Automating GDPR Compliance for Network Monitoring and Security Infrastructure with Big Monitoring Fabric

Beginning May 25, 2018, the General Data Protection Regulation (GDPR)[1] enacted by the European Parliament will take effect, requiring organizations to protect the private data of citizens of all 28 EU member states. These regulations are designed to ensure the personal data privacy of EU subjects, including the deletion of personal data that is not required once transacted. Meeting these new regulations requires awareness of where data originates, as well as the ability to isolate and purge sensitive data as needed.

GDPR specifically applies to organizations that meet the following criteria:

- A presence in an EU country
- No presence in the EU, but handles personal data of EU subjects
- Greater than 250 employees
- Fewer than 250 employees but its activities impact the data rights of EU subjects

Given its broad scope, GDPR will have a significant impact on data handling operations not only for organizations operating within the EU, but nearly all organizations receiving and processing data from EU citizens. Assessing data processing operations and complying with GDPR by the 2018 deadline poses a significant challenge, as its regulations may apply across multiple groups, business units and technology tiers within an organization.

One obvious area within IT that will be impacted by GDPR is network monitoring and security infrastructure and its associated processes.

GDPR Impact on Network Monitoring and Security

Network monitoring and security tools are designed to receive and process traffic from the network for the purposes of assessing performance or security threats. Network traffic frequently includes data — encrypted or unencrypted — that could be defined as private, such as credit card information or transaction history.

Given that most data center operators have tools to monitor and secure their network and applications, they run the risk of incurring penalties if any of this infrastructure receives the private data of EU subjects, particularly if these tools do not "need" to see the sensitive data, in the way that, for instance, an e-commerce system may need to briefly access it for transaction purposes.

Organizations must continue to monitor and secure their networks even as they're subject to privacy regulations. But getting and staying GDPR compliant without compromising security or performance visibility into the network is no easy task — particularly if your data center processes data from multiple regions and deploys multiple tools and network recorders. Figuring out what incoming traffic requires extra-sensitive handling, and under what circumstance it can be accessed — then automating its delivery to tools — is critical to getting and staying GDPR compliant, even as traffic flows increase.

Leveraging Big Monitoring Fabric to Achieve GDPR Compliance

Big Monitoring Fabric is a next-generation visibility and security architecture that enables organizations both within and outside EU countries to more effectively implement GDPR compliance practices.

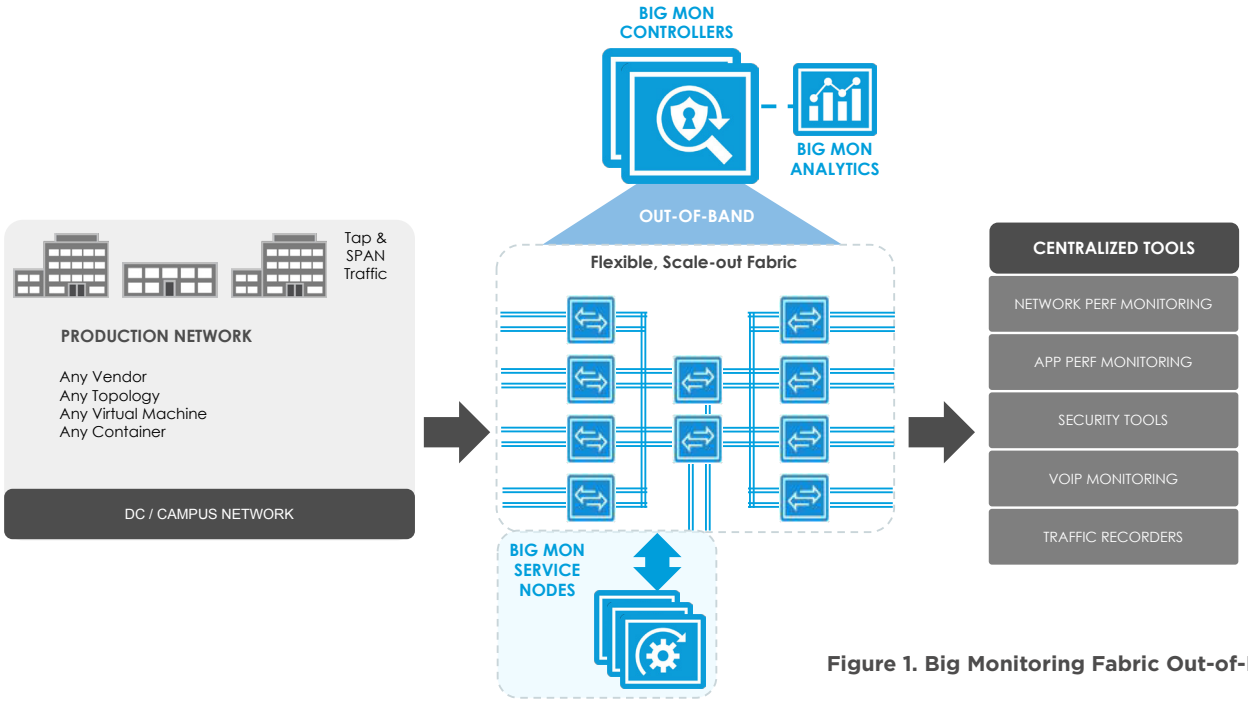

Figure 1. Big Monitoring Fabric Out-of-Band

Big Mon combines the functions of traditional network packet brokers (NPBs) with the intelligence, agility and flexibility of a software-defined networking fabric. It delivers network packets to both passive and active performance and security tools, and allows network and security teams to define delivery policies for every tool, including the identification and elimination of sensitive data before it reaches tools.
Unlike traditional NPBs, which function box-by-box, Big Mon acts as a single logical NPB — built with open networking switches and x86-based DPDK Service Nodes, managed from a high-availability controller. This superior design allows the entire visibility and security architecture to be operated — and data delivery defined — through a single pane of glass. Every tool has continuous or on demand visibility into all traffic, across every rack, every location, and every workload.

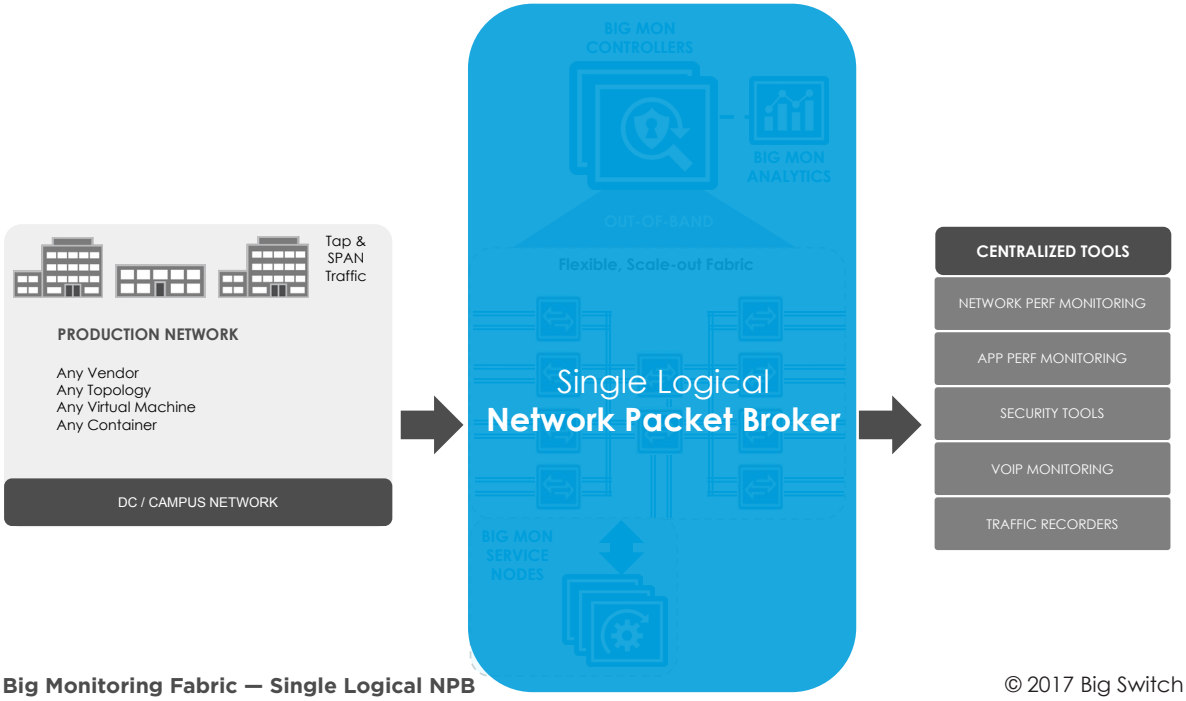

Figure 2. Big Monitoring Fabric — Single Logical NPB

All traffic delivery rules, including packet aggregation and filtering, advanced packet handling, and flow generation are programmed through the controller. Tools can be centrally located, policies can be uniformly rolled out, and troubleshooting can be done with a few clicks. No need to manually map traffic to each tool. Tool policies set at the controller automatically map the right traffic to the right tool at the right time.

A built-in Analytics module also provides critical traffic context, while optional Service Nodes enable advanced packet handling.
Because Big Mon provides the "eyes" into the data center network for a variety of monitoring and security applications, it can be used to ensure that these applications do not receive data that could breach GDPR standards. One or all of the following capabilities can be leveraged for GDPR compliance:

1 - OBSCURE PRIVATE INFORMATION

One of the most important capabilities for GDPR compliance is the removal of personal data that should not be transferred to a tool or application. Big Mon enables data center operators to automate data removal in several ways, including packet masking and packet slicing.

PACKET MASKING

Packet masking, leveraging Big Mon's Service Node, enables users to mask a defined portion of a packet (e.g., the payload) for the purposes of preventing that information from reaching unauthorized systems.

PACKET SLICING

Big Mon's Service Node also enables a packet to be sliced at a particular offset in order to eliminate sensitive or unneeded data.

The removal of sensitive data through these and other options (such as non-delivery of sensitive packets) can be defined and automated through Big Mon's single pane of glass.

2 - SECURELY MONITOR SENSITIVE DATA

Most sensitive data traversing the network is encrypted, which denies APM/NPM tools the visibility needed for them to do their job. SSL decryptors must be deployed to decrypt this traffic. Big Mon's unique next-gen architecture enables scalable security service chaining, where an SSL decryption tool feeds decrypted traffic to one or multiple tools and then re-encrypts it before forwarding the traffic to its destination. Users can also leverage Big Mon's single pane of glass to gain visibility across their security infrastructure and ensure that their organization's security policy is complied with — even when the security infrastructure is deployed at multiple remote locations.

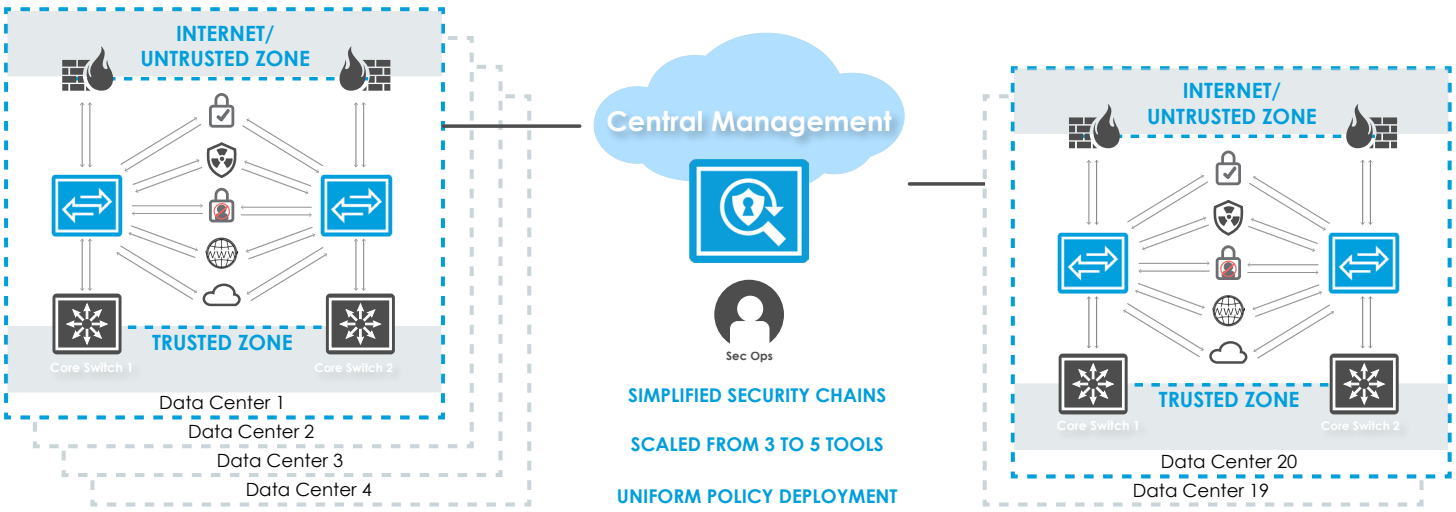

Figure 3. Fortune 20 Energy Company deploys Big Mon Inline in global data centers

3 - GAIN UNPARALLELED VISIBILITY AT SCALE

NETWORK ANALYTICS
Big Mon Analytics module gathers and displays top talkers, top applications, top flows, and various other host, application, flow, and latency related information from the production network. It also displays various policy, event, and interface statistics for the Big Mon Fabric itself. This information can be visualized through configurable dashboards of historical time-series based graphs in the graphical user interface (GUI).

The Analytics module available through Big Mon can be used to identify traffic and users covered by GDPR — for example, based on traffic geolocation tags or other user identifiers.

FILTERING POLICIES BASED ON GDPR RELEVANCE
Once relevant traffic has been identified, policies can be set up on Big Mon to automate the segmentation of that traffic for additional handling from one or more points in the production network before it is delivered to one or more tools.

ROLE-BASED ACCESS CONTROL (RBAC)
Big Mon allows traffic to be delivered based on specific tools or users, which may be useful as part of comprehensive data management framework, as some tools and systems may be granted access to sensitive data for legitimate, allowable use — such as may be the case where the use is time-limited, or where there is a court mandate in place.

Once traffic that is subject to GDPR has been defined and access assigned based on tool or user, further actions can be implemented to more sensitively handle this data.

Conclusion

While the implementation of a comprehensive GDPR compliance framework may be challenging, aligning your monitoring and security infrastructure with the EU's new regulations can be as simple as leveraging Big Monitoring Fabric for your network visibility requirements. With Big Mon, network owners can now precisely define the traffic each tool receives — eliminating unnecessary or sensitive data so that tools can perform at their best and information privacy is assured.

Big Monitoring Fabric is the next-generation visibility fabric today's data centers demand, enabling network owners to realize the benefits of pervasive network visibility for all monitoring and security tools, while simplifying and automating regulatory compliance.

1. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf