

LANTRONIX®

**Securely Access and Manage Firewall-  
Protected Equipment...*From Anywhere***



Lantronix, Inc.  
15353 Barranca Parkway  
Irvine, CA 92618  
Tel: +1 (800) 422-7055  
Fax: +1 (949) 450-7232  
[www.lantronix.com](http://www.lantronix.com)

# Contents

Introduction .....	3
Remote Device Management.....	3
Overcoming the Hurdles.....	4
Beyond Analog and Cellular Modems .....	5
ManageLinx Provides Secure Remote Access for Firewall-Protected Environments .....	5
Creating a ManageLinx Virtual Device Network.....	6
ManageLinx Features and Benefits .....	8
ManageLinx Target Applications .....	8
Conclusion.....	9

## Introduction

Businesses today are constantly challenged to control costs, boost profitability and essentially do more with less. This translates into the need for original equipment manufacturers (OEMs) to increase output, maximize equipment uptime and improve reliability for their customers through manufacturer service programs. To meet these goals, OEMs need to provide product service solutions that are cost-effective and easy-to-deploy and manage, while providing a quantifiable return on investment (ROI). Not an easy task by any means.

OEMs are increasingly leveraging a category of solutions called remote product services (RPS). RPS solutions provide wireless or Internet-based connectivity to remotely access and evaluate a company's asset data and help them identify problem areas, avert failures and implement corrective actions including repairs, upgrades or new processes. RPS enables companies to meet the challenges in today's business climate and provide better service, better product quality and improved profitability.

Organizations of all sizes outsource various aspects of their business, from production to an array of professional services. Considering the high cost of maintaining a large amount of a company's equipment assets, remote product services from the supplying OEM or even third-party managed service providers (MSPs) can be a prudent business decision. Where the challenge lies, however, is in making outside access to equipment for remote management seamless and secure, without circumventing IT policy.

This paper will define the market potential for OEM service organizations to remotely manage their clients' networked devices. It will explain the complexities involved in achieving the remote access required. It will highlight the need to address firewall security issues and the importance of easy-to-deploy solutions for non-networking professionals tasked with installing, integrating and often configuring remote access devices.



## Remote Device Management: A Winning Solution, But Not Without Challenges

The market revenue for remote product services is estimated to grow from less than \$50 billion in 2006 to more than \$290 billion by 2011 according to AberdeenGroup<sup>1</sup>. According to their report, this growth is largely fueled by improved customer retention and reduced field service and repair costs. Key findings from companies that use RPS include:

---

<sup>1</sup> Source: *The Remote Product Service (RPS) Update*. AberdeenGroup, November 2006.

- 38% improvement in customer retention
- 30% reduction in field technician dispatches
- 28% improvement in first technician call resolution
- On average, companies are able to achieve asset uptimes of greater than 95%
- RPS users are 3 times as likely to achieve 91% or higher service contract compliance

A frequently experienced roadblock to implementing RPS is the company's own security requirements. The means for protecting data and proprietary intelligence generally make it difficult to achieve the level of remote access required. Firewalls are universal among businesses, and managing multiple vendor relationships, accounts and passwords is a significant burden for overworked IT staff. Given the work involved, many companies are unwilling to invest the energy to manage the work that comes with changing or opening a port to allow remote monitoring. However, until it is possible to pass through border firewalls, realizing the full benefits of RPS simply cannot be achieved.

What is required to solve this issue is a means for accelerating remote product service by enabling secure remote device access to firewall-protected equipment while maintaining IT security policies and firewall integrity.

Of equal concern to most companies is overcoming the list of deployment issues. Businesses worry about the potential high cost of installing a remote solution – they employ installers of the equipment or device, but may not have trained network technicians or IT personnel onsite to do the job. Another concern is the difficulty in configuring a remote access solution. For a RPS solution to have widespread adoption, it needs to be easy to deploy and configure, be highly reliable and maintain security and keep equipment, service and downtime costs at a minimum.

## Overcoming the Hurdles: Fully-Secure Remote Firewall Access and Seamless Integration

The challenge of establishing remote access for service organizations lies in overcoming two major hurdles, the first being the need to establish remote access within the parameters of a secure firewall. Firewall configuration is typically based on conservative thinking and designed to be rigorous in defending information and access. Data security is the leading obstacle to RPS adoption because a company's security policies are critical to business operations and cannot be hampered, even to increase company profitability. Therefore, the integrity of firewalls must be maintained. Changing security specifications in order to allow for remote access is not an option.

By default, most firewalls are configured to stop all traffic originating from the Internet to gain access to the organization's protected network. Establishing a secure proxy between system administrators and networked devices is one way to address this issue. However, even with a mutually-authorized consent approach, access must be well defined and strictly monitored and controlled. Access to non-specified devices that can pose a security risk must remain prohibited. In short, the firewall must remain intact to defend the organization against outside risks.

The second challenge for OEMs is the requirement for secure, seamless deployment and configuration. Since the deployment of remote monitoring devices is typically handled by personnel who are not necessarily network professionals, there is a risk of unnecessary downtime or potential errors that could adversely affect both the network and the equipment being monitored. Because of this, remote access devices and software must be easy to deploy and configure so that non-network professionals can initiate setup and manage it efficiently and cost-effectively.

## **Beyond Analog and Cellular Modems: Broadband Provides the Long-term Answer**

Until now, many service organizations have used analog modems to achieve remote access to the network and direct access to specific devices. Though this remains a typical method of connection, the very nature of modem technology makes an already challenging task more difficult. Though widely available at many speeds, modem technology is generally known to be slow and difficult to configure and manage. Modems have limited bandwidth and require a dedicated phone line which involves a recurring monthly charge.

Considering the issues with analog, cellular modem technology may seem like a more attractive solution, and in many situations, a cellular solution is acceptable. However, cellular modems come with their own set of difficulties. To begin with, cellular modems by their nature can be insecure. And, attempting to circumvent a firewall using a cellular router solution or “drop-in” network presents an ongoing issue regarding unauthorized access to areas of the network. Poor signal quality of the cell connection within buildings along with its limited bandwidth and availability prevents timely and accurate access to networked devices. Adding to these issues, cellular modems again contribute to unnecessary costs for organizations due to recurring monthly fees. In addition, cellular modems do not answer the deployment difficulties, thus resulting in added costs for an organization.

To achieve a totally secure Internet connection and help reduce costs, broadband technology is much faster and comes with few reliability issues. Indeed, broadband connectivity has become the standard for most of today’s businesses and home users alike. Because of this, it makes sense to leverage this existing network connection for a cost-effective remote access solution. Users enjoy the benefits of faster, higher bandwidth to achieve real-time access to information while administrators are able to audit access and activity effectively.

A broadband solution lays the foundation for the continuing evolution of managed services, including emerging and future “smart services” or “remote product services,” which will transcend simple connectivity. Data from networked devices can be easily gathered to improve business processes, manage proactive equipment maintenance and provide greater business intelligence for a broad range of improvements.

## **ManageLinx Provides Secure Remote Access for Firewall-Protected Environments in an Easy Plug-and-Play Solution**

Understanding the immediate need to resolve the firewall and integration issues, Lantronix now offers ManageLinx™. ManageLinx is an easy-to-deploy solution

*Lantronix ManageLinx*

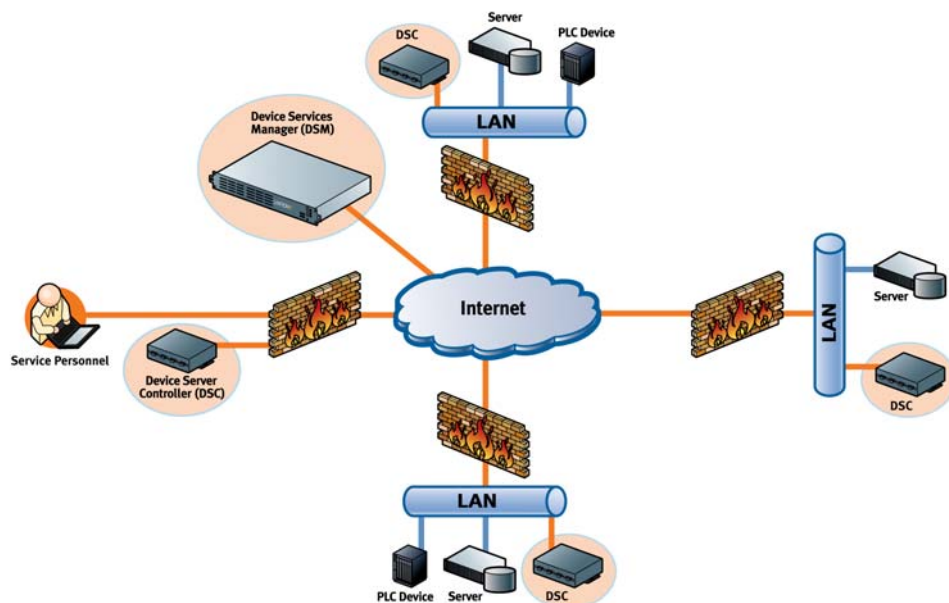
enabling service providers to securely access and manage thousands of networked devices across firewalls from a central point of access. ManageLinx is the only RPS solution to effectively address the access-through-firewall and remote deployment issues.

The ManageLinx solution from Lantronix consists of two distinct components – a Device Services Controller (DSC) and a Device Services Manager (DSM) to safely, securely and seamlessly provide remote access, management and control of any networked device behind a firewall – from anywhere on the Internet. The DSC acts as a point of presence on the local network and enables access to core device network architecture services. The DSM is a publicly accessible management platform. Both the DSC and DSM provide an extensible platform for OEMs wishing to deploy their own software solutions.

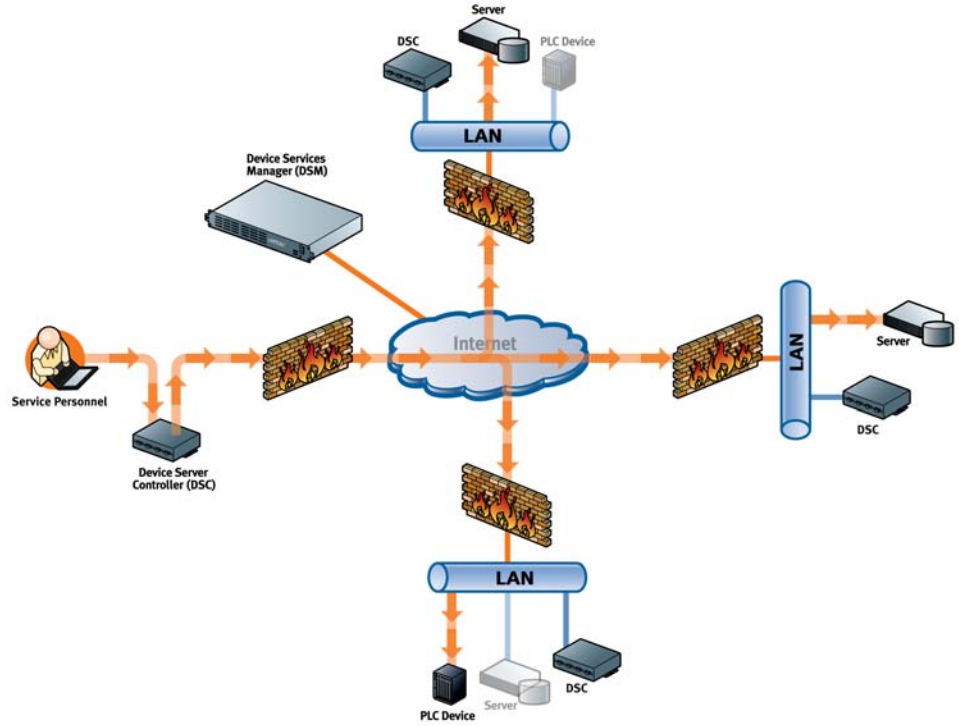
With ManageLinx, MSPs and OEMs can access equipment using existing software applications to remotely monitor product performance, diagnose part failures, trigger corrective workflows and carry out repairs. This provides them the ability to more easily and quickly create value-added service models for their customers – increasing their revenue and competitive offering.

Utilizing popular, everyday broadband connections, ManageLinx creates a “Virtual Device Network” (VDN) providing secure remote access to only specific IP addresses of authorized equipment, without visibility to any other part of the network or compromising IT policies or firewall integrity.

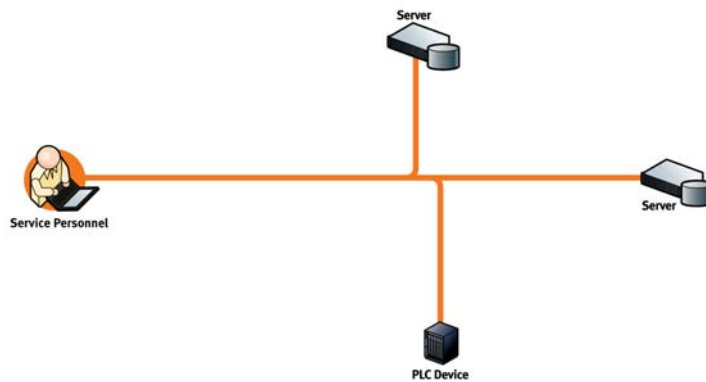
### Creating a ManageLinx VDN is as easy as 1-2-3!



Step 1 - Install ManageLinx VDN components



Step 2 - Create Virtual IPs (VIPs) and configure VDN routes on the DSM



Step 3 - Start using your new VDN!

### ***ManageLinx Features and Related Benefits***

With its advanced features integrated specifically to meet the needs of OEMs and MSPs tapping into potential outsourcing opportunities, ManageLinx enables service organizations to:

- Secure remote access to firewall-protected devices allowing organizations to leverage existing broadband connections and eliminate the need for dial-up access.
- Maintain existing IT policies and firewall integrity (no firewall holes changes needed) while retaining and protecting corporate network security.
- No special client software is required.
- Incorporation logging and audit trails providing regulatory compliance for SOX (Sarbanes-Oxley), HIPPA (Health Insurance Portability and Accountability Act) and SLAs.
- Certificate-based SSH (Secure Shell) encryption to ensure secure, end-to-end communication.

ManageLinx offers users the ability to isolate connected devices for complete administrative control.

Absolutely no on-site configuration is needed, making deployment simple and foolproof. This allows OEMs and MSPs to quickly and easily create value-added service models for their customers, thereby increasing their revenue and competitive offering. Remote DSCs can be configured automatically or with minimal effort. Initial DSC configuration is loaded using a secure configuration file via a flash drive, eliminating the need for a user interface on the remote device. Once power is applied to the DSC, all other needed configuration is automatically loaded over the network.

To begin communications, the host software connects to the appropriate “Virtual IP” (VIP) address associated with a route configured by the VDN administrator. This VIP connection is automatically routed through to the remote DSC to be delivered to the correct device.

### ***ManageLinx Target Applications:***

According to AberdeenGroup, as product-centric companies look to combat saturated markets and falling profit margins on product sales, they are increasingly wrapping post-sale services around their products to grow service-based revenues and profits. To enable these services, leading OEMs are evaluating and deploying Internet-based technologies that allow service organizations to remotely monitor product performance, diagnose part failures, trigger corrective workflows, and carry out repairs.

First and foremost, all RPS solutions require connectivity. ManageLinx provides a clear cost advantage over traditional RPS or virtual private network (VPN) solutions. Coupled with ease-of-deployment and flexible options, ManageLinx can meet the requirements of a wide range of applications including:

#### **Fortune 1000 Device OEMs with Large Service Organizations**

By utilizing ManageLinx, large OEMs can enable access and support for their own internal services. Deployment can be managed through an existing local area network (LAN) infrastructure for efficient resource management and reduced costs. In

addition, ManageLinx can help extend services to remote guest deployments on previously unserved locations outside the corporate network infrastructure that could not be serviced due to firewall access. This allows existing broadband connections to be leveraged without altering the integrity of the firewall and eliminates the need for dial-up remote access.

### **Operational Services for Industrial Control Companies**

ManageLinx enables industrial control companies with current revenue-generating remote services divisions to support their existing products. It also offers the opportunity to accelerate new, untapped revenue streams by including value-added services to equipment at customers' remote sites. For instance, companies can use ManageLinx to add Lantronix SecureLinx Spider™, a remote, distributed KVM-over-IP solution, to servers at remote locations with traditional device server-enabled equipment. Connected directly to the server, Spider provides non-blocked access from any web browser. Spider enables remote administrators to gain BIOS-level access to the server, perform maintenance and solve problems remotely.

### **Remote Monitoring and Security Companies**

ManageLinx enables companies that offer remote monitoring as a revenue service to lower the costs of their traditional RPS or VPN deployments. It also enables services, such as remote fire, environmental or intrusion monitoring, as well as building automation and remote energy management to be quickly and easily extended or added for increased revenue streams.

### **Small- to Medium-Business and SOHO Branch Office Locations**

ManageLinx can provide a cost-efficient solution for smaller edge locations that do not require complex, expensive VPN solutions, but still need reliable and secure remote access.

### **Telecom, Internet Service Providers (ISPs) and MSPs**

Future releases of ManageLinx will include service provider features and models to meet the needs of ISPs, telecommunication companies and MSPs to offer firewall-tunneled access to the low-end market as an additional revenue service.

## **Conclusion**

By solving the firewall access problem, a remote product services business model can easily and quickly be adopted and deployment of future value-added services can be accelerated. Businesses can fully leverage intelligence gleaned from networked devices to develop new revenue streams such as remote monitoring and management, and other specialized business intelligence applications. All this is possible with an end-to-end device networking platform, which can take the risk and complexity out of large scale machine-to-machine (M2M) deployments, and make full-scale device networking more affordable.