Security-Centric SDN (Software Defined Networking)
Table of Contents

A New Approach to Implement Network Security That Works! .......................... 4

Security—The Need Never Sleeps ........................................................................ 4

Defense in Depth .................................................................................................. 5

What’s Wrong with Existing Solutions? ............................................................... 5

The Deepening Crisis .......................................................................................... 6

SDN: A Solution Whose Time Has Come ........................................................... 7

Next-Generation Security Plus SDN = Security-Centric SDN ............................ 7

Separation of monitoring and security enforcement elements ........................ 8

Total visibility ........................................................................................................ 9

Simplified architecture of the security infrastructure ......................................... 9

Leveraging the industry’s best-of-class solutions ................................................. 9

Easy or automated provisioning .......................................................................... 9

A New Dimension of Effectiveness In Network Security .................................... 10

Visibility Enables Vigilance ................................................................................ 10

Security-Centric SDN: A Scalable, Cost-Effective Security Architecture ............. 11
A New Approach to Implement Network Security That Works!

Today’s networks are waging a ceaseless battle against an army of ingenious and fast-evolving threats. Companies—as well as entire nations—must be well-provisioned to deploy a quick, decisive and network-wide response to attack. While the nature of this conflict has not changed much from the early days of the Internet, what has changed is the intensity and number of attacks, the damage they inflict, and their widening compass. We need a new paradigm for ensuring successful deployments of counter-attack solutions: Security-Centric SDN. Net Optics has originated this concept to help organizations marshal an agile, effective response to the changing needs of data centers and converged environments.

Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace. We rely on a vast array of networks to communicate and travel, power our homes, run our economy, and provide government services. However, despite research, new systems and major security investments, these cyber intrusions and attacks are climbing dramatically—exposing sensitive information, disrupting critical functions and imposing high costs on the economy.

When it comes to national security and infrastructure, the stakes are even higher: Confidential defense data, economic progress, and even the physical safety of populations are put at risk by a weak or outdated security infrastructure.

Cyber attacks from “hacktivist” groups, crime syndicates, nation-states and others are now so insidious and sophisticated that perimeter defenses and other point solutions no longer suffice. Organizations need new, digital age technologies plus a cybersecurity posture that remains ahead of emerging threats. These critical goals require a holistic framework that embraces the entire enterprise—human capital, governing policies, management, and operations.

Current defenses, however comprehensive, are losing ground. Organizations can protect themselves only with tailored solutions that include dynamic security programs and a proactive workforce to quickly identify and address specific vulnerabilities.

This ebook begins with a brief overview of the crisis, explaining why existing security solutions have not kept up with bandwidth and protection demands. Ongoing assaults call for multiple security systems working together and providing forensics capability. The technology they rely on must be compatible, scalable and future-ready. Now, the power and ingenuity of the swiftly adopted Software-Defined Networking (SDN) concept allow us to introduce new options and resources for anticipating threats, responding instantly or even proactively to attacks, and keeping the network efficient and healthy.

Security—The Need Never Sleeps

Security more than ever demands “Defense in Depth”—a critical new approach that keeps the network ahead of proliferating threats. Defense in Depth calls for multiple security systems working together and delivering instantaneous feedback for conducting forensics. What are the components for successful deployment of Defense in Depth? We’ll explore that now.

Defense in Depth strategies combine, cascade and join multiple security solutions to work
in concert transparently. They are gaining substantial attention from major vendors. Each component of this solution addresses specific risk factors and attack vectors. Network Packet Brokers (NPBs) help to create the fundamental architecture of Defense in Depth, as they work to integrate multiple products and systems seamlessly, to unify this new paradigm in security. Once united using NPBs, multiple products can focus their combined strengths upon an attacking entity. This is the most effective way to provision the network with an advanced, available and agile defense.

**Defense in Depth**

Critical Network Protection Strategy

Defense in Depth is a robust military strategy whose principles support Cybersecurity. Multiple levels of protection, layered into an IT system, respond instantly and effectively if a security control fails or a vulnerability is breached.

Defense in Depth employs:

- Lifecycle redundancy
- Synergizing of people, procedures, technology and physical security
- Tactical delays to buy time to respond
- System-wide protections, procedures and policies

A Defense in Depth architecture includes deployment of multiple security solutions including, but not limited to:

- Anti-virus software
- Authentication and password security
- Biometrics
- Firewalls
- Intrusion Detection Systems (IDSs)
- Logging and Auditing
- Packet filters
- Physical security
- Timed access control
- Security awareness training
- Virtual Private Networks (VPNs)
- “Sandboxing”

Defense in Depth fortifies reliability while reducing the impact of a breach.

**What’s Wrong with Existing Solutions?**

There is no argument that network security threats are bounding ahead of defenses in complexity, scale and scope. Ideally, Defense in Depth should be a robust, strategic initiative, but today’s security deployments are too often tactical and ad hoc “best effort,” leaving networks at risk and architectures increasingly complex.
In an environment of intense market competition, companies must attain the agility to handle crises and threats. This calls for a fresh perspective on infrastructure and operations offering comprehensive visibility if organizations are to respond proactively and neutralize these threats, or repair the network before serious damages accrue. It’s essential to harness application intelligence and visibility tools to bolster network security and build a strategic response to growing challenges.

**The Deepening Crisis**

**Critical Network Protection Strategy** A quick review of two authoritative security reports, the CheckPoint 2013 Security Report and the Verizon 2013 Data Breach Investigations Report reveals the expanding scope of cybercrime:

**CheckPoint 2013 Security Report:**

- 63% of the organizations investigated in their research were infected with Bots. Once every 21 minutes a Bot is communicating with its command & control center.
- In 2012 more than 5,000 new ways emerged for hackers to cause damage and access systems—and there are still more undiscovered vulnerabilities.

**Verizon 2013 Data Breach Investigations Report:**

- Approximately 70% of breaches were discovered by external parties who then notified the victim—suggesting that internal detection capability is lacking, not widespread, or both.
- 92% of breaches were external—and more than half of those were tied to organized crime groups committing spamming, scamming, payment fraud, account takeovers, and identity theft.
- 47,000+ security incidents were conducted by malicious insiders.
- Hacking constituted 52% of breaches, the Internet enables many hacking methods to be highly scalable, automated, and conducive to anonymity.
- 29% of breaches were social, taking advantage of human nature, such as sending a convincingly crafted malware-laden e-mail to a few key recipients.
• The server network is the most compromised asset category by far over the past five years.
• Only 15% of breaches had a complete and reliable count of compromised records. That leaves the looming shadow of 85% unknown.

“Three-quarters of breaches are of ‘low or very low’ difficulty for initial compromise. It’s not surprising that none receive the ‘highly difficult’ rating. Would you fire a guided missile at an unlocked screen door?”

SDN: A Solution Whose Time Has Come

Software Defined Networking (SDN) allows organizations to add applications more easily, streamline processes, reduce complexity, improve efficiency and provide a better user experience.

In addition to security, SDN’s rapid adoption is driven by the desire to reduce capital expenditure (CAPEX) and operating expenditure (OPEX). SDN offers administrators an accurate view of network topology and usage, which can postpone or even eliminate an upgrade and reduce costs.

Analysts believe SDN has the potential to redefine networking. SDN centralizes and simplifies control of the network itself, increases agility and encourages automation. Plus, SDN keeps data centers abreast of advances in virtualization and secure cloud computing.

SDN also enables the automation and provisioning of monitoring applications and tools based on real-time traffic behavior. It encompasses end-to-end network monitoring with easy implementation and operation.

Now networks can change behavior instantly to respond to threat level, as opposed to implementing static behaviors that always respond similarly regardless of the challenge. Monitoring scenarios involving static configurations remain the same under attack or in “peace time.”

Next-Generation Security Plus SDN = Security-Centric SDN

With today’s data centers at the mercy of invisible threats, it’s essential to harness maximum application intelligence and visibility tools to increase network security and visibility, so that the network architecture itself enables a company to meet increasingly complex attacks. Since most companies operate a mixed architecture, Security-Centric SDN enables integration of multiple solutions’ capabilities in multi-vendor environments. This concept offers ingenious, cost-efficient ways to control burgeoning threats and respond with agility to fluctuating security needs.

For example, NetFlow, which is a general purpose protocol for collecting IP traffic information, can help quickly identify Distributed Denial of Service (DDoS) attacks. When used in the right context, NetFlow can trigger a network to dynamically execute proven defensive behaviors.
Communicated via the SDN controller, control messages can instruct the security device to send the traffic to a specialized tool, which removes the fake packets from the traffic stream, retains the legitimate packets, and returns the clean traffic to the server.

Another popular use case consists of changing the security devices’ modes of operation. This transition enables devices to optimally divert traffic through the most relevant security resources in the network—mitigating an identified risk only when needed.

Security-Centric SDN embodies five basic attributes, explained in more detail below:

- Separation of monitoring and security enforcement elements
- Total visibility
- Simplified architecture of the security infrastructure
- Leveraging the industry’s best-of-class solutions
- Easy or automated provisioning

**Separation of monitoring and security enforcement elements**

Security-Centric SDN separates network elements and security devices and enables automation and provisioning of monitoring applications and tools based on real-time traffic behavior. It permits end-to-end monitoring and improved security, complemented by ease of operation.

By uncoupling the security/monitoring/switch control from the data planes (the control plane decides where traffic is sent, while the data plane actually forwards that traffic to the selected destination), administrators gain tighter control of network traffic flow than ever before. With Security-Centric SDN, they can shape traffic with precision from centralized control consoles.

They can change rules to prioritize or even block packets—particularly beneficial in a cloud or multi-tenant environment. Plus, they can manage traffic loads using economical off-the-shelf switches and conduct switching across multi-vendor hardware and ASICs.
This capability also benefits cloud-based Infrastructure as a Service (IaaS).

Centralizing the control plane gives administrators new capabilities as well as the freedom and flexibility to introduce new applications without the inconvenience and complexity of configuring individual devices.

**Total visibility**

Efficient network monitoring is another benefit of the SDN revolution, promising far-reaching improvements. Security-Centric SDN allows the network administrator to examine the entire data stream by means of leveraging different platforms to work together. These create a complete picture of network activity, making it possible to identify problems down to the packet level, plus perform troubleshooting, identification and resolution.

**Simplified architecture of the security infrastructure**

Integrating multiple security devices to work together introduces many challenges, since each tool must be deployed in an in-line fashion.

This is because cascading tools or offering advanced configuration options like high availability or redundancy are all challenging—even at the physical level. How does one cascade multiple products to work together?

How can one ensure symmetric routing and switching in such an environment?

Using NPBs, it is possible to instrument an entire network, without changing rules. In the context of Security-Centric SDN, NPBs provide the basic infrastructure that makes this solution possible.

**Leveraging the industry’s best-of-class solutions**

Security-Centric SDN assures that best-of-class network security solutions work together, so one needn’t “trade” one solution for another. The ability to create this unified tool environment allows Security-Centric SDN users to combine their ideal security solutions in a way that also meets performance and redundancy needs.

Security-Centric SDN does not require deploying new security solutions. Such solutions can be added according to organizations’ threat and risk management programs.

**Easy or automated provisioning**

Automated provisioning reduces network complexity, as well as monitoring access rights and privileges to support security and user privacy. Such provisioning helps enable compliance and minimize vulnerability to threats. Network provisioning can be automated by leveraging open interfaces between the network and other IT systems. The SDN architecture enables provisioning of new services and delivery of applications in a dynamic IT infrastructure. Separating the network’s data and control planes provides interfaces or APIs which provision services automatically and immediately by means of software rather than device by device. The less manual configuration, the lower the risk of error—particularly in a highly dynamic environment.
A New Dimension of Effectiveness In Network Security

Previously, deploying network security solutions required networking changes in order to assure proper inspection of relevant traffic. Organizations needing multiple security gateways had to develop a highly complex routing and switching mechanism to forward various network streams to different inspection elements. When using a network switch, that switch’s proprietary firmware worked to guide packet forwarding—essentially treating all packets alike. Confidence in this approach was shattered by some spectacular and costly security failures.

These exposed an unpleasant truth: the network was actually a wide-open invitation to opportunistic threats. With adversaries constantly probing for weakness and mounting deadlier attacks, a company could not be too future-ready.

The new security paradigm demands separation of network elements, with automation and provisioning of security applications and tools according to real-time traffic behavior. Also needed is the ability to differentiate among packets and forward them to diverse—or even multiple—tools with precision.

Thus, SDN could not have arrived at a better time, moving the management and configuration of network routers from hardware into software and decoupling network control to the software application called a controller. With SDN, the decisions of where to send the next packet are not made by static routing protocols but by agile, flexible and responsive external applications.

Visibility improvements allow an administrator to view the network in its granular entirety. SDN provides a fluid, malleable and dynamic environment in which applications can be brought up, brought down, and moved where necessary, as well as changed and replicated on a more horizontal architecture.

Visibility Enables Vigilance

Visibility is vital to network security, decision-making and troubleshooting. Core business applications as well as social media services such as P2P networking and Facebook call for uninterrupted vigilance. With organizations operating worldwide and people constantly on the move, the need for total visibility cannot be overstated.

Not only is visibility key to ensuring optimal function and value for the organization’s tool investment; it’s also essential to managing threats proactively and staying ahead of those who would invade and damage the network. By joining networks and applications, SDN also enhances automation, network control and effective management, helping companies gain higher returns on their network investments.

The pre-SDN network is static and tightly coupled, with no modularity. Basically, users received everything that came with that box and could not “mix and match.” Proprietary, vendor-specific protocols determined (and limited) control. Visibility was confined to the network edge or to random monitoring of data that was easily viewable. This limited visibility became an increasing issue as applications grew more diverse and devices that accessed or hosted these applications grew more pervasive. Now, and going forward, visibility is absolutely critical to obtaining accurate information about the state of the network and the threats it faces.
Security-Centric SDN: A Scalable, Cost-Effective Security Architecture

Net Optics Security-Centric SDN provides a way to scale existing security and other monitoring tools without a costly overhaul. An organization achieves total network visibility and protection across the entire breadth and depth of physical, virtual, and private cloud environments.

This new approach separates network elements from security and monitoring devices, enables automation and provisioning of monitoring applications and tools based on real-time traffic behavior, provides end-to-end network monitoring and improves security, along with simplifying operation. Deploying Security-Centric SDN in data centers across the board is the next logical next step.

Security-Centric SDN marries an SDN controller with Network Packet Brokers (NPBs) and a customer’s chosen security solutions. NPBs, with their ability to “chain” solutions, integrate multiple systems, and distribute traffic, provide the ideal means for a dynamic response. Such chaining of security solutions supports and enables Defense in Depth. It embodies dynamic attack monitoring; the use of NPBs for traffic distribution; and use of the network controller for assessing the network, provisioning SDN, and reacting to network activity. Under attack, Security-Centric SDN enables administrators to send orders that redirect data to forensics tools to expose and analyze the attack.

Summary: The Importance of Creating an SDN Strategy

Today’s monitoring drawbacks include a static configuration, a high tool-per-monitoring-point ratio, SPAN port limitations, and limited attack blocking and prevention. In the face of spiraling attacks, there is an immediate, urgent need to adopt new methodologies and approaches to ensure visibility and to manage—not just across a single vendor’s SDN implementation, but across multiple deployments of many different systems. Security-Centric SDN offers a holistic, agile solution to the many security challenges that are now part of the networking landscape. Organizations can now leverage network progress for a robust defense and secure future path, even amidst rapidly mutating threats.

About the Author

Bob Shaw, President and CEO, Net Optics Inc.

As President and Chief Executive Officer of Net Optics since 2001, Bob Shaw is responsible for conceiving and implementing corporate vision and strategy to position Net Optics as the leading provider of intelligent access and monitoring architecture solutions in both physical and virtual environments. Under Shaw’s guidance, Net Optics has achieved consistent double-digit growth, launched more than 35 new products, acquired over 8000 customers, and expanded its global presence in over 81 countries. The company has been included in the elite Inc. 5000 list of highest performing companies three years in a row; won Best of FOSE honors; received the coveted Red Herring Top 100 North America Award for promise and innovation, the Best Deployment Scenario Award for Network Visibility, and many other accolades. Shaw’s leadership experience spans startups to Fortune 200 organizations, where he held Senior Vice Presidential executive positions. Shaw earned both a Bachelor of Arts degree in Business and a Bachelor of Science degree in Economics from Geneva College in Pennsylvania.