THE COMPLETE GUIDE TO THE

CISCO DNA CENTER

AN END-TO-END RESOURCE FOR EVERYTHING CISCO DNA CENTER RELATED

CISCO ACADIA TECHNOLOGY GROUP

TABLE OF CONTENTS

TABLE OF CONTENTS CONT.

I. INTRODUCTION

What is DNA and Why Does Your Firm Need It Right Now?

DNA, or Digital Network Architecture, is an open and protractible software-driven engineering platform allowing conversion of your business with real-time features to facilitate faster innovation, simplify your operations and reduce your compliance risk.

Benefits:

- DNA simplifies enterprise network management over a centralized dashboard.
- Networks deploy in minutes instead of days, using perceptive workflows. Cisco DNA Center makes it foolproof to design, provision and employ policy across your network.
- Lower your costs by increasing network uptime through policy-driven provisioning and channeled remediation. This lets you reduce the time spent managing even the simplest network operations.
- Enables “hyper-microsegmentation” making your network vastly more secure. Every communication session can be put into its own isolated segment.

Intent-Based Networking for Enterprises

Gartner, Inc., a global research and advisory firm providing insights, advice, and tools for leaders in IT, reported that by 2020 more than 1,000 enterprise-level companies will be using intent-based networking (IBN) systems. This is the most exciting advancement in networking since ethernet switching. Firms can centrally manage network operations and deploy crucial security protocols to keep all data safe in our cybercrime climate.

So, what is Intent-Based Networking, and what does it mean to you? Simply put, IBN streamlines network management at scale, securing continuous and uninterrupted alignment with your business goals. The traditional networks companies relied upon had to be manually configured to their individual need-based specifications. IBN eliminates that hassle and time spent on manual setups by taking your firm's defined business intent and uses instead network automation and intent-based policies to make those tailored changes. This allows for network changes at scale, and contextual analysis before, during and after any network changes and guarantees the network is performing to its fullest capacity.

IBN is based on three primary principles:

Translation: IBN translates the network operator's intent, letting them express what they need to the network to do instead of how the network will do it.

Activation: This function takes your intent and construes it into policies. The activation function installs these policies across your network through automation.

Assurance: Your intent is continuously validated and verified that it is being honored by the network. This is rapidly moving toward a closed loop system. A closed loop system automatically regulates to a desired state without human interaction. As compared to open loop systems that requirement manual input.

IBN is based on three primary principles:

Benefits:

Think about all of the different domains that network infrastructures are managed: wired, wireless, campus and branch sites, WAN, LAN, data centers, and, of course, the almighty cloud. And that's not including clients and their applications that have their own operational procedures. One of the great benefits of IBN is that it accommodates all of these domains by translating intent-based policies across your firm's entire network. And once those policies are embedded, continuous assurance checks are performed across those domains to confirm compliance. IBN works seamlessly and flawlessly across your domains. But this is just one of the perks. Other benefits include:

Increased agility: Organizational needs are fluid, no matter your industry. With IBN, enterprises can quickly respond to meet changing directives with very little to no manual intervention. Onboard your new applications quickly and painlessly, with the comforting knowledge that ongoing assurance guarantees that the integrity of your network changes remains intact. IBN's automation and standardization supports a higher scale than traditional networking.

Improved efficiency: When network operators are able to reduce the time they spend on network design, testing, troubleshooting and repair, that means a cut in operating expense costs.

Better compliance and security: The major drawback for manual network configurations is that they are prone to human error. It is a difficult feat to consistently apply every network policy, and this inevitably leads to security gaps. Gaps mean cyber threats have an inroad into your network. IBN automatically applies policies, therefore reducing human error and eliminating lapses in security. Integrity verification is built in, making certain that policies aren't contradicting each other, and you can effortlessly implement microsegmentation and contain any potential threats.

Downtime reduction: IBNs predict the impact of changes you make to the network and can alert network operators to potential issues as they crop up, even taking steps to correct those issues within the company's parameters.

The best way to take advantage of intent-based networking is to partner with the Cisco DNA Center.

II. INTENT-BASED NETWORKING WITH CISCO DNA CENTER

Acadia and its partner Cisco Digital Network Architecture (DNA) provide an open, software-driven design structure that easily enables IBN. It incorporates Cisco SD-Access which entwines your network into a single fabric across both wired and wireless. SD-Access gives you a high-level vantage point of your network and also provides you with simple intent-based networking tools.

DNA Center provides users with an instinctive dashboard consisting of five general sections:

1. **Design**: This section allows you to design your own network using local typologies and physical maps. Device discovery is no longer a hit-or-miss endeavor, but simple and automatic.

2. **Policy**: The policy center is where you can create and define user and device profiles, set up virtual networks, access control policies, traffic copy policies, and application policies.

3. **Provision**: With DNA Center, provisioning is now an easy task that can be completed in just a few clicks. You can assign policies based on identity – such as a particular user group or specific devices – and that police follows the identity regardless of location. And when you add new devices to the network, they are assigned a policy based on identity.

4. **Assurance**: You have the peace of mind that comes with DNA Center Assurance support which consistently improves your network's performance. Assurance proactively monitors your network and provides instant alerts when issues are detected. Steps for remediation are immediately provided, streamlining the troubleshooting for your NetOps team.

5. **Platform**: The DNA Center Platform uses open APIs, allowing for enhanced integration with your existing tools. Achieve new insights from your existing data by creating automated workflows to transform manual tasks.

Cisco's Digital Network Architecture (DNA) is the perfect vehicle to deliver Automation Enablement, which is the foundation for next generation networking. We live and do business in a nanosecond world that is constantly evolving. It can be overwhelming to try and keep up with the latest technology in today's highly connected world, but automation enablement is the cornerstone for tomorrow's networks.

Automation enablement is based on intent-based-networking. A company defines a business intent, for example, such as encrypting data as it moves from the user device to the server. An intelligent network integrates with IBN policies and makes changes automatically, making manual configuration of connections obsolete.

Your firm benefits from automation enablement by increasing its agility, managing network operations more effectively, improving regulatory compliance, reducing downtime and beefing up security to keep sensitive data out of the hands of cyber criminals.

III. GETTING STARTED WITH INTENT-BASED NETWORKING

Enterprise-level firms considering intent-based networking need to take a systematic approach for a solid foundation, and should consider t6he following steps:

1. First, determine your firm's business case for implementing IBN.

2. Perform a detailed assessment on your existing infrastructure and determine which aspects of that infrastructure will support intent-based networking, and what will need to be upgraded.

3. Choose a technology partner like DNA Center with expertise in your industry will assist you with network upgrades, installation and deployment of your IBN solution.

At Acadia Technology Group, we know both the benefits and pain points of getting started with intent-based networking. Our Cisco engineers are experienced and will advise and assist you every step of the way with implementing a networking solution that fits your firm's unique needs. Contact us today for more information on intent-based networking.

IV. HOW YOUR FIRM CAN ACHIEVE POWERFUL RESULTS WITH DNA CENTER

To accelerate your firm's growth in this ever-changing technological environment, forward-thinking companies need to embrace new tools to push ahead of the competition. One critical tool to the leverage enterprise digital transformation into growth is centralized network management.

What is centralized network management and what does that have to do with intent-based networking and DNA Center? Central network management is an architecture constructed around a single, powerful server which handles all of the major processing. Other workstations connect to this central network server and submit their workload, such as applications, data exchange and storage, and utilities. The server does all the rest, faster, more efficiently and with little or no downtime.

Enterprises that implement centralized network management through Cisco DNA Center are seeing powerful results. The system keeps up with rapid endpoint expansion, facilitates great improvement in both the wired and wireless experience, and security is enhanced to keep your regulatory compliance in order and your sensitive data on lockdown. Network reliability is notably improved. And although the initial investment may seem overwhelming at first glance, costs are ultimately decreased, and your firm's bottom line grows. Your stakeholders will thank you.

At Acadia Technology group, we understand that digital transformation in our fast-paced technology-based environment is critical to the expansion of your enterprise. With Acadia as your partner, our resources become your resources, and we'll provide real-world solutions customized to the unique needs and goals of your organization.

V. DNA CENTER: PAINLESSLY ACHIEVING REGULATORY COMPLIANCE

We are bombarded daily with news of data breaches from nearly every industry, from health care providers, to financial institutions, email domains, and even social media giants like Facebook and Twitter. It's no wonder that network security is one of the highest priorities for enterprises today. Cybercrime is rampant, and once one leak is capped, another springs up.

According to Gartner, security spending will reach an all-time high of $124 billion this year, up 8.7 percent from 2018. This is especially true for enterprises struggling to keep sensitive credit and debit card information secure to meet regulatory compliance. The Payment Card Industry Data Security Standards (PCI DSS) recommend network segmentation as a primary means to achieve compliance.

To streamline network segmentation – and save your company a headache – Acadia and Cisco DNA Center can eliminate much of the manual configuration involved and allow for granular microsegmentation. Microsegmentation – a method of creating separate secure zones in data centers and cloud deployments, allowing companies to isolate workloads from one another and secure them individually – makes network security more granular.

These tools work together symbiotically to harden your network security through simplifying and streamlining microsegmentation. To harness full advantage of Cisco's network visibility and segmentation tools, companies are turning to Cisco's DNA Center. It combines the tools in the Cisco suite into an intuitive dashboard:

Management: This gives you complete control from a single dashboard, providing a high-level view of your entire network.

Automation: DNA Center provides automated device discovery, drag-and-drop policy creation, and zero-touch device deployment. Policies are automatically applied, keeping your network secure and compliant.

Security: DNA Center integrates Stealthwatch and ISE, tools facilitating identity-based security.

Assurance: Since microsegmentation is only as effective as your network, DNA Center Assurance aggressively monitors your network, alerting you in real-time to opportunities for optimization.

To be certain your firm is on the right path for regulatory compliance, choosing to work with a trusted third party is a smart move. It takes careful planning, design and implementation. At Acadia, we're experienced in Cisco network and security solutions. Partner with us today to find out how microsegmentation and compliance can work for you.

VI. NETWORK SCALABILITY PAIN POINTS AND AUTOMATION SOLUTIONS

Endpoint users connecting to the network are growing at an exponential rate. Forbes, Inc. recently reported that by the year 2023, IoT connections are expected to top 3.5 billion users. It's an exciting time, and one that is ripe for business opportunities, but those exploding numbers also leave your NetOps teams under the heavy burden of endless manual configuration. The potential for lack of consistency and unwieldy network complexity just isn't worth it when firms have other options available to achieve the same goals.

Network scalability is certainly critical to keeping up with the endless demand of the IoT, but that in and of itself comes with a whole new set of challenges. How do NetOps teams keep your network performing at its peak? Maintaining and expanding that network to accommodate the increased demand requires a significant amount of time and attention, which can take your NetOps team's focus away from other important tasks that could have long-term effects. The last thing your enterprise needs is to have network design become haphazard and piecemeal because of tedious manual configurations.

A truly scalable network will function at its peak no matter how many users are accessing it. It should be simple and painless to maintain, without disruption every time devices need to be added. Quick and easy should be your firm's buzz words when it comes to scalability. Fortunately, they're our buzz words, too – network automation makes these goals achievable without the headache.

Cisco's DNA Center brings powerful network automation tools to the table, making facilitating network scalability simple:

Automation Software Image Management: This tool allows users to manage software upgrades and control the consistency of image versions and configurations across the network, speeding up software deployment and patching.

Automation Plug-And-Play: Automation Plug-And-Play enables zero-touch provisioning for new device installation. Cisco devices are provisioned as soon as they connect to the network.

Enterprise Network Function Virtualization: This automation support for ENFV facilitates branch virtualization, saving precious time in setting up network virtual services.

EasyQoS: This is an automation tool that creates an end-to-end quality of service chain across your network.

DNA Center also wraps in SD-Access, which is Cisco's proprietary software-defined networking technology. SD-Access weaves your network into a single, tensile-strong fabric.

SD-Access drives DNA Center's automation capabilities, and enables several automation workflows, including:

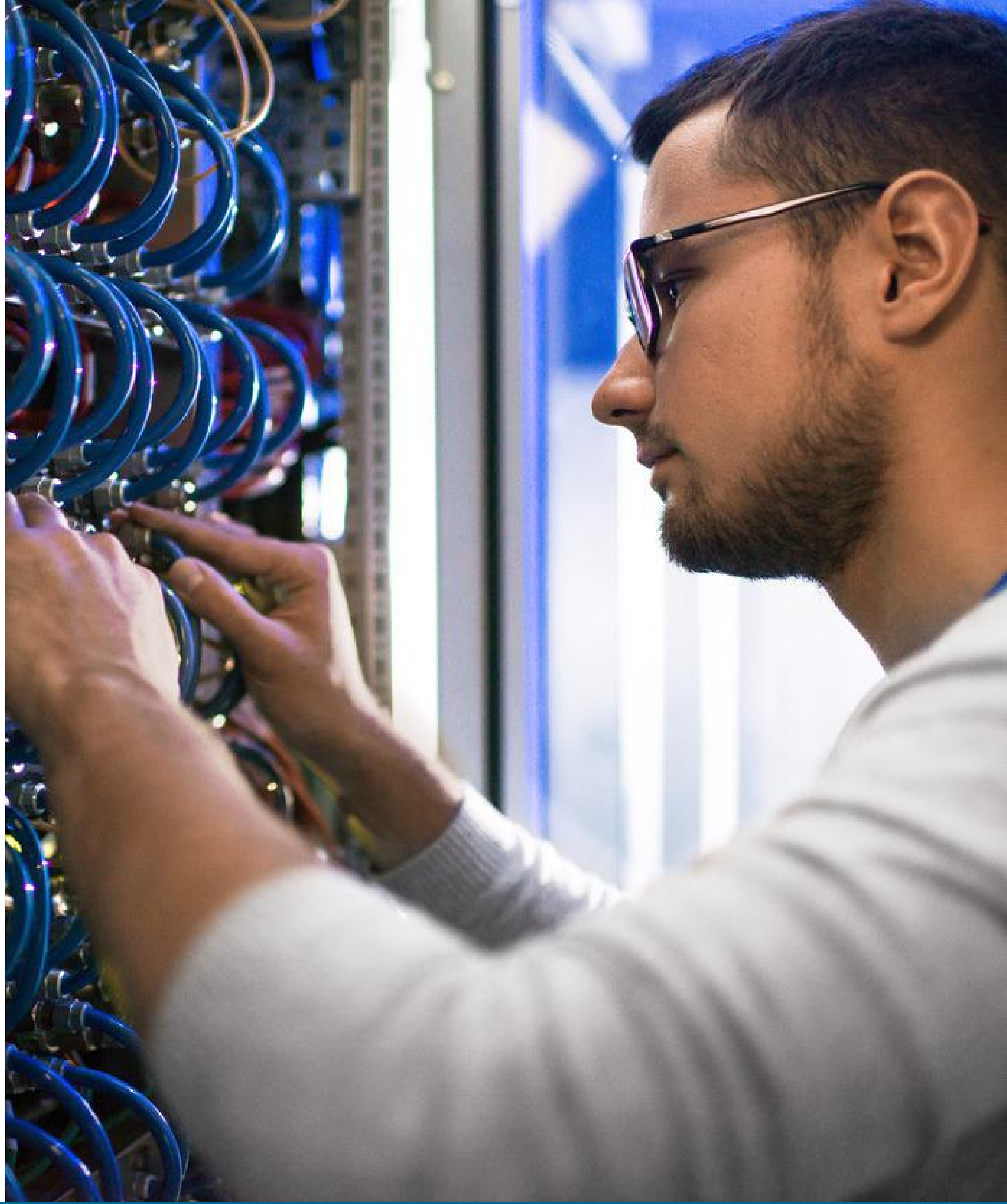
- Virtual networks
- Group-based policy setting
- Automated host onboarding
- Deployment pre- and post-verification

DNA Center and SD-Access automate wireless network configuration, making scalability simple and easy to manage. Defined policies are automatically applied, hardening security while drastically reducing the workload on your NetOps team. DNA Center gives you end-to-end visibility across your entire network.

VII. OPEN SOURCE: NEW INSIGHTS FOR HELP DESK TICKETS

When Cisco DNA Center's Open Source Platform was announced earlier in the year, it rippled throughout the industry. By Cisco opening up this Platform, developers and third-party partners now had access to APIs, which businesses of all kinds utilize for in-depth network analysis. Thanks to the DNA Center Platform, enterprises have the chance to accomplish powerful results through network automation, eliminating wasted time and enhancing organizational efficiency.

We've all been there: IT troubleshooting is a frustrating, time-consuming task, which more often than not robs attention away from other pressing issues. With the DNA Center, the solution is at your fingertips. The DNA Center Platform offers Intent and Integration APIs, which translate the information into a language that's understood and immediately accessible by NetOps teams. It also offers 360-degree transparency of any device on your network, giving your IT teams deeper insights into the issues at hand, and letting them resolve those issues quickly.



All of these components work together to streamline help desk ticketing. Even user-generated tickets contain important information about past issues and topology (both physical and logical/signal). Even if resolving said issue requires a network change, NetOps can click a button to implement that change. An open source DNA Center offers unique and exciting opportunities for innovative process improvement, all while keeping your environment secure.

So what can DNA Center's Open Source do for you and your enterprise? Open Source is full of robust information available through the Platform. Your team can take several approaches to unlock the full potential of Open Source:

Review your current IT workflows: Are there bottlenecks in your processes? Where are they and why? Does your ticketing system have too many steps? Take an introspective look at your IT operations and find the areas where additional information from Open Source, or automatic ticket generation would enhance efficiency for your team.

Integrate the appropriate APIs: An in-house development team can explore DevNet, Cisco's Open Source development platform, which encompasses learning tracks and a sandbox to enable exploration.

Work with a trusted partner: With all the possibilities that Open Source has to offer, firms would solidly benefit from working with a trusted partner like Acadia. We can help you implement the Open Source tools in a way that supports your business goals.

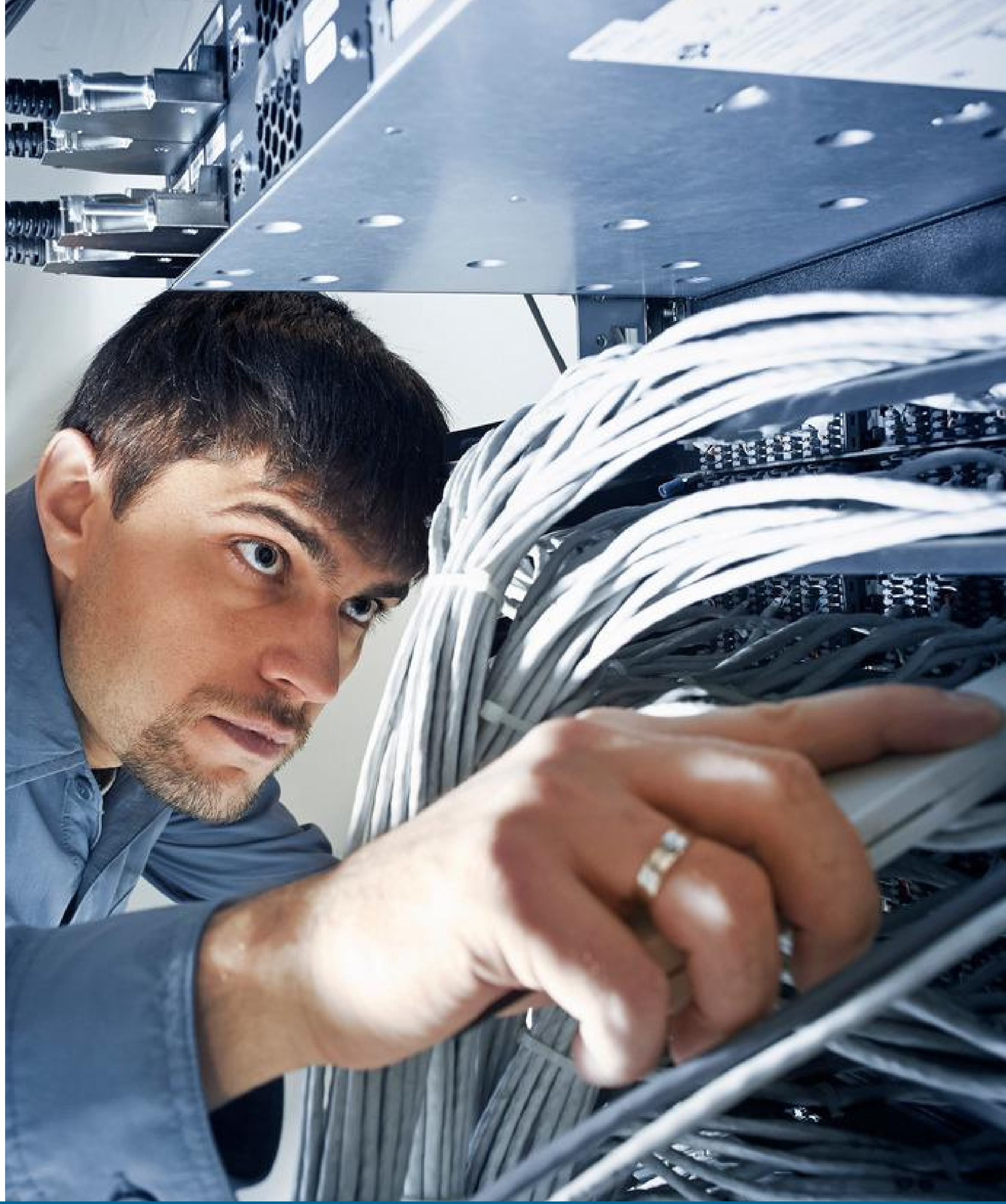
VIII. DNA CENTER INTEGRATION: PREPARING FOR THE BIG CHANGE

According to International Data Corporation (IDC), digital transformation spending will increase by 42 percent by the end of 2019. More CIOs are turning to centralized network management solutions such as Cisco's DNA Center to prepare their firms for the changeover, to maintain their competitive edge, reap all the benefits of digital transformation and ensure the optimal performance of their networks.

So how should your enterprise start planning for the change to centralized network management? First things first: Evaluate your infrastructure. Make certain your firm's hardware, software and network will support DNA Center. Some considerations:

Hardware requirements: Integrating SD-Access may require upgrading switches and routers. SD-Access requires ISR 4400 Series routers or ASR 1000X/HX Series routers. The Cisco hardware requirements for switches are:

- Cisco Catalyst 3850/3650 Series Switches
- Cisco Catalyst 4500E SUP8-E Supervisors
- Cisco Catalyst 9000 family of Switches
- Cisco Catalyst 6500/6800 Series with SUP2T and SUP6T with 6800 series line cards
- Cisco Catalyst 6840 and 6880 Series Switches
- Cisco Nexus 7700 (with M3 series line cards)



Your network: Cisco recommends increasing your maximum transmission unit (MTU) to 9100s bytes on interfaces across all switches and routers to meet the needs of SD-Access. SD-Access fabric can be used on traditional hierarchical networks as well as other topologies.

Software requirements: SD-Access can run on top of individual virtual machines or dedicated appliances for DNA Center and Identity Service Engine (ISE), depending on your firm's needs.

After your current infrastructure has been evaluated and it's been determined it meets all prerequisites, begin reviewing your plans for the upgrades based on DNA Center requirements. Organizations typically take one of two approaches to upgrading to SD-Access:

Parallel installation: This approach installs SD-Access and DNA Center in parallel to your existing network. This simplifies upgrading, in that you can switch back to your existing network if needed. However, it is also more expensive in terms of resource demand due to running two networks until the upgrade us complete.

Incremental installation: With this approach, one switch is upgraded at a time. This approach stretches integration over a longer timeframe, but it is less expensive due to requiring less space and power compared to the parallel installation.

No matter which method your firm decides on, another consideration for your upgrade timeline is the larger, company-wide impact. Once DNA Center is integrated, what employee training will be needed? Which systems and processes will be impacted and for how long? Think globally when considering which installation to employ and consider the impact across the entire organization. Doing this will solidify a realistic timeframe and budget for your impending integration.

The third step before integrating DNA Center is a comprehensive budget review, and, if needed, reworking those budgets in consideration of the larger benefits that DNA Center will bring to your organization. Examine the costs of integrating DNA Center in terms of time, money and resources allocated. Although the costs may seem daunting, investing in DNA Center can solve several business needs, including:

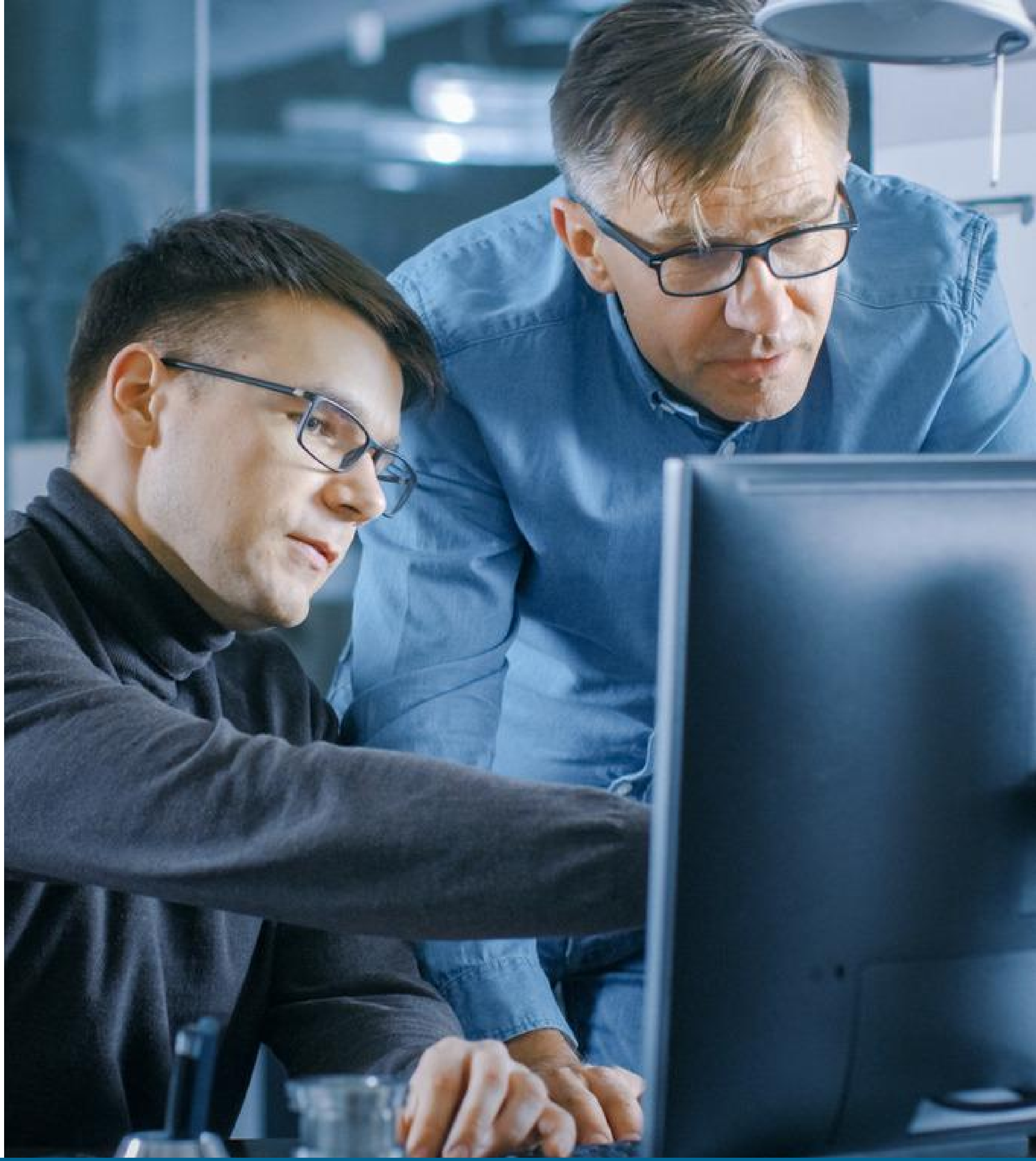
Increased efficiency: IT staff members spend up to 43 percent of their time troubleshooting technical issues. DNA Center provides automated troubleshooting tools to free up your team to focus on larger technology goals. Automated, policy-driven provisioning eliminates manual time-consuming tasks that are prone to human error. Investing in DNA Center frees up your IT team to do more with less.

Network stability: This benefits not only the IT team, but the entire organization. DNA Center's predictive analytics provide insights that improve the network for the entire firm. Expensive downtime is greatly decreased, and customers and employees alike have a richer experience.

Enhanced security: Recent security breaches have driven home the importance of aggressive cybersecurity. DNA Center's tools for micro segmentation and automated policy setting tools harden network security.

Keeping up with IoT demands: Customers and employees are placing increasing demands on your network, both in terms of performance and security. DNA Center provides a well-designed solution, allowing you to manage endpoints from a single dashboard.

Digital transformation: Organizations have more data on customers than ever before, which can be used to enhance and personalize the customer experience, increasing loyalty and, under the right circumstances, revenue.



IX. FAQS: WHAT YOUR PEERS ARE ASKING ABOUT DNA CENTER

Companies are turning to Cisco DNA Center for its robust security features, time-saving tools for network troubleshooting and provisioning, painless endpoint management, and much more. As enterprises move forward and integrate DNA Center into their infrastructure, some have questions about meshing the technology into their current network fabric. Answering these key questions gives firms a clearer picture of the integration process and how business life will improve with DNA Center. So here's what your peers are inquiring about:

Q. Can I customize DNA Center to suit the needs of my organization?

A. Yes. Cisco recently made DNA Center open source, giving programmers access to its APIs. Its resources for developers include the DevNet DNA Developer Center, which is a site with tools and software development kits (SDKs) for developers to explore the DNA Center platform, and the DevNet Code Exchange, which is a code-sharing network with code samples, adapters, and SDKs.

Q. What types of APIs does DNA Center offer?

A. DNA Center offers several types of APIs that can be used for networking. These include:

- **Multivendor SDKs** – These allow integration with network equipment from different vendors.
- **Intent-based APIs** – These enable continuous network alignment that adapts to your enterprise's changing needs.
- **Integration APIs** – These allow integration between Cisco and third-party IT and network systems, streamlining IT operations across domains.

Q. How does DNA Center integrate with existing Cisco solutions such as Meraki?

A. DNA Center integrates well with Meraki because it integrates the Meraki dashboard, combining Meraki simplicity with the power of DNA Center to handle complex network functions. Other solutions may require an upgrade.

For example, firms currently using the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) can migrate to the DNA Center by following Cisco's upgrade path, which allows users to import APIC-EM configurations into DNA Center. It's a seamless migration that allows APIC-EM users to benefit from the enhanced features of DNA Center, including DNA Assurance.

Q. What is SD-Access and how does it relate to Software-Defined Networking (SDN)?

A. SD-Access is Cisco's SDN technology. It's the foundation of DNA Center, creating a single network fabric and enabling end-to-end visibility across your network, allowing easy policy provisioning and task automation. It enables quick network access for any user or device without compromising security.

Q. How is Cisco DNA Center's security approach different from traditional security protocols?

A. DNA Center builds on the traditional security approach, which is typically focused on perimeter defense through firewalls, intrusion detection, access control, and VPNs. This security approach is challenging to maintain in the face of the exploding number of endpoints created by IoT devices.

DNA Center allows you to monitor all the activity across your network. Your network data is collected and analyzed by Cisco tools such as Stealthwatch. Stealthwatch uses machine learning and behavioral modeling to mitigate threats. It detects advanced threats, including malicious patterns in encrypted traffic, which firms can easily view in the DNA Center dashboard.

DNA Center also takes network segmentation several steps further. The fabric woven by SD-Access allows for microsegmentation, enabling firms to easily separate different user groups. Cisco Identity Services Engine (ISE) also helps to drive microsegmentation by allowing you to easily set up user groups. Firms apply policies based on user groups rather than IP addresses, streamlining provisioning.

Current segmentation approaches, such as VRFs, VLANs, and ACLs, are labor intensive and vulnerable to human error. SD-Access simplifies microsegmentation, hardening security without burdening your staff with complicated manual tasks.

Q. What services can help me develop a strategic plan for integrating Cisco DNA Center?

A. A knowledgeable partner can help you plan for DNA Center integration. For example, Acadia Technology Group is an experienced Cisco partner. They work with enterprises to:

Assess their current infrastructure – They can make recommendations regarding what hardware may need to be upgraded or replaced.

Develop a strategy – They'll review the needs of your business and look at how to best integrate DNA Center to meet the needs of your network.

Deploy DNA Center – Acadia Technology Group will deploy DNA Center in partnership with your internal IT staff, ensuring a smooth transition.

ABOUT ACADIA TECHNOLOGY GROUP

Acadia Technology Group is an IT solution provider operating out of Montclair, NJ focuses on the New York Metro area marketplace. A Cisco partner with decades of experience, Acadia Technology Group is responsible for some of the most cutting-edge Internet-of-Things and security solutions within the theme park, finance, and legal markets.

CONTACT US

Click below to continue the conversation with Acadia Technology Group.

CONTACT US

CISCO

ACADIA TECHNOLOGY GROUP