Smart Network. **Smart** Business.

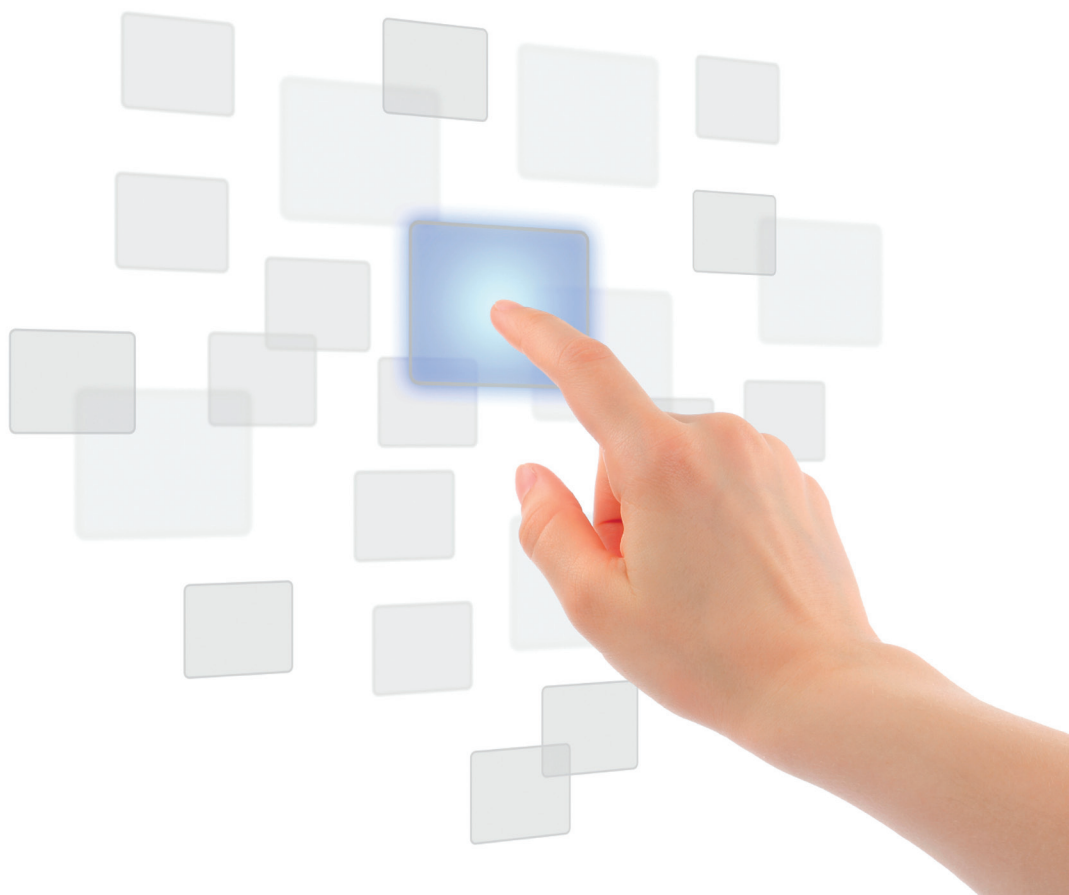# Network Services in the SDN Data Center

SDN as a Network Service Enablement Platform – Whitepaper

Executive Summary

While interest about OpenFlow and SDN has increased throughout the tech media over the last year, it is not always clear what all the hype is about and what will inevitably be the role of networks as we know them today. SDN's are intended to help organizations simplify changes, improve multi-tenant support and increase network utilization. These capabilities are enabled by separating the network control and data planes and by extending an API to the network controller that allows applications to program the network. As the benefits of simplification of the network operation and improvement of the overall network virtualization mature, one of the most important compute elements, the network services, needs to be rethought. How does network security and application delivery play in a software defined world? Is it merely a matter of extending an API and supporting new network encapsulation models in order to truly become SDN ready? Or is there more to it, allowing organizations to benefit from network services in an unprecedented way by taking advantage of the central control of the network?

Radware SDN applications make network services pervasive, improving the overall availability, security and performance of applications by programming the network to be part of the service engine and amplifying the existing benefits from network services and SDN. With Radware SDN applications, ADC and security services transform from device-based solutions requiring a static traffic forwarding configuration, to network wide services that intelligently divert traffic to service engines. Network services can scale to support larger networks at lower capital and operational cost. By building SDN applications that continuously interact with the SDN control plane and program the network, and by leveraging the Radware Virtual Application Delivery Infrastructure (VADI) architecture which enables pooling of disperse resources to operate uniformly, Radware enables an anywhere and everywhere network service paradigm. Radware SDN applications operate through a closed loop network service optimization cycle which constantly collects information from the network and the applications, continuously analyzes the information making intelligent service decisions, and controls the network to assure optimal network service delivery.

Organizations benefit from Radware SDN applications by the unique ability to enable the subject services to any application in the network regardless of physical placement, by enjoying the ability to further scale network services at lower costs and with less operational overhead.

Radware SDN applications are the control point that programs the network to collect and enforce traffic distribution throughout the SDN based on its decision engine.

Table of Contents

Introduction

For various reasons people see SDN as the answer to several challenges the network imposes on modern compute infrastructures. The very dynamic nature of modern compute infrastructures that mobilize and re-scale workloads, and the heavy intra-datacenter communication volume in these networks create new demands in terms of ongoing reprogramming of the network and improving network utilization efficiency.

From a technology perspective, SDN and OpenFlow are about separating the data plane from the control plane of the network. The SDN is divided into switches/data plane elements and to a network controller. Essentially any human or 3rd party interaction with the network is performed through the network controller which in turn programs the network switches and routers to function as desired. One of the key advantages to this approach is the fact that any network operator, or application needs only to communicate with a single device, the network controller. In larger networks where network operators would program multiple networking devices that needed to interact with each other and are prone to significant human error, this approach offers significant advantages. Furthermore, the fact that the network data plane is distributed allows for less focus on the placement of compute, storage and appliances throughout the network as any network physical port can be programmed to perform any function and attach to any elements. This approach unleashes the potential that is held within compute and storage infrastructures that are managed as pools of resources without any physical constraints.

Drivers and Realities of SDN in Data Centers

Some of the interesting questions about SDN is why, how and when will the technology be adopted by end users? Why will people choose SDN technology over legacy network technology? How will SDN components connect compute and storage to existing networks? And when will commercial SDN offerings become a viable alternative to legacy "non SDN" network equipment. In order to evaluate these questions we should review the key problems SDN helps to solve.

1. automation of network configuration as needed by applications
2. multi-tenant network infrastructure support
3. network infrastructure utilization

Solutions for the challenges above are likely the most common benefits associated by organizations as values of adopting SDN. Let's elaborate a bit on each of these;
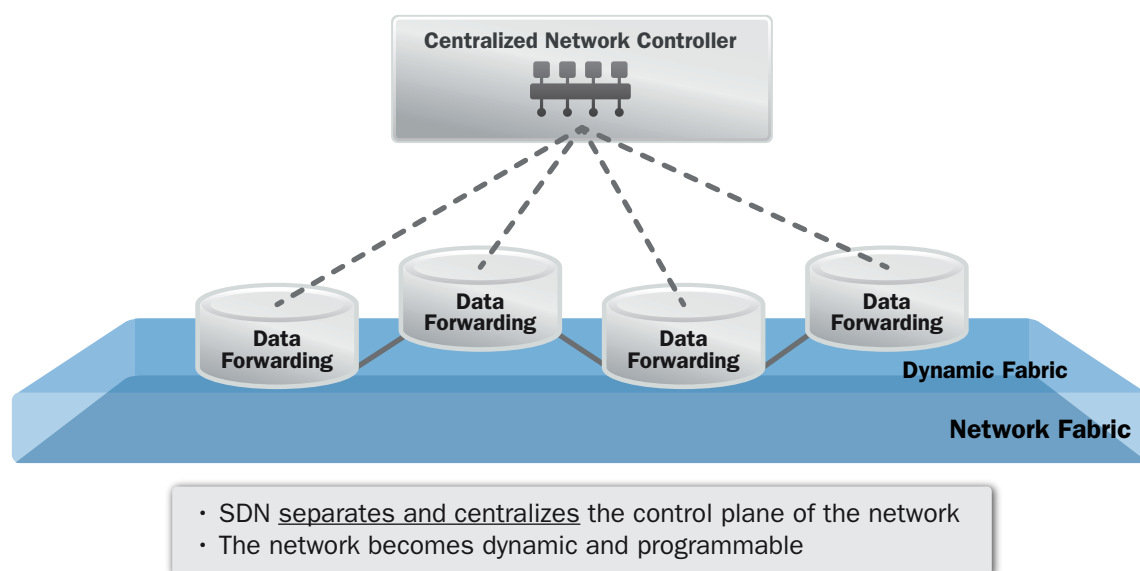

- SDN separates and centralizes the control plane of the network
- The network becomes dynamic and programmable

Figure 1: SDN control & data plane split

Automation of network operations: As datacenter compute becomes more dynamic due to virtual machines being spawned and moved around frequently, applications scale out and overall operations become more automated. Networks have been blamed to hold back the agility of the datacenter. The centralized nature of SDN, and its ability to control large distributed networks, enables the dynamic datacenter to align network resources with application changes in real time. This is true for virtual data-centers mobilizing workloads, multi-tenant /cloud datacenters that dynamically build tenant virtual silos, large global network automating backup/replication routines and elastic applications that dynamically scale out on demand.

Multi-Tenant networks: With the increased popularity of cloud and virtualization technologies, there has been motivation to increase revenue through multi-tenant operations, as well as enterprise by cost savings and organizational efficiency of private cloud solutions. SDN offers a great way to divide the network and allocate a logical portion of the network to each tenant, without impacting the existing network operational model and physical network stability. Furthermore, the provisioning and ongoing tenant related network operations can be automated alongside the tenant related compute operations.

Network utilization: The ability to optimize network usage is of great value, especially where either user experience is critically impacted by network performance or the cost of the network is very high. Looking through the reasons why SDN is a natural suspect to help solve the network utilization problem retorts to the programmatic nature of the SDN. Usually network utilization related activities are driven by applications, or by time of day which is predictable. Being able to inform the network when it should be treating certain traffic in a certain way has also proven to be of great interest to network operators.

Traffic impacts user experience through a higher priority, and allows traffic critical to certain operations to pass through at a steady pace. Letting the applications request from the network what they need is not a new idea, but SDN seems to bring this idea closer to implementation reality.

The Untapped Potential of Network Services

Network services are the necessary evil in any datacenter network. While there have been several best practices proposed on how to secure servers, optimize servers, optimize code, secure identity and access policies, optimize transport and processes, implementing these services is always challenging. However, network services dealing with availability, security and performance always find their very important role in the data center network. Organizations cannot succeed without load balancing, attack mitigation, web application firewalls, firewalls, and various optimization technologies to help run their business applications, keep costs down, and effectively meet business requirements. Evidently, due to the gateway nature of network service appliances, they connect a side of the network without the service to a side of the network that receives the service. Designing the network to accommodate these services in a highly
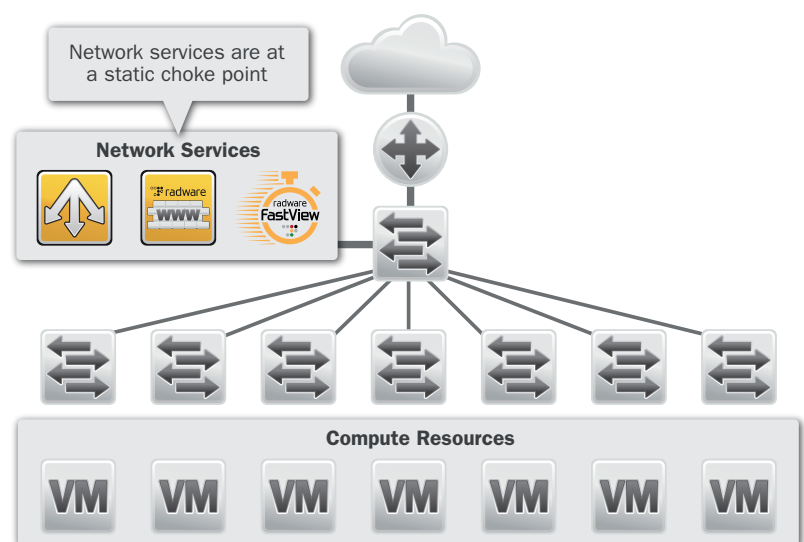

Figure 2: Contemporary networks limited service architecture

available manner, has never been a trivial task. Traffic needs to be routed through these devices without changing the access mechanism to the applications (dns, ip address) that existed prior to the service insertion. Effectively the need is to squeeze the service in without making any changes to the applications. These problems amplify when supporting a multi-tenant service profile is required. Typically, the solutions to these challenges involve sophisticated network design employing many routing, forwarding, state sync and transparent communications network tricks in order to insert the service without creating a single point of failure. Additionally, solving these problems involves over-provisioning of network service appliances that incur unnecessary costs.

The end result is an expensive network tailored to solve a specific problem residing in an exact network location. This design has a very limited ability to scale and create improved economies for the network operator and owner. In typical application life cycle events that require expansion of the application capacity, or the addition of tenants with custom requirements, this design does not support the ability to scale and virtualize the network service as needed. Since the network service appliance resides in a network junction that supports a certain bandwidth, and since the appliance at this junction has a certain network connectivity capacity, there is no simple way to scale up. Similarly, if a larger network service appliance was initially placed in a network junction assigned to serve a certain datacenter silo, and conditions change that require the excess capacity of this appliance to serve different applications or tenants. The service can only be assigned to applications and tenants that physically reside in the same network silo.

What we are seeing is a very tight relationship between the physical placement of a network service appliance, the tenants and applications it serves, and its initial capacity. However, as indicated, realistic requirements prove different. Datacenters tend to be more dynamic and a static resource allocation scheme does not appropriately address the emerging needs. Over the years, point solutions from vendors have aimed to solve this problem by clustering appliances and building a level of abstraction in management systems. These designs fail to automate changes in the network that result from changes in the compute infrastructure and end up introducing additional operational requirements.

Network Services Blended into SDNs

SDN's make a difference. If built right, networks can seamlessly support the lifecycle of applications and multi-tenant environments. However, applications are not going to immediately change their nature and start programming the network. The job of mediating between the requirements of applications and compute infrastructure from the network will remain the job of network services. The network services are responsible for increasing the application capacity and how that reflects on security policies and resource allocation, and introducing security for additional applications. SDN enables far greater interaction between the network services and the network. The network services in an SDN can become blended and be part of the network, available everywhere and centrally managed. By leveraging the central control architecture of the SDN and the distributed data plane, basic network service functionality can be extended through the network and intelligently directed to the optimal network service appliance when advanced functionality is required. Leveraging this capability of SDN tremendously improves the ability to economically size network services and consistently control application quality of experience and address the challenges that stem from the gap between application infrastructure automation capabilities and the static nature of network service designs in contemporary networks.

Radware's SDN Applications

Radware's approach leverages the potential to continuously program the SDN, alongside the existing virtual application delivery infrastructure technology to unleash the full potential of network services. In order to morph the existing network service appliances into network services, Radware is developing service specific SDN applications that continuously interact with the SDN, the Radware appliances and the compute and application infrastructure. Radware SDN applications are the control point that programs the network to collect and enforce traffic distribution based on its decision engine.
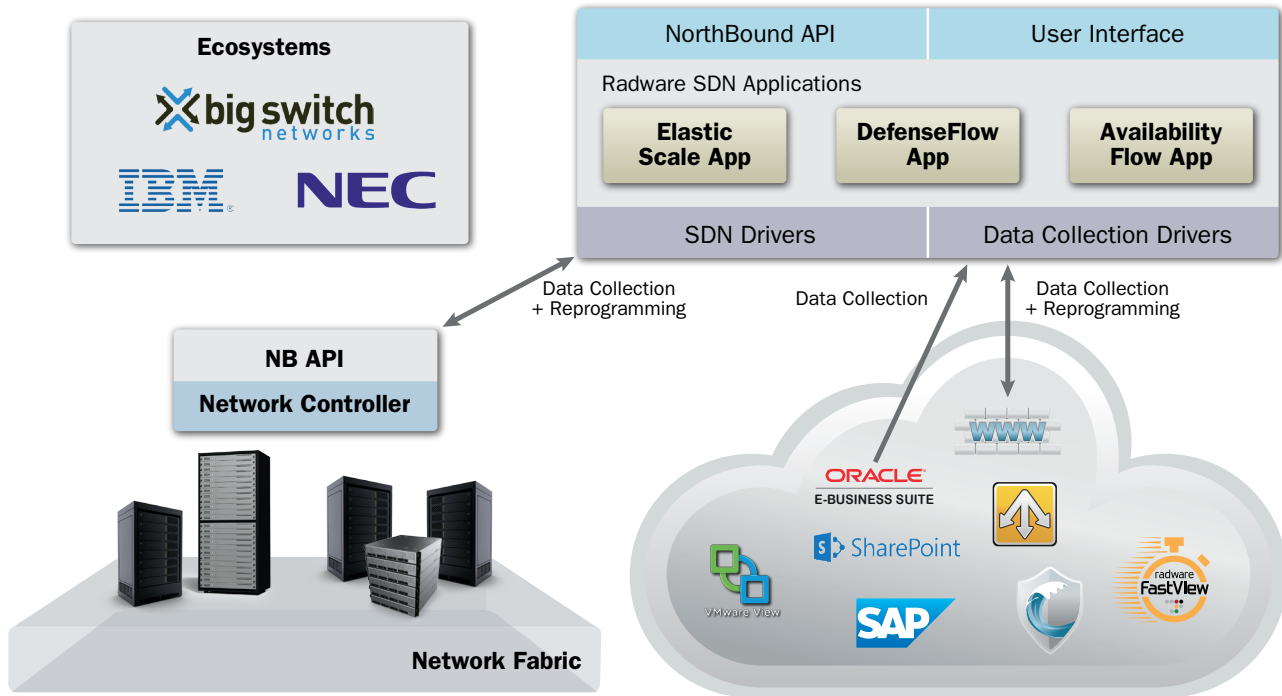
Figure 3: Radware SDN applications logical framework

Radware SDN applications improve application security, performance and availability by programming the SDN to collect data and optimally forward traffic to deliver network services. The native component of the new network stack introduced by SDN includes the data plane networking devices and the control plane SDN controllers. The Radware SDN applications constructing the SDN application control plane, interact with the SDN controller using dedicated SDN drivers and work together with the Radware systems' using the Radware API to collect data throughout the application infrastructure using specific data collection drivers.

Leveraging Radware SDN applications, business applications availability, security and performance are improved throughout the application life cycle and deployed more efficiently. The SDN applications allow organizations to deploy network services more pervasively and easily while continuously optimizing network services as per the ever changing demand and infrastructure conditions. The SDN application intelligence is derived from the existing Radware ADC and security product logic expanding the network services to exist throughout the network by injecting service intelligence into the SDN.

Via this transformation, the network services offer far greater scalability than before, advanced automation options that better align network services with business application changes, and ultimately network services that can exist anywhere in the physical or virtual network supporting any tenant yielding improved network and service engine utilization.

Effectively, through programming the SDN to forward certain traffic to certain ADC and security network services engines, the functions of the single devices can be disaggregated and selectively applied to flows that require these services. Classification of candidate flows, matched against candidate services can either be policy driven or dynamic throughout the lifecycle of the session. As previously stated, the Radware SDN applications transform network services from point devices to pervasive network wide services.
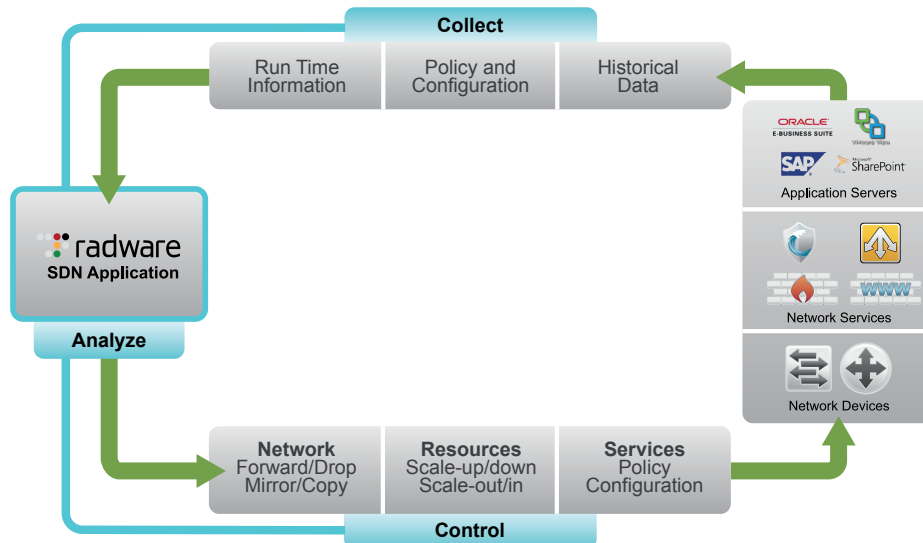
Figure 4: Radware SDN applications closed loop optimization cycle

As illustrated in the diagram above, Radware SDN applications operate through a closed loop optimization cycle in which they constantly collect, analyze and control network services. Information about the network and business applications is collected from different sources; (1) the configuration and policies, (2) the historical information such as logs and (3) the real-time monitoring information. The availability and security metrics of this information are continuously analyzed as per the relevant SDN application according to the network service policy. Ultimately the SDN application either automates or suggests to the network operator, based on the application decision engine, a control action pertaining to network traffic forwarding and service configuration or capacity modification in order to improve service, security or resource utilization.

Summary

To summarize, Radware SDN applications in conjunction with its physical and virtual ADC and security appliances significantly change the way network services are implemented and managed and thus enable networks to deliver increased value through the following capabilities:

1. Injecting application intelligence to the entire network by utilizing the centralized SDN control and the distributed data plane architecture.

2. Automatically scaling in and out security and ADC service engine deployments by controlling SDN traffic distribution per application and compute infrastructure demand.

3. Provide a new architecture that blends application delivery and security into the network fabric in a manner that is not possible using contemporary network technologies.

4. Efficiently and economically utilize application delivery and security resources anywhere on the network (centralized or distributed) by uniformly programming the network and service engine resources to optimize network forwarding functions for intelligent network services delivery.

The following diagram illustrates the ability to intelligently blend services into the network.
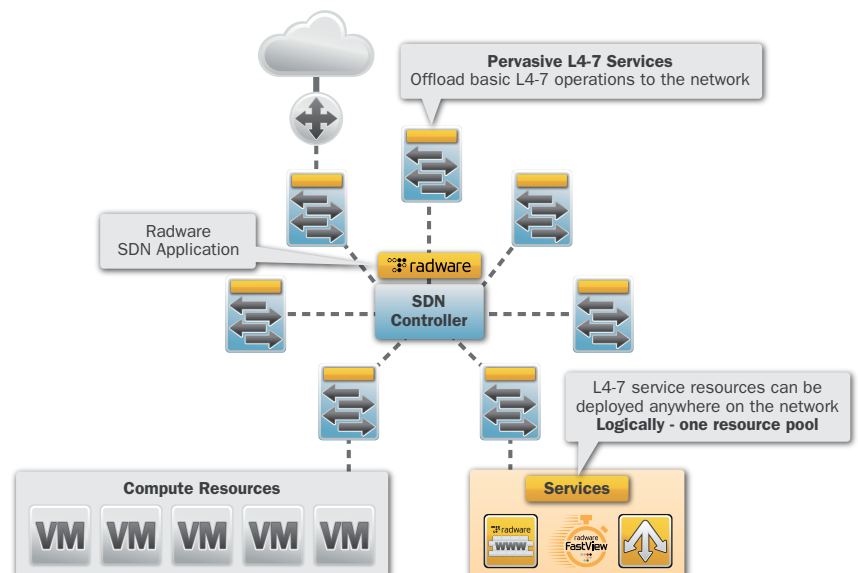

Figure 5: Pervasive network service architecture

Leveraging the blended services framework on top of SDN, Radware is naturally working to build SDN applications that will improve organizations ability to build the following network functionality:

1. Detection and protection from DDoS attacks at the network level – Radware has announced its first SDN application, DefenseFlow that in conjunction with DefensePro and SDN enables organizations to improve scalability and accuracy of the attack mitigation network service.
2. Dynamically scale out network services – as compute infrastructures elastically align with seasonal application demand, network services should align accordingly. Building a framework to elastically scale in and out Alteon ADC, FastView acceleration and AppWall WAF is a natural SDN extension.
3. Improving the scalability of application traffic steering – as demand for application context based traffic steering increases, the consolidation of the classification intelligence residing in the ADC appliance and with the scalability and programmability of the SDN enable efficient utilization of network and service engine resources and offer greater capacity.
4. Site selection optimization – handling end user requests for multi datacenter application deployments in an optimal manner helps improve application QoE and intelligently leverages SDN.

Key Benefits

The key customer benefits from the Radware SDN network service infrastructure are:

- More intelligent application delivery and security decisions throughout the network break existing network barriers when developing business applications. Every application everywhere is entitled for advanced services.
- Simpler implementation of network services allows improved operational efficiency of network management alongside application changes. Not every project needs to become a networking project.
- Lower overall network service solution costs – as network service delivery is partially offloaded to the SDN, there is no need to invest in excess network service appliances and capacity. Deploy network services as needed, and use by many tenants and applications throughout the datacenter.
- Greater scalability – scale your network services throughout the network. No more limited areas are protected or load balanced. Offer uniform services throughout the SDN.
- Easier operation – changing and managing security and ADC functionality becomes simpler as the deployment operates as if it is centralized. Not only does SDN streamline network operations, but Radware SDN applications streamline network service operations.

Learn about Radware's DefenseFlow™ the first in a suite of Software Defined Networking (SDN) applications that leverages SDN technologies to provide DoS & DDoS protection as a native network service. DefenseFlow proactively defends against network flood attacks and automates provisioning of an attack mitigation service.