Doyle Research

Pervasive Security Enabled by Next Generation Monitoring Fabric

By: Lee Doyle, Principal Analyst at Doyle Research

Sponsored by Big Switch Networks

Executive Summary

Enterprise networks have become ever more challenging to secure and manage given the trends of massive growth in bandwidth, deployment of large enterprise data centers, and significant adoption of cloud-based applications. Organizations now have a reliance on the network for critical business functions, including remote access to data center and cloud-based applications.

Hackers and cyber-criminals are exploiting the increased network reliance to threaten most (if not all) organizations with operational disruption and data loss. The exponential growth in the network footprint, the shift in traffic patterns within the data center and the sophistication of cyber-attacks are breaking traditional network security designs – making it impossible to secure the network perimeter. Worse, many security breaches are hard to detect, making remediation impossible. Security products (e.g. firewalls) are increasingly burdened with too many connections and too much traffic, resulting in significant performance impacts.

Monitoring throughout the network is critical to enable network visibility and dynamically mitigate security threats. Network monitoring tools must filter and aggregate huge traffic flows, isolate bad traffic on-demand to improve security, and ensure compliance. The specific benefits of enhanced network-wide visibility include:

- Rapid detection and resolution of application and network security breaches
- Improved network performance and reduced latency
- Ability to dynamically isolate bad traffic
- Improved tool utilization and performance

The introduction of low-cost white box switches combined with SDN software have significantly improved performance, management, and lowered the cost of pervasive network monitoring. IT organizations can benefit from advances in network monitoring performance and capacity to improve application performance, end-user satisfaction, and to identify security challenges.

"We need good, solid network data or performance suffers...

...When provided with scalable network visibility tools, the security teams came running and have seen significant value in threat mitigation"

-- Senior Network Engineer at Fortune 50 Software Company

Challenges of Securing Next Generation Networks

The growth in the frequency of malicious attacks has shifted the security landscape. The assumption must be to design IT security to defend systems when you are attacked (not if you will be attacked). The impact of successful attacks and the related adverse commercial impact have never been greater. The emphasis of security is now geared toward detection, containment, and fast remediation.

Increasing reliance on the network for critical business functions, such as BYOD, mobile access, and SaaS, has opened new avenues for cyber-attacks. This presents significant challenges for network and security teams who need to maintain a high performance, resilient network, while ensuring that it is secure. Visibility into who is accessing the network and the ability to identify anomalous traffic is essential to detecting cyber-attacks and addressing security problems.

As a transit point for all information exchange, the network is the critical point for identifying cyber-attacks. With its ability to inspect all network traffic, network monitoring systems are key to detecting anomalies and variances compared to normal traffic flows. As networks grow, the amount of traffic can quickly exceed the capabilities of security devices and related management tools. High performance, intelligent network monitoring systems capture the packets, apply pattern matching, and can then send the appropriate traffic or meta-data to the appropriate security appliances. Thus, monitoring can help match (limited) security performance with rapidly growing network performance. The visibility provided by network monitoring enables the ability to make rapid decisions in real time in response to threats before they have time to affect the entire infrastructure.

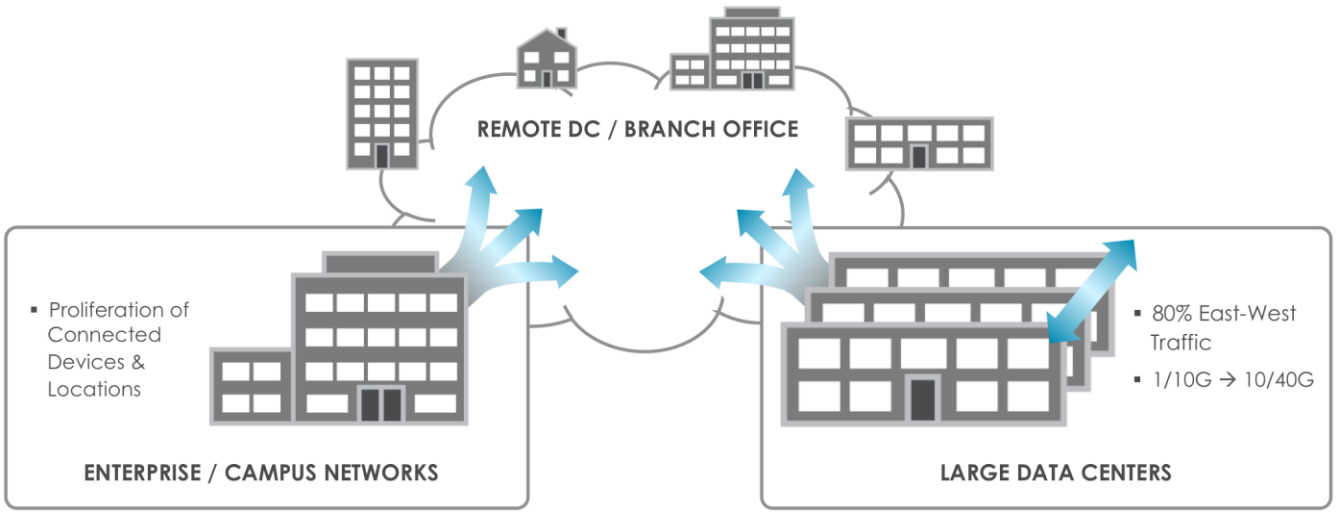

Figure 1: Trends in Data Center and Campus Networks

Network Monitoring Requirements for NGN Networks

Enterprise networks, including data center, campus, and branch networks, have become ever more challenging to secure and manage given the trends of massive growth in bandwidth, BYOD, deployment of huge virtualized data centers, and significant adoption of cloud-based applications (see Figure 1). Network monitoring fabrics analyze traffic to improve troubleshooting, threat detection, application performance monitoring, and network performance monitoring.

Data Center Networks

The advent of large-scale data centers and cloud-based applications have resulted in tremendous growth in network traffic and have changed the flow of network traffic. These changing traffic patterns have increased the security challenges and the ability to address network performance issues. Growth in traffic created by increased use of video, software as a service, and cloud is driving a wave of data center network upgrades from 1GB to 10/40GB links. The widespread adoption of server virtualization is changing the directions of data center network traffic flows from the North/South flow of client-server apps to the East/West of server-to-server traffic. The scale of many data centers has increased significantly with hundreds or thousands of ethernet links (at 10GB) moving to 40GB and 100GB over the next few years. The volume of traffic in an upgraded network can overwhelm the tool and monitoring infrastructure designed for lower bandwidth networks.

The key requirements for monitoring data center networks include:

- Hyper-scale performance (and the ability to support future growth in traffic flows)
- Support for multiple data centers located in geographically separate locations
- Ability to secure growing east-west traffic
- Operational simplicity despite exponential growth in visibility requirements

Campus/Branch Networks

Network monitoring requirements at campus and branch networks are evolving as these networks cater to an expanding set of wireline and wireless connected devices and need visibility across multiple geographically dispersed locations. The key requirements for monitoring campus/branch networks include:

- Granularity of monitoring networks on-demand and at every location, to enable uniform enforcement of security policies, audit and compliance
- Ability to support integrated monitoring of wireless and wireline (ethernet) links
- Centralized provisioning, automation, and management (security) (OPEX)
- Ability to monitor network performance and bandwidth latency – prioritization of voice/video traffic

The Value of SDN-based Network Monitoring

With a centralized controller, open APIs, and support for commodity white box ethernet switches, SDN provides significant benefits for network monitoring. SDN allows for the decoupling of security and network traffic management and can provide separate information and operational flows for network and security managers. SDN also enables centralization of monitoring tools and staff in few data centers, thus dramatically reducing operations costs while allowing operations teams to monitor networks across the entire organization.

Open ethernet switch hardware provides high performance at a significantly lower CAPEX allowing for scalable network monitoring through the network. The SDN controller allows for centralized management of a monitoring infrastructure that can scale across multiple large data centers as well as to remote (branch) locations. A logically centralized controller also enables dynamic service insertion – for both customized tools and 3rd party security applications.

Key benefits of SDN-based network monitoring are:

- Ability to centrally monitor and enforce policies across all network traffic (e.g. every rack in a data center, all remote locations, out of band and inline traffic monitoring)
- Optimal tool utilization by offloading traffic selection, filtering and replication to the visibility fabric
- Efficient operations with centralized tools, and dynamic management of service chains
- Economically scale-out the network monitoring infrastructure as the network foot print grows

Big Switch Enables Pervasive Security

Headquartered in San Clara, CA, Big Switch Networks is a leading provider of open SDN solutions including Big Cloud Fabric and Big Monitoring Fabric.

Big Monitoring Fabric

Big Monitoring Fabric (BMF) is a 1G/10G/40G/100G network visibility fabric that leverages high-performance, bare metal Ethernet switches (white-box or brite-box) to provide pervasive security monitoring and visibility of an organization's network traffic. Using SDN-centric architecture, BMF enables scale-out fabric for enterprise-wide monitoring, single pane of glass management, and multi-tenancy for multiple IT teams to simultaneously perform network monitoring (see Figure 2).

Big Switch has a number of partnerships to leverage the SDN ecosystem, including relationships for white box hardware from DELL, Accton, Quanta, Edge Core and security (and other Layer 4-7) software from FireEye, Riverbed, BlueCoat, A10, Cyphort, Telchemy.

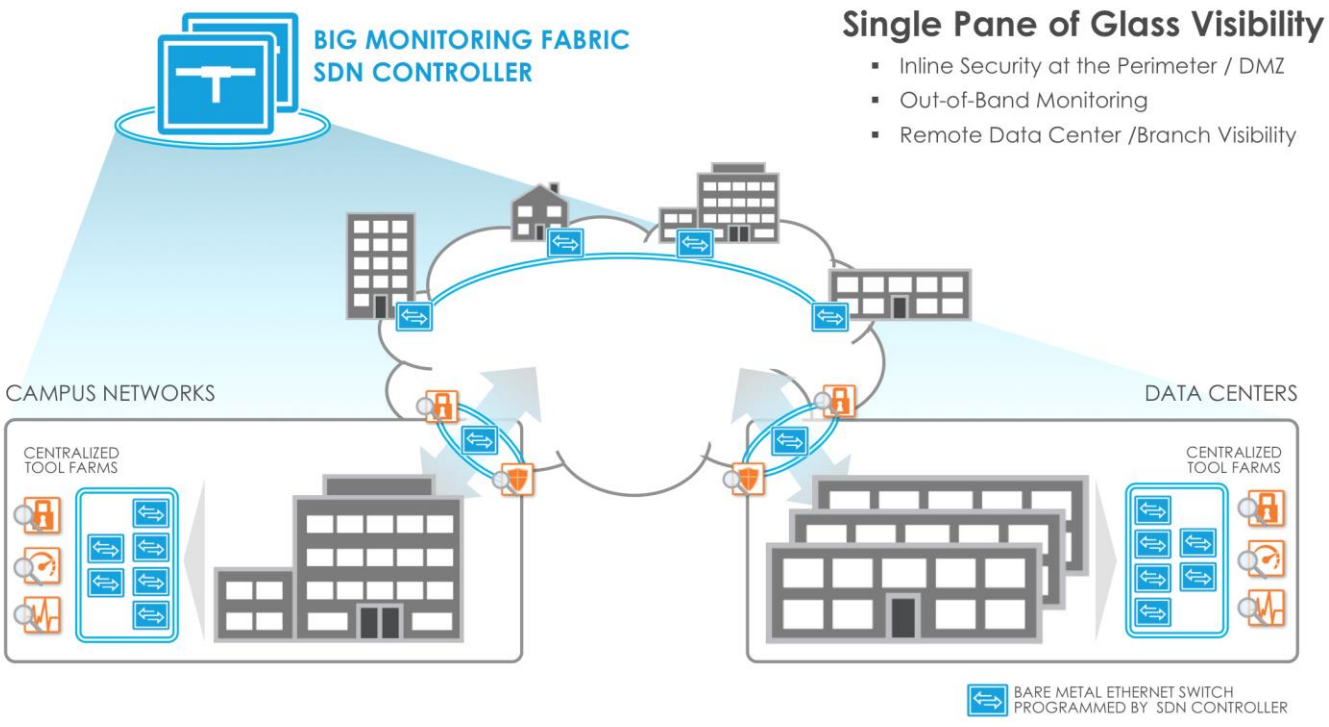

Figure 2: Big Monitoring Fabric - SDN Controller Managing Bare Metal Ethernet Fabric

Big Monitoring Fabric is provisioned and managed through the Big Monitoring Fabric controller. This operating model allows for an easier integration with existing management systems and supports fine-grain, role-based access control for multi-tenant operations. Big Monitoring Fabric switches can be deployed in either of the two deployment modes:

- **Out-of-Band** —Deployed adjacent to the production network. Connects to SPAN/TAP ports from the local and remote production networks
- **Inline**—Deployed in the DMZ, the solution supports load balancing across multiple instances of the same tool as well as chaining of a set of security tools on a per-policy basis (Figure 3)

By deploying a commodity Ethernet switch at each monitored location, the entire Big Monitoring Fabric (including inline, out-of-band and remote location switches) is operated and managed centrally via the BMF Controller with high availability.

Some of the generic advanced features of Big Monitoring Fabric include: **Application Protocol Recognition** (or deeper packet matching capability), real-time flow level visibility with **sFlow Generation**, Intel x86 based **Service Nodes** for packet manipulation functionality and in-built **Advanced Analytics** with support for multiple trackers.

When deployed in Inline-mode at the perimeter of a network, Big Monitoring Fabric Controller supports additional features including (see Figure 3):

- Highly Resilient Architecture to protect against network, tool or controller failures
- Asymmetric Tool Chaining different tool chains for traffic coming into / leaving the DMZ
- Load Balancing across multiple instances of lower bandwidth tools (1G/10G).
- Supports dynamic, programmatic (REST API based) configuration to drop certain marked flows (e.g. DDoS mitigation)

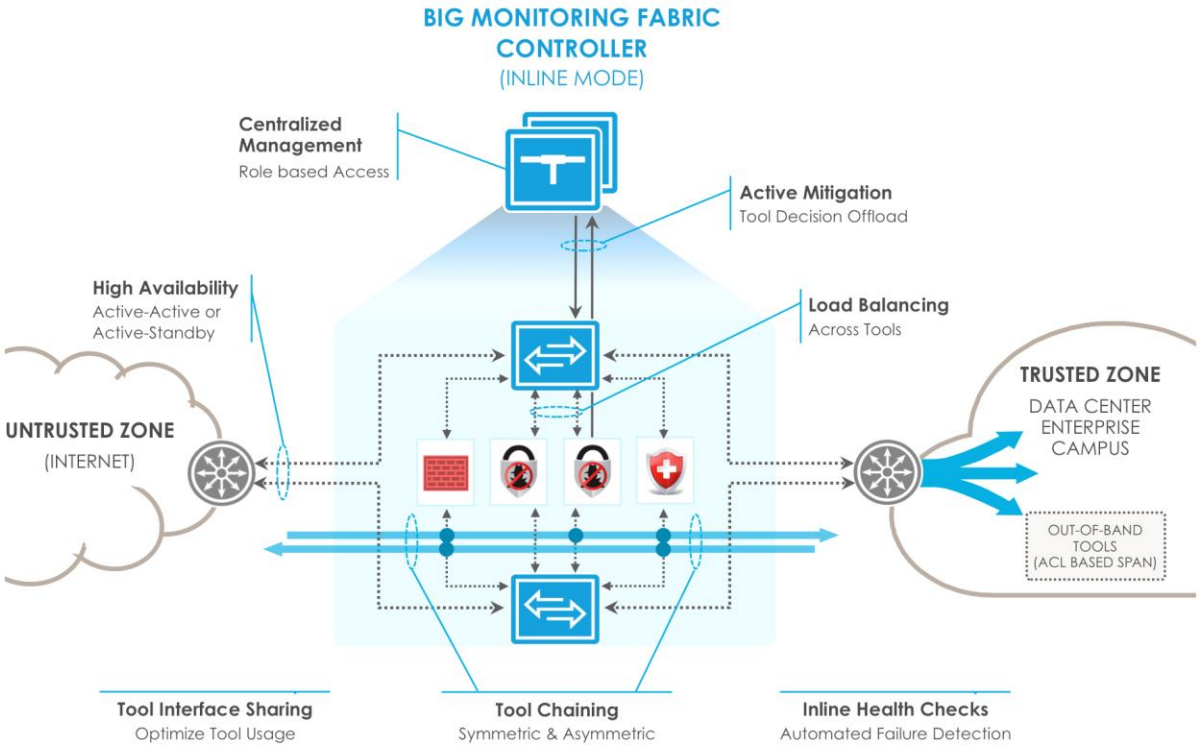

Figure 3: Big Monitoring Fabric - Inline Deployment

"For our security initiative, we selected Big Switch for our inline monitoring due to its ease of deployment and operation, modular scalability, and excellent feature set."

-- Network Engineer at Fortune 50 Petroleum Refining Company

Recommendations for CXOs

Pervasive network security is increasingly difficult in an age where IT must support high speed networks, data center virtualization, mobility, and broad user access to cloud-based applications. Reliance on the network for remote access to internal and cloud-based applications has eroded the security perimeter. All organizations are at risk for cyber-attacks and intrusions are increasingly hard to detect. Security threats can (and have) cause significant disruption to IT operations and loss of sensitive data.

Existing network security systems (e.g. firewalls) are becoming overwhelmed by increased network traffic and are proving vulnerable to threats outside and inside the security perimeter. Hyperscale networking designs with commodity ethernet switch hardware and SDN software provide the scalability and cost effectiveness to allow IT managers to "see" all the network traffic. This increased visibility allows traffic to be funneled to the appropriate security and compliance tools.

The open SDN ecosystem delivers significant white box hardware price/performance benefits – with over 60% Capex savings in most instances, when compared to traditional NPB solutions. SDN software provides open APIs for integration of 3rd party applications and ease of customization for specific requirements. The centralized SDN controller can monitor network traffic in remote data centers, campus, and branch locations. Centralized policy provides for auto discovery of network resources, tracking of network access, and ease of management via a single pane of glass for the fabric.

IT Managers need network monitoring products that are powerful, cost effective, and easy to use. These tools must fit seamlessly into the existing network environment and easily adapt to changing network environment. Doyle Research recommends that IT Managers evaluate network monitoring products based on the following criteria:

- Capacity to handle high network performance demands at scale
- Ability to see the entire network – LAN and WAN, physical and virtual
- Integration with existing security infrastructure
- Quality of the automation and centralized administration tools

"We wanted more points of input than our traditional NPB could handle economically, so we decided to go with a white box solution and Big Monitoring Fabric to gather packets and forward them to the tools as needed."

--Ted Turner, Senior Network Engineer at Intuit

Meet the Author

Lee Doyle is Principal Analyst at Doyle Research, *providing client focused targeted analysis on the Evolution of Intelligent Networks. He has over 25 years' experience analyzing the IT, network, and telecom markets. Lee has written extensively on such topics as SDN, NFV, enterprise adoption of networking technologies, and IT-Telecom convergence. Before founding Doyle Research, Lee was Group VP for Network, Telecom, and Security research at IDC. Lee contributes to such industry periodicals as Network World, Light Reading, and Tech Target. Lee holds a B.A. in Economics from Williams College.*