



got visibility?

100% visibility is needed to manage a network for bottom-line results. You either have it or you don't. Congruity Inspector delivers 100% on-line operations visibility in a single automated reporting process. Inspector improves IT management with less effort, at a lower cost and with better results.

IT - Business Management Software

***Increase IT and Employee Productivity
Reduce Overhead and Operating Costs
Increase Bottom-line Results***

Automated Compliance Reporting

***GLBA, HIPAA, CIPA, FISMA, NIST
Comprehensive Penetration Testing
Consistent Change Control Process***

Congruity Inspector Software tracks how your network is used and performs and its impact on your business bottom line. Every detail is viewable via a centralized Web console enabling IT or executives to proactively manage technical and personnel resources to achieve desired results. Fully-automated operation makes it easy to use and cost-effective to own. Inspector logs traffic directly from the network, not from sys logs, presenting an objective summary of on-line business operations. On-demand access to information translates in to immediate productivity gains, lower overhead and reduced costs. All findings are listed based on network impact and importance. It's simply a better and more efficient IT - business management process.

Full Accounting Visibility

Network devices such as firewalls, IPS and filters can't report what they miss. Control devices are designed to stop certain traffic. They are not designed for comprehensive reporting and don't log the packet details which are needed to identify potential access control issues, misuse and data leaks. Inspector scans every packet entering and leaving the network providing full accounting visibility and reports: source - destination, port, protocol, service, application, content, bandwidth for all communications.

Content Visibility

Congruity Inspector performs content analysis on all Web use, Email and file attachments, identifying words and other user-defined content associated with on-line communications. The customizable dictionary allows you to create a lexicon of words related to your business to track relevant content. Inspector's full content indexing enables identification of policy violations and data leaks connected with specific user activity.

Cost Center Visibility

Two of the biggest cost centers in business are employees and network technology. Inspector provides visibility into on-line user productivity, network resource loads and IT service performance. 100% return on investment (ROI) is frequently achieved after first use thru reclaimed bandwidth/storage, risk mitigation, reduction of on-line abuse, non-business activity and SPAM, and the proactive management of problem systems and users.

Congruity Inspector Features: *100% visibility into all online communications *Fast Install *No agents *Automated operation *Centralized device-independent log *Zero effort regulatory compliance *Objective reporting with full disclosure *Affordable. For more information go to www.congruitytech.com



For more information about how to get 100% visibility into your IT operations, please contact us at: 303-800-5421



Use Cases and Benefits

Whether driven by internal users or Internet events, change is constant and requires regular observation. IT managers and operations personnel need 100% visibility into the network to manage proactively. The following use cases show how ***Congruity Inspector cuts operating costs while improving the network management process and productivity.***

Network Transparency: You need objective information to effectively manage. Inspector's automated device-independent reports provide network transparency into key performance areas. It enables clear separation of duty and job function so responsible parties can manage operations, technology and users.

- On-line User accountability: Email, Chat, Social Networking, Web use/abuse, disclosure
- IT/technician accountability: bandwidth, SLA, access control
- HR accountability: policy monitoring and violation documentation
- Executive oversight: centralized reporting dashboard

Change Control: Events can have a huge impact on network operations and employee productivity. Inspector provides in-depth information enabling you to assess and manage change events more effectively.

- Mergers & acquisitions, restructuring: document holes or problematic behavior
- Workforce reduction, layoffs: emailing or uploading of files and documents, sabotage, job searching
- Significant news events: streaming content, poor response times
- IT budget/staff reduction: demonstrate need for resource allocation
- Application Integration: measure load and impact on network and other applications
- Remote site connectivity: measure bandwidth, usage and performance

Regulatory and Policy Compliance: Regulated businesses must document their processes and ensure the security and confidentiality of IT systems and data. Inspector offers a consistent, automated process for documenting internal controls, policy and usage status, producing full-disclosure compliance reports and archives suitable for 3rd party audit review requirements. Inspector identifies and classifies policy violations such as:

- Excessive Web use
- Poor firewall rules
- Data leaks
- Email of personal financial/health information
- Circumventing corporate Email and filtering systems
- Gaming, social networking

Trust But Verify: Managing a network is complex and difficult. Inspector is a powerful defense-in-depth process for verifying systems status and control effectiveness under actual operational conditions.

- Web filtering effectiveness: URL-based filters do not identify the content in Web pages
- Spam filter effectiveness on Email system: Spam is constantly changing so filters must be tuned
- On-line Communications: what applications are in use to move information in and out of the network
- Verify who, when, how often exposed services are being accessed: foreign operatives accessing network

Network Troubleshooting: Inspector provides information to quickly isolate and correct problems without all the wasted effort collecting data. When problems arise, dig in, see all the data and fix it fast.

- Virus-compromised workstation: identify workstations sending out SMTP email directly to port 25
- Bandwidth consumption: see what applications are consuming the most bandwidth and when
- Failed network access: may be a sign of compromise or bad configuration
- Internal port scanning: identify compromised machines
- Unauthorized applications: see where unauthorized software is installed