WHITE PAPER

Empowering IT Innovations and Reducing Complexity with Unified Access

Sponsored by: Cisco Systems

Rohit Mehra

January 2013

EXECUTIVE SUMMARY

Businesses across a broad range of industries are increasingly dependent upon networked applications and communications. As these enterprises rely on their networks for customer and business processes and service delivery, the network has become a critical component for business enablement and growth. And as trends including the growth in mobile devices, bring your own device (BYOD), and Internet-enabled devices become increasingly prevalent, the importance of both the wired network and the wireless network increases. Unfortunately, wired networking equipment and wireless networking equipment have traditionally operated in separate realms, with inconsistent features, policies, tools, and management. This increases the network administrator's burden and drives up management costs and complexity.

Cisco has recently released a new set of unified networking and management platforms designed to bring consistency and continuity to all aspects of the campus network, from the wiring closet to WLAN controllers — and everything in between. Based on a new common ASIC that natively handles both wireless (LAN) traffic and wired (Ethernet) traffic, these products provide unified management and policies to the access network. Cisco's vision, driven by a realization that both aspects of the network — wired and wireless — are equally important, is seeing the enterprise campus being built on the foundation of "One Policy, One Management, and One Network."

By implementing such an architectural approach to unifying wired and wireless networks, IT and network managers can introduce new levels of efficiency, gain greater levels of manageability, and improve user experience. They can improve levels of performance and flexibility while improving their security and policy stance within the enterprise. Enabling greater levels of business innovation and growth while controlling costs, IT can demonstrate how it is driving innovative value-add to the business.

SITUATION OVERVIEW

Megatrends Impacting the Enterprise Network: Rise of the 3rd Platform

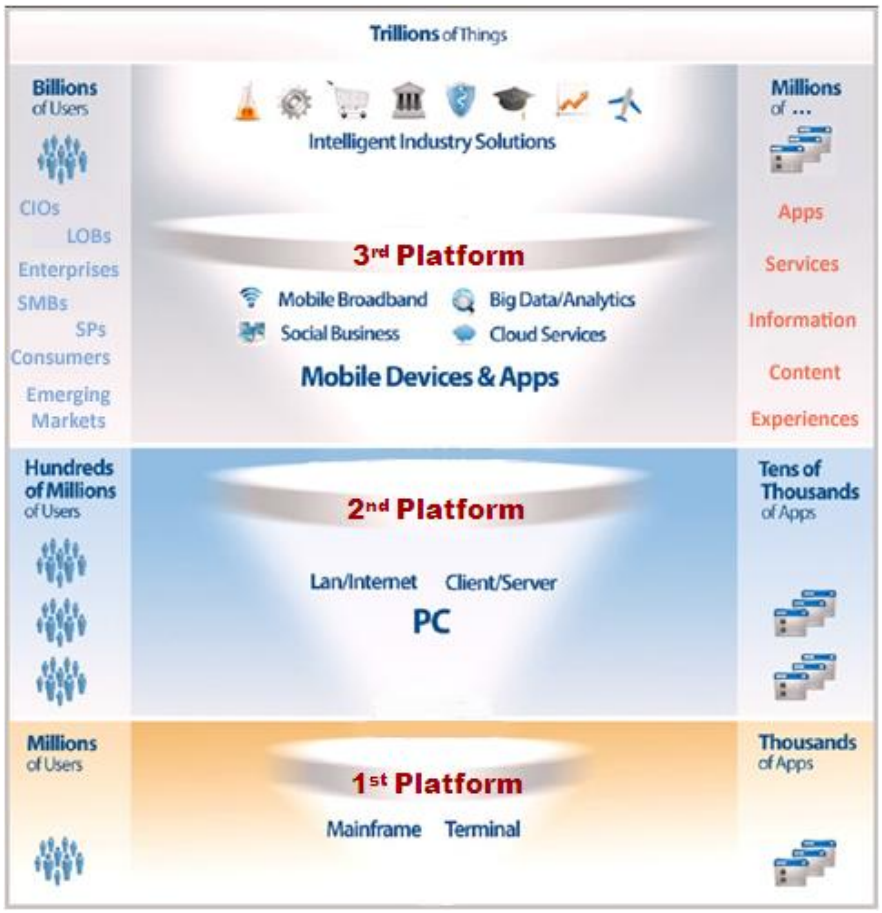
The world is changing rapidly, with new technology and business pressures on the network. IDC observes that we are currently in the midst of a one-in-a-generation shift

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

in computing and technology that IDC refers to as the rise of the "3rd Platform" (see Figure 1). The 1st Platform was the rise of computing in general and was characterized by mainframes accessed via terminals. The 2nd Platform was ushered in by the PC and the client/server paradigm and enabled greater personalization of computing and networked users accessing enterprise applications.

FIGURE 1

The Rise of the 3rd Platform



Source: IDC, 2013

Today, we are in the midst of the 3rd Platform, enabled by mobile broadband, social media, big data, and cloud services. In this era, users are accessing apps and services across a variety of enterprise IT assets, resources, and networks.

Key trends contributing to the 3rd Platform include an explosion in the number of devices, the majority of which are mobile devices and BYOD within the enterprise, and the transition toward the formation of what IDC calls an "Interactive Network of Things."

Mobility

Mobility is a cornerstone of the 3rd Platform paradigm and is changing the face of enterprise IT. While IDC research shows that PCs remain the most important single device for getting work done in the enterprise, information workers are increasingly relying upon mobile devices including laptops, smartphones, and tablets for work purposes. This trend, which is increasing the number of devices per enterprise employee, is adding to IT's security and management challenges. As the number of mobile devices grows, so do the demands on enterprise networks to support them. The amount of traffic rises as information workers depend, to a greater degree, on mobile devices accessing cloud-based services instead of local applications resident on their PC, and complexity rises as network administrators must manage increasingly complex wireless networks in addition to wired networks, which usually require separate sets of policies, security, and management.

Bring Your Own Device

A key consequence of the growth of mobile devices is the bring your own device trend, in which employees access enterprise networks, data, and applications using their own smart mobile devices — whether or not doing so is officially sanctioned by the organization. Surveys show this trend is on the rise: in one recent IDC study, 83% of enterprise IT managers indicated they expect tablets to become an integral part of how they conduct business, and in another recent study, 68% of information workers said they use personally owned devices to access business applications.

The BYOD trend places even greater pressures on the network. Not only do administrators need to accommodate an even greater amount of wireless traffic, but now they must enable employees to access corporate assets without compromising network or application security. One key approach to enabling this is the increasing deployment of cloud-based services and applications that enable secure enterprise application access. BYOD itself is not sufficient to enable enterprise mobility; it's the deployment and access of cloud-based enterprise applications and services that enable workers to conduct critical business functions over their mobile device. Another challenge comes from the rate of change that BYOD exacerbates within the enterprise — while laptops typically have a three-year life span, BYOD devices are frequently changed over an 18- to 24-month period, often driven by a technology refresh cycle or by the cellular plan being used with the device.

The Growing "Interactive Network of Things"

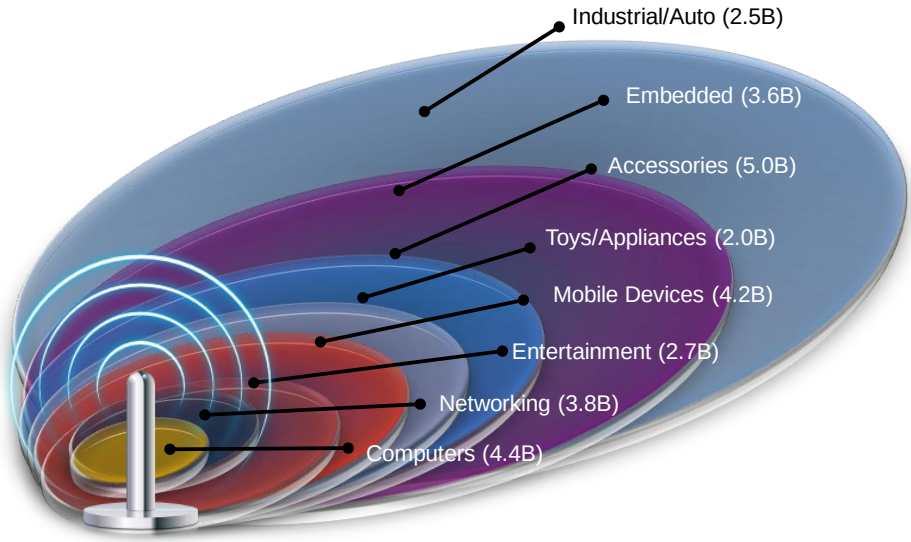
As the world becomes increasingly connected, and data and information become key drivers of the business, we are entering an era with a continued and rapid increase in the number of connected devices, all communicating with data, voice, or video — or a combination of all three.

From embedded systems to networked IT resources and industrial applications to machine-to-machine communications, this "Interactive Network of Things" is a network that is growing rapidly and expected to reach nearly 30 billion devices by the year 2020 (see Figure 2). Gone are the days when servers and PCs were the only connected devices to the enterprise network: today, smartphones, tablets, IP phones, videoconferencing and surveillance systems, RFID readers, point-of-sale devices,

building management and security systems, and other non-computing devices are adding traffic and management complexity, while also adding to the security challenges across wired and wireless networks.

FIGURE 2

The Interactive Network of Things, 2020: Nearly 30 Billion Devices Connected



Source: IDC, 2013

For another perspective on how this phenomenon of connected devices and applications will shape the networks of tomorrow for a cross section of industries, applications, and use cases, refer to Cisco's blog on the "Internet of Everything," which includes the following statement:

> It is important to note that while many of these new devices are connected wirelessly, many more use wired connections. It is easy to get caught up in the hype that the world is moving to wireless and that wireline networks no longer matter, but this is not true. A large number of connected PCs, servers, and other devices maintain wired connections to corporate networks, and network administrators must provide high quality of service for both wireline and wireless networks.

CIO Priorities

Today, CIOs have their own set of challenges. While they are concerned about supporting some of the trends outlined here, they must also focus on corporate goals including growing the business, acquiring new customers and maintaining customer loyalty, and reducing costs.

Growing the Business

As the world's economies continue their path toward recovery, businesses are making fundamental shifts in priorities. IDC has observed that many businesses have reached the trough of cost takeout and for the first time in several years have shifted their emphasis back to top-line revenue growth. This is particularly true in an uncertain macroeconomic environment, where many businesses are now looking for areas of strategic opportunity to position themselves to add capacity and take advantage of a rising economy as and when it happens.

Acquiring New Customers and Maintaining Customer Loyalty

To grow the business, enterprises must acquire new customers and, once they are acquired, retain them. And as we continue our evolution to an information- and service-based economy, IT in general and the network in particular play an increasingly critical role. Businesses are looking to differentiate themselves by creating innovative new experiences for customers, using not just traditional online delivery models but also fresh new mobile experiences for customers.

Reducing Costs

Even as companies renew their focus on top-line growth, the pressure to maintain or control costs remains paramount. Businesses pared costs back significantly during the recession by focusing on greater levels of efficiency and productivity. As businesses once again look toward strategic growth, many remain committed to maintaining a lean posture and leveraging existing resources rather than adding what they may consider to be new bloat. For IT organizations, this means finding ways to do more with less and extend the value of existing capital investments, while for network administrators, this means finding new ways to squeeze out even greater levels of management efficiency.

IT and Network Challenges

A more specific look at IT shows that key challenges further complicate the role of the CIO and IT staff. These challenges include disparate infrastructure management and insufficient policy and security capabilities that add up to overall operational complexity.

Disparate Infrastructure Management

IT organizations must often deal with heterogeneous environments, whether they are brought about deliberately through a best-of-breed approach to procurement, through successive waves of technology refreshes, or as the result of corporate mergers and acquisitions. Either way, these environments increase complexity for IT or network managers and administrators must coordinate separate sets of policies and separate management tools for different parts of their network.

Insufficient Policy and Security Capabilities

Organizations do not always have access to the appropriate policy and security capabilities to manage the challenges brought about by the mobile and BYOD environments and how they intersect with other IT infrastructure, including the wired network. This is particularly true in wireless networking (WLAN), which, being a shared medium, has not typically offered support for features such as quality of service (QoS) and traffic shaping as available on the wired side of the house.

Increase in Operational Complexity

As the number and types of supported devices increase in diversity, network managers find themselves dealing with greater levels of complexity managing overlay networks. While tools do exist to alleviate the operational burden of handling traffic across networks, routing traffic across wired networks for security or quality-of-service reasons, besides increasing operational complexity, generally adds to network overhead.

TAKING AN ARCHITECTURAL APPROACH TO UNIFIED ACCESS

Fortunately, organizations can take architectural approaches to their network, enabling them to address the pressures brought about by megatrends such as growth in mobile and BYOD, CIO challenges to achieve top-line growth while maintaining costs, and IT challenges to improve infrastructure management in the face of security and operational complexity. Namely, they can take a holistic, unified access approach to their wired and wireless networks.

Traditional overlay approaches to wireless networks deployed over wired network infrastructure have worked well so far, but the increased performance requirements of wireless networks, and the associated security and management issues arising from device proliferation, have resulted in increased complexity:

- A lack of seamlessness between the wired and wireless segments of the network
- A lack of management visibility into who and what is being managed — exacerbated as the number and types of mobile devices per user increase
- The tendency for IT to be perceived as the bottleneck, especially in terms of providing an enhanced user experience for access to network and IT applications (The burden of adapting the network to meet the organization's changing needs falls on IT, and IT is often the department that must say "no" to supporting new initiatives. This places IT in a difficult position, especially when C-level executives are the ones making the demands.)

Taking an architectural approach to unified access offers:

- A simpler, more efficient way to enforce the security and QoS policy — for both wired networks and wireless networks — at the network edge so that it is closer to the user and can be applied with greater levels of consistency
- Benefits to management from reduced operational complexity
- Networking innovation that results in greater empowerment for IT and true support to the business

Unified Wired-Wireless Network Access

As wireless networks in the enterprise have proliferated, the need to deploy these in conjunction with the underlying wired network infrastructure has always been there. Irrespective of the WLAN deployment type — autonomous, integrated, or controller based — the very aspect of wireless traffic traversing the enterprise wired infrastructure has always intrigued industry pundits, vendors, and customers looking for ways to improve network performance and related efficiencies. Higher-capacity wireless LANs further exacerbated this requirement, clearly pointing to the fact that the overlay network model would only work to a point. Eventually, the elimination of redundant network devices such as distributed controllers had to be the solution — and routing traffic from one medium over the other to centralized controllers would also have to give way to a solution that provides optimal traffic paths and shaping at the edge of the network. This gives rise to the notion of unified network access, where a single network device is capable of forwarding and handling all types of IP traffic, whether wired or wireless.

Common Security and QoS Policy Considerations

Here again, the device proliferation wave we are seeing as a result of the "consumerization of IT" has created awareness across IT and security managers for the need to bring together the security policy under a single umbrella, irrespective of what is being accessed in the enterprise — as well as how, where and, of course, by whom it is being accessed. These context-based security and QoS policy considerations are best appreciated when you can take a unified view of these capabilities across the enterprise.

Integrated Network Management for the Enterprise

Wired and wireless network management are indeed complex domains in their own right, leave aside trying to find suitable integration points. But even if some integration were to be achieved, IDC believes this is one area that would provide appropriate returns that could far outweigh the associated investments for enterprise IT. While there are several domain-specific areas of network and operational management (e.g., RF and AP management in WLANs), there are several areas of network management that can be integrated, providing a "single pane of glass" for the network manager. This can relate to reduced operational, troubleshooting, and training costs, which can be further leveraged in other areas such as converged databases for operational functions.

USING CISCO UNIFIED ACCESS SOLUTIONS TO ENABLE BUSINESS INITIATIVES

In 2013, Cisco announced the final pieces of a new Unified Access networking portfolio designed to reduce complexity from the network. With these products, Cisco has for the first time enabled its customers to implement true unified access across their entire network with consistent networkwide intelligence and operations.

The goal is to connect people, devices, and cloud services all using a single network architecture, extending from access and core switches to wireless controllers and APs. Cisco refers to its Unified Access vision as "One Policy, One Management, One Network."

One Policy

One Policy refers to the ability for customers to implement a single set of policies across the entire infrastructure, both wired and wireless. The primary product under the Cisco One Policy vision is the Cisco Identity Services Engine (ISE). ISE manages One Policy across wired, wireless, and VPN networks, enforcing compliance, enhancing infrastructure security, and streamlining service operations. Cisco ISE simplifies the design and implementation of policy and security. The highlights of ISE's latest enhancements include tighter integration with MDM solutions, and enabling policy management across the entire network from a single security platform.

Cisco ISE provides consistent security and quality-of-service control to wired and wireless networks from the network edge all the way through the enterprise campus and to the datacenter. It represents a single common place for policy enforcement, whereas in previous Cisco products, there would have been separate places for wired and wireless. It supports third-party MDM integration with a variety of endpoint devices, a real-time cloud-based device feed service to simplify the profiling process, and automatic policy compliance checks covering parameters such as pin lock, encryption, and jail broken status.

One Management

One Management signifies the ability for network administrators to manage their entire network using a single set of management tools and procedures. The primary product to support the Cisco One Management vision is Prime Infrastructure. Cisco Prime Infrastructure is a converged life-cycle management platform for wired and wireless that empowers IT departments to more effectively manage their networks and the services they deliver with comprehensive visibility, operational efficiency, and lower total cost of ownership (TCO). IT professionals can now manage their networks through unified and simplified Cisco Prime Infrastructure, which streamlines the ordering, deployment, and life-cycle management of converged wired and wireless networks.

Cisco Prime Infrastructure 2.0 provides a 360-degree experience to visibility and problem remediation for applications, services, and end users as well as support for automated best practices workflows to accelerate time to value while minimizing disruption and reducing operational overhead.

With its One Management approach, Cisco provides consistent networkwide intelligence and operations as well as networkwide visibility for faster troubleshooting. Since wireless traffic is translated into wired, all the tools and technologies that already exist to manage the Cisco wired network can now be used for wireless as well.

One Network

The "One Policy, One Management, One Network" vision is at the heart of Cisco's approach to Unified Access. The foundation of this vision, One Network, is based on these foundational concepts:

- **Converged wired and wireless infrastructure.** The products in Cisco's Unified Access portfolio have one physical infrastructure that is designed to increase business agility and scale and to deliver greater operational efficiencies than previous generations of Cisco offerings.

- **Consistent networkwide intelligence and operations.** The Unified Access products include a common set of network capabilities and context-aware intelligence for policy, visibility, analytics, and granular QoS. These are applied across the entire wired and wireless infrastructure and enable simplicity and a consistent user experience for network operators and users.

- **Integration with Cisco Open Networking Environment (ONE).** Cisco's Unified Access product portfolio provides industry's first common interfaces across wired and wireless to enable a blueprint for delivering a programmable data plane with Cisco OnePK for the enterprise campus and support for software-defined networking (SDN), further enhancing business agility.

Cisco has released two switch/controller products that fall under the One Network umbrella:

- **Cisco Catalyst 3850 access switch.** This is a converged wired/wireless access switch with an integrated WLAN controller. It supports up to 40Gbps of wireless data throughput per switch (up to 160Gbps in a 4-switch stack) and 480Gbps stacking bandwidth. It provides native conversion between wired and wireless traffic and comes with a variety of features including StackPower and granular QoS.

- **Cisco 5760 wireless controller.** This wireless controller supports a 60Gbps line rate (or 120Gbps if full duplex is counted). It is the first Cisco IOS-based wireless controller. It can be used in centralized or converged deployment modes and provides the same granular quality of service that was previously only available on Cisco wired products. It is also designed for resiliency and support for N+1 redundancy.

With the One Network approach, Cisco now has a single platform for both wired switches and wireless switches, including a common IOS across the 3850 switch and the 5760 wireless controller. These platforms use a new programmable Unified Access Data Plane (UADP) ASIC that is common to both products and provides common features, operations, and support for future features and intelligence.

Cisco One Network also provides multilevel wired and wireless QoS capabilities that allow bandwidth fair share policies across the entire network based on granular information such as access point, radio, SSID, user, and application.

Deployment Flexibility and Investment Protection

In addition to providing benefits to organizations today, deploying Cisco Unified Access enables organizations to protect their investments by introducing greater levels of flexibility and future proofing their network. Examples include:

- Support for current high-performance 802.11n access points while building an infrastructure that will support next-gen 802.11ac infrastructure with significantly higher capacity
- Wireless deployment options with integrated controller capability in the wired switch infrastructure, suited for enterprise branch and midmarket deployments
- Centrally deployed controller deployment options for larger networks without the need to route all traffic back to the wireless controller
- Converged access with built-in LAN switching and wireless controller functionality delivered by the same chip, direct wireless termination on the access switch, and native wireless to wired traffic convergence at the network edge

Benefits

Customers taking a holistic, end-to-end architectural approach to their network can realize a number of benefits including:

- **Manageability.** Having a single platform for wired and wireless and a common IOS and set of features and policies across both aspects of the network reduces management complexity. Simpler single-pane-of-glass management tools reduce the management burden. Networkwide visibility enables faster troubleshooting, and since wireless traffic is now converted to wired, all the tools and technologies on the wired side can be used for wireless as well.
- **Enhanced user/customer experience.** Consistent security and QoS control irrespective of whether the customer is accessing the wired or the wireless network streamlines the user experience. Policy and QoS can be applied to both wired and wireless — at the network edge and through the enterprise backbone.
- **Flexibility.** Organizations can scale more rapidly, taking advantage of the common infrastructure, and can more easily incorporate network components. This enables greater business agility and provides future investment protection.
- **Performance.** With the distributed wired/wireless data plane, all wireless data traffic no longer needs to be tunneled back to a centralized control point.
- **Security policy that is pervasive across the infrastructure.** Organizations can benefit from implementing a single security policy but also achieve greater levels of resiliency with fast stateful recovery (e.g., by rolling over to a second stateful switch for both wired traffic and wireless traffic).

OPPORTUNITIES/CHALLENGES

IDC sees a number of opportunities and challenges for Cisco as it brings its Unified Access offerings to market.

Opportunities include:

- **For customers: Accelerating business innovation and growth.** Customers that rearchitect their networks to take full advantage of these features can achieve the benefits of improved business agility, driven by new innovative user services enabled by networkwide intelligence, scale, faster service rollout, and better change management. With a common IOS throughout the network, from core routers to campus switches, enterprises can better scale to meet BYOD and cloud demands, execute faster service rollouts, and conduct more efficient change management.

- **For customers: Driving greater business efficiencies.** Greater business efficiencies can be delivered by improved simplicity and the ability to implement converged infrastructures, greater network consistency, better data analytics, the introduction of open and programmable interfaces, and smarter network designs and operations.

- **For enterprise IT: Demonstrating innovative value-add to the organization.** This is an opportunity for IT to "look good" and to demonstrate its value to the business by adding much-needed intelligence and demonstrating that it is taking the long view of the enterprise network.

- **For Cisco: Establishing new differentiated, value-added offerings.** The network equipment market is highly competitive, with vendors competing on innovative new technologies and providing solutions that reduce companies' total cost of ownership and drive attractive return on investment (ROI). By addressing the needs of customers, Cisco is again pushing the boundaries of its current offerings and is working to differentiate itself from other vendors in the market.

Challenges include:

- **Demonstrating the ROI of the solution.** Implementing these new technologies will require new capital expenditures for many enterprises and may have an effect on ongoing operational expenditures as well as network managers learn the intricacies of bringing the wireless and wired worlds closer together like never before. Cisco will have to demonstrate how the benefits and savings to the broader business will yield an attractive ROI to make the change worthwhile.

- **Dealing with cultural change.** With separate wired and wireless networks operating for years, at times with distinct IT teams, a cultural change across the networking industry will be necessary. Ethernet and IP-savvy network managers must learn the nuances of RF and security policy, while RF and security policy managers must learn the nuances of the Ethernet and IP. This will eventually reflect in an IT organization that needs to be seen as a partner to the business — not as the bottleneck or simply the people that say no**.**

CONCLUSION

The network is a critical component of all business functions and is a key enabler for customer acquisition and service delivery. With the proliferation of mobile devices, BYOD, and network-attached devices, enterprise networks must handle greater levels of complexity. But inconsistent management tools and policies across the wired and wireless segments of the network increase the burden for network managers and drive up management costs and complexity.

With its new Unified Access networking products, Cisco allows enterprises to take an architectural approach to wired and wireless networks. With its "One Policy, One Management, One Network" approach, Cisco is providing switches and wireless controllers built on a common ASIC platform and running a common IOS. Network administrators can operate a common set of network policies and use a single set of management tools for their entire network.

An architectural approach to unifying wired and wireless networks can help businesses realize greater levels of manageability, enhanced user/customer experience, greater levels of flexibility and performance, and improvements in security and policy. Businesses can accelerate their rates of business innovation and growth while driving greater levels of business efficiencies. It's a win for the enterprise and a win for IT.