



Mapping PCI Data Security Standard Requirements against the Reliant MPS Redbox

The Reliant MPS Redbox can help bring a Retailer’s payment card environment into compliance with all twelve of the PCI Data Security Standards high level requirements.

PCI Requirement	Supported (Y/N)	Description
1. Install and maintain a firewall configuration to protect data	Y	Inherent to the MPS Architecture. The Redbox provides a multiport firewall as part of the solution to provide network access control and network segmentation. Additionally, the architecture provides a means to automate the validation of firewall rules on all Redbox systems.
2. Do not use vendor-supplied defaults for system passwords and other security parameters	Y	Inherent to the MPS Architecture. MPS platforms have been standardized and hardened to prevent unauthorized access and are monitored centrally to ensure ongoing system integrity. Additionally, the MPS monitors configurations of POS, application files and other systems to demonstrate that hardened configurations remain in place and detect any unauthorized changes.
3. Protect stored data	Y	Cardholder data is not stored in the Reliant solution, but the solution can be extended to support features such as encryption key management depending on the POS system requirements and features of the environment.
4. Encrypt transmission of cardholder data and sensitive information across public networks	Y	Inherent to the MPS Architecture. Encrypts transmission of cardholder data over untrusted networks and non-cardholder data environments through an industry standard VPN that terminates at the merchant headquarters location.
5. Use and regularly update anti-virus software	Y	All MPS components include Anti-Virus Software. The system supports use of third-party AV solutions for Windows or Linux POS hosts.
6. Develop and maintain secure systems and applications	Y	Inherent to the MPS Architecture. Supports System Development Lifecycle requirements through central management console for remote Redboxes. Changes, which range from simple patches to the addition of entirely new features, are controlled centrally and propagate across the Redbox network without the need for any remote hands support. Additionally, the system supports use of third-party configuration control solutions such as Microsoft’s Active Directory.
7. Restrict access to data by business need-to-know	Y	Inherent to the MPS Architecture. Access control implementation is flexible depending on environment characteristics. Supports PCI requirement for “separation of duties” and for secure non-console administrative access with two-factor authentication. Additionally, the system supports use of third-party access control solutions such as Microsoft’s Active Directory.
8. Assign a unique ID to each person with computer access	Y	Inherent to the MPS Architecture. See item 7 above.
9. Restrict physical access to cardholder data	Y	Small form factor of MPS appliance allows it to be easily secured in a manager’s back office or small telecommunications closet
10. Track and monitor all access to network resources and cardholder data	Y	Inherent to the MPS Architecture. The system automates log collection and aggregation at both store and central locations. Logs are collected from a variety of systems including POS and back-office servers. MPS provides flexible log reporting and alerts on specified events.
11. Regularly test security systems and processes	Y	Inherent to the MPS Architecture using a variety of technical controls, including: <ul style="list-style-type: none"> • Network-based alerts can be forwarded via email or the MPS log server • File Integrity Monitoring of POS and backoffice systems including daily comparison of critical windows system files • Vulnerability Scanning is supported to meet the PCI requirement for quarterly scans of internal systems. • Rogue Access Point Detection is supported in a manner consistent with recent guidance from the PCI Standards Council Special Interest Group for Wireless Security.
12. Maintain a policy that addresses information security	Y	Documentation of compliance is central to the solution. Reliant provides a thorough description of all controls provided by the MPS system in its MPS Auditor’s Guide. The guide has met stringent requirements for PCI documentation by passing several Level 1 PCI audits.