



Link Mountain, LLC PO Box 182 Port Sanilac Michigan, 48469 – www.linkmountain.com

PCI service perspective for Hosting Providers, Data Centers and ISPs

An introduction to Link Mountain, LLC

Penetration testing

We list this first not because it is the most important for service provider companies like yours, but because it may be the best possible way to get to know us. Chances are good that either you, one of your clients or someone you know will soon need an annual penetration test (or one of the other services we list below) for PCI-DSS compliance. Here is our simple proposal – just give them our email address – sales@linkmountain.com. We don't mind if you give them contact information for our competitors as well, and we don't mind if you don't recommend us right away – you can just tell them 'We heard about this company, we don't have any experience with them yet but you might ask them for a quote'.

Here is what you can expect:

1. You or your client will award us the contract because we will have the lowest rates, present ourselves professionally and provide excellent references.
2. You or your client will be very happy with the services performed.
3. You will receive a check from us for 10% of the contract value within 30 days of our receipt of payment.

We will extend the same offer for secure code reviews or any of the other services we provide. Our quotes will typically come in at one third of TrustWave, Verisign or McAfee, and one half of other competitors.

This gives you a way to get to know us, our quality of service, our low rates and dependability through your client's experiences, without even the need of recommending us. We would be happy to provide you with references from PCI-DSS QSAs (Qualified Security Assessors) and ASVs (Approved Scanning Vendors) for whom we have done similar work.

Now for the services we offer, from a hosting, data center or ISP perspective...

Shared Hosting

We can help you offer PCI-Compliant shared hosting environments for your clients. This is a rapidly growing niche, as there are many small businesses that need card processing but can't afford the overhead that comes with owning their own server. PCI-DSS compliance has increased the cost of ownership dramatically, and many small businesses are moving to PCI compliant shared hosting environments because it is the only solution that makes sense for them. There is more than one option open to a hosting company that wants to provide this service to their shared hosting clients. We will briefly outline two approaches here.

1. PCI-DSS Appendix A approach. This approach leverages the specific ‘Shared Hosting’ provisions of the PCI-DSS 1.2, at 2.4 and appendix A. In addition to the general PCI services listed below, we can help you implement the following, specific to the ‘Appendix A’ approach :
 - PCI-DSS 1.2 at A.1.1 and 2 - Process segregation and access controls
 - PCI-DSS 1.2 at A.1.3 - Central logging solution appropriate to shared hosting environments
 - PCI-DSS 1.2 at A.1.4 - Developing forensic policies appropriate to shared hosting environments
 - Agreement language specific to shared hosting PCI-DSS requirements
 - Pre-written information security policies for your shared hosting clients.
2. Payment Application approach. This approach allows you to segregate the payment related code base (yours or your clients) from the rest of the code base. You then deploy the payment portion of the code base as a separate web application, on a server well segregated and dedicated to payment applications, and validate the application either under PA-DSS or PCI-DSS. In general, the more you segment your network and isolate payment related code, the cheaper it is to comply with PCI-DSS. This approach achieves significant isolation. This approach also affords much greater flexibility in your actual shared hosting environment because the payment processes (and the accompanying constraints) are isolated from the shared hosting servers. ***This factor is very important as more small companies with various existing platforms and architectures seek PCI compliant shared hosting environments.*** In addition to the general PCI services listed below, we can help you implement the following, specific to the ‘Payment Application’ approach :
 - Assistance with the requirements of PA-DSS (unless validated under PCI-DSS)
 - Agreement language specific to Payment Application PCI requirements
 - Pre-written information security policies for Payment Application clients.

Dedicated Servers

Dedicated servers present a greater challenge because the client has more control and you have less control. This makes it difficult to guarantee a ‘PCI-DSS compliant dedicated server’, because your clients can make non-compliant configuration changes. *What you can do* is provide a dedicated server that is properly configured, resides on a well segmented network with appropriate firewall rules and is PCI-DSS compliant AS IS, and ready for your client’s customization. Your clients can ‘move in’ to a dedicated server knowing that the network and host configuration is already compliant. In addition to the general PCI services listed below, we can help you implement the following, specific to dedicated servers:

- Agreement language specific to dedicated servers
- Pre-written information security policies for your dedicated server clients.
- Help you develop an established process and policy for standing up PCI compliant dedicated servers while keeping costs to a minimum.

Co-located Servers

CoLo servers are much like dedicated servers in that the network configuration can be PCI compliant, but that’s where it ends because you don’t have control of the host configuration. This makes it harder to define standard procedures, but CoLo clients are usually ready to take on the requirements



Link Mountain, LLC PO Box 182 Port Sanilac Michigan, 48469 – www.linkmountain.com

themselves, with networking support from you. You can offer your clients a compliant network on which to locate. We would be happy to find a mutually agreeable arrangement with you for your clients who have host and application PCI needs for CoLo servers.

Development and Code Review Services

For Hosting Providers, Data centers and ISPs, there is a revenue opportunity centered on PCI-DSS requirements for secure code reviews. For your clients with custom payment applications, PCI-DSS requires that all new code be reviewed for security faults before deployment, and the review has to be conducted by someone knowledgeable and *without a reporting relationship* with the person who wrote the code under review. This puts the hosting provider in a position to offer secure code review services, since most small businesses do not have sufficient operating budget to maintain personnel solely for secure code review. This is even truer for independent developers who need to write payment code for their clients – these ‘one man shops’ have no way to meet this requirement without outside help. These clients also are required to have ongoing developer training, which the hosting provider is also in an excellent position to provide.

- We can provide you with secure code review services on any code you or your clients develop for payment applications.
- We can provide secure coding training for you or your clients as required by PCI-DSS 6.5

General PCI-DSS services:

Your clients with PCI-DSS compliance needs will need all of the following services. They will either get them from you in a boxed and prepackaged solution like PCI compliant shared hosting or dedicated servers, or they will need to arrange for these services independently. We would be happy to extend a 10% revenue sharing arrangement with you for any of your clients who have any of the following PCI needs, except where otherwise noted:

- Assistance with network segmentation issues
- Central logging solutions
- Quarterly internal scans
- Quarterly external scans (10% commission does not apply because we partner with another provider for this – we will be happy to negotiate an equitable arrangement with you however)
- IDS/WAF validation
- Annual penetration testing
- Secure code reviews
- Secure code training
- IDS and Web Application Firewall solutions
- Managed security services
- Selecting and negotiating with QSAs
- End to End PCI-DSS consulting