FUTUREWEI Whitepaper

Storage System Compliance & Security (GDPR)

To be removed for release

V 0.1	12/4/20	initial draft
V 1.0	2/18/21	first review

Contents

1 INTRODUCTION

1.1 COMPLIANCE & SECURITY

Compliance and security are often mentioned together, but they are not the same thing:

- Compliance is a one-size-fits-all, point-in-time snapshot that demonstrates an organization meets the minimum requirements of specific regulatory standards such as GDPR, PCI-DSS and GLBA in the finance industry, and HIPAA in healthcare.
- Security is the whole system of policies, processes and technical controls that define how an organization stores, processes, consumes and distributes data so that it is effectively and verifiably protect from cyber threats. Security is a big part of compliance.

Compliance and security are different components of a necessary and crucial system. Each relies on the other to keep data secure. When a company meets compliance frameworks with its internal security measures, the implementation of both will keep data safe and an organization's integrity and reputation intact.

1.2 OBJECTIVES

Our goal is to create requirements for storage systems that is an alliance of both security and compliance in a systematic and controlled way.
In this document, we will first analyze the key requirements of GDPR compliance (chapter 2). With these requirements, and other cyber threats analysis, we will come up with main parts of security in storage systems (chapter 3). Then we will analyze security and compliance in major storage vendors (chapter 4 & 5). Chapter 6 is focused on the trends in security. In the last chapter, we analyze the gap of current storage systems and proposes a framework for the compliance and security.

Note: although we focus on GDPR compliance in this document, the whole framework is flexible enough for all other regulations.

2 GDPR COMPLIANCE

2.1 GDPR INTRODUCTION [10]

The General Data Protection Regulation (GDPR) is European Union's law designed to protect personal data. The designers of GDPR try to promote innovation with data utilization in this data economy and at the same time protect information from being misused and lost into wrong hands. EU is actively monitoring the progress of GDPR and will take actions (such as fines) against enterprises that are not GDPR compliant. Thus, ensuring GDPR compliance is one of the most critical tasks inside a European enterprise. As many information systems are serving global customers including European customers, the influence of GDPR often goes beyond the European borders and has impact on global enterprises.

GDPR compliance poses both legal and technical challenges to an enterprise. Any information flow within an enterprise must be carefully analyzed to ensure GDPR requirements are satisfied. Storage systems, as where data are stored, are often considered to be the center components to ensure GDPR compliance. GDPR compliance is often a critical requirement raised by storage customers in Europe.

2.2 GDPR AREAS OF FOCUS

Security and compliance are always top priorities for enterprise business. Currently, the GDPR compliance by enterprise business is focused on following areas:

1. Data Subject Requests

- Provide access, rectification, erasure, and portability within one month of the request.
- Provide legal information such as controller identity and contact details, the purposes and legal basis of the processing, the categories of data, the recipients, and the expected storage period.

2. Security of Processing

- Implement security defense and restrictions to reduce data risks, including monitoring, data minimization, pseudonymization and encryption techniques.
- Risk management including 72-hour breach reporting.

3. Lawfulness

- Processing is lawful only if there is one of consent, necessity, legal obligation, protection, public interest, official authority, or legitimate interest.
- Keep data subjects informed and manage requests in a transparent, efficient, and effective manner, and consider appointing a DPO.

4. Accountability

- Ability to demonstrate compliant collection, use and retention of personal data.
- Provide data protection impact assessments, codes of conduct and certification mechanisms.

2.3 Security of Processing in GDPR

Article 32 of the GDPR requires each controller and processor to implement appropriate technical and organizational measures to ensure secure personal data processing appropriate to the risk, including inter alia as appropriate:

a) the pseudonymization and encryption of personal data.
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

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.

Article 25 of the GDPR (Data protection by design and by default) means, a company should implement appropriate technical and organizational measures and necessary safeguards from the design state and through the lifecycle.

2.4 Key Requirements for Security of Processing

After carefully analyzing *GDPR art. 32 "Security of Processing"* and related articles, we come into conclusion of some key requirements which bring more values to customers for security of processing in storage system.

2.4.1 Data Protection

Storage systems should implement various data protection techniques to protect personal data from accidental destruction, loss, alteration.

- Raid or Erasure Coding
- Snap shots
- Disaster Recovery techniques, including asynchronous/synchronous replication, 3DC etc.
- Backup/archive techniques
- Data verification techniques

2.4.2 Access Control

Storage systems should implement various access control techniques to protect personal data from unlawful destruction, loss, alteration, or access to personal data transmitted, stored, or otherwise processed

- Identify the right of access for all groups
- Create roles and access policies
- Grant data access against GDPR-risk model validation
- Monitor and identify risks and violations

2.4.3 Encryption

Encryption is not mandatory under the GDPR. But article 32 of the GDPR includes encryption as an example of an appropriate technique measure, depending on the nature and risks of your processing activities.

- Manage encryption policies for data subjects
- Provide at-rest and in-transit encryption solutions for data subjects
- Encryption solutions should meet current and future standards, such as FIPS 140-2
- Manage keys for data subject requests, including access, update and delete (crypto erasure)
- Provide key managers for secure key create, rekey and removal

2.4.4 Crypto Erasure

- Need to destroy personal data by delete encryption keys
- Need to destroy all historic backups
- Need to destroy events related to the data asset
- Must destroy the data without undue delay (30 days)

2.4.5 Pseudonymization - masking

Pseudonymization is not mandatory under the GDPR. But article 32 of the GDPR includes pseudonymization as an example of an appropriate technique measure, depending on the nature and risks of your processing activities. Both encryption and masking are pseudonymization techniques.

- Provide tokenization of personal information elements (identifiers) to keys (pseudonyms) that cannot be externally identified
- Information is stored in a manner linked to pseudonym rather than identifiers.
- Provide reverse tokenization when end user requests information
- In case of removal, remove the identifier to destroy the linkage between the pseudonyms and identifiers.

2.4.6 Risk Management

- Data security impact assessment
- Define policy rules and groups that help monitor, audit, record, and provide alerts on any unauthorized activities related to personal data by privileged and unprivileged users and applications
- Use the rules for audit trails for DSRs

2.4.7 Monitoring

- Monitor accesses with predefined rules

2.4.8 Incident Report

- Report data breach within 72 hours
- Report data rectification or erasure or restriction of processing if required by data subject
- Report who accessed personal data, when it was accessed, where they access from, how it was accessed if required b data subject
- Report unlawful accesses to the controller or processor

- Save all events in persistent media

2.4.9 Data Minimization

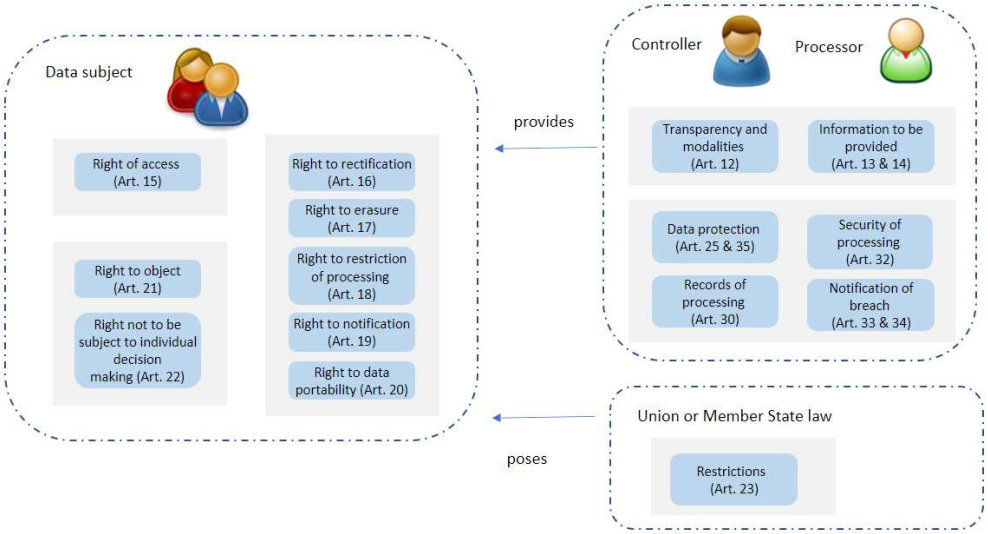
- Only retain personal data that is necessary for the purpose
- Remove personal data that should not be held or further used after the purpose of data collection is fulfilled
- Remove personal data when the agreed period is passed
- Remove personal data in limited time (30 days)

2.5 Data Subject Request

Certain privacy laws and regulations provide a right for certain individuals (known as 'data subjects' under the GDPR or 'consumers' under the CCPA) to be able to receive or request action be taken with respect to certain personal data.

The data subject request (DSR) is one of the most challenging components of GDPR. It provides individuals in the EEA (European Economic Area) the right to request what personal data has been collected, how that data is being used and to have that data exported, restricted, changed, and erased.

- Access (i.e., the right to know what personal data a controller or processor has about the individual),
- Rectification (i.e., the right to update incorrect personal data),
- Erasure (i.e., the right to be forgotten),
- Restriction of processing
- Informed for personal data rectification or erasure or restriction of processing
- Portability (i.e., the right to export personal data in a machine-readable format)
- Objection (i.e., the right to object processing of personal data including profiling)



2.6 KEY REQUIREMENTS FOR DSR

After carefully analyzing the GDPR articles, we come into conclusion of some key requirements which bring more values to customers for DSR feature in storage system.

2.6.1 Metadata Indexing

- File level metadata includes file name, size, location, owner, dates, extension, ACLs and more
- Metadata should be light-weighted
- Metadata should leverage metadata report and analysis
- Metadata should be persisted for retrieval

2.6.2 Access and Update

- A user can access the personal data on a controller or processor
- A user can update the personal data when the data is incorrect
- Access control policies should be applied
- Access/Update should finish in a timely manner
- Access/update should be recorded and monitored and audited
- Provide alert on unauthorized users or applications

2.6.3 Delete

- Maintain policies to remove raw data on timelines (within 30 days)
- Remove revision history along with data asset
- Remove events related to the data asset
- Remove the identifiers to destroy the linkage between the pseudonyms and the identifiers
- Support crypto erasure when the personal data is encrypted.

2.6.4 Query

- Search keywords and filters based on subject tags and other asset properties
- Search revision history based on subject tags
- Search events based on subject tags or catalog
- Preview capabilities to ensure that you are selecting the correct data asset
- Reviews about assets created by collaborators within the catalog

2.6.5 Consent Management

- Record/Update a specific purpose for personal data
- Support restriction of processing from data subject
- Support object processing of personal data
- Support not to be subject to individual decision-making including profiling
- Support policies for personal data with limited time
- Support actions for personal data when purpose or time limit expires

2.6.6 Retention

- Support policies for personal data with certain purpose
- Support policies for personal data with limited time
- Support actions for personal data when purpose or time limit expires

2.6.7 Audit History

- Log details about every change made to personal data
- Provide a full history for compliance, audit, and reproduction

2.6.8 Incident Report

- Report data breach within 72 hours
- Report data rectification or erasure or restriction of processing if required by data subject
- Report who accessed personal data, when it was accessed, where they access from, how it was accessed if required b data subject
- Report unlawful accesses to the controller or processor
- Save all events in persistent media

2.6.9 Data Portability

- Allow user to move, copy or transfer personal data from one environment to another, without affecting its usability
- Provide safe and reasonable fast ways for personal data transfer
- Restrict data transfer out of EU

2.7 Key Requirements for Lawfulness

Art. 5 – 11 of the GDPR require processing of personal data to be lawfully, fairly and in a transparent manner. Processing is lawful only if there is one of consent, necessity, legal obligation, protection, public interest, official authority, or legitimate interest.

- One such lawful basis the data subjects' consent. Consent management (sector 2.6.5) should be implemented with transparency.
- Other lawful bases, including legal obligation and legitimate interest, do not require data subjects' consent. In these cases, data classification or data mapping techniques can be used for a full understanding of the underlying data.
- Appoint a DPO (Data Protection Officer).

2.8 Key Requirements for Accountability

Art. 5 of the GDPR says the organization should be able to demonstrate compliance with "accountability". The requirements for accountability include:

- Data protection/security impact assessment (Art.35)
- Maintain a record of processing activities (Art. 30).
- Provide code of conduct (Art. 40), procedures and policies (Art. 72), certification mechanisms (Art. 42 & 43).

3 SECURITY OF STORAGE SYSTEMS

Security is an important part of regulatory compliance. Article 25 of the GDPR (Data protection by design and by default) means, a company should implement appropriate technical and organizational measures and necessary safeguards from the design state and through the lifecycle. In this chapter, we try to design secure storage systems with compliance.

3.1 ROOT OF TRUST [3]

3.1.1 Overview

Modern computing systems consists of hardware, firmware, and software components at multiple layers of abstraction. A vulnerability in any of the components could compromise the trustworthiness of the security of the system. Strong security assurance is possible by grounding security mechanisms in roots of trust (RoT). Roots of trust are highly reliable hardware, firmware and software components that perform critical security functions. Roots of trust provide a firm foundation from which to build security and trust.

Many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. The Trusted Platform Module (TPM), for example, could be the ultimate hardware system where the core root of trust in the system must reside.

Root of Trust starts a chain of trust operations, such as

- Public key infrastructures (PKIs) to generate and protect root and certificate authority keys.
- Code signing to ensure software remains secure, unaltered, and authentic.
- Creating digital certificate for authenticating proprietary electronic devices.
- Network deployment.

3.1.2 Requirements

The following requirements apply to every RoT including an initial or an enhanced RoT:

- **Computing Engine, Code, and Data:** A Root of Trust shall consist of a computing engine and executable code (providing the root of trust security function(s)), co-located on the same platform. A Root of Trust may require data and/or key(s); if so, the data and/or key(s) shall be co-located on the same platform as the computing engine and executable code.
- **Security Services:** A Root of Trust shall provide one or more security services.
- **Certification:** The Vendor/Manufacturer shall design a Root of Trust for a certification process for a platform or for a device.
- **Unique Identifiable Ownership:** A Root of Trust SHALL have a single identifiable owning entity.
- **Mutability:** Code and/or data of a Root of Trust SHALL be immutable, or its mutability SHALL be controlled only by the unique identifiable owner.

- **Ownership Transfer:** If a Root of Trust implements an ownership transfer mechanism designed by the initial owner/provider of the RoT, then the current owner of the Root of Trust SHALL provide a mechanism to authorize the transfer of ownership to the new owner.
- **One RoT per Platform:** A Platform SHALL contain one and only one Root of Trust.
- **Temporal:** The Root of Trust SHALL include the code which executes first upon the initialization of the computing engine during cold boot in that platform.
- **Manufacturer Identity:** A Root of Trust SHALL have an identifiable manufacturer.

For a Non-Bootstrapped Root of Trust:

- **Provenance:** The platform manufacturer SHALL create and provision the Root of Trust during the manufacturing process.

For a Bootstrapped Root of Trust:

- **Provenance:** The platform manufacturer SHALL create and provision the Initial Root of Trust Component during the manufacturing process.
- **Temporal:** The Initial Root of Trust Component SHALL include the code which executes first upon the initialization of the computing engine during cold boot in that platform.
- **Verification:** A parent Root of Trust Component (i.e. either an Initial RoT Component or another eRoTc) SHALL verify the integrity of the code and data of an Extended Root of Trust Component before the first execution of the eRoTc.
- **Location:** The iRoTc and all the eRoTc(s) that compose a Bootstrap Root of Trust SHALL be located on the same platform.

3.1.3 RoT Security Services

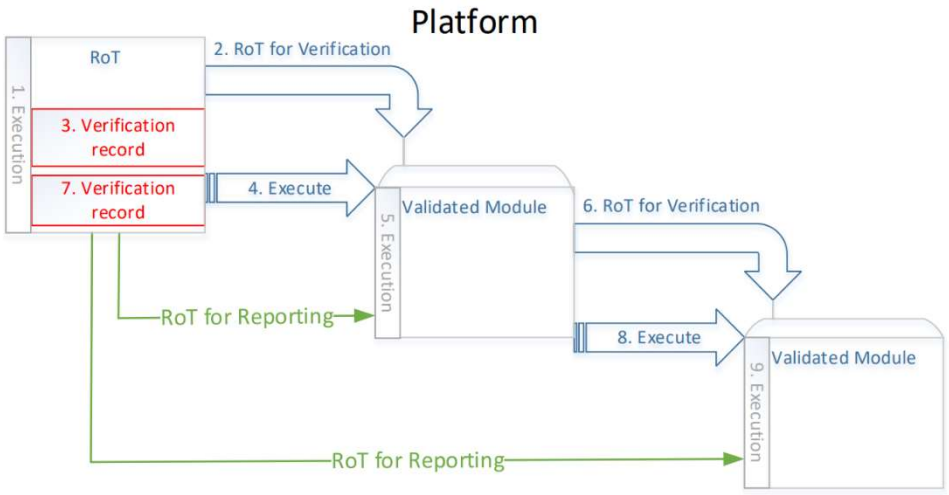
A Root of Trust may contain any combination of following security services:

- **Authentication**: The Root of Trust for Authentication maintains one or more shielded locations for the purpose of securely storing and preserving the integrity of at least one credential. It also includes an interface to maintain authorized access to and use of the contents of the shielded locations as well as protecting it from unauthorized use and disclosure.
- **Confidentiality**: The Root of Trust for Confidentiality maintains shielded locations for the purpose of storing sensitive data, such as secret keys and passwords.
- **Identification**: The Root of Trust for Identification maintains a shielded location for storing a secret value, such as a symmetric key or an asymmetric private key, for the purpose of establishing the identity of the Root of Trust.
- **Integrity**: The Root of Trust for Integrity maintains shielded locations for the purpose of storing and protecting the integrity of non-secret critical security parameters and platform characteristics. Critical security parameters include, but are not limited to, authorization values, public keys, and public key certificates.

- **Measurement**: The Root of Trust for Measurement provides the ability to reliably create platform characteristics. The Root of Trust for Measurement may calculate the cryptographic hashes of code and data.
- **Authorization**: The Root of Trust for Authorization provides reliable capabilities to assess authorization tokens and determine whether they satisfy policies for access control.
- **Reporting**: The Root of Trust for Reporting reliably reports platform characteristics.
- **Update**: The Root of Trust for Update verifies the integrity and authenticity of signed updates, and upon successful verification, authorizes the initiation of the update process.
- **Verification:** The Root of Trust for Verification verifies the integrity and authenticity of signed objects.

3.2 Chain of Trust [3]

A Chain of Trust extends a service from a RoT or module to other modules. A good example is a Chain of Trust for Verification, in which the RoT contains a verification service, and uses that service to verify a module that contains a verification service like the verification service in the parent. A Chain of Trust shall always start in a RoT. Like Roots of Trust, Chains of Trust shall contain at least one security service.



A storage system shall provide security services for compliance, such as GDPR and other regulations. The services could be provided by the root of trust, or other security modules that are chains of trust.

3.3 Threat Intelligence Storage Systems

Threat intelligence is the information a vendor uses to understand the threats that have, will or are currently targeting the platform. The vendor should analyze the information and prepare, prevent, and identify cyber threats that may take advantage of valuable resources.

In this sector, we discuss different categories of the security services that storage systems should provide with threat intelligence. The security provided by storage systems fulfills the requirement by *GDPR Art. 25 "Data protection by design and by default*".

3.3.1 Cyber Threats

Cyber threats are malicious acts that seek to damage data, steal data, or disrupt digital life in general.

Traditional threats include threats from external networks and from internal networks. Security threats from external networks include:

- Traditional network IP attacks
- Operating system and software vulnerabilities
- Viruses, Trojans, and worms
- Structured Query Language (SQL) injection attacks
- Phishing attacks
- Zero-day attacks

Security threats from internal networks include:

- Fast-changing attacks, compromising intranet security
- Untimely patch upgrade and antivirus database update, leaving worms to spread through vulnerabilities
- Unauthorized Internet access, causing frequent leakage of internal confidential information
- Random connections of portable computers, compromising network border security
- Abuse of software and hardware, imperiling asset security
- Network applications are not monitored, causing low working efficiency.
- Loose management of peripherals, causing data leakage and virus spread
- Security management regulations cannot be put into practice due to the lack of technical basis.

Storage security should be safeguarded by technical measures. Data integrity, confidentiality, and availability must be monitored to prevent unauthorized access to storage resources and data.

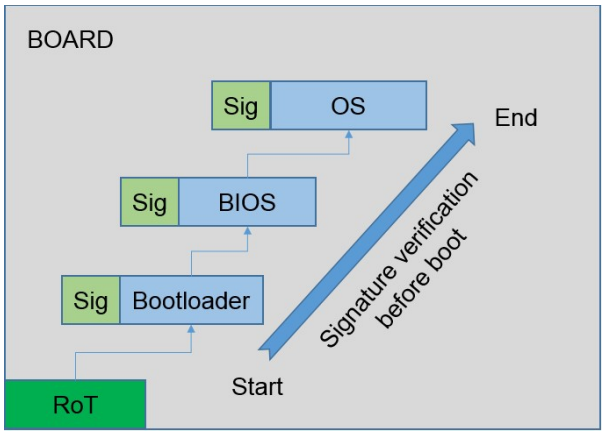
Storage products face the following security threats:

- Data leakage
- Data damage
- Temporary or permanent loss of accessibility and availability
- Law and regulation incompliance

3.3.2 System Security

Secure boot

The root of trust should be integrated into hardware and firmware to prevent software and physical attacks. Software integrity is ensured by a chain of trust for verification.



Software Package Integrity Protection
The software package should use digital signatures for installation or upgrade. The upgrade module of the storage system should verify the digital signatures and perform installation or upgrade.

Security Patches
Regular installation of security patches can eliminate system vulnerabilities and prevent virus, worms, and hackers from attacking systems.

3.3.3 Network Security

Physical and logical Isolation
Host I/O channels, disk I/O channels, GE switching channels should be redundant to protect three function planes: service plane, control plane and management plane. Each plane should complete fault diagnosis, rectification, and isolation independently without affecting other planes.
Storage systems may support multi-tenants feature. Each tenant should be logically isolated from other tenants.

Remote System Management
Secure transmission protocols (SSH, SFTP, HTTPS, SNMP, etc.) should be used for remote system management.

Remote Data transmission
If the data is transmitted across untrusted networks (replication, etc.), IPsec should be used to ensure data transmission security

3.3.4 Service Security

Role-based Access Control
Users can access their storage based on the default roles of system administrators, and/or user-defined roles.

User Security Policies

Users can configure login and account audit policies, such as session timeout duration, password lock, lock mode, login security info, user-defined info, etc.

Password Security
Password policies should be configured to prevent brute force password cracking. Password should be encrypted for storage and transfer, and password change is authenticated.

Authentication and Authorization
Local users' SSH login and web login should be authenticated with password, public key authentication or certificate authentication.
System administrator domain authentication should support AD and LDAP.

3.3.5 Data Security

Data Protection Technologies
Most storage vendors implemented various data protection techniques for high availability, and to protect personal data from accidental destruction, loss, alteration.

- Raid or Erasure Coding
- Snap shots
- Disaster Recovery techniques, including asynchronous/synchronous replication, 3DC etc.
- Backup/archive techniques
- Data verification techniques

Data-in-transit
Data in transit, also referred to as data in motion and data in flight, is defined into two categories:

- Information that flows over public or untrusted network.
- Information that flows in the confines of a private network such as a corporate or enterprise LAN.

Encryption protocols (IPsec, SMB3 encryption, etc.) are used to prevent the network attack.

Data-at-rest
Data at rest encryption is designed to prevent the attacker from accessing the unencrypted data by ensuring the data is encrypted when on disk. It may also be required by an organization's need for data governance and compliance effort. Regulations such as HIPAA, PCI and FedRAMP, layout specific safeguards regarding data protection and encryption requirements. Data at rest encryption is a mandatory measure for compliance with some of the regulations. Storage systems need to support different levels of encryption: disk level (SED), volume level, file/directory level, etc.

Tokenization is another approach to protecting data at rest that replaces sensitive data with non-sensitive substitutes, referred to as tokens, which have no extrinsic meaning or value. Tokens require significantly less computational resources.

Data-in-use
Data in use refers to active data which is stored in a non-persistent digital state typically in computer memory, CPU caches or registers. Data in use may contain sensitive data including certificates, encryption keys or personally identifiable information.

Full memory encryption is commonly used to protect Data in use.
Enclaves enable an "enclave" to be secured with encryption in RAM so that data is encrypted in RAM but available inside CPU and CPU cache. Intel has introduced the concept of "enclave" as part of the SGX (software guard extensions).
Cryptographic protocols, including secure multi-party computation and homomorphic encryption, allows for private computation of data on untrusted systems.

For the time being, data in use technologies are not widely used in storage systems. But it is of increasing interest to businesses, government agencies and other institutions.

Key Management System (KMS)
A KMS is used to deal with the generation, exchange, storage, use, crypto-shredding, and replacement of keys. It includes cryptographic protocol design, key servers, user procedure and other relevant protocols.

KMIP is an extensible key management protocol that has been developed to manage and exchange keys and related information.

Public-key infrastructure (PKI) is a type of KMS that uses hierarchical digital certificate to provide authenticate and public keys to provide encryption. PKI are used in the form of SSL and TLS.

Crypto-Shredding
Crypto shredding, or secure erasure, is the practice of deleting encrypted data by deleting or overwriting the encryption key. Crypto shredding has a benefit of being a quick and effective way to remove encrypted data. Legal obligation from rules (the right to be forgotten in GDPR) is a good motive to use crypto shredding for compliance.

3.3.6 Risk Management
Risk management in security is the process of identifying, assessing, and controlling security risks to a storage system.
Risk Assessment
A Data Protection Impact Assessment (DPIA) is required under the GDPR at the time you begin a new project that is likely to involve other people's personal information.

Monitoring
A storage system should monitor data and file activity to create audit trails of personal data access with detailed reporting, to deliver compliance evidence to internal and external administrators.

Audit Management

Audit management organizes information and simplify process for conducting internal auditing.

Logging
Operation logs record all operations performed on the management plane, including event time, user ID, port, network address, event type, event results, etc.
Users should be able to configure policies for creation, deletion, and dump mechanisms.
Logs can be queried with various mechanisms.

Incident Management
A storage system should assess data breaches or other abnormalities, along with predefined sets of policy rules, and provide alerts on any unauthorized activities by privileged and unprivileged users and applications. These same rules are also used to create audit trails.

3.3.7 Miscellaneous

Antivirus / Antimalware
Storage vendors are well positioned to provide those integrated anti-virus solutions, to make sure that viruses are not resident on the storage systems. NAS vendors may use 3rd party software designed to scan storage system itself during end user access (user access triggered) or based on manually scheduled policies from a central antivirus can server. See our anti-virus white paper for more information.

Intrusion Detection
Intrusion detection is a software application that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It also scans a network or system for harmful activity or policy breaching.
Intrusion detection system (IDS) can be classified as network intrusion systems (NIDS) and host-based intrusion detection systems (HIDS). It can also be classified by detection approach: signature-based detection (recognizing bad patterns) and anomaly-based detection (detecting deviations from a model of good traffic, which often relies on machine learning).
Some storage vendors, including Huawei, already provide intrusion detection systems.

4 SECURITY OF PROCESSING IN ENTERPRISE STORAGE

In this chapter, security of processing features from various storage companies are elaborated.

4.1 COMPARISON CHART

Many storage vendors have designed secure storage systems with common features such as access control and encryption. They also claim to have basic compliance with GDPR regulations. But many regulations are newer than the system architecture, and understanding these regulatory requirements are difficult. The companies might oversee some of the regulations, laws, and other risks. Each company needs to carefully analyze the requirements to implement secure storage systems.

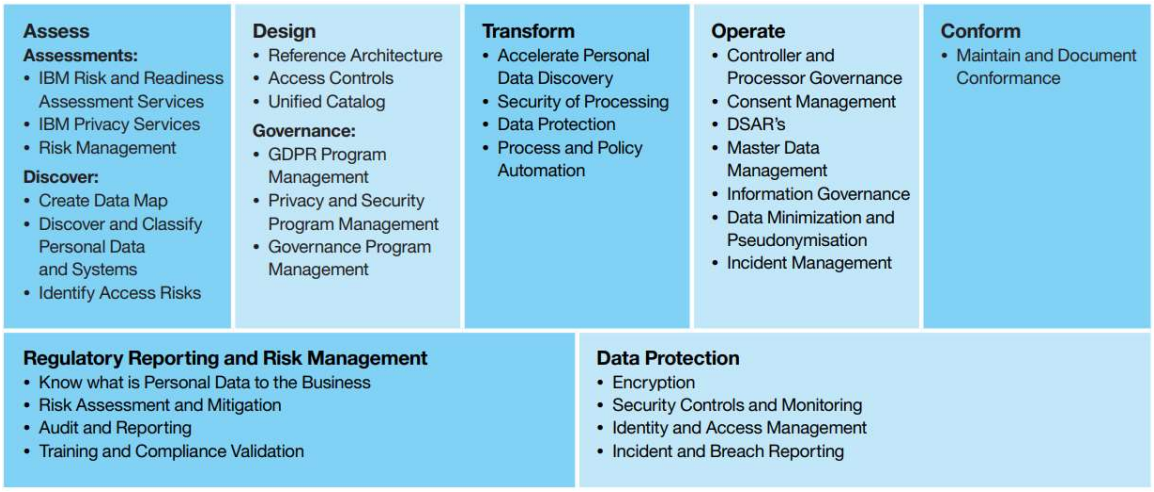
To compare different vendors on the market, we compiled a table to show the differences among them.

	Access Control	**Encryption**	**Crypto Erasure**	**Risk Mgmt**	**Data Minimization**	**Masking**
Vendor E	Yes	Limited, SED based	Yes	Limited	Limited	No
Vendor N	Yes	Yes, disk level or volume level	Yes	Limited	Limited	No
Vendor P		Limited, SED based	Limited, SED based	Limited	Limited	No
Vendor I	Yes	file and database encryption, tokenization, application encryption, rekey	Yes	Yes	Yes	Yes
Vendor H	Yes	Limited, SED based	Limited, SED based	Limited	Limited	No

4.2 IBM® SOLUTION [6]

4.2.1 Overview

IBM® has created a GDPR Framework that highlights five phases to help achieve readiness, as shown in Figure 2: Assess, Design, Transform, Operate and Conform. The goal of the framework is to translate GDPR obligations into actions and outcomes that help clients effectively manage both security and privacy, to help reduce risk and avoid incidents.

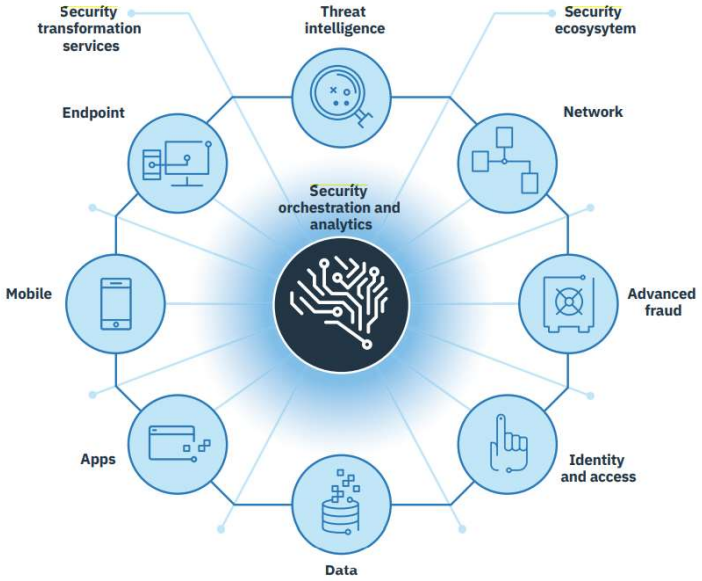


The IBM® solution provides a "Security Immune System" that forms a foundation for identifying, correlating, and mitigating threats across the various security domains using deep analytics, cognitive computing, and orchestration. This security immune system is focused on three things: prevention, detection, and response.

IBM® solutions provide data encryption for GDPR readiness. Included are file and database encryption, tokenization, and application encryption, plus the ability to encrypt and re-key data without taking applications offline.

Using a variety of different masking techniques, IBM® can help protect data such as telephone numbers, national identification numbers, email addresses or names in test systems without losing the underlying contextual meaning.

A GDPR Accelerator is available that includes a GDPR Data Security Impact Assessment, along with predefined sets of policy rules and groups that help monitor, audit, record, and provide alerts on any unauthorized activities related to personal data by privileged and unprivileged users and applications. These same rules are also used to create audit trails for DSARs, such as requests for personal data access, rectification, erasure, or transfer.



4.2.2 Capability

Access Control: ongoing security is enabled through granting data access against a GDPR risk model validation. Monitoring and enforcement occur through managing the data access lifecycle, and continuously certifying access to identify related risks and violations.

Encryption: include file and database encryption, tokenization, and application encryption, plus the ability to encrypt and re-key data without taking applications offline.

Masking: Masking can be performed across cloud and on-premises workloads, with predefined data privacy classifications and rules designed to speed time to implementation and simplify your reporting needs. This capability can also potentially reduce the consent duties and obligations.

Incident Management: IBM® provides tools and services to help you automate, collaborate, and deploy proactive incident readiness, management, and reporting capabilities to meet GDPR obligations. Augmenting an incident response platform and incident response services are capabilities for all elements of a breach investigation, including reporting to the relevant supervisory authority.

4.3 DELL EMC® SOLUTION [7][8]

4.3.1 Overview

EMC® GDPR solution includes breach response, data governance, risk assessment and compliance management.

[i]

4.3.2 Capability

EMC® has many products and solutions that include powerful search capabilities across specific data sets, and can also export or delete data to help customers meet their GDPR requirements:

- DP Search for Networker and Avamar backups.
- SourceOne for email, file, and SharePoint content.
- Mozy for endpoint backups.
- Isilon Search for content on Isilon Storage.

Solutions about international personal data transfer (select where data can be stored):

- Virtustream, Mozy and Spanning include choices for the geographical locations of the data storage.
- ECS solution for data moving out of public clouds to private clouds.

Data minimization and retention.

- Data domain solution will tier data for longer retention periods to private or public cloud.
- SourceOne archive platform can archive data for longer term.

Accountability:

- RSA Archer can document and evaluate GDPR-related infrastructure, policies and procedures, risks, controls, third parties, outstanding issues, and plans.

Security techniques:

- Dell Encryption Enterprise delivers a layered multi-key approach for encryption.
- Dell Data Guardian can protect data, control data access and gain visibility into data usage.
- Dell Endpoint Security Suite Enterprise and Dell threat defense are advanced threat preventions solutions using AI and ML that prevents malware from execution.
- RSA NetWitness Endpoint is an endpoint detection and response tool that monitors endpoints and provides analysis of all behavior and processes.

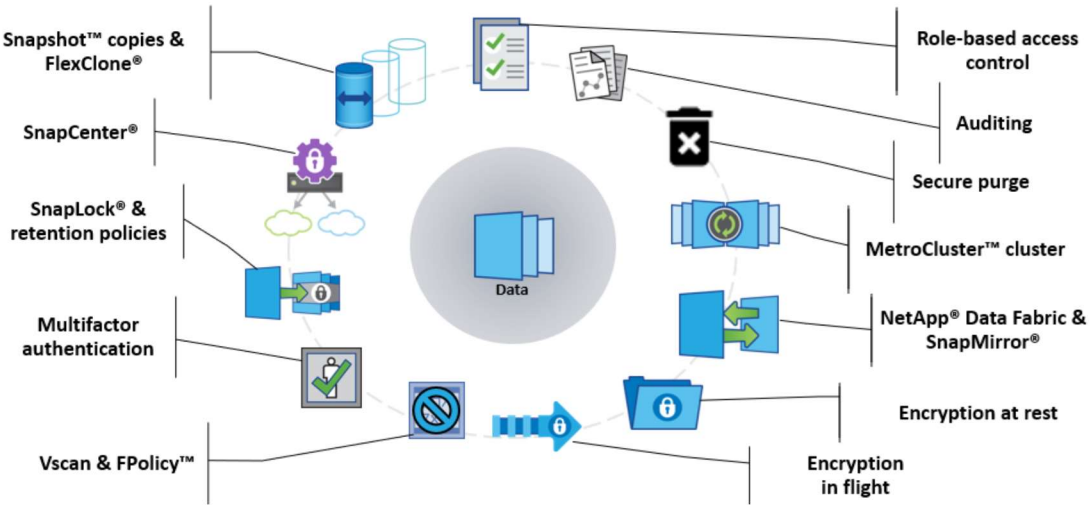
4.4 NETAPP® SOLUTION [9]

4.4.1 Overview

Netapp® defines data privacy framework as:

- **Govern.** Defines the policies and procedures of how data is to be used, controlled, and retained.
- **Identify and validate.** The process of finding the organization's data and validating that the type of data being captured is correct for the organization.
- **Deploy and manage.** Determines the organization's strategy and policies for how data is deployed and managed, including breach detection.
- **Secure and protect.** Determines the organization's methodology for making data secure, available, and protected.
- **Respond.** Defines the process of how the organization responds to a data breach, audit, or user request for data.

The following picture shows some of the Netapp® solutions that assist in developing the three areas of the data privacy framework (identify and validate, deploy, and manage, secure, and protect). These are the key Netapp® technical solutions that assist with GDPR.



4.4.2 Capability

Netapp® provides following capabilities for *security* of processing:
Encryption at Rest: ONTAP® can prevent data theft or loss by using encryption at rest, which encrypts data while it's resting by using hardware such as Netapp® Storage Encryption (NSE), which encrypts the disk drives, or by using software such as Netapp® Volume Encryption (NVE) to specify which volumes to encrypt. Netapp® E-Series systems also provide a hardware disk encryption solution called full-disk encryption (FDE).

Encryption in Flight: ONTAP® provides file-level protocol encryption for both NFS (through KRB5P) and SMB (SMB3 encryption) while the data is transmitted across the network. It supports AES-256 encryption level and ensures that the data reaches the destination without being compromised during transit.
RBAC: Role-based access control (RBAC) allows administrative accounts to be restricted and/or limited in what actions they can take on the system. Both ONTAP® and E-Series systems support this capability, which prevents a single account from being allowed to perform all potential actions available on the system.
Multifactor Authentication: Multifactor authentication (MFA) can be configured to mandate authentication of system administration accounts through a verified third-party identity provider. This process helps to verify that an actual administrator is the one using the admin account.
Vscan and FPolicy: Netapp®'s malware prevention techniques. Vscan provides a way for Netapp® antivirus scanner partners to verify that files are virus free. FPolicy integrates with Netapp® partners to monitor file access behaviors and to prevent unwanted access or change to files based on policy settings. This helps prevent ransomware from getting a foothold in the first place.
Secure Purge: In ONTAP® 9.4 and later, secure purge provides the capability to cryptographically shred individual files from solid-state drives (SSDs) with no down time.
SnapLock and Retention Policies: ONTAP® SnapLock compliance software uses a data retention policy to prevent any change to the data after the first write for a predetermined period. Once the data is written, no one can change or modify it until the SnapLock retention period has expired.

5 DSR IN ENTERPRISE STORAGE

In this chapter, DSR features from various storage companies are elaborated.

5.1 COMPARISON CHART

Many storage vendors use storage system level metadata for basic DSR services such as search, access, rectification and delete. But these solutions cannot satisfy the advanced requirements for data governance and DSR performance.

To compare different vendors on the market, we compiled a table to show the differences among them.

	Search	**Access/ Update/ Delete**	**Secure Erasure**	**Consent Mgmt**	**Retention**	**Report**	**Pseudo-nymization**
Vendor E	Yes	Yes	Yes	Yes	Yes	Yes	No
Vendor N	Limited search (file name)	Yes	Yes, file encryption based	No	No	Yes	No
Vendor P	Limited search (file name)	Yes	Limited, SED based	No	No	Yes	No
Vendor I	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Vendor DB	Yes	Yes	No	Yes	Yes	Yes	Yes
Vendor H	Limited search (file name)	Yes	Limited, SED based	No	No	Yes	No

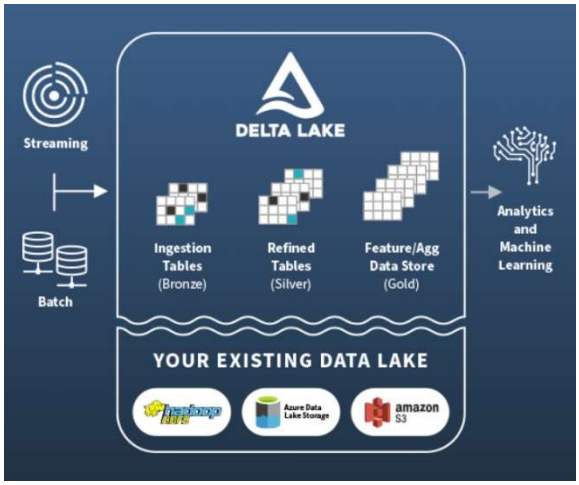
5.2 DATABRICKS® SOLUTION [4][5]

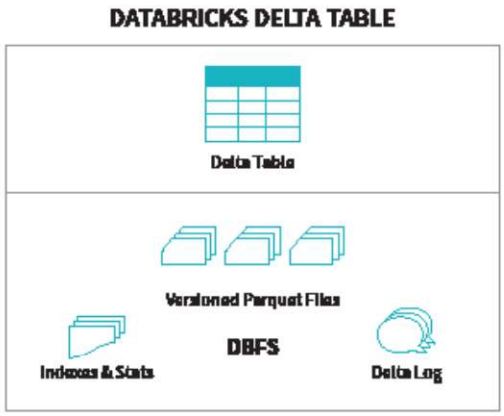
5.2.1 Overview

Databricks® provide following features for GDPR compliance:

- Delete: offers functionality to be able to permanently delete notebooks and cells, along with the corresponding revision history, that may contain personal data, and making sure that, once marked for deletion, those contents are permanently purged within 30 days after being marked for deletion;
- Pseudonymization: implemented pseudonymization techniques and redaction techniques to add an additional layer of protection on personal data (like a user email address) that might be recorded in Databricks®' usage logs.
- Databricks® Delta Lake: a unified data management system built into the Databricks® platform, that dramatically simplifies the task of being able to perform data subject requests against data stored in data lakes.
- DSR: has put in place systems to be able to process data subject requests in a timely manner; and
- self-certified to Privacy Shield, certified to ISO27001, and attested to ISO27018, the internationally recognized industry standard approach for protecting personal data in the cloud. Additionally, on an annual basis, Databricks® obtains an independently audited SOC 2 Type II report, which can be made available to you under NDA.

Delta Lake is an open-source storage layer that brings reliability to data lakes and help to process DSRs in a data lake scenario. Delta Lake runs on top of your existing data lake and is fully compatible with Apache Spark APIs.





Delta lake is based on the notion of Databricks® Delta tables built atop the Databricks® File System (DBFS) which manifests:

- Versioned Parquet files (based on Apache Parquet1)
- Indexes and stats
- The Delta log (ACID transactions)

5.2.2 Capability

Delta lake has the following features for GDPR compliance:

ACID Transactions: Multiple data pipelines can read and write data concurrently to a data lake. ACID Transactions ensure data integrity with serializability, the strongest level of isolation.

Updates and Deletes: Delta Lake provides DML APIs to merge, update and delete datasets. This allows you to easily comply with GDPR/CCPA and simplify change data capture.

Schema Enforcement: Specify your data lake schema and enforce it, ensuring that the data types are correct and required columns are present, and preventing bad data from causing data corruption.

Time Travel (Data Versioning): Data snapshots enable developers to access and revert to earlier versions of data to audit data changes, rollback bad updates or reproduce experiments.

Audit History: The Delta Lake transaction log records details about every change made to data, providing a full history of changes, for compliance, audit, and reproduction.

Pseudonymization: or reversible tokenization of personal information elements (identifiers) to keys (pseudonyms) that cannot be externally identified. Information is stored in a manner linked to pseudonym rather than identifiers. Structured pipelines help

to locate and remove the identifier to destroy the linkage between the pseudonyms and identifiers.

Access Control: Maintenance of strict access and use policies on the combination of the identifiers and pseudonyms

5.3 IBM® SOLUTION [6]

5.3.1 Overview

IBM® uses a unified governance catalogue to create the foundation for a unified information governance strategy for the GDPR. It helps answer questions about where personal data is located, why it is being collected and stored, and who has access. As such, its benefits are not limited to GDPR readiness: it can help you comply with other rules and regulations that might affect you, now or in the future. It is also the first step toward driving more informed business outcomes by making valuable data available to business users throughout the organization.

IBM® combines a bottom-up approach (using data inventory tools) with a top-down mapping approach (conducting interviews with business and technical users to get a first-hand look at what data resides where, and what business value users draw from that data).

IBM® personal data discovery accelerator tools can help you accelerate and enhance the data mapping process for both structured and unstructured data, across on-premises and cloud environments. By quickly analyzing and classifying the contents of your data stores, these tools can help you create a detailed catalogue of personal data stores, locations, purposes, owners, data subject types and more.

5.3.2 Capability

Incident Management: The 72-hour breach reporting window is a short one that could greatly benefit from automation. IBM® provides tools and services to help you automate,

collaborate, and deploy proactive incident readiness, management, and reporting capabilities to meet GDPR obligations. Augmenting an incident response platform and incident response services are capabilities for all elements of a breach investigation, including reporting to the relevant supervisory authority.

Consent Management: Validating that personal data is used appropriately and the processing has a legal basis, such as consent for the specific purpose, is a key GDPR obligation. Data Subject Consent Management is a capability that lets the business inform the end user what data is needed for which purposes. The consent choices made by the end user for each purpose are stored in a central repository for use by all channels and all applications in the organization.

DSAR (Data Subject Access Requests**):** Organizations are required to provide this information without undue delay, and within one month at the latest. This pattern includes case management to track requests, a request portal, identity validation including multifactor authentication, and audit trails to track access and create audit reports. The IBM® solution provides frameworks for case management and workflows to expedite DSARs.

Data Disposal: Removing data that no longer serves a purpose for the business can help maintain data quality and comply with the GDPR principle of storage limitation.

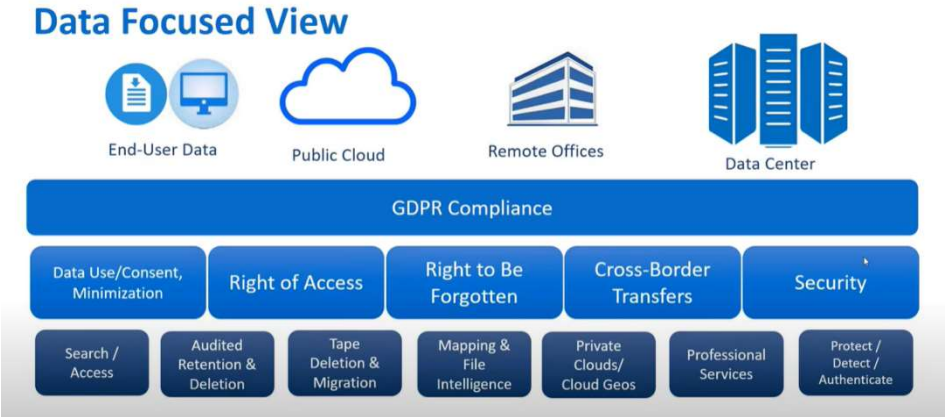
Master Data Management provides a normalized view of where different sources have pieces of the subjects' personal data, what data you hold for them and precisely where that data is located. This is a critical service capability to support DSAR requests and breach notifications.

5.4 DELL EMC® SOLUTION [7][8]

5.4.1 Overview

EMC® partners with Index Engines® for better data governance. Index Engines® offers:

- Classification, search, and management of personal data.
- Architected petabytes class data environments.
- Management of both primary and secondary data sources.



5.4.2 Capability

EMC® & Index Engines® provide following capabilities for DSR:
Search/Access: locate the data with name, id, etc., and give back the data with understandable format.
Audited Retention & Deletion: GDPR limits the data to be retained for a certain purpose and in a certain period. Beyond that the data need to be deleted.
Mapping/File Intelligence: map where the data is, decide whether it is a cross-border transfer, get some details about contention to make decision about the actions.

5.5 OTHER VENDORS

Many storage vendors claimed GDPR compliance without add-on data cataloging tools. They use their own metadata service for basic DSR services such as search, access, rectification and delete. But these solutions cannot satisfy the advanced requirements for GDPR DSR.

6 TRENDS

Every year, new directives and regulations are adding complexity to compliance operations across all industries. Some of the most pressing issues are inability to keep pace with regulatory changes, lack of valuable security insights, and siloed approaches to governance and risk management. Leveraging new technologies into compliance and security can help organizations manage and comply with continually shifting regulations proactively. Let's review some of the most important technologies for compliance & security, especially in storage industry.

6.1 AI IN SECURITY

6.1.1 Introduction

Cyber-attacks are increasing in frequency, sophistication, and effectiveness. The ongoing trend of successful attacks demonstrates that legacy security systems are not keep pace with modern threats. This is because the traditional approach only detects well-defined threats. Under this new paradigm, AI technology is used to identify unseen cyber-threats at scale, in a variety of dynamic environments, in real time, without human intervention. The AI in cyber security market is projected to generate a revenue of $101.8 billion in 2030, increasing from $8.6 billion in 2019, progressing at a 25.7 CAGR during the forecast period (2020 – 2030).
The market is categorized into threat intelligence, fraud detection/anti-fraud, security & vulnerability management, data loss prevention, identity & access management, intrusion detection/prevention system, antivirus/antimalware, unified threat management, and risk & compliance management, based on applications.

6.1.2 AI applications

- AI Incident Prevention & Threat Detection
  Supervised Machine Learning: Combining machine learning and old technologies (static and custom rules), software can identify and block advanced threats. Unlike rule-based model, an ML trained model is aimed at rendering an entire class of attacks useless, essentially eliminating the need for hundreds or thousands of rules a security analyst would have to create and maintain to deliver comparable protection. It continuously hunts for threats without human intervention.
  Unsupervised Machine Learning: It can identify key patterns and trends in the data, without labeled-data training. Unsupervised machine learning is used to analyze network data at scale and make billions of calculations based the current evidence instead of knowledge of past threats. It classifies data and detects compelling patterns. Based on this, it detects deviations from "normal" behaviors.
- Automated Response
  When a potential thread is identified, the software should take decisive actions in real time to stop the attach and avoid the risk. AI and ML enable companies to reduce incident response time and comply with security best practices.
- AI Analysis

AI Analysis can be used to triage incident reports from many customers. The supervised machine learning deploys experts' knowledge on how analysts triage threatening and suspicious activities. It adapts to new and unique situations. AI analysis saves critical time and boost productivity by allowing human experts focus on strategic decision-making.

6.2 Data Classification and Protection

Different data has different requirement for security. A one-size-fits-all security approach will create areas of too much security and others of too little, increasing the risk for the organization.

6.3 Risk & Compliance Management

We should use threat intelligence, attacker activity and internal asset criticality to provide a better view for risk management. It is also critical to organize data with different compliances.

6.4 Automation in Security

Risk assessment tends to be either skipped entirely or done on a limited basis. Automatic risk assessments will allow for limited risk automation and visibility into where the risk gaps exist.

Automation can also be used in data validation, cleaning and speeding up the time-consuming elements in GRC systems. Another area is to help users with categorization and auditing.

8 SOLUTIONS FOR STORAGE SYSTEMS

8.1 4-LEVEL GDPR COMPLIANCE MODEL

We conclude 4 levels of GDPR compliance for storage vendors:

Level-1: Basic Compliance

Currently most vendors declare basic GDPR compliance, with basic security services and DSR support.

Level-2: End-to-End Provable Compliance

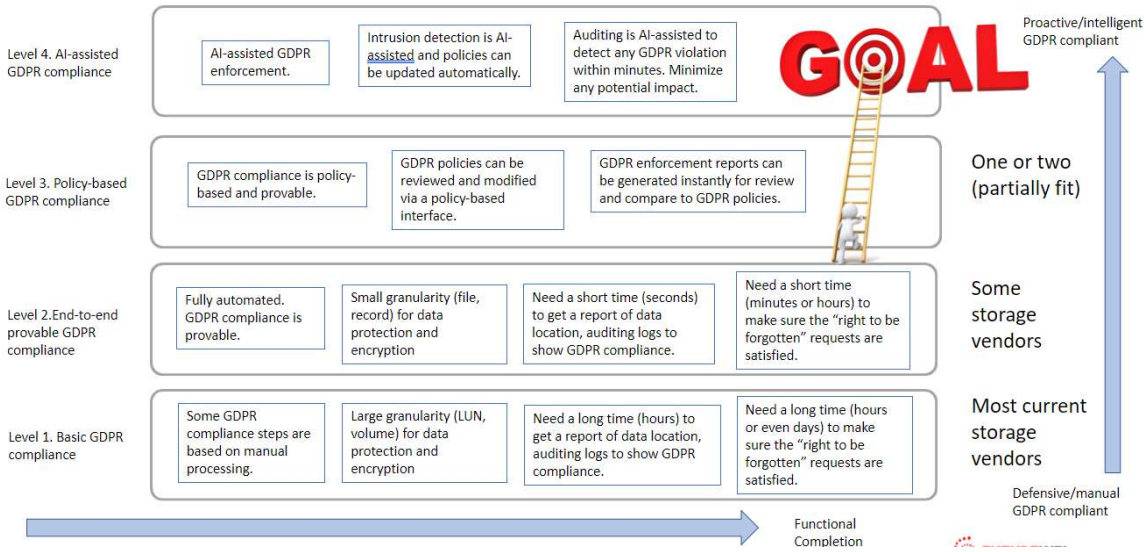
In this level, GDPR compliance is provable, and with some improvements in performance.

Level-3: Policy-Based Compliance

Some storage vendors, such as IBM®, uses data catalogue to organize policies for GDPR and other regulatory compliance.

Level-4: AI-Assisted Compliance

In the highest compliance, AI/ML is used for GDPR compliance, including areas such as intrusion detection and monitoring.



8.2 GAPS

Based on current storage systems, most of storage vendors currently are in either level-1 or level-2 GDPR compliance. In this sector, we are going to propose what we believe the most important gaps for competitive GDPR compliance and security.

For security:

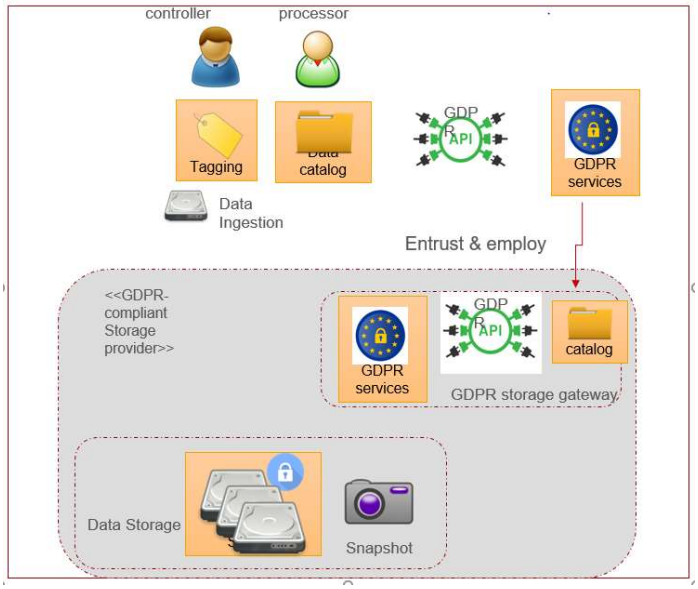
Encryption & Crypto Erasure: Many storage systems use SED which support disk level encryption and crypto Erasure. But they do not provide the capability to cryptographically shred individual files from solid-state drives (SSDs). We need finer granularity for file systems to better support "right to be forgotten".

Pseudonymization: Validating that personal data is used appropriately and the processing has a legal basis, such as consent for the specific purpose, is a key GDPR obligation. We need good consent management to help simplify consent for enterprises and provide more control over how and when data is used.
Data Minimization: Data should be retained for as long as is required to achieve the purpose. Consent management and retention together helps the company to limit personal data collection, storage, and usage, thus realize data minimization.
Risk Management: We need risk assessment for regulatory compliance. We need reports to identify who accessed personal data, where they accessed it from, when it was accessed, and how it was accessed can be used to send notifications to auditors, controllers, and data protection officers.

For DSR:
Metadata Indexing: File level metadata should include more information such as file size, location, owner, dates, extension, ACLs and more. The information can be used for report and analysis.
Consent Management: Validating that personal data is used appropriately and the processing has a legal basis, such as consent for the specific purpose, is a key GDPR obligation. We need good consent management to help simplify consent for enterprises and provide more control over how and when data is used.
Retention: Data should be retained for as long as is required to achieve the purpose. Consent management and retention together helps the company to limit personal data collection, storage, and usage, thus realize data minimization.
Report & Audit: we need reports to identify who accessed personal data, where they accessed it from, when it was accessed, and how it was accessed can be used to send notifications to auditors, controllers, and data protection officers
Incident Report: The 72-hour breach reporting window is short and could greatly benefit from automation. We need tools and services to automate, collaborate, and deploy proactive incident readiness, management, and reporting capabilities to meet GDPR obligations.

8.3 FRAMEWORK FOR EXISTING SOLUTIONS

We propose a GDPR storage gateway on top of storage systems for GDPR compliance services. This gateway includes:
GDPR APIs: to receive requests from controllers and auditors, and to register/request incident report by controllers and auditors.
Data Catalog: Core element for processing data subject requests. It organizes metadata, statistics, logs, and other information together for a complete view for GDPR compliance. It also works with other module such as security module by applying policies.
Compliance & Security Services: this module includes GDPR services such as security and incident report.



8.4 DATA CATALOGUE

We propose to put GDPR related personal data in data catalogue.
Data catalog is a tool that "creates and maintains an inventory of data assets through the discovery, description and organization of distributed data sets" (Gartner).
A detailed and accurate data catalogue can create the foundation for a unified information governance for the GDPR. It organizes information about personal data stores, locations, purposes, owners, data subject type and more.

Benefits of a data catalogue for GDPR compliance:
Better Governance: with the policies defined, it gives storage system better control over other modules such as security and risk management.
Enriched metadata: the metadata repository acts as an index for personal data, making it easier to understand the underlying data. Basic storage system level metadata is inadequate for GDPR compliance.
Increased DSR efficiency: the metadata helps the data subjects to search/ access/ update/ delete personal data faster and in the time limit.
Reduced risk: data access policies should only be available to users who have special permissions within the catalog. Data subjects have greater confidence that their personal data is used only for a given purpose, in compliance with GDPR regulations.

With data catalogue, it is easier to achieve level-3 GDPR compliance (policy-based compliance). Data catalogue benefits are not limited to GDPR readiness. It also helps to comply with other rules and regulations, now or in the future.

8.5 COMPLIANCE & SECURITY SERVICES

Security services work together with data catalogue for fine granularity. Different type of data needs different level of security. With different policies, we can ensure personal data gets enough service, while not impacting the overall performance.

In this sector, we focus on the fields that storage systems need for level-4 GDPR compliance and advanced security systems.

8.5.1 Data Classification

Different data has different requirement for security. A one-size-fits-all security approach will create areas of too much security and others of too little, increasing the risk for the organization. On the other hand, basic system-level information or metadata is inadequate for data administrators who spend a significant amount of time searching for data. They also struggle to identify files and objects that contain sensitive data.

To overcome these data challenges, large enterprises are tuning to data catalogs that offer exceptional data visibility. Data catalogue provides a rich metadata layer on top of the storage sources. This metadata, together with custom and automated tags, enable users to inspect, classify, and gain insights from massive data.

A basic method for classification is applying custom tagging. This enables organizations to classify and categorize data and align this data with different needs.

Automatic identification and classification of sensitive or personal data can also be used. AI/ML can scan and extract sensitive glossary from unstructured data. Content based data classification enables users to easily setup policies and create metadata for data catalogue.

8.5.2 Encryption & Masking

Many major storage vendors use SED which support disk level encryption and crypto Erasure. But they do not provide the capability to cryptographically shred individual files from solid-state drives (SSDs). To support “right to be forgotten”, data subject may want to erase personal data by file or directory. We may need software encryption with finer granularity for file systems. Software encryption normally has the problem of slow processing. But with hardware offload, the process can be accelerated. Also, only personal data with certain policies need to be software encrypted.

Masking need less computation power for Pseudonymization. Masking can help protect data such as telephone numbers, national identification numbers, email addresses or names in logs, file names and other places when it is not encrypted. Also, it is a good way for crypto erasure, if the link between the real information and the mask is removed.

8.5.3 Data Minimization

Data minimization includes consent management and data retention. With data catalogue, the system can control the personal data to be used appropriately and has a legal basis.

Consent Management

The GDPR requires that all organizations must have the consent of EU citizens to process their personal data. Consent is strictly related to a processing purpose. Each processing

purpose is related to one or more activities, such as marketing, analysis, etc. all the requirements regarding one processing purpose can be stored in one consent item. The system needs good consent management to help simplify consent and provide more control over how and when data is used.

Data Retention Management
The GDPR states that personal data may only be kept for no longer than is necessary for the purpose for which it is processed. An organization should identify appropriate retention periods to hold the personal data and create retention policy.

Retention policy defines and manages retention requirements for regulatory compliance. The users have controls that require the personal data to be archived for a certain period of time. We can use several techniques for data retention. For example, crypto erasure can ensure data that should not retain to be removed quickly (the right to be forgotten).

Consent management and retention together helps the company to limit personal data collection, storage, and usage, thus realize data minimization.

8.5.4 Risk Management

Risk management is a full lifecycle from monitoring, detecting, responding, incident reporting, and recovery. we need to identify who accessed personal data, where they accessed it from, when it was accessed, and how it was accessed can be used to send notifications to auditors, controllers and data protection officers. We need to define policy rules and groups that help monitor, audit, record, and provide alerts on any unauthorized activities related to personal data by privileged and unprivileged users and applications.
AI/ML techniques can be used in this area for level-4 compliance, such as detect & response.

Risk Assessment
Risk assessment should be done for regulatory compliance. Article 35 of the GDPR covers Data Protection Impact Assessment with a template.

Monitor
Storage system faces both internal and external threats. Security threats across multiple layers (OS, application, network) must be monitored in real time. Monitoring often works with other security components, such as antivirus and intrusion detection system, to get abnormal information.

Detect & Respond
When a cybersecurity event occurs, the system should be able to detect and take action to the incident. Some security components, such as antivirus and intrusion detection systems, can help detect and respond to these events. In addition, storage systems can take further actions to the events.

Logging

Storage systems log information on who accessed personal data, where they accessed it from, when it was accessed, and how it was accessed. The information should be saved securely, so that it can be retrieved in case of data breach or auditing.

Incident report
We need to send notifications to auditors, controllers, and data protection officers after an incident happened. The GDPR requires reporting data breach within 72 hours. The report should include all related information about the incident.

Recovery
Storage systems should have certain capabilities to restore services impaired by a cybersecurity incident. For example, intrusion detection system should be able to kill malicious connections and restore the network performance.

8.5.5 Location Management

The GDPR (art. 44 ~ 50) imposes restrictions data transfer outside of EU. Storage systems should be able to detect the data location (via data catalogue). When the data is transferred for any reason (replication, tiering, archiving, etc.), the operation should be halted, and an event should be sent to administrator. An intelligent location management should automatically allocate proper location for data transfer operations.

9 REFERENCES

1. GDPR Compliant Data Management System Whitepaper.docx
2. Futurewei Storage Anti-Virus White Paper.docx (sharepoint.com)
3. Root of Trust Definitions and Requirements v1.1 (globalplatform.org)
4. Privacy FAQs - Databricks®
5. Delta Lake on Databricks® - Databricks®
6. IBM® pathways for GDPR readiness
7. Tackling the GDPR An Actionable Approach with Dell EMC® and Index Engines®
8. Getting Ready for GDPR with Dell (rsa.com)
9. Netapp®: GDPR and Data Privacy
10. General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu)