Case Study PCI-DSS Data Protection

PCI-DSS Data Protection

Using Data Privacy Manager (DPM) to address PCI-DSS data protection requirements

The Challenge

Organizations seeking to process and store credit card data are obliged to comply with PCI DSS standards that mandate the use of encryption to protect credit card data.

PCI DSS Requirements and Testing Procedures V4.0, requirement 3: Protect Stored Account Data:

- Protect data-at-rest: using encryption or tokenization, and protect encryption keys
- Protect data-when-display: Show at most, BIN + last 4 digits

Ideally the organization would have access to a simply mechanism to implement and manage these protections across multiple databases, servers and applications with the ability to manage and audit data protection.

The Solution

Randtronics DPM provides a comprehensive array of data protection methods that enable organizations to easily achieve and demonstrate compliance with PCI-DSS data protection requirements.

1. Server Encryption

Encrypt **DB server**
protect DB plus Log files, reports, passwords, certificates, config files, key files, etc.

2. Field-level encryption and Tokenization

Wide range of data protection options[1] for data-at-rest stored in Database

Protects data even from Database Administrator

3. API Integration

Easy-to-code, calls to invoke wide range of data protection options[1]:

- Allows data to be safely stored in public cloud databases,
- Use outsource IT organization without increasing data breach risk
- Maintains complete control over data sovereignty (as you control where encryption master keys are stored)

4. Flat File Tokenizer

Sanitize sensitive data in CSV and Text Files.

- Strip sensitive data from reports being shared
- Eliminate PII from archives
- Wide range of data protection options including [1]

Note 1: Options include standard encryption, format preserving encryption, tokenization and masking

Benefits

- Protect data on any server environment with a Windows or Linux operating system with Transparent Data Encryption
- Zero Trust protection: supports field-level data protection that provides protection from all unauthorized access including system administrators and database administrators
- Enables production data to be safely sanitised for Test data sets and Analytics
- Protection and centralized management of keys with option for high-assurance masterkey protection in hardware
- Simplified demonstration of data protection compliance through use of a centralized, policy-driven and fully auditable data protection platform

Randtronics
For more information, please visit
www.randtronics.com