Pervasive Performance and Security Monitoring with ExtraHop and Big Switch

Achieve scalable application and network performance monitoring across the enterprise by deploying ExtraHop's stream analytics platform with Big Switch's SDN-based Big Monitoring Fabric. The joint solution enables simplicity, scale, and economics of IT Operations by providing pervasive visibility and deep analytics for application performance and security.

THE CHALLENGE

Faced with ever-increasing complexity and dynamism, IT Operations and security teams need visibility more than ever. Specifically, they require:

- *Visibility across siloes:* IT organizations often lack a "source of truth" that spans the entire environment: web, database, storage, authentication, encryption, and other elements. This cross-tier visibility is needed to streamline troubleshooting and speed up security incident response.
- *Empirical observation available to everyone:* Traditional methods of analyzing network traffic are expensive and only useful to network professionals. All IT and security teams can benefit from access to the definitive, empirical data derived from the network.
- *East-west traffic visibility at low-cost:* Traditional network monitoring tools for security primarily cover the perimeter, but do not analyze the traffic inside the data center. Ubiquitous DC traffic monitoring needs to be achieved at lowest possible costs.

THE SOLUTION

ExtraHop and Big Switch have partnered to deliver a scalable, cost-effective solution for all IT teams to gain deep visibility into their data in flight. The joint solution combines ExtraHop's stream analytics capabilities with an SDN-powered Big Monitoring Fabric built with open networking switches, to offer unparalleled visibility into all network activity at a fraction of the cost of traditional box-by-box alternatives. Big Monitoring Fabric delivers based on user policies, the most important portions of the TAPped and SPANed traffic to the ExtraHop platform to ensure efficient, comprehensive monitoring and detailed analytics. Combining SDN-driven policies from Big Switch and ExtraHop's proactive monitoring and remediation, customers can gain the optimal application experience and business efficiency.

THE SOLUTION COMPONENTS

The ExtraHop Platform

The ExtraHop streaming analytics platform transforms raw packets into structured wire data, so that you can see what's happening in your environment in real time, across all tiers, and across the entire application delivery chain. IT organizations use the ExtraHop platform for proactive monitoring and remediation, optimization and tuning, security monitoring and compliance, and business analytics.

- Automatically discover and classify every device and application on the network
- Observe every transaction for insights into applications, infrastructure, and users
- Make sense of your wire data with turn-key Big Data capabilities

The Big Monitoring Fabric

The Big Monitoring Fabric (BMF) is a next-generation, multi-tier, scale-out solution that leverages open networking and software defined networking (SDN) design principles. The BMF Controller fully manages multi-tenant monitoring policies, provisions the fabric, programs the forwarding paths of monitored flows, and centrally controls all switches and their interconnections. This enables data center wide monitoring with the ability to tap every rack and send it to any tool. With the ability to tunnel monitoring traffic, this capability is being extended to every location across the enterprise. Features supported are TAP/SPAN aggregation, flow filtering, replication, load balancing, and deep packet matching up to 128 bytes. The BMF can optionally be connected to one or more service node appliances managed by the controller to provide advanced packet functions such as deduplication, packet slicing, and regex matching. Existing NPBs can also be repurposed efficiently as service nodes in service chain, thereby offering investment protection.

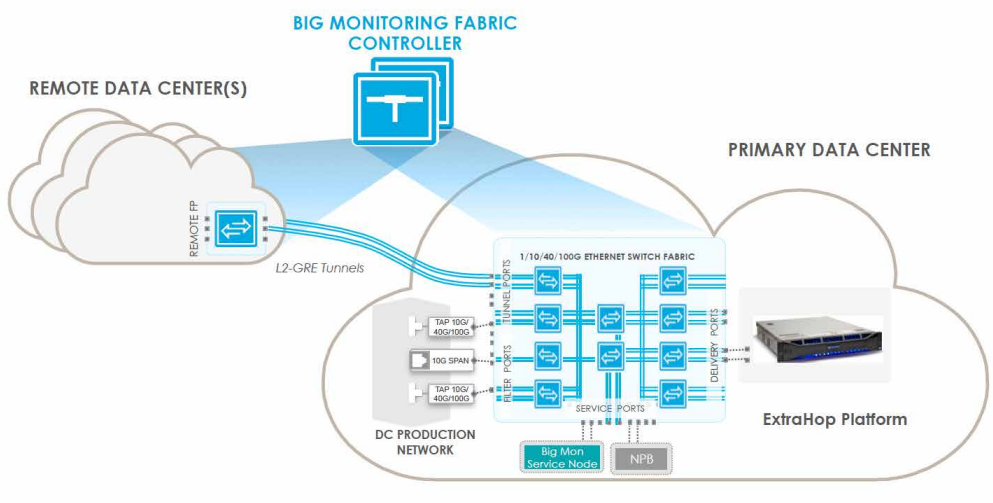

Figure 1: ExtraHop platform deployed along with the Big Monitoring Fabric

KEY SOLUTION BENEFITS

- **Deep Analytics for all data in flight:** With the Big Monitoring Fabric, IT organizations can forward traffic from throughout the enterprise to the ExtraHop platform for analysis. This joint solution makes it possible to perform in-depth L2-L7 analysis on all data in flight for improved performance monitoring, troubleshooting, threat detection, incident response, and business analytics.

- **Enables customized analytics:** The ExtraHop platform enables the rapid definition of new metrics that are customized for individual organizations through a programmable interface for the ExtraHop stream processing engine. The platform's universal payload analysis enables monitoring of any custom protocol based on TCP or UDP.

- **Flexible, scale-out deployment:** Thousands of 1G/10G/40G/100G ports can be connected to the Big Monitoring Fabric, and tapped traffic from any port can be automatically directed to ExtraHop for analysis, thus providing broad and on-demand application analytics. This also allows for all the tools to be co-located centrally in a single administrative domain thus accelerating deployment and enabling rapid change management.

- **Multi-tenant tool and tap sharing:** The solution provides the ability for multiple administrators (SecOps, IT Ops, DevOps) to monitor the same traffic by having it delivered simultaneously to multiple devices. Each of these administrators act as a tenant in the system with ownership of their respective tools, and can securely define policies through BMF Controller's role-based access control (RBAC) capability.

- **Operational agility with Centralized Programmability:** Monitored traffic is steered from a single, centralized management pane (GUI, CLI or REST APIs). Even when more switches or policies or tenants are added to the fabric, operational overhead of managing the fabric is negligible. With robust REST API capabilities in the BMF controller and the ExtraHop platform, policies can also be changed programmatically in real-time in response to a specific trigger.

- **Tremendous cost savings:** The Big Monitoring Fabric solution has Big Switch's Switch Light OS running on open networking switches that are managed by an SDN controller to form a scale-out fabric for monitoring. This disaggregation of hardware and software allows significant cost reduction and hardware vendor choice compared to proprietary NPB solutions. Consequently, for the same budget, customers are able to significantly broaden the visibility of their ExtraHop deployment.

ABOUT EXTRAHOP

ExtraHop makes data-driven IT operations possible for the real-time enterprise. With the ExtraHop stream analytics platform, organizations can transform packets into wire data. The cross-tier insights gained from ExtraHop help ensure the continuous performance, availability, and security of mission-critical systems; improve coordination across teams; and increase IT agility. The ExtraHop platform is used by hundreds of customers, including Fortune 500 companies such as Sony, Lockheed Martin, Microsoft, Adobe, and Google. To experience the power of the ExtraHop platform for yourself, explore our interactive online demo.

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