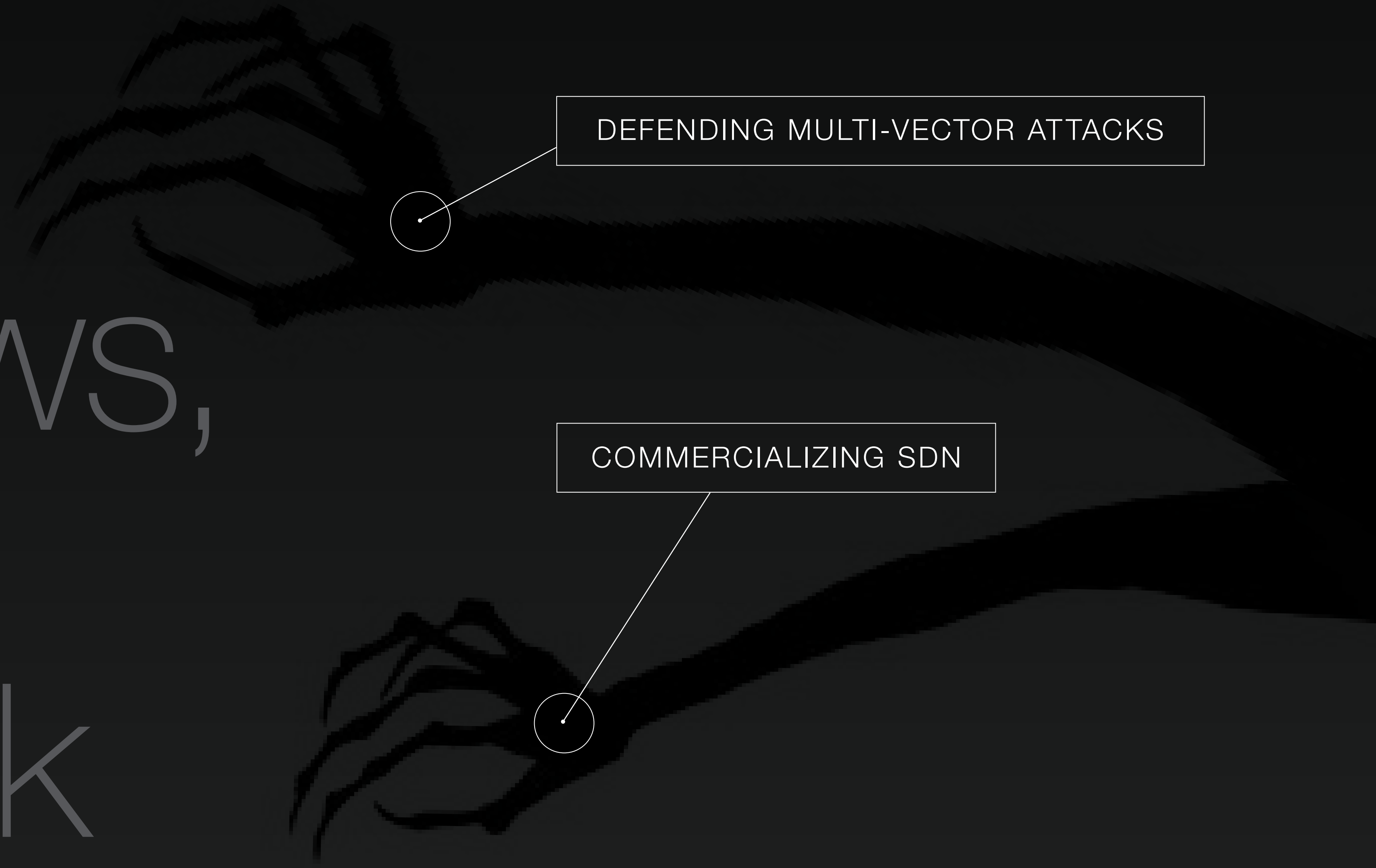
Taking advantage of SDN services to intelligently automate network security

How to monitor and mitigate application and volumetric attacks with software driven policies

Two Shadows, One Network



DEFENDING MULTI-VECTOR ATTACKS

COMMERCIALIZING SDN

Your network hums along every day, delivering crucial services to enterprises and individuals. But, you can sense the menace of not just one — but two — shadows hanging over your network. One threatens to cause harm and can go unseen. The other hangs in the background, eager for your attention.

The threatening shadow is the increasing number of high profile, sophisticated attacks on carriers' networks.

Carriers are on guard for DDoS attacks at the network layer. Because there's a troubling blind spot in legacy network security solutions, hackers can get in through Layers 4–7, the application layers. Application attacks deploy multiple vectors, honing in on specific applications or functions by mimicking legitimate user traffic with the intent to cripple network functions or gain access to digital assets.

Learn more. Application attacks put carriers' networks and reputations at risk.

Find out more about the impact of application attacks and how to stop them in Radware's new eBook.
"How do you stop what you can't see?:
The Imminent Threat of Application Attacks
and How to Defend Against Them"

COMMERCIALIZING SDN

The second shadow is the pressure to move your software-defined networking (SDN) strategy from the white board to proof-of-concept trials to commercialization. SDN promises to revolutionize how networks are managed and provisioned with dynamic, automated centralized controls. But, SDN silos and proprietary SDN controllers from multiple vendors can make it difficult to manage security network wide from your SDN control plane.

SHINING A LIGHT ON THE SHADOWS

The good news is there's a solution that easily fits in your SDN architecture and provides clear value, to automate control of security for the entire network, monitoring and mitigating application and volumetric attacks in real time.

> *Shadows are lurking. Now is the time to shine a light on them by adding automated security detection and mitigation when planning and rolling out SDN.*

01 The Opportunity: Network Automation and Intelligence

It's a matter if when — not if — carriers deploy SDN and related services. The benefits are just too compelling. According to the Open Networking Foundation, "SDN is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications."

To meet the challenges caused by the explosive growth of video, mobility and cloud services, carriers are adopting open and programmable network architectures that increase business agility and lower costs. Cyber attackers, however, exploit the growing attack surface presented by open and new services. Legacy security approaches are insufficient in dealing with new type of attack techniques and targets.

Carriers like AT&T and NTT are already implementing SDN capabilities to reduce costs and more flexibly manage services.

THE SDN ADVANTAGE

An SDN architecture provides an intelligent central console that decouples the network control plane from the forwarding plane. This enables carriers to meet two critical business objectives:

1. Leverage network-wide intelligence to create more valuable services, and
2. Automate the manually intensive task of provisioning, operating and troubleshooting hardware intensive networks and compete like a cloud provider with a flexible software-defined data center (SDDC) model.

Global control of the network eliminates the need for manual interfaces into network equipment with programmable interfaces. Tasks such as configuration and policy management can be automated. This saves time and money.

The network can also automatically respond to changes in network behavior. This enables a learning network where carriers can now better harness the plethora of data they have to improve performance and customize service offerings in ways that would have been impossible to do manually.

AUTOMATION LEADS TO DRAMATIC RESULTS

Thanks to a software-based architecture in more than 100 markets, AT&T reports a 95% improvement in the time it takes to provision enterprise services. The carrier cites the automation of ordering, provisioning and management capabilities as the key reason.

AT&T Leads the Way

AT&T is widely recognized as a leading advocate of SDN. The carrier plans to have a 75% software-centric network by 2020.

In 2013, the company published an AT&T Domain 2.0 Vision White Paper that spells out much of its technology vision, including a "revised architecture that borrows from cloud technologies and suggests adding domains to our program that will allow for rapid innovation, new business models, greater customer value, greater opportunities for third parties to participate in the customer value chain and an increased choice of suppliers."

SDN AND NETWORK SECURITY

By separating the control and data planes, SDN is not limited by physical devices to control and manage traffic flows. With no physical barriers, SDN controllers can monitor traffic, detect threats and mitigate attacks anywhere in the network with the use of a software-based network security solution. The challenge is how to bridge the silos of multiple vendors' SDN controllers to work together in the carrier's SDN control plane.

According to Patrick Donegan, senior analyst for Heavy Reading, SDN facilitates a

> *"network wide, software driven policy environment that enables either a uniform delivery of security throughout the network, or more granular, fine-grained delivery per application, service or both."*

ESG Research recently asked enterprise security professionals to "define the most attractive uses cases for SDN-enabled network security." Responses include:

- "Selectively blocking malicious traffic from endpoints while still allowing normal traffic flows."
- "Automate network security remediation tasks"
- "More granular network segmentation for network security."

SDN Basics

For a more detailed explanation of SDN and its architecture framework, visit SDX Central's *"What's Software-Defined Networking (SDN)?" page.*

SECURITY IMPACTS OF SDN

Phase	Exiting Security Capabilities	New Security Capabilities
Pre-SDN	Vendor-specific capabilities are “baked” into the forwarding plane. Difficult to coordinate on a network-wide basis.	Service introduction may necessitate software or hardware upgrades on the forwarding plane.
SDN	Vendor-agnostic. No linkage to the vendor forwarding plane, supports a common security policy approach. Well suited to agile, network-wide implementations	New security capabilities are designed to be implemented network-wide without provisioning additional hardware or software on the forwarding plane.

Source: *“Service * Security Agility Strategies for SDN & NFV Network,” Jim Hodges, Heavy Reading*

NTT’s Take on Security and SDN

Interview with Patrick Ng, EVP, NTT Communications America

“Global infrastructure attacks are becoming more distributed and diffused. Denial-of-service attacks have become an alarming threat to the largest networks in the world. From the survey we commissioned from Ovum, [we learned that] half of the respondents (49%) saw security as their top investment area. We understand their concerns, and [we are] determined to help enterprises mitigate these threats by providing secure, reliable and robust network services.”

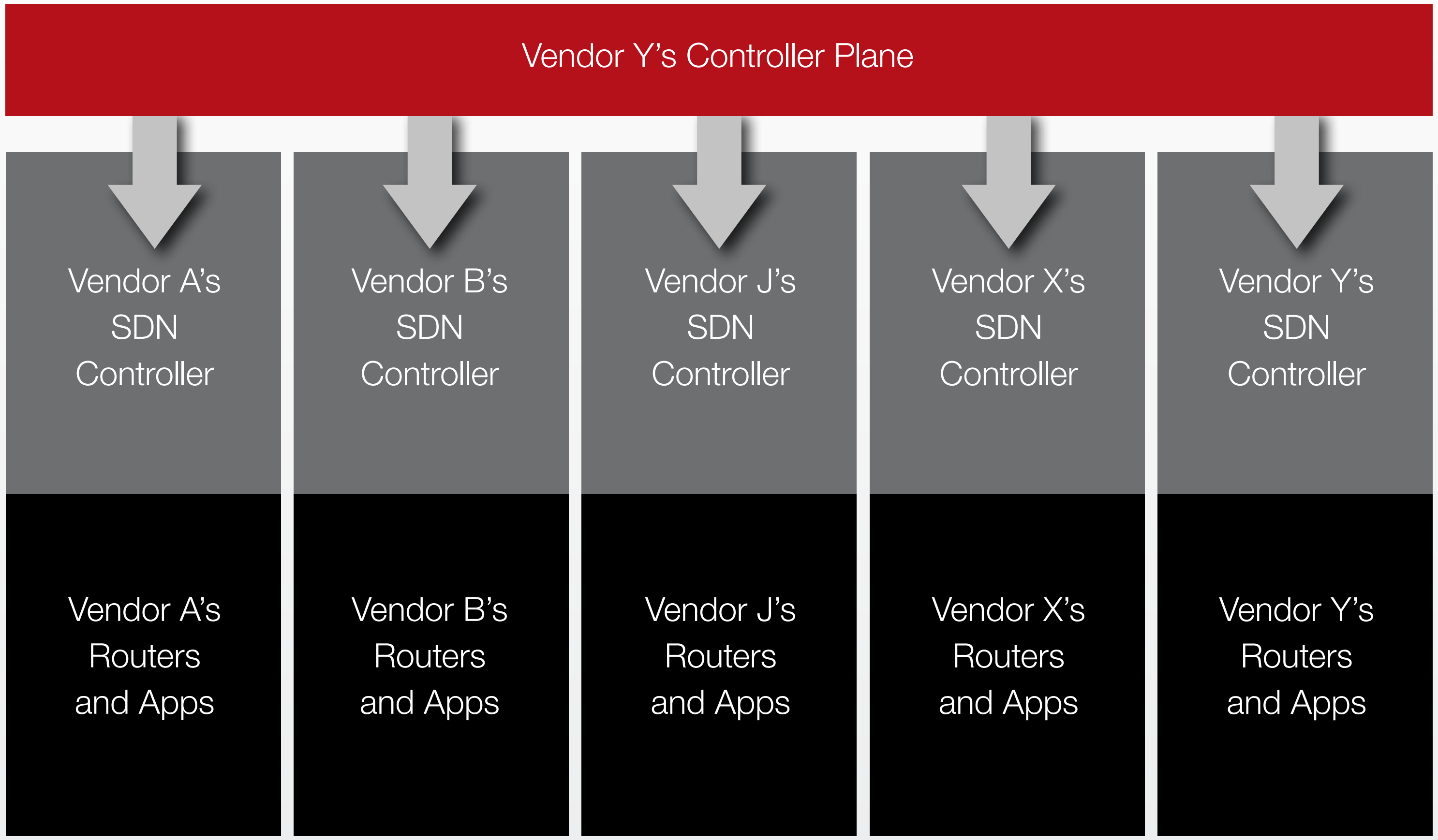
radware

02 Silos of SDN

SDN decouples management of the network from its hardware elements and applications.

Best practices dictate that network architectures use equipment from multiple vendors to provision SDN-enabled services so you're not beholden to one company for everything. But in current implementations, this scenario creates "Silos of SDN" requiring each vendor to provide an SDN controller that communicates with the carrier's central SDN control plane.

Silos of SDN


Vendor Y's Controller Plane
Vendor A's SDN Controller
Vendor B's SDN Controller
Vendor J's SDN Controller
Vendor X's SDN Controller
Vendor Y's SDN Controller
Vendor A's Routers and Apps
Vendor B's Routers and Apps
Vendor J's Routers and Apps
Vendor X's Routers and Apps
Vendor Y's Routers and Apps

As part of the SDN network architecture, every vendor today provides an SDN controller that feeds data to the carrier's SDN control plane. In this scenario, network security is managed by security operations engineers and does not take advantage of the automated network wide capabilities of SDN.

A MISSED OPPORTUNITY

Because each vendor’s controller feeds directly to the SDN control plane, it can be a challenge to seamlessly manage security across the entire network. Security operations engineers must still monitor each vendor’s routing tables and mitigate attacks manually. The carrier misses out on the promise of SDN to fully automate network defense functions and create globally enforced policies.

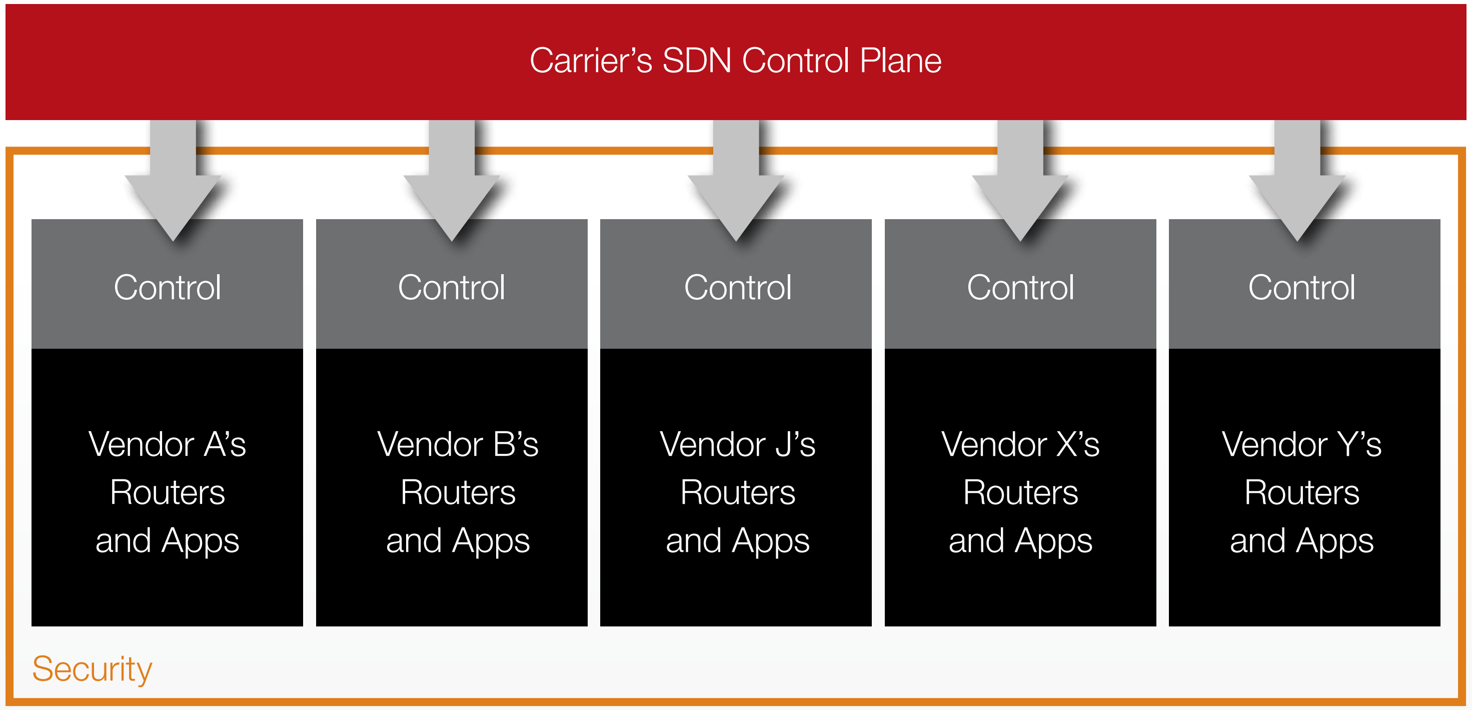
OPPORTUNITY COSTS

Missing out on automation benefits isn’t the only downfall to maintaining an old siloed security model in an SDN architecture:

- The network is still exposed to Layer 4–7 application attacks that are not detected by legacy security systems.
- Operating expenses are higher.
- Legacy security systems and manual attack mitigation are prone to more errors.
- Security operations engineers are diverted from developing potential new revenue-producing services.

03 Lifting the shadow

As carriers plan and deploy SDN architectures, it's important to consider how to bridge the "Silos of SDN" that feed data to the SDN control plane. With the right solution, carriers can get automated control of security across the entire network.


Carrier's SDN Control Plane
Control
Control
Control
Control
Control
Vendor A's Routers and Apps
Vendor B's Routers and Apps
Vendor J's Routers and Apps
Vendor X's Routers and Apps
Vendor Y's Routers and Apps
Security

The key is uniting information about attacks or security issues from all vendors' equipment in one automated control center. This capability requires incorporating a single security solution in the SDN architecture that interoperates network wide with the SDN controllers that feed data from various vendors' router and applications to the SDN control plane.

ALL FOR ONE

With multi-vendor interoperability and the ability to accept telemetry from multiple disparate sources, the right network security solution provides one automated control center for the entire network. As a result, security operations engineers can focus on higher value tasks: identifying future security threats and trends and developing potential next generation revenue-generating services.

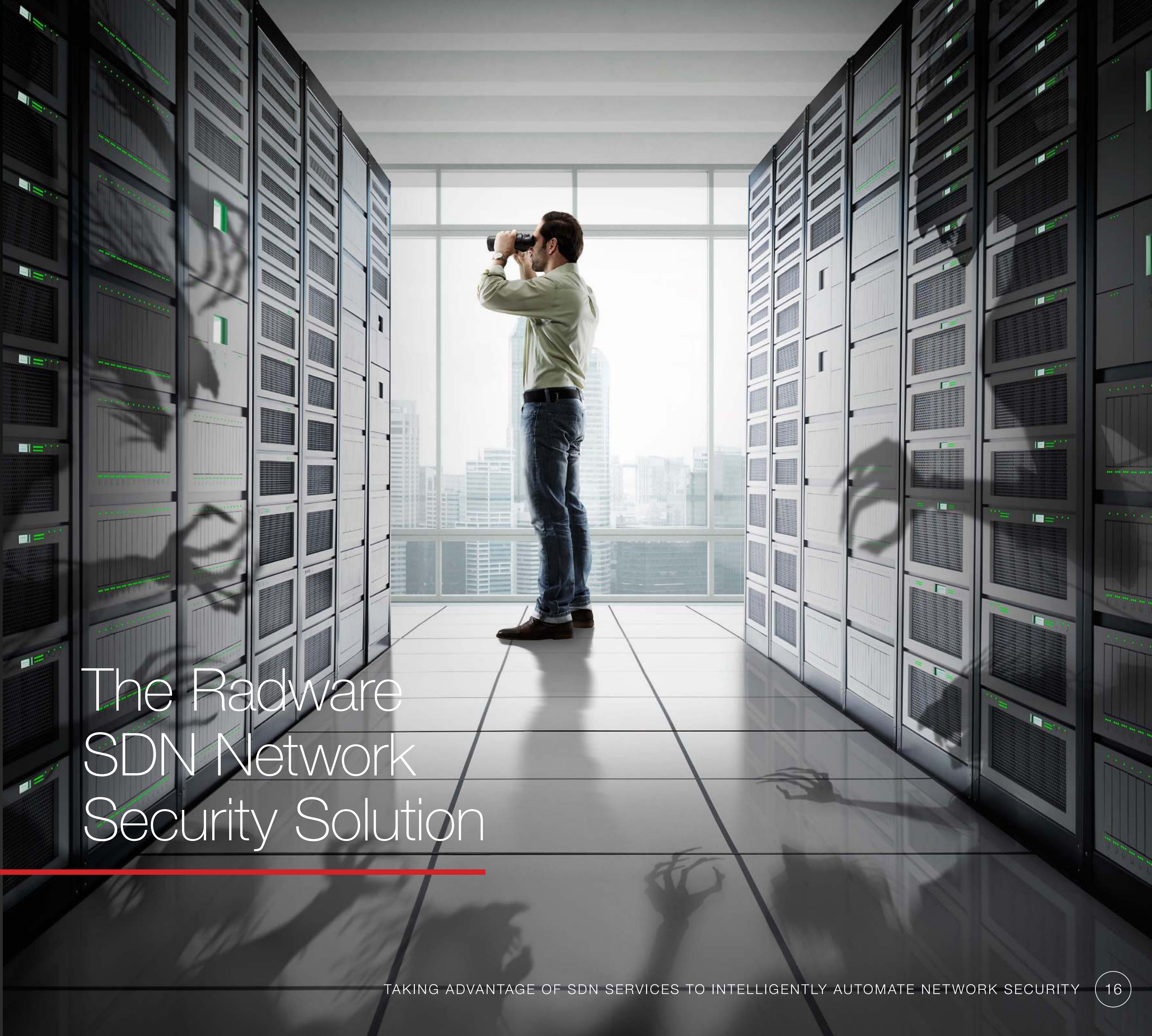
Now, the network security solution can take advantage of the programmability of SDN to proactively provide better protection for the entire network at the least cost and provide previously unachievable network agility.

AUTOMATION = FLEXIBILITY

Rapid response to threats is the main line of defense to stop attacks. Automation enabled by SDN enables carriers to define "best fit rules" for their networks to mitigate security threats in real time without manual intervention. For example, carriers can define rules that in real time under attack implements a fine grain filter that routes suspect traffic to a mitigation center for further analysis/scrubbing, or sets an ACL rule on an edge router to prevent an incoming threat based on a specific set of criteria.

BIG DATA FOR BETTER ANALYTICS

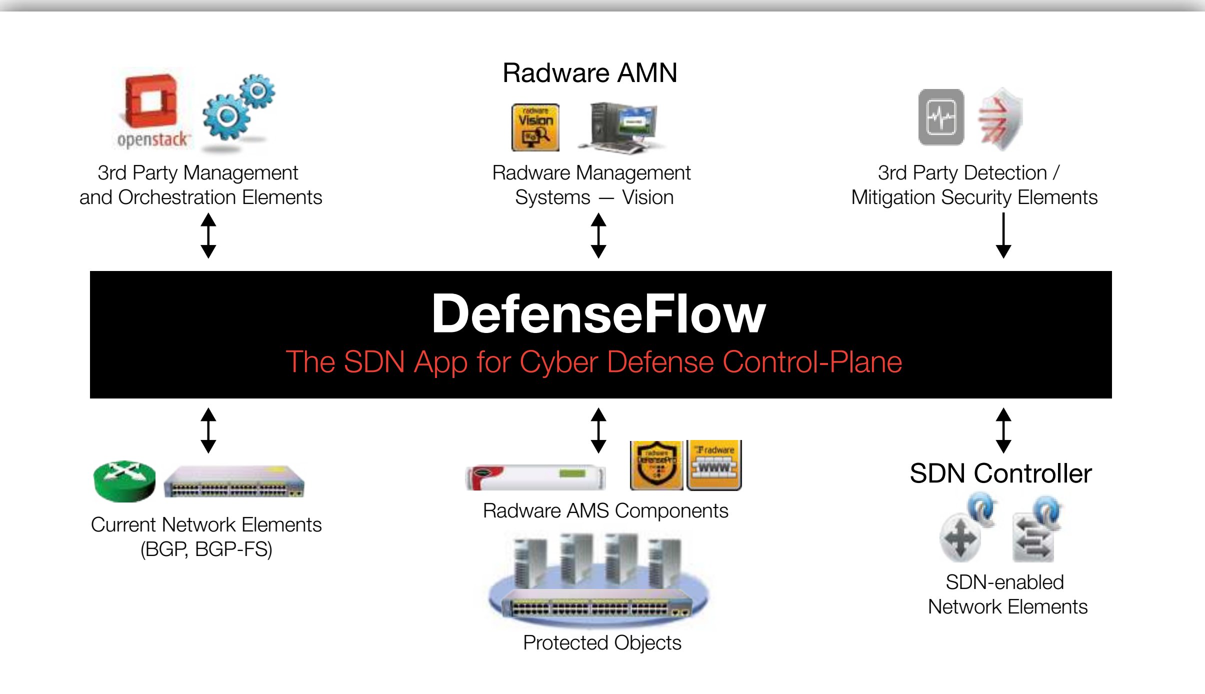
With a network security solution that analyzes disparate telemetry from multiple interoperable network domains, carriers are able to derive more intelligence from any or all network elements and applications. By analyzing the data, carriers can be more predictive about potential attacks and stop the most complex network assaults as or even before they happen.



04 The Radware SDN Network Security Solution

Radware's DefenseFlow should be part of your SDN architecture to provide the intelligence needed to analyze network-wide telemetry from multiple sources and quickly perform optimal mitigation based on automated network policy rules.

DefenseFlow is a software product that leverages network technologies to provide attack mitigation as a native network service. It is the first SDN application that programs networks for DDoS security and it provides network-wide mitigation services and defense against any DDoS attack in real time. DefenseFlow operates on open standard controllers in any SDN-enabled network infrastructure. DefenseFlow analyzes telemetry from Netflow, Openflow, SDN controllers, or any third party input supported by OpenDaylight.


openstack
3rd Party Management and Orchestration Elements
Radware AMN
Radware Management Systems — Vision
3rd Party Detection / Mitigation Security Elements
DefenseFlow
The SDN App for Cyber Defense Control-Plane
Current Network Elements (BGP, BGP-FS)
Radware AMS Components
Protected Objects
SDN Controller
SDN-enabled Network Elements

Radware DefensePro improves the speed and quality of volumetric and application attack detection by accessing telemetry points from network elements from multiple vendors throughout the network up to layer 7.

DefenseFlow can also migrate existing Netflow deployments to SDN utilizing DefenseFlow Flow Collector for statistics collection and traffic diversion operations. This enables Carriers to implement hybrid modes such that migrations from traditional Netflow to SDN-based deployments can be seamlessly completed.

THE POWER OF AUTOMATION

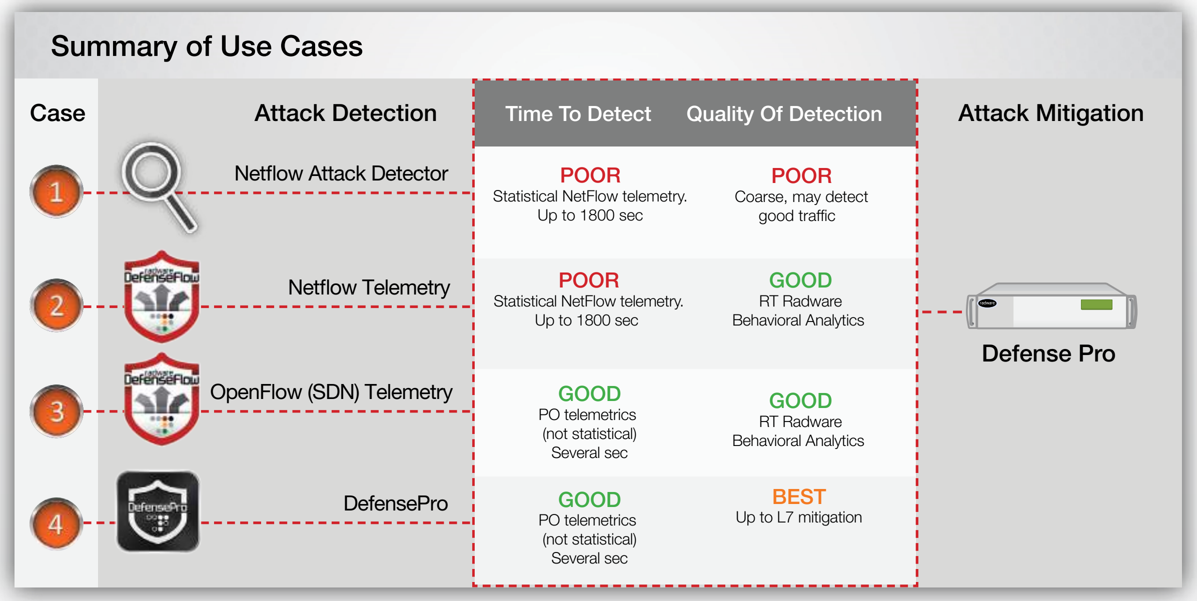
Rapid response to attacks based on pre-configured policies is the best way to stop threats before they cause damage. It's the main benefit of automating an SDN-enabled security solution to protect your network.

With DefenseFlow, all telemetry flows to the SDN application where traffic is automatically analyzed. The network is essentially self-healing because if issues are detected, DefenseFlow mitigates threats based on preconfigured policy rules. Attacks are handled at a finer, granular level because "best case rules" determine how they are mitigated.

By eliminating the need for manual intervention, operating expenses are reduced and manual errors are a thing of the past. Security Operations Center (SOC) engineers can finally move from reactive firefighting to proactively innovating better security processes and architectures

FASTER IS BETTER

Currently, most carriers' telemetry inputs are predominately NetFlow. DefenseFlow interoperates with NetFlow to leverage your investment. As networks evolve, OpenFlow is a better choice because it provides faster and more granular access to flows. DefenseFlow easily supports the migration to OpenFlow, enabling carriers to offer tighter Service Level Agreements to enterprise customers for faster detection and mitigation.



Summary of Use Cases

Case	Attack Detection	Time To Detect	Quality Of Detection	Attack Mitigation
1	Netflow Attack Detector	POOR Statistical NetFlow telemetry. Up to 1800 sec	POOR Coarse, may detect good traffic	Defense Pro
2	Netflow Telemetry	POOR Statistical NetFlow telemetry. Up to 1800 sec	GOOD RT Radware Behavioral Analytics	
3	OpenFlow (SDN) Telemetry	GOOD PO telemetrics (not statistical) Several sec	GOOD RT Radware Behavioral Analytics	
4	DefensePro	GOOD PO telemetrics (not statistical) Several sec	BEST Up to L7 mitigation	

Radware DefensePro expands network protections by detecting application attacks through Layer 7.

EXPANDING DEFENSES TO APPLICATION LAYERS

Legacy security solutions primarily use Netflow telemetry to detect volumetric attacks. But, we know multi-vector attacks also target application layers. In conjunction with Defense Flow, Radware DefensePro taps all telemetry inputs in the network to detect and mitigate both volumetric and application attacks. DefensePro offers hardware-based and virtual options to leverage any architecture in your network today to enable network wide automated security defense powered by your SDN control plane. DefenseFlow can operate with DefensePro deployed in any of the following use cases:

- Always On Carrier Cloud – DefensePro works in the cloud as an always-on defender against application level attacks. If DefensePro detects an attack, it issues a real-time signal to the DefenseFlow SDN application for automated mitigation.
- Enterprise CPE – DefensePro works at the enterprise location to monitor for application level attacks and communicates with the DefenseFlow SDN application for automated mitigation.
- Virtual Network Detection – Virtual DefensePro runs on white box servers. Virtual detection points are deployed around the network that do not require hardware and provide superior information to NetFlow or Open flow telemetry points. Virtual DefensePro can be operate anywhere in the network to continuously review traffic from Layer 2-3 through layer 7 to detect volumetric and application attacks.

The result is a much better, richer source of network and application data from which the SDN control plane makes fast, optimal, automated mitigation decisions to protect the network at all layers based on predefined policies.

BANISHING TWO SHADOWS WITH ONE SOLUTION

With its superior detection and mitigation capabilities, DefenseFlow offers investment protection that supports legacy NetFlow telemetry, as carriers migrate to Openflow and SDN. Carriers now have the ability to fully automate the operations of the network security solution and to leverage network wide intelligence to offer superior real time protection of traffic flows with previously unrealizable network speed and agility.

For more information, visit Radware DefenseFlow radware

About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for carriers, virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down.

For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.