

## Take Control of Your Network Traffic

### Stop network abuse with Total Traffic Control

Your network is being abused. Right now you don't know why, how much or by whom, but you know it is. And it's not just spam and porn that reduce productivity and threaten legal liabilities. It's the bandwidth-sapping (and often copyright-infringing) downloads of MP3s and DVDs, virus-infected laptops brought in the backdoor and unleashed on the network, excessive use of instant messaging or email, overburdened applications, and more.

Delivering a one-two punch with both extensive traffic reporting and all the tools to resolve detected issues, Lightspeed Systems Total Traffic Control was built to meet the demands of today's network environment.

### Detection + Resolution = Total Traffic Control

**Extensive traffic monitoring and reporting** gives you incomparable insight into your network anytime, anywhere using a web browser. Total Traffic Control **monitors everything** going in and out of the local network as well as everything running inside the network. The resulting detailed reports reveal your entire network's activity or an individual's activity so you know exactly what requires your attention.

View summary and detail reports to detect busiest protocols or applications, excessive downloads and uploads, top email senders and receivers, spam and virus activity, web surfing habits, and more.

Reports of an individual's network activity reveal protocols and applications used, files uploaded and downloaded, keywords used in search engines, instant messaging performed, and web sites visited with content category, web addresses and time stamps.

**Real security** measures detect and stop known and unknown attacks as well as detect and remove spyware and malware. With gateway intrusion prevention and client Security Agent software, Total Traffic Control gives you the power to:

- Stop known viruses, spyware, and malware with virus signatures at the email gateway and host
- Stop known network attacks at the gateway with intrusion prevention rules
- Stop unknown, or "zero-hour," threats by setting "program permissions"
- Easily add your own program permissions, virus signatures, and intrusion prevention rules

Virus signatures and intrusion prevention rules are contained in open databases that you may modify as needed with easy-to-use wizards. Updates from Lightspeed Systems are automatically retrieved daily or hourly. These updates are then pushed to all clients running the Security Agent on your network. All modern Windows operating systems are supported (2000, 2003, and XP).

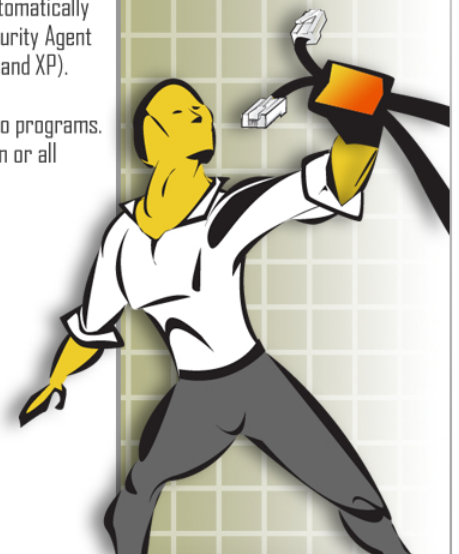
Unknown threats are effectively addressed by extending Microsoft's built-in security to programs. You can apply any of the following permissions to an individual program or to all known or all unknown programs. Permit program(s) to:

- Talk on the network
- Accept incoming network connections
- Write to another program's memory
- Modify other programs
- Execute other programs
- Modify critical registry entries
- Access critical system files
- Run at users' full security access

In addition to current processes monitoring, the TTC Security Agent also provides an inventory of installed and in-use applications.

### Total Traffic Control many tools, one vendor

- Extensive reporting
- Host & gateway security
- Spam blocking
- Content filtering
- Bandwidth management
- Firewall security



**Spam blocking** increases user productivity, frees up bandwidth and limits legal liabilities that arise when employees are required to use email that exposes them to offensive content.

TTC provides eleven proven lines of defense including:

- Application of your content filter rules
- Realtime Blackhole List (RBL) server lookups
- Virus scanning of the message body and any attachments
- White and black lists
- End-user whitelisting
- Bayesian statistical analysis to learn the latest spammer techniques and what your organization considers spam
- Adult subject-line scanning
- User-definable spam patterns for zero-hour attacks

Users may also be given access to manage their individual spam and whitelists. Taken in combination, you have the power to minimize false negatives and false positives network wide.

**Content filtering** detects and/or blocks access to inappropriate material on the Internet. TTC's content filtering has all the expected features (e.g., high-quality database, exception rules for users, times, types of files, categories, reporting), but is fundamentally different in many ways.

- Millions more categorized sites than leading competitors
- Database ownership, not rental
- Complete control of database
- Peer-to-peer application and file-type blocking
- Daily updates from Lightspeed Systems and your like-minded peers

**Bandwidth management** allows you to prioritize mission-critical applications like email, voice over IP, and accounting while limiting or blocking risky instant messaging and bandwidth-sapping file-sharing applications like Kazaa and BitTorrent. You can even prioritize or limit traffic directly from network reports. These measures also result in cost savings and high availability of Internet and WAN links.

**Stateful-inspection firewall security** protects your network resources using policies to manage traffic by user, group, IP address, application, DiffServ marking, time of day, URL, and many other options.

## Next Steps

- View live demo reports at: [reports.lightspeedsystems.com](http://reports.lightspeedsystems.com)
- Ask for a quote
- Get a 2 week trial
- Talk to someone
  - 601-319-5085
  - [jharper@howardcomputers.com](mailto:jharper@howardcomputers.com)

**No one else on the market offers such an inclusive network traffic management product.**

**HOWARD**  
COMPUTERS