Wazuh’s support for GDPR

Whitepaper

What is GDPR?

The European Union's General Data Protection Regulation (GDPR) has been drawn up to standardize data privacy legislation across Europe, with the main aim of providing data protection for all citizens of the European Union. To this end, it seeks to enhance the privacy of such data and also to reform the way in which EU organizations approach data privacy.

The GDPR replaces the Data Protection Directive 95/46/EC and was finally approved by the EU Parliament on 14 April 2016 with an implementation date set for 25th May 2018.

What are the objectives of GDPR?

As mentioned above, the main objective of the GDPR is to protect the personal data of European citizens. Going a little deeper, the GDPR aims to guarantee the privacy of such data, giving people more control over the use of their information by companies in terms of how the data is processed, stored and/or destroyed.

A secondary objective is to establish a simpler regulatory environment for international activities by facilitating business operations through the unification of data protection legislation in the EU.

Who is affected by GDPR?

Compliance with the GDPR is mandatory:

- For any organization with a physical presence in at least one EU country.
- For any organization that processes or stores data on citizens residing in the EU.
- For any organization that makes use of third-party services that process or store information about EU citizens.

It is the organization's responsibility to ensure compliance with data protection by indicating how it will be processed.

What data does GDPR process?

When we refer to personal data, we refer to any information concerning an identifiable person. In this sense, the definition of personal data has been significantly increased to include online identifiers, IP addresses, economic information and so on. There is special mention of data considered to be sensitive personal data (religious, political, racial, ethnic, etc.) and considered to be personal identification information. It is not just about data that can be used for fraud or identity theft. In addition, any data that is reflected as personal data in the Data Protection Act will also be considered as personal data in the GDPR. At this point, we can say that a data fissure is a security breach that leads to the alteration, variation, loss, destruction, unauthorized access or disclosure of personal data transmitted, stored or processed by an organization that must comply with the GDPR.

What sanctions can be applied for non-compliance?

Non-compliance with the GDPR is not to be taken lightly. The fines can reach as high as 4% of the company's annual revenue volume or up to EUR20 million, whichever is the greater. The aim of these high penalties is to prevent organizations from considering non-compliance with the GDPR.

What are the main pillars of GDPR?

The GDPR is based on eight fundamental rights:

- The right to be informed: Provides transparency on how the individual's personal data is used.
- The right of access: Provides access to the individual's personal data, how it is used and any supplementary information that may be used in conjunction with the personal data.
- The right to rectification: Provides the right to have the individual's personal data rectified if incorrect or incomplete.
- The right to erasure: Grants the right to have the individual's personal data removed from any place if there is no logical reason for its storage. Also known as the right to forget.
- The right to restrict processing: Allows the individual's personal data to be stored, but not processed.
- The right to data portability: It offers the possibility of requesting a copy of the individual's stored information for use by another organization.
- The right to object: Provides the right to object to the processing of the individual's personal data.
- The right not to be subject to automated decision making and profiling: Provides the right to object to automated decision making on the individual's personal data.

What measures should be taken to comply with the GDPR?

Based on the official GDPR document [Council of the European Union (April, 2016), "General Data Protection Regulation", Legislative acts and other instruments] and on compliance guidelines such as the RSA Osterman Research [Osterman Research, Inc. (July, 2017) "A Practical Guide for GDPR Compliance", An Osterman Research White Paper], we have drawn up a series of basic requirements for adhering to the GDPR.

Chapter	GDPR title	GDPR description	Wazuh mapping
gdpr_I	Chapter I General Provisions	Legal base to control and process personal data.	N/A
gdpr_II	Chapter II, Principles	Basic principles of the regulation.	N/A
	Chapter II, Article 5 Head1 (f)	Ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, verifying its modifications, accesses, locations and guarantee the safety of them. File sharing protection and file sharing technologies that meet the requirements of data protection.	gdpr_II_5.1.f
gdpr_III	Chapter III, Rights of the data subject	Regulation of the data subject's rights.	N/A
	Chapter III, Article 14, Head 2 (c)	Restrict the processing of personal data temporarily.	gdpr_III_14.2.c
	Chapter III, Article 17	Permanently erase personal information of a subject.	gdpre_III_17
gdpr_IV	Chapter IV, Controller and processor	Management of the control and processing of the data.	N/A
	Chapter IV, Article 24, Head 2	Be able to demonstrate compliance with the GDPR by complying with data protection policies.	gdpr_IV_24.2
	Chapter IV, Article 28, Head 3 (c)	Ensure data protection during processing, through technical and organizational measures.	gdpr_IV_28
	Chapter IV, Article 30, head 1 (g)	It is necessary to keep all processing activities documented, to know all the places where personal and sensitive data are located, processed, stored or transmitted.	gdpr_IV_30.1.g
	Chapter IV, Article 32, Head 1, (c)	Data Loss Prevention (DLP) capabilities to examine data flows and identify personal data that is not subject to adequate safeguards or authorizations. DLP tools can block or quarantine such data flows. Classify current data appropriately to determine specific categories of data that will be subject to the GDPR.	gdpr_IV_32.1.c
	Chapter IV, Article 32, Head 2	Account management tools that closely monitor actions taken by standard administrators and users who use standard or privileged account credentials are required to control access to data.	gdpr_IV_32.2
	Chapter IV, Article 33	Notify the supervisory authority of a violation of the data in 72 hours and in certain cases, the injured parties.	gdpr_IV_33
	Chapter IV, Article 35, Head 1	Perform a data protection impact evaluation for high risk processes. Implement appropriate technical measures to safeguard the rights and freedoms of data subjects, informed by an assessment of the risks to these rights and freedoms.	gdpr_IV_35.1

gdpr_IV	Chapter IV, Article 35, Head 7 (d)	Capabilities for identification, blocking and forensic investigation of data breaches by malicious actors, through compromised credentials, unauthorized network access, persistent threats and verification of the correct operation of all components. Network perimeter and endpoint security tools. Anti-malware and anti-ransomware to prevent malware and ransomware threats from entering your devices. A behavioral analysis that uses machine intelligence to identify people who do anomalous things on the network.	gdpr_IV_35.7.d
	Chapter IV, Article 37	Designate a data protection officer.	N/A
gdpr_V	Chapter V, Transfer of personal data to third countries or international	Prevent data being transferred outside the EU to a 3rd country or international organization (except for specific protections).	N/A
gdpr_VI	Chapter VI, Independent supervisory authorities	Each Member State shall provide that it is the responsibility of one or more supervisory authorities to monitor the application of this Regulation in order to protect the fundamental rights and freedoms of natural persons.	N/A
gdpr_VII	Chapter VII, Cooperation and consistency	The lead supervisory authority shall cooperate with the other supervisory authorities concerned and exchange all relevant information.	N/A
gdpr_VIII	Chapter VIII, Remedies, liability and penalties	Any interested party shall have the right to lodge a complaint with a supervisory authority.	N/A
gdpr_IX	Chapter IX, Provisions relating to specific situations	Member States shall reconcile by law the right to the protection of personal data, including processing for journalistic purposes and for purposes of N/A academic, artistic or literary expression.	N/A
gdpr_X	Chapter X, Delegated acts and implementing acts	Management of delegated acts and implementing acts.	N/A
gdpr_XI	Chapter XI, Final provisions	Manages relations with directives, previous agreements, commission reports and defines the entry into force.	N/A

Wazuh supports GDPR

As we can observe, certain requirements for GDPR compliance are strictly formal with no place for support at the technical level. However, Wazuh offers a wide range of solutions to support most of the technical needs of GDPR.

gdpr_II_5.1.f

It is necessary to ensure the confidentiality, integrity, availability, and resilience of the processing systems and services by ascertaining their modifications, accesses, locations and guaranteeing their security, as well as of the stored data. To control at all times access to the data, when access takes place and by whom and to control how the data is processed.

Data protection and file sharing technologies that meet data protection requirements are also necessary as it is vitally important to know the purpose of the data processing and whether the data processor, in the case of third parties, is authorized to do it.

Concept. File integrity monitoring.

One of the solutions that Wazuh offers is File Integrity Monitoring. Wazuh monitors the file system, identifying changes in content, permissions, ownership, and attributes of files that you need to keep an eye on.

Wazuh's **File Integrity Monitoring** (FIM) watches specified files and triggers alerts when these files are modified. The component responsible for this task is called Syscheck. This component stores the cryptographic checksum and other attributes of a known good file or Windows registry key and regularly compares it to the current file being used by the system, looking for changes. Multiple configurations are possible for monitoring in real time, in intervals of time, only specific objectives, etc. In the same way that personal data files are monitored, Wazuh can monitor the shared files to make sure they are protected.

gdpr_III_14.2.c

Occasionally, an individual may request that the processing of his or her personal data be temporarily restricted. The entity in charge of processing and storing such data must ensure that within the stipulated period of time there is no access to such data.

Concept. Temporary access restrictions.

With Wazuh we can review the alerts generated and check that there are no alerts in the period stipulated using Syscheck.

gdpr_III_17

In some scenarios, an individual may request the permanent deletion of their personal information. In this case, the entity in charge of the processing and storing of the subject's data must delete such information when the individual's request for deletion is accepted, normally when the storage of the same is meaningless.

Concept. Permanent data deletion.

Wazuh has the ability to monitor deleted files using Syscheck, ensuring that the individual's personal data has been permanently deleted in response to their request.

gdpr_IV_24.2

The ability to demonstrate GDPR compliance by complying with data protection policies. In most cases, it will be necessary to comply with additional security and data protection policies. Therefore, the entity in charge of processing and storing the data must be able to comply with these policies.

Concept. Policy and compliance monitoring.

With **Policy and compliance monitoring**, Wazuh monitors configuration files to ensure they are compliant with your security policies, standards and/or hardening guidelines. Agents perform periodic scans to detect applications that are known to be vulnerable, unpatched, or unsecurely configured.

Policy monitoring is the process of verifying that all systems conform to a set of predefined rules regarding configuration settings and approved application usage. Wazuh uses three components to perform this task: **Rootcheck**, **OpenSCAP,** and **CIS-CAT**.

gdpr_IV_28.3.c

Ensuring data protection during processing, through technical and organizational measures. In the process of processing data, it is necessary to ensure the protection and integrity of the same in order to avoid any alteration that may be harmful to the individual to whom the information belongs.

Concept. Data protection in the processing.

By using Syscheck and through technical measures, Wazuh can ensure this protection, monitoring and ensuring that the protection measures established in the security policies are complied with.

gdpr_IV_30.1.g

It is necessary to document all processes and activities to carry out an inventory of data from beginning to end and an to audit, in order to know all the places where personal and sensitive data is located, processed, stored or transmitted.

Concept. Document and record all data processing. Audit logs and events.

Wazuh facilitates the documentation of a large amount of information about file access and security. It offers the possibility to store all the events that the manager receives in archived logs. In addition to storing alerts in alert logs and the ability to use more logs and databases for various purposes, such as audits.

gdpr_IV_32.1.c

Tools may be needed to block or quarantine such data streams like a DLP. Properly classify current data to determine specific categories of data that will be subject to GDPR.

Concept. Categorize files.

Through **Active Response**, Wazuh can execute an action according to Syscheck alerts. These actions can create the desired quarantine zone for the specified data. Wazuh makes it possible to create specific rules for categorizing files. It also performs various countermeasures to address active threats, such as blocking access to an agent from the source of the threat when certain criteria are met. It can execute a script in response to the activation of specific alerts based on the alert level or rule group. Any number of scripts can be started in response to a trigger.

gdpr_IV_32.2

To control access to data, you will need account management tools that closely monitor actions taken by standard administrators and users using standard or privileged account credentials. In this way, the data protection officer will be able to check who is accessing and processing the data, whether they are authorized to do so and whether they are who they say they are.

Concept. Account management with/without privileges.

Wazuh offers functionalities to monitor access and use of standard or privileged accounts through its multiple monitoring tools.

gdpr_IV_33

Notify the supervisory authority of a violation of the data in 72 hours and, in certain cases, the injured parties. It is an obligation. Any breach of security that endangers the data stored or any violation of the

integrity and security of the same must be reported within the established period of time with a maximum delay of 72 hours.

Concept. Security breach notices.

Wazuh can facilitate this communication, for example, with a notice by mail when a specific alert or a group of alerts are triggered, related to the monitoring of files that contain the personal data. The rules used in event analysis can be configured to send emails to the relevant security officers.

gdpr_IV_35.1

Perform a data protection impact evaluation for elevated risk processes. Implement appropriate technical measures to safeguard the rights and freedoms of data subjects, informed by an assessment of the risks to these rights and freedoms.

Concept. Risks evaluation.

Wazuh has security measures in place to safeguard personal data and is able to support risk assessment by categorizing Syschek alerts for certain files. For example, you can add the alert level of an event to support a risk assessment.

gdpr_IV_35.7.d

Necessary security measures include data breach identification, blocking and forensic investigation capabilities for rapid understanding of access attempts through active breaches by malicious actors. This could occur through compromised credentials, unauthorized network access, active advanced persistent threats and verification of the correct operation of all components.

Security tools are necessary to prevent the entry of unwanted data types and malicious threats and to ensure that endpoints are not compromised when requesting access to the network, system, and data. Anti-malware and anti-ransomware are needed to ensure the integrity, availability, and resilience of data systems, to block and to prevent malware and rescue threats from entering devices.

Behavioral analysis services that use machine intelligence to identify people who do anomalous things on the network may be required to provide early visibility and alert when employees who become corrupt. Such tools can also highlight bizarre activities, such as employees logged on to devices in two different countries, which almost certainly means they are at risk for accounts.

Concept. Security monitoring.

To meet these security requirements, Wazuh provides solutions such as **Intrusion and Anomaly Detection**. Agents scan the system looking for malware, rootkits or suspicious anomalies. They can detect hidden files, cloaked processes or unregistered network listeners, as well as inconsistencies in system call responses. In addition, an integration of Wazuh with NIDS is viable.

Anomaly detection refers to the action of finding patterns in the system that do not match the expected behavior. Once malware (e.g., a rootkit) is installed on a system, it modifies the system to hide itself from the user. Although malware uses a variety of techniques to accomplish this, Wazuh uses a broad-spectrum approach to find anomalous patterns that indicate possible intruders. The main component responsible for this task is Rootcheck. However, Syscheck also plays a significant role.

We may become aware of application or system errors, misconfigurations, attempted and/or successful malicious activity, policy violations, and a variety of other operational and security issues through Wazuh rules. **Using Automated logs analysis**, Wazuh agents read operating system and application logs and securely forward them to a central manager for rule-based analysis and storage.

It is worth highlighting the ability to detect vulnerabilities. Now agents are able to natively collect a list of installed applications and to send it periodically to the manager (where it is stored in local SQLite databases, one per agent). In addition, the manager builds a global vulnerability database, using public **OVAL CVE** repositories and later cross correlating this information with the agent's application inventory data.

Why use Wazuh?

As we have just seen, Wazuh offers extensive support for GDPR compliance, but it can do much more. Wazuh will help you gain greater visibility into the security of your infrastructure by monitoring hosts at the operating system and application levels. This solution, based on lightweight multi-platform agents, provides:

- File integrity monitoring.
- Intrusion and anomaly detection.
- Automated log analysis.
- Policy monitoring and compliance.

This diverse set of capabilities is provided by integrating **OSSEC**, **OpenSCAP** and **Elastic Stack** into a unified solution and simplifying their configuration and management. Wazuh provides an updated log analysis ruleset and a RESTful API that allows you to monitor the status and configuration of all Wazuh agents. It also includes a rich web application (fully integrated as a **Kibana** app) for mining log analysis alerts and for monitoring and managing your Wazuh infrastructure.

With Wazuh you will have scalability and reliability, facilitated by the possibility of implementing a cluster-based model for managers to scale horizontally. Additionally, it can be deployed with **Puppet, Chef, Ansible** and **Docker**. Wazuh supports TCP for agent-manager communications and is equipped with anti-flooding functions to prevent large bursts of events from being lost or negatively affecting network performance. It also has AES encryption used for agent-manager communications.

Wazuh performs intrusion detection using an enhanced log analysis engine with native JSON decoding and has the ability to dynamically name fields. You can make use of native rules for **Suricata** and have a native integration with the **OwlH** project for Suricata. It is equipped with support for IP reputation databases (e.g. **AlienVault OTX**) and modules for native integration with **Amazon AWS** (pulling data from CloudTrail).

It's already used to follow various standards, implementing best of breed technical solutions to help companies comply with **PCI DSS** security controls, through a custom IDS rule set (for both OSSEC and Snort) to detect attacks that could compromise credit card data. Wazuh also supports the **GPG13** best practice guide which includes tasks such as event log management and the use of intrusion detection and prevention systems.

These are just Wazuh's main features, but there are more. As it is open-source software, its possibilities increase day after day. Therefore, there is no excuse not to try Wazuh.

References

Council of the European Union (April, 2016), “General Data Protection Regulation”, Legislative acts and other instruments URL: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf.

Osterman Research, Inc. (July, 2017) “A Practical Guide for GDPR Compliance”, An Osterman Research White Paper.

EU GDPR, https://www.eugdpr.org/, Last access 5/10/2018.

Agencia Española de Protección de Datos, https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf, Last Access 5/10/2018.