



**MARCUS
NETWORKING**
Technology & Telecom in One Company

ACHIEVE LEGISLATIVE COMPLIANCE

If you rely on your IT infrastructure to maintain data integrity and protect your business from financial losses, then it's important to invest in network monitoring and maintenance to achieve compliance with legislated standards.

Marcus Networking can play an important role in helping you achieve standards compliance and maintain the integrity of your IT infrastructure. Figuring out how to comply doesn't have to be complex and expensive. We're already familiar with the standards and our complete managed services model enables us to quickly identify any areas of your IT network that are not yet up to standard. To assess your level of current compliance, we'll conduct a non-intrusive network scan. The scan focuses on the seven key areas listed below, and is a great way to establish a baseline for making improvements. These seven areas (known as SAS70) have been defined by the American Institute of Certified Public Accountants.

IT REQUIREMENT	MARCUS NETWORKING ADVANTAGE
Controlled Environment	Industry-Standard Best Practices, Network Health Monitoring, Roles and Permissions Management, 24x7 Monitoring, Security Patch Management
Physical Security	SNMP-based Monitoring, Event Logging, Asset Discovery
Disaster Management	Readiness Planning via Reports, Performance Monitors, Backup Management, Collaborative Services
Availability	Continuous Monitoring, Remote Management, Deep Monitoring of Critical Servers
Information Security	ISO17799-Compliant Solution, Password Controls, Auditing, Intrusion Detection, Vulnerability Assessment
Network Security	Firewall Management, Microsoft Integration
Network Health Visibility	Summary Reports, Asset Inventory, Capacity Planning, Customer Dashboards

SOLUTION OVERVIEW

Our remote monitoring and management platform consists of:

Onsite Manager

A single, lightweight piece of software installed once at each site. Onsite Manager performs secure, comprehensive scans of your environment to gather the up-to-date information that Marcus Networking needs to manage your IT assets with unparalleled efficiency.

With Onsite Manager, we can monitor and manage anything with an IP address, including: desktops, laptops, servers, managed switches, routers, firewalls, gateways, VoIP switches and phones, printers, faxes or scanners, off-the-shelf and custom applications, environmental control devices and specialized equipment, internal and external websites, SaaS resources, virtual machines and much more.

Device Manager

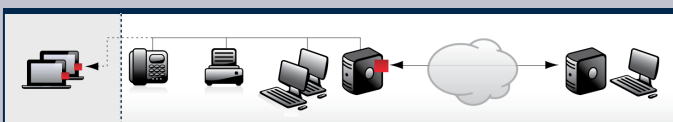
Installed on equipment that can't be directly monitored by Onsite Manager, such as roaming laptops, remote servers, home offices, or on an onsite Windows 7 PC if you don't have a server.

Service Center

A powerful, web-based, centralized dashboard that allows us to:

- view the asset health and performance data sent by the Onsite Manager;
- drill down to details as required;
- perform rapid remote remediation;
- configure advanced services;
- produce a range of useful reports so you'll know exactly what's going on in your environment; and much more.

With an Onsite Manager installed at your site, Marcus Networking can easily monitor the health and performance of your assets



DEVICE MANAGERS
@ Offsite Devices

ONSITE MANAGER
@ Your Site

SERVICE CENTER
Administered by
Marcus Networking

1208 East Broadway Road, Suite 106, Tempe, AZ 85282 ▪ 602.427.5027

www.marcusnetworking.com



THE ADVANTAGES OF IT EXPERTISE

From an IT perspective, compliance regulations ensure accurate disclosure of risk to investors and safeguard misuse of personal information. Companies must have effective processes in place that focus on security, privacy and assessment of risk.

ACT NAME AND DESCRIPTION

Sarbanes-Oxley (Sarbox)

Manage a secure and controlled infrastructure for data, processes, and historical information.

Gramm-Leach-Bliley (GLBA) and The New Capital Accord (Basel II)

Implement systems for security and authorized access, and build safeguards against threats and hazards.

Federal Food & Drug 21-CFR-11(21-CFR-11)

Ensure security, integrity, and availability of information. This is of particular concern to the health care industry that relies on the accuracy of patient / product information.

Payment Card Industry Data Security Standard (PCI-DSS)

Ensures network standards to reduce vulnerabilities, and protect cardholders from fraud. Five goals: maintain secure networks; protect transaction data; reduce vulnerabilities; implement strong access control measures; and regularly monitor and test networks.

Notification of Risk to Personal Data Act (NORPDA – US 2003), European Data Protection Directive (EUDP)

Ensures that an agency notifies individuals if their personal information has been acquired by an unauthorized source. The impact to IT is to improve security and reporting systems.

The Health Information Portability & Accountability Act (HIPAA)

Ensures patient record privacy by improving IT security and interoperability of information systems, as well as improved reporting systems.

Personal Information Protection & Electronic Documents Act (PIPEDA)

Balances an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes.

APPLIES TO:

Global

Public Companies

Global

Finance Sector

US

Healthcare Sector

Global

Credit Card Merchants

US and Europe

Any company

US

Healthcare Sector

Canada

Any company

MARCUS NETWORKING ROLE:

SECURITY, RISK MANAGEMENT

Monitoring for security, virus protection, intrusion detection, vulnerability management and user authentication. Asset management and error logging for audit trails.

SECURITY, PATCHES, PLANNING

24 x 7 monitoring for security breaches and vulnerabilities using industry standards for security. Alerts, patch management and remote management help ensure network availability.

SECURITY, AVAILABILITY

Secure environments and authenticated users. Reports indicate overall network health and help ensure the availability of data.

SECURITY, 24X7 MONITORING

24x7 monitoring for any intrusion or attempted unauthorized access, as well as system failures that could impact prompt response.

SECURITY, 24X7 MONITORING

Instant detection and notification of unauthorized access. Remote management allows for rapid action against intrusion. Patch management ensures up-to-date system security.

PRIVACY, AVAILABILITY, REPORTING

Best-in-class tools to ensure security and availability of network systems, as well as protecting them from unauthorized entry.

PRIVACY, REPORTING

Best-in-class tools to ensure security and availability of network systems, as well as protecting them from unauthorized entry.



CONTACT US FOR MORE INFORMATION:

Sales

602.427.5027

sales@marcusnetworking.com

www.marcusnetworking.com