Table of Contents

PCI Compliance Overview.............................................................................................................................3
Introduction .............................................................................................................................................3
The Importance of PCI DSS.......................................................................................................................3
PCI DSS Requirements .............................................................................................................................4
Enabling PCI Compliance with Radware APSolute® Solutions.................................................................4
  Radware APSolute™ Product Suite Overview.......................................................................................4
    AppDirector® .........................................................................................................................................4
    AppWall® ..............................................................................................................................................4
    AppXML® ............................................................................................................................................5
    DefensePro® .........................................................................................................................................5
    Inflight™ .............................................................................................................................................5
    LinkProof® .........................................................................................................................................5
Detailed Compliance Matrix.......................................................................................................................5
Appendix ....................................................................................................................................................10
  PCI Requirements and Security Assessment Procedures............................................................................10
  Build and Maintain a Secure Network.......................................................................................................10
  Protect Cardholder Data ..........................................................................................................................11
  Maintain a Vulnerability Management Program ........................................................................................11
  Regularly Monitor and Test Networks.......................................................................................................12
  Maintain an Information Security Policy ....................................................................................................13
PCI Compliance Overview

Introduction
The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by the major credit card companies as a guideline to help businesses that process card payments prevent credit card fraud, electronic break-in, and various other security vulnerabilities and threats. Any credit card merchant or service provider processing, storing, or transmitting payment card data must be PCI DSS compliant. The penalties for non-compliance range from the imposition of large fines up to losing the authorization to process credit card payments. Compliance can come at a hefty price tag for most of these businesses as they seek to incorporate the required security measures within their organizations and networks.

The Importance of PCI DSS
The driving force behind the effort to secure all credit card data is the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. The founding payment brands established the independent policy body in the face of mounting governmental legislation, rising consumer loss from identity theft and fraud, and the ever-increasing sophistication of techniques and ploys employed by the latest generation of hackers. The collaborative council mandated that businesses meet specific security requirements designed to protect card holder data by a December 31, 2007 deadline.

To foster compliance, the card associations have offered both incentives and penalties. As an incentive, merchants are offered protection from PCI related fines, which can be as high as $500,000 per incident, if they are compliant at the time of the breach. This is what is known in the industry as “safe harbor.” Merchants that are not compliant at the time of breach do not receive immunity from the levy of incident-related fines and may in fact face additional monetary penalties if generally found in non-compliance. Some card brands have threatened to levy increased fines against larger merchants, up to $25,000 per month, until they achieve compliance.

Achieving compliance is a costly matter for these businesses involving certifications by quality security assessors (QSAs), the implementation of various security technologies within and without the network, and the addition of trained staff for maintaining and monitoring related processes and infrastructure.

Why is Addressing PCI Compliance Important Today?
Compliance is mandated by the payment card brands and not by the PCI Security Standards Council. However, for most merchants, the deadlines for validating compliance with the PCI DSS have already passed. Furthermore, starting June 30, 2008, PCI DSS 1.1 section 6.6 is now a major requirement in many countries across the globe.
PCI DSS Requirements

Businesses must implement the following six categories of security principles in order to be compliant with the PCI standard:

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

Detailed requirements associated with the above principles are available for review in the Payment Card Industry (PCI) Data Security Standard (DSS) version 1.2 published October 2008 at https://www.pcisecuritystandards.org/.

PCI Requirements and Security Assessment Procedures are discussed in the Appendix of this document.

Enabling PCI Compliance with Radware APSolute™ Solutions

Radware APSolute® Product Suite Overview
This section provides an overview on Radware’s products that enable PCI Compliance as part of Radware APSolute™ Product Suite

AppDirector®
AppDirector is an intelligent application delivery controller (ADC) which enhances the delivery of applications over IP networks by ensuring the full availability, maximum performance and complete security of your business-critical applications, at all times. By optimizing server infrastructure resources and enabling seamless consolidation and high scalability, AppDirector drives productivity and creates faster Return on Investment (ROI). AppDirector provides application acceleration features, such as web compression, secure socket layer (SSL) offloading, TCP optimization, and caching for the fastest application and transaction response times.

AppWall®
AppWall is a Web Application Firewall (WAF) appliance which secures Web applications and enables PCI compliance by mitigating Web application security threats to prevent data theft and manipulation of sensitive corporate and customer information. AppWall incorporates advanced, patent-protected Web application security filtering technologies to seamlessly detect threats, block attacks and report events. AppWall improves the security and availability of business-critical Web applications and creates a higher return on investment (ROI) for Web-based applications.
**AppXML®**

AppXML is a comprehensive Web services Security Gateway that functions as a trusted intermediary for exchanging secure Web Services between an enterprise and its business partners. In addition, by enabling interoperability with existing Identify Management systems in the organization, it enables enterprises to achieve a higher ROI through secure, efficient e-business process integration. The AppXML appliance combines hardware and software to improve the speed of XML document processing and secure XML-based and Web Services communications.

**DefensePro®**

DefensePro is a real-time intrusion prevention system (IPS) and DoS-protection device that maintains business continuity by protecting applications against known attacks and emerging network attacks such as: non-vulnerability based attacks that misuse the application, zero-minute attacks, SSL attacks and VoIP service misuse – all without blocking legitimate user traffic and with no need for human intervention.

**Inflight™**

Inflight is an out-of-path, network-based pervasive monitoring appliance which captures all user transactions from “in-flight” network traffic and delivers real-time events for business applications. With real-time business events, companies can identify business activity embedded in Web transactions and respond instantaneously, while enabling their networks to intelligently manage resources based on user and business requirements.

**LinkProof®**

LinkProof is the industry leading multi-WAN load balancing solution ensuring connectivity to the Internet and intranets through multiple ISPs, using diverse transport technologies including DSL, VPN, cable, metro Ethernet, etc., minimizing any connectivity loss due to service failure.

## Detailed Compliance Matrix

The following table outlines the twelve PCI DSS 1.2 requirements, details how Radware’s solutions and products address each requirement and their business value for customers. Specific PCI compliance sections that are addressed are noted where appropriate.

Note: To view the detailed PCI DSS requirement description, click the link of each requirement.

<table>
<thead>
<tr>
<th>Compliance Category</th>
<th>PCI DSS Requirement</th>
<th>Enabling PCI Compliance with Radware</th>
</tr>
</thead>
</table>
| Build and Maintain a Secure Network | Requirement 1: Install and maintain a firewall configuration to protect cardholder data | - AppDirector  
  » Only traffic that complies with user defined policies (Layers 3 through 7) is routed to its destination, thus inbound and outbound traffic is restricted to that which is necessary for the cardholder data environment (PCI section 1.2.1).  
  » Specific Virtual IPs (VIPs) for the DMZ environment are defined to ensure that inbound Internet traffic is limited to IP addresses within the DMZ (PCI section 1.3.2).  
  » The NAT capability provides IP masquerading to prevent internal addresses from being translated and revealed on the Internet (PCI section 1.3.8)  
  » The Segmentation capability ensures that inbound and outbound traffic from and to the DMZ and the cardholder data environment always passes through a firewall. |
<table>
<thead>
<tr>
<th>Compliance Category</th>
<th>PCI DSS Requirement</th>
<th>Enabling PCI Compliance with Radware</th>
</tr>
</thead>
</table>
| Build and Maintain a Secure Network                     | Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters | ・DefensePro  
  » Applies signature protection with an eCommerce profile to send an alert when default passwords as used (such as “public” community).  
  » Create user-defined signatures to send an alert when vendor-specific default passwords are used by the systems at your site.  
  ・Inflight  
  » Monitors all HTTP/S management traffic for user names and passwords. The solution can send an alert for any combination of user names and passwords that are suspected as defaults.  
  ・All products  
  » All Radware’s products include secure management consoles, enabling administrators to modify the default security settings, including system passwords, SNMP password and SSL related passwords. |
| Protect Cardholder Data                                  | Requirement 3: Protect stored cardholder data             | ・AppWall, AppXML:  
  » Mask cardholder data in all Web transactions (AppWall) and Web services transactions (AppXML) to ensure that:  
    o Cardholder data traversing through the organization LAN is protected and is not exposed to any system component or any user inside the organization’s LAN  
    o All outbound traffic does not contain any un-protected cardholder data (all sensitive cardholder data is masked before it is sent to the public network)  
  » The above capabilities, in combination with Requirement 4, ensure a fully-secured path between the organization data center and the end-user  
  ・Inflight  
  » Process sensitive business events and mask all sensitive data before sending the processed data |
| Protect Cardholder Data                                  | Requirement 4: Encrypt transmission of cardholder data across open, public networks | ・AppDirector  
  » SSL- encrypts transactions before sending them to the public network.  
  » Employs strong cryptographic keys.  
  » Enables storing certificates in one central place instead of all individual servers.  
  » Central certificates management decreases the need to manage and secure each individual server certificate.  
  » Transactions that are not validated on AppDirector do not reach the Web servers and applications, reducing security risks.  
  ・DefensePro & AppXcel:  
  » Apply SSL-based attack protection to prevent encrypted attacks from bypassing inspection by network security tools. |
<table>
<thead>
<tr>
<th>Compliance Category</th>
<th>PCI DSS Requirement</th>
<th>Enabling PCI Compliance with Radware</th>
</tr>
</thead>
</table>
| Maintain a Vulnerability Management Program             | Requirement 5: Use and regularly update anti-virus software or programs | • DefensePro  
  » The automatic attack signature database update ensures the most up-to-date coverage against attacks that exploit known application and operating system vulnerabilities.  
  » Zero-minute attacks protection prevents self propagating malware spread activity. A zero-minute attack exploits an application or OS vulnerability for which a signature or a software patch does not exist or has not been applied yet. This helps you consolidate and plan your patch management. |
| Maintain a Vulnerability Management Program             | Requirement 6: Develop and maintain secure systems and applications | • AppWall  
  » AppWall is a Web application firewall installed in front of public-facing Web applications as required by PCI section 6.6.  
  » Addresses all the Web application development guidelines as defined in section 6.5 of the PCI document  
  » Protects against the OWASP Top Ten vulnerabilities in Web Application security.  
  » Addresses new threats and vulnerabilities on an on-going basis and ensures these applications are protected against known attacks.  
  » Protects against WASC Web Security Attack classification.  
  » Out-of-the-box security policies based on negative security model addressing a wide range of security threats.  
  » Positive security model delivering automatic applications learning capability for maximal security protection without intervention.  
  » Highly granular policy control based on the application path.  
  
**Note:** For an in-depth discussion on how Radware AppWall addresses PCI DSS 1.2 sections 6.5 and 6.6, please refer to the AppWall White Paper.  
  
• AppXML  
  » Protects business applications against XML and Web Services-specific security risks. |
## Implement Strong Access Control Measures

<table>
<thead>
<tr>
<th>Compliance Category</th>
<th>PCI DSS Requirement</th>
<th>Enabling PCI Compliance with Radware</th>
</tr>
</thead>
</table>
| Implement Strong Access Control Measures | Requirement 7: Restrict access to cardholder data by business need to know | • DefensePro  
  » Applies server cracking protection (brute force attack protection and application scans prevention) to prevent username/password cracking attacks and discovery of Web application vulnerabilities that can be used to attack web servers.  
  » Implements access control rules to limit and control access to sensitive services and data.  
• AppXML  
  » Provides policy based access control for Web Services ensuring that only authorized users can access specific Web Services.  
  » Manages WSDL exposure. Exposes different parts of WSDL according to user business need to know.  
• AppDirector  
  » Controls traffic redirection and access to different services according to Layer 3-7 policies. Prevents un-authorized users from accessing applications.  
• Inflight  
  » Tracks and audits any user access to Web-based applications.  
  » Sends, in real-time, this information to a third-party analytic system to perform a real-time analysis of users behavior and alert on any breech in policy. |
| Implement Strong Access Control Measures | Requirement 8: Assign a unique ID to each person with computer access. | • AppDirector  
  » Enables the insertion of a unique ID to each user and tracks this ID, ensuring that each user is directed to the same server where he/she has been authenticated.  
  » Reduces transactions to several servers but only to the original servers which addressed the initial request,  
• Inflight  
  » Monitors and correlates between each Web transaction and the individual user who performed the transaction, ensuring that each individual is uniquely accountable for his or her actions as required by this PCI requirement.  
  » Enables an organization to track the entire user web session according to each user unique ID.  
• All products  
  » Radware’s products include user authentication and password management capabilities. All actions related to users’ credentials are audited and controlled. |
<table>
<thead>
<tr>
<th>Compliance Category</th>
<th>PCI DSS Requirement</th>
<th>Enabling PCI Compliance with Radware</th>
</tr>
</thead>
</table>
| Regularly Monitor and Test Networks | **Requirement 10:** Track and monitor all access to network resources and cardholder data. | • **Inflight**  
» Monitors all access (that is based on HTTP/S) to any system component and links it to the individual user who accessed the system component (PCI section 10.1).  
» By monitoring all HTTP/S traffic from and to all system components, Inflight can create a detailed audit trail providing organizations with the ability to reconstruct all the individual user activities (PCI section 10.2). For example, the detailed audit trail can provide information about all individual user access to cardholder data (PCI section 10.2.1) as well as all actions taken by any individual with root administrator privilege (PCI section 10.2.2).  
» Inflight can create a detailed audit record per each user transaction including all trail entries as required by section 10.3.  
» Inflight aggregates all the Web related auditing tasks to a central location, preventing the need to synchronize the clock and times of all the separate system components that Inflight monitors. Inflight internal clock synchronization mechanism ensures its internal clock is always in synch with the organization’s NTP server (PCI section 10.4).  
» Inflight does not store logs internally but rather sends all log entries to a third-party analytic system ensuring that log trails can not be alerted (PCI section 10.5).  
• **DefensePro**  
» Real-time monitoring including the Security Event Dashboard, Top Scan activity Dashboard, network behavioral monitoring, Web server behavioral monitoring and log view. The behavioral monitoring tools help to identify normal versus abnormal use (anomalies) of network and application resources.  
» Uses the Top attack sources report to monitor unauthorized access to network resources and cardholder data.  
• **AppXML**  
» Tracks and monitors all user access to the different Web Services offered by the organization.  
• **LinkProof**  
» Audits all traffic flows in the data center network. |
<table>
<thead>
<tr>
<th>Compliance Category</th>
<th>PCI DSS Requirement</th>
<th>Enabling PCI Compliance with Radware</th>
</tr>
</thead>
</table>
| Regularly Monitor and Test Networks | Requirement 11: Regularly test security systems and processes. | • DefensePro  
  » Proactively detects and prevents not only known vulnerabilities, but also emerging attacks for which no security patch or signature exists, such as non-vulnerability attacks that misuse the application resources and zero-minute attacks for which an attack signature does not exist yet.  
  » DefensePro is a self-learning and self-adapting system that creates baselines of normal network bandwidth, server traffic and user behavior. It detects automatically abnormal network, server, and user patterns and mitigates attacks in real time.  
  » The Automatic Signature data base update ensures the most up-to-date coverage.  
  **Note:** Section 11.4 requires using the intrusion prevention system to monitor all traffic and send an alert about suspected compromises. |
| Maintain an Information Security Policy | Requirement 12: Maintain a policy that addresses information security for employees and contractors. | • DefensePro  
  » Easy to use management system allows you to create and maintain a suitable security policy to each part of your network.  
  » Highest port density in the industry allows you to manage up to 8 physical segments with the same device, allow you to create global policies and segment specific policies, providing better control, manageability and relevancy.  
  • AppDirector  
  » Defines and enforces Layers 3 through 7 related policies in order to ensure that users are only redirected to permitted server farms.  
  » Blocks specific users from accessing non-permitted applications. |

**Appendix**

**PCI Requirements and Security Assessment Procedures**

The following section describes each PCI requirement in details. The requirements information is quoted from the original PCI DSI 1.2 document at [https://www.pcisecuritystandards.org/](https://www.pcisecuritystandards.org/).  

**Build and Maintain a Secure Network**

**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

Firewalls are computer devices that control computer traffic allowed between a company’s network (internal) and un-trusted networks (external), as well as traffic into and out of more sensitive areas within a company’s internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees’ Internet access through desktop browsers, employees’ e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources.
Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

The following sub-sections are specifically referred in the document:

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.
1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).

**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**
Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

**Protect Cardholder Data**

**Requirement 3: Protect stored cardholder data**
Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

**Requirement 4: Encrypt transmission of cardholder data across open, public networks**
Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

**Maintain a Vulnerability Management Program**

**Requirement 5: Use and regularly update anti-virus software or programs**
Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business approved activities including employees’ e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

**Requirement 6: Develop and maintain secure systems and applications**
Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.
The following sub-sections are specifically mentioned in the document:

6.5: Develop all Web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following [OWASP requirements]

6.6: For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:
- Reviewing public-facing Web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes
- Installing a Web-application firewall in front of public-facing Web applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know
To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Requirement 8: Assign a unique ID to each person with computer access.
Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Requirement 9: Restrict physical access to cardholder data.
Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.
Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs

The following sub-sections are specifically referred in the document:

10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

10.2 Implement automated audit trails for all system components to reconstruct the following events:
- 10.2.1 All individual accesses to cardholder data
- 10.2.2 All actions taken by any individual with root or administrative privileges
- 10.2.3 Access to all audit trails
- 10.2.4 Invalid logical access attempts
- 10.2.5 Use of identification and authentication mechanisms
- 10.2.6 Initialization of the audit logs
- 10.2.7 Creation and deletion of system-level objects
10.3 Record at least the following audit trail entries for all system components for each event:
10.3.1 User identification
10.3.2 Type of event
10.3.3 Date and time
10.3.4 Success or failure indication
10.3.5 Origination of event entries.
10.3.6 Identity or name of affected data, system component, or resource

10.4 Synchronize all critical system clocks and times.

10.5 Secure audit trails so they cannot be altered.
10.5.1 Limit viewing of audit trails to those with a job-related need.
10.5.2 Protect audit trail files from unauthorized modifications.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6

10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

**Requirement 11: Regularly test security systems and processes.**
Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

**Maintain an Information Security Policy**

**Requirement 12: Maintain a policy that addresses information security for employees and contractors.**
A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, “employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the company’s site.