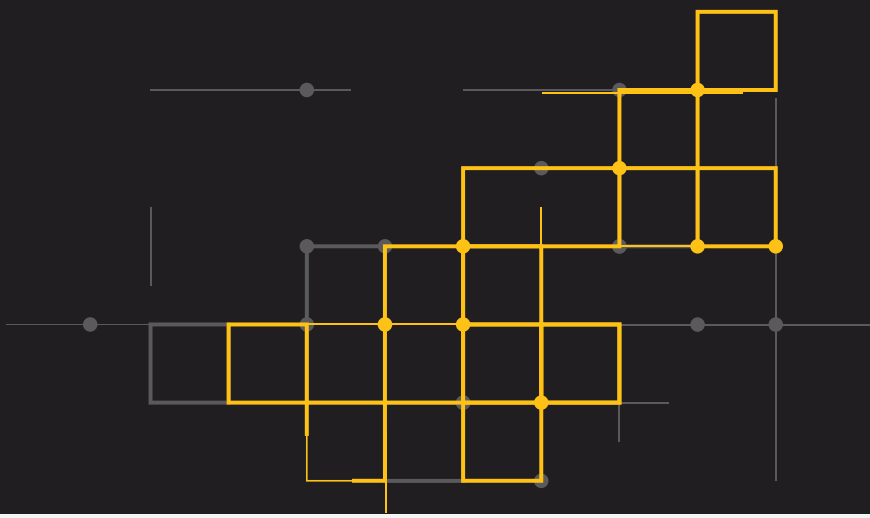
Solution Brief

Symantec Technology Integration Partner: Big Switch Networks



Business Challenge

Sophisticated threats are dramatically growing in frequency, size and complexity. To combat these advanced persistent threats, IT organizations need to monitor and analyze a large portion of their data center traffic. In addition to Internet and WAN edge (north-south) traffic, continuous monitoring of public/private clouds, Big Data analytics and Virtual Desktops requires access to high-bandwidth application-to-application ("east-west") traffic in the data center. Optimal tapping/mirroring of the entire data center network is increasingly becoming a necessity to secure applications and maintain business continuity.

Solution Overview

Symantec and Big Switch Networks are partnering to provide customers an efficient, simplified and cost-optimized solution to combat increasingly sophisticated network attacks in the data center. The solution offers the combined benefits of Symantec's Security Analytics and Big Switch's SDN-based Big Monitoring Fabric leveraging bare metal switches. It enables policy-driven monitoring and delivery of data center-wide traffic flows (both north-south and east-west traffic) to Security Analytics, which then detects advanced persistent threats and malware. The joint solution helps quickly identify advanced and targeted attacks that might slip past traditional security tools while leveraging the benefits of a software defined network SDN-based fabric for operationally simple, ultra-low cost, and scale-out monitoring environment.

How it Works

The solution is comprised of Big Monitoring Fabric, a modern SDN-based monitoring fabric built with bare metal Ethernet switches, to which Symantec's Security Analytics is attached. For data center wide scaling, the Big Monitoring Fabric is typically deployed in a two or three-tier topology. Typically, there is a layer of filter switches that aggregate TAPs and SPANs and another layer of delivery switches to which security tools connect. An optional layer of core switches can be inserted between filter and delivery layers. Traffic that comes through the filter ports is subject to user-defined policies for filtering, replication or even modification via third-party services such as NPBs. It is then delivered to the Symantec Security Analytics tools that are wired at the other end of the fabric through the delivery ports. Security Analytics then analyzes the traffic and provides clear, actionable intelligence about security threats to applications, files, and web content.

big switch networks

Partner: Big Switch Networks

Partner Product: Big Monitoring Fabric

Symantec Product: Security Analytics

Symantec

The joint solution enables consolidation of the analytic devices to a single farm, thus preventing the choke points typically seen in static, box-centric approaches. This is made possible by the SDN-based Big Monitoring Fabric Controller, which fully provisions the fabric – programs the forwarding paths of monitored flows, manages policies, as well as centrally controls all bare metal switches and their interconnections. Management of the centralized Big Monitoring Fabric is done via the state-of-the-art controller's GUI or CLI, or REST-API.

Key Features and Benefits

Flexible, Scale-out Deployment

Hundreds of 1G/10G/40G TAP and SPAN ports can be connected to the Big Monitoring, and any network traffic can be directed to any of the connected Security Analytics devices at any time. With this solution, customers can enjoy a multi-fold increase in monitored traffic throughput and reach.

Policy-based Multitenant Tap and Tool Sharing

Multiple groups can access the same traffic and have them sent to multiple tools that they respectively own. Furthermore, existing NPBs can still be leveraged for advanced features, such as time stamping or packet slicing, by attaching them as service nodes to the Big Monitoring Fabric.

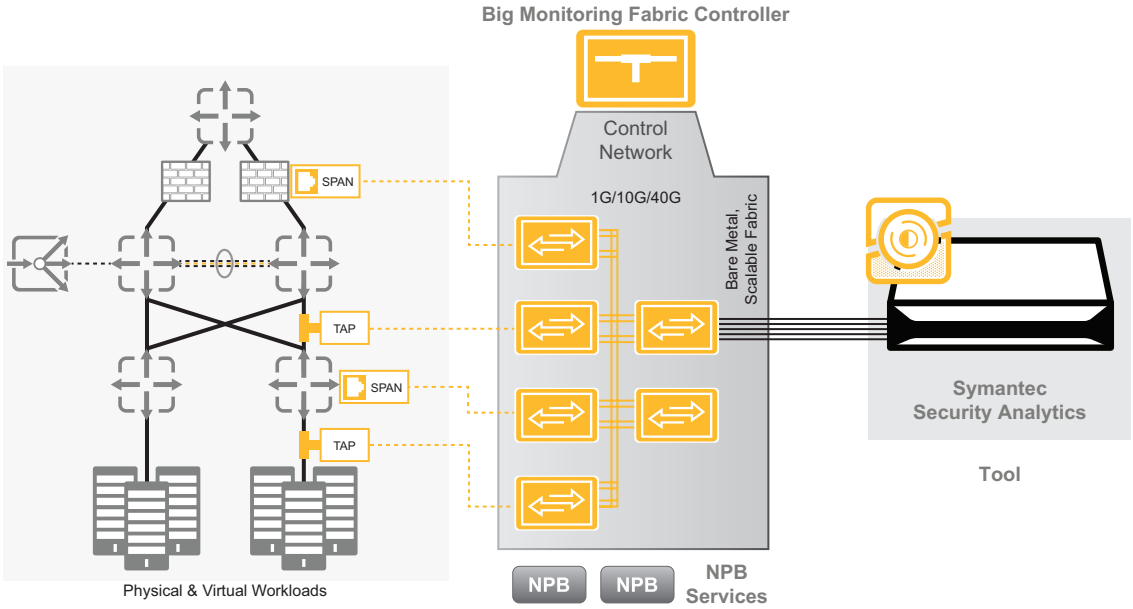


Figure 1 - Symantec Security Analytics deployed along with the Big Monitoring Fabric

Massive Operational Simplicity

The solution is based on SDN architecture with a logically centralized, programmable Big Monitoring Fabric Controller controlling and managing all fabric switches. Moreover, the Big Monitoring Fabric Controller is also the single-pane-of-glass for all fabric-wide operations, policy management and tenant management. Even when more switches or policies or tenants are added, operational overhead of managing the fabric is negligible.

Tremendous CapEx savings

The Big Monitoring Fabric is based on bare metal switches that are built with best-in-class networking ASICs. Big Switch's Switch Light OS runs on these bare metal switches and interacts with the Big Monitoring Fabric Controller. This disaggregation of HW and SW allows tremendous cost reduction compared to proprietary HW-based solutions. It also provides customers a choice of hardware switch vendors for their monitoring needs.

About Big Switch Networks

Big Switch Networks is the market leader in bringing hyperscale data center networking technologies to a broader audience. The company is taking three key hyperscale technologies – OEM/ODM bare metal and open Ethernet switch hardware, sophisticated SDN control software, and core-and-pod data center designs – and leveraging them in fit-for-purpose products designed for use in enterprises, cloud providers and service providers. The company's Big Monitoring Fabric is an entry level solution to monitor existing networks, and the flagship Big Cloud Fabric is the industry's most advanced bare metal switching fabric intended for new data center pods such as private cloud, big data and VDI. For additional information, email info@bigswitch.com, follow @bigswitch or visit www.bigswitch.com.

For More Information

Learn more about Symantec Technology Integration Partners on our website.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_sb_TechPartner_SA_BigSwitchNetworks_EN_v1a