White Paper

Meeting the Challenge of Multicloud Networking: Optimizing Cloud Workloads and Application Experience

Sponsored by: Cisco

Brad Casemore
November 2020

IDC OPINION

As organizations continue to pursue digital transformation to achieve greater agility, efficiency, and competitive advantage, they are adopting hybrid IT and multicloud as integral means to those ends. As a result, formerly centralized applications and workloads residing in on-premises enterprise datacenters are being distributed across clouds. At the same time, workforces are becoming increasingly mobile and dispersed, working from campuses, branch offices, and increasingly – as a result of the COVID-19 pandemic – home offices. These trends are redefining the parameters of the traditional datacenter and compelling organizations to modernize and extend their network infrastructure to accommodate distributed multicloud workloads as well as application access spanning an unprecedented variety of network endpoints and locations.

> Multicloud networks need to be capable of delivering the agility, flexibility, elastic scaling, operational efficiency, and security required by cloud-centric organizations.

The network is the central nervous system that enables and supports digital transformation. Indeed, within the context of multicloud, the network has never been more important than it is today. In fact, the migration of applications and workloads to public IaaS and SaaS clouds has driven a clear need for an expansive and robust multicloud network infrastructure – extending from workloads to access – capable of delivering the agility, flexibility, elastic scaling, operational efficiency, and security required by cloud-centric organizations.

This white paper examines the need for a comprehensive multicloud network that can meet the requirements of IaaS and SaaS cloud workloads as well as the demand for continuously available, responsive, and secure access to cloud applications.

Note: All numbers in this document may not be exact due to rounding.

SITUATION OVERVIEW

Even before the COVID-19 pandemic struck, enterprises worldwide had embraced multiple clouds as a key means of achieving digital transformation objectives. While most enterprises still have valuable workloads running in on-premises environments, they had adopted SaaS where appropriate, and a growing number of organizations were taking new and existing workloads to IaaS and PaaS clouds (e.g., AWS, Microsoft Azure, Google Cloud, and IBM Cloud).

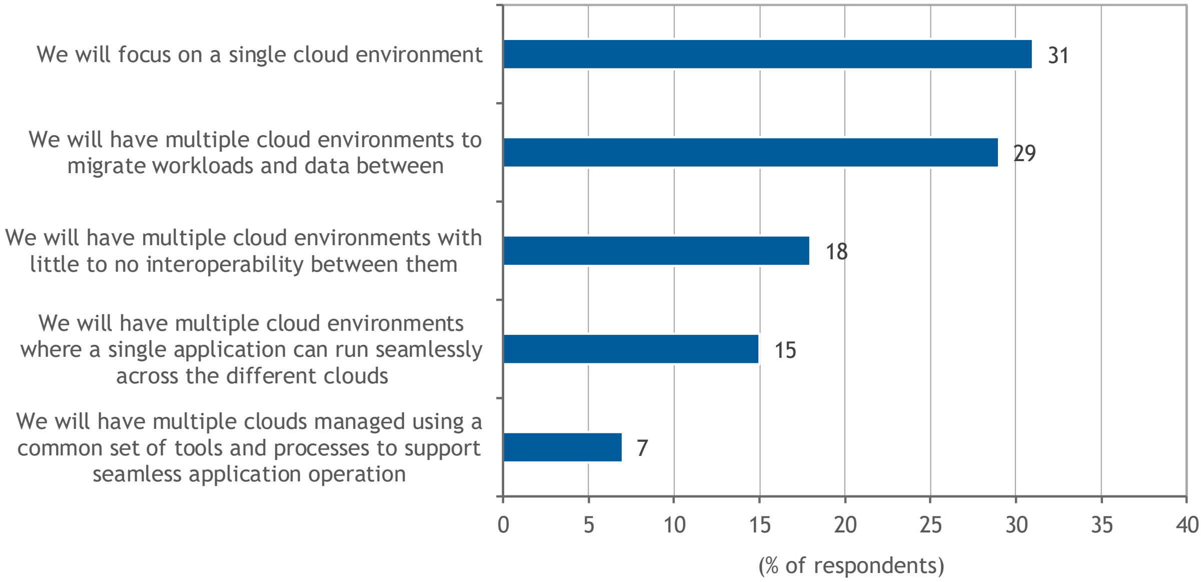
The pandemic has accelerated that trend, with enterprises increasingly considering the role of cloud in facilitating an effective strategy for business resilience and continuity.

However, before COVID-19, the principal driver for the adoption of public cloud was the desire for greater business agility in support of digital transformation. That objective remains, but now it is reinforced by a desire to achieve greater business resilience, encompassing business continuity as well as supporting the addition of more digital services. According to IDC's 1Q20 *Cloud Pulse Survey,* 69% of organizations are investing in a multicloud strategy (see Figure 1).

FIGURE 1

Investment in Multicloud Strategies

Q. Over the next two years, how would you describe your organization's use of different on-premises and off-premises cloud environments?



n = 837

Source: IDC's *Cloud Pulse Survey,* 1Q20

Organizations that were already on the cloud journey are accelerating their pace, and those that were considering moving in that direction are moving quickly off the fence. The datacenter network, as well as the wide area network (WAN) extending to multiple clouds, branches, and edge locations, will have no choice but to evolve as the acute need for business resilience becomes a long-term objective.

As enterprises execute their cloud strategies, they invariably find that infrastructure modernization, including network infrastructure, is both acutely required and highly challenging. In IDC's 2019 *Datacenter Operational Survey,* enterprise respondents identified "ensuring data security and compliance" and "improved network performance" as their top 2 priorities and challenges in hybrid IT and multicloud environments. Similarly, in IDC's 3Q19 *Cloud Pulse Survey,* 59% of enterprise respondents indicated that "integrated network processes across cloud providers" would be an important area for cloud investments during the next two years.

59% of enterprise respondents indicated that "integrated network processes across cloud providers" would be an important area for cloud investments during the next two years.

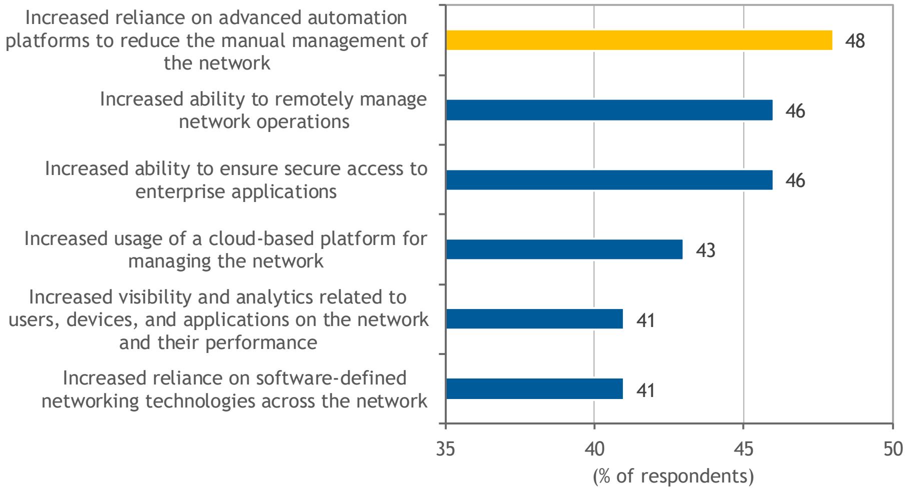
Network modernization for multicloud must begin with a basic and irrefutable principle: The distributed application is the new center of gravity for networking. In the multicloud era, enabled by ever greater levels of intelligence and automation, networks must be more closely aligned with the dynamic needs of applications and workloads than ever.

Indeed, network automation is an area in which COVID-19 has driven increased enterprise interest and adoption. In IDC's June 2020 *Future Proofing Enterprise Networking Survey,* enterprise respondents were asked to identify areas of increased investment in the post-COVID-19 world. Nearly half (48%) of the respondents cited "increased reliance on advanced automation platforms to reduce the manual management of the network," with related areas also receiving prominent mention (see Figure 2).

FIGURE 2

Areas of Increased Network Investment in the Post-COVID-19 World

Q. In which of the following areas, if any, will your organization increase investments as a result of new business operations that are required because of COVID-19 or in a post-COVID-19 world?



n = 254

Source: IDC's *Future Proofing Enterprise Networking,* June 2020

While networking has been software defined in the on-premises datacenter and, more recently, even across the WAN (in the form of SD-WAN), the rise of multicloud means that the need for control and agility – delivered through intelligent, policy-based network automation – extends even further. As IT goes hybrid, supporting distributed applications that reside on premises and in public clouds, there's a need not only for a consistent, extensible network and security policy spanning this new landscape but also for a new way of routing traffic expeditiously and reliably through cloud middle miles and cloud cores, providing secure ingress and convenient on-ramps into clouds to mitigate latency, improve availability, and enhance application experience.

A comprehensive understanding of multicloud networking extends from the now distributed multicloud datacenter, where applications and workloads reside, to the endpoints (users and devices), at campuses, branch offices, home, and other edge locations, where application experience is ultimately delivered.

With applications as the center of gravity, the point of orientation for all networking, enterprises must consider application-centric network modernization from the core to the edge, covering the entire application journey from workload optimization to application access and experience.

MODERN OPERATIONS FOR MULTICLOUD NETWORKS

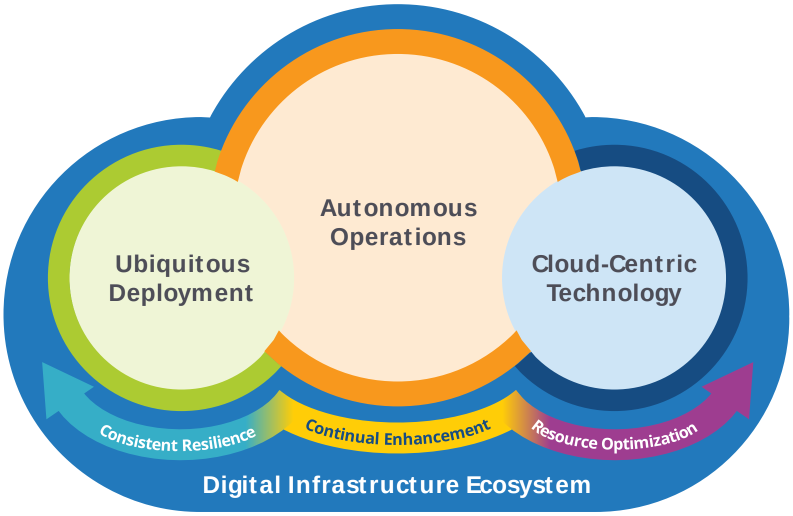
Not surprisingly, new demands will be placed on IT operations, including network architects and cloud architects. Indeed, IDC forecasts major operational and organizations shifts in the next few years. IDC predicts that, by 2023, 55% of enterprises will replace outdated operational models with cloud-centric models that allow for better alignment between IT operations and public cloud operations and facilitate organizational collaboration, resulting in better business outcomes.

> IDC predicts that, by 2023, 55% of enterprises will replace outdated operational models with cloud-centric models that allow for better alignment between IT operations and public cloud operations and facilitate organizational collaboration, resulting in better business outcomes.

A more autonomous and dynamic future of digital infrastructure relies heavily on connected cloud architectures that enable enterprises to migrate and integrate workloads and data running in different types of clouds located in multiple physical locations (see Figure 3).

FIGURE 3

IDC's Future of Digital Infrastructure Framework



Source: IDC, 2020

For network operators, including network professionals and cloud architects, the ramifications will be profound. Architectures and the underlying infrastructure must become more agile, flexible, and consistent across multiple cloud environments, and the same demands are being made on those who operate and manage networks.

In response, network engineers and network operators are looking to adopt controller-based architectures and gain knowledge and proficiency in areas such as automation, programmability, and cloud (APIs and virtual private clouds [VPCs]/VNETs). Network operations (NetOps) teams must master not only automated provisioning and elastic scaling of network infrastructure – to support the dynamic ebbs and flows of digital business and to keep the business online and running during exceptional circumstances – but also the post-deployment Day 2 needs of being able to provide faster troubleshooting and remediation of issues that can impair network availability and performance and thus affect application experience.

Networks now serve as the core (or central) nervous system, with a brain (in the form of controllers), a spinal cord (in the form of a network fabric), and sensitive nerve endings (in the form of telemetry). With these capabilities, networks and their operators support increasingly important applications and data and help keep the business running during disruptions or crises.

Network operators are expected to leverage pervasive real-time telemetry and visibility to provide faster identification, isolation, and automated resolution of network security incidents. In this context, policy- and event-based detection and prevention will be essential to ensure that networks and their operators play valuable roles in protecting the integrity and resilience of applications. This requires advanced visibility and analytics capabilities across enterprise and public networks, extending holistically from datacenter and cloud cores to WAN, internet, cloud, and edge networks and ultimately to where applications are accessed at endpoints in campuses, branches, and homes.

Many of these capabilities will be enabled by AI/ML technologies as mechanisms, but for network operators and the organizations to which they belong, the value will be realized through tangible business outcomes. In IDC's view, by 2023, more than 70% of enterprises will adopt a proactive posture to network operations across multicloud networks, delivering better alignment with business objectives through a reconciliation of the need for centralized visibility with the imperative of moving fast in support of digital business objectives or in response to disruptions and threats that affect business continuity.

By 2023, more than 70% of enterprises will adopt a proactive posture to network operations across multicloud networks.

CHALLENGES OF MULTICLOUD NETWORKING FOR DISTRIBUTED WORKLOADS

With applications and microservices proliferating across the network (in the datacenter, as public cloud services, as network-hosted services, and at edge environments), the datacenter network is no longer geographically defined and relegated to a specific physical location. Instead, it has become a growing set of interconnected "nerve clusters" alongside applications and data, which increasingly will be placed where they will deliver the greatest business efficacy and value.

The fact is networking for these increasingly distributed workloads, applications, and microservices is a complex undertaking. That complexity often includes time-consuming manual provisioning. Daunting routing challenges across regions and clouds, and differences between specific clouds in areas such as number of routes, segmentation, and available throughput, promote the need for specialized expertise across various cloud-specific APIs and cloud-specific network services. Application dependencies also have to be taken into account. On average, each business application has four to eight application dependencies, and those dependencies are on track to multiply in the years ahead. IDC forecasts that, in 2021, 47% of applications will be built using modular development frameworks characterized by containers and microservices, according to IDC's 1Q19 *Cloud Pulse Survey*.

Enterprises want the capacity to stretch existing policies, governing tenants or workloads, across network fabrics that traverse on-premises and cloud environments.

In networking, complexity always manifests in costlier and lengthier processes. In addition to the challenges mentioned previously, enterprises pursuing multicloud often find that they must overprovision their firewall services and implement convoluted symmetric routing to accommodate firewalls across clouds. They also struggle to achieve the cloud's promise of elastic autoscaling, especially in relation to seamless insertion of network and security services higher up the stack.

These issues are compounded by the lack of cross-cloud networking expertise in most enterprise IT departments. To be fair, not many enterprises are well equipped to quickly come up to speed on the various architectures, network APIs, and network and security services offered by different IaaS clouds, much less devise a homegrown approach that brings consistency and proficiency to management.

In effect, enterprises want the capacity to stretch existing policies, governing tenants or workloads, across network fabrics that traverse on-premises and cloud environments, with centralized policy provisioning and management applied over this increasingly critical facet of network infrastructure.

Increased Focus on Holistic Workload Protection

Distributed application environments have also created a need for holistic workload protection. To be sure, in the context of hybrid IT and multicloud, where legacy applications remain relevant even as enterprises embrace a future that includes a growing complement of cloud-native applications, workload protection is of paramount importance. Legacy workloads must still be protected, but the advent of multicloud introduces larger attack surfaces and proliferating points of vulnerability. What's more, the ascent and primacy of applications mean the integrity and security of workloads, irrespective of where they reside and how they were architected, are chief concerns for all enterprises. That's why it's essential for modern security mechanisms and models to be pervasive across legacy and cloud-native workloads characterized by containers and microservices.

> It's essential for modern security mechanisms and models to be pervasive across legacy and cloud-native workloads characterized by containers and microservices.

Today, enterprises use a range of point products to address workload protection use cases. For example, they have separate tools to address discovery, security enforcement and microsegmentation, compliance and audit, network forensics, simulation, network visibility, container security, and software vulnerability and process behavior. Unfortunately, these disparate tools, even when they have kept pace with evolving requirements, function as discrete and disconnected puzzle pieces that provide only partial and fragmented elements of workload protection. Point products also inherently lack the ability to deliver "network effects," in which a product or technology is used systemically across a growing number of use cases, with benefits and value multiplying as it addresses each additional use case.

Increasingly, enterprises, which are seeking to mitigate the complexity of managing multicloud environments, are looking for ways to consolidate the tools they use to achieve holistic workload protection.

CHALLENGES OF MULTICLOUD NETWORKING FOR SECURE ACCESS AT THE EDGE

At the edge, too, new user access challenges have emerged as a growing percentage of the applications that are accessed and consumed reside in SaaS or IaaS public clouds rather than in traditional on-premises datacenters.

This results in some common networking challenges for both SaaS and IaaS, as well as some challenges that are unique to each realm. For SaaS, IT teams must be capable of ensuring that applications are delivered reliably and securely to employees and other stakeholders across a distributed (and increasingly diffused) enterprise landscape, without having direct control of much of the interconnecting networks. The WAN plays a critical role here, and it has been modernized, in the form of SD-WAN, to address the needs of SaaS applications, which have network requirements that include adequate bandwidth, low latency (especially for collaborative apps), packet loss and packet reordering, and jitter.

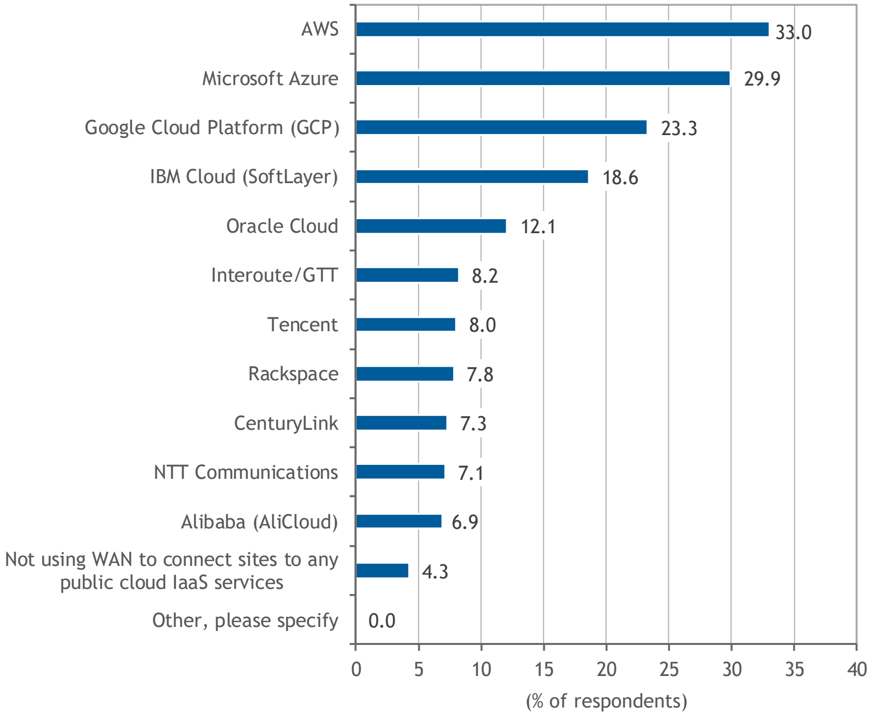
In IDC's 2019 *Software-Defined WAN (SD-WAN) Survey*, 73% of enterprise respondents indicated that SaaS and cloud services were currently important to their WAN technology choices.

In IDC's 2019 *Software-Defined WAN (SD-WAN) Survey,* 73% of enterprise respondents indicated that SaaS and cloud services were currently important to their WAN technology choices, with that percentage rising to more than 78% when they were asked to consider how the situation might change in the next 12-24 months. What's more, only 4% of organizations reported not having a WAN connection to at least one IaaS provider (see Figure 4).

FIGURE 4

Use of WAN to Connect to IaaS

Q. Is your organization currently using WAN to connect sites to any of the following public cloud IaaS services?



n = 1,223

Base = all respondents

Notes:

This survey is managed by IDC's Quantitative Research Group.

Data is weighted by country GDP.

Use caution when interpreting small sample sizes.

Source: IDC's *Software-Defined WAN (SD-WAN) Survey,* November 2019

With the advance of hybrid and multicloud, enterprises will seek simple means of connecting sites to multiple clouds and having rich telemetry and visibility to gain actionable insights that assist in refining application-based declarative policies and facilitate expedited troubleshooting, identification, and remediation of application and network issues across the multicloud landscape. The reasons are clear. The traditional WAN is deficient when it comes to supporting both SaaS and IaaS applications. That's because the traditional WAN came of age in the client/server era when applications resided exclusively behind the firewall in enterprise datacenters. WANs were designed and constructed to support and secure static branch-to-datacenter and branch-to-branch traffic, not to support increasingly branch-to-cloud application traffic. Further, the traditional WAN is poorly suited to the security requirements associated with these cloud applications.

From an SD-WAN perspective, certain requirements have come to the forefront. A need arose for declarative intent-based application-centric policies and pervasive visibility into application context and performance over the WAN all the way to the cloud provider, as well as visibility into the performance of underlying public internet and cloud networks themselves.

That is particularly true as internet and cloud networks play an increasing role in supporting workloads and application experience. More than ever, network operators require pervasive visibility so that they can proactively detect and identify potential network degradation and disruptions that could affect cloud application performance and experience.

For access to IaaS workloads and SaaS applications, a multicloud-capable SD-WAN offering should support intent-based automation that gives network operators the control to provide the best possible application experience. A multicloud-capable SD-WAN should offer optimal dynamic path selection, integration with cloud services (middle miles and cores), and optimizations when and where needed for real-time cloud applications affected by latency or jitter.

Importance of Multicloud Access Security

Enterprises must provide robust security for multicloud access. An effective framework to secure multicloud access must fuse both networking and security in edge environments and cloud-based security capabilities for consistent protection of users and data regardless of their locations. Workforces are more dispersed than at any time in IT history, but irrespective of whether they're in a branch or remote office or in a coffee shop or working from home, they always require secure network access and the best possible consistent experience across on-premises, SaaS, or IaaS applications and workloads. Unfortunately, this is where traditional security architectures and the sprawl of disparate tools fall short of the mark, leaving users vulnerable and businesses exposed.

Network and security teams increasingly recognize that they need a holistic yet simple approach that integrates network and security functionality to deliver secure multicloud access. Security functionality for multicloud access can be delivered from the cloud or integrated into the SD-WAN edge router – or a combination of the two.

Security functionality for multicloud access can be delivered from the cloud or integrated into the SD-WAN edge router — or a combination of the two.

Cloud-based security provides consistent, ubiquitous protection and should comprehensively address areas such as DNS security, secure web gateway, firewall as a service, cloud access security broker (CASB), and zero-trust access. In addition, security should include protection against unknown or zero-day threats, based on segmentation, advanced threat intelligence, and behavioral insights.

In SD-WAN scenarios, IT teams not only want the reduced costs and application performance benefits of direct internet access (DIA) at the branch but also want to ensure that it comes with no compromise to security. Secure cloud connectivity at the branch offers a viable approach, with strong protection as well as lower bandwidth consumption, lower latency, and cost savings that accrue from reduced dependence on expensive private WAN transports. With a full security stack — next-generation firewall, IPS, AMP, and URL filtering — as well as analytics and visibility for actionable insights, organizations can ensure that security and networking are effectively combined to ensure and protect the integrity of the applications on which businesses depend.

In the case of some organizations that are highly regulated or prohibit direct internet access, recourse can be made to a hybrid approach that facilitates aggregated access from multiple branches to the internet and public clouds through regional colocation or interconnection facilities, which can host and run a full-stack security framework.

HOW TO GET STARTED WITH MULTICLOUD NETWORKING

As organizations enact a multicloud strategy as part of their digital transformation efforts, a comprehensive step-by-step multicloud networking approach will be essential to ensuring that the plan succeeds and delivers both business value and operational efficiencies. One way to proceed is to set a networking course that aligns closely to both application requirements and cloud principles and cloud operating models, delivering on the promise of greater agility, increased flexibility, and enhanced operational simplicity.

This will translate into an emphasis on applications, from where workloads reside to where applications are consumed and experienced by users. Any multicloud network that is misaligned with workload requirements risks falling short of the mark. Likewise, any multicloud network that doesn't consider application experience and engagement runs the risk of not delivering the desired benefits.

After organizations evaluate their distributed applications and current and future cloud objectives, a multicloud networking approach can proceed with an emphasis on two primary considerations:

- **Applications:** Workloads, including modern architectures composed of microservices and containers, must be supported by an agile, flexible, and elastically scalable network that delivers consistent and simple provisioning, management, and security.
- **Access:** Highly available and responsive access to applications (including on premises, IaaS, and SaaS) must be delivered with consistent security, reliability, and performance to users and devices anywhere.

Getting Started with Multicloud Networking for Distributed Workloads

1. **Extend network visibility and analytics.** As applications are distributed beyond the traditional datacenter, IT teams need to extend their telemetry, visibility, and analytics capabilities to ensure that applications remain available and responsive at all times. Because the multicloud network now comprises datacenter, WAN, broadband, and cloud networks, it's important to achieve visibility across all these domains. Advanced analysis of data aggregated from multiple domains, together with the increased use of AI/ML as supporting technologies, will provide faster troubleshooting and remediation in these increasingly complex and distributed environments.
2. **Extend policy-based network automation.** In the context of digital transformation and business resilience, agility and flexibility are understandably prized. Network automation tools should enable NetOps teams to adopt new multicloud processes and mitigate the increased complexity of managing distributed workloads across disparate cloud environments. Policy-based automation tools are evolving alongside cloud to enable efficient and accurate connectivity of network service/functions within multicloud environments.

   Automation tools typically have adapters that allow them to work with a range of cloud services from different cloud service providers. Therefore, the right automation tool will enable interoperability in a hybrid and multicloud architecture. The automation tool will also remove application and data portability constraints between clouds and on-premises datacenters. IT organizations can limit interoperability concerns by utilizing automation tools that integrate seamlessly with a wide range of cloud services and cloud service providers.
3. **Protect workloads and data from attack.** Workload protection is a growing business concern across a multicloud environment, and organizations need to gain visibility into threats to ensure that they implement a viable defense. Visibility must be both pervasive and real time, capable of sensing and facilitating responses to anomalies and threats that span users, devices, applications, workloads, and processes (workflow).

   From a network standpoint, visibility must be available within datacenters – into north-south and east-west traffic flows – between datacenters, and out to campus and branch sites as well as to clouds. Visibility should extend up the stack, too, all the way to application components and behavior, giving organizations views into potentially malicious activity such as data exfiltration and the horizontal spread of malware from server to server. Containers and microservices will place an even greater premium on full-stack visibility.

   Once visibility is achieved, organizations can seize actionable insights to implement policy-based segmentation comprehensively and effectively, protecting against lateral propagation of attacks within and between datacenters and preventing malicious parties from gaining access to high-value datacenter assets, including sensitive data.
4. **Combine automation and insight tools for closed-loop intent-based networking (IBN).** Bringing policy-based automation together with AI-enabled insights in a closed-loop IBN model can result in automation of the complete network management life cycle and provide network infrastructure that continuously tracks and adheres to business intent. IDC predicts that simple, declarative management models with enhanced verification capabilities and better closed-loop processes will be increasingly informed by streaming telemetry and pervasive network visibility, resulting in the growing trust of automated network infrastructure through 2025. This trust will extend from provisioning to AI-assisted Day 2 network operations. Such capabilities can collectively help

Getting Started with Multicloud Networking for Distributed Workloads

1. Extend network visibility and analytics.
2. Extend policy-based network automation.
3. Protect workloads and data from attack.
4. Combine automation and insight tools for closed-loop intent-based networking (IBN).

IT operations with operational consistency and efficiency from on-premises datacenters to hybrid and multicloud environments. The value is even greater if such operational consistency and efficiency can be attained within the realm of current staff capabilities and ongoing skills shortages.

Getting Started with Multicloud Networking for Secure Access

1. **Deploy a secure SD-WAN.** As mentioned previously, the complexity of multicloud IT environments creates challenges for IT, as each cloud provider has a different management interface, APIs, and network constructs and services. Consequently, enterprise IT is compelled to apply multiple complicated and time-consuming approaches to ensure a consistent and secure user experience for each cloud service (e.g., AWS, Microsoft Azure and Office 365, Google, and Salesforce).

   Given the challenges, IT teams should deploy a simple secure SD-WAN architecture to simplify and automate branch connectivity to provide full-service branch offices with dynamic connectivity to accommodate a mobile workforce and increased adoption of SaaS and IaaS applications. This SD-WAN would provide the consistency to operate any cloud network through the same constructs that enterprise IT is used to.

   At the same time, this same SD-WAN will enable secure direct internet access and/or access through interconnect providers to cloud applications for increasingly distributed users. The inherent inefficiencies of an MPLS network, which backhauls internet traffic across branch office links to a corporate hub, add to cost and complexity while compromising performance and latency. Many organizations benefit significantly by installing a secondary link for direct internet access link at their branches to offload internet-bound traffic.

Getting Started with Multicloud Networking for Secure Access

1. Deploy a secure SD-WAN.
2. Optimize SD-WAN for SaaS and IaaS performance and security.
3. Apply cloud-based security for consistent secure access.
4. Consider colocation and SD-cloud interconnects.
5. Integrate policy management across SD-WAN datacenter cloud networks and campus/branch LAN.

2. **Optimize SD-WAN for SaaS and IaaS performance and security.** Cloud applications have become increasingly valuable to business operations at all locations. Today, for example, SaaS applications – such as Salesforce, Microsoft Office 365, and Webex – are integral to business operations and success. SD-WAN features should automatically and dynamically select the fastest, most reliable path to SaaS applications for enterprise users, leveraging real-time traffic steering to deliver an optimal user experience. Should an internet service issue cause connectivity to fall below acceptable levels, an SD-WAN offering must be able to automatically identify and select the next best path to maintain application performance.

   Similarly, SD-WAN should make connecting to IaaS environments such as AWS and Azure simple, automated, and secure. A centralized management console helps network and operations teams automate virtual private cloud connections to IaaS environments. Built-in intelligence helps meet automated connectivity requirements (relating to loss, latency, and jitter) and finds the optimal path to IaaS applications, ensuring service delivery and performance while monitoring hosting infrastructure for anomalies.

3. **Apply cloud-based security for consistent secure access.** As workloads and data move beyond the office and security moves to the cloud, the traditional perimeter-based security model is insufficient. In this context, a need arises for comprehensive access security spanning clouds, datacenters, branches, and mobile and remote home users to deliver secure access across the complete connectivity landscape. A single cloud-native platform can converge and consolidate networking and security capabilities that were traditionally delivered in multiple, siloed point products. The benefit is both comprehensive security and lower operating costs.

4. **Consider colocation and SD-cloud interconnects for aggregating and accelerating cloud connections.** SD-WAN allows distributed architectures to use colocation facilities to serve as regional hubs for branches. Colocation hubs streamline multicloud access by reducing the number of cloud egress points, regionalize security to reduce attack surfaces, and encourage network efficiency through simpler enforcement of end-user application policies.

   Moreover, as enterprises require a guaranteed underlay to connect to IaaS workloads and SaaS applications, SD-WAN should be capable of working with interconnect providers that provide MPLS-like reliability with the agility characteristic of software-defined networking. By leveraging cloud interconnects, IT teams can seamlessly connect enterprise SD-WAN sites to multiple, disparate clouds quickly, with the requisite performance and reliability.

5. **Integrate policy management across SD-WAN, datacenter networks, and campus/branch LAN.** Traditionally, network operators have been accustomed to managing operations in separate distinct domains. This model can introduce obstacles to delivering consistent services, slowing down the organization's ability to meet the changing business needs. In a multicloud world, the network needs to keep pace.

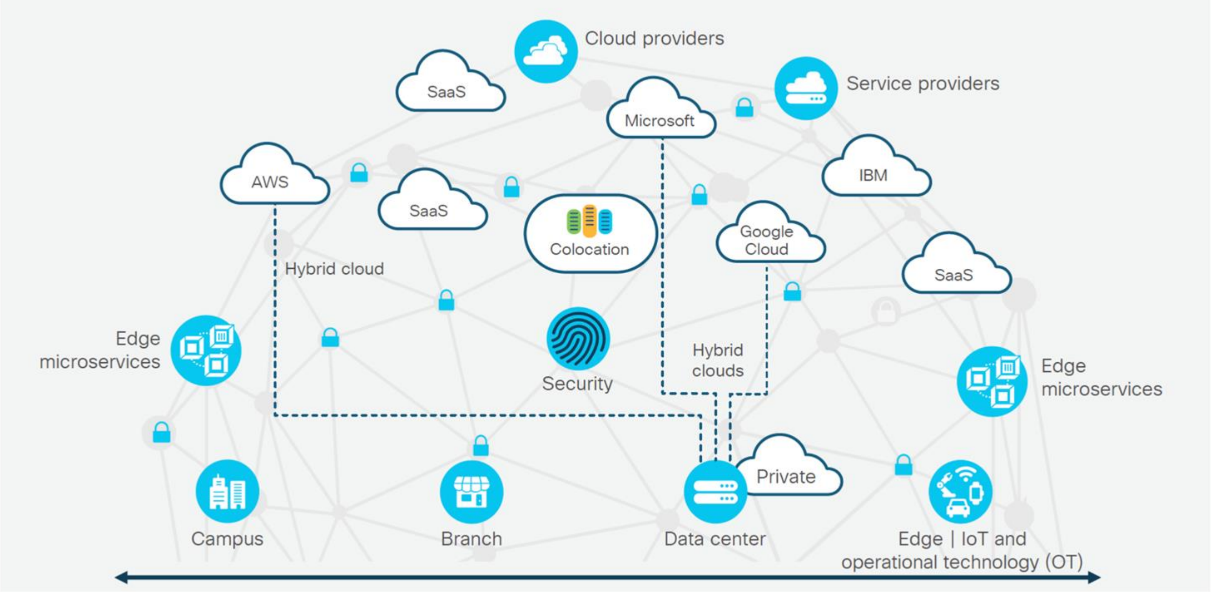
   As such, there is a growing requirement for automation of network operations consistently and securely across multiple domains, from user to workload, with end-to-end policy-based automation to achieve cross-network segmentation, application service levels, and access policies.

CISCO'S APPROACH TO MULTICLOUD NETWORK MODERNIZATION

Cisco has developed a networking approach to multicloud that is designed to enable the management of distributed applications as well as secure, reliable access to those applications. In both cases, intent-based networking is at the core of Cisco's approach toward providing the automation, insights, and security required in an increasingly complex multicloud environment (see Figure 5).

FIGURE 5

Cisco's Multicloud Networking: Secure Access to and Connectivity Between Diverse Application Services



Source: Cisco, 2020

Cisco's Multicloud Networking for Distributed Workloads

Cisco's networking approach to hybrid IT and multicloud helps cloud and network architects develop a consistent, simplified operating model that extends from on-premises datacenters to public cloud as well as to edge environments. It has been developed with a view toward simplifying the inherent complexities of multicloud, with inclusion of AI-assisted Day 2 network operations.

Cisco's multicloud networking for workloads portfolio includes management, network, security, and software components (see Figure 6).

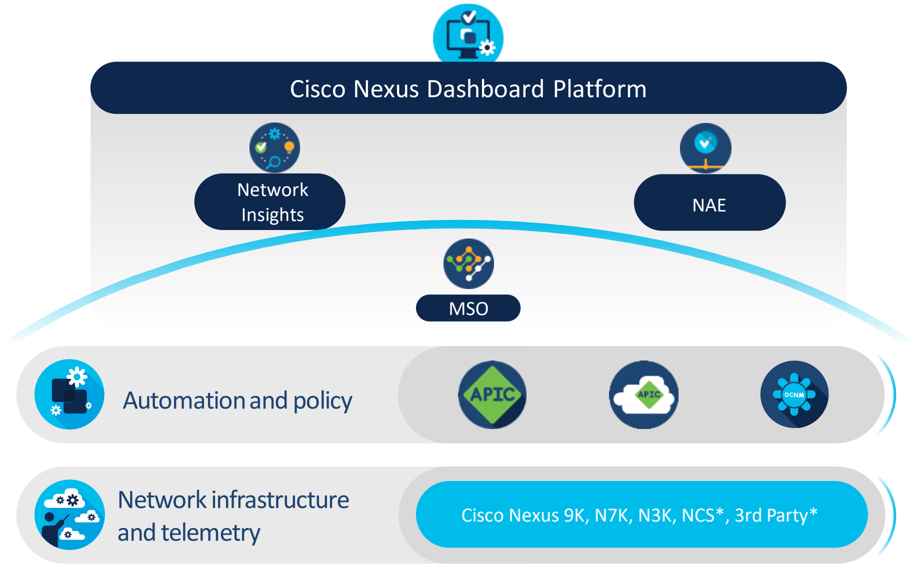
Unified Multicloud Network Operations

The **Cisco Nexus Dashboard Platform** provides for unified proactive operations and facilitates actionable insights across datacenter and multicloud networks. It helps reduce operational complexity by providing a uniform onboarding experience for datacenter sites and for Cisco and third-party operational services. Supported services include:

- **Cisco Multi-Site Orchestrator (MSO)** is a hybrid cloud tool designed to orchestrate Cisco ACI network policy and automation across on-premises, cloud, and edge.
- **Cisco Nexus Insights** provides monitoring and analysis in real time to identify anomalies, provide root cause analysis, assist with capacity planning, and accelerate troubleshooting.
- **Cisco Network Assurance Engine (NAE)** provides continuous analysis and verifies that the network state is consistent with the desired intent.

FIGURE 6

Cisco's Multicloud Networking Portfolio for Distributed Workloads


Cisco Nexus Dashboard Platform
Network Insights
NAE
MSO
Automation and policy
APIC
APIC
DCNM
Network infrastructure and telemetry
Cisco Nexus 9K, N7K, N3K, NCS*, 3rd Party*

*Roadmap

Source: Cisco, 2020

Network Automation for Multicloud Workloads

Cisco ACI is an intent-based, software-defined datacenter networking solution designed to support application agility and multicloud automation. Cisco ACI elements include:

- **Cisco Application Policy Infrastructure Controller (APIC)** is the ACI controller that enables network automation, programmability, and centralized management.
- **Cisco Cloud ACI** translates ACI policies to cloud-native constructs and services offered by cloud services providers such as AWS and Microsoft Azure.

Cisco Data Center Network Manager (DCNM) is a management platform for all Cisco NX-OS-enabled deployments, spanning new fabric architectures and storage networking across on-premises and cloud environments.

Securing the Multicloud Datacenter

Cisco Secure Data Center comprises Cisco ACI, Cisco Firepower Next-Generation Firewall, Cisco Stealthwatch, and Cisco Tetration that combine to help secure modern datacenter and cloud environments. Their combined capabilities include:

- Visibility across a datacenter and multicloud environment, including users, devices, networks, applications, workloads, and processes
- Segmentation to reduce the attack surface and prevent attackers from moving laterally, with granular control from the network to the individual application
- Threat protection to stop breaches and quickly detect, block, and respond to attacks before hackers can steal data or disrupt operations

Multicloud Networking for Access

Extending Enterprise Networks to SaaS and IaaS Environments

Cisco SD-WAN OnRamp is designed to provide consistent, advanced connectivity to one or more clouds (IaaS and SaaS) directly from the branch through internet, through interconnect providers, or even via colocation environments. SD-WAN provides users the same levels of security and application performance in the cloud as in on-premises environments. Furthermore:

- **Cisco SD-WAN Cloud OnRamp for IaaS** extends enterprise WAN to public clouds and integrates public cloud infrastructure into the SD-WAN fabric. Cloud OnRamp for IaaS for AWS and Azure support cloud-native constructs such as AWS Transit Gateway and Azure Virtual WAN, simplifying branch connectivity to applications hosted in public clouds through Cisco vManage's single pane of glass.
- **Cisco SD-WAN Cloud OnRamp for SaaS** uses real-time analytics to steer users over the best performing path for optimal application performance, supporting popular SaaS applications as well as direct internet access from branch sites and gateways at regional datacenters.
- **Cisco SD-WAN Cloud OnRamp for Colocation** aggregates branch offices in key regional colocations and allows IT operators to securely deploy multicloud connected network services such as firewalls and load balancers at the network edge for enhanced quality of service, simplified management, and increased security.
- Cisco SD-WAN, through interconnect providers, helps create a virtual dedicated interconnect from branches to the cloud to enhance the availability and reliability of connectivity to multiple cloud providers.

Securing Multicloud Access

Cisco combines networking and security capabilities to deliver full-stack multilayer security on the SD-WAN platform and in the cloud. The integrated SD-WAN security approach arms IT with threat defense wherever it is needed – for branches connecting to multiple SaaS or IaaS clouds, to datacenters, or on the internet. Cisco SD-WAN with Cisco Umbrella delivers a fully cloud-enabled Secure Access Service Edge (SASE) architecture.

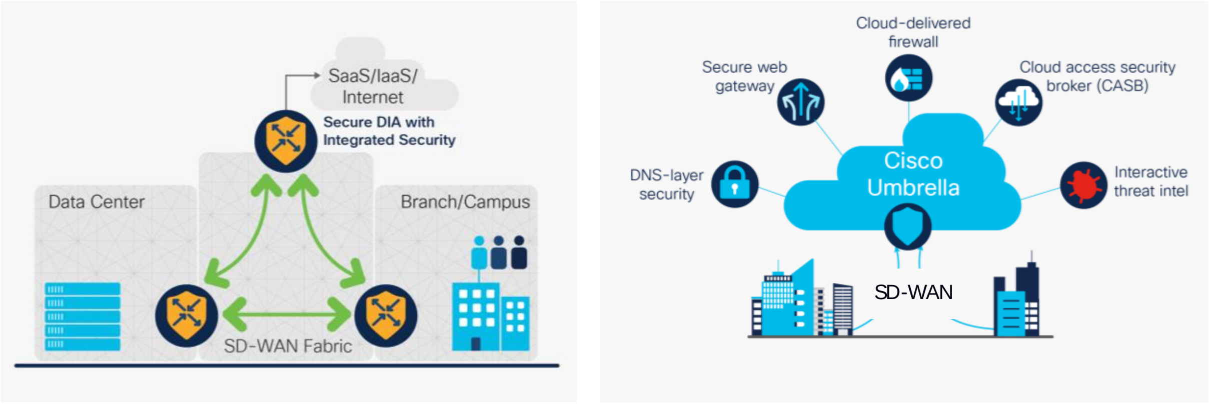
SD-WAN Security

Cisco SD-WAN provides threat protection and visibility to guard against web-based attacks. Delivered by means of the Cisco Umbrella cloud or through the built-in capability of the router, enterprises can gain visibility into and control over SaaS and internet applications (see Figure 7). Furthermore:

- **Cisco SD-WAN with Umbrella Cloud Security** provides a range of cloud-delivered security services such as DNS security, secure web gateway, firewall as a service, cloud access security broker (CASB) and zero-trust access. This offers protection against malicious web traffic and advanced attacks as well as automated setup from Cisco SD-WAN.
- **Cisco SD-WAN On-Premises Security** has embedded SSL decryption, enterprise firewall, intrusion prevention, URL filtering, and malware sandboxing that provide secure WAN access and meet onsite compliance demands.

FIGURE 7

Cisco SD-WAN and SASE Offer Secure Access Choices for Multicloud



Integrated On-Premises Security

Cloud Security and SASE

Source: Cisco, 2020

Cisco Cloud Security and SASE Framework

Cisco combines elements of SD-WAN networking, cloud-based security, and zero trust within a SASE framework.

- **Cisco Umbrella** is a cloud security service that unifies multiple security functions into a single service, helping businesses of all sizes embrace direct internet access (DIA), secure cloud applications, and extend protection to roaming users and branch offices.

- **Cisco Duo** is a user-centric zero-trust security platform for all users, all devices, and all applications. Duo's multifactor authentication (MFA) allows organizations to verify the identity of all users anywhere — before granting access to on-premises or cloud-based applications.

CHALLENGES/OPPORTUNITIES

The opportunity of modernizing and transforming enterprise networks for multicloud offers tremendous promise for customers and vendors alike. By modernizing the core-to-edge network to accommodate modern applications, hybrid IT, and multicloud, organizations are better able to provide the agility, flexibility, elastic scaling, reliability, and security required across a distributed application landscape. The benefits include faster time to market for products and services, improved business resilience, greater overall IT efficiencies, and faster provisioning, troubleshooting, and remediation, as well as better and more responsive application delivery to users, resulting in improved digital experiences.

For organizations seeking to modernize their networks for multicloud, key challenges include understanding their current and future application environments and alignment between IT and lines of business (LOBs) and developers.

For organizations seeking to modernize their networks for multicloud, a key challenge will be understanding their current and future application environments, including their plans to deploy applications in public clouds (both IaaS and SaaS). In addition, organizations will have to ensure that their IT operations, including their networking teams, are closely aligned with lines of business (LOBs) and developers to ensure that infrastructure is well aligned with strategic intent and business objectives as well as with developer and application requirements.

For Cisco, the principal challenges will be ensuring that its multicloud networking portfolio continues to adequately accommodate, support, and adapt to evolving hybrid and multicloud requirements, through both the depth of product features in areas such as rich telemetry and visibility and the breadth of capabilities across multiple public clouds.

Cisco's networking products and technologies must continue to innovate and provide support for connectivity between workloads and applications residing in on-premises and public cloud environments while mitigating the complexity of establishing and maintaining consistent network and security policies across multiple cloud providers. In addition, the portfolio at the edge, for SD-WAN, will have to continually evolve to keep pace with the needs of network operations teams and with cloud, application, and security requirements.

Finally, Cisco will have to ensure that it meets customers' needs better than its traditional and nontraditional competitors, including other datacenter networking SDN and IBN vendors as well as multicloud networking start-ups and providers of IaaS public cloud services.

CONCLUSION

The imperative of digital transformation and the growing embrace of multicloud are redrawing the boundaries of the datacenter and redefining not only what's required of a datacenter network but also network requirements at the edge, where applications are accessed and ultimately experienced. That's because applications and workloads, the digital lifeblood of modern organizations, are now distributed, residing not only in on-premises datacenters but also on multiple public clouds. This changes not only workload placement, but it also alters traffic flows and access requirements at the branch, campus, and even work-from-home (WFH) environments.

While managing and fully leveraging multicloud is a complex and daunting proposition, a modernized multicloud network built to accommodate and deliver distributed workloads can significantly reduce complexity and meaningfully contribute to the successful execution of multicloud strategies and digital transformation initiatives.

Intent-based networking, which involves the use of declarative intent and closed-loop network processes, can bring simplicity to this multicloud networking landscape, enabling network operators and cloud architects to manage networks proactively and maintain availability and reliability while defining and enforcing zero-trust network security across all places in the multicloud network.

If network and cloud architects develop and execute on a strategic road map for network infrastructure aligned with their application and multicloud strategies, they will be able to deliver the agility, flexibility, scalability, and security required to support and deliver distributed workloads, bringing unprecedented business value to their organizations.

If network and cloud architects develop and execute on a strategic road map for network infrastructure aligned with their application and multicloud strategies, they will be able to deliver the agility, flexibility, scalability, and security required to support and deliver distributed workloads, bringing unprecedented business value to their organizations.

MESSAGE FROM THE SPONSOR

Cisco's intent-based networking solutions help organizations realize their multicloud objectives, such as managing distributed applications across multiclouds and optimizing user experiences.

Cisco multicloud networking solutions are helping IT teams deliver connectivity, security and consistent policy across multiple clouds for ease of management and simplicity. With flexible consumption models, a broad and diverse ecosystem, and innovations to simplify operations and reduce risk, IT can extend the datacenter to anywhere the data lives and provide users secure access wherever they need it.

To learn more about Cisco's portfolio, please visit http://www.cisco.com/go/multicloudnetworking

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice