

PCI DSS Compliance

Solution Brief

Attacks on credit card and payment systems are rampant. Only recently have organizations begun to realize that their credit card processing systems were an enticing target for cyber criminals. Now attacks have become systematized, and are so aggressive that every organization that handles credit card information must take extraordinary care to protect that data from theft. The seminal 2009 Data Breach Investigation Report published by Verizon itemized the level of those attacks. 38% used custom malware that would avoid detection by standard anti-virus products. 91% of the stolen records in 2008 can be attributed to organized crime according to the report and 34% of the attacks came through partners. While the payment industry has attempted to enforce minimum standards of protection for credit card processors 81% of the victims Verizon investigated were not PCI compliant. Aberdeen Group found that on average, only 53% of organizations sensitive data is adequately protected from insider abuse.

by Richard Stienon
Chief Research Analyst, IT-Harvest

Compliance with PCI DSS was mandated by December, 2007. Organizations that fail to comply face fines of up to \$500,000 if the data is lost or stolen and risk not being allowed to handle cardholder data. According to the Privacy Rights Clearinghouse, between January 2005 and August 2007, more than 159 million records containing sensitive personal information have been involved in security breaches.

The Payment Card Industry is capable of removing or restricting a company's right to process credit card payments. One such action led to the dissolution and sale of a large payment processor, Card Services International.



As companies are faced with repercussions that include liabilities that exceed any punitive actions from the Payment Card Industry there are additional measures that should be deployed. First and foremost it is imperative that access to data by high risk users be strictly controlled (PCI DSS sections 7 and 8). This includes partners, contractors, vendors, and trusted insiders. Insiders may be database analysts, developers, system administrators, perhaps even remote store managers.

2009 Data Breach Investigation Report

38% of attacks used custom malware that would avoid detection by standard anti-virus products.

91% of the stolen records in 2008 can be attributed to organized crime

34% of the attacks came through partners

81% of the victims were not PCI compliant

53% of an organizations sensitive data is adequately protected from insider abuse

Control Objectives	PCI DSS Requirements	Xceedium
Build and Maintain a Secure Network	Do not use vendor supplied defaults for system passwords and other security parameters (Req 2)	GateKeeper prevents default password use
Protect Cardholder Data	Encrypt transmission of cardholder data across open public networks (Req 4)	All GateKeeper sessions are encrypted using SSL/TLS.
Implement Strong Access Control Measures	Restrict access to cardholder data by business need-to-know (Req 7) Assign unique ID to each person with computer access (Req 8)	Xceedium GateKeeper enforces granular access control by role, group and individual. GateKeeper tracks and controls users by unique IDs and their source IP addresses.
Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data (Req 10)	GateKeeper has event tracking and auditing as well as full session recording for graphical and command line sessions.
Maintain an Information Security Policy	Create and update a policy that addresses information security (Req 12)	Xceedium allows the creation, enforcement, change, auditing and reporting of information security policy.

Xceedium GateKeeper

Xceedium's GateKeeper appliance offers an easy to deploy solution for controlling access to critical systems that fall within the domain of PCI DSS. It has a small footprint in that it resides between those critical systems and high risk users. With the Xceedium GateKeeper deployed these high-risk privileged users log in to the GateKeeper with unique credentials that are bound to the identity of the individual and completely integrated with existing authentication and directory systems. Based on identity each account is limited to only specific back-end resources and applications and, at a granular level, only explicitly defined actions.

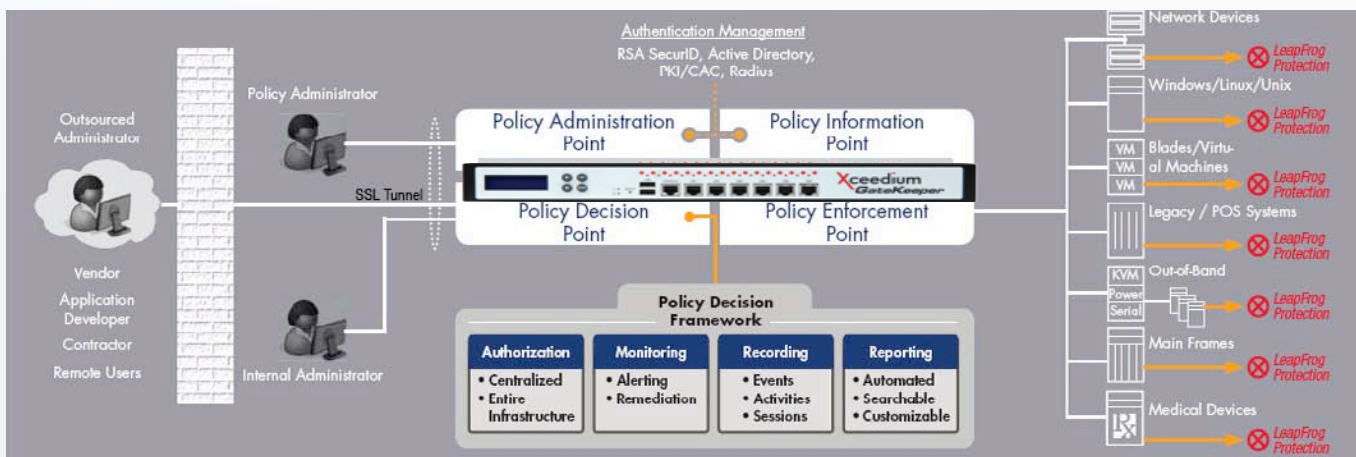
The Xceedium GateKeeper is an effective containment solution that restricts access to just those resources that are required for each individual to accomplish their job. Complete continuous recording of every session provides an audit trail and can be quickly output in formatted audit reports tailored to PCI DSS compliance. Individual sessions also can be searched for information and played back from any point in time.

Access to these systems must be strictly controlled, contained to authorized areas, and all activity must be logged; and ultimately, an audit trail must be in place. Xceedium's GateKeeper provides this functionality in a hardened appliance that can be deployed in front of these critical systems.

Of the key features of the Xceedium GateKeeper one to note is the ease of deployment with a zero-footprint restrictive access methodology to control all access to internal systems be they network infrastructure devices or specific applications running on particular servers. This zero footprint access model allows organizations to adhere to PCI mandates even when dealing with users who access systems from unmanaged endpoints, such as vendors, outsourced personnel and other third parties.

The Xceedium GateKeeper appliances deployed at each data center location provide the centralized control, tracking of activity, and audit reports that allow a credit card handling organization to impose measures that ensure they are in compliance with PCI requirements.

“attacks have become systematized, and are so aggressive that every organization that handles credit card information must take extraordinary care to protect that data from theft.”



Key Features

- Controls access with a secure appliance-based platform for high-risk users
- Centrally defines policy and controls access via a single point of ingress
- Creates a secure, zero-footprint channel for accessing all components of the IT infrastructure
- Compartmentalizes and contains activities of high-risk users (LeapFrog Prevention™)
- Monitors and alerts about violations in real time
- Remediates by terminating access for the offending party
- Centrally records all activities in every session
- Easily creates compliance reports for testing of controls

Benefits

- Lowers cost of controlling and auditing high risk users
- A single control and management point requires less administrative resources
- Fast and effective deployment
- Enforces best practices for access control
- High-risk user monitoring in existing alerting and operations infrastructure
- Enforces policy in an overlay structure Leverages existing solutions
- Makes auditing user activity and meeting compliance not only easy but possible
- Provides an end-to-end audit trail ensuring accountability

Certifications

- FIPS 140-2 Level 2
- JITC PKI/CAC
- CC-EAL2, CC-EAL3, CC-EAL4 (In process)

CLI

- Telnet, Serial
- Secure Shell (SSH)
- Graphical Session Recording

Supported GUIs

- Windows, Mac, X-Windows
- HTTP, Citrix, VNC, IP KVM
- Terminal Services / RDP with Session Recording