



White Paper

Cisco ONE Sets Stage for Software-Defined Future in the Access Network

Sponsored by: Cisco

Rohit Mehra
January 2018

Elaina Stergiades

IDC OPINION

As enterprises start to realize the value of digital transformation (DX), enterprise IT increasingly has the charter to help understand and address key application requirements and IT infrastructure initiatives that will drive better business outcomes. Further, the profile of enterprise IT as an enabler of DX requires it to move toward more flexible and dynamic approaches to IT and network infrastructure, providing a foundation that leads to improved application and user experience. Increased network intelligence and automation can now be considered foundational to new IT initiatives that increasingly are delivering actionable business insights right at the access layer of the network.

SITUATION OVERVIEW

Trends Across the Network

Increased Prevalence of Wireless Connectivity

The enterprise network is becoming mission critical across organizations. Enterprises demand higher performance of their wired LANs and wireless LANs (WLANs). WLAN has transitioned from a secondary or niche network access method in many organizations to the primary network for mission-critical devices and applications. IDC's end-user surveys show a high majority of respondents confirming that most of their network traffic traverses the WLAN.

However, the wired LAN remains necessary for many use cases. Consequently, as wired and wireless networks in today's digital paradigm need consistent policy, security, and QoS settings, IDC recommends that organizations evaluate the potential benefits of unified wired and wireless access. In IDC's *Campus Network Innovation Survey*, adopters of unified wired and wireless LAN strategies cite improved security visibility (71.1%) and ability to enforce consistent application policy (65.7%) as top benefits, alongside operational efficiency benefits.

The Rise of Software-Defined Access Architectures

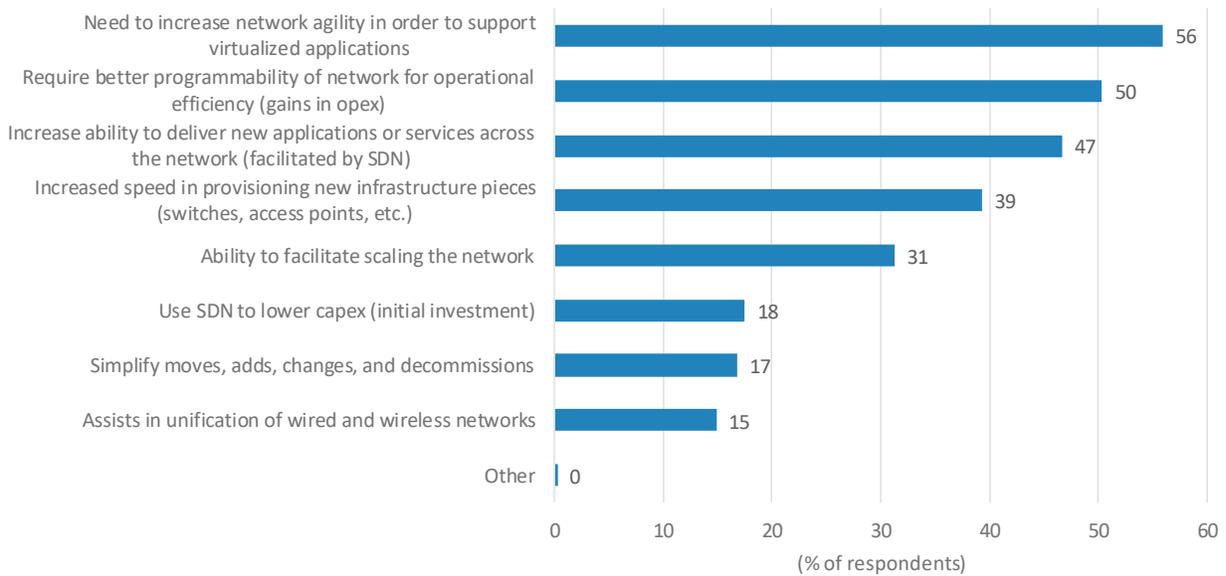
The increased mission criticality and complexity of enterprise access networks in tandem with the network's role in digital transformation are bringing forth an era where network automation will leap from enterprise IT wish lists to requirement lists. A major factor contributing to this is the rise of software-defined architectures for the access network. From integration of a diverse set of homegrown proprietary tools to best-of-breed access solutions, the architectural changes that made waves through the datacenter just a few years ago are starting to make waves in the enterprise. According to IDC's

2017 SDN Survey (Datacenter and Enterprise Campus), nearly half of the respondents had deployed some form of software-defined access, 44.3% were using software-defined topologies for their wired network, and 44.0% were doing so for their wireless network (n = 328). Network agility and programmability (which enables automation) were cited as the top reasons for implementing a software-defined access solution in the enterprise campus (see Figure 1).

FIGURE 1

Agility, Programmability, and Service Delivery Lead Among Drivers for Software-Defined Access in the Enterprise Campus

Q. Which of the following factors is the primary motivation for considering or implementing SDN in the campus?



n = 328

Base = respondents who are using or planned to use SDN in the campus

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

Data is weighted by GDP by country.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

Source: IDC's SDN Survey (Datacenter and Enterprise Campus), 2017

The Business Value of Network Agility

Network agility, programmability, and automation have already demonstrated operational benefits in early adopter organizations. In *The Business Value of Creating Digital-Ready Networks with Cisco DNA Solutions* (IDC white paper #US41903216, November 2016), IDC's Business Value practice used its standard methodologies to study the Cisco DNA use cases of eight early adopters of a software-defined access solution. IDC found promising quantifiable benefits within these organizations:

- On average, enterprise IT spent 18% less time "keeping the lights on," meaning that time spent on day-to-day configuration, maintenance, and troubleshooting tasks could be redirected to more strategic initiatives with the lines of business.
- In turn, IT departments found their networking teams' efficiency grew by 28%.
- Organizations were able to more quickly deploy both physical and virtual network infrastructure. On average, organizations reduced time to service anywhere from 18% to 44%, depending on the type of infrastructure.

Increased capabilities in network analytics, AI, and machine learning are expected to bring greater levels of programmability and automation across the network. Innovations in software-defined access will bring this programmability and automation to the enterprise campus network.

Growing Scale of Connected Devices

The scale by which the number of network-connected devices and applications has grown is tremendous. For example, according to *Worldwide Business Use Smartphone Forecast Update, 2017-2021* (IDC #US43066817, September 2017), from 2016 to 2021, the number of enterprise-owned smartphones will increase from 1.47 billion to 1.73 billion. This does not include "BYO" devices; IDC surveys have found that around half of enterprises have formal BYOD policies. Compounding the scale of network-connected enterprise devices is the burgeoning Internet of Things (IoT) phenomenon. According to *Worldwide Internet of Things Forecast, 2017-2021* (IDC #US43087717, September 2017), the global install base of IoT devices will grow from just under 700 million in 2016 to over 36 billion in 2021. The vast majority of these devices will be connected in the enterprise.

Network as a Service

In recent years, the adoption of cloud-managed network infrastructure has borne "network as a service" (NaaS) subscription models, where on-premise network equipment such as Ethernet switches and wireless access points are managed through the cloud to implement an up-to-date network infrastructure that can support a digital enterprise. This not only adds flexible agility to scale the network – up or down – as demands fluctuate but also plays well to many enterprise IT departments' increased reliance on opex-oriented pay-as-you-go financing models.

Trends Illuminate New Network Demands

As enterprises of all sizes are considering their plans for digital transformation to take advantage of innovative technologies that can enable strategic business initiatives from the back office to the point of customer engagement, they must rethink their network architectures to ensure the agility that DX requires. Primarily, enterprises need to ensure that their networks are ready for:

- **Automation.** Today's network is mission critical to business objectives and, as a result, supports unprecedented numbers of applications and devices, including Internet of Things devices. Enterprise IT need not be bogged down by manual tasks when there are more strategic, forward-looking initiatives that it can be enabling, including partnering with the lines of business for next-generation product and service delivery.
- **The evolving security landscape.** Once upon a time, enterprise networks were insular entities around which a perimeter could be set to create a "walled garden" of threat protection. Today, the proliferation of outside devices, web-accessed public cloud applications, and autonomous IoT devices requires a 360-degree reexamination of network security. This merits a discussion of the value of tighter integration of security tools within the network infrastructure.
- **Making actionable use of network insights and analytics.** Recent advances in networking technology have made it easier to use the network as a sensor to collect data about user, device, and application behavior. Enterprises are unlocking a wave of new opportunities around using data to fine-tune customer engagement over the network as well as baseline the network's "normal" regarding performance and security. Network analytics promote the business value of the network by helping ensure uptime and providing an actionable platform for customer insights.
- **An intelligent and intuitive network.** In sum, the previous three points, enabled by a growing software-defined orientation, create a next-generation enterprise network. Automation, analytics, and end-to-end, tightly integrated "foundational" security create a dynamic network with unprecedented intelligence and intuitiveness. This opens the door for enterprise IT to spend its time on more transformational tasks and begins the network down a path toward self-optimization and self-healing.

To take advantage of innovations ranging from mobility to IoT to Big Data-enabled SaaS applications, the network must be refreshed with these factors top of mind. Software-based network architectures, such as software-defined access, are driving new innovations in deploying and managing networks that allow for the flexibility and agility needed in the digital era. As well, what should not be overlooked is how flexibility in the way that network infrastructure software is licensed can be a major component to providing the agility needed for dynamic network environments in the digital age.

How Software Drives Enterprise Network Business Outcomes

As digital disruption has shaken up the competitive environment within many industries, organizations are looking to digitally transform business processes and employee and customer engagement and painlessly unlock the power of data. A next-generation network with software-driven agility and subscription-based flexibility is a major pillar of enabling digital transformation to achieve business outcomes.

To help enterprises navigate these trends, network infrastructure vendors must offer comprehensive and agile software platforms for managing an end-to-end network from datacenter to edge, including management and visibility of the full network security stack. Two trends are especially driving network infrastructure innovation: a rapid expansion in software functionality and the increased availability of software-defined access solutions. IDC defines software-defined access as the ability to provide

consistent and secure access (to any user, endpoint device, or application) through software-defined data plane and control plane abstraction to enterprise campus and branch network infrastructure, such as Layers 2 and 3 Ethernet switching, WLAN access points and control infrastructure, and access routers. While many software-defined topologies heavily leverage open source controllers and standardized hardware such as white-box switching, software-defined access infrastructures can also be designed from proprietary network infrastructure. Software-defined access can enable multiple benefits, including the following:

- **Network assurance.** A critical element of software-defined access infrastructure to consider is its ability to collect network data and convert that into actionable analytics to ensure continuous uptime. A network analytics dashboard should provide key data points on network health, where the network needs to be further optimized, and what needs immediate troubleshooting.
- **Encrypted traffic analytics.** The availability of encrypted traffic analytics is another crucial point to consider. A new security breach technique is for bad actors to use encryption to disguise malware as legitimate network traffic. Network infrastructure with foundational security and analytics capabilities can thwart this by analyzing net flow metadata without decrypting traffic flows, further preventing costly data breaches and ensuring network uptime.

Rationalized Subscription Software Suite Emergence

The move to a software-defined access orientation and foundational security for enterprise network infrastructure can be complex, especially against the backdrop of the growth of enterprise mobility, public cloud SaaS, and increasingly skillful security breaches. The possibility of having to purchase and implement multiple software modules can be overwhelming for enterprise IT departments that are preoccupied with other DX-related initiatives. Enterprises seeking software-defined access solutions are wise to consider a rationalized subscription software suite with embedded support.

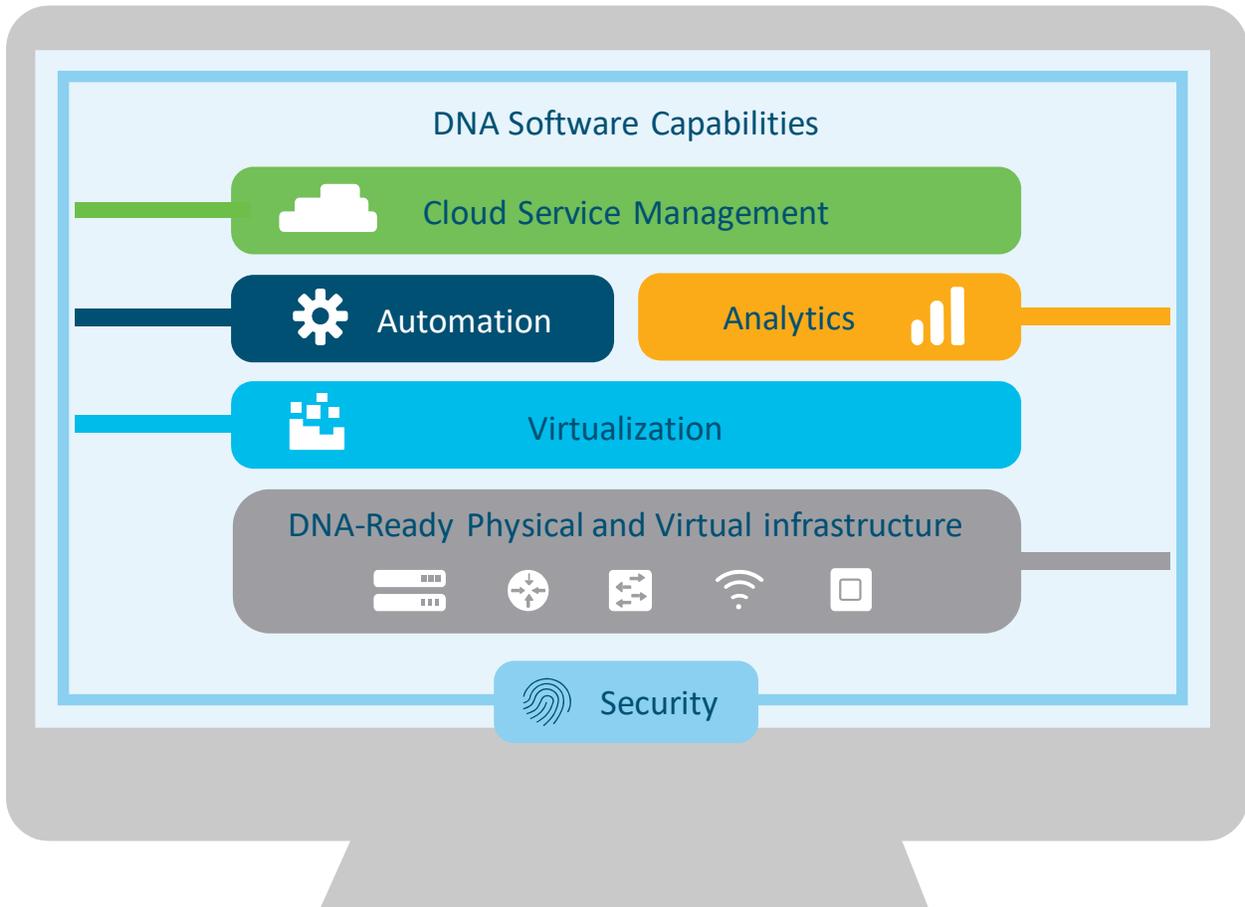
CISCO DNA OVERVIEW

Cisco Digital Network Architecture (DNA) is an open and extensible software-driven architecture (see Figure 2). Leveraging the benefits of programmability, automation, and analytics, Cisco DNA can benefit IT staff by allowing them to spend less time on manual, repetitive, and reactive network configuration and troubleshooting tasks, instead focusing on proactive, future value-creating strategic initiatives that better align the network with business outcomes.

Cisco DNA is a forerunner of Cisco's new intent-based networking approach that leverages Big Data and analytics and machine learning capabilities alongside automation and programmability to achieve greater levels of business agility on the network, reducing the amount of time it takes to optimize the network to an organization's fast-changing business needs. Cisco DNA is managed through the centralized DNA Center management console.

FIGURE 2

Cisco Digital Network Architecture



Source: Cisco, 2017

To accommodate trends in enterprise networks and their impact on customer requirements, Cisco has recently updated its Cisco ONE portfolio by introducing subscription offers for Access – switching and wireless. Cisco ONE Software is a valuable and flexible way to buy software for datacenter, WAN, and access domains. Cisco ONE streamlines the process of purchasing, managing, and upgrading network infrastructure software.

Cisco offers several options for deploying DNA in the access network. Subscriptions are offered on three- and five-year terms, with three tiers of licensing offers available: Cisco ONE Advantage, DNA Advantage, DNA Essentials.

Figure 3 illustrates the structure of software offers for switching.

Cisco ONE Advantage for Switching

Cisco ONE Advantage is the optimal choice for enabling all Cisco DNA use cases. Included in Cisco ONE Advantage for switching is (see Figure 3):

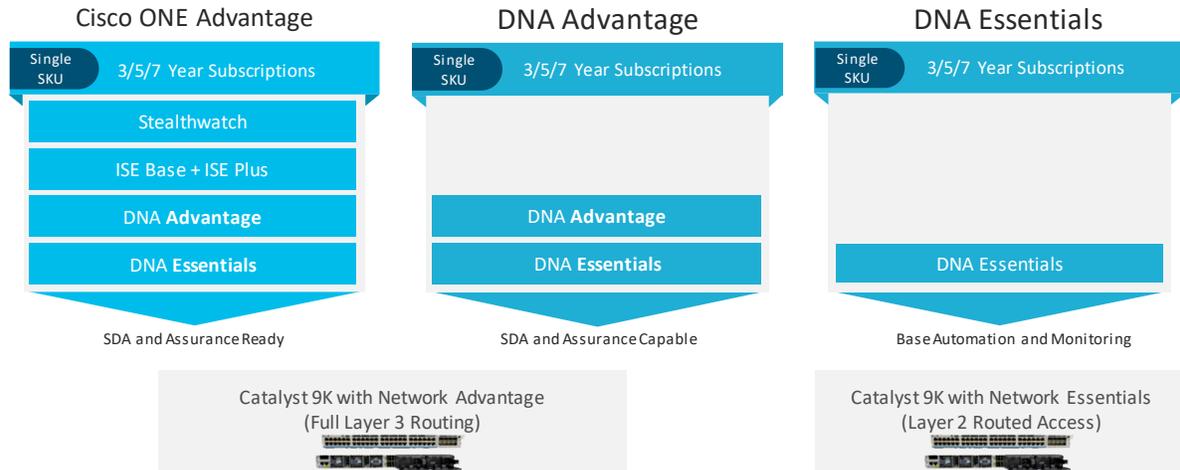
- **Stealthwatch.** Cisco Stealthwatch collects and analyzes end-to-end network data to give networks of all sizes comprehensive internal visibility and protection. It helps security operations teams gain real-time situational awareness of all users, devices, and traffic on the extended network so they can quickly and effectively respond to threats.
- **ISE Base + ISE Plus.** Cisco Identity Services Engine (ISE) allows network administrators to see and control users and devices connecting to the corporate network from a central location. With Cisco ONE Advantage, customers receive not only the functionality of Cisco ISE Base (AAA, 802.1x, guest management, MACsec link encryption, TrustSec, and ISE APIs) but also the BYOD, profiling and feed services, EPS, Cisco pxGrid, and location services integration of the ISE Plus add-on.
- **DNA Advantage.** DNA Advantage includes all the functionality of DNA Essentials while adding Software-Defined Access (SDA), additional security and IoT functionality (Encrypted Traffic Analytics), mDNS GW, assurance and analytics, and telemetry and visibility (ERSPAN, AVC, NBAR2).
- **DNA Essentials.** DNA Essentials refers to the basic monitoring capabilities and automation and element management functionality within DNA. DNA Essentials includes support for containers, Python, EEM, ANI, Flexible NetFlow, and Wireshark.
- **Cisco ONE Subscriptions.** Offers are available on Cisco Catalyst 3000, 4000, and 6000 Series as well as on recently announced Cisco Catalyst 9000 Series switches.
- **Software Support.** This includes TAC, knowledge base access, and software downloads.

For customers that would prefer to take a gradual approach to a software-defined architecture, DNA Advantage and DNA Essentials can be purchased as standalone modules.

Overall, Cisco ONE operationalizes the benefits of Cisco DNA and SD-Access in an easily consumable and manageable way that is modular and flexible for the dynamic needs of the digital enterprise.

FIGURE 3

Cisco ONE Switching Overview



Software Support included in all subscriptions

Source: Cisco, 2018

Cisco ONE Advantage for Wireless

Like with the switching offer, Cisco ONE Advantage is the optimal choice in wireless for enabling all Cisco DNA use cases. Included in Cisco ONE Advantage for wireless is (see Figure 4):

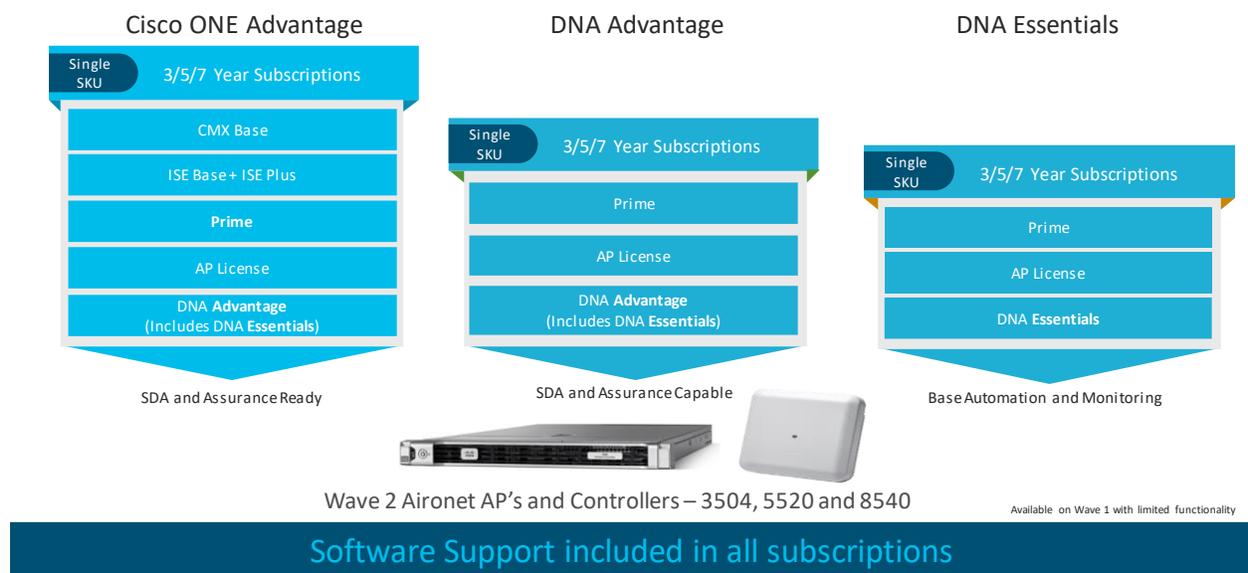
- **CMX Base.** This is the core module for all location services and applications and can be leveraged for advanced analytics and vertical-specific use cases and applications.
- **ISE Base + ISE Plus.** Cisco Identity Services Engine allows network administrators to see and control users and devices connecting to the corporate network from a central location. With Cisco ONE Advantage, customers receive not only the functionality of Cisco ISE Base (AAA, 802.1x, guest management, MACsec link encryption, TrustSec, and ISE APIs) but also the BYOD, profiling and feed services, EPS, Cisco pxGrid, and location services integration of the ISE Plus add-on.
- **AP license.** The AP license includes flexible network segmentation, optimized RF, enhanced security, and other advanced features that ensure reduced network downtime.
- **Cisco Prime Infrastructure.** Prime provides core management for wireless and wired networks, connecting the network to the device, user, and application – end to end and all in one. It delivers increased application visibility, assurance, single-pane management, and simplified deployment of Cisco value-added features.
- **DNA Advantage.** DNA Advantage includes all the functionality of DNA Essentials while adding Software-Defined Access, additional security and IoT functionality (Encrypted Traffic Analytics), mDNS GW, assurance and analytics, and telemetry and visibility (ERSPAN, AVC, NBAR2).

- **DNA Essentials.** DNA Essentials refers to the basic monitoring capabilities and automation and element management functionality within DNA. DNA Essentials includes support for containers, Python, EEM, ANI, Flexible NetFlow, and Wireshark.
- **Underlying Hardware.** This includes Wave 2 Aironet access points and controllers: 3504, 5520, and 8540.
- **Software Support.** This includes TAC, knowledge base access, and software downloads.

For customers that would prefer to take a gradual approach to a software-defined architecture, DNA Advantage and DNA Essentials can be purchased as standalone modules.

FIGURE 4

Cisco ONE Wireless Overview



Source: Cisco, 2018

CHALLENGES/OPPORTUNITIES

With any major technology investment, especially one that turns traditional networking paradigms on their heads, IT decision makers must carefully consider challenges against opportunities. One challenge that may arise is the perception that Cisco historically has not been a first mover on software-defined access architectures. Until very recently, Cisco was known as a traditional hardware and perpetual license-oriented vendor. Moreover, even with its recent forays into software-defined access architectures, Cisco has mostly retained a proprietary approach to software-defined architectures, thereby taking a different approach than many of the more open source early movers in this arena. Some stakeholders may advocate for a more open solution, and proponents of Cisco ONE and SDA will need to be prepared with a business value case.

On the other hand, IDC believes there is exciting potential for customers and for Cisco in this transition. For Cisco, Cisco ONE, DNA, and SDA make a bold statement signifying Cisco's stated goal of transitioning from a hardware company to a hardware- and software-enabled technology company. Customers that may have previously felt torn between their long-standing successful relationships with Cisco and embracing the software-defined era now have compelling options for embracing software-defined architectures with a Cisco flavor. IDC believes this transition will help recast Cisco as a key player in the enterprise infrastructure software space and bolster Cisco's leadership as a forward-looking network infrastructure provider for the digital age.

CONCLUSION

The increased affinity of cloud applications and deployments in conjunction with other DX initiatives has brought to light an increased need for more dynamic and flexible IT/network architectures and "as a service" business and consumption models. When required at scale, they also lead to new levels of automation, which ultimately benefits IT as it alleviates the need for routine and mundane provisioning and troubleshooting tasks. This significant market shift is transformational, especially as it relates to software becoming intrinsically more valuable in its own right and providing the flexibility needed in an adaptable IT environment that is secure and scalable. Within this context, IDC recommends that IT and network practitioners take a closer look at software licensing and consumption models for their enterprisewide infrastructure requirements, such as the Cisco ONE example illustrated in this white paper.

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

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2018 IDC. Reproduction without written permission is completely forbidden.

