PCI-GENERAL™ A Secure MySQL Database Appliance

Highlights

- Address regulatory compliance requirements with built-in security features
- Encrypt MySQL data transparently (TDE)
- Prevent privileged user from accessing MySQL data
- Operate MySQL database in an environment secured through a transitive trust model
- Achieve non-repudiation through cryptographically signed compliance reports
- Store encryption keys in FIPS 140-2 Level 2/3 compliant smart-cards with built-in key rotation and revocation capabilities

Organizations are under increasing pressure to protect all kinds of data in order to comply with industry mandates like PCI DSS and government regulations like HIPPA/HITECH. On one hand, the loss of cardholders information can irreparably damage consumer's trust in the brand and adversely impacts stakeholders, but the loss of patient record information can lead to *civil and criminal penalties*. In other words, the fallout from a data breach can far outweigh the cost associated with implementing a data security solution in the first place. Organizations that store their regulated data in a MySQL database have to be extra vigilant. Here are some of the challenges associated with storing regulated information in a MySQL database:

The MySQL database stores data in *flat files*. A malicious *"root"* administrator can easily view or alter such files. This could lead to disclosure of regulated information. The HIPPA/HITECH act requires that appropriate steps be taken to secure patient information in order to qualify for relief under *safe harbor*. The PCI mandates require that *cardholders data must be encrypted*. However, there is no easy way to encrypt MySQL data. Some level of programing effort could enable an organization to encrypt data using the MySQL programming interface. The organization then must deal with pivotal issues such as key management and having to make changes to their application. Lack of implementation of a proper key management solution can result in only two possible outcomes: (1) a successful *data compromise* or (2) not being able to *access data* when it's needed the most.

Organizations looking to secure their information stored in a database against a *malicious database administrator* sometimes resort to encrypting database columns. However, it's virtually impossible to protect information against a *malicious database administrator*. Why? Because a malicious database administrator can impersonate a database user who has been granted access or simply interject himself into the path of clear text data by modifying a stored procedure or triggers utilized to decrypt columns.

Furthermore, the MySQL database depends on the operating system for its security. Once a server OS is compromised, the MySQL's access controls or encryption can no longer protect valuable data. The problem is exacerbated by the fact that the circle of trust for most MySQL servers (users with root privileges) is generally large and poorly controlled.

Highlights

- Secure MySQL binary logs against tampering
- Control MySQL user privileges
- Attain separation of duties (SOD) through role-based platform management
- Go through an audit with a secure MySQL appliance specifically designed to enable regulatory compliance
- Get security updates for the entire stack from a single source
- Avoid costly mistakes and save time by deploying a hard or virtual MySQL database appliance tuned to provide maximum security and performance

In order to solve these and other security related problems, Packet General has created the industry's first combined software and hardware solution for MySQL database. PCI-GENERAL™ is a secure MySQL database appliance tuned to provide maximum security and performance. PCI-GENERAL™ eliminates the need for organizations to have to create a patchwork of security solutions to secure data and achieve compliance. Here are some of the main benefits of using PCI-GENERAL™:

Regulatory compliance and data security

PCI-GENERAL™ has been designed to enable compliance through real data security. The added data security measures do not require any changes to be made to the MySQL database. Hence the MySQL client applications continue to operate normally even though the MySQL data is being safely stored in a fortified and secure operating environment. Any attempt to compromise data results in a real time alert.

PCI-GENERAL™ transparently encrypts the MySQL data using FIPS 140-2 compliant algorithm.

PCI-GENERAL™ employs FIPS 140-2 Level 2/3 smart cards to store the encryption keys with built-in provisions for:
Secure key distribution
Key rotation
Key revocation
90-day password rotation

PCI-GENERAL™ doesn't allow a privileged ("root") user to access MySQL data. Any attempt to compromise data by the privileged user results in generating a real-time alert.

PCI-GENERAL™ also prevents the MySQL database administrator from changing the MySQL log files.

PCI-GENERAL™ uses role based platform management. Assignment of privileges is based on job classification.

PCI-GENERAL™ generates audit trails which are cryptographically signed, time stamped and are stored in an encrypted format to avoid tampering. The audit trails are retained on-line for 90-days in order to satisfy compliance requirements.

PCI-GENERAL™ security specifications

Security Specifications	Description	PG-100	PG-200	PG-300	PG-E50V	PG-150V
Encryption algorithm used	Advanced Encryption Standard (AES) - symmetric-key encryption standard (U.S. FIPS PUB 197 (FIPS 197).	Y	Y	Y	Y	Y
Key size	256 bits	Y	Y	Y	Y	Y
Key storage	Federal Information Processing Standard (FIPS) Publication 140-2/3 based smart cards running EAL4/EAL5 operating system.	Y	Y	Y	N	Y*
Key distribution	Secure distribution conducted during the appliance installation.	Y	Y	Y	N/A	Y
Key revocation	Authenticated revocation - a single step process.	Y	Y	Y	N/A	Y
Key rotation	Built-in key rotation.	Y	Y	Y	Y	Y
Non-repudiation	Cryptographically signed reports stored in an encrypted data vault.	Y	Y	Y	N	Y
Protection against malicious privileged user	The OS “root” user is not allowed to view/alter the MySQL data. The MySQL “root” user is not allowed to alter the MySQL binary logs.	Y	Y	Y	Y	Y
MySQL data encryption	Transparent data encryption of MySQL data. “On-demand” encryption of various MySQL databases. MySQL client applications remain unchanged.	Y	Y	Y	Y	Y
MySQL binary log file	Logs are protected via strong encryption.	Y	Y	Y	Y	Y
MySQL backups	Encrypted backups with proper key management.	Y	Y	Y	N	Y
MySQL service	Privileged operation - protects against physical loss of an appliance.	Y	Y	Y	Y	Y
Firewall	Built-in customized firewall.	Y	Y	Y	Y	Y
Services	Minimal set of services that are needed to run the MySQL server in a secure and controlled environment.	Y	Y	Y	Y	Y
Platform management	Role-based platform management.	Y	Y	Y	Y	Y
Security updates	Automated and tested updates. Single source for all security updates.	Y	Y	Y	Y	Y
Hardened MySQL appliance	Appliance footprint < 700MB.	Y	Y	Y	Y	Y
Management	Secure web based administration.	Y	Y	Y	Y	Y

* Certain limitations apply

PCI-GENERAL™ appliance specifications

Available models:

Model#	PG-100	PG-200	PG-300	PG-E50V	PG-150V
Operating System	Secure PG-OS	Secure PG-OS	Secure PG-OS	Secure PG-OS	Secure PG-OS
CPU - Quad-code Intel Xeon 2.4GHz 4 x 12M Cache, Turbo, HT, L2 Cache 8MB L3 Cache, 1066MHz Max Mem	1	2	2	SMP Virtual	SMP Virtual
Memory - Registered w/ ECC 1333MHz Dual Ranked RDIMMs	12GB	24GB	48GB	Minimum 2GB	Minimum 2GB
Storage - SATA 10000-RPM 16MB Cache 3.0Gb/s	500GB RAID-5	500GB RAID-5 w/ Hot Spare	500GB RAID-5 w/ Hot Spare	N/A	N/A
Disks	3	4	4	N/A	N/A
NIC/LOM	2x GbE LOM	2x GbE LOM	2x GbE LOM	N/A	N/A
Availability	Hot-swap HDD; 500W Redun-dant PSU;	Hot-swap HDD; 500W Redundant PSU; Memory RAS	Hot-swap HDD; 500W Redundant PSU; Memory RAS	N/A	N/A
Enclosure	1U	1U	1U	N/A	N/A
Power Supplies	Redundant 500W (80+GOLD) Auto Ranging 100V ~240V)	Redundant 500W (80+GOLD) Auto Ranging 100V ~240V)	Redundant 500W (80+GOLD) Auto Ranging 100V ~240V)	N/A	N/A
Dimensions	1.69 x 17.09 x 24.69 (in)	1.69 x 17.09 x 24.69 (in)	1.69 x 17.09 x 24.69 (in)	N/A	N/A
Weight	35.02lbs (15.9Kg)	35.02lbs (15.9Kg)	35.02lbs (15.9Kg)	N/A	N/A
Operating Environment	50 to 95 °F 10 to 35 °C	50 to 95 °F 10 to 35 °C	50 to 95 °F 10 to 35 °C	N/A	N/A
# transactions	Number of "sql-bench" encrypted transactions/sec	500*	650*	750*	N/A

* Performance data represents the maximum capabilities of the system as measured under optimal testing conditions.

Packet GENERAL Networks™

DEFEND YOUR DATA™

Packet General is a data security company focusing on regulatory compliance.

Packet General product portfolio includes PCI-GENERAL™, an encrypted MySQL appliance, File-GENERAL™, a secure file repository and Vault-GENERAL™, a secure data vault for sharing of regulated information amongst partners. Packet General is based in New York, USA.

For more information about Packet General, please visit www.packetgeneral.com or call +01 631 546 5047.