

Demystifying the Payment Card Industry - Data Security Standard

Does ADTRAN Comply?

What is the PCI DSS?

In short, the *Payment Card Industry (PCI) Data Security Standard (DSS)* is a stringent set of requirements to help retailers protect their customers' identity by securing their payment account transactions (credit card/debit) and stored card information. It is not a federal law, nor a certification process; it's merely a robust set of requirements.

The security standard was made available in early 2005, but getting buy-in from millions of merchants has taken time. The latest version of the standard Version 1.2, has created a lot more pressure and momentum in the industry for compliancy.

Who does the PCI DSS affect?

Any merchant that stores, processes or transmits the Primary Account Number (PAN) (credit or debit) must comply with the PCI DSS. This could be a local storefront (brick and mortar) or companies with only an on-line presence.

Who makes up the PCI?

American Express, Visa International, MasterCard Worldwide and Discover Financial Services, and JCB International are the five founding members of the PCI security standard. This is the first time that all five competing brands have come together for one cohesive effort.

Who is pushing for compliance?

The founding members listed above are pressuring their customers (the banks) around the globe. The banks in-turn pressures their customers (the merchants) to comply with the PCI standard. The so called *pressure* is through the use of a carrot-and-stick approach. Visa's approach calls for levying punitive fines on banks that fail to get their merchant customers to comply with the PCI standard (\$5,000 to \$25,000 a month) — while promising multimillion-dollar incentive packages for banks that prod their largest customers into complying (over \$20 million set aside in an incentive fund).

What's the motivation for the merchant to comply?

All merchants are required to comply with the PCI data-security standards or they too will face punitive fines! Fines could be as high as \$10,000 per month, per merchant, for non-compliance. For repeat offenders, the merchant may lose the right to process any payment card transactions. Either way, this could break a small business.

So, how does the PCI DSS affect ADTRAN?

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. In short, it covers all "system components" associated in or connected to the cardholder data processing/storing environment, which includes any *network component*, server, or application. *Network components* include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Are ADTRAN products "PCI Certified"?

The PCI council does not offer a certified "stamp of approval" for networking equipment. There are no formal tests that need to be completed, no official logos, or websites that list certified products. Even though ADTRAN's NetVanta internetworking products meet all the technical requirements outlined by the security standard (relative to *network components*), its up to a proper implementation for a merchant to meet compliancy.

What are the Requirements for the PCI DSS?

The primary focus of this document is to educate you on the PCI DSS requirements at a very high-level and where ADTRAN products comply. This paper does *not* dive into the technical details on how to configure these devices to be compliant. If you would like to review each requirement in detail, download the security standard by visiting www.pcisecuritystandards.org. The latest version of the standard, PCI DSS v1.2 includes detailed network and physical security requirements. We won't list them all here, but we will identify some of the pertinent items pertaining to our products/industry.

The 12 Requirements

You'll find that there are six logical groupings of the 12 overall requirements. Within each requirement there are several sub-requirements that specifically document in detail a particular security concern and a proposed method of protection. You'll also find that not every requirement pertains to the use of *network components*, where ADTRAN products are applicable.

- A) 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
- B) Protect Cardholder Data**
 - Requirement 3: Protect stored cardholder data
 - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- C) Maintain a Vulnerability Management Program**
 - Requirement 5: Use and regularly update anti-virus software
 - Requirement 6: Develop and maintain secure systems and applications
- D) 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
- E) 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
- F) Maintain an Information Security Policy**
 - Requirement 12: Maintain a policy that addresses information security

Let's take a slightly deeper look at each requirement, what are the detailed specifications, and how ADTRAN products fulfill each.

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

Synopsis:	There are 25 sub-requirements within this section and, as you can see by the title, it's entirely focused on a successful firewall implementation.
ADTRAN Stance:	ADTRAN's NetVanta product line meets each and every sub-requirement within this section, for each product includes a stateful packet inspection firewall and Network Address Translation (NAT).
Sub-Requirements:	<ul style="list-style-type: none"> 1.1.3 - A firewall is required at each Internet connection and between any DMZ and the internal network 1.2.0 - Build a firewall configuration that restricts connections between publicly accessible servers and any system storing cardholder data 1.2.1 - Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. 1.2.2 – Secure and synchronize router configuration files. 1.2.3 – Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment. 1.3.0 – Prohibit direct public access between the Internet and any system component in the cardholder data environment. 1.3.1 – Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment. 1.3.2 – Limit inbound Internet traffic to IP addresses within the DMZ 1.3.3 – Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment. 1.3.4 – Do not allow internal addresses to pass from the Internet into the DMZ 1.3.5 – Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ. 1.3.6 - Implement a stateful inspection, also known as dynamic packet filtering 13.8 - Implement IP masquerading to prevent internal address from being translated and revealed (i.e.: PAT, NAT)

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Synopsis:	This sounds pretty rudimentary, but hackers (external and internal to the company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information, or directly from the vendors' website. According to the Visa Cardholder Information Security Program (CISP) Bulletin, August 2006, this was #3 in the Top Five Data Security Vulnerabilities.
ADTRAN Stance:	This requirement outlines "best practices" type of procedures and is clearly dependent on a proper installation/implementation. <i>But</i> , there are some key hardware features/technology outlined in this section, which are all supported using the NetVanta line of products, like the use of SSH/HTTPS to encrypt device access and the use of 802.1x or a RADIUS/TACACS server and SecureID type devices for user authentication. Our NetVanta Wi-Fi products also adhere to this requirement by using key technologies like WPA/WPA2, disabling SSID broadcast, and also 802.1x user authentication.
Sub-Requirements:	2.1.0 - Always change vendor-supplied defaults before installing in the network (i.e.: passwords, SNMP community strings, unnecessary accounts) 2.1.1 - For wireless environments change wireless vendor defaults (i.e. WEP keys, SSIDs, passwords). Disable SSID broadcasts and enable WPA or WPA2 2.3.0 - Encrypt all non-console administrative access. Use SSH, VPN, SSL/TLS.

Requirement 3: Protect stored cardholder data

Synopsis:	This requirement does not pertain to the moving of cardholder data electronically over the network, but rather protecting the data while it is being stored. This section outlines the various types of data that can, and cannot, be stored, in whole or as parts (Magnetic strip, PAN, cardholder name, expiration date, and/or personal identification number (PIN)). In addition, it outlines the protection of data using disk encryption, encrypted databases, password protected backup material, and even retention policies (how long to archive data) and the policies associated to the proper disposal of stored data. This is the #1 security concern according to the VISA CISP Bulletin, on the Top Five Vulnerabilities.
ADTRAN Stance:	ADTRAN products have no direct relevance to this requirement.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Synopsis:	This section stipulates the use of strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (i.e.: Wi-Fi, GSM, and/or the Internet). You'll find this section covers an encryption scheme from both a wired and wireless network perspective.
ADTRAN Stance:	This requirement explicitly recommends IPSec VPN for the wired network and the use of WPA or WPA2 for the wireless network, which are both covered with the NetVanta line of internetworking products.
Sub-Requirements:	4.1.1 - For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS.

Requirement 5: Use and regularly update anti-virus software or programs

Synopsis:	Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. So, this requirement focuses on the deployment of anti-virus software on individual employees' computers and any corporate wide anti-virus systems.
ADTRAN Stance:	ADTRAN products have no direct relevance to this requirement.

Requirement 6: Develop and maintain secure systems and applications

Synopsis:	In today's high-tech computer world, keeping up with hackers, newly discovered vulnerabilities, worms, virus, trojan horses, macro virus, etc., it's a full time job for software engineers and system analysts to stay one-step ahead of the bad guys! This requirement deals with the maintenance and delivery of the numerous services packs, security patches, and software fixes associated to securing personal computers, application software, application servers, and operating systems. The Visa CISP Bulletin stated that this is the second highest security concern in the Top Five Vulnerabilities.
ADTRAN Stance:	ADTRAN's NetVanta products all run a common operating system, the ADTRAN Operating System (AOS), which typically releases three major revisions a year with minor updates on a monthly basis. Upgrading the AOS can be performed onsite, remotely, via Compact Flash™, or distributed network-wide using n-Command. ADTRAN's n-Command is a suite of network productivity tools for NetVanta -based networks, that offers the ability to discover devices, make mass configuration changes, backup and restore device configurations, upgrade firmware to groups of devices, globally modify Access Control Lists (ACLs), and generate inventory reports for asset management.
Sub-Requirements:	6.1.0 - Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

Requirement 7: Restrict access to cardholder data by business need-to-know

Synopsis:	This requirement ensures critical data can only be accessed by authorized personnel. It addresses access control, establishing privileges, restricting access, assigning IDs and the privileges necessary to perform job responsibility. There are system level access controls that our ADTRAN products can perform, but for the most part this is usually accomplished with server/workgroup software, typically through the standard server/PC operating system.
ADTRAN Stance:	For the most part, this section can be supported using any of the NetVanta line of products with 802.1x user authentication and a unique login/password scheme with assigned user privileges. For a more corporate wide approach, the NetVanta's also integrate with a RADIUS/TACACS server and SecureID devices.
Sub-Requirements:	7.1.0 - Limit access to computing resources and cardholder information only to those individuals whose job requires such access. 7.2.0 –Establish an access control system for systems components with multiple users that restricts access based on a user's need-to-know, and is set to "deny all" unless specifically allowed. 7.2.1 – Coverage of all system components 7.2.2. – Assignment of privileges to individuals based on job classification and function 7.2.3 – Default "deny-all" settings

Requirement 8: Assign a unique ID to each person with computer access

Synopsis:	Assign some type of unique user identification (ID) to each person with access to critical data and systems. This allows for the establishing of permissions and privileges, as well as for tracking purposes.
ADTRAN Stance:	The NetVanta products support this section by using 802.1x user authentication and a unique login/password scheme with assigned user privileges. For a more corporate wide approach, the NetVanta's also integrate with a RADIUS/TACACS server and SecureID devices as well. The use of SSH/HTTPS is used to encrypt passwords and an encrypted VPN tunnel can be used to protect the data while transporting across a public infrastructure.
Sub-Requirements:	<p>8.2.0 - In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> • Password • Token devices (e.g., SecureID, certificates, or public key) • Biometrics. <p>8.3.0 - Incorporate two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.</p> <p>8.4.0 – Render all passwords unreadable during transmission and storage on all system components using strong cryptography based on approved standards.</p>

Requirement 9: Restrict physical access to cardholder data

Synopsis:	This requirement is protecting the physical access to the systems and data that houses cardholder information. It includes restricting the physical access to the systems that house the data, backup data, or any removal of hardcopies.
ADTRAN Stance:	If physical access is obtained to an active NetVanta switch, the unused switch ports can easily be set to "disabled" therefore the intruder can not access your network through an available port. In addition, with MAC authentication, an active switch port will only grant access to an approved MAC address. If you have a need for surveillance cameras to monitor sensitive areas like server/storage rooms, MDF/IDF, and/or wiring-closets, the NetVanta line of switch and switch/routers offer Power over Ethernet (PoE) which can be used to power your cameras located in discrete, out-of-the-way locations.
Sub-Requirements:	<p>9.1.0 - Facility access control using badge readers, security codes, or standard lock and key.</p> <p>9.1.1 - Security cameras to monitor sensitive areas.</p> <p>9.1.3 - Restrict physical access to wireless access points, gateways, and handheld devices.</p> <p>9.5.0 - Storing media back-ups in secure locations</p> <p>9.10.0 - Destroy media containing cardholder data when it is no longer needed for business or legal reasons</p>

Requirement 10: Track and monitor all access to network resources and cardholder data

Synopsis:	This section is covers the tracking and monitoring of systems and user activities through the use of controls logs, systems logs, event logs, etc. The presence of logs allows thorough tracking and analysis if something does go wrong.
ADTRAN Stance:	All activity passed through a NetVanta device can be monitored, and most can be logged on a real-time basis to a SYSLOG server for further examination. For the need to synchronize system clocks, the NetVanta devices all use the standard Network Time Protocol (NTP) to assure that every network device is in sync.
Sub-Requirements:	<p>10.2.4 - Invalid logical access attempts</p> <p>10.3.0 - Record at least the following audit trail entries for all system components for each event:</p> <ul style="list-style-type: none"> 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 10.3.6 - Identity or name of affected data, system component, or resource. <p>10.4.0 - Synchronize all critical system clocks and times.</p>

Requirement 11: Regularly test security systems and processes

Synopsis:	Vulnerabilities are continually being discovered by hackers and researchers, and being introduced by new software. This area is to proactively test the systems to verify and maintain a secure implementation of the security standard. In addition, the requirement stipulates the use of an Intrusion Prevention System (IPS) Intrusion or an Intrusion Detection System (IDS).
ADTRAN Stance:	The Adtran Operating System (AOS) stateful packet inspection firewall (included in NetVanta and Total Access routers), in its own right, is an active intrusion prevention device blocking malicious traffic, stopping well-known attacks and threats in an intrusion detection system fashion before they impact your network, and yet allows legitimate traffic to flow unhindered. ADTRAN has been deployed in PCI-compliant networks addressing this requirement. The AOS has the ability to send email notifications based on firewall or Syslog events as specified in requirement 11.4b. The AOS firewall and router represents only a segment of your PCI network which can also include additional software and hardware components to protect cardholder data. When used in conjunction with an enterprise-wide intrusion detection/prevention system, ADTRAN can interface with industry leading IDS/IPS vendors to insure that malicious activities/traffic occurrences are stopped before they impact the network and your business.
Sub-Requirements:	11.2.0 - Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). 11.3.0 - Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: 11.3.1 - Network-layer penetration tests 11.3.2 - Application-layer penetration tests. 11.4.0 - Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up to date.

Requirement 12: Maintain a policy that addresses information security

Synopsis:	Being the final requirement, this section is quite detailed and outlines various policies, procedures, and processes to successfully implement and maintain the Data Security Standard.
ADTRAN Stance:	ADTRAN products have no direct relevance to this requirement.