MLine
IT CONSULTING & SERVICES

GDPR Compliance IT Guide

Products	Description	GDPR Relevance
SIEM	Security Intelligence and Event Management (SIEM) technologies can be applied for facilitating compliance to GDPR and simplifying its integration with existing compliance regulations. A properly configured SIEM system can validate your data security controls by centrally collecting, normalizing, and managing data from across your environment. It can correlate data and events by using rules and alerts that are mapped to or translated to GDPR requirements. Most importantly, a SIEM system can provide 24x7 visibility of security through the use of dashboards and visualizations and gather and store evidence that proves you're in compliance with the appropriate GDPR controls. At glance a SIEM system can provide **Extensive auditing capability** **Privileged user monitoring:** Track privileged user accesses and activities carried out on personal data to ensure that data processing is performed in accordance with the GDPR. Detect and get alerted for user behavior anomalies in real time to prevent personal data leakage. **Breach prevention:** Collect logs from network perimeter devices (firewalls, IDSs, IPSs etc) and correlate the data with threat feeds to prevent breach attempts originating from outside the network. **Real-time data notifications:** Fulfil the GDPR requirement by detecting data breaches and generating an incident analysis report that provides information on a breach's impact. **Extensive reporting based on stored historic data/event logs**	Article 32: Security of processing. Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Also requires regular testing the effectiveness of technical measures for ensuring security of the processing Article 33: Notification of a personal data breach to the supervisory authority The GDPR will require companies to develop or update internal breach notification procedures to supervisory authorities within 72-hour. SIEM Systems can systematically collect event logs and produce the necessary alerts. SIEM internal database can store events for historical reasons. Article 34: Communication of a personal data breach to the data subject GDPR requires when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
Patch Management	Using Patch Management to identify and update missing patches and outdated third-party software on your Servers and workstations. GDPR requires an organization to ensure ongoing testing assessment and evaluation of data security measures.	Article 32: Section 1d Security of processing A Patch Management Server can be used to identify and update missing patches and outdated third-party software on your Windows servers and workstations. A Patch Management also enables you to inventory your Windows machines and report on unauthorized software installations on your network.
Risk Intelligence	Performs scans to discover personally identifiable information across your systems and points out potential vulnerabilities that could lead to a data breach. RI can audit PII data to help ensure it is being stored, in accordance to the requirements of GDPR. The reports from RI can be helpful in providing evidence of due diligence when it comes to the storage and security of PII data.	**Article 4(1), recitals 26 and 30 : *Definition of Personal data*** Companies need to know perfectly all information assets, know exactly what data is personal data and what data is not, be able to segregate it and handle it accordingly. For example, personal data may reside on: HR data client/customer data prospect/direct marketing/targeted advertising data etc.
Network Monitoring & Visibility Solutions	It's crucial to implement network monitoring in order to quick identify network issues breaches or potentially harmful attacks. Such solutions can provide beyond others Intelligent alerts Multi-vendor network monitoring Identification of Malicious or unauthorized traffic Updated and automated network topology and dependency aware intelligent alerts Monitoring encrypted traffic Identifying and masking personal data Analytical Compliance Reporting	Article 32: Security of processing Article 33: Notification of a personal data breach to the supervisory authority Article 34: Communication of a personal data breach to the data subject Monitoring of network in all aspects is fundamental service in order to identify network issues that could lead to a possible breach, like increased or unusual traffic, multiply or random attacks to a firewall etc. GDPR requires to inform data subject without undue delay and Supervisory authorities within 72-hours
Data Loss Prevention	DLP technology assists organizations to understand is processed (at rest, in motion and in use). DLP helps companies to identify and protect sensitive data using a variety of advanced data detection techniques in many forms eg: • **Discover** where data is stored across all of your cloud, mobile, network, endpoint, and storage systems • **Map data** processing to a system or person and record it. • **Identify** confidently regulated data, track its use, and location • **Monitor** how data is being used, whether your employees are on or off the network • **Protect data** from being leaked or stolen—no matter where it's stored or how it's used Also DLP integrates with encryption and Cloud Access Security Brokers technologies to protect email, removable media, individual files and data in the cloud	**Article 4(1), recitals 26 and 30 : *Definition of Personal data*** Article 24 Responsibility of the Controller 'The controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation'. Chapter 5 (Articles 44 – 50) are focused on the 'Transfers of personal data to third countries or international organizations'. This section explains the conditions of when personal data can be transferred or processed outside of the EU, including Article 46: (Transfers subject to appropriate safeguards).
Encryption	Regulatory requirements make auditable and centrally managed encryption solutions a strong requirement for many companies that need to comply with regulations such as GDPR. Endpoint Encryption combines strong full-disk and removable media encryption with an intuitive central management platform to protect sensitive data from loss or theft and help administrators prove a device was encrypted should it go missing. Endpoint Encryption can be complimented with email & files/folders encryption solutions.	Article 32: §1. a Security of processing **§3** Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
Penetration Testing	Penetration testing technics aim to expose unauthorized access to sensitive or restricted information and data within the organization's infrastructure. GDPR instructs for applications and critical infrastructure to be tested regularly for security vulnerabilities. Services such as penetration testing and regular vulnerability assessments would help meet this recommendation.	Article 32: §d Security of processing. GDPR requires a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
	With Secure WEB Gateway, companies are able to consolidate a broad feature-set that protects your enterprise from the ever-increasing sophistication and volume of threats in your web traffic. Installed between users and their interactions with the Internet, the Secure WEB Gateway inspects content to identify malicious payloads and then filter, strip, block or replace web content to mitigate risks and prevent data loss.	Article 32: Security of processing. Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. **§2** In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

Note: All the above products fall also into GDPR Article 25 : (Recital 78) ***Data protection by design and by default***

We Support Green IT