

Case Study: Data Privacy from Authorised Users

The requirement for organisations to enforce strong security and data protection for sensitive information has never been greater. Industry and government regulations, legal implications, fines, brand damage and loss of customer confidence have all become major factors for ensuring adequate data privacy measures are being taken.

The needs for data privacy can be summarised as follows;

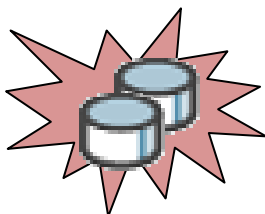
- The risk to brand damage and reputation.
- Potential legal and compliance implications.
- The value of information.

Traditional security measures have been focussed on protecting the perimeter of the organisation (Firewalls, IDS/IPS). Although still necessary, a more 'data centric' approach is needed for data confidentiality to protect from both external and internal threats, contractors and outsourced service providers. The need to protect sensitive customer, financial and internal data has been increasingly made more public. Failure to provide adequate security and data privacy can have serious and long-term negative consequences for any organisation.



Data Protection

Just one incident can severely damage your reputation and your ability to conduct business effectively, leading into the future. Data breaches can incur costs from a variety of sources including legal, fines, brand damage, and public relations. It is crucial that your company is accountable to all stakeholders, customers, and employees.



Security

Good data privacy and security practises require organisations to protect their data against the threat of data theft. With an increased risk for both internal and external users, security measures should be taken to protect the confidentiality of data.

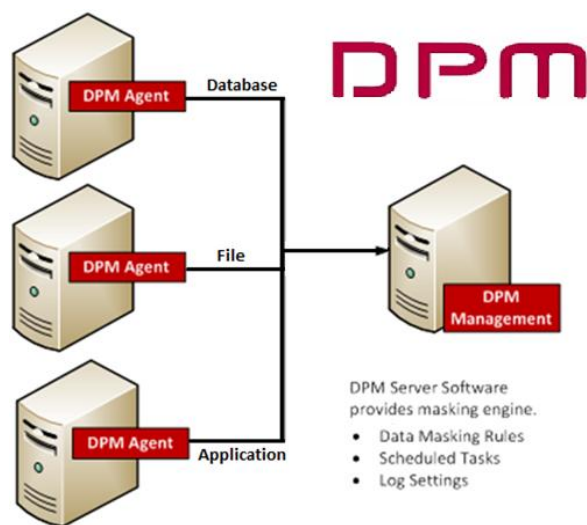


Compliance

Current industry and government compliance standards require sensitive information to be protected. Compliance standards such as PCI DSS state that it is mandatory to mask Credit Card numbers when displayed (Requirement 3.3) for unauthorized users. DPM provides a simple data privacy and compliance solution for PII, PCI DSS, HIPPA, and other data privacy standards.

securing your business

Randtronics Data Privacy Manager (DPM) provides comprehensive data protection for sensitive information to facilitate data privacy and compliance. It is an inexpensive way to provide need-to-know access to internal and external users for ensuring data protection.



Randtronics DPM provides robust capabilities to protect, transform and mask sensitive data anywhere within the organisation. Randtronics DPM provides centralised security rules and policies management that you apply to heterogeneous environments. DPM is simple to install, and easy to use. Graphical user interface enables managing masking rules and security policies from a single central location. No special knowledge of data masking or algorithms is required during operational processes.

Dynamic Masking for Databases

DPM provides strong data protection within DB environments. Unlike other masking solutions DPM protects data in production as well as test & dev environments. With its robust masking capabilities DPM transforms data using a combination of different characters and masking ranges. No changes required for client applications. It provides high performance and supports multiple concurrent connections.

Masking for Structured and Unstructured Files

DPM removes the risk of inappropriate visibility of data within flat files, documents from the customers, internal reports, application logs etc. The DPM solution can search and discover target data in the files and masking it according to the specified security policies. The DPM scheduling capabilities allows for automated masking with both Single and Batch mode. It supports various file type including TXT, CSV, XML, PDF and Word.

Plug-in for Encryption and Tokenisation

DPM supports the extension of both Encryption and Tokenisation modules to expand its data privacy capabilities. Tokenisation protects sensitive data by replacing it with surrogate values of the same size and type whereas original data is encrypted and securely stored in a centralised location. DPM provides out-of-box tokenisation solution as well as adapters for other 3rd party vendors. Encryption is provided either natively, software or dedicated hardware security modules (HSM).

securing your business