How Reflection Software Facilitates PCI DSS Compliance

How Reflection Software Facilitates PCI DSS Compliance

In 2004, the major credit card companies—including Visa, MasterCard, and American Express—joined forces to create the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS applies to all companies that store, process, or transmit cardholder account data. Its purpose: to ensure data privacy for consumers via strict security controls across the industry.

A series of compliance deadlines have sent organizations scrambling to meet the 12 broad PCI DSS requirements. These requirements range from being relatively easy to implement, such as ensuring up-to-date anti-virus software, to complex and demanding, such as tracking access to network resources and cardholder data.

This white paper tells how Micro Focus® Reflection® terminal emulators, file transfer utilities, and SSH clients and servers can help you achieve PCI DSS compliance. By the time you're done reading, you'll know which Reflection products can help you address specific PCI requirements—and how they do it. You'll also see that Reflection enables compliance beyond terminal emulation and file transfer into areas you may not have considered before.

The 12 PCI Requirements

The PCI DSS consists of 12 requirements designed to help ensure that cardholder data is secure and that the network and systems handling the data are well protected. The 12 requirements fall into the groups listed in Figure 1.

How Reflection Handles Your Host-Centric Security Issues

To help you understand how Reflection products can facilitate PCI compliance, this section summarizes key host-centric security issues and describes how Reflection products address them.

Build and Maintain a Secure Network

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. Use and regularly update anti-virus software.
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. Assign a unique ID to each person with computer access.
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.

Figure 1: The 12 broad PCI DSS requirements. Reflection products facilitate compliance with requirements 1, 2, 4, 6, 7, 8, and 10.

Security for Servers

Host systems store cardholder data and run applications that enable access to that data. Host systems may also be file servers holding cardholder data in files that need to be transferred over public networks. Due to the sensitive nature of the data, organizations need to restrict access to this data and encrypt it as it travels over the network.

Reflection solution: Reflection for Secure IT is a family of Secure Shell clients and servers for Windows and UNIX. With Reflection for Secure IT servers, you can build secure, encrypted tunnels for data in motion—including communications from client-based emulators, file transfer utilities, or any application that uses the TCP/IP protocol.

Reflection for Secure IT also performs another critical security function—tracking access, including access with administrator privileges, to system components. By enabling the configuration of audit logging, Reflection for Secure IT delivers key information (who accessed the system through the SSH server and when) to standard logging facilities on the host system.

Security for Workstations

Users and system administrators frequently rely on client-based utilities for accessing host applications and files. The user IDs and passwords used to gain access to host systems, as well as the sensitive information passing between the workstation and the host system, all need protection from prying eyes while in transit.

Reflection solution: Reflection for Windows and Reflection for the Web terminal emulators support a variety of encryption technologies (including SSH and SSL/TLS) and authentication methods (such as Kerberos) that match the capabilities enabled on the host system. With this support, security officers can feel confident that both user account credentials (such as passwords) and sensitive information (such as cardholder data) will be encrypted as they pass between the host and the terminal emulation screen.
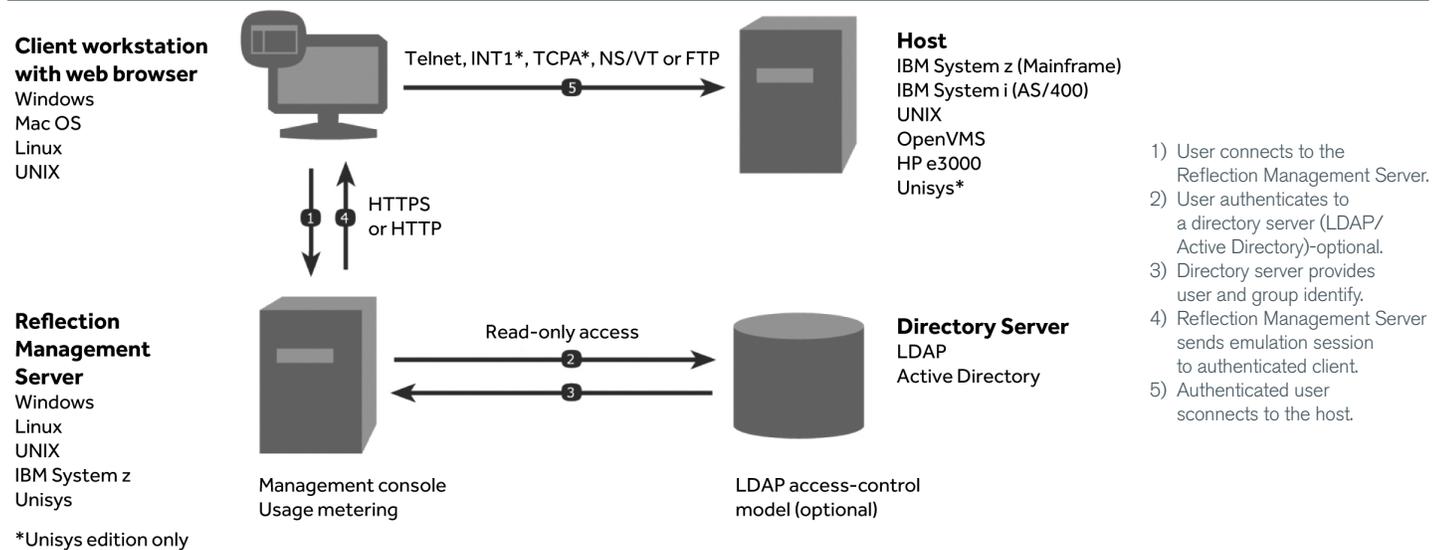
Reflection Secure FTP clients, included with the Reflection emulation products, also support a variety of encryption technologies and authentication methods. These technologies and methods help to ensure that files containing sensitive information cannot be accessed by unauthorized users and are encrypted before they enter the network.

Security for System Access

Client terminal emulators provide access to private host data—which means access to emulation sessions must be tightly controlled.

Reflection solution: Reflection for the Web provides authentication and access control that leverages existing user directories (such as Active Directory). Users cannot access emulation sessions unless they have been approved by an administrator.

Specific session configurations can be assigned to users and groups within a domain. These sessions are launched through links on a protected web page or portal. When users access the page, they are authenticated against the user directory and granted access only to pre-designated host sessions.

Client workstation with web browser
Windows
Mac OS
Linux
UNIX

Telnet, INT1*, TCPA*, NS/VT or FTP
⑤

HTTPS
or HTTP
① ④

Host
IBM System z (Mainframe)
IBM System i (AS/400)
UNIX
OpenVMS
HP e3000
Unisys*

Reflection Management Server
Windows
Linux
UNIX
IBM System z
Unisys

*Unisys edition only

Management console
Usage metering

Read-only access
②
③

Directory Server
LDAP
Active Directory

LDAP access-control model (optional)

1) User connects to the Reflection Management Server.
2) User authenticates to a directory server (LDAP/Active Directory)-optional.
3) Directory server provides user and group identify.
4) Reflection Management Server sends emulation session to authenticated client.
5) Authenticated user sconnects to the host.

The Reflection Road to Compliance

This section explains how Reflection can help you meet PCI DSS requirements 1, 2, 4, 6, 7, 8, and 10.

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

Section 1.1 of the PCI DSS documentation specifies that certain protocols—including Secure Sockets Layer (SSL) and Secure Shell (SSH)—may pass through the firewall without special justification or documentation. But protocols such as FTP, which are considered risky, require justification and documentation to be allowed through the firewall.

Section 1.2 specifies that firewalls must be configured to deny all traffic—except for protocols required by the cardholder data environment—from untrusted networks.

Here's how Reflection products facilitate compliance with Requirement 1:

REFLECTION FOR WINDOWS

All Reflection for Windows products support encryption of the terminal data stream using acceptable secure protocols, including SSH and SSL/TLS.

REFLECTION SECURE FTP

The Reflection Secure FTP utility supports standard FTP, SFTP, and FTP/S client functionality over acceptable secure protocols, including SSH and SSL/TLS.

REFLECTION FOR THE WEB

Reflection for the Web supports encryption of the terminal data stream using acceptable secure protocols, including SSH and SSL/ TLS.

In addition, Reflection for the Web includes the Reflection Security Proxy, which enables firewall-friendly host access. Hosts are hidden behind the firewall and proxy, and multiple hosts can be accessed through a single open port in the firewall.

REFLECTION FOR SECURE IT

The SSH servers in Reflection for Secure IT provide the server-side mechanism for supporting SSH connectivity from Reflection terminal emulation and file transfer clients.

Requirement 2: Do Not Use Vendor Supplied Defaults for System Passwords and Other Security Parameters

Section 2.3 requires that all non-console administrative access to key systems be encrypted. SSH and SSL/TLS are listed as acceptable protocols.

Here's how Reflection products facilitate compliance with Requirement 2:

REFLECTION FOR WINDOWS

Reflection for Windows products can be used for non-console administrative access to host systems. All support encryption of the terminal data stream using acceptable secure protocols, including SSH and SSL/TLS.

REFLECTION FOR THE WEB

Reflection for the Web supports encryption of the terminal data stream using acceptable secure protocols, including SSH and SSL/TLS.

The Reflection Security Proxy also provides encrypted connections to host systems, such as Unisys, that lack native encryption support.

REFLECTION FOR SECURE IT

Reflection for Secure IT Secure Shell clients offer utilities for interactive and scripted remote administration tasks over the SSH protocol.

The SSH servers in Reflection for Secure IT provide the server-side mechanism for supporting SSH connectivity from Reflection terminal emulation clients.

Requirement 3: Protect Stored Cardholder Data

Section 3.3 stipulates that primary account numbers (PANs) should be masked when displayed.

Here's how Reflection Desktop, a Windows-based terminal emulator, facilitates compliance with Requirement 3:

REFLECTION DESKTOP

Reflection Desktop includes a configurable privacy filters feature that can mask PANs displayed in history windows, printed reports, and clipboards.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Requirement 4 stipulates that "sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit." Section 4.1 goes on to specify that strong cryptography and security protocols be used to safeguard sensitive cardholder data in transit.

Here's how Reflection products facilitate compliance with Requirement 4:

ALL REFLECTION PRODUCTS

All implementations of the SSH and SSL/TLS protocols in Reflection products use strong cryptography— including Triple DES and AES algorithms—to encrypt cardholder data sent over the network. In most cases, these cryptographic implementations have been FIPS 140-2-validated by an accredited third party.

Requirement 6: Develop and Maintain Secure Systems and Applications

PCI DSS section 6.1 requires you to install the latest vendor-supplied security patches within one month of their release.

To keep up with the rapidly evolving landscape of security threats, you need to partner with a vendor that monitors the leading security alert services and notifies you of relevant security vulnerabilities.

Our security experts maintain a series of technical notes, available on our support site, that describe published security vulnerabilities. Customers with Maintenance can download the appropriate security patches. Our technical support team is also available to help you deal with any security issues that arise in our products.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

This requirement mandates that only users whose job requires access to cardholder data be granted that access, and that the default configuration for users, unless otherwise allowed, be set to "deny all."

Here's how Reflection for the Web facilitates compliance with Requirement 7:

REFLECTION FOR THE WEB

All host systems offer some level of authorization and access control. You can add an additional layer of security with Reflection for the Web, which lets you control the utilities, such as terminal emulators and file transfer utilities, that access your hosts.

Here's how it works: Users are required to sign onto a website that provides links to terminal emulation and file transfer sessions. Authentication and access sessions can be managed through your existing access control directory (e.g., Active Directory). You can control access at the user or group level. The default setting in Reflection for the Web will deny access to unauthorized users.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Falling under the objective of "implement strong access control," this requirement specifies that users must identify themselves prior to receiving access to cardholder data. It also specifies support for a variety of authentication methodologies and the use of two-factor authentication for remote access.

Here's how Reflection for the Web facilitates compliance with Requirement 8:

REFLECTION FOR THE WEB

By putting an authentication and authorization layer in front of access to terminal emulation and file transfer utilities, Reflection for the Web allows the unique IDs assigned within an existing user directory to be used for access control.

In addition to password-based authentication, Reflection for the Web also supports digital certificates and public keys for authentication.

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

Logging mechanisms and the ability to track user activities are critical to PCI DSS compliance. Requirement 10 governs which events get logged for the purposes of auditing and which specific data points get captured in the logged event.

Here's how Reflection products facilitate compliance with Requirement 10:

REFLECTION FOR SECURE IT

As a provider of server-based Secure Shell services, Reflection for Secure IT offers robust logging capabilities. Key events in the operation of Reflection for Secure IT servers, including incoming client connections and authentications, are logged to a variety of configurable systems, including standard operating system event logs.

REFLECTION FOR THE WEB

During terminal emulation and file transfer sessions, Reflection for the Web logs incoming access events and details about the host systems to which users are connecting.

REFLECTION FOR SECURE IT

Reflection for Secure IT Secure Shell clients offer utilities for interactive and scripted remote administration tasks over the SSH protocol.

The SSH servers in Reflection for Secure IT provide the server-side mechanism for supporting SSH connectivity from Reflection terminal emulation clients.

More Capabilities, Faster Compliance

Meeting the wide range of PCI DSS requirements isn't easy. Implementation may cross departmental boundaries, involve several teams, and affect multiple system platforms. The effort involved can be both time consuming and expensive.

Unfortunately, no single security solution can meet all of your PCI compliance needs. But Reflection products, which offer more PCI compliance capabilities than any other terminal emulation solution, can provide a broad base of support. With tools that reside on both servers and user workstations, Reflection products are built to reduce your time to compliance and support safer information sharing.

And here's more good news: Once you've successfully met your PCI requirements, your organization will be well down the path towards compliance with other, newer regulations.

About Micro Focus

Since 1976, Micro Focus has helped more than 20,000 customers unlock the value of their business logic by creating enabling solutions that bridge the gap from well-established technologies to modern functionality. The two portfolios work to a single, clear vision—to deliver innovative products supported by exceptional customer service. **www.microfocus.com**

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Seattle, Washington
206 217 7100
800 872 2829

Additional contact information and office locations:
www.attachmate.com

MICRO® **FOCUS**