A White Paper from the Experts
in Business-Critical Continuity™

Directed Circuits Meet Today's Security Challenges in Enterprise Remote Monitoring

Liebert®

EMERSON™
Network Power

Executive Summary

With continued efforts to reduce overhead, more companies are looking to outsource the monitoring of critical data center infrastructures as a way to cut costs and gain the expertise of service providers who offer this service as their core business. It makes sense for an automobile manufacturer, for example, to invest in employees who are experts at building cars instead of spending dollars on data center equipment and the personnel required to monitor and maintain it.

But the skyrocketing number of incidents involving security breaches and data theft are inciting IT security administrators to question the security and reliability of remote monitoring techniques. Identify theft is the fastest growing crime world wide, with the Privacy Rights Clearinghouse Chronology of Data Breaches reporting the number of personal records lost surpassed 100 million in December, 2006.

Within two months, 52 more breaches were reported, representing the loss of 3.6 million additional records to hackers and others intent on obtaining — and sometimes selling — personal information.

Mandates resulting from legislation such the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes Oxley Act have companies more concerned than ever about internal and external compliance. As a result, companies are seeking remote monitoring solutions that enable them to compile the documentation they need to perform internal and external audits while keeping IT equipment functional and data secure.

Introduction

Concerns about security have resulted in some companies keeping their enterprise remote monitoring functions in-house, with dedicated personnel monitoring equipment 24 hours a day. Financial institutions, for example, are frequently targeted by hackers and sometimes choose to lock down their IT systems and allow no transmission of data from outside their facilities.

While entrusting on-site employees with the task of monitoring equipment is certainly a secure practice, it is costly since someone must provide this service 24/7. In addition, in-house personnel may not have the expertise provided by a service vendor.

In one instance, a company with internal staff monitoring its IT system did not receive an alarm when battery capacity began to decline because the system's computer was set to hibernate after a certain period of time. Employees monitoring the equipment were not aware the computer had gone into hibernation. After the system went down, the company turned its IT monitoring function over to a service provider.

In the past, remote monitoring has been limited to dial up modems, dedicated private lines and virtual private networks (VPNs). Dial-up is somewhat secure but unreliable because the modem has to dial out to communicate alarm data. While dial-up service is relatively inexpensive, the process is slow and users still incur a monthly cost for phone lines.

Another problem with dial-up is that information transmitted from equipment contact closures is generic and does not provide enough detail for diagnosis and troubleshooting. Personnel, therefore, must be dispatched to the site to determine the problem. In instances where parts must be ordered, field personnel will be required to make two or more visits, which is time consuming and costly. The modem connection also represents a single point of failure.

Some organizations use dedicated private lines (T1, T3) to facilitate their remote monitoring function. While this alternative is secure because connectivity is point to point, it is very expensive.

Virtual Private Networks (VPNs)

Since firewalls are often a challenge when implementing remote monitoring solutions, VPNs are growing in popularity because they provide a secure tunnel through a corporate firewall. Most companies today use VPNs for employee and/or vendor/supplier connectivity, with costs varying according to how the VPN is implemented and the number of people connected.

Most VPNs include a concentrator, with separate PCs for every user and a shared password or token (such as a PIN) for gaining access. Maintaining passwords for a VPN is expensive since, for security purposes, user passwords are typically changed every couple of months, which requires individuals on the system to change their settings. Although tokens are costly, using both a password and a token — referred to as two factor authentication — is the most secure method of gaining access to a VPN.

Managing a VPN is time consuming because every person granted access must be added to the system, with passwords and/or tokens issued and policies or rules established. Companies typically manage what data users can access through the VPN since everyone who gains entry into the network will not automatically have access to all of the data available.

Since firewalls are often a challenge when implementing remote monitoring solutions, VPNs are growing in popularity because they provide a secure tunnel through a corporate firewall.

Directed circuits represent the best solution for enterprise remote monitoring because they are more secure and provide a superior connection compared to other remote connections, such as VPNs.

Employees, for example, may be able to access company and customer data, but suppliers and vendors will likely be restricted to areas that apply directly to them and the equipment or service they provide. For this reason, service providers administering remote monitoring solutions through VPNs must have a separate PC per client VPN connection with specific security access privileges issued.

VPNs also raise concerns about security because any time someone opens a wireless connection to the network; the network becomes vulnerable to attack. As an example, if an employee takes a laptop home in the evening to work on a project, a teenage neighbor could hack into the company's network while the employee has the VPN open.

In addition, VPNs are session-based; they are not "always-on." To facilitate 24/7 remote monitoring, the VPN must be nailed up, which means the tunnel is constantly open and the network vulnerable.

Recent legislation relative to protecting and managing confidential information requires that anyone accessing a network through a remote connection log in and receive a time stamp to facilitate both internal and more formal external audits. Many organizations require that VPN users employ both a token and password to gain access. VPN remote connection security audits have the potential to fail, however, because of uncontrolled encrypted access into the customer network and open in-bound ports on the enterprise's firewall.

Directed Circuits — Technology for the Future

Directed circuits represent the best solution for enterprise remote monitoring because they are more secure and provide a superior connection compared to other remote connections, such as VPNs. Directed circuits provide connectivity software that utilizes a unique outbound connection, ensuring mutual consent and security between the service organization and the enterprise IT organization.

Simple Network Management Protocol and Network Interface Cards

Some approaches include a simple network management protocol (SNMP) and a network interface card (NIC) that communicate the alarm over an Internet connection so the remote monitoring service provider can track information to determine trends in parametric data. Utilizing SNMP and NICs allows service providers to obtain a level of detail and intelligence that is impossible to achieve by pulling device alarms from equipment contact closures.

SNMP and NICs include very specific alarms that can be diagnosed remotely. Some send out a "heart beat" or signal at short intervals across an always-on outbound connection. This continuous communication check facilitates dynamic maintenance because if an alarm is generated, the provider will immediately send the customer a report so action can be taken. If a customer loses Internet connectivity or equipment becomes unplugged, for example, an alarm will signal the service provider and the customer will be contacted.

Today, NICs are part of the standard configuration for most data center infrastructures, including UPS units, generators and air conditioners. Even if equipment does not come standard with a NIC, alarm concentrator products are available that tap into contact closures and facilitate translation of contact closure data so alarm data can be communicated through a SNMP.

Directed Circuit Architecture

Directed circuit architecture includes a gateway appliance that secures and delivers alarms and parametric data through encrypted communication. The gateway appliance is designed for one specific task — to provide direct circuit monitoring of IT equipment. The appliance has limited access, meaning it will only monitor what the vendor has a contract to monitor. If the customer wants the service provider to monitor other equipment, the service provider will authorize the appliance to recognize the new equipment and then it will lock down the gateway again.

When an authorized technician wants to access a specific piece of equipment through the directed circuit, he or she must enter a user ID password and the gateway appliance will either grant or deny access according to the service contract. Access will be logged on both the vendor and customer sides to provide a documented audit trail for auditing purposes.

Parametric data is retrieved by downloading data at intervals to study trends and identify potential problems, which improves service response times.

The gateway appliance is designed for one specific task — to provide direct circuit monitoring of IT equipment.

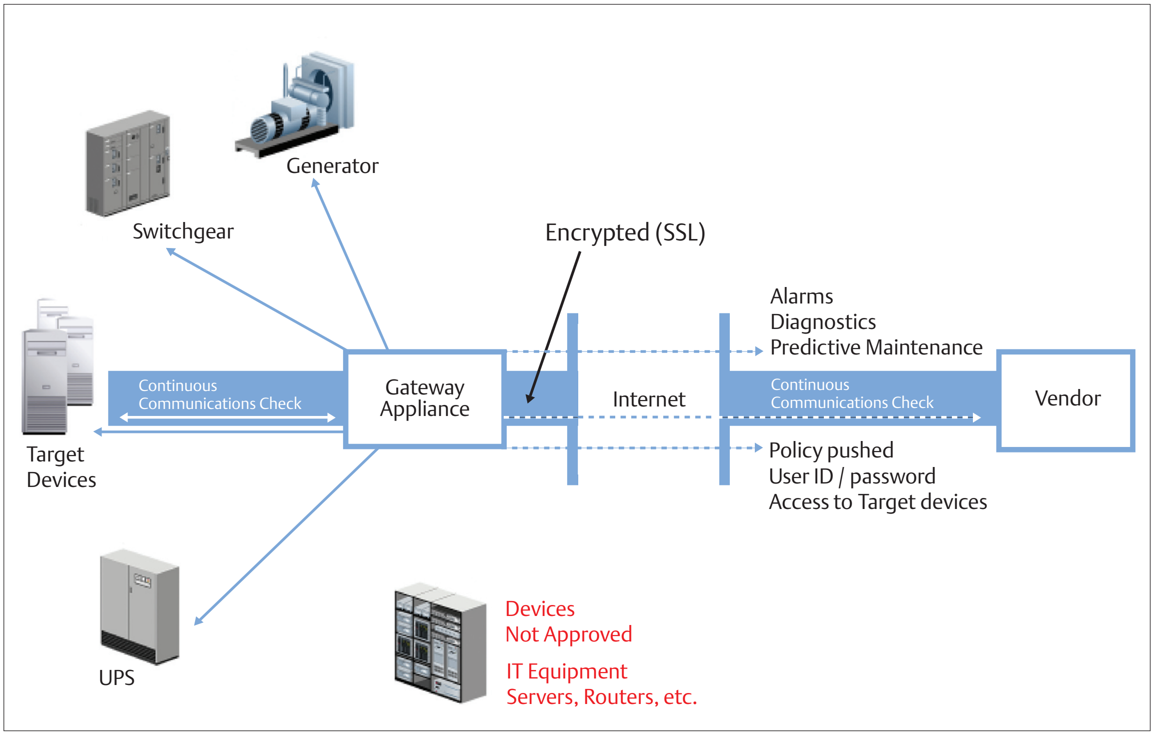

Figure 1. The Directed Circuit Automated Process provides an on-demand connection for authorized technicians and issues a documented audit trail for the customer and vendor.

Directed circuits represent the best solution because they increase security, enhance regulatory compliance and improve service response times.

Data may show, for example, that temperatures in an IT center are consistently high; the customer will receive a report indicating this abnormality. Data can also be used to monitor battery performance, with rising resistance and a decrease in voltage reported so the customer will realize the battery will soon need replacing.

Directed circuits are the most cost effective alternative for remote monitoring because they allow vendors to monitor hundreds of pieces of equipment over multiple sites. Other advantages include continuous verification of monitoring system integrity and elimination of on-site server and software licensing fees.

Conclusion

Although various options are available to facilitate remote monitoring of critical IT equipment, directed circuits represent the best solution because they increase security, enhance regulatory compliance and improve service response times. They also reduce costs for both the service organization and the customer because the service provider can monitor hundreds of pieces of equipment over multiple sites. And, there are no on-site server and software licensing fees.

Companies should keep in mind, however, that network security is more than protecting data from hackers and others. It is assuring that mission critical systems are up and available at all times and the power delivered to the data center is clean and will not interrupt the transfer of information.

Emerson Network Power
1050 Dearborn Drive
P.O. Box 29186
Columbus, Ohio 43229
800.877.9222 (U.S. & Canada Only)
614.888.0246 (Outside U.S.)
Fax: 614.841.6022

EmersonNetworkPower.com
Liebert.com

While every precaution has been taken to ensure accuracy and completeness in this literature, Liebert Corporation assumes no responsibility, and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Specifications subject to change without notice.