Enterprise Cloud: The Changing Nature of Data Center Networking

The Evolution of Enterprise IT

Introduction

The role of IT is fundamentally changing from a cost-efficient enablement technology to a more strategic element of the enterprise. For companies born before the digital era, IT is a key player on their path to digital transformation; for more recent businesses designed with technology at their core, IT represents a foundational pillar on top of which everything else is built.

With this shifting role, IT's decades-long emphasis on TCO is being eclipsed by a new-found focus on security and automation. Whether it's the continuous risks posed by a dynamic threat landscape, the threat of digital disruption, or an inability to keep pace with the latest trends, virtually every enterprise needs to be more agile. And, with the continued evolution of compute, storage, and applications, networks have been exposed as a bottleneck to change.

Put simply, enterprise IT is more critical than ever. The network itself represents both a risk and an opportunity as IT leaders plot out their evolutionary paths.

Shifting Priorities

As technology evolves, it drives changes in what companies expect from—and how they approach—IT. This, in turn, changes the way solutions are seen and evaluated. A recent PwC survey of enterprise IT leaders reveals their top priorities for data center networking solutions:

CIO	VP/Manager of IT
Security	Security
Automation and orchestration	Automation and orchestration
TCO savings	Technology innovation
Agility	TCO savings
Technology innovation	Agility

While the priorities vary slightly in order of importance depending on the respondent, the top five are remarkably similar between those responsible for setting overall IT direction and those accountable for delivering that strategy.

Major Insights into Networking Priorities

This research into IT leader priorities yielded a number of valuable insights into how data center networking solutions must evolve.

Insight #1: Security is more than just a CISO consideration

That security tops the list of enterprise priorities is not surprising. The industry has been rattled by a constant barrage of breaches and attacks, all of which seem to be increasing in both frequency and impact—to the point that security is now a board-level discussion at virtually every enterprise.

What is surprising is that it's not just security teams that consider effective defense a top priority. The PwC survey found that networking leaders consider security the top priority for their data center networking strategies. This signals an all-hands-on-deck mentality. Within IT, you're either part of the solution, or you're part of the problem.

> *"My entire team knows that security is incredibly important, and is a prime topic from our board."*

Security as a top-tier networking consideration has two major implications. First, the network must play an active role in surfacing threat intelligence. This puts a greater emphasis on streaming telemetry and integration with threat monitoring solutions. Second, the network must help isolate threats, using dynamic policy enforcement to quarantine bad actors.

Insight #2: Automation has overtaken TCO as a priority

Automation has overtaken TCO as a primary driver for enterprise IT, ranking just behind security for both CIOs and VPs of IT. However, it's worth noting that both agility and technology innovation rank in the top five for both sets of stakeholders.

Considered collectively, automation, agility, and innovation suggest that future benchmarks for data center networking will be more about IT's ability to keep pace than to contain costs. If the network interferes with digital transformation and new service delivery, then CIOs and their networking teams will find corporate life more difficult.

> *"A key area of focus in the future is the ability to configure the network with more intelligence, flexibility, and coordination between the security and network teams to* ***enable self-automated networks****."*

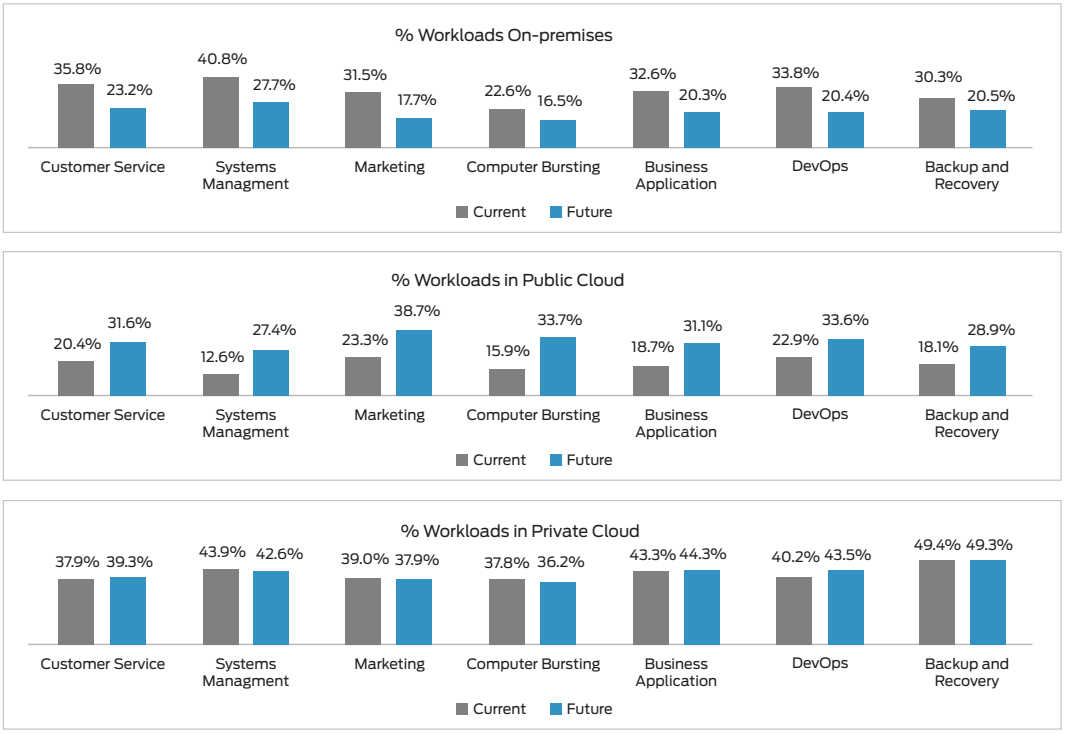
Leaders need to recognize the fact that increasing automation to realize more agile IT will require more than an investment in new technology. Enterprise change management will need to adapt as networks move from Information Technology Infrastructure Libraries (ITILs) to more agile processes. This will also trigger a need to educate and retrain personnel so that they are proficient across heterogeneous environments that make greater use of integrated tools and automated workflows.

Insight #3: Cloud is here and now

Cloud will be the context against which all of these changes play out. Companies will not simply retool their existing environments to create a more secure, more automated network; it will require a greater commitment than that. Enterprises not already in the cloud will have to move some or most of their workloads to either public or private clouds over the next three years.

As shown in Figure 1, PwC's research found that this movement to cloud is happening across all major classes of workloads, from customer service to broader business applications.

The move to cloud means that solving for security and automation requires that both the current state of IT and the likely hybrid and multicloud future state be considered. While solutions might be deployed narrowly to start, they will eventually need to be extended to service multidomain environments at some point in the future. Additionally, given the dynamic nature of cloud, these solutions must be able to support or even drive dynamic workload placement in a multicloud setting.



Source: PwC Enterprise Data Center Survey, 2017

Figure 1: Distributed workloads across clouds

Operating Within Constraints

While the PwC findings indicate that security and automation are top data center networking priorities, this does not mean that IT leaders can operate without constraints. Indeed, the Number 3 concern for CIOs remains total cost, while VPs of IT list TCO as priority Number 4.

The reality is that enterprise networks are expected to support their company's security and automation objectives without driving costs to unaffordable levels. This means that enterprise IT will have to carefully—and cost-effectively—navigate the transition from legacy to multicloud technologies, each of which will have different tools and processes.

The Rise of Cloud-Grade Networking

The changes in enterprise IT imperatives will force a rethinking of how networks are designed, built, and managed. With the cloud playing a prominent role, enterprises will evolve from primarily relying on enterprise-grade networks to building out cloud-grade networks.

Juniper Networks® Cloud-Grade Networking builds on carrier-grade reach and reliability, as well as enterprise-grade control and usability, bringing cloud-level agility and operational scale to networks everywhere. Cloud-Grade Networking essentially adds a new set of principles and capabilities to what the industry already knows, making networks more secure, highly automated, less capital-intensive, and ultimately better suited for innovation, both on and within the network.

Juniper's approach to Cloud-Grade Networking enhances security and drives deep automation, all with a budget friendly approach that includes the services and support to ensure that the enterprise—not just the network—completes the migration.

Complete End-to-End Integrated Security

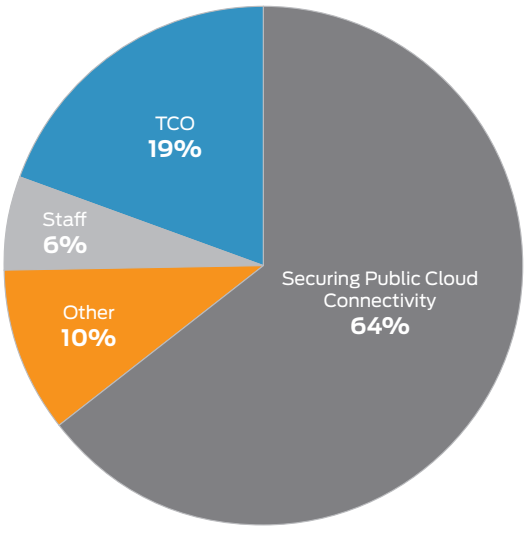
According to the PwC survey, the biggest pain point for enterprises is securely connecting their on-premises and private clouds to the public cloud.

Juniper's Software-Defined Secure Network (SDSN) framework, a unified cybersecurity platform powered by automation, machine learning, and real-time intelligence, helps enterprises overcome this challenge. SDSN creates a unified enforcement domain across all network assets, delivering consistent and automated defense across diverse environments in any cloud, and an open ecosystem for threat intelligence sharing and integration across any vendor.

Juniper's SDSN solution provides enterprises with:

- Unified security across multiple domains, ideal for multicloud architectures
- Automated policy enforcement and remediation on network devices
- Flexibility and lower cost through an open architecture that supports multivendor solutions

When asked to identify the biggest pain point in their enterprise data center, IT respondents to the survey ranked Securing Public Cloud Connectivity with on-premises and private cloud environments their top challenge.



Source: PwC Enterprise Data Center Survey, 2017

Figure 2: Secure public cloud connectivity is a top concern

Securing hybrid and multicloud environments

Using Juniper's SDSN approach, all Juniper Networks SRX Series Services Gateways and the vSRX Virtual Firewall connect to Juniper's cloud-based malware protection solution, Juniper Sky™ Advanced Threat Prevention, ensuring they are armed with the latest threat information to detect and block zero-day attacks. To support hybrid and multicloud deployments, vSRX Virtual Firewall is also available in AWS and Azure environments, allowing enterprises to connect their physical SRX Series firewalls in a private cloud to vSRX virtual firewalls in the public cloud via IPsec VPN secure data transport.

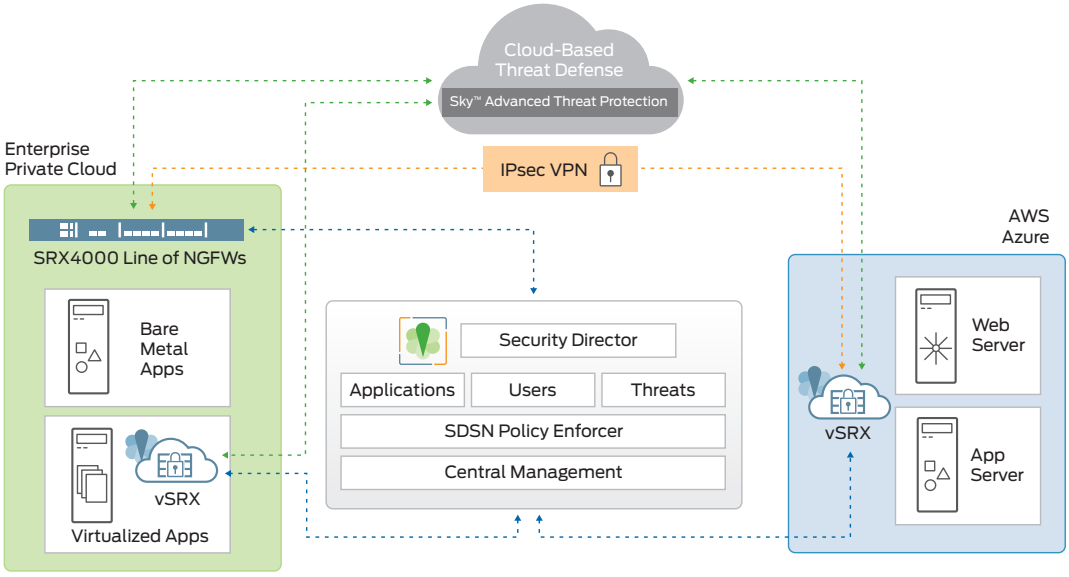


Figure 3: Secure connectivity between private and public cloud with Juniper SDSN

Automating security policy management

For many enterprises, the ability to manage policies in a multivendor network is a particular challenge. SDSN addresses that with Policy Enforcer, a component of Junos® Space Security Director. Policy Enforcer dynamically deploys policies to Juniper Networks QFX Series switches, EX Series Ethernet Switches, and SRX Series firewalls, as well as non-Juniper third-party switches (including Cisco), automating what has traditionally been a highly manual, labor-intensive task.

Fully Automated Self-Driving Networks

Juniper not only provides customers with comprehensive automation—one of the priorities identified by PwC for enterprises transitioning their data centers—but also offers machine learning and intent-based networking capabilities.

These automation and orchestration capabilities can turn any cloud-grade data center into a Self-Driving Network™ that combines telemetry, workflow automation, DevOps, and machine learning to create an infrastructure that is responsive, adaptive, and ultimately predictive.

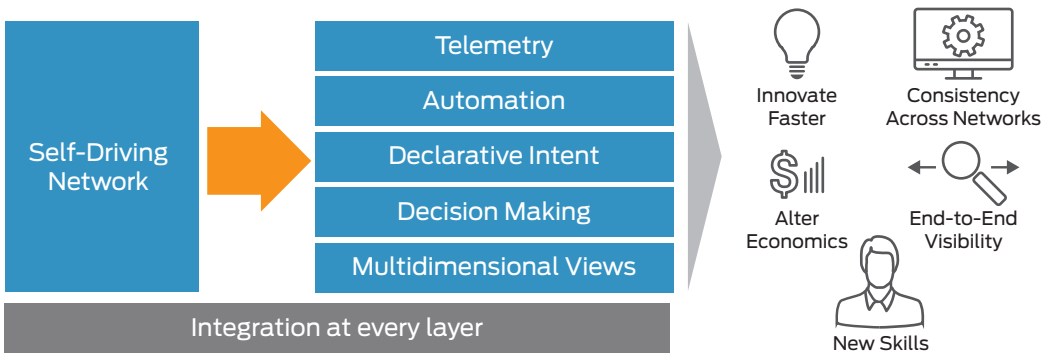


Figure 4: The Self-Driving Network runs on business intent

The Self-Driving Network can help you:

- Improve the economics of networking
- Deploy applications and services faster and with less effort
- Shift resources away from maintenance and towards value-enhancing activities

The Junos OS automation advantage

At the heart of Juniper's Self-Driving Network lies Junos OS, a cloud-grade operating system purpose-built for automation. The Junos operating system features a rich set of automation capabilities, ranging from real-time telemetry to programmable interfaces to native support for various automation frameworks, including Puppet, Chef, Ansible, and Salt.

Recently, an independent industry expert, Ivan Pepelnjak, compared different vendor network operating systems based on eight key automation parameters. Junos OS scored a full 100% on all eight features, far outpacing Cisco Nexus OS (50%), Arista EOS (75%), and Brocade VDX (37.5%), among others.

1 On-device APIs to read/write configuration and operational data ✓Juniper Networks: Pass	2 Structured operational data for easy programmatic analysis ✓Juniper Networks: Pass	3 Structured device configuration data for easy programmatic analysis ✓Juniper Networks: Pass	4 Atomic configuration changes to avoid partial updates ✓Juniper Networks: Pass
5 Configuration rollback to minimize risk ✓Juniper Networks: Pass	6 Full configuration replacement that makes templates easy to use ✓Juniper Networks: Pass	7 Configuration difference analysis to simplify manual approvals ✓Juniper Networks: Pass	8 Industry standard data models for configurations ✓Juniper Networks: Pass

Figure 5: Juniper scores 100% in 8 key parameters suggested by Ivan Pepelnjak
(Source: http://blog.ipspace.net/2016/10/network-automation-rfp-requirements.html)

Software-defined automation

The Self-Driving Network relies on intent rather than precise instructions provided through thousands of lines of complex configurations. In a software-defined world, the SDN controller acts as the point of control, translating intent into multivendor device primitives that drive the network. This architectural shift in how networks are managed is the major driver behind PwC's survey findings indicating that SDN is an essential part of enterprise IT's plans for the future.

Juniper integrates its Juniper Contrail® SDN controller with its fabric underlay to leverage the power of intent-based networking and SDN, delivering the world's most automated data center infrastructure. With Juniper Networks AppFormix®, Juniper adds a layer of application visibility to create a closed-loop system that can dynamically tune the infrastructure based on real-time conditions in and around the network.

With Juniper's data center fabrics such as Junos Fusion and Junos OS handling most of the routine, day-to-day operations, users can spend more time innovating and less time just keeping the lights on. In fact, Juniper customers report they have more time to spend on value-driving activities.

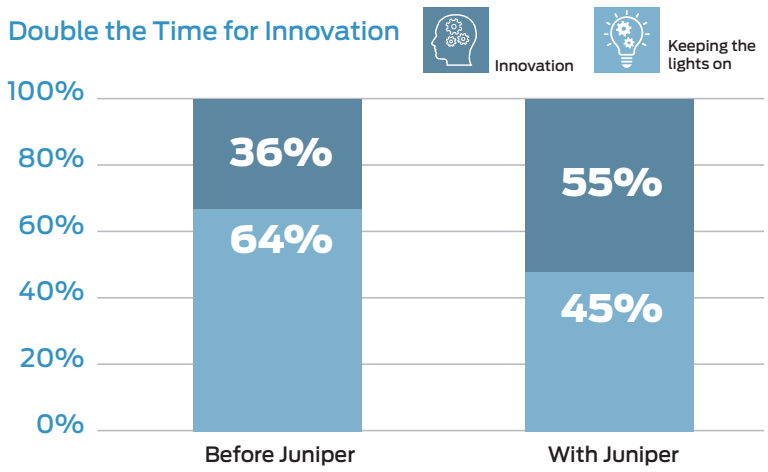


Figure 6: With Juniper, customers can spend more time on innovation

Conclusion: Navigating Change

It is clear: enterprises must adapt, both to keep pace with technological changes and to respond to increasingly difficult outside factors. Whether it's because of the rise of professional hackers or the threat of digital disruption, IT needs to be faster and nimbler.

This sets the scene for a profoundly difficult task:

- Enterprises must evolve.
- Threats are immediate, which means this evolution needs to happen quickly.
- The future will include the cloud, which means that change must also incorporate a new way of thinking about data center networking.
- While the future is in the cloud, the present is still steeped in legacy solutions.
- All of this change, from legacy solutions to the cloud, has to fit within the current budget.

The blunt truth is, this transition will be difficult. Not all companies will succeed. But uncertain times create opportunities for those who do.

Successful IT leaders will need to shift how they design, build, and maintain their data center networks. Specifically, they will:

- Embrace hybrid cloud architectures while preparing for the inevitable multicloud future
- Explicitly adopt a pervasive security posture that leverages the network as the foundation for detection and prevention
- Leverage automation and SDN as cost-effective ways to provide dynamic network control

Most people look at the changing landscape as a product of technology. They will continue to use current evaluation criteria to support their data center networking strategy under the premise that their existing technology philosophies will translate to future success.

But the challenges are not purely technical, and they will not be solved by simply deploying new hardware and software. Successfully migrating from where IT is today to where it needs to be tomorrow requires a journey. And it is that journey—not merely the networks—that requires architecting.

For more information, please visit the following links:

- Smart Cloud Integration: Let your network take you further
- Building a Self-Driving Network
- Software-Defined Secure Networking
- Proving the Business Value of Network Transformation – IDC White paper
- Juniper Data Center Blog
- Juniper's Cloud-Grade Networking Technology Vision

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

3200061-001-EN Oct 2017