CONSENTRY NETWORKS

CONSENTRY NETWORKS SUPPORT MATRIX

FOR THE PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD

Section	Description	ConSentry Support
1.1.4	Description of groups, roles, and responsibilities for logical management of network components.	The ConSentry platform allows logical grouping of users/groups across the enterprise to access/application use roles/responsibilities.
1.1.5	Documented list of services/ports necessary for business.	The ConSentry platform contains documentation and controls access by user/groups to specified services/ports.
1.1.6	Justification and documentation for any available protocols besides HTTP and SSL SSH and VPN.	The ConSentry platform can identify, track, and enforce policies around the exception protocols.
1.1.7	Justification and documentation for any risky protocols allowed (for example, File Transfer Protocol [FTP]), which includes reason for use of protocol and security features implemented.	The ConSentry platform can identify, track, and enforce policies around the exception protocols to ensure that only authorized [justified] users can access these protocols/ports.
1.1.9	Configuration standards for routers.	The ConSentry platform can enforce application use/access very close to the actual users [rather than waiting for traffic to reach the WAN router or perimeter router on network egress].
1.2	Build a firewall configuration that denies all traffic from "untrusted" networks/hosts, except for:	The ConSentry platform can enforce a whitelist of approved hosts/networks/applications and deny all other traffic.
1.3.2	Restricting inbound and outbound Internet traffic to ports 80 and 443.	The ConSentry platform can restrict communications to specific ports and even to specific applications on approved ports [deep inspection to detect port cloaking].
1.3.4	Stateful inspection, also known as dynamic packet filtering (only "established" connections are allowed into the network).	The ConSentry platform maintains state on user application flows to track dynamic port assignments for authorized application activity. It will also support stateful inspection filtering for "firewalling" internal hosts or services.
1.3.6	Restricting outbound traffic to that which is necessary for the payment card environment.	The very foundation of the ConSentry platform is granular policy management of what applications users are allowed to run over the network. The ConSentry platform can be configured to automatically block any application on the network for a given user or user group that is not approved/allowed.

Section	Description	ConSentry Support
1.3.8	Denying all other inbound and outbound traffic not specifically allowed.	The very foundation of the ConSentry platform is granular policy management of what applications users are allowed to run over the network. The ConSentry platform can be configured to automatically block any application on the network for a given user or user group that is not approved/allowed.
1.3.9	Installation of perimeter firewalls between any wireless networks and the payment card environment, and configuration of these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment.	The ConSentry platform is a multi-port device which, for example, can have a wireless network segment with restrictions on user activity.
4.1	Use strong cryptography and encryption techniques (at least 128 bit) such as SSL, PPTP, IPSEC to safeguard sensitive cardholder data during transmission over public networks.	The ConSentry platform can block specified application traffic that is not adequately encrypted.
4.1.1	For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a WLAN. Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.	The ConSentry platform can block specified application traffic that is not adequately encrypted.
4.2	Never send cardholder information via unencrypted e-mail.	The ConSentry platform can block specified application traffic that is not adequately encrypted.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	The ConSentry platform will work in conjunction with various host posture checking agents and will allow/deny network access based on compliance to the stated policy.
6.1	Ensure that all system components and software have the latest vendor-supplied security patches.	The ConSentry platform will work in conjunction with various host posture checking agents and will allow/deny network access based on compliance to the stated policy.
8.1	Identify all users with a unique username before allowing them to access system components or cardholder data.	The ConSentry platform will restrict user access to any network resources until the user is authenticated and authorized for network access.
10.2	Implement automated audit trails to reconstruct the following events, for all system components:	The ConSentry platform contains complete audit trails of individual user activity on the network. The system automatically coalesces user identity [user name, IP address, MAC address] to L7 application.
10.3	Record at least the following audit trail entries for each event, for all system components:	The ConSentry platform contains complete audit trails of individual user activity on the network. The system automatically coalesces user identity [user name, IP address, MAC address] to L7 application.

CONSENTRY NETWORKS

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