Plixer

BROCHURE

5 key steps for GDPR compliance

Intro

The General Data Protection Regulation (GDPR) was adopted in April 2016 and went into effect May 2018. The European Parliament established GDPR as a mechanism to protect the personally identifiable information (PII) of European Union citizens. PII, as defined by GDPR, does not only encompass details like name, address, and birthday, but is much broader and includes online identifiers such as IP address, MAC address, cookie data, etc.

GDPR provides EU citizens with specific rights pertaining to their PII and outlines how organizations must treat that data. GDPR has forced organizations to change the way they collect, store, manage, transmit, share, and protect PII.

Who GDPR applies to

Although the EU established GDPR, it extends legal liability beyond the borders of the EU so that any organization anywhere in the world that maintains any PII of EU citizens must comply.

Step 1: Understand where customer data is stored

First, you should review your network to determine every place where customer data is stored. GDPR covers all IT systems and devices, including mobile devices and public, private, and hybrid cloud environments.

Once you've established every place where customer data is stored, all traffic to and from those assets can be monitored with Scrutinizer.

Step 2: Leverage network traffic analysis to monitor every conversation

Under GDPR, data controllers must maintain a record of processing activities under its responsibility.

Once you know where customer data is stored, use Scrutinizer to monitor every conversation and understand who has accessed what data. Use security analytics in conjunction to look for and alarm on abnormal behavior. Then, if and when you encounter an issue, you will have access to historical forensic data to investigate it. This will allow incident response team members to quickly identify root cause, remediate the problem, identify what information may have been accessed, and return the business to normal.

Step 3: Monitor for data exfiltration

Now that you know where sensitive data exists and who has rightful access, you can employ a least privilege approach to ensure that only those people access it, as well as look for patterns indicating low-and-slow data theft.

This can be difficult, however, if the security and network teams work in data silos. In many organizations, the network team has exclusive access to traffic information that would be highly valuable to the security team.

Scrutinizer was designed as a single platform that both the network and security teams can use effectively. When both teams have access to the same data set, threats like low-and-slow data theft can be detected and mitigated much faster.

> ❝
> A network traffic analytics platform… is invaluable for any organization worried about GDPR compliance.”

Step 4: Set up a system for rapid investigation

The aspect of GDPR that is likely to cause organizations the greatest difficulty is the requirement of breach notification.

If a breach occurs at a data processor, they are obligated to notify the data controller without undue delay. Data controllers are legally obligated to notify the Supervisory Authority within 72 hours of becoming aware of a data breach. 72 hours is an incredibly small window of time to investigate and understand what happened. A network traffic analytics platform like Scrutinizer is invaluable for any organization worried about GDPR compliance. You must be able to collect details on every conversation on the network and be able to quickly deliver reports and identify root cause.

Step 5: Document an incident response process to help navigate the relevant data

Incident response preparedness is a combination of people, process, and technology:

People will always play a central role, and every organization must allocate resources with the specific responsibility of responding to security incidents.

Process is the definition of what should happen and when. The process defines who is involved, who must be notified, how information should be escalated, which departments must be engaged and which technology tools are available to the team.

Technology delivers the historical forensic data required to identify what happened and quickly return to normal.

Again, don’t treat security and network teams as separate. Incident response must be a cooperative effort, and both teams need access to a common data set.

By establishing a clear incident response plan and practicing regularly, your organization will be better prepared to quickly respond and contain an attack or intrusion.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.