Seamlessly Comply with the GDPR

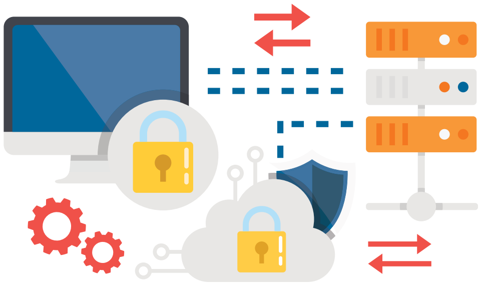
Leverage Data Virtualization to Manage Data Access from a Single Point.

SOLUTION
GDPR Compliance

The European Union's General Data Protection Regulation (GDPR) will go into effect on May 25, 2018, and all businesses that serve European Union customers will be required to comply. The GDPR details how companies must protect personal information, and companies are advised to begin preparations immediately (if they have not already begun) since the regulation has been published as of May 2016. Companies that fall out of compliance with the GDPR will not only be required to pay fines, but may also face lawsuits and additional audits. Should companies actually suffer a data loss as a result of noncompliance, they would also have to pay the substantial price of rebuilding customer trust, and recovering from damage to the brand.

To comply with the GDPR, companies will have to demonstrate that personal data is:

- Processed lawfully and fairly, and in a transparent way.
- Collected for specific, explicit, and legitimate purposes.
- Limited to only what is necessary for processing.
- Kept accurate and up-to-date.
- Stored so that the subject is identified only when necessary.
- Processed in a secure manner so it does not fall into the wrong hands or become lost, damaged, or destroyed.
- Protected "by design": All new systems will need to be developed with privacy in mind.



Many companies will find it challenging to comply with the GDPR, since data is often stored across myriad heterogeneous data sources, both on premises and in the cloud. Forrester, in a brief entitled "You Need An Action Plan For The GDPR"[1] stresses that companies may be called upon to report on security measures, even in the absence of a breach. Companies may need to report on where specific records are stored, where they are transferred to, and who has the authority to view it. In many cases, they may also be called upon to explain their rationale for all technical decisions.

In the same brief[1], Forrester cautions that the GDPR's "privacy by design" requirement will be the most difficult one to meet, since security and privacy experts will need to play an active role in product development.

To prepare for GDPR, companies will need a bird's-eye view into all of the data, and a way to establish security controls over the entire infrastructure from a single point. Data virtualization provides this capability, enabling companies to quickly and easily comply with the GDPR without investing in new hardware or re-building existing systems from the ground up.

[1] Brief: You Need An Action Plan For The GDPR", Forrester Research, Inc., October 14, 2016

Data Virtualization for Seamless GDPR Compliance

Fine-grained Security and Complete Auditability

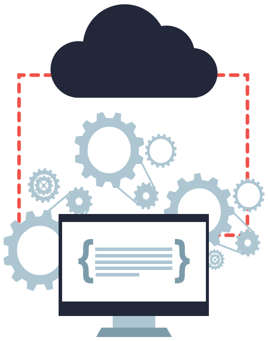
Data virtualization provides companies with fine-grained control over sensitive customer information stored across multiple systems, by establishing a single, unified access layer across on-premises and off-premises systems. When data consumers need to access a source, they do so through the data virtualization layer, which contains the metadata for accessing each source, and returns a secure, virtualized view of the data to the consumer, in real time. These views are traceable and auditable, and will only be delivered to authorized consumers.

Complete Data Lineage and Agile Business Rules

At any point in time, companies can understand, and report on, the full lineage of any sensitive data set, including its original source, any views, and any modifications. In addition, through the data virtualization layer, companies can establish sophisticated rules for automating GDPR compliance, such as masking data on the fly, so it cannot be viewed by users who lack the requisite credentials. Again, such rules can be applied quickly and effectively across diverse systems, since they are being applied in the data virtualization layer.

Facilitates Privacy by Design

Data virtualization is also particularly well suited to helping companies to comply with the GDPR's "protected by design" requirement. By definition, a data virtualization layer does not require a source to be of a prescribed type, or to be accessed in a certain way. New sources can easily be added to the infrastructure by connecting them to the data virtualization layer, where it is immediately subject to the same security controls and auditability as any other source on the system, irrespective of the data source technology.



Eliminates Unnecessary Data Movement

With a data virtualization layer in place, no data needs to replicated for reporting purposes, and no ETL scripts need to be rewritten. A data virtualization layer operates with a company's existing infrastructure, configured exactly as it is. It merely abstracts the access functions, so that users perceive the data as existing in a single virtual repository. For GDPR compliance, security administrators can control all access through a single point.

Secures Data-at-rest and Data-in-motion

The data virtualization layer can perform role-based authentication at any level, guest, employee, or corporate; apply data-specific permissions including row- and column-level masking; define schema-wide permissions and policy-based security. The virtualization layer secures data in transit via SSL/TLS protocols, and authenticates users via industry proven protocols such as LDAP, pass-through with Kerberos, Windows SSO, OAuth, SPNEGO authentication, and JDBC/ODBC Security.

Benefits

Access to the most up-to-date data through real time access to data sources.

Fewer copies of personal data.

Data on-premises and off, combined through the same governed virtual layer.

Full auditing and monitoring capabilities, including logs of which users view which data.

Captures full data lineage, helping security stake-holders to understand the original sources for all data.

On the fly data masking capabilities, across the enterprise.

Consistent management of security controls, applied via a single access point.

With a data virtualization layer powered by the Denodo Platform, companies can

Apply a cost-benefit-based approach to data privacy and security.

Leverage data privacy and security to drive superior customer experiences.

Consistent management of security controls, applied via a single access point.

Easily instill data privacy and security into new initiatives that require information access.

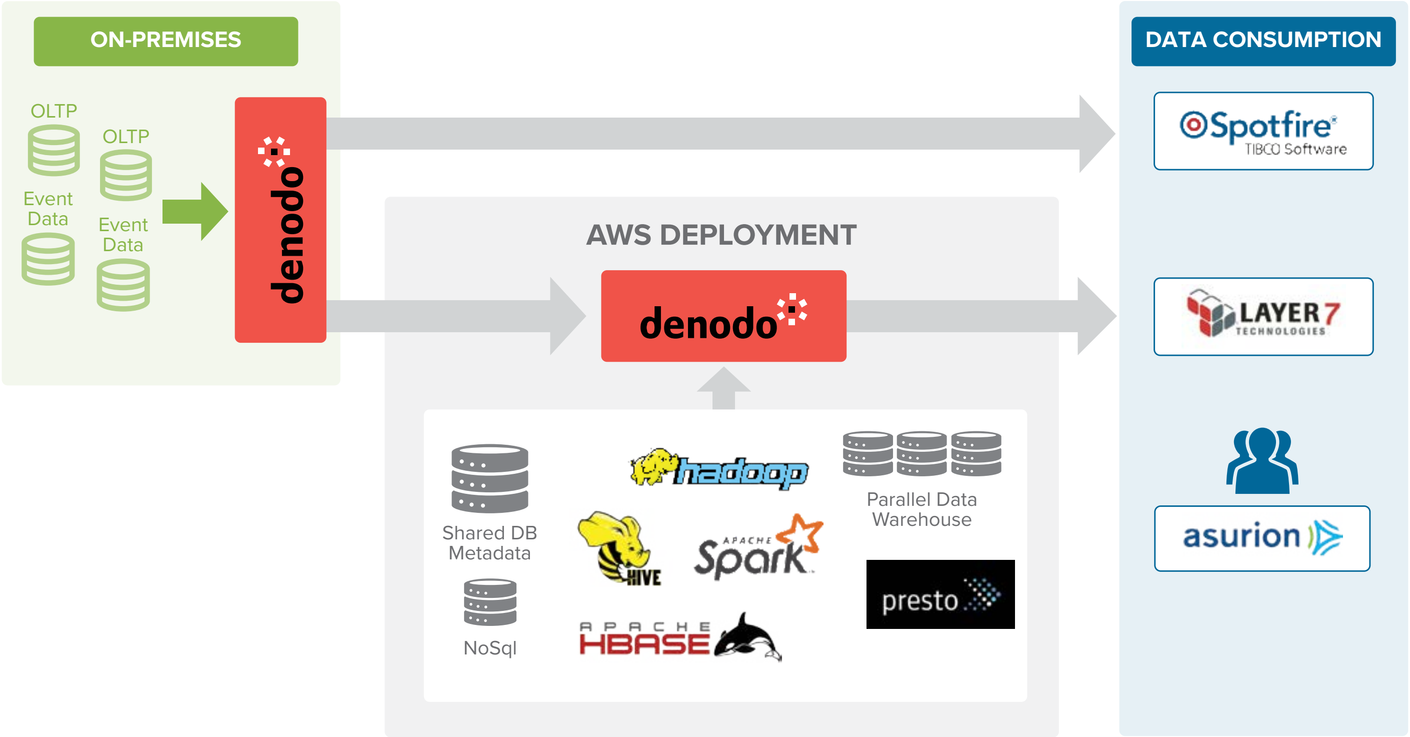
On the fly data masking capabilities, across the enterprise.

Case Study: Asurion

Asurion is the leading provider of global technology support and protection products. The company wanted to modernize its infrastructure to include cloud-based analytics, but because it faced strict restrictions on migrating personally identifiable information, and needed to maintain compliance with a set of increasingly stringent governmental regulations, Asurion needed to centralize security management companywide, around a single point of control.

Solution

Leveraging the Denodo Platform, Asurion set up a data virtualization layer that runs on an Amazon Web Services (AWS) instance in the cloud. By standardizing access to all data sources (including on-premises and cloud) through the data virtualization layer, Asurion is able to use the virtualization layer to implement security controls across the enterprise data holdings, greatly simplifying security management.



> *"The Denodo Platform was one of the easiest and most successful rollouts of critical enterprise software I have seen, and it was immediately successful in handling our initial security use case."*
> Enterprise Architect, Asurion.

Results

After implementing the data virtualization layer, Asurion was able to:

- Control security across the entire infrastructure from a single access point.
- Easily meet regional data security requirements.
- Perform complete audits of data access, as needed.
- Quickly and easily add new, compliant sources.

WESTPOLE
a prodware company

DV4EI (data virtualisation for european institution) is a group of companies advocating data virtualisation accross european institutions
Westpole is a member of DV4EI and the European point of reference in the IT market for the Digital Transformation of pioneering companies, ready to face the technological and digital challenges of tomorrow, to embrace innovation and transform their activities and their way of doing business. visit westpole.be

denodo

Denodo Technologies is the leader in data virtualization providing agile, high performance data integration, data abstraction, and real-time data services across the broadest range of enterprise, cloud, big data, and unstructured data sources at half the cost of traditional approaches. Denodo's customers across every major industry have gained significant business agility and ROI.

Visit www.denodo.com