White Paper

Networking for the Distributed Multicloud Datacenter

Sponsored by: Cisco Systems

Brad Casemore
August 2019

IDC OPINION

As organizations continue to pursue digital transformation to become increasingly efficient and maintain a competitive advantage, they are adopting hybrid IT and multicloud as a means of expediting their journey. As a result, formerly centralized applications and workloads residing in on-premises enterprise datacenters are becoming distributed. This trend is redefining the parameters of the traditional datacenter and compelling organizations to modernize and extend their infrastructure to accommodate increasingly valuable distributed workloads.

In this new era, a mere extension of the datacenter network to the cloud is insufficient. The datacenter network must also be comprehensively modernized to feature declarative, intent-based management, resulting in simpler provisioning and more efficient day-to-day operations. There is also a need for pervasive real-time analytics and visibility that can help maintain business intent and expedite troubleshooting and remediation of network issues that could compromise or impair application performance. In addition, the modernized datacenter network must feature native integrations with cloud services such as AWS, Google Cloud Platform, and Microsoft Azure, mitigating the complexity of managing network and security policies that must extend to workloads in disparate public clouds.

This white paper examines how Cisco Systems is addressing the needs of the modern distributed datacenter network with a portfolio founded on the precepts of intent-based networking (IBN), featuring hardware performance commensurate with workload requirements and a partner ecosystem that supports a wide range of use cases and application environments.

SITUATION OVERVIEW

The emerging "modern datacenter" is a result of distributed applications and data that span both on-premises and off-premises facilities, driving a need for hybrid and multicloud architectures. This introduces organizational, operational, and technology challenges that must be addressed to achieve a positive outcome for the business. IT organizations need to adapt and shift their technology and operations to meet the increased application and network connectivity demands of the modern datacenter architecture.

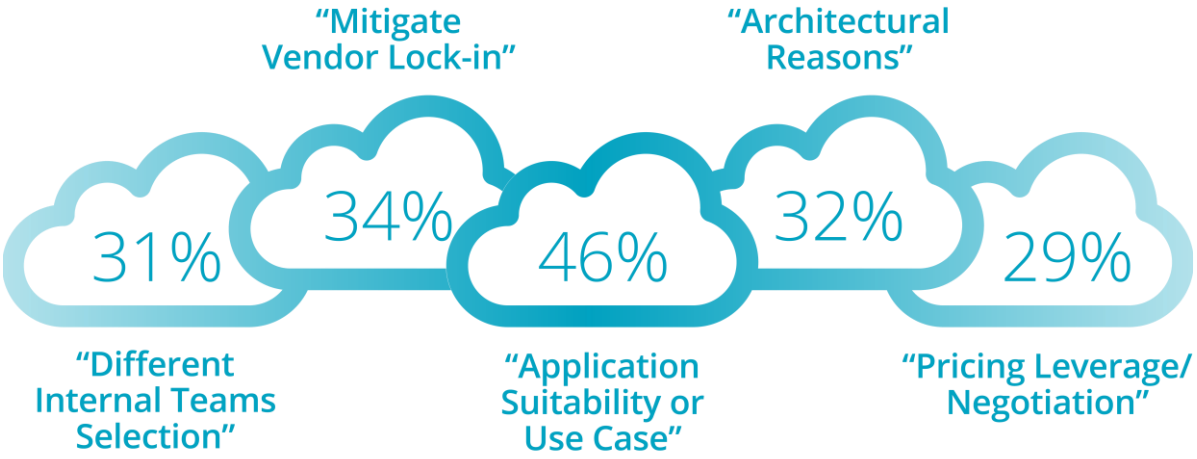
For most organizations seeking to modernize their datacenter infrastructure, the goal is a hybrid cloud or an IT-as-a-service (IaaS) model that supports self-service provisioning, enables real-time insights, and empowers agile, efficient, and flexible operations.

The cloud is a foundational means through which organizations achieve digital transformation, and investments in hybrid cloud and multicloud technologies are ramping accordingly. IDC estimates that by 2020, about 67% of enterprise IT infrastructure and software will be dedicated to cloud-based applications and services. Moreover, as of this year, more than 90% of enterprise respondents to IDC's worldwide *CloudView Survey* indicated that they would evolve their digital transformation strategies to encompass multicloud postures, which necessarily entail distributed workloads.

IDC's *IaaSView Survey* found that respondents had several reasons for adopting multicloud. About 46% of respondents cited application suitability or use case as their primary reason for adopting multicloud, while 34% cited the desire to mitigate cloud vendor lock-in. About 32% of respondents referenced architectural reasons, 31% explained that different internal teams had a need for different clouds, and 29% specified that multicloud conferred pricing leverage/negotiation (see Figure 1).

FIGURE 1

Reasons for Multicloud Adoption



n = 654

Base = respondents indicated that organizations use multiple primary public cloud IaaS providers

Source: IDC's *IaaSView Survey,* May 2018

Taken together, this data suggests that distributed workloads, allocated to on-premises datacenters as well as multiple public clouds, will become the norm rather than the exception.

With the ascent of multicloud, organizations are deploying applications in multiple public and private clouds while leaving legacy business applications in on-premises datacenters. Effectively, multicloud has become the new datacenter, with distributed applications and workloads spanning multiple datacenters. This trend will be accentuated and amplified by the rise of cloud-native microservices, yielding a growing number of business-critical applications developed with the express purpose and innate capability of migrating between cloud datacenters.

Consequently, it becomes critically important for enterprise IT to manage, optimize, and fully leverage multicloud environments in strategic service to business objectives. The inherently complex nature of distributed application environments will make this task exceedingly challenging. Nevertheless, the journey toward digital transformation will necessarily involve a multicloud world, and architecting infrastructure to accommodate and fully realize the flexibility of multicloud is essential to achieve the desired business benefits.

For successful deployment and delivery of multicloud applications, enterprises will require datacenter infrastructure that provides an all-encompassing architectural approach capable of addressing the evolution of applications, the proliferation of distributed workloads, and the resulting complexity of IT management and operations. At the same time, modernized datacenter infrastructure must be highly automated, enabling enterprise IT to evolve toward new IT consumption models, such as cloud and IT as a service, and establish the modern architectural foundation needed to reliably deliver and support the applications that are integral to business agility.

Given the context, the datacenter network is an integral element of a modernized infrastructure, and it must function as an enabler, rather than an inhibitor, of business agility and digital transformation strategies. That means it cannot be constrained by fine real estate or geography. Just as the parameters of the datacenter have been redrawn to accommodate cloud workloads, the datacenter network must also be redefined to deliver cloudlike agility, extensibility, flexibility, and elasticity. At the same time, given that all organizations, enterprises, and service providers must digitize and become more technologically proficient, there is also a pronounced need for a datacenter network that can be managed proactively rather than reactively.

As enterprises embrace multicloud, they should consider the following pertaining to their datacenter network:

- How well does your datacenter network support hybrid IT and multicloud?
- Is consistent network and security policy, including segmentation and microsegmentation, extensible from the datacenter to public clouds, with support for native API integration?
- How well does visibility inform simple declarative intent/policy and facilitate proactive network control and management, including assurance of intent/policy?
- How well does the network support multicloud application, workload, and data portability, as well as seamless connectivity between clouds?

Intent-based networking, in the on-premises datacenter and beyond, plays an important role in responding to the above-mentioned questions. Declarative intent and closed-loop network processes — including application policy and pervasive visibility through actionable analytics — work together to continually inform and maintain desired network state. Given the importance of policy in an age of data breaches and determined attacks, intent and policy assurance capabilities are an integral part of IBN. Through IBN, network operators are moving ineluctably toward increasingly autonomous and self-driving networks, which will be capable of proactive remediation and self-healing, maintaining availability and reliability while helping define and enforce zero-trust network security.

In conjunction with IBN, network analytics and real-time telemetry provide indispensable visibility and predictability, especially for modern applications and multicloud environments, reducing the mean time to detection (MTTD) and, consequently, the mean time to resolution (MTTR) associated with the resolution of service disruptions and outages. Ultimately, the value of AI- and machine learning (ML)-based visibility is that they enable operators to attain predictability and to proactively preclude and remove outages that could affect the availability and performance of applications and workloads.

In the context of digital transformation and clouds, agility and flexibility are understandably prized. Network automation tools enable the portability of applications and data between on-premises datacenters and clouds. Automation has been a key element of computing for many years, and the same benefits of agility and speed are required for multicloud and on-premises connectivity. Network administrators must adopt automation tools to replace manual processes, which are inherently inefficient and error prone, with automated processes that are far more efficient and verifiable. Network automation tools will evolve 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.

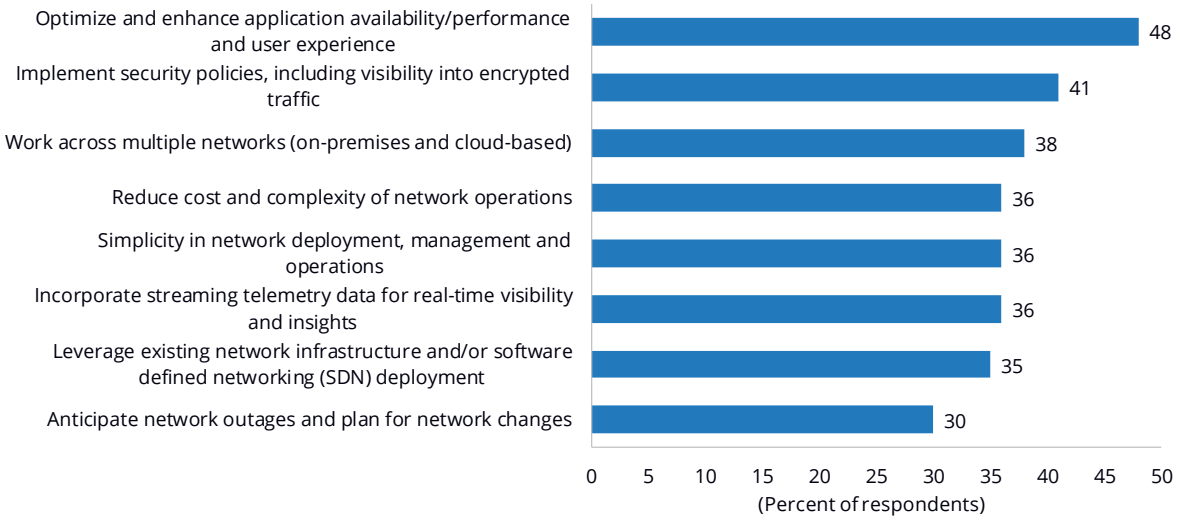
IDC has predicted that simple, declarative management models with enhanced verification capabilities and better closed-loop processes will be increasingly informed by streaming telemetry and pervasive network visibility, resulting in growing trust of automated network infrastructure through 2025. This trust will extend from provisioning to AI-assisted Day 2 network operations.

In the cloud era, enterprises also perceive considerable value in having AI-enabled network automation. In IDC's *IT Strategy and AI Adoption Survey,* conducted earlier this year, IDC found that optimizing and enhancing application availability/performance and user experience was cited as one of the most important aspects of an AI-enabled network automation solution. Also cited frequently was implementing security policies, including visibility into encrypted traffic. Another prominently cited consideration was the ability to work across multiple networks (on-premises and cloud based), followed by reducing the cost and complexity of network operations and bringing simplicity to network deployment, management, and operations. At a similar percentage was "incorporating streaming telemetry for real-time visibility and insights." All of these are important, and it isn't surprising that so many generated high percentages of responses (see Figure 2).

FIGURE 2

Top Priorities for AI-Enabled Network Automation

Q. What do you see as the most important aspects of an AI-enabled network automation solution? (Pick three.)



n = 301

Source: IDC's *IT Strategy and AI Adoption Survey,* February 2019

The previously mentioned capabilities can collectively help 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 available resources.

Indeed, as organizations grapple with the implications of digital transformation and the need to effectively harness hybrid IT and multicloud amid an ongoing skills shortage relative to new processes and technologies, they are demanding approaches that mitigate complexity and deliver simplicity. After all, complexity is the enemy of agility, which is paramount in the context of digital transformation.

Consequently, datacenter networks must be easier to provision, deploy, and manage. Automation, policy creation and modification, and programmability must become simpler.

Finally, even though software-defined networking (SDN) and intent-based networking have placed considerable emphasis on the value of software, hardware should not be considered an afterthought. Enterprise customers will still require network hardware that is reliable, flexible, and scalable and capable of providing the performance headroom needed by organizations in the cloud era.

All of these capabilities and features are required in a modern datacenter network. With the ascendancy of business-critical and distributed applications and workloads, the datacenter network, properly understood, is more important than ever.

CISCO'S APPROACH TO DATACENTER NETWORK MODERNIZATION

Cisco has developed a datacenter architecture that is attuned to the requirements of hybrid IT and multicloud, extending from on-premises datacenters to public as well as to edge environments, all developed with a view toward simplifying the inherent complexities of multicloud, including AI-assisted Day 2 network operations (see Figure 3).

Intent-based networking is at the core of Cisco's approach toward intelligent network automation. It captures business intent and uses analytics, machine learning, and automation to align the network continuously to changing business needs, which can include application service levels, security policies, regulatory compliance, and operational processes. There are four key elements to Cisco's intent-based networking:

- **Intent:** To identify the business or IT outcome that your organization needs
- **Translation:** Capture and translation of intent into policies that the network can act on
- **Activation:** Installation of these policies across the physical and virtual network infrastructure, using networkwide automation
- **Assurance:** Use of analytics and machine learning to continuously monitor and verify that the desired intent has been applied and the business outcome is being achieved

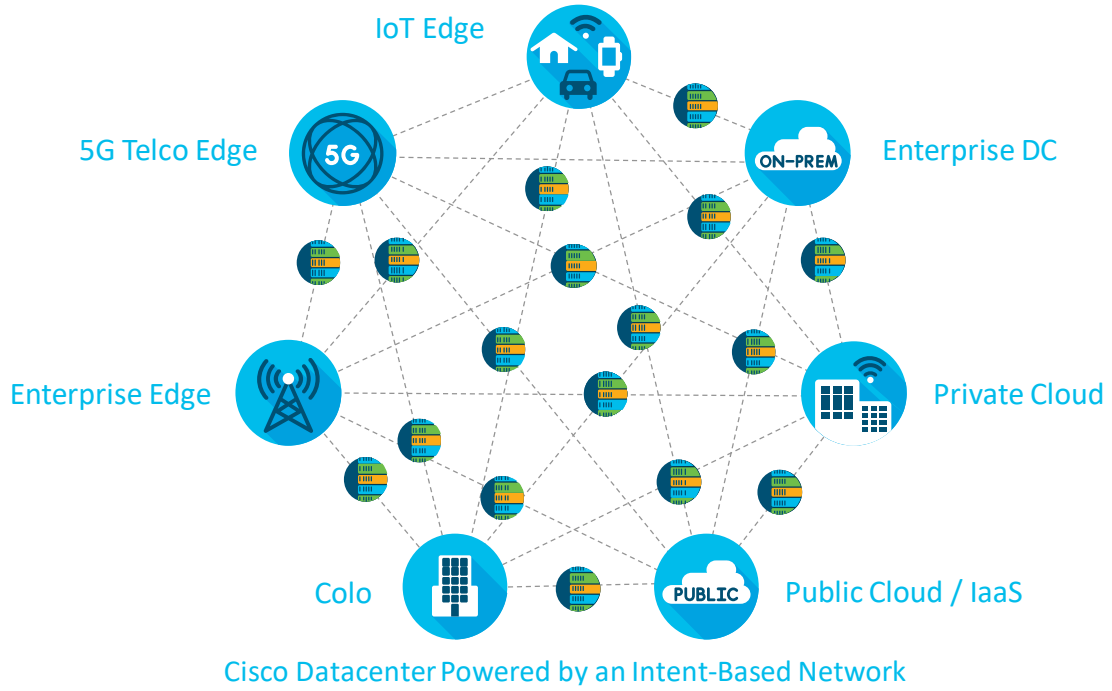
Cisco has developed a multicloud datacenter networking portfolio designed to address the need for a proactive networking environment that can keep pace with the demands of today's digitizing businesses.

Cisco's datacenter portfolio comprises three basic components:

- Network and policy infrastructure, including the Nexus 9000 Series of switches and support for all major hypervisor/virtual switches
- Management and automation with two offerings:
  - **Cisco Application Centric Infrastructure (ACI),** which delivers an automated, policy-based network fabric capable of translating declarative intent and activating and enforcing that intent throughout the network life cycle
  - **Data Center Networking Manager (DCNM),** a programmable solution for VXLAN-EVPN fabrics
- AI-assisted Day 2 operations tools including the Network Assurance extensions, which provide continuous datacenter network assurance and proactively verify network behavior to assure policy and compliance, and Network Insights extensions, which monitor network health and provide fast event correlation for troubleshooting

FIGURE 3

Cisco Datacenter Goes Anywhere Your Data Is



Source: Cisco, 2018

Network and Policy Infrastructure

On the hardware side, Cisco Nexus 9000 Series switches are powered by Cisco CloudScale network silicon and provide high-performance, low-latency, and power-efficient switches capable of operating in Cisco NX-OS software mode or in Cisco ACI mode.

Notably, Nexus 9000 Series switches, which support performance and density up to 400GbE per port, maintain the line rate performance of 400G per port while implementing features for network traffic management, such as policy, high-resolution telemetry and visibility, adaptive smart buffering for differentiated quality of service, and other capabilities that can directly benefit the business. With these capabilities, derived from Cisco's CloudScale network silicon, Nexus 9000 Series switches provide the foundation of a turnkey, fully automated, policy-based architecture with high visibility, for the design and management of datacenter fabrics.

As noted, the Nexus 9000 datacenter switches can provide customers with Ethernet performance at 400G line rate per port. While many customers might not have a current need for such performance, 400GbE will be increasingly required in aggregation areas of the network topology or to support applications in machine learning and deep learning in several data-intensive industries. As always, hardware performance must be at least commensurate with the needs of the application environments and workloads that it supports. Customers can choose to meet those needs with Cisco's custom network silicon (represented by Cisco's CloudScale network processors) or with a range of Ethernet merchant silicon, depending on use cases and requirements.

Management and Automation

ACI

Cisco ACI is an intent-based, software-defined datacenter networking offering designed to support application agility and datacenter automation. ACI Anywhere uses a consistent policy model to enable scalable multicloud networks while providing the flexibility to move applications seamlessly to any location or any cloud without compromising security or availability.

Cisco ACI offers several components to meet specific customer requirements:

- **The Cisco Application Policy Infrastructure Controller (APIC)** provides access to all ACI fabric information, helping enable network automation, programmability, and centralized management.
- **Cisco Cloud ACI** translates ACI policies to AWS' and Microsoft Azure's native constructs and services, providing abstractions that mitigate the complexity of having to work across discrete cloud environments and enabling consistent network and security policy across instances running on-premises and in public clouds. Consistent end-to-end network and security policy can also be extended across other places in the network, including the campus, branch, and 4G/5G and IoT edge environments.
- **Cisco Cloud First (CCF)** provides a seamless architectural approach for digital enterprises to expand their on-premises datacenter to the cloud. Cisco Cloud First allows IT teams to ensure technology and operational consistency between on-premises and cloud, and it also allows IT teams to begin modernizing their networks for the demands of on-premises cloud.
- **Cisco Virtual ACI** extends on-premises ACI networks into remote locations, bare metal clouds, colocation facilities, and brownfield environments without the need for hardware.
- **Cisco Multisite Orchestrator** enables customers to build globally scalable and available datacenter networks with seamless application mobility.
- **Cisco DC App Center** helps find useful applications and services, including AI-assisted Day 2 operations tools. The Cisco DC App Center facilitates collaboration with developers for publishing and monetization of applications using Cisco APIC.

DCNM

For simplification and automation of fabric design and ongoing management, Cisco Data Center Network Manager provides support for all NX-OS-based network deployments, including VXLAN-EVPN fabrics.

DCNM fully automates deployments of VXLAN fabrics with NX-OS. DCNM extends the automation, configuration, and centralized management of NX-OS by removing the complexities of the underlying protocols and increasing the speed and efficiency of deployments. Further:

- Fully automated life-cycle management (including design, implementation, and operation) of an integrated underlay and VXLAN overlay
- Full visibility into the underlay and VXLAN network, providing the ability to correlate underlay and overlay telemetry, thus improving troubleshooting

Assurance and Insights Applications

Cisco offers AI-assisted Day 2 operations tools that deliver a range of benefits to network operators. These include the ability to:

- Troubleshoot across the datacenter, with the ability to take proven, actionable steps with both ACI and NX-OS.
- Monitor network fabrics proactively to gain service-level agreement (SLA) insights, with views into latency and throughput.
- Continuously verify that business intent is being met, and guard against compliance and policy violations.
- Monitor higher-volume and business-critical traffic for efficient use of security, compliance, and application performance monitoring tools.

Cisco Network Assurance Engine (NAE), an app that is a key part of Cisco's IBN solution, is designed to bring a proactive operating model to datacenter networks. Built on Cisco's patented network verification technology, it mathematically verifies the entire network for correctness, giving operators confidence that their network is always operating consistent with intent.

Benefits of NAE include helping datacenter network operators meet the demands for agility, uptime, and security policy compliance. Using the technology, datacenter network operators can predict the impact of potential changes by proactively verifying correct measures and reducing the risk of network errors caused by operator error.

Securing the Datacenter

The Cisco Tetration platform has evolved steadily since its inception. It now implements a zero-trust model through segmentation as part of its ability to provide holistic workload protection across multicloud environments. The objective is to enable organizations to quickly identify security incidents, to contain lateral threat movement, and to reduce attack surfaces. As a platform, Tetration provides an infrastructure-agnostic approach that supports workloads that reside on-premises or in multiple public clouds, securing applications and data on-premises, in clouds, and across all types of infrastructure, including bare metal and virtualized environments.

When ACI and Tetration are used together, the former provides intent-based fabric automation and microsegmentation, whereas the latter delivers application segmentation, as well as policy-informing visibility and holistic workload protection. Tetration performs advanced analytics using an algorithmic approach that includes unsupervised machine learning techniques and behavioral analysis. The Tetration platform not only addresses the requirements of hybrid IT and multicloud — supporting on-premises workloads, private clouds, and multiple public clouds — but also provides customers with a range of form factors, including on-premises physical appliances, virtual appliances, and a software-as-a-service (SaaS) delivery option.

Through ACI and Tetration, customers can implement *defense-in-depth* microsegmentation and application segmentation across heterogeneous environments, infrastructure, and clouds, providing the ability to isolate applications and workloads in adherence to security requirements or compliance demands.

Cisco Portfolio

Cisco has developed its portfolio with the intent of helping customers benefit from technology targeted to meet a variety of use cases that can be integrated into a wide range of environments. The portfolio, as noted previously in this section, is diversified and designed to address the needs and preferences of enterprises of various services across every vertical market. Cisco also offers its datacenter networking products and support worldwide, supported by an ecosystem that includes a wide range of technology partners in datacenter infrastructure, cloud, and related technologies. This ecosystem and the technology partnerships it encompasses are supported by open and extensible APIs, as well by AppCenter, which offers a range of off-the-shelf and customizable integrations.

To ensure that organizations can find ways to deploy these technologies in ways that are amenable to them, Cisco offers flexible deployment options that emphasize simplicity and convenience, providing an architectural approach for digital enterprises to expand their datacenters securely to both multicloud and the intelligent edge.

Cisco has modern datacenter networking customers in a wide range of organizational sizes and industries. Two of the customers are the University of Utah and the TMX Group.

The University of Utah, emblematic of Cisco's customers in the education vertical, has had a Cisco datacenter network in production for approximately four years, helping the university transition to an app-centric approach to network architecture and operations spanning a multisite environment. In financial services, TMX Group has deployed Cisco's ACI to achieve automation, standardization, redundancy (for application and service availability), zero-trust security, and greater operational efficiency across multisite and multitenant application environments.

CHALLENGES/OPPORTUNITIES

The opportunity of modernizing and transforming the datacenter network offers tremendous promise for customers and vendors alike. By modernizing the datacenter network to accommodate modern applications, hybrid IT, and multicloud, organizations are better able to provide the agility, flexibility, elasticity, reliability, and security required across a distributed application landscape. The benefits include faster time to market for products and services, greater overall IT efficiencies, and faster provisioning, troubleshooting, and remediation.

For organizations seeking to modernize their datacenter networks, challenges will include understanding their current and future application environments, including their plans to deploy applications in public clouds. 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 closely aligned with strategic intent and objectives.

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

Cisco's datacenter networking products and technologies must not only provide support for connectivity to applications residing in clouds, but they also must mitigate the complexity of establishing and maintaining consistent network and security polices across a multicloud environment.

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 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 what's required of a datacenter network. That's because applications and workloads, the digital lifeblood of modern organizations, are now distributed, residing not only in the on-premises datacenters but also amid multiple public clouds.

While managing and fully leveraging multicloud is a complex and daunting proposition, a modernized datacenter network built to accommodate distributed workloads can significantly reduce that 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 distributed datacenter network, enabling network operators to manage their networks proactively and to maintain availability and reliability while defining and enforcing zero-trust network security across the full spectrum of multicloud environments.

Cisco's networking portfolio for the distributed datacenter features management and automation software, including the SDN solution Cisco Application Centric Infrastructure; assurance and insights applications for AI-assisted Day 2 operations, including Cisco Network Assurance Engine; and the Cisco Tetration platform focused on securing the datacenter. Cisco's network and policy infrastructure includes Nexus datacenter switches with NX-OS software, powered by both Cisco custom silicon and Ethernet merchant silicon. The portfolio is built to accommodate a broad range of use cases across a diverse array of application environments and infrastructure including public clouds.

If Cisco can successfully meet the challenges outlined in this white paper, it will be well placed to help its customers build modern datacenter networks that offer the agility, flexibility, programmability, scalability, and security required to support distributed workloads to bring unprecedented business value.

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