Big Monitoring Cloud–Enterprise Cloud

The Recorder Node: What Can It Do for You?

Introduction

Network packet recording is taking its place as an essential tool for security and network operations teams. Whether for digital forensics, cybersecurity, troubleshooting, or compliance, packet recording assists in resolving many issues that require historical packet traces to identify and remediate.

Network packet recording usually takes one of two approaches. The first uses the standalone approach; traffic is forwarded with little pre-processing intelligence from within the monitoring fabric. The second is to filter, remove duplicates, and analyze packets from within the fabric prior to reaching and storing within the recorder node. The second approach significantly enhances the quality and readiness of the recorded data for rapid retrieval and troubleshooting.

The Recorder Node (as one of the optional add-ons) to the Big Switch Networks® Big Monitoring Fabric™ (Big Mon) solution selectively captures and stores packet data as fed in from the Big Mon intelligent fabric. The Big Mon Service and Analytics nodes filtered out the non-important packets, while also identifying and alerting on anomalies; this, in turn, improves the quality and efficiency of the data being stored within the Recorder node.

Use Case Overview

Recorded packet data that can be quickly searched and played back has many uses for operations teams. The more common ones include the following:

- Troubleshoot and solve complex security, connectivity, and performance problems including:
  - Data privacy/piracy breaches
  - Ransomware attempts
  - Phishing attacks
  - Unauthorized downloads
  - Denial of services attacks
  - User access of untrusted or unknown websites
  - Anomalous forwarding of mail
- Performing IT forensics and post mortem investigations
- Documenting security and privacy compliance
- Troubleshooting network connectivity and performance issues

---

The six use cases listed within this document offer examples on how packet recording coupled with the intelligence of Big Mon can help network and security operators resolve cybersecurity and operations issues faster, and with greater dexterity. To better understand this here is a quick tutorial on Big Mon Fabric.

Big Monitoring Fabric Background

Big Monitoring Fabric-Enterprise Cloud offers a second generation out-of-band security monitoring solution that intelligently redirects production traffic across a non-disruptive scale-out fabric, deployed on open hardware. Big Mon Fabric leverages the state-of-the-art processing capabilities in the open hardware including Layer 2/3 packet filtering within the switch ASICs, deep packet processing and analytics in x86 server appliances, and efficient packet recording in storage appliances. This approach offers the best price/performance solution for out-of-band monitoring solutions.

Moreover, Big Mon consolidates monitoring centrally for more efficient hosting of third-party operation and security tools. This saves on resources as well as fostering cross-department collaboration.

Big Mon is easily integrated with any production network, whether it is a high-speed data center network where protecting and optimizing applications is business critical, and/ or is a campus network where a lot of rogue devices are used. With the use of TAP, and/ or SPAN ports, Big Mon easily scales out, without the expense of custom switches, and costly NetFlow licenses.

> *"Big Mon's intuitive interface and configuration automation has enhanced our security visibility while reducing our operations overhead.*
>
> **—Infrastructure engineer, Visa**

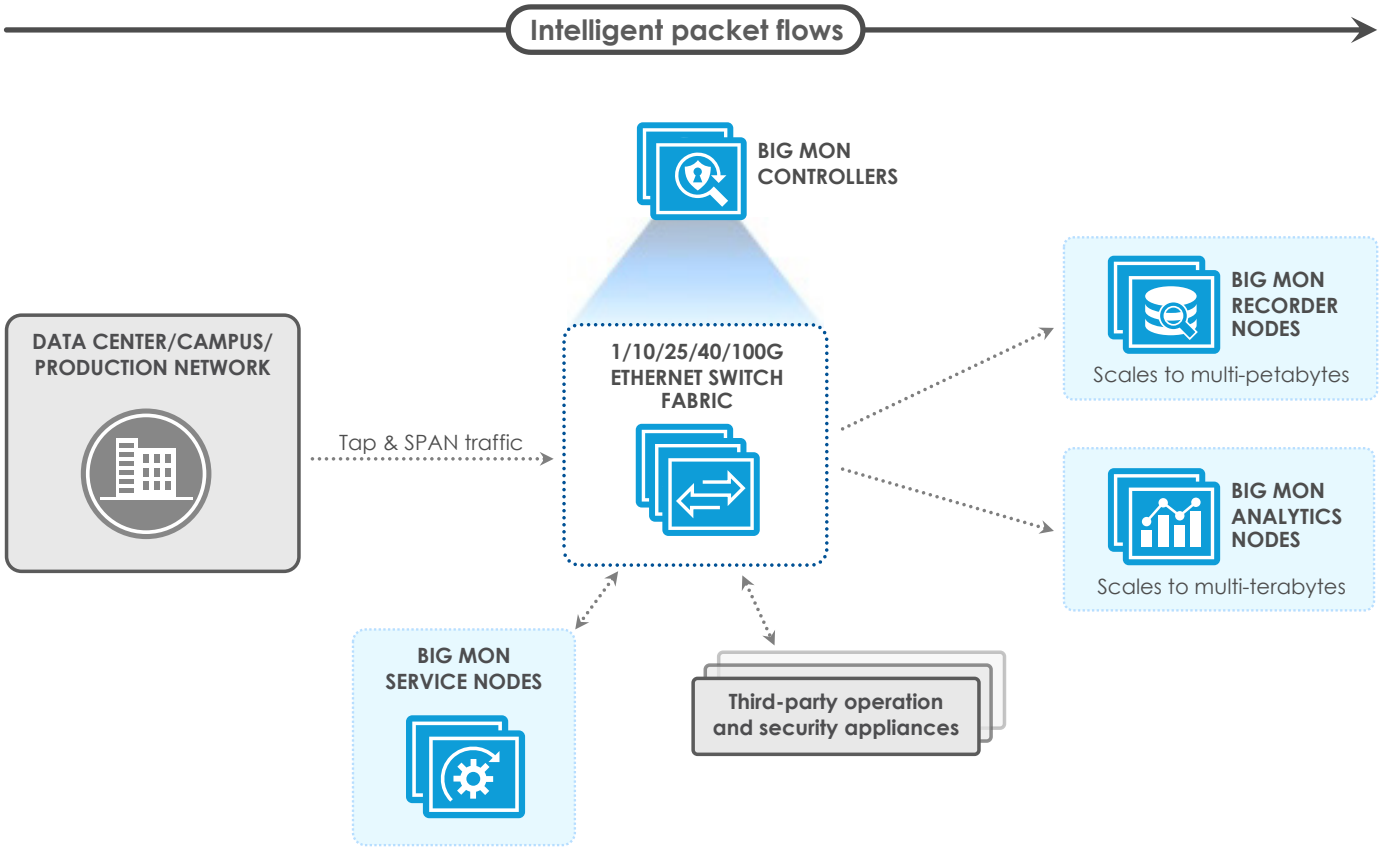

Figure 1. The out-of-band Big Monitoring Fabric-Enterprise Cloud diagram shows packet flows from left to right. Packets are redirected and filtered at wire rate, and intelligently filtered before consumption by the security and monitoring tools. This approach significantly reduces the overall cost of ownership by eliminating unnecessary data processing and storage within the end-node tool appliances.

Putting Network Recording to Use

Recording packet data can be storage intensive, given that only a fraction of what's stored may eventually prove critical to the business, its digital assets, and its reputation.

Filter and capture the relevant data

Optimizing packet-recording resources is analogous to efficient video surveillance. It takes only a few minutes of recorded video to help solve security or behavioral issues. The better the system is at filtering out or discarding irrelevant video, the lower the system's cost of ownership. Recording network/packet data works the same way. Intelligent preprocessing can analyze and scrub the data before recording, thus reducing the required amount of storage and retrieval rates for packet recorders. The easy-to-manage preprocessing and integrated workflows are key benefits of the Big Mon Fabric approach.

Configure easily with GUI, CLI, and API options

IT can easily configure the filters, preprocessing, and analytics workflows via the user-friendly Big Mon Fabric controller interface. The same user interface controls the Recorder Node, the Service Node, and the Analytics Node, offering a consistent user experience across the entire Big Switch Networks solution. Further, IT can choose between the Big Mon CLI, GUI, and/or APIs depending on their interface preferences. For the non-network centric users, the GUI offers a fast-intuitive interface for configuring, visualizing and retrieving recorded data.

Exploring Recorder Node Use Cases

Consider these six use cases that outline how network professionals and their companies benefit from the Big Mon Fabric Recorder Node.

Troubleshoot challenging network outage, performance, and connectivity issues

Network operation teams use the Big Mon Fabric Recorder Node to diagnose reported problems that they cannot reproduce. Playback lets the teams reach back an hour, a day, a week, or further into the past. Replay is sometimes the only way to analyze a problem and determine whether it's systemic, threatening, or just ephemeral. Several users employ Big Mon Fabric Record Node to help diagnose and remediate real-time streaming applications including voice over IP (VoIP) and video. For example, the Recorder can take a recorded TCP/IP session (conversation) and replay this to see the jitter conditions, determine the severity, and then track the issue to the root cause. Without the recorded VoIP calls (as an example), the network team would have had no way to analyze and resolve the issue—and to learn how to prevent it in the future.

Perform forensic analysis for data-privacy breach tracing and troubleshooting

Unauthorized or unintended data sharing outside "IT" trust zones is a common problem. Many violations take place by forwarding data from a personal account to someone outside the trust zone. Further, hackers are always looking for a way in. One of the more common ways in is to exploit a firewall setting that is weak or has not been updated with other changes within the infrastructure. Once a concern, hack, or violation surfaces, the security team must delve into the data to identify compromised data sources and find out where the improperly shared data originated, who sent it, and where it went.

Packet recording plays an essential role when issues arise. Packet header information includes most of the details required to determine the relevant type, source, destination, and time of day. Network teams can configure Big Mon to monitor and record data sources that are most sensitive (patient records, credit card information, personal data, employee data, financial data, for instance) and track only the packet activities specific to that data. The teams can quickly scan the recorded packet data via an easy to use GUI, choosing attributes for sorting the data. That helps find the right fingerprint for taking data breach security actions.

Audit suspicious activities

Many ops teams employ the Recorder Node to audit suspicious activities. That includes VoIP calls, use of untrusted or unknown websites, access of confidential databases, email traffic, file forwarding activities. The Recorder Node records the selected activities and offers clear evidence; security staff can then take action with evidence to back them up. Sophisticated recording options allow for continuous, on-demand, or buffered event-based recording. Teams can filter specific endpoints, subnets, VLANs, traffic types, and port types to record only suspicious activities.

Recorder node resource optimization

Packet recording can consume a lot of disk storage, and not all traffic types, applications, and places in the network are equally critical to monitor and record. Big Mon Fabric Recorder Node deployments leverage the X86 based filtering capabilities within the Big Mon Service Node to use recorder storage efficiently. Filtering the data prior to recording reduces both the storage required and the amount of data to analyze. A Service Node (or more than one) performs preprocessing, such as packet deduplication, packet slicing, and other tasks to optimize recorder storage (see Advantages of Integration). The slimmed-down data sent to the Recorder Node provides enough information on the nature of an attack or violation, with no need to store the entire payload or every copy of a packet.

This approach offers best-in-class search and fast retrieval. Fast retrieval is criticality important when troubleshooting severity one outage and security issues.

Integrated analytics and automate workflows for sophisticated security detection and mitigation

The amount of monitoring data being generated within data centers in general has become too voluminous to handle without the assistance of "machine intelligence. Moreover, machine learning intelligence is being added into workflows, where detection, alerting and even remediation is becoming automated. As each customer has their own unique workflows (often referred to as "runbooks") they need APIs that they can easily program. The integrated multi-function architecture of the Big Mon Fabric solution supports network workflow automation with open APIs.

As an example, several network teams have integrated Big Mon Fabric with third-party intrusion detection (IDS) tools. These teams have created workflows where they send filtered traffic from the Big Mon fabric to their 3rd party IDS tool of choice. Upon detection of a security event, the third-party tool triggers the recorder node to begin recording the traffic. They then leverage the APIs in retrieving the recorded data and for sending to other third-party tools for deeper analytics. The interaction between these tools is automated via the Big Mon APIs.

Replay source to test security patches and fixes

Security detection and mitigation is a moving target. Security tool vendors frequently release patches and updates in response to new security threats and attacks. Many network pros test the effectiveness of updates before deploying them, especially after a breach. The best way to test is with real traffic data. The Big Mon Fabric Recorder Node playback mode enables convenient testing of security patches and fixes with real traffic data. This ensures that the patch and/or updates work as promised.

Summing Up

In summary, network-based packet recording continues as a go-to tool for security and network operations.

As the importance of packet recording grows, network operators can optimize resources by carefully considering how to architect and deploy the technology to avoid wastefully capturing too much data that offers no value.

The Big Monitoring Fabric approach to packet recording is based on a systems approach. Recording effectiveness benefits from wire-speed packet filtering, packet preprocessing, and analytics as integrated workflows. Network operators benefit from reduced total cost of ownership, scaling as needed, and a unified experience across all components of the solution.

Resources

For a hands-on demo of Big Mon Fabric, please click labs.bigswitch.com.

Go deeper into data packet recording in the white paper.

View the Recorder Node product page.

Advantages of Integration

The Big Monitoring Fabric solution smoothly integrates the Recorder Node with Big Mon Analytics Node and Service Node. All three nodes readily scale out to meet growing demand.

Big Mon can integrate third-party service chains, too.

Services of the Big Mon Service Node

- Deduplication
- Packet slicing
- Packet masking
- Header stripping
- Regex matching
- NetFlow generation
- GTP correlation
- UDP replication
- Timestamping

Synergy with the Analytics Node

The Analytics Node makes short work of finding the needle in the haystack of data in the Recorder Node storage. Using built-in or customized settings, network teams can look for only particular anomalous packet data to swiftly zero in on sources and trace root causes.

> *Big Mon Fabric has allowed us to reinforce security posture by rapid impact analysis and mitigation of compromised user credentials.*
>
> **—Managing director, security operations and architecture, University of Oklahoma**

big switch networks

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

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

www.bigswitch.com
info@bigswitch.com