

Pipeline

Knowledge Is Power

www.pipelinepub.com Volume 4, Issue 9

New Opportunities in the Remote Product Services Market

by Randy Krenz

The market for outsourcing Remote Product Services (RPS) is escalating rapidly with some industry experts estimating that it will hit \$290 billion by 2011. RPS is ideal for OEMs, VARs, and service providers tasked with tracking, repairing, and maintaining remote devices and equipment. The rapid increase in the remote services market can be attributed to a number of factors including escalating customer demand for higher availability and reliability of network services in conjunction with reduced in-house IT resources. In this fast growing space, service providers are poised to take advantage of this trend, by not only growing their customer base, but by also improving upon the services they currently offer, thereby fending off potential competitive threats.

The managed services market is ripe for OEMs or VARs looking to displace revenue from diminished product margins, or independent Managed Service Providers that are trying to find ways to increase customer adoption of service offerings. This article will discuss the keys to success in the RPS market by selecting the right RPS tools and offering the appropriate differentiated service levels that meet or exceed customer expectations.

A recent study on RPS by the Aberdeen Group found that the majority of equipment manufacturers surveyed intend to deploy commercial RPS solutions in the next 12 to 24 months. The report also states that those currently offering managed services plan to modify their business processes to incorporate both preventative and proactive approaches into service delivery. As more services move to "proactive" versus "reactive" based models, services organizations that have previously followed the "break-fix" services model will quickly find themselves struggling to protect their customer base from competitive threats. One key way to combat this threat is by offering differentiated service level agreements that guarantee uptime and accelerate problem resolution through proactive management, maintenance, and repair.

When examining the available tools to perform RPS, Service Providers must determine:

- 1: Do the available tools enable my organization to offer differentiated remote-based services?
- 2: Does the introduction of new tools introduce disruption to either my customers or

my support processes?

3: Can the tools be deployed at a cost point that supports the business case for remote services offerings?

A base requirement of any proactive RPS tool is its ability to constantly monitor the health of the device or application so that it can identify potential issues before they reach a critical state. Monitor-only solutions are helpful but are limited by the service level they can offer because the solution still requires a "man in the van" to go to the customer site to address the problem. This scenario increases the chance of failure between problem discovery and resolution and also causes extended downtime if the device or application is already in a fault state.

Some service providers have found success by combining remote monitoring tools with external remote access methods such as VPNs or dedicated circuits. However, these combination solutions can add additional costs to service infrastructures because of the costs involved in deploying, scaling and managing the overlaying remote access methods. In addition, these methods may be unacceptable to customers because of the:

- *security risks they can introduce (i.e. requires holes in firewalls).*
- *additional cost that may need to be passed on to customers to achieve remote connectivity.*



However, there is a new breed of RPS tools that service providers should consider when looking to differentiate their services -- virtual infrastructure solutions. These solutions allow service providers to offer on-demand IP-based remote monitoring and management services without the use of complex VPNs or agents at customer locations. A virtual infrastructure RPS tool creates an overlay management network that makes all the devices appear to be on the same physical network as the service provider's data center, regardless of their actual location across the Internet. Simultaneously, these virtual infrastructure solutions allow customers to maintain security and compliance requirements when outsourcing IT management. By utilizing this new breed of RPS solutions, service providers can concurrently offer proactive monitoring services and differentiated management services while

leveraging existing investments in back-office management tools. By using appropriate RPS tools, service providers have multiple opportunities to offer remote maintenance, integrated remote access, and remote monitoring with differentiated services. Beyond the ability to perform immediate remediation when problems arise, service providers can use RPS tools to leverage the embedded management capabilities of the devices. In addition, these tools can leverage the best-of-breed network management tools and offer value-added services modules such as:

- *details and performance metrics analysis*
- *root cause analysis*
- *asset and customer utilization*
- *upgrade & patch distribution*

Another remote maintenance opportunity for service providers is to offer *preventive maintenance* contracts that can be performed more frequently and at lower costs than traditional preventative maintenance contracts. This can be done for less money because preventative maintenance can be executed remotely without the costs of sending personnel on-site. With the proper remote support tool, service providers can also accomplish all these services without the need for customer intervention.

Before jumping into the enhanced remote maintenance market and selecting a RPS tool, there are some issues that service providers should consider, like security. Most companies that are evaluating outsourcing options are concerned about security. Enterprising service providers can address this concern by using an RPS tool that can perform remote maintenance while meeting customer internal security practices and regulatory obligations.

Service providers can increase the adoption of their remote maintenance service offerings if they can:

- demonstrate that their RPS tools do not introduce any security risks to customer networks.
- guarantee that access can only be gained to devices or applications under contract.
- assure end-to-end security of the management data transported between the service provider and the customer site.
- maintain an audit trail of where, when, and by whom a remote management session was performed to meet any regulatory reporting.
- deploy the services without the need to pass any deployment costs onto customers, or require customers to modify their operational practices or network security in order to accommodate the service.

Another consideration, service providers should bear in mind is the remote maintenance services impact on current customer business practices. The transition from a centralized support team to a "field-based" support team can introduce significant changes to an organization. To mitigate this issue, service providers should look for an RPS solution that allows service technicians to utilize the same diagnostics and remediation tools that they are accustomed to using. If service providers can seamlessly gain remote access to customer assets as if they were on-

site, this will provide a smoother migration, eliminate the need for retraining, and minimize disruption for customers.

In these times, when service providers are scrambling to find ways to increase service solutions to their customers, it makes sense to add value-added proactive-based services to their portfolios. RPS tools provide service providers with new opportunities to add differentiated remote services to their service portfolio beyond remote monitoring that will capture greater market share of customers that require higher asset uptime.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.