UPLOGIX

UPLOGIX WHITE PAPER

Changing Network Management Best Practices Through Secure Remote Management

The complexity of managing data networks has increased over the last decade, but best practices for dealing with the challenges facing network administrators has yet to catch up.

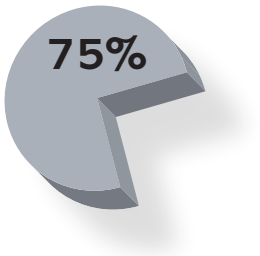
MARCH 2008

WWW.UPLOGIX.COM

Contents

Network Management Challenges

The fundamental flaw is a failure to embrace new technologies to reduce the amount of unproductive "routine tasks" and break/fix activities that are hampering the true goal of improving and innovating service delivery across the network. The scale of the problem is significant with analyst firm The Yankee Group estimating around 75% of IT resources are spent just maintaining the "status quo." As data networks transition to include voice and application delivery, these imperatives are forcing many organizations to reassess how they deal with the physical infrastructure of the network and to evaluate new tools and procedures to get the most out of skilled, but limited technical staff while also driving down costs.



Around 75% of IT resources are spent just maintaining the "status quo." —The Yankee Group

Compliance

Regulatory compliance is increasingly casting a net over every aspect of the business and the critical infrastructure that it runs on. The list of regulatory issues that affect IT infrastructure is growing across all sectors: common standards such as Sarbanes-Oxley Act (SOX) and the Payment Card Industry's Data Security Standard (PCI DSS) as well as industry-specific regulatory agencies like the Federal Energy Regulatory Commission (FERC) which sets certain compliance regulations for power generation. Many of these compliance standards have requirements which mandate the ability to secure, audit and control the usage of network elements and IT systems.

For IT directors, compliance is a mission critical requirement, but difficult to implement across a geographically dispersed infrastructure. Multinational companies face different compliance issues across the US, Europe and Asia which are made even more complicated by state-wide or country-specific requirements. In addition, differences in hardware or software applications as a result of mergers and business partnerships further cloud compliance issues.

Security

Although much of IT security spending is directed at securing the corporate perimeter against external threats, the security of the very infrastructure used to provide this barrier is often overlooked. According to a detailed study conducted by the FBI / CSI in 2006, 52 percent of companies experience unauthorized access to computer systems—but more worryingly—two of the top four types of security attacks are related to insider abuse or unauthorized access to systems.

Two of the top four types of security attacks are related to insider abuse or unauthorized access to systems.
—FBI/CSI

For IT directors, to achieve operational efficiency they must be able to manage more infrastructure per administrator and reduce the time consumed by routine or non-mission critical activities.

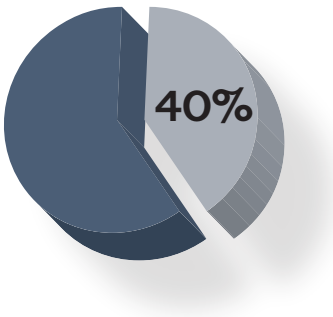
With an acknowledgement that the majority of serious security breaches are in part due to either negligence or malicious intent from within the perimeter—it is vital to secure access and changes made to key infrastructure elements such as firewalls, routers, switches, servers and other communications and network infrastructure.

Operational Efficiency and Downtime

As corporate networks converge to handle all application, email, and Internet and voice traffic—the cost of maintaining high availability is considerable. According to analyst firm Forrester Research, US companies spent in excess of $25 billion on network support personnel in 2006 alone and this figure is set to grow as networks expand across time zones and geographic boundaries. Throwing more personnel at the problem is an expensive and inelegant solution, but often the only viable alternative to the dire consequences of even a small window of downtime. For IT directors, to achieve operational efficiency they must be able to manage more infrastructure per administrator and reduce the time consumed by routine or non-mission critical activities.

Reactive Management

The combined effect of tough compliance, the need for tighter security and the magnified effects of downtime on converged networks is forcing IT directors to look at how they can do more with the same staffing levels and budget. In general, the response has been reactive with many organizations relying on network monitoring systems to generate alerts when things go wrong followed by a fire-fighter approach toward resolving problems. Network management software works well when the network is available but Analyst firm Gartner estimates that 40% of problems faced by network administrators cannot be addressed with in-band software tools.



40% of problems faced by network administrators cannot be addressed with in-band software tools. —Gartner

To counter the difficulty of hiring and retaining technical staff to manage the network, many organizations are turning to outsourcing as an alternative. The rational to shift the problem into somebody else's lap may well fix a short-term issue but does not solve fundamental process weaknesses in the management of the network. The common tasks of routine maintenance and break/fix still remain when outsourcing is in place and without good inherent processes, outsourcing is rarely successful in the long term.

Time for a New Approach?

For an IT director battling with these compliance, security and operational efficiency issues, what is needed is an integrated solution to allow the IT team to do more without having to rip and replace the existing network management platforms. To this end, secure remote management is a new emerging technology category that has been designed from the ground up to offer an elegant alternative to the reactive mentality which is pervasive across the network management landscape.

In the simplest terms, **secure remote management is a hardware bridge between the network operations center (NOC) and every network-connected element to securely and remotely perform common management tasks—even activities that traditionally require an onsite visit.** Secure remote management includes automation abilties to perform simple and mundane tasks quickly instead of wasting the time of a highly paid and skilled network administrator. As a physical access point connected to every network element, the secure remote management hardware is the logical junction to implement security and auditing functions by controlling:

1. Who has access to the network elements,
2. Recording what they do to each element and,
3. Maintaining an accurate and recoverable record of any changes.

Until recently, having an intelligent management device directly connected to each network element was not considered practical or cost effective. However, like the rest of the IT industry, advances in software development, and the reduction in hardware costs compared to the intrinsic value of the network is making the idea of true remote management and automation a viable option.

Secure Remote Management

Physical Description

Uplogix is the first vendor to deliver an integrated secure remote management (SRM) platform to market. The Uplogix Envoy is a Linux-based 1U appliance with onboard storage, battery and connectivity for up to 32 devices via serial or up to 16 devices with both serial and Ethernet connectivity. The unit has dual management interfaces via Ethernet and RS-232 console ports. Out-of-band connectivity is available via an integrated, onboard modem that supports multiple backup connectivity options including PPP/analog, cellular, and satellite. The unit is rack mountable

and connects via serial or Ethernet port to any other device in the rack. This can range from routers, switches, firewalls, satellite communications devices, wireless access points, power controllers and Unix, Linux and Windows servers (Figure 1).

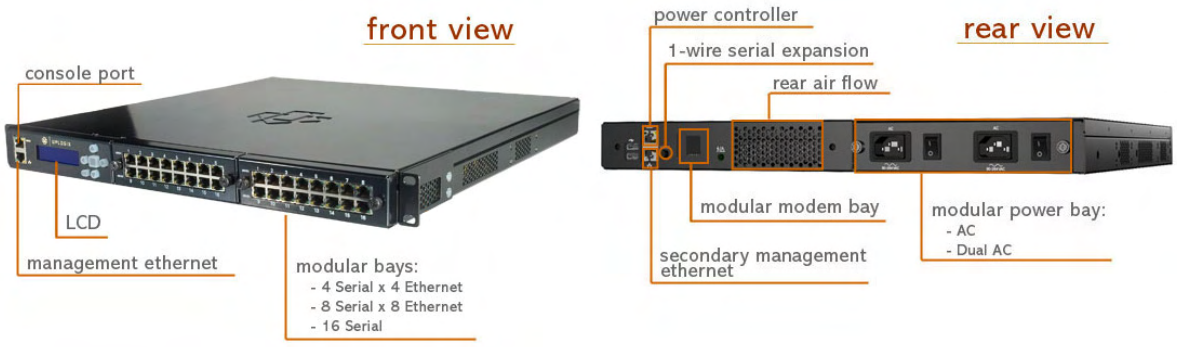


Figure 1: The Uplogix Envoy Remote Management Appliance

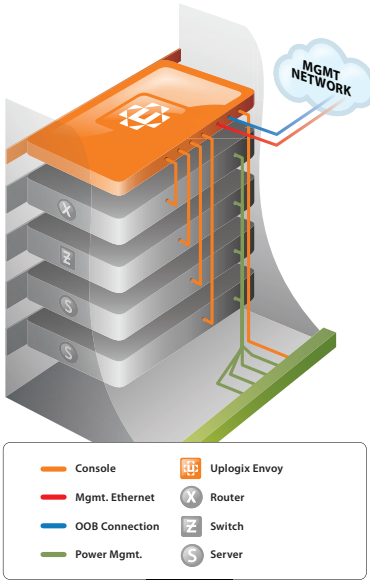


Figure 2: Uplogix Deployment in a Rack Environment

Typical Deployment Scenario

The Envoy appliances reside alongside physical equipment within data centers, branch offices and remote locations (Figure 2), and communicates with a centralized management server, called the Uplogix Envoy Management Station (EMS), via either in-band network connectivity or an out-of-band connection when the primary network is unavailable, to provide secure access, enforcement and control over any connected element. The EMS provides a full inventory of all Envoys and managed devices, including their real-time status—valuable information which can also be delivered to and integrated with existing network management systems such as HP Openview, BMC Patrol, EMC Smarts, SolarWinds and IBM Tivoli/Netcool.

The EMS also integrates with authentication, authorization, and accounting (AAA) systems such as TACACS, RADIUS, and SecureID to control access to network administrators performing tasks such as power cycling, system reboots, device OS upgrades and patches, configuration changes and local password changes. The Envoy can be setup to automate many of these functions using a set of rules, based on the managed device manufacturer's recommended best practices, or can simply act as a local,

secure and reliable conduit for an administrator to remotely perform these tasks. Either automated or with human interaction, all actions performed on any connected infrastructure device are logged and local backup copies of a device's configuration files and operating system are stored on the Envoy to allow rollback. The "rollback" or recovery function is vital as it allows a managed device to be returned to its last-known-good state in the event of a problem such as an improper configuration change, which renders the device inoperable.

All data collected from every Envoy and connected device is stored within an Oracle backend database to allow detailed reporting and analysis across the entire infrastructure from a single location (Figure 3).

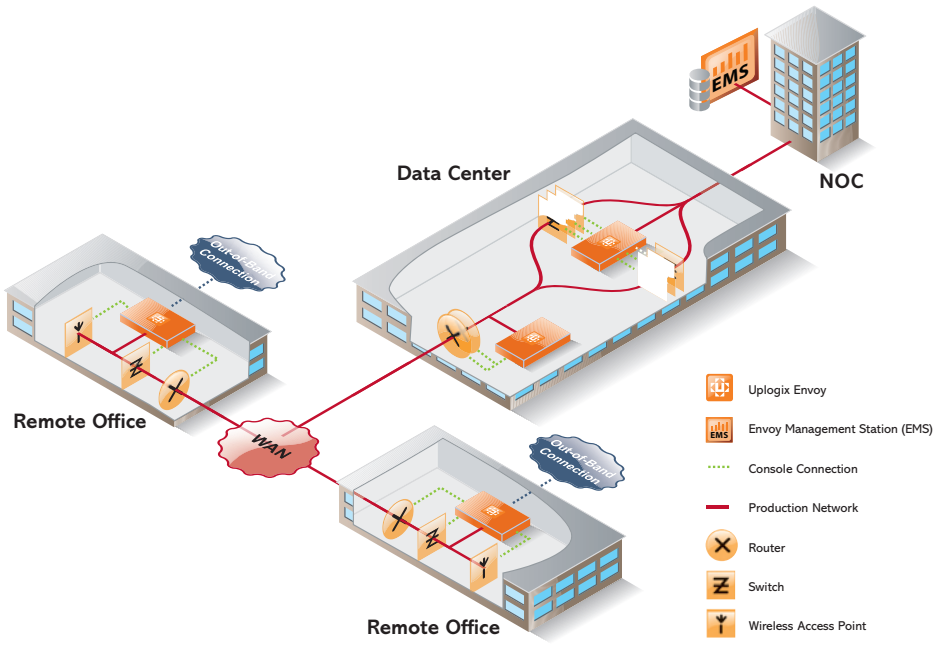


Figure 3: Enterprise-wide Uplogix Deployment

Strategic Use for SRM

For an IT director, the biggest strategic advantage gained in the deployment of SRM is complete visibility and control over network infrastructure irrespective of location. The secure remote management solution from Uplogix allows access to every network element at a physical console, power and interface level with every action performed on an element recorded such as who did what to which element and

what was the result? By recording such detailed information, Uplogix provides the ability to unequivocally answer pressing questions such as:

- Have all our switches been successfully patched to protect against a new vulnerability?
- Do we have full and complete auditing of who's accessing our network infrastructure and the changes being made to meet compliance regulations?
- Is our outsourcer meeting SLA agreements with respect to our network's availability and performance?

At the highest level, SRM is driven by policies that are enacted as part of the business process model. Levels of access, control and enforcement (Figure 4) are decided by the business with Uplogix providing transparent and role-based access to administrators, service delivery managers and security teams to perform only the duties permissible by their role.

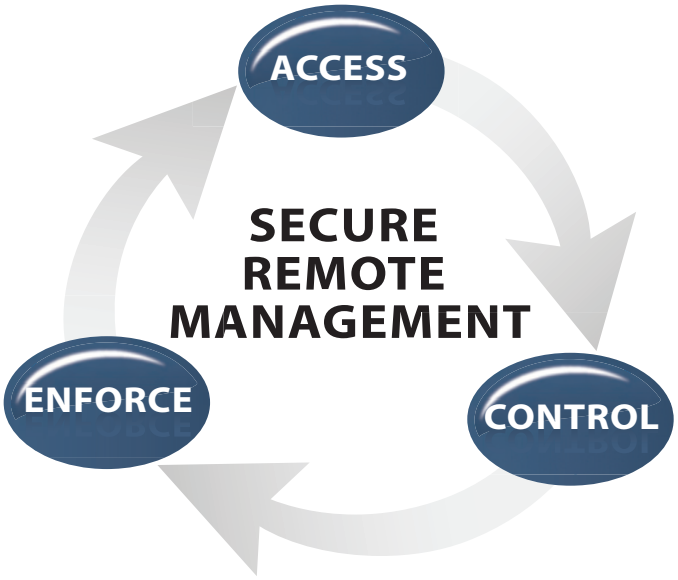


Figure 4: Secure Remote Management Requirements

Tactical Use of SRM

On a day-to-day basis, Uplogix solutions significantly improve the operational efficiency of technical staff across a wide number of areas. One of the most common uses is in resolving a network outage due to a device failure. Although switches and routers have improved in reliability over the last decade, hardware elements will fail, and if a failure is serious enough to break connectivity with a site, traditional software-based network management tools are unable to resolve an issue or even report status of devices at a remote site because they depend on the network itself being up and available in order to function.

The delay between the discovery of a failure and the enactment of break/fix procedures can often have a direct impact on productivity and ultimately revenue. For example, the failure of a switch carrying voice traffic can impede sales or customer service calls, or a poorly patched router at a branch office that fails and cuts of that remote site from the corporate network. A key requirement of a good network management solution is to be able to quickly locate which network element is causing the issue and initiate a targeted response. With the loss of remote site visibility, the out-of-band connectivity of Uplogix is vital in these types of situations as is the ability to pull detailed status information directly from the console of each device. This level of remote control will quickly allow for a number of recovery options such as power cycling which can often rectify an issue, rolling back settings to the last known good configuration, or shutting down or reconfiguring services to bypass a problematic device.

A key requirement of a good network management solution is to be able to quickly locate which network element is causing the issue and initiate a targeted response.

Another common issue negated by Uplogix is a failure of a planned configuration change that has made a device unresponsive, or broken a communication pathway. With large networks maintaining dozens of different types of hardware devices from multiple vendors, operating system upgrades, patches and configuration changes are a weekly, if not daily, occurrence.

Many larger organizations will insist on changes being tested on a non-production network first, but these “clean” environments are rarely able to completely predict the outcome on a more complex live infrastructure and issues still occur. Live environments tend to have higher volumes of traffic and subtle configuration changes that are not reflected in a clean install. In addition, unpredictable user activity or external issues such as a virus outbreak or a new vulnerability can have an adverse affect on a configuration change that was not foreseen during offline testing.

The EMS acts as central manager for enterprise-wide patching and system upgrades, and performs them in a secure and controlled way. If a patch fails or causes an issue, Envoy records all configuration changes to each device and can rollback every device to its last known good state either automatically based on an unresponsive state, or triggered via a user-issued command. In addition, a record of every single patch, upgrade and change is maintained to allow detailed troubleshooting if a problem becomes evident at a later time. Unlike software-based configuration managers which require access via the production network, the physically connected status of Envoy combined with out-of-and connectivity allows recovery even in the event of a critical failure that breaks the production network connection to the device.

Irrespective of activity, Envoy and EMS secures who has access to infrastructure and maintains an accurate record of what has taken place either via the production network or via out-of-band communication. This permanent record cannot be circumvented and is indelible evidence for senior management, auditors and service providers as to the real status of the network.

SRM in the Real World

Challenging Environments – Strategic Overview

Early adopters of the Uplogix secure remote management solution have typically emerged from many sectors. The example of RigNet, a service provider to oil and gas customers at locations across the globe, is an extreme example, but shares the traits of any organization with a large number of remote locations and a centralized management operational structure. Other early adopters with similar challenges include a well-known retail chain and a nationwide healthcare network. Although both less challenging environments than an oil rig, they share the same relatively high cost and logistical difficulties of deploying on-site technical staff to maintain systems and fix problems, and required an improvement in remote management capabilities to which SRM proved a natural fit.

RigNet

The primary responsibility of RigNet's operational team is to ensure that a customer's communications network is always available and delivering a high quality

of service. However, this is especially challenging to control in an industry where customers have remote sites, such as oil platforms, located in inhospitable and often hazardous places.

When communications go "off-line" due to an outage or service disruption, it usually means dispatching a RigNet technician via plane or helicopter to fix the problem—a costly, time consuming, and sometimes dangerous proposition. The same holds true when extensive maintenance has to be performed at a remote site, such as upgrading communications equipment to the latest software revision.

RigNet's executive team selected the Envoy management appliance and the EMS from Uplogix to meet their rigorous network support and automation requirements. Envoy serves as an on-site, virtual network assistant and is deployed at RigNet's teleport and POP locations to manage their internal infrastructure, as well as at end-customer locations to automate problem diagnosis and recovery, perform routine network maintenance and configuration, and ensure network availability, even when the primary connection is down.

Key Benefits:

- Automates over 75% of routine network support and maintenance tasks
- Remotely monitors and manages customers' hybrid satellite and terrestrial networks
- Out-of-band capabilities enable "always up"network availability

If a customer's main broadband satellite link goes down due to mis-configuration or other unforeseen circumstances, the Envoy at the remote, disconnected location automatically dials out to a low earth orbit (LEO) satellite via an integrated external modem to re-establish an alternate, out-of-band network connection to ensure constant management connectivity and availability.

The EMS is used by RigNet's staff to centrally manage all satellite and terrestrial network equipment from a single screen via the web-based portal. From the EMS, administrators can schedule and coordinate all network maintenance and management operations. In addition, the EMS serves as the central repository and reporting interface for all data collection and audit logs provided by the Envoys deployed at RigNet's customer locations.

Where Security is Paramount – Strategic Overview

One significant subset of SRM adopters cites security and compliance as key motivating factors. Financial services is one sector beset by regulatory concerns and although one early adopter has deployed Uplogix across a large part of its organization, the same security fears which its helps alleviate also requires its name to remain undisclosed. For a CIO or security manager, having a system in place which records all modification and changes to mission critical infrastructure is a major benefit. Uplogix solutions were built from the ground up to maintain and enforce authentication, authorization, and accounting (AAA) models. Considering that many of the most serious financial crimes are committed with assistance from within the perimeter, an incorruptible watchdog that see all and records all is a significant defense against internal security breaches.

Financial Institution

One of the world's largest financial institutions faced the challenge of managing a highly distributed and complex global infrastructure, while ensuring compliance with strict security and compliance standards. The bank's IT staff found themselves consistently failing internal security audits as a result of vulnerabilities introduced by the legacy terminal servers that were widely deployed throughout their environment to provide remote access to Solaris servers and networking equipment.

Unlike other remote access products, the Envoy appliances provide encrypted access both in-band and out-of-band.

After a competitive selection process, the bank chose the Uplogix Envoy solution as a tool to improve security and compliance standards. A key requirement was the delivery of out-of-the-box support for Secure Shell Version 2 (SSHv2), which leverages powerful encryption technologies to protect management communication with the bank's Solaris servers. Unlike other remote access products, the Envoy appliances provide encrypted access both in-band and out-of-band.

When the network is functioning properly, Envoy appliances use an in-band Ethernet-based connection to connect to the centralized management server, the Envoy Management Station (EMS). If this primary management link becomes unavailable, the Envoy immediately establishes remote connectivity using a dial-up modem, cellular network, or satellite communications; this secondary link offers the bank the same secure, encrypted access as the in-band connection.

Granular Control

The Envoy satisfied the bank's need to protect root passwords by providing command-level access control and simple role-based permissions to ensure that the right users get the right access to the right devices. While traditional console servers only provide port-level control over permissions, the Envoy can control every command inside the system on a per-user or per-group basis, giving the bank the ability to appropriately delegate responsibilities between the operations, engineering, and security teams in accordance with their management policies. The Envoy also integrates with remote authentication mechanisms, such as TACACS and Radius; if connectivity is lost, the appliances rely on cached authorization data to maintain permissions even during downtime.

Key Benefits:

- Encrypted management access to Solaris servers, both in- and out-of-band
- Granular, role-based permissioning with port- and command-level authorization controls
- Logging and compliance reporting of all user interactions, keystrokes, and changes
- Session management, such as ensuring the proper termination of user sessions to prevent unauthorized "piggybacking" sessions
- Centralized Management of the Appliances

Logging and Compliance Reporting

To ensure compliance with internal audits, the bank relies on the Envoy's robust logging and reporting capabilities. The appliance logs three sets of data, including console data from the Solaris servers and other networking devices, session data detailing user interactions with servers and devices, and change data that records any configuration modifications. The Envoy collects this data at all times—even during outages—to provide complete reporting.

Additionally, the Envoy delivers powerful real-time log inspection capabilities. This enables the Envoy to generate alarms or take automated actions when specific patterns are identified in the log data. For example, the Envoy might generate an alert when a user starts or stops a critical network service on a server or when a potentially detrimental procedure is run on a router.

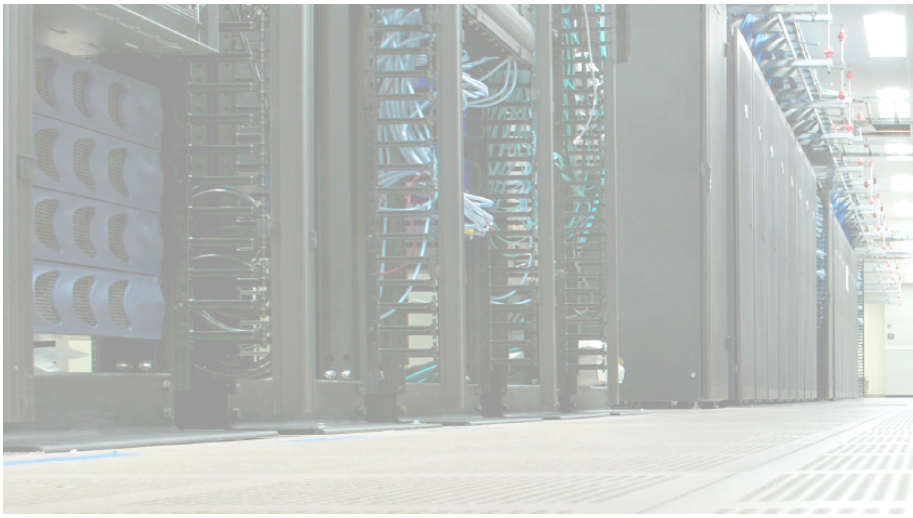
Call to Action

If you look at the core functionality offered by Uplogix, a number of familiar elements are observed. Hardware elements such as a traditional RS-232 console server and out-of-band technology found in a remote access solution combined with patch management software, network management tools, and event driven alerting. Uplogix takes the key elements of a number of existing technologies and integrates them into an elegant solution.

In the real world, getting software applications and hardware devices from multiple vendors and trying to get them to work seamlessly and transparently has always been a challenge. Uplogix takes the best of breed approach across a wide front of connectivity, security and network management technologies and integrates them into a single platform with a single management interface.

Real customers are streamlining operational activities without having to rip or replace existing management systems while IT directors are able to finally answer the big questions around the state of the infrastructure with information that is audited and accurate.

The growth of SRM is assured as it simply allows organizations to do more with less. However, the main stumbling block is not technical, but instead more of a personal or cultural issue. Through surveying a small sample of network administrators who are considering deploying SRM, one honestly expressed negative is that of fear. To paraphrase, remote management and automation could "put me out of a job." Although a natural fear, the reality of customers who have deployed SRM is the opposite: "This technology allows me to do my job better!"



The drivers for adoption of SRM are clear. Tougher compliance issues are forcing organizations to improve the processes and auditability around the management of critical IT and communication infrastructure. Convergence of voice, data, and application traffic across the same network amplifies the negative impact of outages. Tougher security needs to extend inside the perimeter to counter against negligent or malicious actions committed by supposedly trusted staff.

Uplogix delivers a solution that addresses these challenges and by providing a purpose-built architecture, instead of a patchwork of alternatives from multiple third party vendors that are often more costly to purchase, harder to integrate, and add an additional layer of complexity.

Early adopters aside, the majority of enterprises are starting to take notice of the need for a better way to managed distributed networks especially as more traffic heads onto the already congested network infrastructure. IT directors need to work out a long term strategy to cope with the next generation network and consider whether secure remote management has a place in the new network best practice.

For more information, please contact us:

info@uplogix.com

Toll free: 877.857.7077

Local: 512.857.7050

EMEA Office: 44(0)207 193 2798

Uplogix, Inc.

7600B N. Capital of Texas Hwy. Suite 220

Austin, TX 78731-1189

ABOUT UPLOGIX // Uplogix provides the first fully-integrated remote management solution. Our collocated management appliances automate routine administration, maintenance and recovery tasks—securely and regardless of network availability. In comparison, traditional network and systems management depends on the network, uses multiple tools, and remains labor intensive. Uplogix puts the power of your best IT administrator everywhere, all the time.

Uplogix is privately held and headquartered in Austin, Texas with European offices in London. For more information, please visit **www.uplogix.com**.

7600B N. Capital of Texas Hwy. Suite 220 | Austin, Texas 78731
T 877.857.7077 F 512.857.7002 | www.uplogix.com

UPLOGIX