# FireEye and Big Switch Networks

## Combat Cyber Attacks by Deploying FireEye and Big Switch Joint Solutions for Scalable DC-wide Monitoring and DMZ Security Chaining

SOLUTION BRIEF

### INTEGRATED SOLUTION HIGHLIGHTS

- **Organization-wide threat monitoring** - Any traffic across the network can be directed to any FireEye device, thus providing comprehensive threat monitoring. FireEye devices can be co-located in a centralized tool farm, which enables simplified change management and tool scaleout.
- **Simplified Management** – Policies for both out-of-band monitoring and inline DMZ service chaining are managed from the centralized SDN controller which acts as a single pane of glass.
- **Operational agility** – Scale-out architecture enables rapid change management such as adding more switches, policies and/or tenants to the fabric.
- **Enhanced Tool Efficiency** – Granular policies ensure that only the relevant traffic is sent to the tools, and each tool can be part of multiple service chains for optimal tool performance.

### OVERVIEW

FireEye Threat Prevention Platform and the Big Monitoring Fabric (BMF) jointly deliver an efficient, cost-optimized, datacenter-wide threat prevention solution. The joint solution combines the FireEye signature-less protection, which creates real-time threat intelligence along with an SDN-powered open networking fabric to combat cyber attacks with unmatched efficiency and at an unprecedented scale within the data center. In addition, BMF inline solution with FireEye IPS offers policy-based dynamic chaining of security services at the DMZ. Customers can realize the full potential of datacenter-wide threat protection while enjoying the benefits of operational simplicity derived from an SDN-based architecture.

### THE CHALLENGE

As seen by security breaches on some of the world's biggest brands and financial entities, today's data centers need new sophisticated threat protection mechanisms. These modern requirements include:

- **Ubiquitous network monitoring:** Traditional approaches place threat protection devices at selective network locations that are likely to witness cyber attacks, leaving a majority of the network vulnerable. A broader approach for ubiquitous protection is needed both within data center and at the DMZ.
- **Multi-team coordination:** The same strategic spots that demand high scrutiny by security administrators need to be monitored by network administrators for performance. This requires multi-team coordination for TAP/SPAN port sharing, which can add significant operational complexity.
- **Simplified Service Chaining at DMZ:** Increasingly multiple security devices such as IPS, DDoS detection, SSL visibility appliances are deployed inline. A simplified approach is needed for dynamic orchestrating security service chains for intelligently forwarding inline DMZ traffic.
- **Lower cost of monitoring:** With constrained IT budgets, ubiquitous traffic monitoring needs to be achieved at the lowest CAPEX and OPEX.

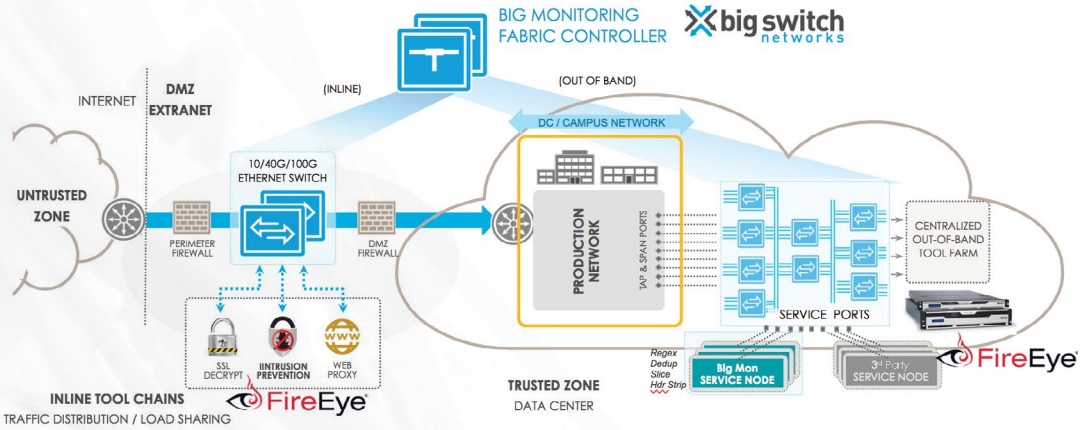
### THE INTEGRATED SOLUTION

**Pervasive DC Security Monitoring**

The security monitoring solution leveraging FireEye platform and BMF is based on a next-gen architecture that offers scale-out, SDN-driven automation and ease of management. Pervasive security monitoring can now be made a reality through real-world use cases such as Monitor Every Rack and Monitor Every Location.

FIREEYE PRODUCT
FireEye NX Series

BIG SWITCH NETWORKS PRODUCT
Big Monitoring Fabric




### DMZ Inline Security Chaining

The BMF inline solution with FireEye IPS leverages an SDN-based approach to simplify and manage dynamically orchestrated service chains based on user-specified policies.

## HOW THE JOINT SOLUTION WORKS TOGETHER

### Pervasive DC Security Monitoring

The Big Monitoring Fabric solution is a fabric of open networking switches managed by a pair of SDN controllers, which act as a single centralized pane of glass for operations. The fabric can be built from as small as a single switch and scaled out to several of them connected together to form one logical switch managed by a central controller. The solution enables DC-wide pervasive monitoring with the ability to tap every rack/machine in the production network and based on policy, direct the right traffic to right FireEye Threat Prevention device in the centralized tool farm. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, that empowers security teams to prevent, detect, analyze, and respond to today's advanced attacks. A very important component of the solution is the Big Mon service node which provides functionality like deduplication, header stripping, packet slicing etc. which enable efficiency of the tools by sending the most important and interesting traffic for monitoring.

### DMZ Inline Security Chaining

This solution uses an SDN-based approach to simplify and manage dynamic service chains at the DMZ. It leverages industry-standard open networking switches with Big Mon controller managing switches which are deployed inline in a HA configuration. The inline security tools such as FireEye IPS directly connect to the switches. The controller acts as central point of control, configures multiple policies as selected by users, to create different traffic paths to selectively steer traffic through the inline devices.

The key benefits that are offered with simplicity of operations through automation and ease of scaling, and the low CapEx investment make these solutions extremely compelling from TCO point of view.

## THE VALUE OF THIS PARTNERSHIP

The collaboration between FireEye and Big Switch has enabled customers to achieve comprehensive, organization-wide threat protection. Big Switch's Big Monitoring fabric with FireEye Threat Prevention Platform enables monitoring of any flow at any time while providing the benefits of zero-touch management and scale-out deployment. With BMF inline solution and FireEye IPS deployed in the DMZ, customers can benefit from a simplified, scalable and dynamically orchestrated service chains, all from a single pane of glass.

## ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

## ABOUT BIG SWITCH NETWORKS

Big Switch Networks is the leader in bringing hyperscale-inspired networking technologies to data centers. The company is taking key hyperscale technologies: open network switch hardware, SDN control software, and core-and-pod data center designs and leveraging them in fit-for-purpose data center switching and monitoring solutions for use in enterprises, cloud and service providers.

**For more information contact CSC@fireeye.com.**

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**