File-GENERAL™
A Secure File Vault
Designed to enable compliance

Highlights

- Transparently encrypt flat files using FIPS 140-2 compliant algorithm and key management
- Achieve compliance with government regulations and industry mandates with a product that has gone through several audits
- Share files only with the intended parties
- Track file accesses with cryptographically signed file logs
- Trusted by tier-1 merchants to secure credit card information and achieve compliance

Every organization needs to share information. Centralized file servers are used to share large files. Generally two types of file servers are used - homegrown file servers that use off the shelf commercial operating systems (“COTS”) and others that are sold as dedicated NAS/SAN devices. However, these file servers are not designed with security or regulatory compliance in mind. Several government regulations and industry mandates require file data to be encrypted and access be controlled in a verifiable manner. Organizations struggle with such compliance requirements and are often forced to deploy point solutions or resort to putting in compensating controls in place. Both approaches fail to protect the most valuable asset of an organization - data.

Another major design flaw exposes organizations legally as well as financially. File servers are designed to implicitly trust the privileged user. This trust allows a malicious system administrator to view confidential information stored in files irrespective of the file ownership. Moreover, a privileged user can easily mask such abuse which makes it even more dangerous. Since there are many administrators within an organization, it’s hard to pin point who acted maliciously. Most organizations are either unaware of this risk or accept it begrudgingly.

File-GENERAL™ - Protects file data

File-GENERAL™ is a new type of a file vault that is dedicated to storing only the confidential files. Access to highly sensitive files stored on File-GENERAL™ is granted by a duly authorized File-GENERAL™ administrator. Smart-card are used to authenticate administrators to eliminate any foul play. All files are transparently encrypted before being stored onto the disk. Access to the sensitive files is logged, time stamped, cryptographically signed. The logs are stored in an encrypted vault.

Achieve Compliance With File-GENERAL™

Highlights

- Available as a virtual or a hard appliance
- FIPS 140-2 Level 2/3 compliant smart-card based key management
- Role-based platform management provides separation of duties (SOD)
- Access data via multiple file access protocols - SMB/SAMBA, SSHFS, SFTP
- Avoid costly security mistakes and reduce operational cost with a ready-to-deploy appliance set to provide maximum security to flat files
- Prevent privileged user from viewing confidential information stored in files

Compliance made easy

File-GENERAL™ strictly controls access to the sensitive files stored in its "Crypto-Shares". Each and every access to a sensitive file is diligently logged. The log files are cryptographically signed and stored in an encrypted vault. Built-in security features designed along with existence of tamper-resistant logs make the process of going through an audit much simpler.
File-GENERAL™ has gone through several compliance scrutinies that are reserved only for level-1 merchants.

Encrypt confidential data transparently

File-GENERAL™ encrypts all types of file data transparently using FIPS 140-2 compliant algorithm. No client software is needed.

FIPS compliant key management

The security of any cryptography-enabled system ultimately depends on the security of the cryptographic material (keys and certificates) used. Key generation, storage, and/or distribution are always critical aspects of any distributed secure system. File-GENERAL™ provides:

- Secure key distribution
- Secure storage for encryption keys using FIPS 140-2 smart-cards
- Key rotation
- Key revocation

Eliminate priviledged user information abuse

File-GENERAL™ employs role-based platform management. The privileged user is not trusted within the File-GENERAL™ trust model. Hence the traditional IT administrators who are responsible for managing file or Active Directory servers have no control over File-GENERAL™ and can’t access the protected data stored in the "Crypto-Shares".

A transitive trust model based data security

Data security and assurance can only be achieved if every layer of the software and the hardware can be trusted. The File-GENERAL™ utilizes a transitive trust model in which data is secured using a stack of trusted components. Starting at the hardware layer, the BIOS verifies that the boot code has not been tampered with, and gives it control; the boot code, in turn, verifies that the kernel has not been modified (a frequent source of compromise by a malicious administrator with physical access to the disk). The kernel then finishes booting, validating each service and each application before it launches them. The Packet General Security Token (PG-ST) is used as the “root of trust”.

Security

Security Specifications	Description
Encryption algorithm used	Advanced Encryption Standard (AES) - symmetric-key encryption standard (U.S. FIPS PUB 197 (FIPS 197)).
Key size	256 bits
Key storage	Federal Information Processing Standard (FIPS) Publication 140-2/3 based smart cards running EAL4/EAL5 operating system.
Key distribution	Secure distribution conducted during the appliance installation.
Key revocation	Authenticated revocation - a single step process.
Key rotation	Built-in key rotation.
Protection against malicious privileged user	The OS “root” user is not allowed to view/alter the file data stored in a secure repository. The “root” and File-GENERAL administrators are not allowed to alter the file access logs.
File data encryption	Transparent data encryption of all types of file data. “On-demand” encryption of Crypto-Shares. No client side agent required.
File access logs	Tamper-resistant logs stored in an encrypted vault.
File access protocols	SMB/SAMBA, SSHFS, SFTP - profiled
File service	Can only be started by the Data Administrator - protects against physical loss of the appliance.
Firewall	Built-in customized firewall.
Services	Minimal set of services that are needed for a secure and controlled operation.
Logs	Cryptographically signed logs stored in encrypted format.
Platform management	Role-based platform management.
Security updates	Automated and tested updates. Single source for all security updates.
Hardened appliance	Appliance footprint < 700MB.
Management	Secure web based administration.

Hardware

Available models:

Model#	FG-100	FG-200	FG-300	FG-150V
Operating System CPU - Quad-code Intel Xeon 2.4GHz 4 x 12M Cache, Turbo, HT, L2 Cache 8MB L3 Cache, 1066MHz Max Mem	Secure PG-OS 1	Secure PG-OS 2	Secure PG-OS 2	Secure PG-OS SMP Virtual Appliance
Memory - Registered w/ ECC 1333MHz Dual Ranked RDIMMs	4GB	8GB	16GB	Minimum 2GB
Storage - SATA 10000-RPM 16MB Cache 3.0Gb/s	500GB RAID-5	1TB RAID-5 w/ Hot Spare	2TB RAID-5 w/ Hot Spare	N/A
Disks	3	4	4	N/A
NIC/LOM	2x GbE LOM	2x GbE LOM	2x GbE LOM	N/A
Availability	Hot-swap HDD; 500W Redundant PSU; Memory RAS	Hot-swap HDD; 500W Redundant PSU; Memory RAS	Hot-swap HDD; 500W Redundant PSU; Memory RAS	N/A
Enclosure	1U	1U	1U	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
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
Weight	35.02lbs (15.9Kg)	35.02lbs (15.9Kg)	35.02lbs (15.9Kg)	N/A
Operating Environment	50 to 95 °F	50 to 95 °F	50 to 95 °F	N/A

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.