent segmentation ensures that access to data from different functions that ought not be widely available is limited to certain network segments and apps.

Secure User-to-Application Communications

During the pandemic, millions of workers moved out of the office to work in their homes. This came on top of an existing trend for distributed working, with enterprises required to connect branches all over the world with secure, high-bandwidth connections.

Enterprise IT must support this transformation by ensuring users can have the same application experience regardless of whether users are inside or outside the office, while also ensuring security of their network, applications, and data – something legacy networks were not designed to handle.

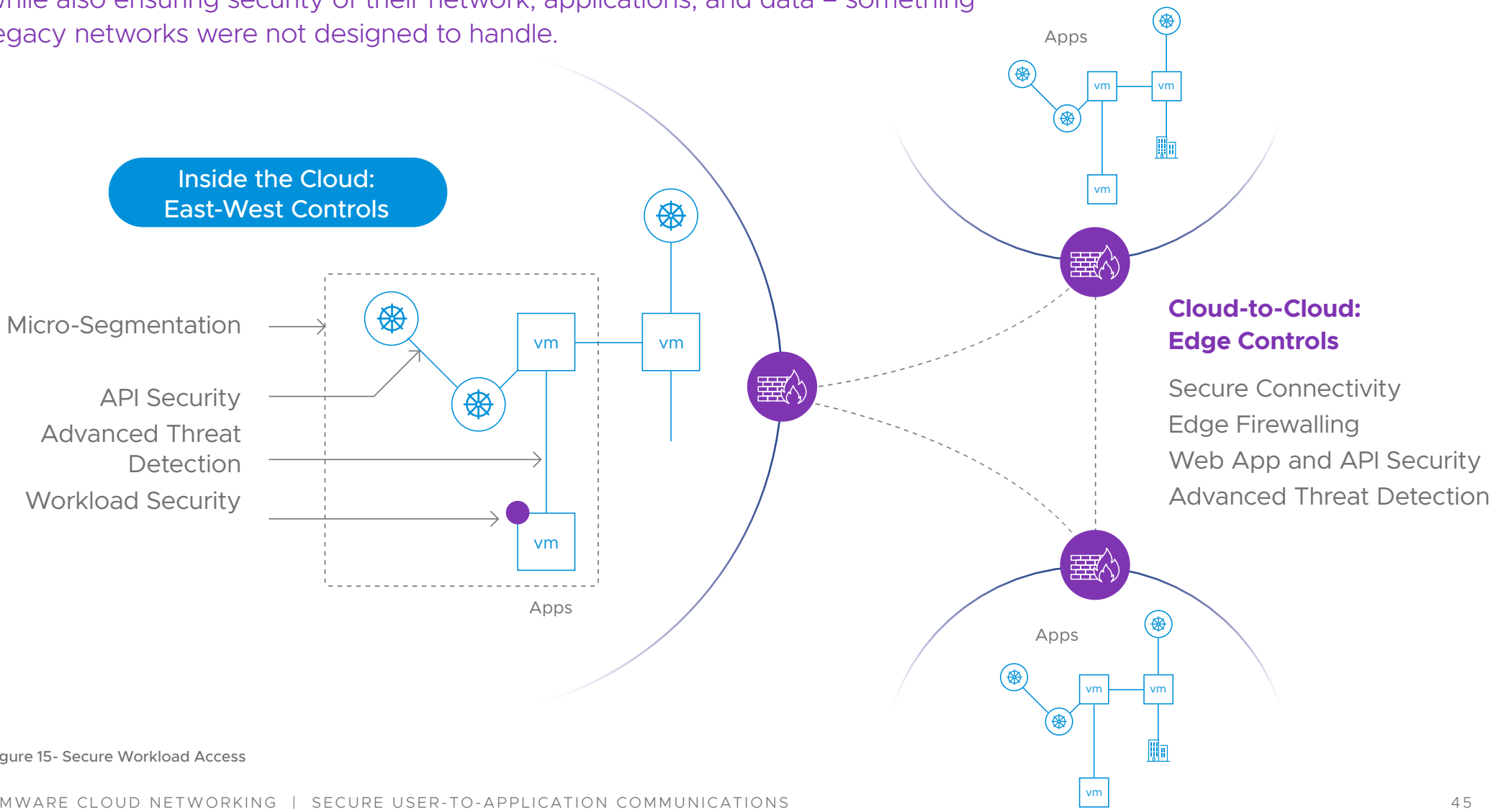


Figure 15- Secure Workload Access

Many Enterprises protect users and applications using separate networking and security stacks, saddling enterprise IT and end users with several challenges:

Inefficient routing for Cloud/SaaS applications, sending traffic to the data center before sending it back to the cloud resulting in poor application experience.

Supporting remote and mobile workers who access applications from anywhere on non-corporate owned devices resulting in larger surface of attack.

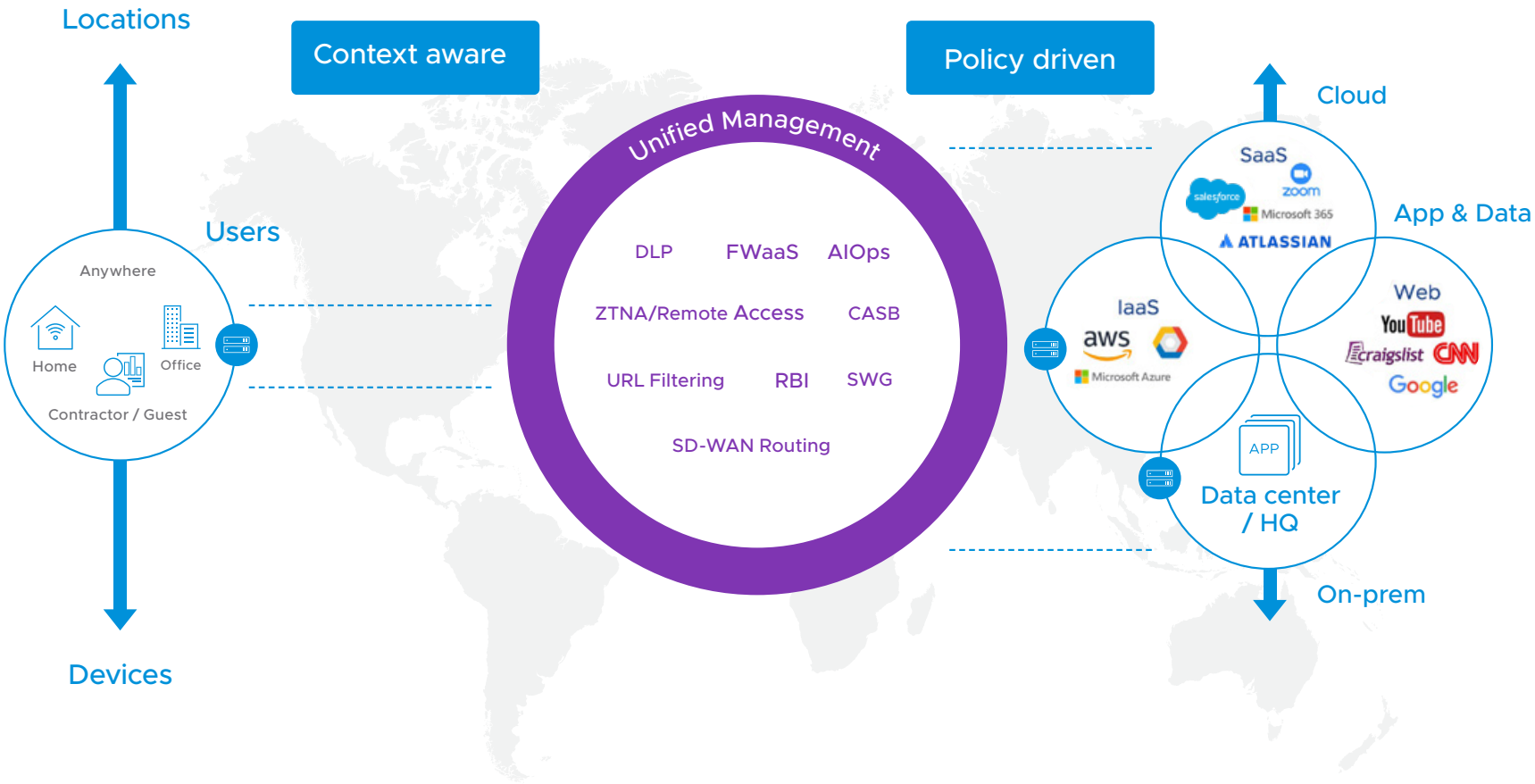
Operational complexities and increased costs with multiple, disparate networking and security solutions from multiple vendors.

Poor visibility into home and branch office LAN environment, making it hard to identify whether the problem is WAN or LAN related.

VMware SASE enables companies to support future needs without worrying if the network can handle the demands. A cloud-native platform, VMware SASE converges industry-leading cloud networking and cloud security to deliver flexibility, agility, protection, and scale for enterprises of all sizes. It can provide connectivity, security and optimized application access for all employees, no matter where they work, enabling access only to the apps they need on the devices they use.

VMware SASE with Comprehensive Capabilities

Addressing networking and security needs for distributed enterprises



VMware SASE includes SD-WAN, Secure Access, and Workspace ONE for zero trust network access, Cloud Web Security for securing web and internet access, and Edge Network Intelligence for AIOps — all through a single platform and delivered in a SaaS model.

Figure 16 - VMware SASE

VMware SASE with Comprehensive Capabilities

With the VMware SASE platform, enterprise IT can:

Provide users with optimized and secure access in the office or at home through SD-WAN, while Secure Access provides remote and mobile users the same experience as in the office, through the Zero Trust Network Access framework.

Protect all users from known and unknown web attacks with VMware Cloud Web Security.

Get advanced analytics and intelligence on application performance from client to POP and to workload running in any Cloud.

Define and manage business policies spanning security and network services via a single interface.

Sequence third-party services to the integrated services.

The VMware SASE platform is an easy to consume one-stop shop for security and network services, enabling a unified edge and cloud service model with a single place to manage business policy, configuration, and monitoring. It provides customers with the intrinsic security measures necessary to effectively operate in the digital world.

Secure Workload-to-Workload Communications

To prevent the lateral movement of threats, organizations also need to secure the communications between workloads that constitute enterprise applications and, by extension, between applications. Such security requires both access control and threat prevention.

In VMware's network security portfolio, access control is provided by the NSX Distributed Firewall. The NSX Distributed Firewall (DFW) implements access control policies at the granularity of the workload. Management of the Distributed Firewall is centralized to simplify operations. This style of per-workload access control is referred to as micro-segmentation or Zero Trust micro-segmentation.

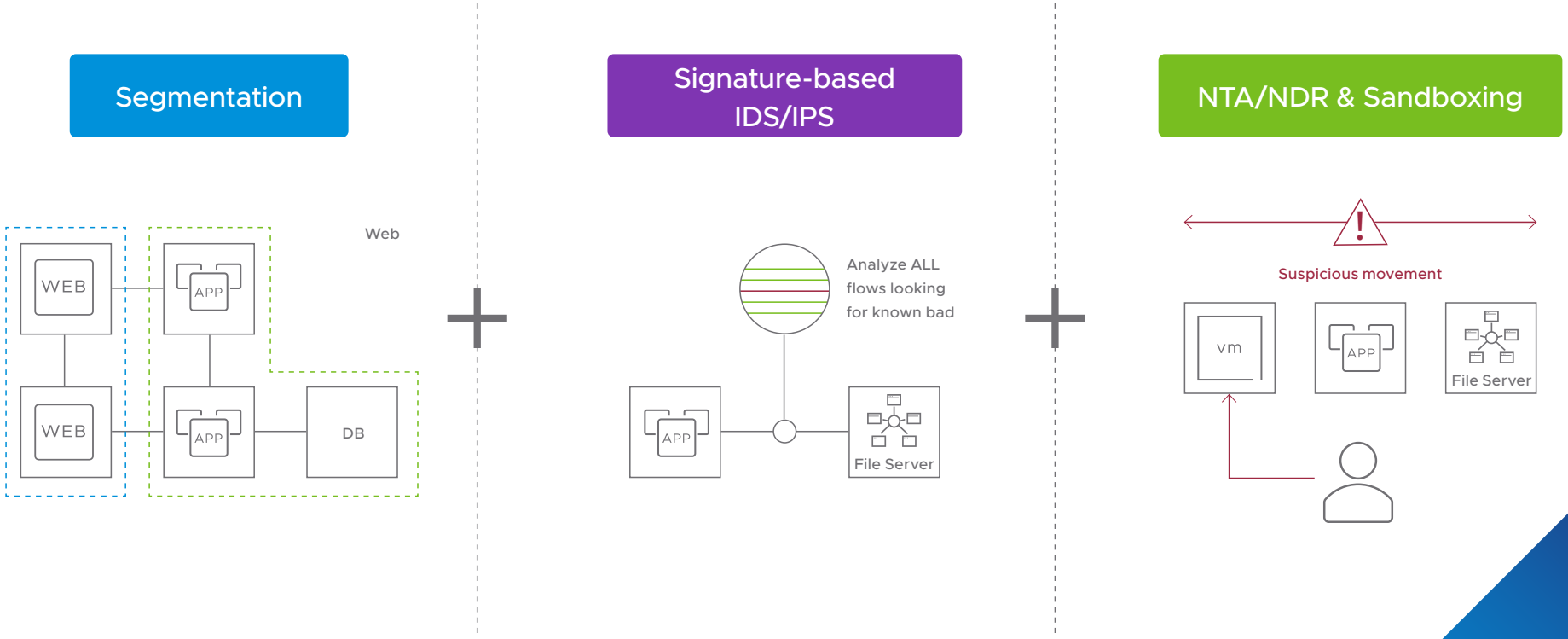


Figure 17 - Secure workload-to-workload communication

However, access control alone is often not enough to prevent lateral movement. Threats can travel inside permitted traffic once a workload has been compromised. The NSX Firewall has an additional capability-set called advanced threat prevention (ATP) that detects and prevents threats in permitted traffic.

Advanced threat prevention is composed from three detection technologies: intrusion detection/prevention (IDS/IPS); network sandboxing and network traffic analysis (NTA); and network detection and response (NDR) – a correlation engine. IDS/IPS primarily uses signatures (pre-recorded patterns) to detect known threats.

Network sandboxing emulates the full system (CPU, memory, and I/O) to observe and interact with running programs (executables) in an isolation environment to determine if the program is malicious or benign.

NTA works by first developing a baseline for normal activity in the network. Subsequently, it used statistical and machine learning techniques to identify anomalies against this baseline. Finally, it uses additional machine-learning and rule-based techniques to determine if an anomaly is malicious.

NDR combines signals from the three detection engines across multiple traffic flows to correlate security events into a small number of "intrusions." Using this comprehensive but condensed view, security teams can quickly understand the scope of the attack, zero in on real threats, and focus their attention on mitigation and remediation before damage can be done.

Advanced Threat Prevention applies to all kinds of workloads – physical, virtual and containerized – across all kinds of cloud infrastructures – private, public, hybrid or multi.

Intelligent Cloud Management

End users will rely on the network infrastructure to transport traffic between applications and users. There needs to be continuous network monitoring and application monitoring to ensure the best user experience.

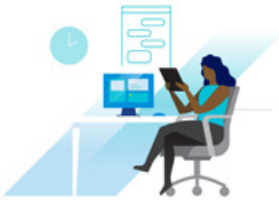
The modern application is the most complex and demanding for networks because of their service level objective (SLO) and resources to drive those applications can be scattered across the cloud or on-premises.

Visibility across this entire path is required to ensure applications are running properly. Tools for monitoring the dataflow for optimum traffic within the enterprise perimeter can be challenging and time-consuming to use. They often don't complete visibility across virtual and physical networks to optimize performance.

Customers need a simple, easy-to-use, end-to-end management tool to troubleshoot and get best practices compliance. They need a system which allows them to monitor and control platforms, traffic and applications throughout their hybrid cloud network.

Such a system should be able to:

Present all the information administrators need to make informed and effective decisions in a single, intuitive interface.



Provide end-to-end visibility and give real-time flow and traffic analysis for applications and services on the hybrid public-private-cloud and on-premises network.

Deliver point-and-click application discovery and performance optimization designed for fast-moving network and business needs.

Easy-to-use troubleshooting for all the apps, services, platforms and sites connected to the network.

Proactive alerting which helps notify before a fault actually occurs.

VMware vRealize Network Insight

vRealize Network Insight simplifies administering and troubleshooting the Modern Network which includes solutions like NSX and connections to other infrastructure like cloud and physical third-party infrastructure. It helps you improve performance and availability with converged visibility across physical and virtual networks.

Benefits of using VMware vRealize Network Insight include:

- Providing network path visibility for Kubernetes pods and services. By providing unrivalled visibility and control of the network, it accelerates segmentation planning and deployment.
- The platform continuously audits your security posture to ensure compliance and instantly flags changes or possible threats in any part of the hybrid network.
- Manage and scale the deployment of resources and web applications quickly, efficiently, and with confidence.
- Application Discovery which maps out the components and dependencies of an applications and how it communicates with the rest of the infrastructure. This complex task is performed via machine learning.
- Easily manage network security consistently across public and private clouds as well as on-premises deployments.
- Reduce business risk by mapping application dependencies to avoid unplanned outages and service degradation, particularly during migrations.
- vRealize Network Insight Assurance and Verification capabilities provide network-wide modeling for virtual and physical networks, further expanding end-to-end network visibility across environments, enabling customers to improve network uptime and resiliency, troubleshoot faster using new search capabilities and proactively identify potential network problems based on intent with a new network-centric topology view.

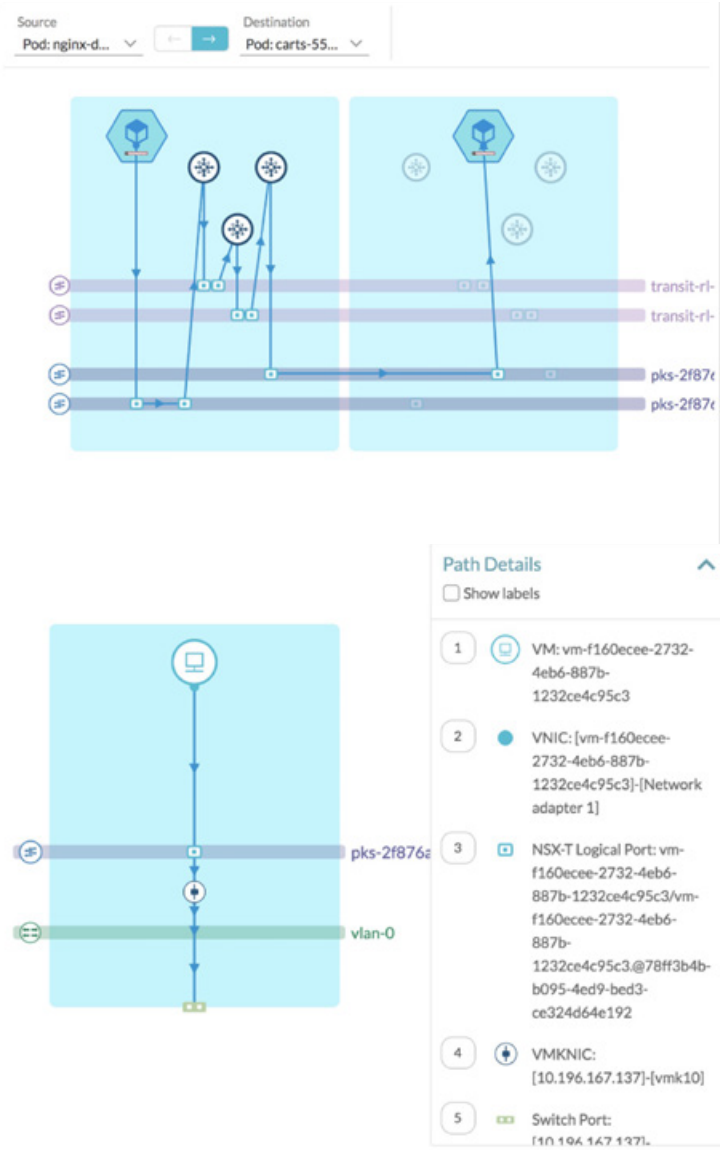


Figure 18- Kubernetes Path Visibility

Use Case: Improved Network Management

Often in large companies, particularly ones which have been through mergers or acquisitions, no one person, team, or system has complete oversight of the network. As a result, if there is a performance issue, tracking it down can be difficult, complicated, and slow. Sometimes, they may not even know all of the applications or dependencies on the network.

VMware vRealize Network Insight utilizes machine learning to analyze traffic flows across the network to discover applications and their dependencies. It can also visualize flows, providing admins with full visibility, from data center to cloud. It can find applications based on criteria such as naming convention, using ServiceNow CMDB data through direct integration, using the metadata tags attached to resources on their network and using something called flow-based application discovery, in which traffic flows are analyzed to discover applications.

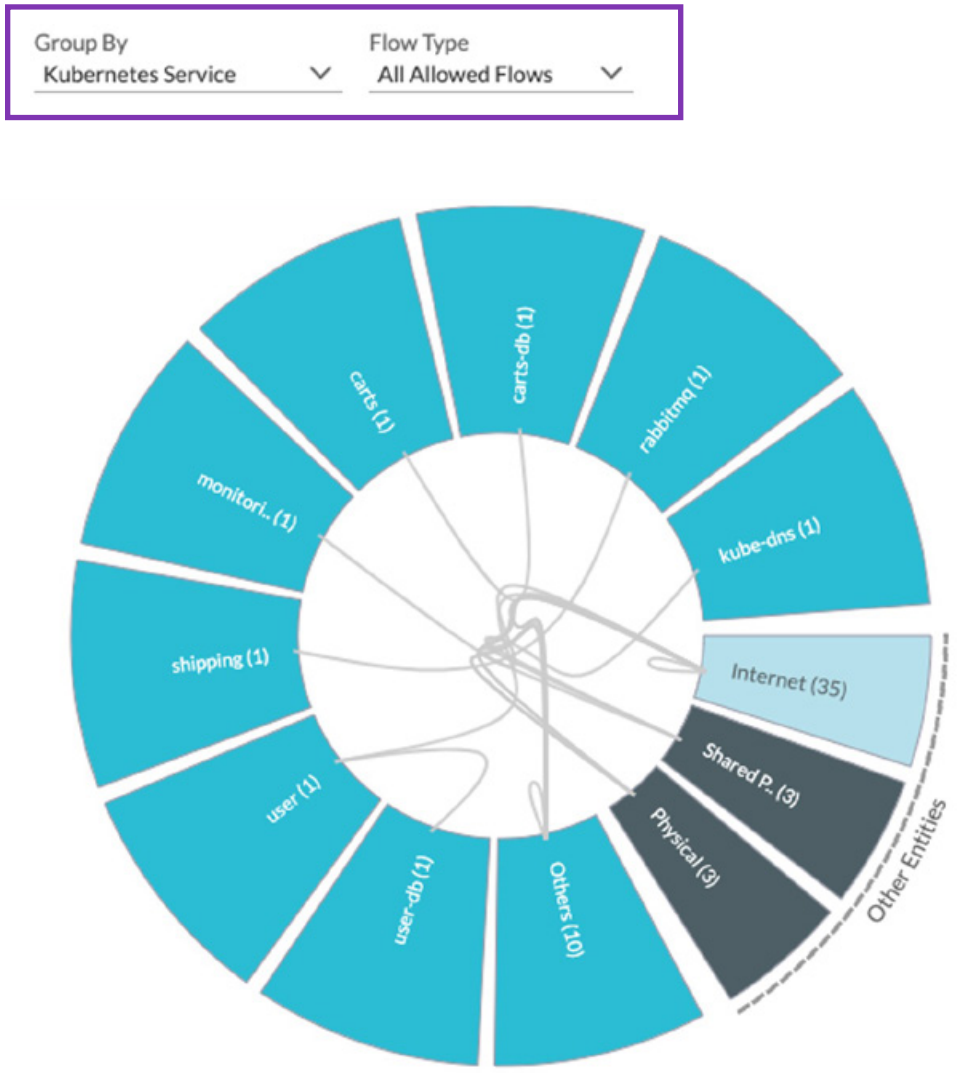


Figure 19 - Traffic flow visualization to help secure application

vRealize Network Insight can also visualize flows to provide full visibility from endpoint to data center to cloud traversing SD-WAN. This helps administrators to quickly track down misconfigurations and pain points that might cause performance or reliability issues.

Having found these resources, administrators can visualize them in VMware vRealize Network Insight, quickly gaining a complete oversight of all the activity on their network. This includes the physical network infrastructure, the underlay network, the overlay network, and the virtualized logical infrastructure built on the physical underlay.

With this newfound and whole-network visibility, administrators can plan, manage, and troubleshoot their networks more effectively to improve application performance for end users.

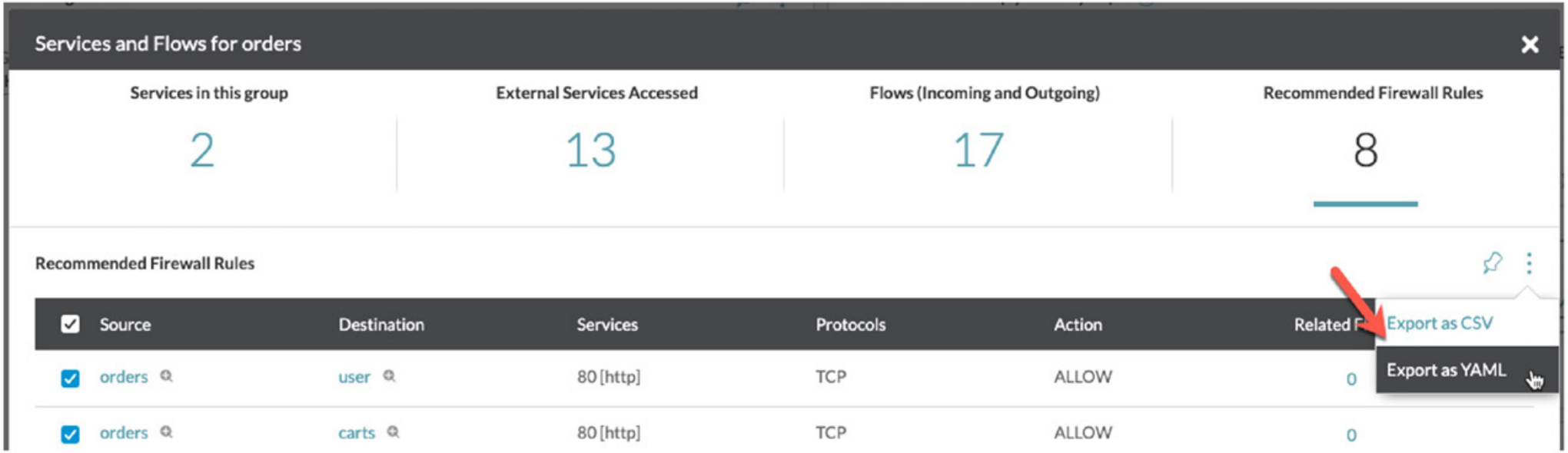


Figure 20 - Plan security policies for micro-services

Use Case: Improving App Security

It's impossible to adequately secure assets for which you don't have complete data. For instance, even if every application and hardware resource on your network is inventoried, if you don't have a full profile of the traffic to each resource, and an idea of how it compares to baseline normal, it's very difficult to spot abnormal activity, such as an intrusion or exfiltration of data.

In this way, administrators have a real-time overview of the entire network. As a result, they can quickly spot and address abnormal and possibly unauthorized activity. vRealize Network Insight makes securing the network and reacting to problems quickly far easier to do.

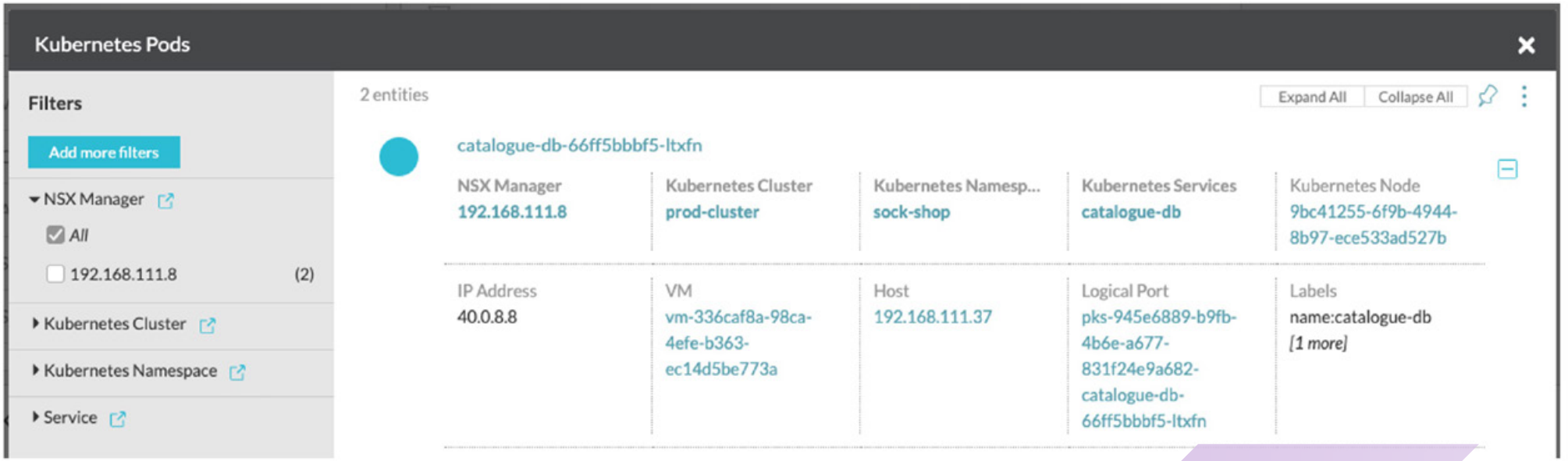


Figure 21 - Connecting the dots between containers and virtual & physical infrastructure

Creating Secure, Seamless Migration Paths

When moving to a cloud setup, or managing a complex cloud environment, administrators often find workload migration to be complicated, time consuming and unnecessarily stressful. Among other problems, they're often faced with technology stacks, on different cloud and on-site platforms, which aren't interoperable.

There may also be networking and security issues across sites. If application dependences aren't properly mapped, the migrations can cause disruption to running applications. All of these issues add up to disruptions to the business and potentially to financial losses.

To avoid these outcomes, administrators need a platform designed to simplify migration. Such an application should:

- Facilitate bulk migration of virtual machines without the need for downtime or extensive reconfiguration.
- Interface between different cloud and infrastructure platforms to ensure the migration of VMs, policies and settings.
- Be able to secure the migration so that data transmitted over wide area networks is encrypted and safe.

VMware HCX

VMware HCX is an application-mobility platform. It simplifies application migration, workload rebalancing, and business continuity across data centers and clouds. Its features enable large-scale app mobility across cloud and on-premises environments to accelerate data center modernization and cloud transformation.

Features of VMware HCX include:

- Migration-planning tools which make it easy to identify application and workload dependences and then group virtual machines for migration.
- The ability to perform scheduled bulk migrations without disruption to running systems.
- Migration across different cloud and on-premises platforms without disruption or downtime.
- The ability to migrate virtual machines without having to re-architect their IP addresses, ensuring seamless continuity of service.
- The ability to migrate virtual machines to vCenter from other hypervisors such as KVM and HyperV
- Facilitates the seamless of extension of the network and IP space across different sites and platforms, ensuring the integrity of policies and boundaries.
- The ability to secure migrations with VPN encryption while optimising the WAN link for maximum performance.

Creating Secure, Seamless Migration Paths

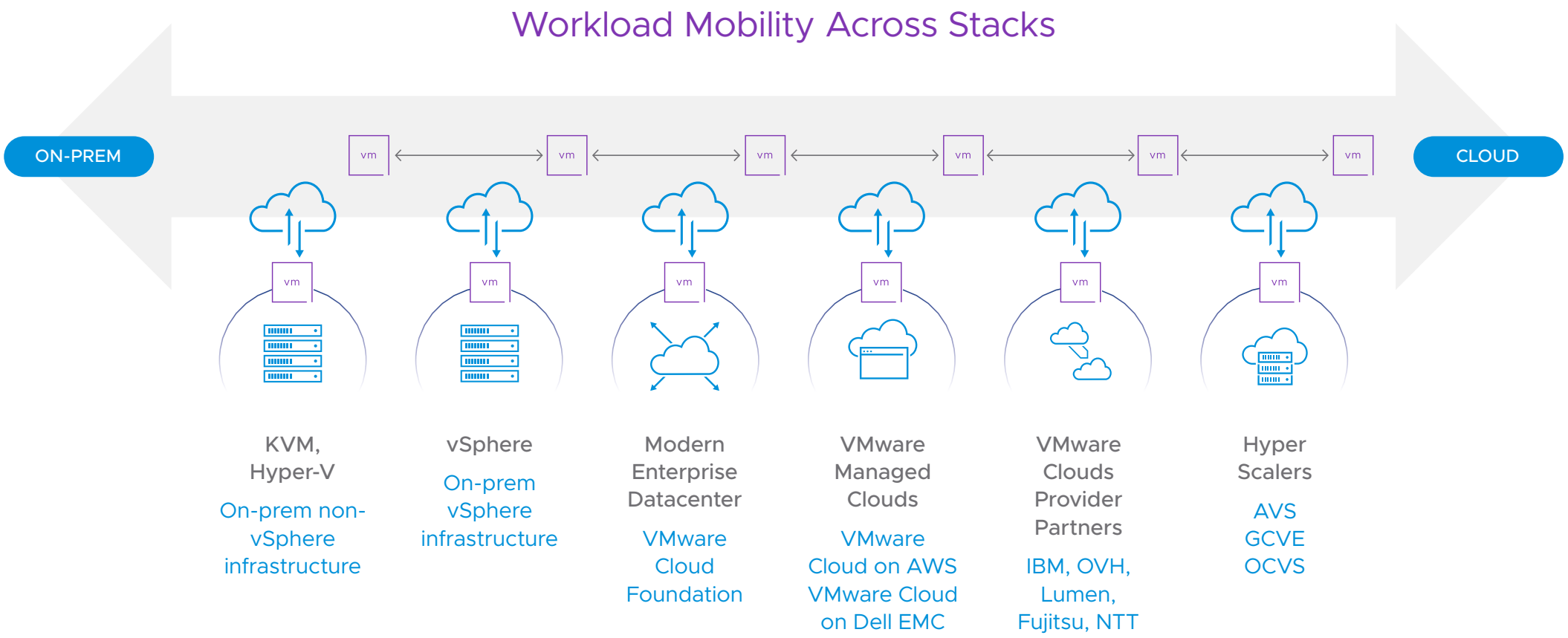


Figure 22- HCX VMware Mobility Platform for Multi-cloud

Case Study: Cloud Migration

When an enterprise migrates part of its data center to the cloud, it needs tools which will ensure continuity of service, security and compliance and data integrity during the move. Without these, service may be interrupted or, in the worst case, data lost.

Using VMware HCX, administrators can use specially designed migration planning tools to discover dependencies. This allows them to group machines for migration in a way that keeps dependencies intact. So, when the new, migrated, machines are spun up for the first time, they have all the services and resources they need to begin operating and taking customer requests.

Thanks to the platform's site-to-site architecture, IP relationships are kept intact during the migration. Again, this means that the new VMs can be spun up without disruption. And because it's easy to schedule bulk migrations, the transfer of data can happen at a time when it's least disruptive for your organization.

With VMware HCX you can also better plan these migrations in multiple waves as HCX provides predictive estimation time and real-time estimation time of workload migrations.

HXC Cloud Migration

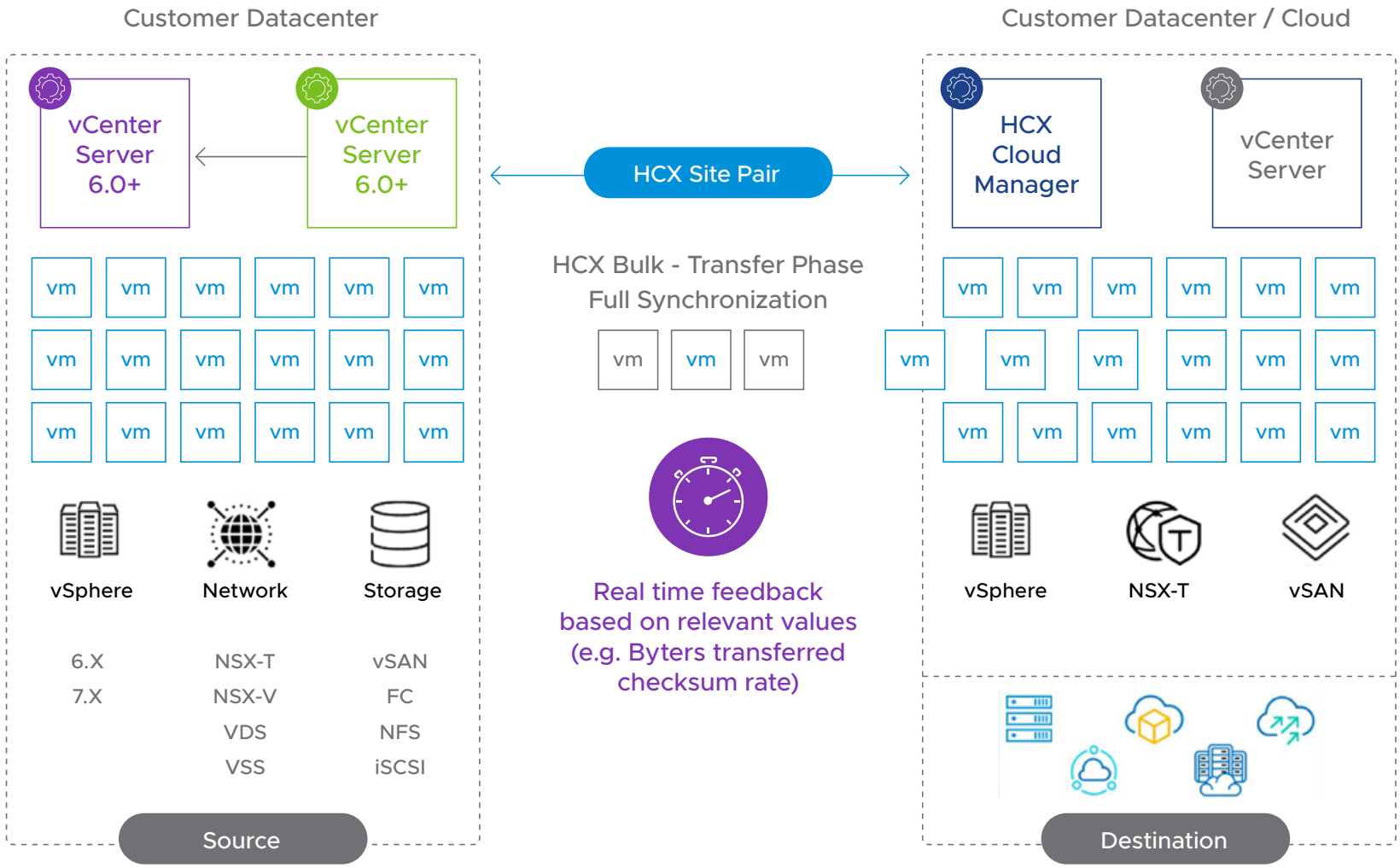


Figure 23 - HCX Cloud migration

Use Case: Data-Center Consolidation

Virtualization allows companies to consolidate their data centers by virtualizing their servers and then migrating multiple virtual servers to a smaller number of physical machines. This increases system utilization, improving return on investment (ROI).

But without a system to automate the consolidation process, there is a significant chance of error leading to disruption. The process is also likely to take longer, and cost more, than it ought to.

With VMware HCX, you have all the tools you need to map dependencies, plan the migration and then consolidate your data-center functions on VMware virtual machines, running on a smaller number of physical systems.

The solution makes it possible to do this without IP re-architecting or the re-mapping of MAC addresses. Using the application's single-pane interface, it's easy to monitor the migration from physical to virtual machines or consolidate VMs running on different hypervisors (KVM or HyperV) to vCenter. Because all traffic is encrypted, you can migrate within or across sites without worrying about security. This combination of visibility and control allows for even complex migrations to proceed with zero downtime.

Next Steps

VMware Cloud Network delivers the agility, flexibility, and comprehensive security businesses need from their IT infrastructure in today's market. By transitioning to multi-cloud networking and security infrastructure, businesses give themselves the ability to respond in real time to rapidly changing customers preferences and demands.

When you work with VMware, modernizing your network is fast, seamless and efficient. Our experts can help you analyze traffic and demanding patterns and then choose exactly the right mix of technologies to meet your needs today and in the future.

Once they have an agreed understanding of your needs and goals, VMware specialists will work with you to set SLOs that reflect this understanding. These SLOs don't just underpin your contract, they're also built-in triggers for infrastructure to automatically scale, without you needing to do anything.

This allows you to maintain the level of customer experience your business relies on, no matter what happens.

To find out how VMware Cloud Networking can help your business out-compete in a rapidly evolving digital marketplace, contact VMware today.

- **1-877-486-9273**
- **sales@vmware.com**

About VMware

VMware is a world-leading specialist in virtualization, cloud infrastructure and intelligent networking. At VMware, we believe that software has the power to unlock new opportunities for people and our planet.

We look beyond the barriers of compromise to engineer new ways to make technologies work together seamlessly. Our compute, cloud, mobility, networking and security offerings form a digital foundation that powers the apps, services and experiences that are transforming the world.

Since our founding over two decades ago, our 24,000+ employee community and ecosystem of 75,000 partners have been behind the technology innovations transforming entire industries – from banking, healthcare, and government to retail, telecommunications, manufacturing, and transportation.

Every day, we work to solve our customers' toughest challenges through disruptive technologies like edge computing, artificial intelligence, blockchain, machine learning, Kubernetes and more – to define the digital foundation that will accelerate the next wave of innovation.

vmware®

Contact Us

To find out how VMware can help your business become more agile, get in touch today:

- 1-877-486-9273
- sales@vmware.com

www.vmware.com