PCI Compliance with Cornerstone MFT Server

Payment Card Industry Data Security Standards (PCI DSS) were developed to increase control of cardholder data to reduce credit card information exposure and fraud. Every company handling, storing, or transferring credit card data must meet PCI standards.

Cornerstone MFT Server helps your company meet PCI standards by providing security of data at rest and in transit, as well as enabling you to restrict access to that data with permissions settings and events management.

Data Protection

Encryption of stored data is vital to security. Cornerstone encrypts data at rest with the PGP algorithm and integrates with NTFSencrypted file systems for added protection and convenience.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

This means your data is encrypted at all times—if information is stolen from the server, it isn't readable. Administrators who have access to the server still can't read files that aren't intended for them. If a computer is left logged into an administrative account, unauthorized users can't access files.

Furthermore, when data is deleted from Cornerstone, it is removed securely and completely scrubbed from the hardware. No one will be able to dig up data ghosts from old server equipment.

Encrypted Transmission

Cornerstone supports both SSL and SSH encryption methods for data in transit, which means even if your information is intercepted, the information won't be usable by anyone but the intended recipient. SSL certificates also authenticate the origin of information transfers, so you know data hasn't been tampered with since the key holder sent it.

Restricted Access

Cornerstone offers a highly granular set of configuration options at the server, group, and user level. Many of the default settings are already PCI compliant; an administrator can easily change the rest from the Cornerstone console. This includes options to force complex passwords to ensure a minimum level of security awareness in your users. You can also set permissions for groups and

users, to restrict access to need-to-know personnel.

Additional Compliance Features

Track Events

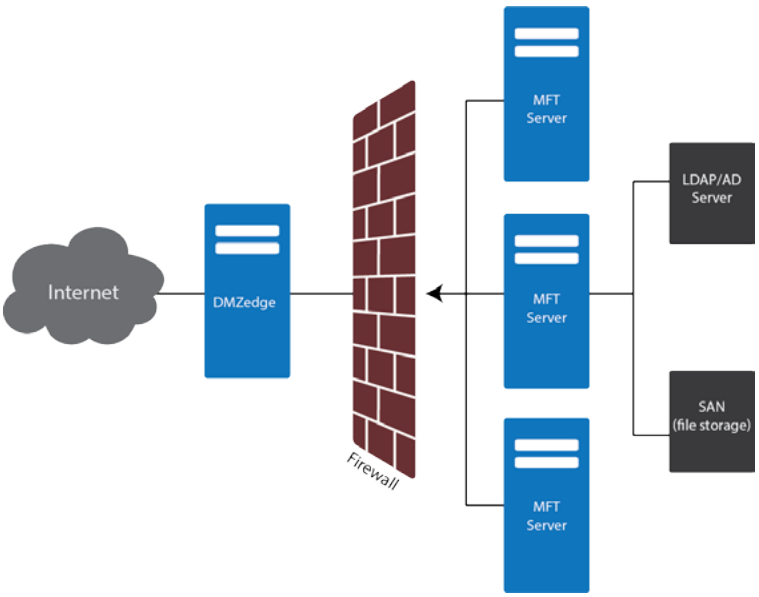
Cornerstone includes StatsTrack, a module which gives you the power to create reports of user activity. This, along with server-wide logging and a powerful Events Management system, allows you to log server activity down to the individual user level.

Maintenance

Cornerstone comes with a year of maintenance with optional longer-term upgrades. Maintenance includes patches and updates, which means your software stays up-to-date, secure, and compliant. Regular update notifications keep you on track and help you stay PCI compliant.

Perimeter Security

Used with DMZ*edge*, Cornerstone gives you added security by allowing you to close all in-bound ports to your corporate firewall. Clients outside the network connect directly to DMZ*edge*.



Cornerstone services these connections by dynamically opening an outbound port to the DMZ*edge*. Cornerstone submits requests to DMZ*edge*, which may then respond.

DMZ*edge* server works as a pass-through only; data is never stored on it and only exists within the corporate firewall. When used in conjunction with on-the-fly PGP encryption, Cornerstone and DMZ*edge* provide the highest levels of security for your stored data.

Contact Information:
South River Technologies, Inc.
Email: sales@southrivertech.com
Toll-Free: 1-866-861-9483
Main: 443-603-0290
Fax: 410-266-1191