Big Monitoring Fabric enables pervasive security and monitoring of network traffic for an organization and selectively delivers it to multiple security, monitoring, performance measurement and compliance tools—both Inline and Out-of-Band. Leveraging an Open Ethernet switch fabric and an SDN controller, Big Monitoring Fabric is a highly scalable and cost-effective network visibility solution.

**BIG MONITORING FABRIC OVERVIEW**

Big Monitoring Fabric (Big Mon) is a next-generation Network Packet Broker (NPB) that leverages SDN-powered, high-performance, open networking switches to provide pervasive security and visibility of an organization’s network traffic, while reducing total cost of ownership (TCO). Big Monitoring Fabric addresses the challenges of traditional NPB solutions, by enabling a scale-out fabric for enterprise-wide monitoring, a single pane of glass for operational simplicity, and multi-tenancy for multiple IT teams (NetOps, DevOps, SecOps) for tenant-specific inline or out-of-band deployments.

**ARCHITECTURE: SDN SOFTWARE MEETS OPEN SWITCH HARDWARE**

Big Mon’s architecture is inspired by Hyperscale Networking designs, which consist of Open Ethernet switch hardware, SDN controller software and centralized tool deployment.

The Big Monitoring Fabric architecture consists of the following components:

- HA pair of SDN-enabled Big Monitoring Fabric Controllers —VMs or hardware appliances—that enable centralized configuration, monitoring and troubleshooting in a simplified manner.
- 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 Nodes (optional)— DPDK-powered, x86-based appliances that connect to the Big Mon fabric (either single or as part of a service node chain) to provide advanced packet functions like de-duplication, packet slicing, header-stripping, regex matching, packet masking, GTP correlation, UDP replication and NetFlow generation.
- Big Mon Recorder Nodes (optional)— x86-based appliances that connect to the Big Mon fabric and managed via the Controller to provide petabyte packet recording, querying and replay functions.
- Big Mon Analytics Nodes (optional)— x86-based appliances that integrate with the Big Mon fabric to provide multi-terabit, security and performance analytics with configurable, Historical time-series dashboards.

Get hands-on experience with our offering, register for a free online trial at:
labs.bigswitch.com

Contact our sales team at:
sales@bigswitch.com

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

*Tech Preview
**BIG MONITORING FABRIC—PRODUCT DESCRIPTION**

Big Mon switches can be deployed in either of the two deployment modes:

- **Out-of-Band**—Deployed adjacent to the production network. Connects to SPAN/TAP ports from the production network.
- **Inline**—Deployed in the DMZ or Extranet (production network).

Big Monitoring Fabric Controller continues to be the single, central point of management for all its out-of-band as well as inline deployed switches. It provides pervasive visibility for physical, virtual and cloud workloads for single / multi-site / cloud deployments.

Big Monitoring Fabric provides not only basic NPB functions like Filtering, aggregation, replication, load-balancing, but also provides advanced packet functions like de-duplication, packet slicing etc. leveraging the DPDK-powered, x86-based service nodes along with unique, multi-tenant, ‘monitoring as a service’ functions on scale-out, open networking switch fabric managed centrally via the Big Monitoring Controller. Furthermore, it also integrates with x86-based Analytics Nodes and Recorder Nodes to capture cloud-native data center traffic at scale as well as provide deep application-level analytics. Big Mon Recorder Node allows high-performance packet recording, querying and replay functions, and Big Mon Analytics Node provides unprecedented network visibility to monitor, discover and troubleshoot network and application performance issues as well as accelerate root cause of security breach discovery. With Big Mon Recorder and Analytics Nodes, customers can now achieve deep network telemetry for both cloud-based and traditional data center environments and have the ability to replay past conversations across users and applications with a single-click. Big Mon’s architecture flexibility allows it to easily extend to multi-cloud environments, including hybrid cloud and public cloud deployments.

---

**SIGNIFICANT CAPEX/OPEX SAVINGS**

The Big Monitoring Fabric enables a high-performance, integrated NPB + Analytics + Packet capture solution, to enable rapid detection and analysis of network performance and security anomalies leveraging open networking switches and commodity HW to provide significant CAPEX/OPEX savings. On the other hand, the traditional NPB-based approach has high TCO due to ever-expanding box-by-box deployment, proprietary hardware and under-utilization (or inefficient use due to organizational silos) of tools—which results in box-level limited data center visibility.

**Open Networking Switch / Industry-standard Server Economics**

Big Monitoring Fabric utilizes the underlying cost efficiencies of the high performance, open networking switches, as well as the industry-standard x86 based appliances, and as a result, it is much more cost-effective to monitor larger volumes of network traffic than vertically integrated NPB solutions.

**SDN-Enabled Operational Efficiencies**

Big Monitoring Fabric is provisioned and managed through the single pane of glass—Big Monitoring Fabric controller CLI, GUI or REST APIs. This operating model allows for an easier integration with existing management systems as well as monitoring tools and hence significantly reduces the operational costs associated with box-by-box management of traditional NPBs.
As data center networks transition to modern 10G/40G and 40G/100G designs to meet demands of cloud computing, data analytics and/or 4G/5G LTE mobile services, the corresponding traffic monitoring networks also need to transition to next-generation designs. The exponential growth seen in data center size, bandwidth and traffic, as well as the demand for a higher portion of network traffic to be monitored have been testing the limits of the traditional monitoring/visibility designs. Traditional box-by-box approach based on proprietary Network Packet Brokers (NPBs) has proven to be cost prohibitive and operationally complex for organization wide monitoring.

With Big Mon’s scale-out architecture, simplified operations and open switch economics, the Out-of-Band deployment mode is rapidly becoming an attractive replacement for NPBs, creating two popular use cases:

- Pervasive Security & Visibility (monitor or secure every link)
- Multi-site Monitoring (monitor or secure remote DCs/POPs/branches/sites or public cloud* environments)

Big Monitoring Fabric 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 Big Monitoring 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 and 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 the Big Monitoring Fabric.

In scale-out designs:

- A 3-layer topology is recommended in which the 3rd “core” layer of switches may be used between the “filter” and the “delivery” switch layers. These switches aggregate traffic from the filter switches and send them to requisite delivery switches to forward to the necessary tools.
- “Service interfaces” may be configured where packets can be sent to one or multiple Big Monitoring Fabric Service Nodes or NPBs for advanced packet services, like de-duplication, packet slicing, regex matching, header stripping, packet masking or Netflow Generation in a chain prior to 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. At the same time, the customers can repurpose (and thus protect their investment on) their existing high-priced NPBs in an even more efficient manner, by chaining them as services nodes to the Big Monitoring Fabric.
- Monitor Every Location: Big Monitoring Fabric can be extended across L3 WAN to enable monitoring of remote DCs/POPs, colo facilities, campus/branch locations, retail sites as well as public cloud* environments. This allows centralization of monitoring tools and staff in few data centers, thus dramatically reducing CapEx and OpEx cost while allowing operations teams to monitor networks across the entire organization. By simply deploying a commodity Ethernet switch at each monitored location, the entire Big Monitoring Fabric (including remote location switches) is operated and managed centrally via the Big Mon Controller with high availability.
Network security for organizations has never been more important in light of continued cyber attacks. Additionally, security practices that monitor/secure the network are rapidly changing, as the networks are demanded to provide more services like cloud computing, Big Data, and BYOD.

As a result, it is paramount to design and maintain the high-performance and resilient characteristics of the network, while ensuring that it is compliant and secure against intrusions/attacks. To address these challenges, customers prefer using inline monitoring and security in their DMZ/Extranet environment. Security tools, by virtue of being inline, can assess every packet and actively prevent or block intrusions that are detected before they can manifest and do the damage. However, inline security architecture poses new challenges in terms of high availability, continued maintenance, and scalability.

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

Big Mon 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 these Ethernet switches. Leveraging the Big Mon controller as the central point of management, Big Mon 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.

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

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

**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**
  - Support chaining of up to 5 tools in a single chain. Supports different tool chains for traffic coming into/leaving the DMZ. Additionally, the same tool interfaces can also be shared (optional) across multiple chains on the switch.
  - Support single-armed service/tools
  - Supports ability to SPAN traffic from various points in the chain.

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

- **Enhance Tool Efficiency**
  - Send 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 the flows to the tool to drop them.

- **Simplify Multi-team operational workflows**
  - Single Pane of Glass management/configuration; No complex, error-prone PBRs needed; Easily load-balance or chain tools.
  - Replicate 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.
<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION / BENEFIT</th>
</tr>
</thead>
</table>
| **Cloud-Native/ Virtual Workload Monitoring** | • 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 either cloud-based or on-premise monitoring 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.  
• 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.  
• 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 & 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
- Supports various Health / Capacity Planning / Troubleshooting dashboards
- Supports Performance views like Top Talkers, Top Apps, TCP connection / latency tracking etc
- Supports Security views displaying Rogue DHCP/ DNS servers, identifies IP / MAC Spoofing etc
- Support various Host views like New Hosts seen, what OS is on the hosts etc
- Supports Automatic alerting on exceeding various thresholds like link utilization etc
- 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.
- Ensures 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 Monitoring Fabric Controller is 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 HA 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 the centralized DC in a centralized DC.  
• Replication of packets across tunnels.  
• Tunneling at 1G, 10G, 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 & 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** | • Architecture enabling 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 which 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 which are persisted as user preferences.  
• Various table export options like JSON, 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, 40G and 100G switches from Dell, Accton and Quanta. The common supported switch configurations are:  
• 48x1G + 4x10G  
• 48x10G + 4x40G (BRCM Trident/Trident+ ASIC)  
• 48x10G + 6x40G (BRCM Trident-II/Trident-II+ 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 as well as optics/cables, included in the Big Monitoring Fabric Hardware Compatibility List (HCL), please contact the Big Switch Sales Team (sales@bigswitch.com). |
**BIG MONITORING FABRIC CONTROLLER APPLIANCE SPECIFICATION**

The Big Monitoring Fabric Controller can be deployed either as a Virtual Machine appliance on an existing server or as a Hardware Appliance.

### Controller VM Appliance Specification

The Big Monitoring Fabric Controller is available as a Virtual Machine appliance for the following environments.

<table>
<thead>
<tr>
<th>ENVIRONMENT</th>
<th>VERSION</th>
</tr>
</thead>
</table>
| Linux KVM   | Ubuntu 12.04  
|             | Ubuntu 14.04 |
| VMware ESXi | Version 5.5.0 U1  
|             | Version 5.5.0 U2  
|             | Version 6.0     |

*Note:* The above table explicitly indicates the Major/Minor/Maintenance versions tested and supported by Big Monitoring Fabric. Versions other than the ones listed above will not be supported.

### Minimum VM Requirements

- 2 vCPU with a minimum scheduling of 1GHz.
- 4 GB of virtual memory.
- 20 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-CTRLR-HWB)

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

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>TECHNICAL SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Xeon 2 sockets (6/8 cores)</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1U Rack Server</td>
</tr>
<tr>
<td>Memory</td>
<td>4 x 16GB</td>
</tr>
<tr>
<td>Hard Drive</td>
<td>2 x 1TB SATA (w/RAID support)</td>
</tr>
<tr>
<td>Networking</td>
<td>4 x 1Gb; 2 x 10Gb</td>
</tr>
<tr>
<td>Power</td>
<td>Dual Hot-plug Power supply 500W - 550W</td>
</tr>
</tbody>
</table>
Big Mon Controller Hardware Appliance Specification (BMF-CTLR-HWDL)

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

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>TECHNICAL SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Processor</strong></td>
<td>Intel Xeon 2 sockets (10 cores)</td>
</tr>
<tr>
<td><strong>Form Factor</strong></td>
<td>1U Rack Server</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>4 x 16GB</td>
</tr>
<tr>
<td><strong>Hard Drive</strong></td>
<td>2 x 1TB SATA (w/RAID support)</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td>2 x 1Gb; 2 x 10Gb, 2 x 10Gb Base-T</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>Dual Hot-plug Power supply 550W</td>
</tr>
</tbody>
</table>
The Big Monitoring Fabric Service Node appliance is an enterprise-class, NEBS Level 3 & ETSI Compliant, 2-sockets, rack-mount hardware appliance, designed to deliver the right combination of performance and value. It is available in 2 form-factors:
- 1U w/ 4x10G bi-directional interfaces, and
- 2U w/ 16x10G bi-directional interfaces.

The Big Mon Service Node provides specialized packet functions like de-duplication, packet slicing, header-stripping, regex matching, packet masking, GTP correlation, UDP replication and 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 Monitoring Fabric.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>TECHNICAL SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SERVICE NODE (STANDARD)</td>
</tr>
<tr>
<td>Processor</td>
<td>Intel Xeon 1 socket (12 cores)</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1U Rack Server</td>
</tr>
<tr>
<td>Memory</td>
<td>4 x 8GB RDIMM, 2133 MT/s, Dual Rank, x8 Data Width</td>
</tr>
<tr>
<td>Hard Drive</td>
<td>1 x 1TB SAS</td>
</tr>
<tr>
<td>Networking</td>
<td>4 x 10Gb; 4 x 1Gb</td>
</tr>
<tr>
<td>Power</td>
<td>Dual Hot-plug Power supply 500W - 1100W</td>
</tr>
</tbody>
</table>
BIG MONITORING FABRIC ANALYTICS NODE HARDWARE APPLIANCE SPECIFICATION (BMF-AN-HWA)

The Big Monitoring Fabric Analytics Node appliance is an enterprise-class, 2-sockets, 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 view with other team members for collaborative analysis, troubleshooting and remediation.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>TECHNICAL SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Xeon 2 sockets (10 cores)</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1U Rack Server</td>
</tr>
<tr>
<td>Memory</td>
<td>8 x 16GB</td>
</tr>
<tr>
<td>Storage</td>
<td>2 x 1TB SATA, 2 x 960GB SSD SAS</td>
</tr>
<tr>
<td>Networking</td>
<td>2 x 1Gb; 2 x 10Gb; 2 x 10Gb Base-T</td>
</tr>
<tr>
<td>Power</td>
<td>Dual Hot-plug Power supply 550W</td>
</tr>
</tbody>
</table>
BIG MONITORING FABRIC RECORDER NODE HARDWARE APPLIANCE SPECIFICATION (BMF-RN-HWA)

The Big Monitoring Fabric Recorder Node appliance is an enterprise-class, NEBS Level 3 & ETSI Compliant, 2-sockets, 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.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>TECHNICAL SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel Xeon 2 sockets (12 cores)</td>
</tr>
<tr>
<td>Form Factor</td>
<td>2U Rack Server</td>
</tr>
<tr>
<td>Memory</td>
<td>12 x 16GB</td>
</tr>
<tr>
<td>Storage</td>
<td>16 x 10TB SAS, 2 x 3.84TB SAS SSD</td>
</tr>
<tr>
<td>Networking</td>
<td>2 x 1Gb Base-T; 2 x 10Gb, 2 x 10Gb Base-T</td>
</tr>
<tr>
<td>Power</td>
<td>Dual Hot-plug Power supply 1100W</td>
</tr>
</tbody>
</table>

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 industrystandard 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.