Access and Manage Equipment Behind Firewalls

ManageLinx™

Think it. Connect it. Control it.

LANTRONIX®

The ManageLinx Solution

Creating the Virtual Device Network

- Securely access and manage firewall-protected equipment… from virtually anywhere
- Save time, increase profitability and improve customer service
- Deploy with ease – no client software; no network configuration
- Maintain customer IT policy and firewall integrity
- Reduce technician service calls

Who Can Benefit from ManageLinx?

Product Support Divisions
Remote equipment service, warranty and maintenance programs

Remote Monitoring and Security Companies

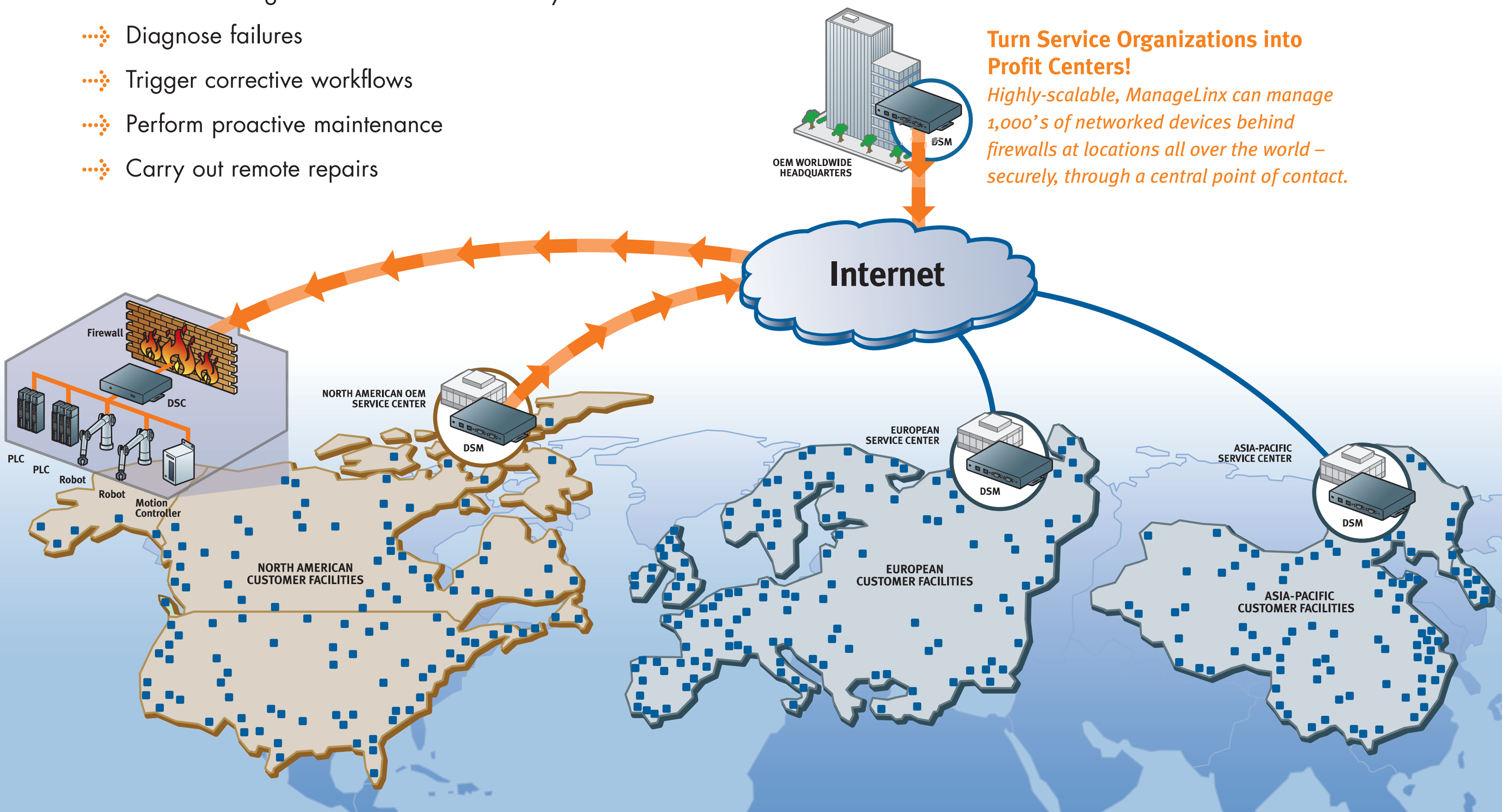
Managed Service Providers (MSPs)
IT infrastructure maintenance and management through customer firewalls

Operational Services Divisions
Access to firewall-protected equipment for contractors and MSPs

Network Access and Device Management for Remote Product Services

ManageLinx can host existing software applications enabling OEM/MSPs to remotely:

- Monitor product performance
- Receive notification of operational or status changes, service outages or anomalous user activity
- Diagnose failures
- Trigger corrective workflows
- Perform proactive maintenance
- Carry out remote repairs


OEM WORLDWIDE HEADQUARTERS
DSM
Internet
Firewall
DSC
PLC
PLC
Robot
Robot
Motion Controller
NORTH AMERICAN OEM SERVICE CENTER
DSM
EUROPEAN SERVICE CENTER
DSM
ASIA-PACIFIC SERVICE CENTER
DSM
NORTH AMERICAN CUSTOMER FACILITIES
EUROPEAN CUSTOMER FACILITIES
ASIA-PACIFIC CUSTOMER FACILITIES

Turn Service Organizations into Profit Centers!

Highly-scalable, ManageLinx can manage 1,000's of networked devices behind firewalls at locations all over the world – securely, through a central point of contact.

Features – Specifications

Device Services Manager (DSM)

Processor: Intel® Pentium® 4, 3.0 GHz
RAM: 512MB
Hard Disk: 160 GB
Ethernet: Two (2) 10/100/1000Base-T (RJ45)
Console: RS-232 (DB9)
USB: Four (4); front (2), rear(2)

Power Requirements: 100-240VAC, 50 to 60 Hz, 250W

Physical Dimensions (LxWxH):
1U, 35.6 x 42.4 x 4.3 cm
(14 x 16.7 x 1.7 in.)

Weight: 7.7 kg (17 lbs.)

Shipping Weight: 10.5 kg (23 lbs.)

Environmental
Operating Temperature: 10° to 35°C (50° to 95°F)
Storage Temperature: -40° to 70°C (-40° to 158°F)

Certifications
FCC, C/UL,TUV, CE

Warranty
2-year limited warranty

Device Services Controller (DSC)

Processor: Intel Xscale IXP420 Network Processor @ 266MHz
256MB SDRAM (can be configured with 32MB to 256MB)
32MB Flash (can be configured with 8MB to 32MB)
8kb EEPROM

Peripherals: 2 x DB9M serial ports
(RS-232/422/485) at 300 – 230 kilobaud
2 x 10/100 Ethernet 1 with PoE (Power over Ethernet)
1 x USB 2.0
1 x device Configuration/Reset button

Input Power: 9 - 30 VDC – barrel connector
802.3af compliant PoE

Physical Dimensions (LxWxH):
12.7 x 17.65 x 3.81 cm
(5 x 6.95 x 1.5 in.)

Weight: 0.86 kg (1.99 lbs.)

Shipping Weight: 1.3 kg (2.8 lbs.)

Environmental
Operating Temperature: 0 to 55° C (32° to 132° F)
Storage Temperature: -40° to 70°C (-40° to 158°F)

Certifications
FCC Part 15, CE (EN55022, EN55024, and EN61000-3), VCCI, UL/CUL and C-Tick

Warranty
2-year limited warranty

Ordering Information

Model Number	Part Number	Description
DSM2000	DSM200002-01	ManageLinx DSM (Device Services Manager)
DSC2204	DSC2204P2-01	ManageLinx DSC (Device Services Controller)

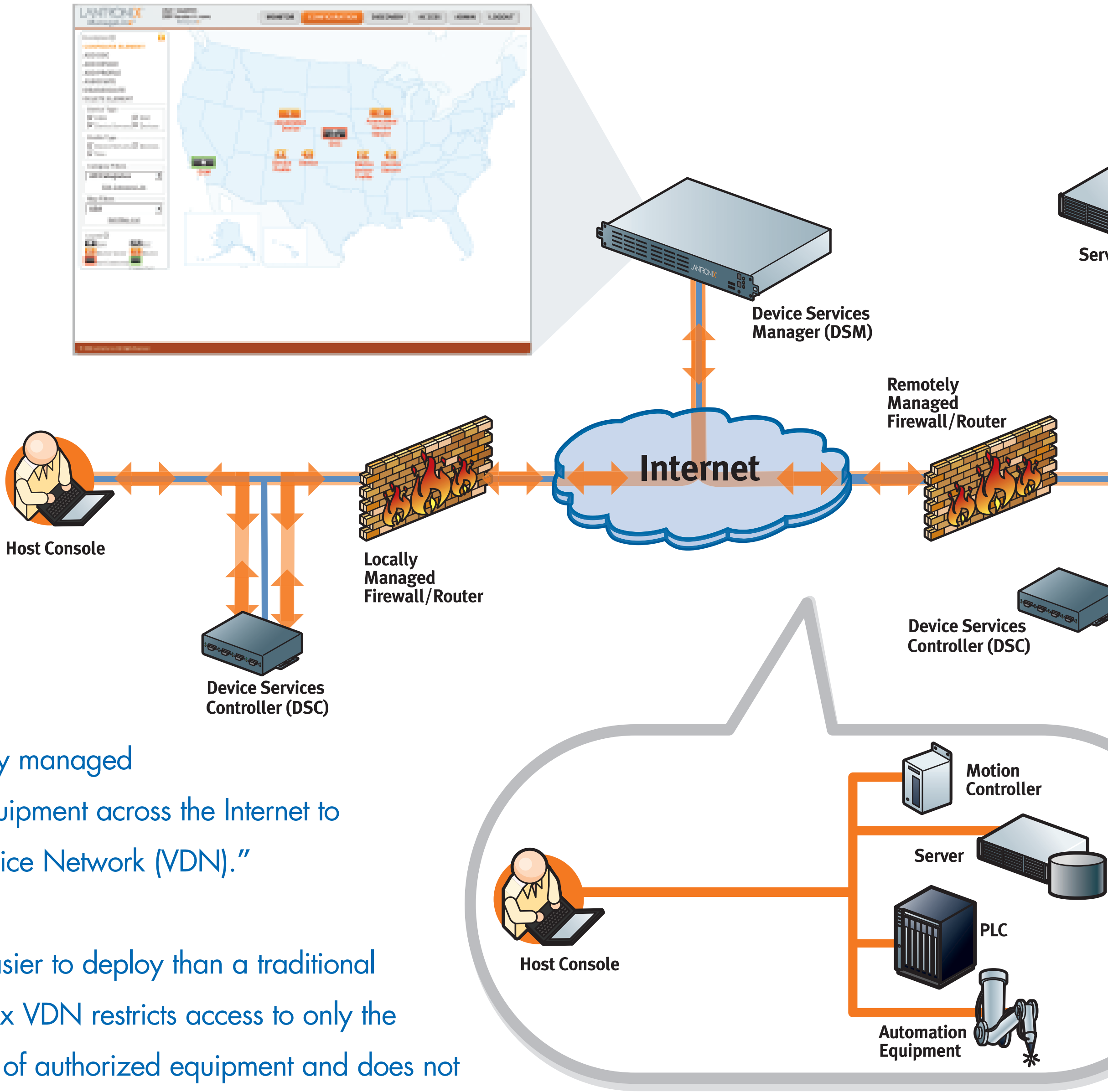
ManageLinx Customer Evaluation Program

Lantronix offers a comprehensive ManageLinx customer evaluation program. For qualified companies, Lantronix will provide up to three DSCs, capable of connecting to and remotely managing individual pieces of equipment. During the course of the program, the evaluating company will have access to a DSM server hosted at Lantronix headquarters in Irvine, California. The evaluating company will have a unique login and secure access to their managed equipment.

For more information, contact Lantronix at (800) 422-7055.

Simple, Highly Secure Access to Equipment Through Fire

ManageLinx is a powerful M2M (machine-to-machine) communications solution that provides secure remote Internet access to virtually any piece of IP-enabled equipment – even behind remote firewalls or VPNs. ManageLinx is a secure and easily managed solution that joins equipment across the Internet to create a "Virtual Device Network (VDN)."



The Virtual Device Network

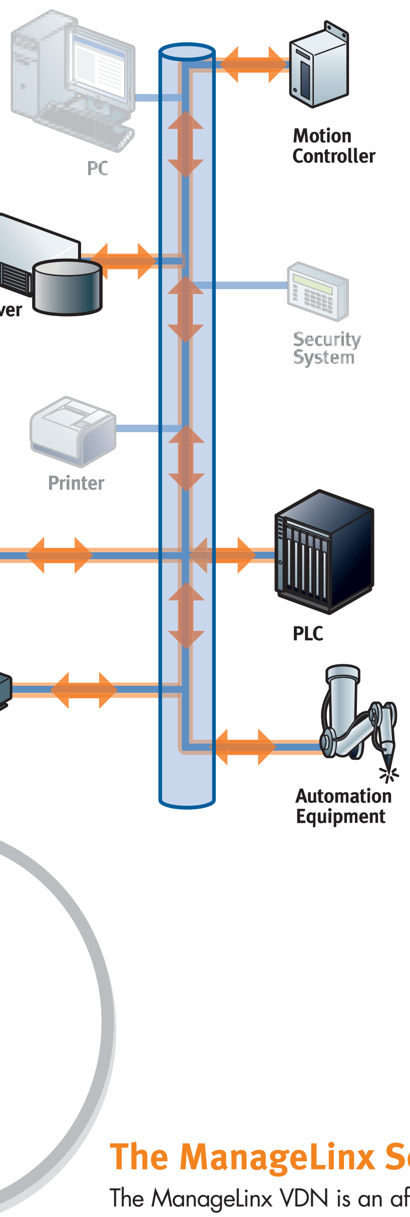
ManageLinx solves the 'access-through-firewall problem' and utilizes existing network infrastructure to create a Virtual Device Network. The VDN provides direct access to only authorized equipment, behind firewalls, from anywhere via the Internet.

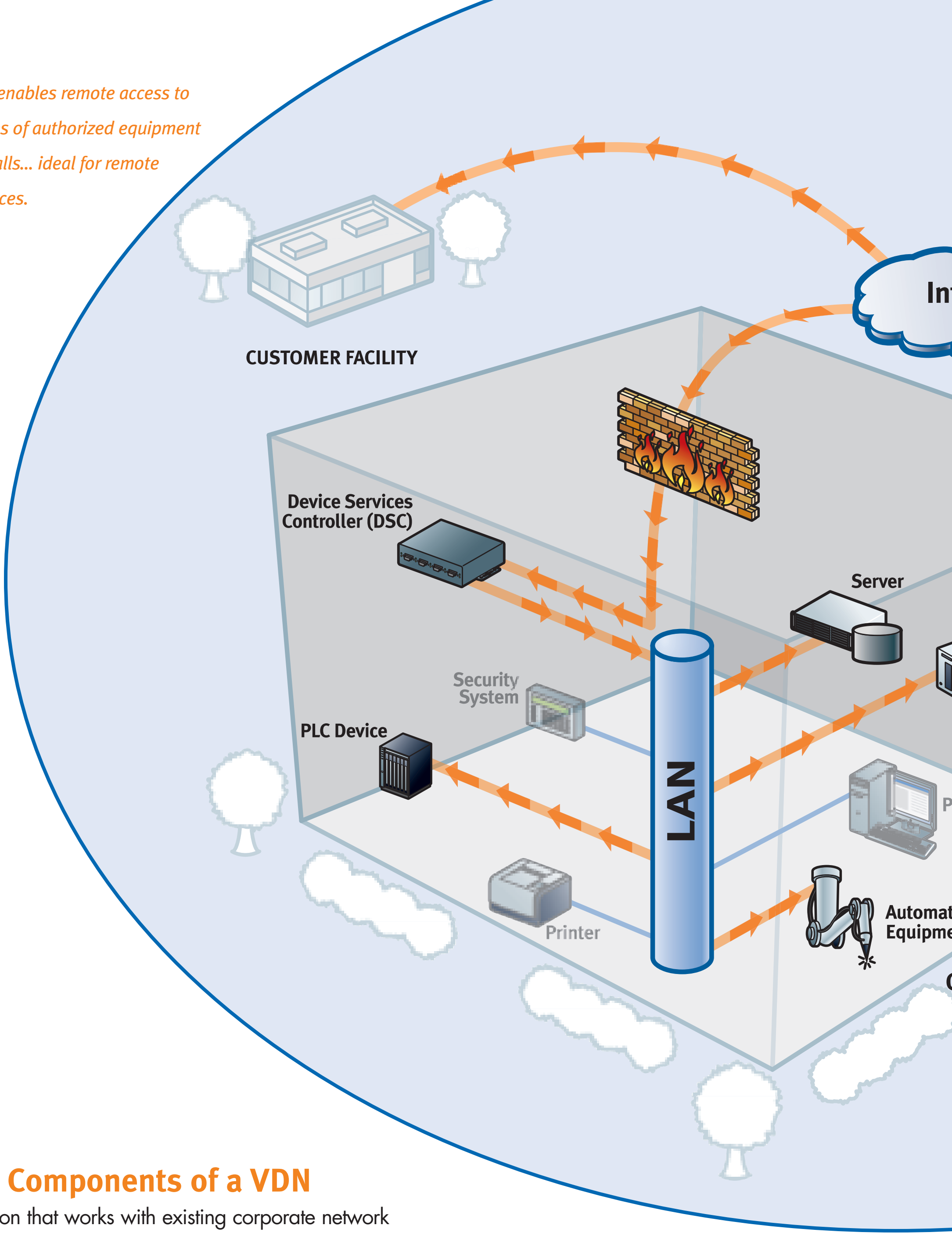
More flexible and easier to deploy than a traditional VPN, the ManageLinx VDN restricts access to only the specific IP addresses of authorized equipment and does not allow visibility to any other part of the network. It does not require any changes to network hardware or configurations. This makes it ideal for service organizations which need to access equipment on customers' networks for remote product support.

OEMs without an existing remote product service model can easily create a new, recurring revenue stream. Those with existing service programs can broaden their reach, accelerate service revenues, improve efficiency and offer a competitive advantage. And end-users benefit from a simple and highly secure solution that provides better product service while maintaining the integrity of their network firewall and IT policies.

walls

ManageLinx enables remote access to specific pieces of authorized equipment behind firewalls... ideal for remote product services.





The ManageLinx Solution – Components of a VDN

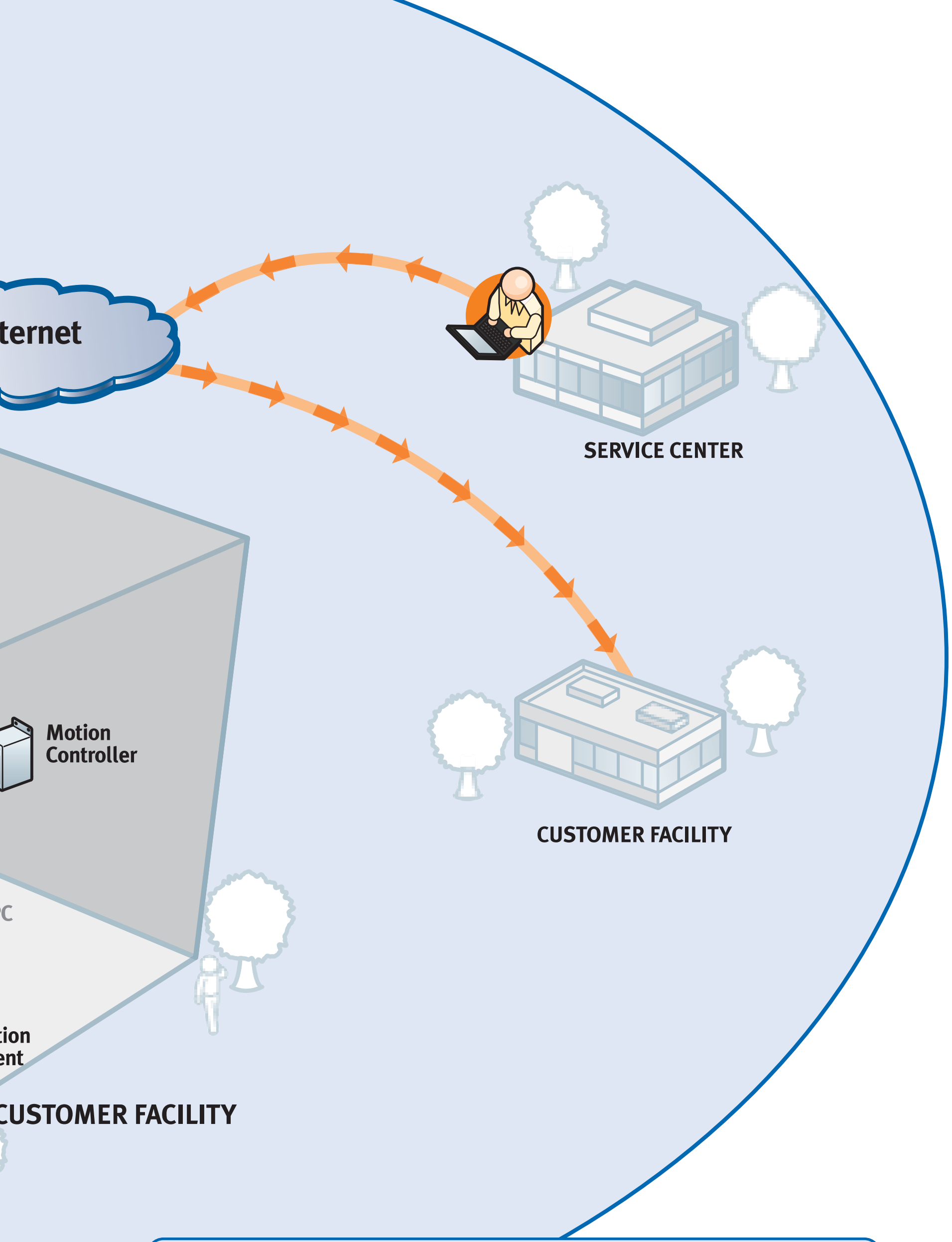
The ManageLinx VDN is an affordable solution that works with existing corporate network infrastructure to provide highly secure remote access to equipment through firewalls. The VDN hardware consists of a publicly accessible *Device Services Manager (DSM)* capable of managing individual *Device Services Controller (DSC)* appliances at each location. Together, these components enable the VDN administrator to discover remote devices, set up and manage individual Virtual IP (VIP) addresses and routes to allow access to individual devices from anywhere on the Internet.

Device Services Controller (DSC)

The Device Services Controller resides on the remote network and mediates communication onto that LAN. In *Device Controller* mode, it provides simple access as well as end-point encryption for all traffic. To provide secure end-to-end communications, a DSC sits on the LAN at each service center location. Operating in *Host Controller* mode, they provide a secure, scalable entry point into the ManageLinx VDN system. Once enabled, the Host/Device Controllers provide encrypted communication through the firewall.

Device Services Manager (DSM)

In addition to serving as a proxy connection point for participating DSCs, the publicly addressable DSM offers a complete Web 2.0-based management system for all system configuration and control. The DSM administrator can configure individual devices, set up automated device discovery on remote networks, perform automated monitoring and enable secure access to any device visible to a participating DSC.



ManageLinx™

How it Works

Many enterprise IT departments do not allow unauthorized third party applications to be installed onto their systems, so for many users current remote access solutions that require dedicated client agents, such as IPSec or SSL VPNs, are not an option. Another problem arises if the application involves remote M2M communications - dedicated VPN clients are simply not available for most appliance-based devices.

ManageLinx is different! Our patent-pending VDN technology enables users to create dedicated TCP/IP connections between any two points on the Internet using low cost, easily deployed hardware appliances. With no client software to install and no changes required to either the network configuration or application software at either end of the connection, ManageLinx provides a secure and totally transparent remote access solution.

The heart of the system is the DSM, a dedicated appliance that relays connections between user hosts and destination devices. Individual DSC appliances serve as a low cost point of presence on participating LANs. Each DSC is capable of acting simultaneously as both a Host Controller (which originates connections from host systems) and a Device Controller (which receives and manages incoming connections to individual remote devices).

To the remote network, a newly installed DSC functions like a newly installed computer. To access devices on a remote network the DSC just needs to establish a single out-bound connection to the DSM controlling the VDN. Once this connection is established, all system configuration, commands and network traffic can pass through the encrypted channel. When the DSC successfully authenticates to the DSM, it can immediately begin providing secure access to individual pieces of pre-authorized equipment.

Benefits of Remote Product Services

Manufacturers are looking to remotely monitor customer product performance, diagnose part failures, trigger corrective workflows and perform service repairs. Research shows that Remote Product Services (RPS) or "smart services" reduce service calls by 30% or more. With an average cost of $209, an organization with just 50 technicians making three calls a day can save $2.3 million a year. With 250 technicians, the savings jumps to $11.3 million! Other benefits include:

- 13.5% increase in asset uptime
- 14.1% decrease in mean time to repair
- 17.6% increase in service revenues
- 7.5% increase in service profitability

Source: AberdeenGroup

Fast... and Easy Deployment

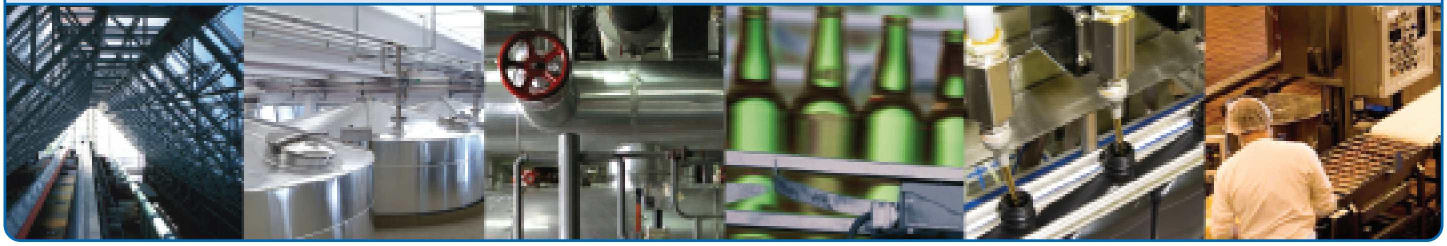
Deploying ManageLinx is simple with Lantronix patent-pending *Virtual IP (VIP) Access™* technology. No networking knowledge is necessary. No end-user configuration or software installation is required – simply plug in the power, plug in the Ethernet connection and insert a USB flash drive with the appropriate bootstrap file. That's it! After setup, the service provider can access authorized remote equipment without changing the network configuration or their customers' existing software. The Web 2.0 interface and built-in "Directed Navigation" system provides graphical views for easy navigation and control.

Bulletproof Security

ManageLinx maintains IT security policies and corporate firewall integrity. As a proxy between administrators and networked devices, access is well-defined and strictly controlled. Devices on the network that are not specifically authorized are invisible to the user. And to ensure accountability, audit logs maintain a record of both device configuration changes and user connections. To prevent snooping, all ManageLinx VDN traffic is encrypted from point of origin until delivery to the end device.

ManageLinx is ideal for:

- **Equipment hosted on other companies' networks**
  (can't install a VPN…limited on-site networking expertise)
- **Many sites, but have relatively few assets at each location**
  (more cost effective than high port count VPNs or switches)
- **Access "non-traditional" embedded resources**
  (automation and control equipment, security panels, VoIP phones, etc.)
- **More advanced level of network security not offered by a VPN**



Access and Manage IT Equipment Behind Firewalls

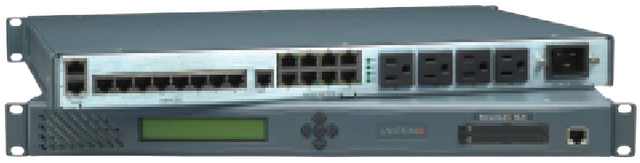
ManageLinx provides firewall access to any networked device, including IT infrastructure equipment such as servers or PBX systems. It can seamlessly integrate with other Lantronix products, including our SecureLinx remote IT management family, for a complete 'end-to-end' remote services solution.

SecureLinx Spider – KVM over IP

SecureLinx Spider™ provides secure remote KVM (keyboard, video, mouse) BIOS-level server management over an IP network. It is a flexible, scalable and affordable KVM-over IP solution in a compact, cable-friendly package. Spider guarantees non-blocked server access from any web browser and offers one of the lowest 'cost-per-remote-user' server management solutions available. And no client software or external power supply is required.

SecureLinx Branch Office Manager

This all-in-one utility for branch offices enables users to remotely manage Linux™, Unix® and Windows® 2003 servers, routers, switches, telecom and building access equipment over the Internet via their console ports. Built-in power management controls the power individually to all IT equipment for reboot, ensuring safe power distribution and reducing in-rush overload. This unique 1U appliance also includes an 8-port 10/100 unmanaged Ethernet switch.



The Virtual Device Network for Remote Product Services

www.lantronix.com

CORPORATE HEADQUARTERS
15353 Barranca Parkway
Irvine, CA 92618 USA
Tel: 800.422.7055
Fax: 949.450.7232
sales@lantronix.com
ftp.lantronix.com

Technical Support
Tel: 800.422.7044 (US only)
Fax: 949.450.7226
www.lantronix.com/support

Premier Partner Program
partners@lantronix.com

European Headquarters
2 Rue Helene Boucher
78280 Guyancourt France
Tel: +33.1.39.30.41.74
Fax: +33.1.39.30.41.73
europesouth@lantronix.com
eu_sales@lantronix.com

Technical Support
+33 (0) 1.39.30.41.72
eu_techsupp@lantronix.com

Germany
+49 (0) 2205.89.68.76
europecentral@lantronix.com

Technical Support
+49 (0) 180.500.13.53

United Kingdom
+44 (0) 118.924.2511
europenorth@lantronix.com

The Netherlands
+31.76.542.6977
europenorth@lantronix.com

Latin America & Caribbean
+1.949.453.3990
la_sales@lantronix.com

Australia & New Zealand
+1.949.453.3990
au-nz_sales@lantronix.com

Japan
2F, R & M Bldg.,
3-5-17. Kita-Aoyama, Minato-ku,
Tokyo 107-0061
Tel: +81.3.5770.4700
Fax: +81.3-5770.4788
japan_sales@lantronix.com

Asia/Pacific
Suite 1905 Lippo Centre Tower 2
89 Queensway Admiralty
Hong Kong
Tel: +852.2918.8277
Fax: +852.2918.8274
asiapacific_sales@lantronix.com

LANTRONIX®

910-536 01/09 PDF