WHITEPAPER

big switch networks

Next-generation Data Center Visibility and Security:

DRIVERS AND BENEFITS

TABLE OF CONTENTS

OVERVIEW

Network owners must continuously monitor and secure the network to ensure its performance and integrity. But as the data center has evolved to accommodate cloud-native applications, increasing business velocity, pervasive cyber-attacks, and flat budgets, many are challenged to operationally and architecturally scale monitoring and security infrastructure.

Traditional methods of gaining visibility into the network—primarily through network packet brokers (NPBs)—are difficult to scale, create visibility silos, and require time-consuming, per-box management.

Today's data centers demand a next-generation approach to network visibility and security—one that allows them see every network, workload and location and to deploy, operate and scale faster, without increasing CAPEX and OPEX.

DATA CENTER FACTORS DRIVING NEXT-GENERATION VISIBILITY AND SECURITY

The factors influencing the need for next-generation visibility and security architectures are cloud-native applications, persistent cyber-attacks, increased business velocity, and stagnant budgets.

1. **Cloud-Native Applications:** The emergence of cloud-native applications, micro-services and containers has driven up east-west traffic within the data center, constraining existing network architectures optimized for North-South traffic. Increasing rack density and more workloads mean that data centers must scale monitoring and security coverage to match. To maintain application SLA and security, visibility and security solutions must be applied to every packet and flow in the data center—every rack, every location, and every virtual machine (VM), container, and cloud workload. Monitoring at scale and ensuring consistent policies for traffic from different sources is challenging in terms of both costs and operational complexity. Adding to the complexity are tool silos, which slow down troubleshooting and lead to visibility gaps.
2. **Persistent Cyber-Attacks:** The rise of cybercrime and attacks from state and non-state actors has created a permanent threat landscape. In response, network owners have adopted a pervasive security approach, requiring visibility across the data center and heightened vigilance in the DMZ. Active security measures that detect and block malicious traffic are increasingly important, as is speed of response.
3. **Business velocity:** The IT organization is expected to roll out services and applications on demand. Service delivery is often tied to SLAs and organizational policies, making speed of execution critical. Network and security teams are expected to deploy, scale and troubleshoot faster, but are constrained by traditional network monitoring components, such as NPBs, which need be managed manually, per box—a laborious, error prone process that slows service rollout and stunts innovation.
4. **Stagnant budgets:** Data center budgets have largely stagnated and are projected to remain flat in the near-term amidst political and economic uncertainty. Stagnate budgets create pressure on network and security teams to optimize capital expenditure and improve operational efficiency to accomplish more with existing resources.

In response to the confluence of these factors, today's data centers must operate smarter, faster, and more efficiently to ensure business competitiveness.

Traditional network monitoring and security architectures, which rely on NPBs to provide network visibility and traffic delivery, are unable to adapt to today's data center requirements. Instead, they pose as a barrier to network and security teams as they attempt to successfully monitor and defend the network, while controlling infrastructure and operational spend.

THE EVOLUTION OF NETWORK MONITORING

Network visibility approaches have historically determined the ability of network owners to scale network and security tools, as they determine the network visibility potential of each tool.

Prior to the introduction of NPBs, network-monitoring architectures used TAPs and SPAN (mirror) ports to deliver traffic to network and security tools. Tools were distributed and effectively static. Any change to a tool's view of the network required the tool to be physically redeployed. Tools were often over or undersubscribed, as TAPs and SPAN ports were not able optimize traffic specifically for each tool. Network migration from 1Gbps to 10Gbps and beyond placed further hurtles to enabling or maximizing tool performance. This deployment model eventually became untenable as networks grew in capacity and the number and type of tools used to monitor and secure the network increased.

TAP or SPAN-only architectures were the first-generation approach to network visibility, and they were eventually supplemented with smarter traffic delivery appliances—legacy NPBs.

SECOND GENERATION NETWORK VISIBILITY: LEGACY NETWORK PACKET BROKERS

Legacy NPBs allow multiple network tools to share access to the same network links—solving the problem of access contention that network owners experienced with SPAN ports and simple TAPs. They also act as intelligent optimization and delivery layers between the network and tools, allowing each tool to receive only traffic of interest, which ensures it operates at peak efficiency—neither over nor undersubscribed.

Most data centers deploying monitoring and security tools use legacy NPBs to deliver real time visibility into the network. Legacy NPBs offer granular control over how network packets are handled prior to offload to tools, and network and security teams can configure these changes remotely, as needed.

Packet handling functions considered standard across NPB vendors include: traffic aggregation, flow replication, L2–L4 filtering, tool load balancing. Some NPBs support additional, advanced functions that deliver more ingestible forms of traffic to tools or support inline tools. These include: deduplication, packet slicing, packet masking, header stripping, flow generation, deep packet inspection. In the DMZ, inline tool chaining has become necessary to deliver traffic, in series, to multiple logically inline tools. These capabilities have significantly enhanced monitoring and security architectures by reducing or eliminating irrelevant traffic to tools, which reduces the time needed to discover and address performance and security issues.

Unfortunately, due to the box-by-box design of legacy NPBs, the coordination of packet handling functions across multiple NPBs and across all connected network links and tools is complex, time consuming and prone to error.

Legacy NPBs operate as standalone appliances, where each one must be configured and managed individually (per-box). Tools connected to a legacy NPB only have access to traffic connected to that NPB, or else require a complex, manual configuration to route the appropriate traffic through multiple NPBs. Each tool is bound to the visibility potential of the physically attached legacy NPB. The result is fragmented visibility that is sensitive to network changes. If the network grows or its architecture is reconfigured, the tools may need to be physically reconfigured. Traffic is segmented by NPB, which creates rigid visibility architectures that are slow to change—impacting the ability of network and security operations to respond to performance or security incidents.

Some legacy NPBs support limited clustering, where multiple NPBs can be interconnected to expand traffic visibility to each tool; however, these clusters are complex to configure and manage and are limited in their ability to scale. They too can lead to visibility silos, as different groups of NPBs provide access to different selections of network links.

Because legacy NPBs promote silos, and are static, time-consuming to manage, and difficult to scale, they create challenges for data centers as they try to operate faster, more efficiently, and more cost-effectively. Siloed, static visibility increases management load, can lead to inconsistent implementation of monitoring and security protocols, and prevents network owners from achieving an overarching view of the network.

THE CHALLENGES LEGACY NPBS INTRODUCE TO DATA CENTERS ARE DETAILED BELOW:

LEGACY NPBS	DC MONITORING & SECURITY CHALLENGES	NEW REQUIREMENTS
STATIC DESIGN • Physically-bound, inflexible • Require manual or physical intervention to make changes to architecture	• Changes to tool views requires physical reconfiguration or manual, per-box management • Lack of resiliency increases risk of visibility loss/gaps	• Make changes on-demand, in software, without box-by-box management or physically reconfiguring / redeploying tools • Resilient design to ensure continuous monitoring
SILOED VISIBILITY • NPB-tool groups have different visibility profiles	• Visibility gaps • Inconsistent monitoring/security protocols • Time consuming to manage separate NPB/tool groups	• Persistent and on-demand visibility throughout the data center—every rack, location, VM, container, cloud
PER-BOX MANAGEMENT • Per-box functionality and management	• Slow, complex, error prone management • No automation/programmable workflows	• Single pane management • Easy to manage, fast to operate
PROPRIETARY HARDWARE • Expensive • Vendor lock in	• High CAPEX • Cost-prohibitive to scale	• Hardware choice • Subscription pricing

Legacy NPBs are preferable to TAP or SPAN-only designs, but as standalone appliances, they are still architecturally disadvantaged—which in turn disadvantages network and security groups as they deploy, operate, and scale data center monitoring and security.

Legacy NPBs, for the reasons outlined above, are an incomplete solution to the challenges of monitoring today's application-driven, security-centric data centers.

NEXT-GENERATION NETWORK VISIBILITY AND SECURITY

Today's data centers require intelligent, agile, and flexible monitoring and security architectures that provide pervasive visibility, single pane management, zero-touch scale, automation, and hardware choice. The capabilities of legacy NPBs are still required; however, the distributed, per-box design of legacy NPBs no long suits the data center, which demands solutions that can be operated quickly and efficiently.

Network owners need a dynamic solution that enables tools to have access to traffic from any rack, any location, any VM, any container, and any Cloud—and scale-out as needed—without physical reconfiguration or box-by-box management. Such a solution would simplify and accelerate change management and time to troubleshoot issues and mitigate attacks, while reducing OPEX and CAPEX.

A next-generation visibility and security architecture must be able to deliver the following benefits to the data center:

- See everywhere, across the organization (every rack, workload, data center, and site)
- Deploy, scale, and remediate faster and more efficiently
- Optimize OPEX & CAPEX

To deliver these benefits, what's needed is a visibility and security architecture that operates as one logical NPB enabling tools to be physically anywhere, but logically everywhere, so they can dynamically monitor and defend the network in real time. A logical "super-NPB," operating as a fabric, would also give network and security teams the single point of management needed to operate and scale efficiently.

To achieve this next-generation NPB architecture, hyperscale principles must be applied to legacy NPB functionality. By introducing a software-defined, controller-based, open-hardware design, data centers can gain a complete view of the network and a single point of configuration and management. This approach contrasts with the traditional, "old-generation" approach to network visibility—and network switching—where appliances operate box-by-box and architectures are rigid.

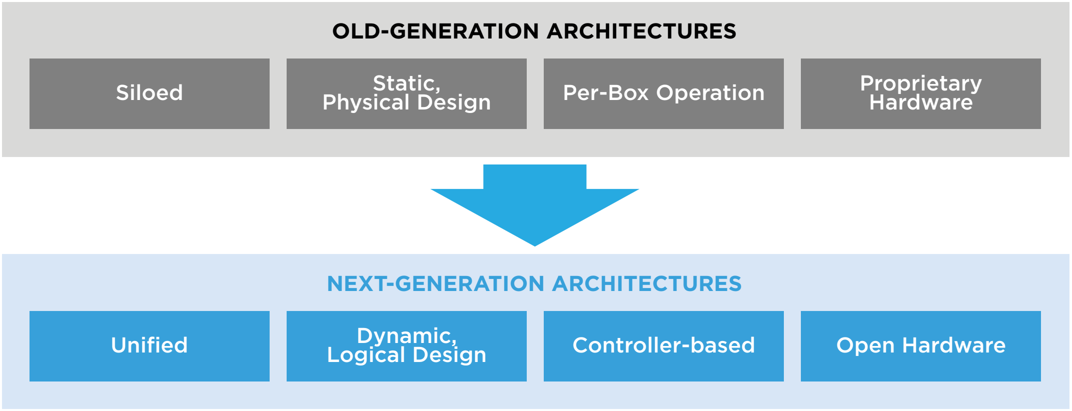
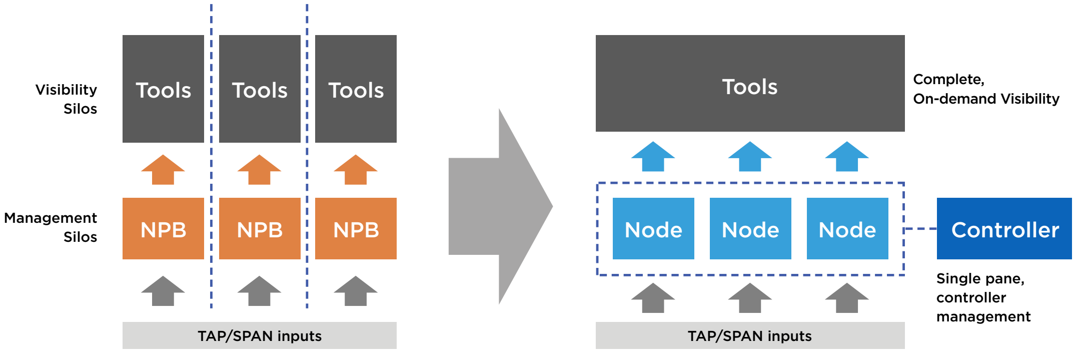


Figure 1: Old-Generation versus Next-Generation Architectures

Hyperscale design enhances visibility and security architectures. Rather than a proprietary, box-by-box architecture, a controller-based SDN fabric enables auto-discovery and configuration of visibility nodes, zero touch scale out, single pane management, built in resiliency, and hardware choice, allowing network and security teams to operate with greater agility and flexibility.



Simplified Traditional NPB Architecture

Simplified Next-Gen Visibility & Security Architecture

Figure 2: Legacy NPB versus Next-Generation Visibility and Security Architectures

Next-generation visibility is an advancement over per-box packet brokering. Standalone NPBs and limited clusters cannot provide a comprehensive view of the network. Instead, these legacy NPBs create pockets of visibility that are challenging to manage and often require tools be uprooted and moved if they need a different view or if there are changes to the network infrastructure. In contrast, next-generation visibility uses an SDN-model, where the underlying nodes are centrally controlled and can change their state dynamically, without physical intervention.

The key characteristics of hyperscale-inspired, next-generation infrastructure are intelligence, agility, and flexibility. Next-generation visibility and security architectures share these characteristics:

INTELLIGENCE	AGILITY	FLEXIBILITY
• SDN controller-based fabric (logical “super-NPB”) • Auto-discovery and configuration • Analytics and alerting	• Single pane management • Automation • Programmable integration • Zero touch	• Open hardware (vendor choice) • Subscription pricing • Scale out • Any workload, anywhere

These capabilities resolve the architectural and operational complexity of legacy NPBs, erasing visibility and management silos and accelerating operations.

A next-generation visibility and security architecture includes both software and open hardware components that can be leveraged to form a customized solution. Components of next-generation visibility and security architectures include:

FABRIC CONTROLLERS

Intelligent, software-based controllers redundantly operate and provide visibility into a fabric of visibility nodes, programming them from a single interface, and allowing configuration changes to be made across the fabric quickly, with limited interaction. A REST API enables the fabric to dynamically interact with tools and workflows, for automation of responses and tasks.

OPEN NETWORKING SWITCHES

Visibility nodes leverage commodity Ethernet switches for cost-effective visibility coverage that supports either inline or out-of-band deployment modes. Interconnected nodes, managed by redundant controllers, form a resilient fabric. None of the nodes need to be individually interacted with, as the intelligence of the fabric resides with the controller—not on-box. Network and security tool views only need to be set at the controller. Mapping of traffic through the fabric occurs automatically, without per-box configuration. In the event a node loses contact with the controllers, it would still be able to operate based on its last programmed configuration.

X86-BASED SERVICE NODES

Advanced packet handling functions, such as deduplication, and deep packet inspection, can be performed by x86-based service nodes. Any traffic traversing the fabric can be sent through the service node to perform desired functions for each tool. This design ensures that advanced packet handling functions are available to the entire visibility fabric, and thus every tool, regardless of where the traffic was accessed. Third-party service nodes (such as legacy NPB or SSL decryptor) could also be integrated with the fabric.

Together, these components can be deployed as simple, small-scale architectures or as large, multi-site designs.

ADVANCEMENTS OF NEXT-GENERATION VISIBILITY AND SECURITY OVER LEGACY NPBS:

LEGACY NPB	NEXT-GENERATION VISIBILITY AND SECURITY
STATIC DESIGN • Physically-bound, inflexible • Require manual or physical intervention to make changes to architecture	**DYNAMIC, LOGICAL "SUPER-NPB" DESIGN** • Make changes in software, on demand • Tools can reside anywhere
SILOED VISIBILITY • NPB-tool groups have different visibility profiles	**COMPLETE, PERVASIVE VISIBILITY** • Persistent and on-demand visibility throughout the data center—every rack, location, VM, container, cloud
PER-BOX MANAGEMENT • Per-box functionality and management	**FABRIC MANAGEMENT** • Single pane management / software-defined visibility
PROPRIETARY HARDWARE • Expensive • Vendor lock in	**OPEN HARDWARE** • Vendor choice • Flexible software pricing

Next-generation visibility and security offers architectural, operational, and business benefits.

For the Business:

- Faster service and application delivery
- Improved service and application availability
- Lowered OPEX and CAPEX

For the Network and Security Architect:

- Accommodates all tools (active and passive) and scales as needed across the global network, regardless of expansion or changes to the network or tools
- Improves tool efficiency and availability
- Reduces solution costs

For Operations:

- Automates tasks and programmatically integrates with tool or team workflows
- Accelerates change management
- Enables faster and dynamic responses to performance and security issues

NEXT-GENERATION VISIBILITY AND SECURITY USE CASES

Next-generation visibility and security enables a unified solution for the data center, so network owners can:

- **Monitor every rack**
- **Monitor every location**
- **Monitor 4G/LTE Mobile Networks**
- **Monitor every VM, Container, and Cloud Workloads**
- **Scale DMZ Security**
- **Dynamically Mitigate Attacks**

MONITOR EVERY RACK

Implementing a pervasive performance and security monitoring solution can be complex and cost-prohibitive at scale. With a next-generation architecture that employs commodity switches and intelligent controllers, network owners can gain easily manageable visibility throughout the data center at compelling price points.

MONITOR EVERY LOCATION

Next-generation visibility and security architectures can be extended across a WAN to enable monitoring of remote data centers and sites. This capability allows tools and operations teams to be centralized, which enables any tool to be leveraged across any traffic, while significantly reducing CAPEX and OPEX. Deploying commodity Ethernet switches at every data center and site enables a global view that covers every location—all centrally managed through the redundant fabric controllers.

MONITOR 4G/LTE MOBILE NETWORKS

Carrier networks often use tunneling protocols that may not be readable to certain tools. Service nodes within a next-generation visibility fabric can perform protocol stripping to enable ingestion by a wider array of tools.

MONITOR VIRTUAL MACHINE, CONTAINER, AND CLOUD WORKLOADS

Implementing consistent monitoring and security protocols across VMs, containers and cloud workloads can be challenging, particularly given that these workloads may be dynamic, short-lived, and produce only intra-host traffic. Delivering traffic from these workloads to a next-generation “super-NPB” fabric enables them to be monitored and secured alongside other network traffic, using the same or similar tools.

Rather than consume valuable host resources or pose a security risk, as with an agent-based approach, a next-generation “super-NPB” programmatically leverages virtual switch SPAN ports on the host to offload copied workload traffic. This design ensures that traffic is unobtrusively directed to tools.

SCALE DMZ SECURITY

Next-generation “super-NPB” security architectures offer a simple, scale-out method for deploying security tools in the DMZ and creating on-demand service chains. Their controller-based design enables integration with tools for rapid programming and response.

DYNAMICALLY MITIGATE ATTACKS

With inline tool chaining, programmatic controller interactions, and high-performance inspection and blocking delivered by x86 service nodes, security owners can augment and scale their inline tools when confronted with massive DDoS attacks.

CONCLUSION

Data centers need an intelligent, agile, highly flexible visibility and security architecture that can centralize the provisioning of network traffic from across the data center and provide cost and operational efficiency.

In the past, network owners have had no unified solution for managing the delivery of traffic to network and security tools, whether inline of out-of-band. The only way to achieve visibility and optimization for tools was to deploy legacy NPBs or leverage TAP or SPAN ports. However, the emergence of hyperscale networking has created a blueprint for the creation of next-generation architectures that scale and adapt for enterprise and service provider environments and radically simplify management.

A controller-based, SDN fabric solution that leverages open hardware to create a logical “super-NPB” is able to deliver the benefits experienced by hyperscale companies to every organization—at any scale. Data centers can now achieve the next-generation visibility and security needed to see and defend everywhere; accelerate and sustain service delivery, and optimize budget.

big switch networks

Headquarters
3965 Freedom Circle, Suite
300, Santa Clara, CA 95054

+1.650.322.6510 **TEL**
+1.800.653.0565 **TOLL FREE**

www.bigswitch.com
info@bigswitch.com

BMF PoV Whitepaper V1 (December 2016)