Point of View

Gigamon and the European Union General Data Protection Regulation

Leveraging Pervasive Visibility to Achieve Compliance

Set to come into effect on May 25, 2018, the European Union (EU) General Data Protection Regulation (GDPR) is a regulation designed to ensure the data privacy and protection of all EU citizens by strengthening and unifying data protection legislation across Europe. The new regulation, which will replace the Data Protection Directive 95/46/EU adopted in 1995 to regulate personal data processing, was designed to improve trust in the emerging digital economy by giving individuals more transparency and control over the use of their personal data. It applies to any organization – regardless of geographical location – that collects or processes personal data on EU residents, and institutes high penalties for non-compliance – up to 4 percent of total global annual sales or €20 million per data breach.

Under the current Data Protection Directive, personal data constitutes any information relating to an identified or identifiable natural person who can be identified, in particular, by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity. Reflective of changes in technology and how organizations collect information on people, the GDPR expands this definition to include online identifiers such as:

- Internet Protocol (IP) addresses, in certain cases.
- Pseudonymized data, depending on the facility of attributing the pseudonym to an individual.

Data Controllers, Data Processors and Data Protection Officers

The GDPR applies to the data processing activities of businesses that are data controllers and data processors with an establishment in the EU. Bearing primary responsibility for compliance, a data controller decides on how and why personal data is processed and can include profit-seeking companies to charities or governments. A data processor, such as an IT firm, does the actual data processing on behalf of the controller.

Data controllers must ensure that personal data is gathered and processed lawfully and for a specific and legitimate purpose, for example, for the purposes of ensuring network and information security or reporting possible criminal threats. Individuals can order a business to erase their data without undue delay where one of the following grounds applies:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing.
- The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2).
- The personal data have been unlawfully processed.
- The data controller is subject to compliance with a legal obligation in Union or Member State law.
- The personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Not only must data controllers delete all copies or links to personal data where the individual withdraws consent but they must also take reasonable steps to inform other organizations that are processing said data. This is known as the "right to be forgotten." Similarly, under a provision called the "right to restriction," data must also be removed – pending investigation – if someone objects to the accuracy of their personal data.

43% of respondents do not have complete visibility into all data traversing their networks

66% of respondents believe that a lack of visibility over data makes GDPR compliance difficult

67% of respondents agree that network blind spots are a major obstacle to data protection in their organization

Source: "Hide and Seek: Cybersecurity vs. the Cloud," survey by independent market research company Vanson Bourne, August 2017.

It is the responsibility of data controllers to ensure their processor abides by the data protection laws and data processors must themselves abide by rules to maintain records of their processing activities. If data processors are involved in a data breach, they are also far more liable under the GDPR than under the current Data Protection Directive.

Data controllers are also responsible for appointing a data protection officer (DPO), whose job is to inform and advise on meeting the GDPR requirements. A DPO should plan to conduct an information audit across the organization to map data flows and document what personal data is held, where it came from and with whom it is shared. A DPO should also ensure the right procedures and technologies are in place to detect, report and investigate a personal data breach. At the same time, a DPO must monitor compliance with data protection policies and regularly review the effectiveness of data processing activities and security controls.

How to Demonstrate Protection and Compliance Using Gigamon

Though the GDPR is technically proscriptive and does not identify requisite tools or technologies, the reality is that many new and existing network security tools will be needed, including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), anti-malware, forensics solutions and next-generation firewalls targeting content-driven policy enforcement. It is also a near certainty that the GDPR will spur renewed investments in existing but lesser-used tool sets, such as:

- Data Loss Prevention (DLP): for identifying and preventing personal data misuse and loss of data in motion (DIM), as well as for auditing and classifying data at rest (DAR) and data in use (DIU).
- File Access Monitoring (FAM): for detecting unauthorized file access.
- Database Access Monitoring (DAM): for detecting unauthorized access to corporate databases.

These toolsets have two commonalities: They need pervasive access to the corporate network and they typically run slower than modern core network speeds. For example, most content-aware DLP tools run at 300-500Mbps, due to their need to perform computationally-intensive file extraction and content parsing. By comparison, a modern core network runs at 10Gbps or 40Gbps.

Traditionally, organizations have deployed DLP tools at the network edge, where they only see egressing data. Yet, most data loss incidents are non-malicious and represent business process failures or honest mistakes on the part of staff. Organizations can best see and remediate these types of incidents in the network core – not at the network edge. For example, how does a DLP tool at the network edge see a user download sensitive GDPR data to their workstation and onto a USB key? The DLP tool must have visibility into core traffic.

To maximize network traffic visibility and optimize the performance of cybersecurity tools – including DLP tools – Gigamon provides the GigaSECURE® Security Delivery Platform. With its ability to monitor and send the right traffic to the right tools at the right time, the GigaSECURE® Security Delivery Platform can form the backbone of any GDPR compliance exercise.

For example, the GigaSECURE Security Delivery Platform can prune out applications, such as video or Windows maintenance traffic, that a DLP does not need to see or analyze. Instead, by feeding a DLP only relevant data, such as emails with attachments, the platform increases the tool's efficiency and chances of catching unwarranted data sharing or exfiltration in a timely manner. An IPS uses Representational State Transfer (REST) to indicate to an endpoint DLP solution that it needs to enforce control of removable devices to prevent a possible data exfiltration event – for example, by blocking any writes to USB devices.

By leveraging the GigaSECURE Security Delivery Platform, organizations can connect these slower, yet powerful inspection tools to faster corporate networks and feed them only the traffic they need to see and analyze for maximum effectiveness.

The GDPR does not tolerate "barely good enough" protections. It requires organizations to demonstrate a high degree of security efficacy and effectiveness, which can be achieved with the GigaSECURE Security Delivery Platform. The Gigamon solution brings the pervasive visibility into network traffic that is needed to eliminate monitoring blind spots, vastly improve the accuracy and precision of data risk detection and help organizations meet the GDPR challenge.

1063-01 08/17

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com