

Network Management for VISUAL Webinar

Hosted by:

TrueFit Solutions, Inc.

800 Cranberry Woods Drive

Cranberry, PA 16066

(724) 772-5959

www.truefitsolutions.com

- Founded in 1997
- IT consulting and technology firm
- Consult, design, deploy, and support networks
- Provide custom development and web solutions
- Provide @Task Project Management Solutions

- Network Services Manager
- Chief Network Architect
- With TrueFit since 1998

- Demonstrate the importance of proactive network management in several key areas, including VISUAL ERP, and its impact on the bottom line
- Arm attendees with practical information regarding network management
- Challenge you to think proactively and help you get there.

- Business Impact of Reactive Network Management
- Best Practices: Network Management
- Utilizing Proactive Network Monitoring to optimize VISUAL productivity and staffing resources

The typical questions:

- Why do we care?
- Why should we do anything other than what we are doing now?
- Why is network management important to my business?

The typical challenge:

- Show me business impact.

To keep the network running smoothly, applications and data available to internal users and customers, and unauthorized people and programs out.

In short: To keep the business running.

So why do we pay so little attention to it?

- Ongoing costs and predictability
 - Costs too much to maintain IT systems now
 - Poor predictability for costs
- Excess downtime
 - Lost productivity
 - Costs to fix
 - Management time and effort to resolve
- Accountability
 - Who owns the problem?

- Networks seem to go down at the most inopportune time:
 - Month end
 - Deliverable due date
 - Important email
 - Lost productivity
- The fact is that network downtime, no matter when, impedes your ability to do business.

- Failures occur without notice
- Hard to plan your day when fighting fires
- Chaotic environment, everything is priority #1
- Frustrated users
- Need to justify all IT expenditures
- Time spent on tasks that should be automated leaving no time to improve systems
- Management dissatisfied with IT results

Being asked to do more with less.....

- Downtime effects your productivity
 - One hour of downtime for a \$4 million revenue company costs \$2,000
 - The average company in the U.S. experiences 2 hours of downtime per week

$$\mathbf{\$2,000/hour \times 2 \text{ hours} \times 4 \text{ weeks} =}$$
$$\mathbf{\$16,000/month}$$

- IT is the #1 variable expense after HR
- Downtime has become the #1 expense in IT

- Reduce preventable IT failures and their duration
- Predict and justify IT costs
- Improve employees productivity and reduce user frustration
- Reduce emergency service/support calls
- Reduce downtime

- How does my organization make this happen?

Proactive Network Management

- Most failures are preventable
- The signs are there, if you are looking
- End-user education along with proper environmental standards, design, and maintenance will create a POSITIVE perception of IT within your organization and keep people productive
- It starts with a network design based on business requirements

- The fact is, if a network is not designed to fit business needs, it will never create the productivity levels needed for success
- It's never a bad time to re-examine your network design and strategy if you are not 100% confident that it aligns with your organization's needs
- If the network doesn't fit the business, network management is moot

- Hours of operation (office, plant, branch offices in other time zones, etc.)
- Access requirements / mobility
- Mission-critical applications (VISUAL)
- Security requirements (must balance with access requirements)
- Connectivity / bandwidth requirements
- Client requirements (PC, thin client, etc.)
- Data Backup requirements

- Server vital statistics
- Server / application performance
- Antivirus system functionality and updates
- Backup system functionality
- Traffic / bandwidth analysis
- Patch Management

- Most of the time, it's the simple, little things that cause big problems
 - Disk space running low, applications crash and valuable time and data is lost
 - Security patches out of date, now you have a worm
 - Hard disk has been generating errors for a month, now it just failed

- Documentation trail is important
 - When did we install what patches?
 - Trending – why is our disk space utilization increasing 10% each month on SERVER1?
 - Why does SERVER2 have the same problem every week?
- Provides you with information you can use to make informed decisions
 - When to upgrade hardware
 - When to enact new standards or policies
 - Creates a solution-oriented environment, as opposed to reactive (duct-tape and chewing gum)

- Automation
 - Microsoft Software Update Services (SUS, WSUS)
 - Microsoft Systems Management Server
 - Managed Services platform (outsourced / internal)
- Automate tasks and create digital log of everything that happens on your network

- Real-time server, application, and network device monitoring to identify problems immediately or BEFORE they occur
- Monitor operating system, hardware, applications, network links, etc. and generate alerts when attention is required
- Alerting capability built into numerous applications (SMTP, SNMP, Windows Messaging, etc.)
- Managed Services platform – monitor it all and generate alerts / view activity from one central console

- Standardize (based on business needs)
 - Workstation hardware
 - Workstation setup and configuration
 - Server and operating system platform
 - Application set
- Document it!
- If users feel there are standards and documentation to support it, based on business needs, perception is more likely to be positive.

- Don't let the inmates run the asylum.
 - If the network is designed and managed properly, the IT staff can work on technology solutions that are driven by business needs.
 - Users will not assume that they need to develop their own solutions for their needs.
 - You will have the time and focus to stay ahead of the users' needs, instead of reacting to problems and fighting fires.

- Put first things first! (Thank you Mr. Covey)
- The first step is to reduce the need for support by being proactive about network design, management, and security.
- The next step is to put a mechanism in place to handle support in a cost-effective manner.

- Turn the problem upside-down:
 - The question is not: How do we handle the increasing support needs of our organization?
 - The question is: How do we reduce the support needs of our organization?

- The network is the foundation of our business, upon which all application functionality is built.

- There is always time to step back and examine network design, management, and security practices – if you focus on making time. A proactive approach will reap huge benefits down the road.
- Make it a corporate focus, because it impacts your financial reports every year.

- Security is a component of network management
- High impact on employee productivity (and hence the bottom line)
- Your data is highly valuable to your organization
- 'Black Hat' community is growing, and the tools they use are getting better and easier to use
- Introduce employee accountability into your network computing environment
- Impact on your customers

- The bad guys
- Well-developed toolsets
 - Virus kits
 - Knowledge of vulnerabilities in popular software
 - Use the Internet to collaborate
 - Don't need to be as technically proficient as the previous generations

- VISUAL applications not available to users
- Network or system outages (network is down, e-mail is down, PC is down)
- Performance impacted on infected computers (servers or workstations)
- 'Security-conscious' users invest time in safeguarding their own computers

- Your information is your money
- Cost of lost data: e-mail, databases, web sites, documents

- Not taking or shipping orders, or doing them manually and potentially creating human error
- Spread a virus or worm to your customers does not make you look good, and may cost you the business
- Services on your network may not be available to your customers

- Viruses/worms (including Trojan horses)
- Spyware/Adware/Malware
- Unsolicited e-mail (spam)
- Hackers
- Internal network users (employees)

- Understanding the threats is crucial to solving the problems.
- Hackers and employees may have a motive for their actions (revenge, 'fun', money).
- Employees may do damage accidentally if proper security measures are not taken.
- Viruses, worms, spyware: do not need a motive and act autonomously.

- All network servers should be under a patch management scenario
- Can be automated (Managed Services / Microsoft SUS) or manual
- Security-related patches and service packs should be kept up-to-date

- Many successful attacks occur because patches are not current
 - Blaster worm

- How does TrueFit's Proactive Network Monitoring provide a solution to the problems?
 - Near-real-time view of VISUAL components, server performance, firewall functionality, critical network services, database engines, backup and virus protection functionality, and network connectivity
 - Alerted to symptoms before they become problems

- How does TrueFit's Proactive Network Monitoring provide a solution to the problems?
 - Immediate identification of root problem – eliminate costly troubleshooting when network services are unavailable

- How does TrueFit's Proactive Network Monitoring provide a solution to the problems?
 - Historical view of past data for trending analysis and IT planning
 - How is my server utilization affected over time as we add users to the system or upgrade software?
 - What server hardware may need upgraded/replaced in the next year?

- Patch management
 - Have critical server updates performed on a pre-scheduled basis

- Solution Demo