Vault-GENERAL™
A Secure File Transfer Vault

Benefits

- Specially designed file vault that allows file transfers in accordance with the HIPPA/HITECH Act and the PCI mandates.
- Provides irrevocable file transfer/access logs for compliance and forensic purposes.
- Eliminates threats to transfer files "at rest" as well as "in transit" through strong encryption.
- Disallows privileged insiders from viewing information stored in the transfer files.
- Enables two or more trusted parties to manage their own users.
- Provides easy access to transfer files from the inside and the outside.

Vault-GENERAL™ is a secure file transfer appliance that allows business partners to exchange sensitive files in a secure and compliant manner.

The current SaaS and appliance based file transfer solutions are unable to help organizations meet the regulatory compliance requirements adequately. Here are some of the main flaws in these solutions that could lead to non-compliance:

- Lack of protection against privileged insiders
- Absence of tamper-resistant logs
- No way to ensure integrity of data stored in transfer files
- No encryption for file data "at rest"

The above mentioned flaws pose considerable risk to the sensitive data stored in the transfer files and are in direct violation of PCI DSS 2.0 mandates as well as the HIPPA/HITECH Act.

Consequences of a successful data breach:

The consequences of a data breach are serious. The Ponemon Institute survey conducted in 2009 revealed that the average cost of a data breach to a business was $6.75 million dollars, which translated into $202 per-record. The survey also shows that the most expensive data breach in the 2009 was nearly $31 million dollars and the least expensive was $750,000[1] . So it's obvious that a data breach can not only tarnish the reputation of the breached entity but can also have serious financial ramifications.

Vault-GENERAL™ mitigates risks:

Vault-GENERAL™ enables compliance by eliminating the above mentioned flaws:

Protection against "privileged insider":

Misplaced trust in the privileged user (“root”) exposes a regular file transfer server to ever-increasing malicious activity. This occurs because the underlying operating system implicitly trusts the privileged user which leads to many problems. For example, a malicious privileged user can view data stored in any file that is being transferred. Moreover, the malicious privileged user can launch subtle attacks by changing data. Any record of such activity can be easily altered or deleted by the privileged user. This not only violates the corporate trust but also results in regulatory non-compliance.

Vault-GENERAL™ eliminates this very critical flaw. A regular "privileged user" has no control over Vault-GENERAL™. In fact the privileged user is not even allowed to view the information stored in the transfer files.

---

[1] Ponemon Inst., 2009 Annual Study: U.S. Cost of Data Breach, 14 (Jan. 2010)

Highlights

- Transparent encryption of transfer files at rest and in transit.
- FIPS 140-2 Level 2/3 smart-cards are used to store keys with built-in provisions for: secure distribution, rotation, revocation
- Privileged insiders are not allowed to view data stored in transfer files.
- Role-based platform management enables assignment of privileges based on job classifications.
- File transfer audit trails are cryptographically signed, time stamped and are encrypted to avoid tampering.
- Logs are retained on-line for 90-days in order to satisfy compliance requirements.

Tamper-resistant file access logs:

Every file transfer/access operation is logged and cryptographically signed and stored in an encrypted vault. The privileged user is not allowed view/alter these log files. Even the Vault-GENERAL™ administrators are denied access to this critical evidentiary material.

Data integrity:

A successful attacker can alter the data stored in transfer files or alter the functionality of the server so that sensitive information is revealed. Users and administrators of the system remain unaware since it's done without altering the expected behavior.

Vault-GENERAL™ eliminates data tampering. Checksums are computed before data is written to the disk. Upon receipt of a read request, the integrity of data is re-established by matching the expected checksum values against the actual checksum values. These powerful capabilities ensure data integrity, not available in other solutions.

Data encryption "at rest":

Vault-GENERAL™not only encrypts files "in transit" but also encrypts them "at rest". Data encryption is transparent hence no client side changes are required. The security of any cryptography-enabled system ultimately depends on the security of the cryptographic keys and certificates used. Key generation, storage, and/or distribution are always critical aspects of any distributed secure system. Vault-GENERAL™ uses several cryptographic keys to provide a comprehensive solution. The encryption keys are stored on FIPS 140-2 Level2/3 compliant smart-cards. The key management system is equipped to revoke and rotate keys.

In short, the Vault-GENERAL™ solution is suitable for organizations that are looking for the following attributes in their file transfer solution:

- Exchange data in a manner that enables compliance with PCI DSS 2.0 or the HIPPA/HITECH Act.
- Looking for shorter and less expensive audit engagements.
- Keep complete control over their transfer file setup
- Prevent their privileged insiders from accessing sensitive information stored in the transfer files
- Minimize data transfer costs as new partnerships are established.

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.