Not All Encrypted Storage is Secure

By Michael Ryan CEO, South River Technologies

Sensitive and confidential documents stored on your servers need to be protected. PGP (Pretty Good Privacy) Encryption is likely a requirement on your security checklist. PGP is a method of securing digital information and is usually used to encrypt data "at rest."

Not all PGP implementations offer complete point-to-point security. Standard PGP implementations often leave your data exposed, or leave images of unencrypted data on disk.

Standard PGP Implementation

A file is sent to a server using a secure protocol. When it reaches the server, an unencrypted version is written to disk. The file is encrypted, and a new, encrypted version is written to disk. The unencrypted version is marked as deleted. In some implementations, the original encrypted version is scrubbed, but sometimes that file image remains until the operating system re-uses that space.

Streaming PGP Implementation

A file is sent to a server using a secure protocol. When it reaches the server, it is encrypted and written to disk in a single step. Using this method, no unencrypted data is written to disk, and there is no need to remove the original file image after encryption.

Whether implementing a secure server internally, or through a service provider who offers encrypted storage, you need to know how it works.

Streaming PGP is essential to a managed file transfer solution, as it ensures that non-encrypted data is never present in the storage repository. While this may not seem obvious, it's critical to ensuring that your data is never exposed.