big switch networks

Big Monitoring Fabric™ – Enterprise Cloud

CLOUD-FIRST SECURITY AND VISIBILITY

Big Monitoring Fabric – Enterprise Cloud is a cloud-first network packet broker that enables pervasive security and monitoring of enterprise on-premises and cloud workloads and the selective delivery of them to multiple security, performance, and compliance tools — both inline and out of band. Powered by an SDN controller to manage a fabric of Open Ethernet switches and industry- standard x86 servers, Big Monitoring Fabric – Enterprise Cloud presents an easy to use, highly scalable, and integrated network visibility solution.

BIG SWITCH NETWORKS

Our mission is to deliver cloud-first data center networking and monitoring solutions — enabling enterprises realize the benefits of simplified productivity, improved scalability, and pervasive security with a dramatically improved TCO.

Big Monitoring Fabric – Enterprise Cloud is a cloud-first network packet broker that provides an integrated on-prem visibility fabric for deeper monitoring and pervasive security of out-of-band and inline workloads in the enterprise data center, DMZ, and extranet environments.

Get hands-on experience with our offering. Register for a free online trial at **labs.bigswitch.com**

For general inquiries contact us at **info@bigswitch.com**

BIG MONITORING FABRIC - ENTERPRISE CLOUD OVERVIEW

Big Monitoring Fabric – Enterprise Cloud (BMF-EC) is industry's first network packet proker (NPB) that leverages an SDN-controlled fabric using high-performance, open networking (whitebox or britebox) switches and industry-standard x86 servers to deploy highly scalable, agile, and flexible network visibility and security solutions. Traditional box-based, hardware-centric NPBs are architecturally constrained to meet emerging security and visibility demands of cloud- native data centers. BMF-EC addresses the challenges of traditional NPB solutions, by enabling a scale-out fabric for enterprise-wide security and monitoring, a single pane of glass for operational simplicity, and multi-tenancy for multiple IT (NetOps, DevOps, SecOps) teams.

ARCHITECTURE: SDN SOFTWARE MEETS OPEN SWITCH HARDWARE

BMF-EC's architecture is inspired by Hyperscale Networking designs, which consist of Open Ethernet switch hardware, SDN controller software and centralized tool deployment.

The BMF-EC architecture consists of the following components:

- High-availability pair of SDN-enabled Big Mon controllers — VMs or hardware appliances — that enable centralized configuration and simplified monitoring and troubleshooting.
- Big Switch's SDN-enabled Switch Light OS is a production-grade, ONIE-deployable, lightweight OS, that runs on the switches in the Big Mon fabric.
- Open Ethernet Switches (White Box or Brite Box). Include Dell EMC and HPE open networking switches, as well as ODM switches from Accton — use merchant silicon ASICs used by most incumbent switch vendors and have been widely deployed in production data center networks. These switches ship with Open Network Install Environment (ONIE) for automatic and vendor-agnostic installation of third-party network OS.
- Big Mon Service Node (optional). DPDK-powered, x86-based appliance that connects to the Big Mon fabric (either singly or as part of a service-node chain) to provide advanced packet functions like deduplication, packet slicing, header stripping, regex matching, packet masking, GTP correlation, UDP replication and IPFIX/NetFlow generation.
- Big Mon Recorder Node (optional). x86-based appliance that connects to the Big Mon fabric, managed by the controller to provide petabyte packet recording, querying, and replay functions.
- Big Mon Analytics Node (optional). x86-based appliance that integrates with the Big Mon fabric to provide multi-terabit, security, and performance analytics with configurable historical time-series dashboards.

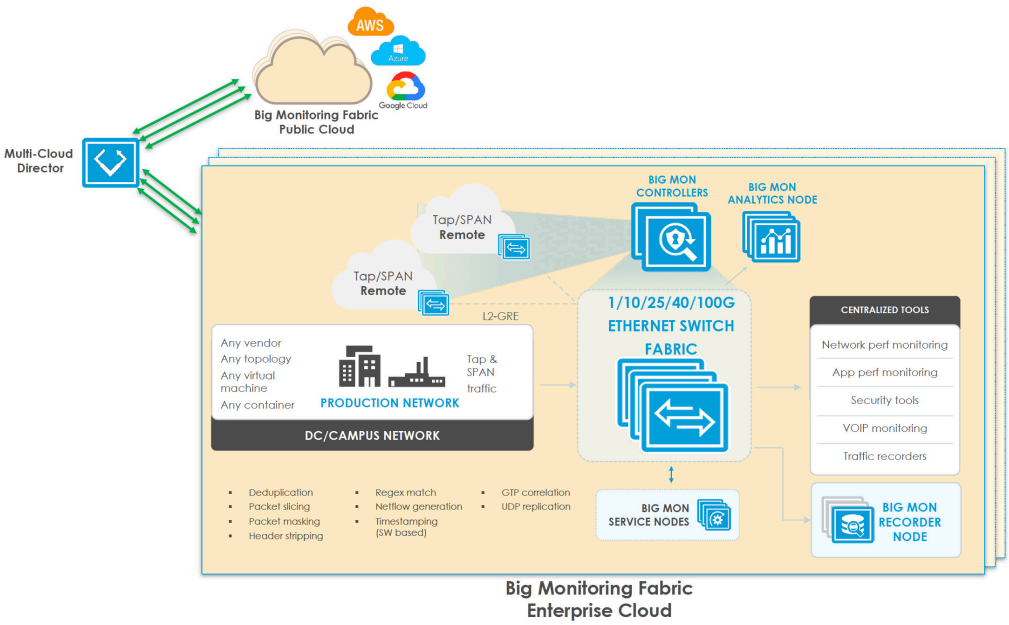

Figure 1: Big Monitoring Fabric Architecture

SIGNIFICANT CAPEX/OPEX SAVINGS

The BMF-EC enables a high-performance, integrated NPB + analytics + packet capture solution that supports rapid detection and analysis of network performance and security anomalies. BMF-EC leverages open networking switches and commodity hardware to provide significant savings, both capital and operational. By contrast, the traditional NPB-based approach has high TCO due to ever- expanding box-by-box deployment, proprietary hardware, and under-utilization of tools or inefficient use of them due to organizational silos.

Open, Industry-Standard Hardware Economics

BMF-EC utilizes the underlying cost efficiencies of the high performance, open networking switches, as well as the industry-standard x86 based appliances. As a result, BFC-EC is much more cost-effective for monitoring larger.

SDN-Enabled Operational Efficiencies

BMF-EC is provisioned and managed through the single pane of glass, thanks to the Big Mon controller CLI, GUI or REST APIs. This operating model allows for easier integration with existing management systems and monitoring tools. This SDN approach hence significantly reduces the operating costs associated with box-by-box management of traditional NPBs.

.

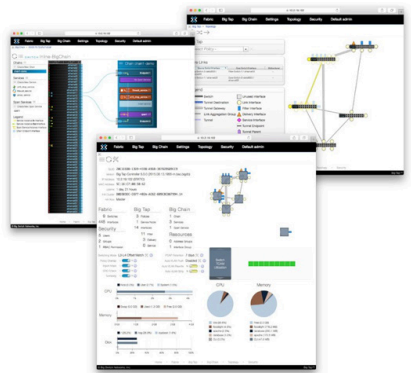

Figure 2: Monitoring Fabric Graphical User Interface (GUI)

BIG MONITORING FABRIC - ENTERPRISE CLOUD PRODUCT DESCRIPTION

BMF-EC switches can be deployed in either of the two deployment modes:

- Out-of-band mode. Deployed adjacent to the production network. Connects to SPAN and tap ports from the production network.
- Inline mode. Deployed in the DMZ or extranet (production network).

In both modes the Big Mon controller serves as the single, central point of management for all deployed out-of-band and inline switches. The controller enables pervasive security and visibility for physical, virtual, and container workloads for single, multi-site, and cloud deployments.

BMF-EC provides both basic and advanced NPB functions. In addition to basics such as filtering, aggregation, replication, and load-balancing, it also provides advanced packet functions like deduplication and packet slicing. BMF-EC's advanced functions leverage the DPDK-powered, x86-based service nodes, supported by unique multi-tenant, monitoring-as-a-service functions on a scaled-out, open networking switch fabric managed centrally by the Big Mon controller. BFC-EC also integrates with x86-based analytics and recorder nodes to capture cloud-native data center traffic at scale. The nodes also support deep application-level analytics. The Big Mon Recorder Node allows high-performance packet recording, querying, and replay functions. The Big Mon Analytics Node provides unprecedented network visibility to monitor, discover, and troubleshoot network and application performance issues, as well as accelerating discovery of root causes of security breaches. With Big Mon Recorder and Analytics nodes, users can achieve deep network telemetry for both cloud-based and traditional data center environments. With these tools, the network team can replay past conversations across users and applications with a single click.

Big Mon's architectural flexibility allows it to easily extend to multi-cloud environments, including hybrid cloud and public cloud deployments, centrally managed via the Big Switch Networks Multi-Cloud Director.

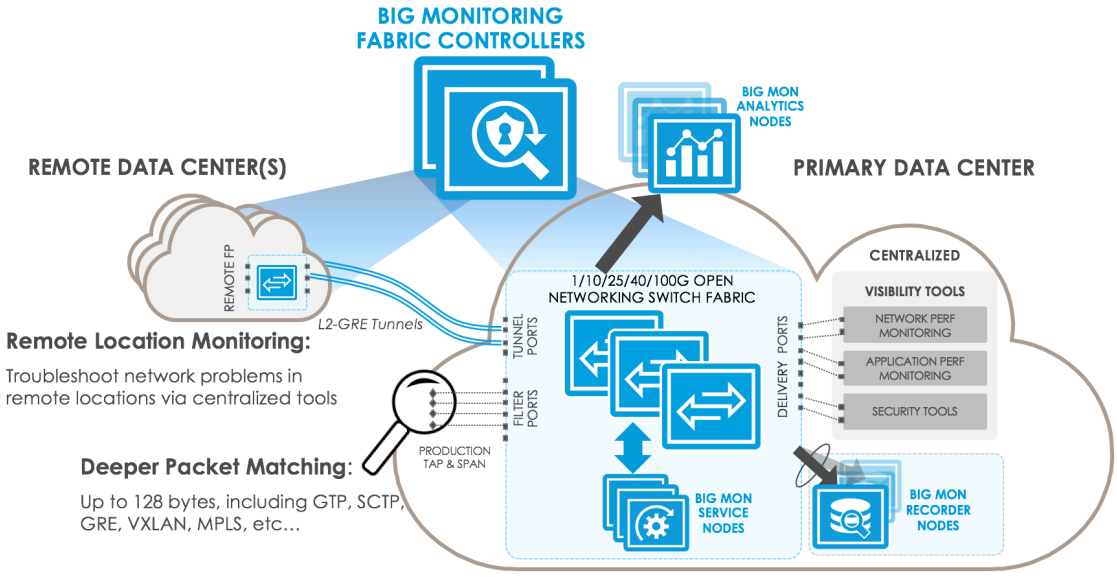

Figure 3: Big Monitoring Fabric — Monitor Every Location with Centralized Tools and Management

OUT-OF-BAND

Data center networks are transitioning to modern 10G/40G, 25G/100G, and 40G/100G designs to meet demands of cloud computing, data analytics, andr 4G/5G LTE mobile services. The corresponding traffic monitoring networks also need to transition to next-generation designs. The exponential growth in data center size, bandwidth, and traffic and the demand for monitoring a greater portion of network traffic together test the limits of traditional monitoring/visibility designs. The traditional box-by-box approach based on proprietary network packet brokers (NPBs) has proven to be cost prohibitive and too operationally complex for organization-wide monitoring.

With BMF-EC scale-out architecture, simplified operations, and open switch economics, the BMF-EC Out-of-Band deployment mode is rapidly becoming an attractive alternative to NPBs. Two popular use cases have emerged:

- Pervasive security and visibility: monitor or secure every link.
- Multi-site Monitoring: monitor or secure remote DCs/POPs/ branches/sites or public cloud* environments.

BMF-EC OOB supports topology agnostic, highly scalable fabrics. Depending on the customers' requirements, a range of topologies is supported—from a single-switch fabric to a scale-out, multi-switch/multi-layer fabric. A typical multi-layer BMF-EC OOB fabric design has a layer of open Ethernet switches labeled as filter switches and a layer of open Ethernet switches labeled as delivery switches. Most switch interfaces in the filter-switch layer are wired to passive optical taps or switch/router/ firewall SPAN ports in the production network; they are configured as filter interfaces in the Big Mon controller software user interface. Switch interfaces in the delivery-switch layer are wired to tools and are configured as delivery interfaces. Filter interfaces (where packets come in to the fabric) and delivery interfaces (where packets go out of the fabric to tools) represent the primary functions of BMF-EC OOB.

.

In Scale-Out Designs

- A 3-layer topology is recommended. A 3rd core layer of switches goes between the filter and delivery switch layers. The core switches aggregate traffic from the filter switches and send it to requisite delivery switches to forward to the necessary tools.
- Service interfaces may be configured: packets can be sent to one or more Big Mon Service Nodes or NPBs for advanced packet services, like deduplication, packet slicing, regex matching, header stripping, packet masking, or IPFIX/NetFlow generation in a chain before delivery to the security or performance monitoring tools. The Big Mon Service Node provides a simple, high-performance and cost-effective solution wherever specialized packet functions are required. In this design, IT can efficiently repurpose existing high-priced NPBs by chaining them as services nodes to the BMF-EC OOB, thereby protecting the investment.
- Monitor every location: Enterprises can extend BMF-EC OOB across L3 WAN to enable monitoring of remote DCs/POPs, colo facilities, campus/branch locations,and retail sites, as well as public cloud* environments. This allows centralized monitoring tools and staff in few data centers, dramatically reducing capex and opex while empowering operations teams to monitor networks across the entire organization. By simply deploying a commodity Ethernet switch at each monitored location, the entire BMF-EC OOB (including remote location switches) is operated with high availability and managed centrally via the Big Mon controller.
- OOB (including remote location switches) is operated and managed centrally via the Big Mon Controller with high availability.

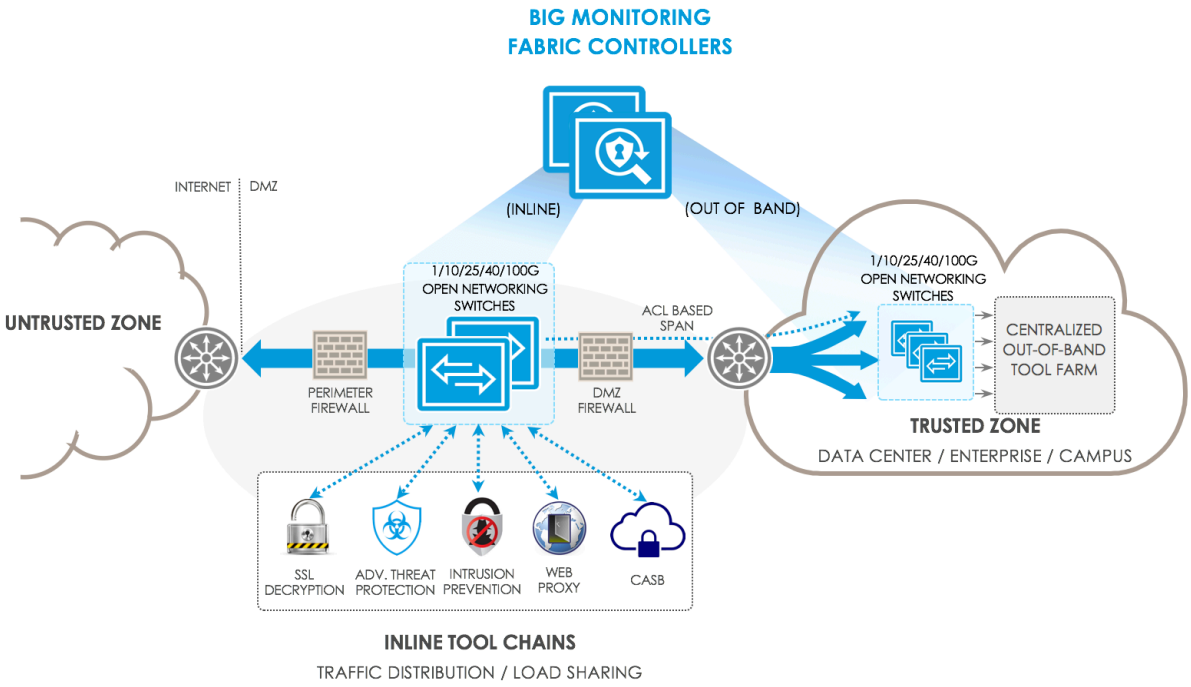

Figure 4: Big Monitoring Fabric Inline In-band Security and Monitoring Tool Chaining in the DMZ

INLINE

Network security for organizations has never been more important in light of continued cyber attacks. In addition, security practices that monitor and secure the network are rapidly changing, as the networks must provide more services, such as cloud computing, Big Data, and BYOD.

As a result, netowork design and maintainance must balance priorities of high performance and resilience, while ensuring that it remains compliant and secure against intrusions and attacks. To address these challenges, many enterprises prefer inline monitoring and security in the DMZ/extranet environment. Inline security tools can assess every packet and actively prevent or block detected intrusions before they can manifest and do damage.Inline security architecture poses new challenges, however, in terms of high availability, continued maintenance, and scalability.

BMF-EC Inline enables pervasive security in the DMZ and addresses the challenges faced by traditional solutions while offering lower-cost and SDN- centric operational simplicity.

BMF-EC Inline consists of a Big Mon controller and open Ethernet switches deployed in high-availability configuration. The inline security tools directly connect (optionally via link aggregation) to the Ethernet switches. Leveraging the Big Mon controller as the central point of management, BMF-EC Inline configures policies that create paths through the inline tools. The solution supports load balancing across multiple instances of the same tool as well as chaining of a set of tools on a per-policy basis.

Key Feature Highlights:

High-Availability Architecture

- Highly resilient against network, tool or controller failures.
- Supports customizable inline health check with aggressive health timers.

Tool Chaining and Sharing

- Supports chaining of up to 5 tools in a single chain. Supports different toolchains for traffic coming into and leaving the DMZ. Optionally, the same tool interfaces can be shared across multiple chains on the switch.
- Supports single-armed service and tools.
- Supports the ability to SPAN traffic from various points in the chain.

Tool Oversubscription/Load Balancing

- Load balance higher data bandwidth (10G/25G/40G/100G) across multiple instances of lower bandwidth tools (1G/10G/25G/40G).

Enhance Tool Efficiency

- Sends only relevant traffic, as opposed to all traffic.
- Supports dynamic, programmatic (REST API-based) configuration to drop certain marked flows (e.g. DDoS) or even bypass (whitelist) certain flows for a tool on the switch. In such scenarios, the fabric switch drops the marked flows rather than ending flows to the tool in order to drop them.

Simplify Multi-Team Operational Workflows

- Single-pane-of-glass management and configuration. No complex, error-prone PBRs needed. Easily load-balance or chain tools.
- Replicates certain traffic (at line-rate) via a rule-based SPAN to send to offline tools for further processing.

The Big Mon Controller is the unified, single point of management for inline/out-of-band monitoring.

FEATURE	DESCRIPTION / BENEFIT
Cloud-Native/ Virtual Workload Monitoring (VM/Container/Cloud)	• Support scalable, agentless monitoring of Virtual Machines. • Support centralized, dynamic VM monitoring. • Support centralized, dynamic container monitoring*. • Monitor cloud-native workloads and deliver them to various monitoring/security/ compliance tools*.
Advanced Filtering & Deeper Packet Matching Capabilities	• L2/L3/L4 header filtering on ingress and packet replication (as required) in the fabric for multiple egress tools. • Deeper Packet Matching (DPM) with masking (up to 128 bytes in packet). Supports matching on inner header fields for encapsulated packets (e.g MPLS, VXLAN, GRE) and/or protocols (e.g. GTP, SCTP). • IPv4 and IPv6 based filtering. • IPv4, IPv6, MAC Address masking, TCP Flags, DSCP matching. • Support filtering on inner VLAN of a Q-in-Q packet
Specialized Packet Functions	• Packet De-duplication—Enhances tool efficiency, by dropping duplicate packets. • Packet Slicing—Improves security and tool throughput by stripping off the payload. • Packet Masking—Improves security by hiding user/confidential information such as Credit card, SSN, passwords, medical or financial data to comply with SOX, HIPAA and PCI regulations. • Regex Pattern matching—Improves filtering of traffic based on regex patterns anywhere within the packet. • Header stripping for VXLAN, Cisco Fabric Path, LISP, PPPoE, ERSPAN and MPLS packets. Generic user-defined header stripping function is also supported. • IPFIX/Netflow/sFlow Generation Function is also supported. • L2GRE tunnel packet decapsulation. • VLAN tag stripping—Useful for stripping RSPAN tag. • VLAN tag push—Useful for filter interface tagging. • Match on inner packet post stripping. • GTP correlation—Associates user plane GTP-u data with control plane GTP-c sessions based on IMSI, IMEI, and TEID. Supports load balancing of GTP correlated data to multiple analytics tools while preserving subscriber data flow consistency without any filtering or drops. Supports filtering, whitelisting, and blacklisting of subscriber traffic. • UDP Replication – Supports replication of UDP packets like NetFlow, IPFIX, sFlow, Syslog, and SNMP and send them to multiple, different collectors • Additional specialized packet functions (like SSL decryption) can be realized by service chaining 3rd party NPBs as service nodes
Big Mon Recorder Node	• Enables Traffic Capture for Cloud-Native Network Defense & Rapid Remediation at Scale • Leverages easy to use, scale-out, high performance industry-standard x86 based appliances • Integrated / centralized configuration and operational workflows via Big Mon Controller • Feature-rich capturing, querying and replay functions • Supports PTP / NTP based timestamping • Programmable and scriptable via REST APIs

Big Mon Analytics Node	• Enables app-aware analytics for cloud-native network defense and rapid remediation at scale. • Leverages easy to use, scale-out, high performance industry-standard x86 based appliances. • Integrated/centralizes configuration and operational workflows via Big Mon Controller. • Supports various health/capacity planning/troubleshooting dashboards. • Supports performance views like Top Talkers, Top Apps, TCP connection/latency tracking. • Supports security views displaying rogue DHCP/DNS servers, identifies IP/MAC spoofing. • Support various host views such as New Hosts seen and what OS is on the hosts. • Supports automatic alerting on exceeding various thresholds such as link utilization. • Supports sFlow/NetFlow collection to provide real time application level visibility, including tunneled or encapsulated traffic, enable detection of security attacks like DoS/DDoS and support sub-second triggering.
Network-Wide Visibility (Monitor or Tap Every Rack)	• Packet filtering, aggregation, tool port load-balancing, and packet replication functions. • Single switch or scale-out 1/2/3 layer fabric designs: 1G, 10G, 25G, 40G & 100G. • Centralized fabric/policy definition and instrumentation of open Ethernet switches within the network. • Programmatic event-triggered monitoring (via REST API). • Multiple overlapping match rules per filter interface based on a variety of L2, L3, L4 header, as well as via deeper packet matching (DPM) attributes. • Time/packet-based scheduling of policies. • Efficient utilization of open Ethernet switch capabilities via Controller Policy Optimizer Engine.
High Performance, Highly Scalable Network Monitoring Fabric	• High availability for the controller as well as the fabric. • Auto Fabric Path Computation that detects and responds to failures in the monitoring network. • Policy-based load balancing of core links with failover detection to efficiently utilize fabric bandwidth and ensure resiliency. • Detection of service node/link failure and an option to bypass the service. • Link aggregation (LAG) in the open Ethernet fabric (including across core links, service node links, and delivery links). • Tagging policy or tap (filter) interfaces. • Supports a variety of security and monitoring tool vendors. • Supports a variety of NPBs as stand-alone or chained service nodes.
Centralized Management, Configuration, Troubleshooting	• Big Mon Controller is the single pane of glass for fabric and policy management. • Policies can be configured from a centralized controller to forward flows from multiple filter interfaces to multiple delivery interfaces, including optional service nodes. Packet replication is made at the last common node to optimize the fabric bandwidth. • GUI, REST API, and CLI for configuration and viewing operational state. • Centralized interface, flow, and congestion-statistics collection. • Simplified install/upgrade of the fabric via the Big Mon Controller (zero-touch fabric). • Supports IPv6 Management IP address. • Supports virtual IP addresses for the controller high-availability pair.
Multi-DC/Multi-Site Tunneling (Tap Every Location)	• Centralized monitoring of remote DCs/POPs/branches/sites (across L3 WAN). • Support tools located in a single tool farm in a centralized DC. • Replication of packets across tunnels. • Tunneling at 1G, 10G, 25G, 40G and 100G bandwidths. • Rate limiting of monitored traffic before entering L3 WAN. • Tunneling enabled on a per-switch basis.

Security and Controlled Access (Monitoring as a Service)	• TACACS+, RADIUS-based authentication and authorization. • Role-based access control (RBAC) for administratively defined access control per user. • Multi-tenancy for advanced overlapping policies across multiple user groups to monitor the traffic from the same tap interface to various tool interfaces. • Tenant-aware Web-based management GUI, CLI, and REST API. • Self-service monitoring across multiple groups/business units using the same underlying infrastructure.
Packet Capture (With Controller Hardware Appliance Only)	• Quick and easy 1G/10G interface available for packet capture on the controller hardware appliance. • Additional 1TB hard disk available. • Configurable auto deletion of older pcap files.
Marker Packet Generation	Injection of a marker packet into the tool or pcap file.
BigSecure Architecture	• Enables Dynamic Cyber-defense for Terabit DDoS attack mitigation. • Enables DDoS detection tools to offload dynamic, large scale attack mitigation to the underlying network.
Fabric wide CRC check (Graphical User Interface)	Allow/Disallow bad CRC packets in the production network to reach the tools for analysis.

Rich Web-Based GUI	• The dashboard shows the resources used by the fabric as well as a bird's eye-view of the topology.
	• A highly attractive as well as functional GUI topology view that shows:
	  • All the switches/ports in the fabric.
	  • Paths taken across the fabric on a per-policy basis.
	  • An intelligent context-sensitive properties panel triggered by a mouse-over on a topology object.
	• Customizable tabular views that persist according to user preferences.
	• Various table export options like JSON and CSV are available throughout the GUI.
	• Presents a highly intuitive, simplified management and operations workflow.

Support for Ethernet-Based Open Switch Vendors	Support for 1G, 10G, 25G, 40G and 100G switches from Dell, HPE, Accton and Quanta. The common supported switch configurations: • 48x1G + 4x10G • 12x10G + 3x100G (BRCM Maverick ASIC) • 48x10G + 4x40G (BRCM Trident/Trident+ ASIC) • 48x10G + 6x40G (BRCM Trident-II/Trident-II+ ASIC) • 48x25G + 6x100G (BRCM Tomahawk+ ASIC) • 32x40G (BRCM Trident-II/Trident-II+ ASIC) • 64x40G (BRCM Tomahawk ASIC) • 32x100G (BRCM Tomahawk ASIC) For the complete list of supported switch vendors/configurations and optics cables included in the Big Monitoring Fabric Hardware Compatibility List (HCL), please contact the Big Switch Sales Team (sales@bigswitch.com).

BIG MON CONTROLLER APPLIANCE SPECIFICATION

The Big Mon Controller can be deployed either as a virtual machine appliance on an existing server or as a hardware appliance.

Controller VM Appliance Specifications

The Big Mon Controller is available as a virtual machine appliance for the following environments.

ENVIRONMENT	VERSION
Linux KVM	Ubuntu 12.04 Ubuntu 14.04
VMware ESXi	Version 5.5.0 U1 Version 5.5.0 U2 Version 6.0.1 Version 6.0.5

Note: The above table explicitly indicates the Major/Minor/Maintenance versions tested and supported by Big Mon – Enterprise Cloud. Versions other than the ones listed above will not be supported.

MINIMUM VM REQUIREMENTS
4 vCPU with a minimum scheduling of 1GHz
8 GB of virtual memory
400 GB of Hard disk
One virtual network interface reachable from physical switches

Note: A VM's performance depends on many other factors in the hypervisor setup, and as such, we recommend using hardware appliance for production deployment.

Big Mon Controller Hardware Appliance Specification (BMF-CTLR-HWB)

The Big Mon controller is available as an enterprise-class, 2-socket, 1U rack-mount hardware appliance designed to deliver the right combination of performance, redundancy, and value in a dense chassis.

FEATURE	TECHNICAL SPECIFICATION
Processor	Intel Xeon 2 sockets (6/8 cores)
Form Factor	1U Rack Server
Memory	4 x 16GB
Hard Drive	2 x 1TB SATA (with RAID support)
Networking	4 x 1GB; 2 x 10GB
Power	Dual Hot-Plug Power supply 500W - 550W

Big Mon Controller Hardware Appiance Specification (BMF-CTLR-HWDL)

The Big Mon controller is available as an enterprise-class, 2-socket, 1U rack-mount hardware appliance designed to deliver the right combination of performance, redundancy, and value in a dense chassis.

FEATURE	TECHNICAL SPECIFICATION
Processor	Intel Xeon 2 sockets (10 cores)
Form Factor	1U Rack Server
Memory	4 x 16GB
Hard Drive	2 x 1TB SATA (with RAID support)
Networking	2 x 1GB; 2 x 10GB, 2 x 10GB Base-T
Power	Dual Hot-Plug Power supply 550W

BIG MON SERVICE NODE HARDWARE APPLIANCE SPECIFICATION (BMF-SN-HW, BMF-SN-HWBL, BMF-SN-HWC, BMF-SN-HWDL)

The Big Mon Service Node appliance is an enterprise-class, NEBS Level 3 & ETSI compliant, 2-socket, rack-mount hardware appliance, designed to deliver the right combination of performance and value. It is available in 2 form-factors:

- 1U w/ 4x10G bidirectional interfaces.
- 2U w/ 16x10G bidirectional interfaces.

The Big Mon Service Node provides specialized packet functions like deduplication, packet slicing, header stripping, regex matching, packet masking, GTP correlation, UDP replication and IPFIX/ NetFlow generation. Once connected to the fabric, the Big Mon controller auto-discovers the service node and becomes the single, central point of management and configuration of the service node. This highly scalable architecture allows chaining of multiple service nodes that are connected to the fabric via the service node chaining function of the Big Mon Fabric – EC.

FEATURE	TECHNICAL SPECIFICATION	
	SERVICE NODE (STANDARD)	SERVICE NODE (LARGE)
Processor	Intel Xeon 1 socket (12 cores)	Intel Xeon 2 sockets (12 cores)
Form Factor	1U Rack Server	2U Rack Server
Memory	4 x 8GB RDIMM, 2133 MT/S, Single Rank (HW) 6 x 8GB RDIMM, 2666 MT/s, Single Rank (HWC)	8 x 8GB RDIMM, 2400 MT/S, Single Rank (HWBL) 12 x 8GB RDIMM, 2666 MT/s, Single Rank (HWDL)
Hard Drive	1 x 1TB SAS	1 x 1TB SAS
Networking	4 x 10Gb; 4 x 1Gb (HW) 4 x 10Gb; 2 x 10Gb + 2 x 1Gb (HWC)	16 x 10Gb; 4 x 1Gb (HWBL) 16 x 10Gb; 2 x 10Gb + 2 x 1Gb (HWDL)
Power	Dual Hot-Plug Power supply 500W - 1100W	Dual Hot-Plug Power supply 800W - 1100W

BIG MON ANALYTICS NODE HARDWARE APPLIANCE SPECIFICATION (BMF-AN-HWA)

The Big Mon Analytics Node appliance is an enterprise-class, 2-socket, rack-mount hardware appliance designed to deliver the right combination of performance and value. It is available in a 1RU form-factor.

Big Mon Analytics Node provides scale-out analytics with configurable, historical time-series based dashboards for health, performance, capacity planning and security. It also acts as a collector for NetFlow and sFlow packets to provide real-time application level visibility, including tunneled or encapsulated traffic, enable detection of security attacks like DoS/DDoS, and support sub-second triggering. The highly intuitive and customizable GUI dashboards support a Google-like search to quickly drill down and focus on the possible issues quickly. It not only provides variety of reporting and alerting functions but also allows the user to easily share custom dashboard views with other team members for collaborative analysis, troubleshooting, and remediation.

Figure 6: Big Mon Analytics Node.

FEATURE	TECHNICAL SPECIFICATION
Processor	Intel Xeon 2 sockets (10 cores)
Form Factor	1U Rack Server
Memory	8 x 16GB
Storage	2 x 1TB SATA, 2 * 960GB SSD SAS)
Networking	2 x 1Gb; 2 x 10Gb, 2 x 10Gb Base-T
Power	Dual Hot-plug Power supply 550W

BIG MON RECORDER NODE HARDWARE APPLIANCE SPECIFICATION (BMF-RN-HWA)

The Big Mon Recorder Node appliance is an enterprise-class, NEBS Level 3 & ETSI compliant, 2-socket, rack-mount hardware appliance, designed to deliver the right combination of performance, capacity, and value. It is available in a 2RU form-factor, supporting a 1x10G interface and a total available storage of 160TB.

The Big Mon Recorder Node provides high-performance packet recording, querying, and replay functions. Once connected to the fabric, the Big Mon controller auto-discovers the recorder node, ensuring a single point of configuration and device lifecycle management. Multiple recorder nodes can be clustered together to present a view of a single, logical recorder node that allows users to store more network traffic for longer periods and retrieve packets from the single logical recorder node interface via the controller. This architecture provides true scale- out characteristics while maintaining the agility and simplicity in the user workflows. The recorder node provides feature-rich capture, query, and replay functions. The recorder node allows the user to replay the specifics of an event to derive root cause and predict future trends for various performance issues and security threats.

FEATURE	TECHNICAL SPECIFICATION
Processor	Intel Xeon 2 sockets (12 cores)
Form Factor	2U Rack Server
Memory	12 x 16GB
Storage	16 x 10TB SAS, 2 x 3.84TB SAS SSD
Networking	2 x 1Gb Base-T; 2 x 10Gb, 2 x 10Gb Base-T
Power	Dual Hot-Plug Power supply 1100W

ABOUT BIG SWITCH NETWORKS

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, Big Mon Recorder Packet, and Big Mon 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.

big switch networks

Headquarters
3111 Coronado Drive, Building A
Santa Clara, CA 95054, USA

+1.650.322.6510 **TEL**
+1.800.653.0565 **TOLL FREE**

www.bigswitch.com
info@bigswitch.com