

# SOFTWARE-DEFINED NETWORKING

Keeping Pace with Network Complexity in the Public Sector



# INTRODUCTION

For today's government IT leaders, it's a fact of life: Despite an ever-growing demand for information technology services, budget cuts require doing more and more with less and less.

In 2015 alone, the federal information technology budget shrank by \$2.4 billion, and state and local governments also suffered cuts. And those aren't the only problems faced by the public sector: security compliance, network complexities, demands for better efficiency—the list goes on. Meanwhile, citizen expectations intensify, particularly following high-profile data breaches that left huge swaths of sensitive, private civilian data vulnerable.

So where does that leave government IT programs? How can government agencies improve visibility and control while balancing growing business demands and shrinking budgets?

**Software-defined networking (SDN)** offers a solution. Today, public sector IT must quickly deploy and run new applications (both within and atop their networks) to deliver results—all without disrupting their mission. Enter SDN.

By accelerating application deployment and delivery through policy-enabled workflow automation, SDN allows administrators to manage network services while dramatically reducing IT costs.

To offer a better understanding of SDN's benefits—including how it applies to public sector challenges—GovLoop partnered with Force 3, a network security company that provides infrastructure services to design, deploy, support and maintain both public and private sector technology needs. In this report, we tackle the challenges faced by government IT professionals and the solutions offered by software-defined networking. Read on to gain a better understanding of SDN, including:



Why software-defined networking matters for government IT professionals



How SDN increases network flexibility and simplicity, while enhancing security and automation



The best practices for successful SDN adoption

## TRADITIONAL NETWORKS VS. SOFTWARE-DEFINED NETWORKS

To fully grasp why SDN is such an advancement for public sector IT, you must first understand the limitations of traditional networks, which are generally:



**PROBLEMATIC TO MAINTAIN**, due to inconsistent system configurations



**LABOR-INTENSIVE**, because they require frequent manual procedures



**LIMITED IN VISIBILITY**, after all, you can't see everything from a single viewpoint, and you risk having your network fall out of compliance

SDN addresses these traditional network shortcomings by using software to enable network intelligence—in other words, designing a network to become smarter and application aware. In essence, the network can dynamically adapt to the needs of the application.



# A NEW BLUEPRINT FOR THE PUBLIC SECTOR

As use cases increasingly illustrate the potential of SDN to address IT challenges, the public sector is recognizing SDN's value. Still, as a quintessentially next-generation concept, software-defined networking—or at least the overall understanding of it—remains relatively abstract. Force 3's practice director of next generation networking, Jon Kim, prefers to position SDN as a new architecture.

"Software-defined networking is essentially an improved blueprint," Kim says. "Rather than going back to the traditional network design, you need an improved blueprint describing how you build a next-generation network to support today's rapidly evolving IT needs."

Simply put, SDN offers a new approach to designing, building, operating and managing networks.

SDN introduces a centralized touch point for all network administration thus reducing the need for manual process. By creating a virtual overlay network, SDN allows for separation from the physical network. As a result, users can share the network, while still maintaining proper traffic separation and security.

In short, by automating business workflows, SDN benefits any organization seeking to optimize workload deployment.

---

"Software-defined networking is essentially an improved blueprint," Kim says. "Rather than going back to the traditional network design, you need an improved blueprint describing how you build a next-generation network to support today's rapidly evolving IT needs."

# THE BENEFITS

## Efficiency, Flexibility, Customization, Automation

Where resources are limited and staff time is at a premium, efficiency is everything. But efficiency is not the strong-suit of traditional networks—especially in contrast with SDN.

For example, in a traditional network infrastructure, executing workflows often requires manual input and participation from various teams: applications teams, system administrator teams, network teams, security teams, etc. Consequently, adopting new services under such a segmented structure requires a lot of manual, complex interactions between different teams.

Software-defined networking, on the other hand, takes on many of these tasks, allowing IT teams to tackle their more imperative projects—a critical benefit when resources are tight and staff time is limited.

“SDN provides automation and programmability so that IT staff can keep pace with new business requirements,” says Rob Chee, Force 3’s principal security architect. “IT teams can effectively use the tools provided by vendors to automate remedial tasks.”

Taken one step further, IT teams can automate multiple tasks with an orchestration tool. This removes potential human error occurring during configuration and can allow developers to self-provision approved workloads without administrator involvement.

“Traditional datacenter networks haven’t customarily been built in a flexible, agile manner,” adds Greg Stemberger, Force 3’s principal network architect. “Instead, they’ve been very static. You build it once, you put it in place, and you let it provide connectivity in the way you go.”

But, Stemberger explains, today’s networks must be more agile and flexible.

“That’s where software-defined networking comes in,” Stemberger says. “It adds that element of network software—network intelligence in software—and it offers more flexibility for driving the infrastructure as a collective system and providing services that meet business requirements.”

“SDN provides automation and programmability so that IT staff can keep pace with new business requirements,” says Rob Chee, Force 3’s principal security architect. “IT teams can effectively use the tools provided by vendors to automate remedial tasks.”

### Key Benefits of Software-Defined Networking



#### Agility

Traditional networks cannot keep up with the speed of evolving business demands. SDN provides dynamic control and configuration of network-wide traffic and devices.



#### Security

Firewalls at the perimeter of the datacenter cannot protect against intra-datacenter threats. SDN implements granular security throughout the datacenter to provide protection between individual systems.



#### Costs

Traditional networks are labor intensive. Through automation, SDN limits manual involvement, lowers deployment time, and minimizes potential errors introduced during the deployment. This dramatically lowers the operational cost of deployment.



#### Provisioning

Current provisioning of new servers and network services requires manual changes to many different endpoints. SDN allows administrators to accelerate the deployment of new applications and network services across the datacenter in just minutes, rather than days.

# THE 4 PRINCIPLES OF SOFTWARE-DEFINED NETWORKING

When it comes to software-defined networking, Force 3's experts explain the concept—including its relevance to customers and the best practices for adoption—using four principles. These guidelines provide insight into the specifics of software-defined networking and how to maximize its benefits for your organization.

## Centralized Management

Large, distributed networking environments require numerous manual touches, consequently decreasing efficiency and risking security. In a non-centralized network, it's harder to push updates or see everything happening, not to mention compare traffic or performance. This provides a more effective way to interact with the networks in order to drive changes.

SDN eliminates these concerns by centralizing management of networking capabilities. Meanwhile, it also consolidates and enhances network visibility and allows users to drive changes into the infrastructure from a central touch-point.

## Network Automation

For network automation, traditionally when you stand up a server (like a virtual machine) you allocate the CPU, memory and storage resources, but then you also have to involve the security team and put the firewall rules into place. You have to engage the network team and define the virtual local area network (VLAN) required for the virtual machine.

But SDN combines all of that via automation, from building the virtual machine to what VLAN it has to be on, which security parameters it requires and its connection to that virtual machine for user access, along with communication between servers within the data center.

When the server is built, whether it's in production or development, all the relevant network and security parameters are also automated. It eases the burden to configure all required parameters for this virtual machine to be operationally accessible.

## Network Abstraction

Network abstraction builds on network automation. While network automation allows us to drive infrastructure changes in a much more effective, less error-prone manner, network abstraction builds on that same concept.

Network abstraction allows you to deliver services anywhere in the network. Essentially, the network is abstracted using intelligent software in the software-defined networking paradigm. As a result, instead of purpose-filled network functions, IT departments can uniformly deliver services in a more abstracted manner anywhere on the infrastructure.

## Programmability

Another feature of the intelligent software that drives the SDN infrastructure is programmability.

We're interacting with the network in a much more programmatic fashion. This lets us make infrastructure changes that properly reflect the state, the requirements of the networks, and what they need from the network.

SDN products provide programmability through open REST APIs, (a common set of functions allowing moves, adds and changes via HTTP protocols). These APIs allow for two enhancements. First, SDN functions can be scripted to accelerate workload deployment. Second, the openness of the APIs allows for tight integration with other related programs, whether they come from the same vendor or a third-party vendor enhancing the solution. This provides a new level of powerful capabilities, enabling a multi-vendor solution.



# CONCLUSION

Public sector IT departments face many challenges today: reduced budgets, smaller staff sizes, network complexity challenges, shadow IT and more. But as they build and expand their networks, software-defined networking can address these obstacles.

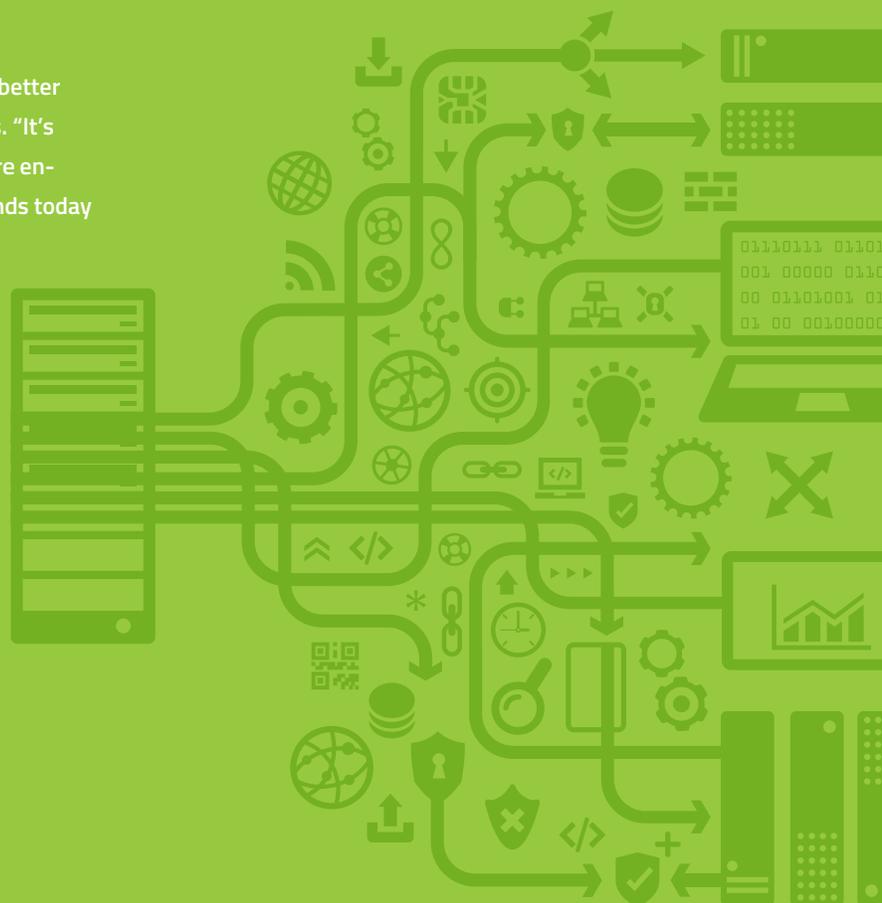
SDN changes how public sector agencies deploy, manage, support and configure their networks. Its promise lies in network automation, orchestration and enhanced custom integration, not to mention better visibility, so that public sector IT can do more with less.

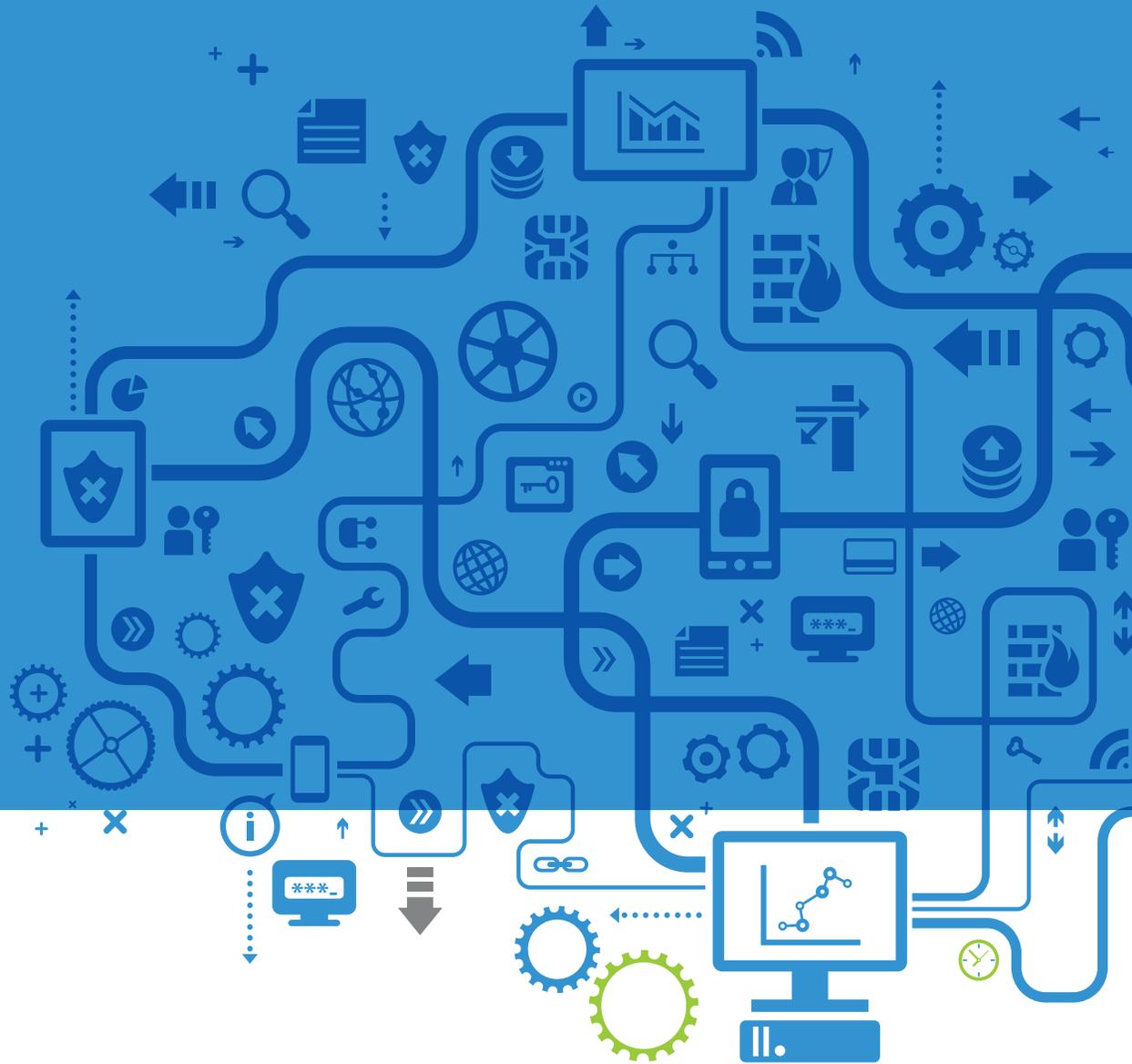
By automating and centralizing network administrative tasks, SDN streamlines operations. Combining applications and network services into a centralized policy allowing datacenters to be more effective. Finally, SDN offers more agility by letting you quickly customize network parameters as your business needs evolve and change.

“SDN offers a fresh, innovative approach for IT, creating better and smarter organizations for tomorrow,” Kim concludes. “It’s still new and evolving. But when correctly adopted, you’re enhancing the capability to keep pace with business demands today and for tomorrow.”

---

“SDN offers a fresh, innovative approach for IT, creating better and smarter organizations for tomorrow,” Kim concludes. “It’s still new and evolving. But when correctly adopted, you’re enhancing the capability to keep pace with business demands today and for tomorrow.”





Force 3 is *the* Network Security Company. We provide infrastructure services to design, deploy, support and maintain your technology needs. Whether through enterprise networking, mobility, collaboration, data center or next-generation technology, our expert engineers and strategic partnerships enable us to provide secure, high quality solutions for clients who demand value and reliability.



in partnership with:  
**vmware**<sup>®</sup>

**1.800.391.0204**

**[sales@force3.com](mailto:sales@force3.com)**

2151 Priest Bridge Dr,  
Crofton, MD 21114, United States

13655 Dulles Technology Dr,  
Herndon, VA 20171, United States

