PCI Checklist

The following is a checklist of the items OmniNet addresses from the PCI DSS v3 requirements.

In some cases OmniNet can be considered a compensating controls as described in Appendix B in the PCI DSS v3 standard document, which would help cover other areas not directly addressed below.

1.1.0 – OmiNet uses best practice firewall and security configurations
1.1.1 – partial – any firewall configuration changes are automatic when in a PCI environment. We don't cover physic changes
1.1.4 – provide firewall
1.1.7 – partial - give ability to review
1.2.0– by default all the rules are built to restrict all access to cardholder network.
1.2.1 – firewall restrictions
1.2.2 – partial – we secure and synchronize OmiNet configuration
1.2.3 – We separate the networks with firewalling
1.3.0 – This is the default configuration and the only one for the PCI network.
1.3.1 – We provide the capability to have a DMZ and have cardholder data network separated. Also give ability to limit the inbound ports to the DMZ
1.3.2 – the inbound is limited by IP and port
1.3.3 – this is accomplished through automatic rules.
1.3.4 – Anti-spoofing is implemented with the MDS system
1.3.5 – OmiNet restricts access from cardholder network to internet, only for authorized traffic
1.3.6 – OmiNet provides stateful inspection.
1.3.7 – OmiNet give the capability for this type of segregation
1.3.8 – OmiNet does not disclose private network IP by implementing NAT.

2.1.0– partial – OmiNet forces the setting of passwords and does not have a default password.
2.1.1 – In the case of OmiNet Pro, you can assign wifi to the cardholder network, there are no defaults, all settings such as password and encryption must be manually set.
2.2.0 – OmiNet itself is built with highest levels of configuration standards and is always kept up to date, but does not update other network components (computers, servers etc..)

4.1.0 – partial – OmiNet implements a DLP and will block and credit card numbers being transmitted in clear text.
4.1.1 – OmiNet provides wireless with the ability to only use WPA2.

5.1.0 – partial – OmiNet deploys network based anti-virus but does not deploy software version on computers. This will come in the future with Shield Agent.
5.1.1 – AV signatures are updated hourly or receive push updates if necessary.
5.1.2 – partial – OmiNet provides this from the network level but does not deploy software.
5.2.0 – all AV is kept current and scans all data in motion. Logs are generated and retained.
5.3.0 – network based AV is running all the time and cannot be disabled by the end user.

8.3.0 – We do NOT provide 2 factor for remote access. If remote access to cardholder network is required, users should add 2 factor authentication.

10.1.0 – partial – log web traffic and internet usage
10.3.0 – partial for all. OmiNet logs and creates an audit trail for internet bound or off network traffic.
10.5.0 – partial – for those audit trails that OmiNet produces and store, we ensure tamper proof by implementing applicable section 10.5 items.
10.6.0 – partial – a report is produced by OmiNet that shows security events and suspicious activity.
10.7.0 – OmiNet retains log history for at least 1 year

11.1.0 – Currently we do not automatically but can with involving support.
11.4.0 – OmiNet provides Intrusion Prevention

Toll Free: 866-424-4489
OmniNet www.omninet.io
1800 Continental Blvd Suite 200
Charlotte, NC 28273 | USA