Modern Network Analytics: Simplified, System-wide Visibility

A UNIFIED NETWORK MONITORING FABRIC WITH INTEGRATED SCALE-OUT ANALYTICS IS THE BEST WAY TO MEET THE CHALLENGES OF TODAY’S DATA-DRIVEN PRODUCTION ENVIRONMENTS

OVERVIEW

Production networks generate invaluable data for understanding application performance problems, security issues, day-to-day troubleshooting, and Mean Time to Resolution (MTTR). But as the volume of data flowing through the network continues to surge, capturing and analyzing that data is becoming more difficult and complex. Network managers are forced to pivot from a packet-monitoring tool to a network flow collector to a device-metric monitoring tool, and back again—all in separate dashboards with different parameters, widgets, and reports.

Scouring through performance reports and checking into dozens of dashboards to identify network issues or security breaches is inefficient, and the siloes of network data created by this approach limit visibility into overall network performance and connected devices. With the volume and speed of data traversing our production networks today, sifting through mountains of data to discover root causes isn’t feasible.

Today’s data centers need a next-generation approach to network visibility that takes advantage of bare-metal technology to unite the network under a single pane of glass and incorporates an analytics layer to dynamically monitor the network without edges to help defend the network in real time while providing better value, simplicity, and scalability.
THE PEOPLE, PROCESS, AND TECHNOLOGICAL SHORTCOMINGS OF TRADITIONAL ANALYTICAL APPROACHES

Analytics tools haven’t evolved to keep up with the volume of data pouring through production networks. As a result, network managers have dealt with network expansion and monitoring tools in an ad hoc manner, adding tools for different departments and analytics as needed. This fire-fighting approach is often subject to impulsive reaction to industry events/news and internal emergencies with little consideration for the future of the infrastructure. Then, the technologies being used are fragmented; infrastructure vendors offer different monitoring interfaces and disparate data streams, and analytic tool companies typically focus on one proprietary interface, format, and data stream for specific analytics.

Moreover, rigid processes on the change-management front based on compliance standards is inconsistent with the need to move quickly with security analytics. Further exasperating the problem is the expansion of application by DevOps and enterprise IT into public clouds. As customers increasingly move to cloud computing, new sources of monitoring information are introduced—but those are siloed from the enterprise data center.

To monitor traffic on the scale large networks are seeing today, network administrators are deploying specialized technologies such as telemetry, sFlow, or NetFlow. But that approach is costly, inefficient, and not easily scalable. Upgrading to a bigger and faster analytics appliance is frequently needed in just a year or two and often on a regular basis after that in response to network speed upgrades and sheer traffic volume growth. As you add network packet brokers (NPBs) to meet that increased bandwidth need, infrastructure management becomes more complex and expensive. But visibility remains limited by the reach of your individual tools that monitor those bands.

There has to be a better approach.
There is.

A SINGLE UNIFIED VIEW OF THE NETWORK, MANAGED BY A SINGLE PANE OF GLASS

By replacing discrete NPBs with a single “fabric” of open networking switches, a network manager can essentially create a single logical NPB managed by a pair of redundant, intelligent, software-defined networking (SDN) controllers, with all monitoring tools receiving network-wide information in a single, centralized tool farm.

Correlation of data would no longer be needed, and if the network grows, an unlimited number of switches and monitoring tools can be added to the fabric without creating silos or the need to add a controller.
This setup has two main differentiators compared to current network architecture:

• The SDN architecture provides immense simplicity. IT teams can add switches and monitoring tools without the hassle of another piece of equipment to manage because all the orchestration, configuration, and troubleshooting—including of cloud-based and remote locations—is done through the single-pane-of-glass dashboard.

• The fabric operating system can be put on top of switches from most manufacturers and retain the same ability to be managed from the single pane of glass. Because the OS simply aggregates between the hardware and software, the IT team has more power over how to manage or scale the fabric.

That architecture offers six significant benefits:

1. Simplicity
2. Scale-out architecture that the customer can continually add to without increasing management touch points
3. Controller is REST API-driven, allowing customers the flexibility to add or enhance per their needs / system
4. Agility in orchestration, troubleshooting, deployment, and upgrade scenarios
5. Cost savings because there is just one infrastructure enterprise-wide
6. Increased options for high-performance equipment that doesn’t need to be replaced every two years even with cloud and DevOps as the big disrupters

This controller-based architecture is inspired by the design principles that hyperscale organizations like Google and Facebook pioneered to implement a logical, scale-out, open networking switch architecture that leverages intent-based principles to deliver simplicity and agility at an unprecedented scale.

BIG MON ANALYTICS: INTEGRATED END-TO-END NETWORK VISIBILITY WITH SCALABILITY

One vendor has pioneered this type of architecture for enterprise data center use: Big Switch Networks. The Big Monitoring Fabric is a highly scalable monitoring fabric built with open networking switches and an intelligent controller layer. Then, an analytics layer built with industry-standard x86 servers can be laid on top of that fabric to provide real-time and historical analytics to help optimize and secure your network.

This results in network-wide visibility inclusive of all endpoints and the ability to better address the security, connectivity troubleshooting, traffic accounting, and application performance needs at scale through a single-pane-of-glass dashboard. The analytics node also acts as a collector for NetFlow and sFlow packets, to provide real time application level visibility, including tunnelled or encapsulated traffic, enable detection of security attacks like DoS/DDoS and support sub-second triggering. The centralized control for wire speed filtering and processing data can reduce the oversubscription issues within each individual tool.

With this Big Mon Analytics Node, network administrators can:

• Examine top talkers and applications in use
• Track down a non-compliant operating system in the network
• Show the general latency profile of a production network and isolate a specific device to show its latency, protocols used, and user information
• Track down and determine why traffic is unexpectedly going out of the environment, and find out if it is a misconfigured device or a security risk
All of that information is gained by snooping the control plane packets that are already coming to the switch fabric. No query of the network required, meaning zero impact on the production network.

The common monitoring infrastructure can be used by multiple departments, with data feeds filtered based on access control. If, during the course of investigation, a member of the IT team wants to share a view with someone, they can simply grab the URL and send that exact view to the other person, making the Big Mon Analytics Node a good tool for collaboration.

CONCLUSION

Network visibility is the key to optimizing and securing production networks. But as the volume of data traversing our data center continues to grow, bandwidths increasingly fragment, making visibility difficult to achieve.

By uniting the network in a single fabric with an integrated analytics layer managed under a single-pane-of-glass, data centers can get centralized, end-to-end visibility into the network, whether the source is on premise, coming in from the demilitarized zone, or a private connection with AWS, Azure, or Google clouds.

It’s a solution that can be deployed non-disruptively as an out-of-band monitoring network with rich analytics. And by consolidating budget currently allocated to multiple different organizations into this single enterprise-wide infrastructure, reducing technology duplication, data centers could discover cost savings—particularly when you consider the obsolesce and non-scalability of current infrastructure architecture.

The result? Better security, troubleshooting, and application performance insight with simplified management, OPEX and CAPEX cost savings, and unprecedented scalability.

To learn more about our Big Mon Analytics Node offering, call 650-332-6510 or visit www.bigswitch.com.
ABOUT BIG SWITCH

Big Switch Networks is the Next-Generation Data Center Networking Company. We disrupt the status quo of networking by designing intelligent, automated and flexible networks for our customers around the world. We do so by leveraging the principles of software-defined networking (SDN), coupled with a choice of industry-standard hardware. Big Switch Networks has two solutions: Big Monitoring Fabric, a Next-Generation Network Packet Broker, which enables pervasive security and monitoring of data center and cloud traffic for inline or out-of-band deployments and Big Cloud Fabric, the industry’s first Next-Generation switching fabric that allows for choice of switching hardware for OpenStack, VMware, Container and Big Data use cases. Big Switch Networks is headquartered in Santa Clara, CA, with offices located in Tokyo, Melbourne, London and Istanbul. For additional information, email info@bigswitch.com, follow @bigswitch, or visit www.bigswitch.com.

Big Switch Networks, Big Cloud Fabric, Big Monitoring Fabric, and Big Monitoring Analytics Node are trademarks or registered trademarks of Big Switch Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.