

Protecting Sensitive Data During Monitoring

Traffic Visibility in Compliance With Data Protection Regulations

Over the last two decades, governments around the world have passed legislation regulating the flow of personal information across the global network. In 1996, the United States of America introduced the Health Insurance Portability and Accountability Act (HIPAA), followed by the Payment Card Industry Data Security Standard (PCI-DSS) in 2004 – both of which are in force today.

China and other countries have enacted cyber security laws over the past decade. China’s most recent law was adopted in 2016 and went into effect in June 2017.

In 2016, the European Union introduced the General Data Protection Regulation (GDPR), which has been enforced since May 2018.

The purpose of these regulations is to protect individual privacy and other sensitive data, given that so much of our personal information is in electronic form, stored in servers, and transmitted across networks.

Network monitoring must comply with data protection regulations. NETSCOUT® monitoring and security solutions, in particular its nGenius® Packet Flow System (PFS) products, help ensure that network visibility monitoring operations comply with these regulations, whether in localized datacenters, within the cloud, or in a hybrid network.

Necessary Features for Visibility Network Compliance

Data protection regulations define the types of personal data that may be collected and recorded, as well as where this data can be sent. For compliance reasons, networking and security teams need to understand which countries’ data will be traversing the network, what paths the data will take, where the data will be stored, and the locations that will have monitoring tools and security applications deployed. Once this is understood, the company will need a visibility solution (such as a NETSCOUT PFX unified packet plane) that supports selectively removing or masking out data within packets and obfuscating monitoring traffic as it is backhauled from remote sites to central monitoring locations.



Figure 1: The NETSCOUT unified packet plane powered by PFOS (Packet Flow Operating System) logically separates the network from the monitoring systems.

Masking and Slicing

Data protection regulations may require organizations to configure applications in their network monitoring solutions to hide or remove data from the IP packets being monitored, such as IP addresses, credit card information, or other sensitive data contained in the payload¹ of the IP packet.

Data protection regulations may also restrict what data is allowed to be transmitted outside of an organization's network environment and across national borders. These restrictions can apply to monitoring traffic as well.

The NETSCOUT PFS portfolio supports conditional masking and slicing of certain IP packet types and at specific locations within the packets.

- Masking is the act of writing user-defined data over existing data in the IP packet, effectively hiding the original data, at a specified starting point in the packet.
- Slicing is the act of removing data from an IP packet, starting at a specified point. This has the added benefit of reducing the size of the packet and also the amount of traffic to be forwarded to the monitoring and security tools. Slicing may be preferable to masking if there are numerous elements of sensitive data scattered throughout an IP packet.

With the NETSCOUT solution, there is no limit as to where the masking or slicing occurs in each packet.

These capabilities are available on the nGenius Packet Flow eXtender (PFX) product which can be added to any PFS deployment requiring these functions.

Conclusion

Ensuring your network visibility solution complies with data protection regulations requires knowing your company, its network, and its monitoring and security needs.

Responsibility lies with the operators of the network, as well as the monitoring and security applications, to ensure data is protected by design and by default, managing the data control, forwarding, and processing functions.

NETSCOUT is ready to partner with you to help identify the needs of your monitoring and security infrastructure. NETSCOUT nGenius solutions provide the tools to enable you to successfully comply with modern data protection regulations.

¹ the part of the IP packet that is the "actual data," minus all headers and descriptive metadata attached for transport and routing through the network.



Corporate Headquarters
 NETSCOUT Systems, Inc.
 Westford, MA 01886-4105
 Phone: +1 978-614-4000
www.netscout.com

Sales Information
 Toll Free US: 800-309-4804
 (International numbers below)

Product Support
 Toll Free US: 888-357-7667
 (International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us