

Fundamental to protecting cardholder data is restricting, by user, who can access what data on the LAN. ConSentry Networks has developed an access control platform that learns a user's identity and role and restricts that user's access to only those resources appropriate for the role.

APPLICATION SOLUTION BRIEF: **PCI COMPLIANCE**

How Network-Based Access Controls Can Help with PCI Compliance

PCI – HOW NETWORK-BASED ACCESS CONTROLS CAN HELP WITH COMPLIANCE

In the wake of several security breaches, the Payment Card Industry, an industry group set up by the major credit card brand companies, has set out to define security requirements for handling credit card data. The group's Data Security Standard (DSS) version 1.1 specification details the steps any entity that processes, stores, or transmits credit cards must take to protect cardholder data.

As with any specification, of course, much is left to interpretation. In the case of the PCI DSS, it's the Qualified Security Assessors (QSAs) who end up interpreting the specification to see whether a company is compliant with the spec. The spec details only the result of a given security parameter – it does not define how a company must achieve that security.

No single process, technology, or system can enable a company to become PCI compliant. Instead, businesses will need to take multiple steps, including deploying security products, to help in this process. Network access controls, in particular those based on identity and role, can play a significant part in helping companies achieve PCI compliance.

Some network access control systems include the ability to authenticate users to a network, track all their activities, learn the user's role, apply access policies based on that role to govern which resources the user

can reach, and detect anomalous behavior on the part of users or applications that might signal an attack.

HOW CONSENTRY HELPS SATISFY PCI REQUIREMENTS

Fundamental to protecting cardholder data is restricting, by user, who can access what data on the LAN. ConSentry Networks has developed an access control platform that learns a user's identity and role and restricts that user's access to only those resources appropriate for the role. The platform also provides an audit trail of all user activity.

ConSentry has worked with several companies to apply its access control technology to the PCI regulation. The company has been able to help electronic funds processors and other companies achieve compliance in a quick timeframe (see the ConSentry case study "ConSentry Delivers PCI Compliance and More for a Fortune 500 Financial Company" for more details on one example).

The following matrix provides some insight into how ConSentry can be part of an organization's efforts to meet the PCI requirements. It details the various aspects of the PCI DSS 1.1 specification where ConSentry can deliver concrete tools that achieve the requirement.

We can be reached at info@consentry.com if you have any additional questions.

REQUIREMENT	DESCRIPTION	HOW CONSENTRY CAN HELP ADDRESS THE REQUIREMENT
1: Install and maintain a firewall configuration to protect cardholder data		
1.2	Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.	Build an access policy that blocks traffic from unknown addresses and another access policy to alert on any protocol other than those needed for cardholder data environment.
1.3.5		Implement a “deny all” policy for any traffic not between a user in a PCI role and a PCI server.
1.3.7	Denying all other inbound and outbound traffic not specifically allowed	Implement a “deny all” policy with specific allowances, by address, time of day, and other parameters to support data access.
1.3.8	Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)	Set an access policy to deny all traffic from and to the wireless access point.
1.4.2	Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	Implement a “deny all” policy for traffic destined to the at-risk IP addresses.
2: Do not use vendor-supplied defaults for system passwords and other security parameters		
	Addressed through password-management best practices	
3: Protect cardholder data		
3.4	Render PAN, at minimum, unreadable anywhere it is stored. . . .	Per Appendix B, provide a compensating control via the LANShield’s network segmentation; access control by address, applications, and user groups; limiting access to the data beyond controls in AD; detecting database attacks via anomaly detection.
4: Encrypt transmission of cardholder data across open, public networks		
	Addressed through WAN encryption.	
5: Use and regularly update anti-virus software or programs		
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	Deploy ConSentry posture check agent to validate state of AV software and to log user violations.
6: Develop and maintain secure systems and applications		
	Addressed through application development and patch management.	
7: Restrict access to cardholder data by business need-to-know		
7.1	Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	Establish role-based access control, leveraging data in the identity store, to deny access to all but those in a “PCI” role.
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed.	Require access based on authentication by user vs. by machine, combined with role-based access control, to limit access for those in a “PCI” role.

REQUIREMENT	DESCRIPTION	HOW CONSENTRY CAN HELP ADDRESS THE REQUIREMENT
8: Assign a unique ID to each person with computer access		
8.1	Identify all users with a unique user name before allowing them to access system components or cardholder data	Deny access to cardholder systems for any unauthenticated user.
9: Restrict physical access to cardholder data		
	Addressed via physical security measures.	
10: Track and monitor all access to network resources and cardholder data		
10.1	Establish a process for linking all access to system components to each individual user.	Build ConSentry InSight reports that detail every username that has accessed the cardholder resources.
10.2.1	Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data	Run a nightly InSight report to detail each username that accessed the cardholder data.
10.3	Record at least the following audit trail entries for all system components for each event: user identification; type of event; date and time; success or failure indication; origination of event; and identity or name of affected data, system component, or resource.	ConSentry InSight retains a complete log of all interaction with any system, noting each of these details.
10.7	Retain audit trail history for at least one year, with a minimum of three months online availability.	ConSentry InSight retains recent data within its database and supports archiving to outside database schemes for longer-term retention.
11: Regularly test security systems and processes		
11.1	Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.	The ConSentry LANShield Switch prevents any new device, including a wireless access point, from passing any traffic without first authenticating, so it will block rogue devices.
12: Maintain a policy that addresses information security for employees and contractors		
	Addressed through policy development and communication.	

ABOUT CONSENTRY NETWORKS

ConSentry Networks delivers secure switching, enabling enterprises to control every user and secure every port on the LAN through its LANShield product family – the LANShield™ Switch, LANShield Controller, and InSight™ Command Center. More than 100 enterprises today rely on ConSentry’s award-winning secure-switching platforms to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry is backed by blue-chip venture capital firms Accel Partners, DAG Ventures, INVESCO Private Capital, and Sequoia Capital; and is headquartered in Milpitas, California. www.consentry.com

Corporate Headquarters
 ConSentry Networks
 1690 McCandless Drive
 Milpitas CA 95035
Phone 408.956.2100
Fax 408.956.2199
Toll-Free 866.841.9100
 Email info@consentry.com
www.consentry.com

Worldwide Locations
 London, United Kingdom
Phone +44 (0) 00870 351 9494
 Frankfurt, Germany
Phone +49 69677 33 4
 Tokyo, Japan
Phone +813 5532 7630

For a complete listing of all our office locations go to:
www.consentry.com/company.html

