Conquering PCI DSS Compliance

Any organization that stores, processes or transmits information related to credit and debit card payments has a responsibility to protect each cardholder’s personal data. To help accomplish this goal, the Payment Card Industry (PCI) Security Standards Council developed the PCI Digital Security Standard (PCI DSS). This set of standards provides a global framework of practices designed to prevent, detect and react to security incidents. Entities expected to comply include merchants, financial institutions, e-commerce companies, non-profit and educational organizations, restaurants, professional services providers, Cloud Service Providers (CSPs), Managed Security Service Providers (MSSPs) and even individuals who accept payment cards for product sales and services.

The PCI DSS Standards

The PCI DSS, which covers technical and operational components in the payment card transaction environment, expects entities to:

Build and maintain a secure network
- Install and maintain a firewall configuration to protect cardholder data
- Eliminate vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data
- Safeguard stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program
- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement strong access control measures
- Limit access to cardholder data to only those individuals whose jobs require such access
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly monitor and test networks
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an information security policy
- Develop, implement and enforce an information security policy for all personnel
Conquering PCI DSS Compliance

Compliance: Costly and Complex
Organizations that must comply with PCI DSS face a number of obstacles, including the following:

- **Lack of In-House Expertise** — The complicated process for PCI DSS compliance usually includes determining which system components are impacted, examining the compliance of those components, validating alternative control technologies/processes, reporting and submitting required documentation, and clarifying or updating report statements. Adding to the complexity is the fact that requirements vary depending upon an entity’s classification or risk level. Moreover, each payment card brand has its own specific compliance enforcement program. Rarely does a merchant or other entity have the in-house expertise required to fully interpret and comply with all the variables.

- **CAPEX Investment** — In many cases, the hardware and software an organization uses for its day-to-day operations does not meet the technical requirements of the PCI DSS. This means entities may face a considerable capital outlay in the name of security compliance. The tab continues to grow as ongoing maintenance, capacity expansions and upgrades to meet changing regulations and increased threats are added to the total investment cost.

- **Diminished Operational Efficiency** — Unless an organization invests in specialized IT staff and in-house compliance experts, it will find itself diverting the attention of team members away from operations that grow revenue and improve customer service to focus instead on complex security compliance activities. Most organizations impacted by PCI DSS do not have spare headcount to determine security requirements, review and update documentation, conduct risk assessments and install and maintain security network hardware and software.

- **Constantly Evolving Security Environment** — Organizations not only must fight current attacks but also anticipate and thwart future ones. Threats can originate from evolving network technologies, protocols and devices, as well as sophisticated hackers, internal breaches, Bring Your Own Device (BYOD) and wireless environments, increased personnel access, business partner security breaches and even natural disasters.
Managed Security: Effective and Essential

Often the most effective way to approach PCI DSS compliance is to work with a PCI Compliant CSP or MSSP. A managed security approach that encompasses both technology and threat management provides an organization with efficiencies and functionality far beyond what can be accomplished in house, including:

- **Lowered CAPEX** — Organizations can reduce or even eliminate their cost of capital investment for PCI DSS compliance by jettisoning the purchase and maintenance of specialized hardware and software, and taking advantage of a hosted cloud network or an MSSP’s purpose-built resources. Retained capital resources can then be used for projects that more significantly impact enterprise growth.

- **Predictable OPEX and Workforce Efficiencies** — In addition to reaping the benefits that come from converting burdensome CAPEX spending to OPEX predictability, organizations can reduce or eliminate the need for staff to devote time to security compliance activities and instead focus on projects that contribute directly to organizational profitability.

- **Decreased Risk** — A CSP or MSSP provides immediate access to new technologies and applications in an always-changing card-processing ecosystem where vulnerabilities may appear almost anywhere, including point-of-sale devices, wireless hotspots or Web applications, servers and more. By keeping ahead of sophisticated hackers and data thieves who constantly devise new ways to breach security, organizations will see increased customer confidence and protected brand reputation, as well as avoided lawsuits, insurance claims and fines.

- **Accelerated Time to Market** — By partnering with a cloud provider or MSSP and its security compliance experts, an enterprise reduces precious time spent researching, purchasing and installing specialized hardware and software, and developing complicated security processes. It can instead focus on other critical operational issues required for a timely launch or expansion.

By keeping ahead of sophisticated hackers and data thieves, organizations will see increased customer confidence and protected brand reputation, as well as avoided lawsuits, insurance claims and fines.
What to Look for in a Provider

Windstream’s PCI compliant Data Centers and MSSP offerings are able to combine security technologies and security management into a single, unified package, so organizations can quickly and cost-effectively get the help they need to comply with PCI DSS.

The many benefits that organizations gain when choosing a provider such as Windstream include:

- **Access to experts** trained in the interpretation and implementation of regulations and their impact on an organization’s network

- **Enterprise-class Cloud Data Centers** that include vulnerability assessments, threat detection, penetration testing and incident response to help identify and deal with security issues before and after they occur

- **Technologies and processes** for access control, authentication, data encryption and accountability practices on all Local Area Networks (LANs) and Wide Area Networks (WANs), and for users accessing the network remotely through Virtual Private Networks (VPNs) and WiFi

- **Quick and easy scalability** for growing enterprises

- **Risk-free, easy deployment** and a single point of contact for all issues

- **Real-time protection** with application intelligence that detects and prevents malicious traffic from gaining network access, and protects against viruses, worms and phishing attacks

- **Security log storage and robust reporting**

Finally, organizations must ensure the services they obtain meet the requirements of PCI DSS. Although each entity ultimately is responsible for its own compliance, confirming that cloud and MSSP services meet regulations allows an organization to rest assured that the specific piece of the compliance puzzle being outsourced will meet regulatory requirements.
Conclusion

With a company like Windstream as your CSP and MSSP for compute, storage, networking, email and web security, you can stop worrying about outdated equipment, hardware failure and lack of capital resources. You also gain access to seasoned professionals who use powerful security technology and highly accurate threat intelligence to provide comprehensive, 24 x 7 network protection and regulatory compliance.

Windstream’s Security Services team members will work with you at every point to implement and maintain the most cost-effective solutions to safeguard your network and your business. Rely on their expertise with complex security demands and strict regulatory compliance requirements so you can strengthen security while freeing your IT resources for projects that contribute to your business goals — and your bottom line.