<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Lightspeed Configuration</td>
<td>3</td>
</tr>
<tr>
<td>Security Agent Policies</td>
<td>3</td>
</tr>
<tr>
<td>Installation &amp; Update Source</td>
<td>6</td>
</tr>
<tr>
<td>Content Filtering Policies</td>
<td>7</td>
</tr>
<tr>
<td>Spam Filtering Properties</td>
<td>9</td>
</tr>
<tr>
<td>TTC Security Server Updates</td>
<td>10</td>
</tr>
<tr>
<td>Client Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Installation or Update Source</td>
<td>10</td>
</tr>
<tr>
<td>Outdated Operating Systems</td>
<td>11</td>
</tr>
<tr>
<td>Windows Updates</td>
<td>11</td>
</tr>
<tr>
<td>Disable Autorun/Autoplay</td>
<td>12</td>
</tr>
<tr>
<td>User Rights</td>
<td>12</td>
</tr>
<tr>
<td>Network Security</td>
<td>12</td>
</tr>
<tr>
<td>Firewalls</td>
<td>12</td>
</tr>
<tr>
<td>Switches and Routers</td>
<td>13</td>
</tr>
<tr>
<td>Network Shares</td>
<td>13</td>
</tr>
<tr>
<td>Case Study</td>
<td>13</td>
</tr>
<tr>
<td>Conclusion</td>
<td>14</td>
</tr>
<tr>
<td>About Lightspeed Security Manager</td>
<td>14</td>
</tr>
<tr>
<td>About Lightspeed Systems</td>
<td>15</td>
</tr>
<tr>
<td>For More Information</td>
<td>15</td>
</tr>
</tbody>
</table>
Introduction
Lightspeed Systems Technical Support has uncovered some very common issues with deploying our software and general network security.

This paper focuses on four main topics:

• Lightspeed Server Configuration
• Client Configuration
• User Rights
• Network Security

Addressing any one of these topics will help increase the security and performance of a network, but we encourage you to think about working with all of them as a whole.

Also, we strongly recommend that you implement your increased restrictions gradually during the testing phase. Naturally, if multiple changes are implemented at one single point in time, it will be more difficult to track down potential problems.

Throughout this paper we offer recommendations on configuring Lightspeed software specifically, as well as your network more generally.

Lightspeed Configuration

Security Agent Policies
Lightspeed Security Manager is an all-encompassing desktop security solution providing real-time virus checking, on-demand virus checking, registry monitoring, file integrity checking for PCs and Macs, and detailed reports of the workstations that the agent is installed on.

The Security Agent is the component of this solution that is installed on desktop machines. On the Total Traffic Control Server, extensive Security Manager reports with links to numerous Security Manager utilities support the effectiveness of the Security Agent by providing real-time tracking of:

• Active programs
• Management of unapproved and unknown programs
• Tracking of attempted security breaches
• Detailed software and hardware inventories (PC agent only)

BEST PRACTICE: Configure the Default policy before deployment.

Before you deploy the Security Agent across the network, it is essential that you plan how the clients will act once the product is installed. The Lightspeed Security Agent has many different options that must be
configured in the Security Server Management Console (SSMC). Here are some quick tips on items that should be addressed on the server before the client is installed.

*Policies > Property Sets > Security Agent Sets*

**Security Agent and Virus Update Sources** - Define this as your local TTC Security Server by an IP Address or DNS name. DNS name is preferable because a proper DNS name can be routed across the Internet, allowing mobile devices to receive the proper updates even when they're off the network. If this setting is left undefined, updates to the Security Agent will be received from Lightspeed Systems corporate server. As a result, you will not be able to manage the properties of any of your Security Agents.

**User Identification** - Enable this option to ensure the server will always know the username of the current logged-in account on the workstation. This field is highly important when trying to provide different levels of content filtering to a particular username, group, organizational unit, etc. See the Content Filter Policies section below.

In most cases, the Identification Server should be defined as the IP address of the TTC Security Server's Management NIC. In multi-server environments, define this setting as the IP address of whichever server the Security Agent and User Agents are configured to use as the ID (identification) server—generally the TTC Policy Server (not the Rocket appliance) that is used for content filtering. Note that the ID Server and the Security Agent Update Source do not need to be the same server.

**Active Protection / Virus Scanning Properties** – Enable active threat scanning. The default option is to *report only when a virus or spyware is found*. It should be changed to Quarantine the file or Delete the file to prevent a virus or spyware from continuing to try to execute.

**Scan Type** - To fully take advantage of the Lightspeed product, we strongly encourage customers to run a full initial scan on the client machine. We are aware that on certain client machines this full scan may take hours to complete, but the impact that it will have on viruses, spyware, and malware is worth the time of the initial scan. Lightspeed doesn't only rely on virus signatures to find bad programs on the Web. We utilize a vast database, which we have developed, that requires the initial scan before it can work.

<table>
<thead>
<tr>
<th>![Tip icon] TIP: Use imaged machines to avoid longs scan on each client</th>
</tr>
</thead>
<tbody>
<tr>
<td>If your network uses imaging software, we suggest that the client be installed, then a full scan (initial) run on this machine. When the scan is complete, make this the new image that is pushed out to other machines across the district. By doing so, your user machines will not require a long scan.</td>
</tr>
</tbody>
</table>

**Removable Media** - Removable media is a common way for viruses to come into a network. With this option you can allow or disallow the Read, Write, and Execute rights from these devices. Remember, removable media can be considered a floppy drive, CD-ROM drive, or thumb drive. You can also assign different rights based on usernames, organizational units, groups, and more. This means you can allow
your staff to have all access rights, while giving students only the ability to read/write to the removable media.

Exclusions - Under certain conditions you will need to exclude scanning of certain folders on your computer. You can enter these exclusions here. This should be used only when necessary, as it creates a potential security hole on your system. One example of where this is appropriate is if the Security Agent is running on your TTC server: you should consider entering the Lightspeed traffic directory under the Scan Exclusions (usually found in c:\program files\lightspeed systems\traffic). This way, the Security Agent will not harm the antivirus capabilities of the TTC spam filter when the Security Agent is installed on that server. Another example is to exclude folders on servers for Microsoft Exchange or Microsoft SQL Server.

Categories – The Lightspeed Security Manager categorization system is a huge advantage over many other types of applications. For each virus, malware, and spyware program Lightspeed discovers, both a signature and a FileID are created. A virus signature takes a little time to complete; however, a FileID can be created instantly when a bad program is discovered. Because of this, locking down the machines will help unwanted programs from being run.

Local Administrator Access - These options help increase or decrease the users’ awareness of which product is installed on their computer. For instance, Show System Tray Icon will display a Lightspeed-based logo, so the user has the ability to open the properties options locally.

Disabling the System Tray Icon is the best method. If possible, the network administrator should also refrain from disabling the option to "Enable Security Agent properties changes by local administrators."

TIP: Use My Big Campus Personal File Storage
If your district uses My Big Campus, users can store their files there using the unlimited file storage feature. This allows students to share and access files, and pass them along to their teachers—eliminating the need for removable (and potentially contaminated) media.

TIP: Know what you’re blocking with Audio-Video and Security.nettools categories
Sometimes users opt to block the Audio-Video and Security.nettools categories. The Audio-Video category will block programs like QuickTime, Windows Media Player, and Flash Video player. The Security.nettools category will block programs like VNC. Be generally aware of what these categories mean before changing the Lightspeed Security Manager default policy.

NOTE: Virus and FileID updates
The Lightspeed TTC Security Server receives new virus and FileIDs every 30 minutes through the critical update process.
With this setting disabled, even if the user accesses the local properties page, he/she will not be able to change the settings.

**Use Super Clients** (Available under Advanced Options> Super Clients) - If your network is large, updating every security client back to one server can cause network performance issues. Although Lightspeed has the ability to allow machines to get updates from different servers, Super Clients provide an alternative that increases network performance by decreasing the bandwidth needed to run updates across the WAN.

At remote sites with hundreds or thousands of clients, select a machine to act as the Super Client—the update source for the location. Now the site's clients no longer need to cross the WAN to get updates from a centralized server.

For example, if you had 20 remote locations with 5,000 computers on each, you could have 20 Super Clients. This way, when the TTC Security Server pushes out an update, it will only need to push it to 20 Super Clients. Then, the 100,000 client machines would get their updates from their local Super Clients. This helps with the security of the network, and it conserves bandwidth to improve network performance.

**Installation & Update Source**

**BEST PRACTICE:** Ensure that all clients have the Security Agent installed and that Security Agent updates come from right source.

Many issues with Security Manager are simply a result of the Agent not being installed on all machines, or not being configured to get updates from the proper source. There are many different ways to deploy the Security Agent across an Active Directory or Novell network. The most troublesome problem that we have seen is that the clients are being installed, but they are not being pointed to the proper update source. This means that if you simply download our Security Agent package and install it on system machines, those clients will automatically be pointing to our corporate servers—not your local TTC Security Server.

**TIP: Virus Scan Scheduling**

Be sure to configure the scan time for a time when the PC is likely to be turned on.
Content Filtering Policies
While Internet filtering is typically used to block inappropriate content, it is also useful for adding an extra layer of network security.

BEST PRACTICES: Ensure name resolution; block security risks; and block proxies that can bypass the filter.

Name Resolution
Client Agents - Use one of the Lightspeed client agents, the Security Agent, or the User Agent to guarantee that the TTC Server knows who is logged in at every workstation. This will ensure that users get their assigned policy without having to prompt them for their network username and password.

Authenticate Unknown Users - Mobile devices with Internet capabilities, such as the iPhone, iPad, and iPod Touch, pose a potential threat to school networks. If there are no security measures in place (e.g., 802.1x authentication, etc.) to deny personal machines access to the network, then consider using the Authenticate Unknown Users option under Properties > Content Filter > Properties > Authentication. Forcing unknown users to authenticate with their network username and password before accessing the Internet will ensure their web traffic is reported correctly and controlled by the correct policy.

TIP: Use only LTDP authentication
Once you deploy the client agent, go to Tools > Administrative Tools > User Resolution Settings and uncheck all authentication methods except for LTDP. This will help to ensure the proper authentication method is used.

Blocking Content Based on Security Risk
Property Set > Content Filtering > Normally Blocked Categories > Security
The websites included in the Lightspeed Security categories promote ways to hack websites and networks, cause harm to the network infrastructure, and bypass content filtering policies. Additionally,
many of these sites contain harmful code that attempts to install malware. The following Security categories should be blocked in order to stop these kinds of threats to your network.

**Parked** - Pay-per-click hosting websites that park expired domains make up the websites in this category. In almost all cases, users are not trying to access these websites; they have simply mistyped the URL. In the Internet's early days, a 404-error page would display saying the website cannot be found. Now, some folks count on the fact that people mistype web addresses and use the mistake to generate business and drive people to the proper website. They can get paid per click-through. Why would we want these sites blocked? In many cases, spyware can get installed, pop-up ads will open, and the user will become vulnerable to content that wasn't being sought.

One example is Chevrolet's website. The URL [http://www.chevrolet.com](http://www.chevrolet.com) displays the corporate website for Chevrolet, the automotive company. Switch the "o" and "e," though, to [http://www.chevrelot.com](http://www.chevrelot.com), and it redirects to [http://carsarecool.net](http://carsarecool.net), which is a spam website full of links to useless search results.

**Security.warez** - Sites in this category promote illegal access and sharing of software and other copyrighted material. Proactively blocking illegal downloads can help protect a school from lawsuits.

**Security.phishing** - The goal of these scam sites is to get a user's personal information. Often a phishing site appears to be a legitimate site, and users are prompted to type in their name, address, phone number, credit card information, social security number, and more.

**Security.spyware** - Sites in this category are known to spread advertising-supported spyware.

**Security.Virus** – The Lightspeed content-engine software scours our website database for any new virus, malware, Trojan, backdoor, hacker tool, or other harmful application.

**Security.hacking** - Blocking hacking websites is much like blocking access to the security.warez sites.

**Security.proxy** - Anonymous proxies have become a common problem for every network administrator as students and staff attempt to bypass the filter and access blocked sites.

**Blocking Access to Anonymous Proxy Servers**

*Property Set > Content Filtering > General*

Anonymous and secure proxies are frequently used to bypass content filtering policies. Follow these steps to combat their use.

**Block Search Engine Keywords** - Blocking users from searching for a variety of keywords can be very helpful. For example, you can choose to block searches for "proxy" and "proxies" so users don't have access to a list of potential proxy websites.

More information: [Wiki Article 10793](http://example.com). This article includes a list of commonly blocked keywords.

**Block non-HTTP traffic to blocked IP addresses** - When blocking content categories, the content filter blocks users from accessing websites via the HTTP protocol. There are many other protocols that can
allow users to bypass your content filtering policies, such as HTTPS, RDP, VPN, SSH, and more. This option blocks all connections to an IP address, regardless of the protocol, if that IP address is in a category that is set as blocked.

(Will this stop your users from accessing online banking or secure access to valid websites? No, because those IP addresses are usually in categories that we are not blocking. The only time this option will take effect is when the IP address is in a blocked category for the corresponding policy's property set.)

**Block unknown URLs** – Every day thousands of new websites are created. Choosing to block all unknown URLs eliminates the risk of encountering an inappropriate or unsecure site. To minimize over-blocking, the TTC Server tracks each requested unknown URL. Every evening, the TTC Server uploads these unknown URLs to the Lightspeed server farm, where they are analyzed, categorized, and then pushed out to all TTC Servers via the nightly database update.

**Block unknown URLs matching proxy patterns** - Specifically created to help address the new anonymous proxy servers, this option will detect requests destined for anonymous proxy websites based on the signature of the traffic. This option should only be enabled if the Block Unknown URLs option is *not* enabled.

**Blocked file extensions** - If you choose not to block unknown URLs, Lightspeed recommends using this option, which allows users to access the content on the unknown website while denying them the ability to run or download various file extensions (e.g., .exe, .flv, .zip).

**Block search engine keywords** - Blocking users from searching for a variety of keywords can be very helpful. For security purposes, you can choose to block searches for "proxy" and "proxies" so users don't have access to a list of potential proxy websites. See [Wiki Article 10793](#) for a list of commonly blocked keywords.

**Additional Blocking Options**

**Authenticate unknown users** - Mobile devices with Internet capabilities, such as the iPhone, iPad, and iPod touch, pose another threat on school campuses. If there are no security measures in place to deny non-school related machines access to the Internet, then consider using the Authenticate Unknown Users option. Forcing all users to authenticate with their Active Directory or Novell Network username before accessing the Internet through the school network will ensure that the data they access is tied to policies and reporting.

**Block file extensions** - Under every "allowed" content filter category, you can deny running a certain file extension.

**Spam Filtering Properties**

Spam filtering plays an important role in protecting a network from the threat of viruses, spyware, and malware.

**BEST PRACTICE:** Educate users and provide end-user management to minimize over-blocking.
Many organizations benefit from educating end users about email security best practices, including instructing users not to open an email if they don’t know the person who sent it. It can take time to educate your end users, but it is extremely beneficial once they get the concept.

*Properties > Spam Mail Blocker > Properties*

**Block virus infected** - Lightspeed has a vast database filled with thousands of virus signatures and FileIDs. Our spam blocking product (Lightspeed Email Manager) uses this database to ensure unwanted programs are not spread by email.

**Send spam mail summary emails to users** - To relieve administrative burden, this option allows end users to manage their own spam through a daily Mail Summary report sent directly to them. Inside this email, the end user can choose to forward a message from the spam queue, read it, and then Personally Allow it to their mailbox.

**NOTE: Messages containing a virus cannot be forwarded**

If a message is determined to contain a virus, the end user will not be allowed to forward the message, nor will the network administrator. This message is specifically tagged and removed from the database so no one can inadvertently release a virus onto the network.

**Enable automatic personal allow list generation** - By monitoring outbound email traffic, this option creates a one-to-one relationship between the sender (inside the network) and the receiver (outside the network), which ensures the receiver’s subsequent emails will be allowed through.

**Block mail using content database categories** - This option enables the Spam Mail Blocker to use the Content Database to evaluate incoming email by checking: the IP address of the sending mail server, the domain that the IP address of the sending mail server resolves to, the domain from the sending email address (From address), and any URLs or links in the body of the message. If any of these items is listed in a Content Database Category that is set to Block in the Spam Mail Blocker's "Blocked Content Categories" report (*Properties > Spam Mail Blocker > Blocked Content Categories*), the message will be blocked as Spam.

**TTC Security Server Updates**

Lightspeed works continuously to keep up to date with the latest scanning methods and technologies. As a result, it is imperative that you verify your TTC Security Servers are getting their updates. Virus signatures, or critical updates, are downloaded every 30 minutes. Verify under *Databases > Database Updates > Sources* that the Times in the Last Updated column are current.

**Client Configuration**

**Installation or Update Source**

BEST PRACTICE: Set the Update Source at the time the Security Agent is deployed.
There are many different ways to deploy the Security Agent across a network. A common problem when the clients are deployed is that the proper update source isn’t configured at the time of the installation. This means that if you simply download and install our Security Agent package by running the .msi file explicitly, the clients will update to our corporate servers—not your local TTC Security Server.

More information: [Lightspeed Wiki Article 11120](#). This article provides details on the three best ways to install the product on PC machines using Active Directory Group Policies, ZenWorks, or Manual/Login Scripts.

More information: [Lightspeed Wiki Article 20085](#). This article provides details on the three best ways to install the product on Mac machines.

With Active Directory Group policies, Novell ZenWorks, or Login Scripts, a Network Administrator can build an installation package one time and push out the clients automatically. If a new machine is added to the network, no changes will need to take place. If using Active Directory Group Policies or ZenWorks, make sure the .MST file is created properly.

Outdated Operating Systems
While many schools were given Microsoft Windows 95/98, it’s important to note that Microsoft gave an end-of-support notice for both these operating systems in 2006. As a result, the Lightspeed Security Agent does not support Windows 95 or Windows 98. This means that as technology changes and new vulnerabilities are discovered, these operating systems do not receive security patches from Microsoft or Lightspeed Systems.

Our strong recommendation is to either upgrade these machines to a supported OS or terminate them from the network. If these machines cannot be removed from the network, we suggest that all Windows 95/98 machines be placed on a separate VLAN and given only the bare-minimum network access. This way, when a Win 95/98 machine becomes infected, it will not disrupt the functionality of the entire network.

Windows Updates
Keeping the client machines up to date is just as important as keeping the Lightspeed TTC Security Server up to date. There are many vulnerabilities, or exploits, that exist on the Internet, and they can render a machine useless without having to run a particular virus on the local machine. Microsoft has tried to take measures to help end users keep their machines up to date. A virus-scanning program’s job is simply to deny viruses, malware, and spyware programs from running. Many virus programs are not designed to act as a software-based firewall on the local computer that it is running. Even if they were, in most globalized networks, personal firewalls must be disabled so network administrators can remotely manage the client machines properly.

Windows Server Update Services - In a large-scale environment, it is not best practice to have all the clients getting their updates from Microsoft every day automatically. This would require the clients be on, and most of the clients would be downloading the same file from the Internet at, or around, the same time. Microsoft has a solution called Windows Software Update Server that allows administrators
to choose a server on their network to act as the update source for the clients. This way, all the clients will get their Windows updates from this one localized server, and that server is the only machine that will need to download from the Internet. This is the best way to ensure that all security patches are installed on the workstations. By using this type of option, you can also choose not to automatically push out updates. You can first try out the appropriate patches against an array of test machines, verify that it will not disrupt the client computers, and then choose when to deploy it across the environment.

Microsoft Virus-Scanning Recommendations - Microsoft has recommended quite a few directories for the virus scanning programs not to scan. You can find the additional information at http://support.microsoft.com/kb/822158/. Some of the information is very specific to the Windows updates process.

Disable Autorun/Autoplay
Often a virus is launched unintentionally. (Users may tell you they didn't run any unknown programs.) To keep programs from auto-running, we recommend that you disable the Autorun and Autoplay options, or enable the option to prompt the user before running a program. See Microsoft's knowledge base article, http://support.microsoft.com/kb/967715. This way, user intervention is required to run a program—whether from a floppy disk, CD-ROM, or flash drive.

User Rights
Many older school-related applications would only run if a user had local administrator rights to the PC. Giving out administrator rights to non-administrators is very dangerous because it allows anyone to uninstall, install, and modify almost anything on the client machine. This is extremely risky if a user uninstalls your virus scanning program. Take advantage of access rights enforcement tools to:

- Deny users from installing or uninstalling applications on client machines.
- Disallow users from being able to login locally or remotely to servers.
- Limit the user's ability to see or run certain programs.

Microsoft, Novell, and Apple have done a great deal of work to give network administrators the tools they need to lock down a user on the network. Take the time to review these options.

Network Security
Many books have been written about network security, so we'll only touch on a few items here.

Firewalls
Firewalls are top of mind when contemplating network security. A firewall's main purpose is to protect the network from the outside world. In a school environment, though, you are battling hackers from both the inside and the outside world. So, it is important that a firewall administrator take a few precautions when allowing or disallowing applications across the network. For example, users typically do not need access to the Remote Desktop Protocol (TCP Port 3389). RDP was created for
administrators to remotely access and administer servers or client machines, but it can also provide an opportunity to bypass your Content Filter by remotely logging into outside machines. Although the data they access will be going to their home machines, the material will be displayed on the school’s computer monitor and will likely violate your acceptable use policies.

On the network, if you are hosting your own email server (e.g., Exchange or GroupWise), then it is recommended that the firewall only allow outbound email that is coming from the source IP address of your mail server. Otherwise it is possible a user will send spam messages from your network, and your firewall will translate (NAT) the outbound connection to a single IP address. If a Real-Time Blacklist Server gets a hold of that IP address as a known spammer, then all your valid emails coming from your mail servers will soon be blocked by many servers out on the Web. It is very time consuming to get your IP address off those lists.

Switches and Routers
Options on your switches and routers allow you to segment your network. Use VLANs to lock down access to your servers or other segments of the network. Also, consider enforcing 802.1x authentication. This will prevent computers brought from home from accessing the network.

Network Shares
Many viruses spread across the network by using open network shares that are accessible to all machines on a network. Review each server’s network shares to verify who has rights to these shares. If a particular user or group of users does not need full access rights to the shares, then remove the access and the risk.

Case Study
Memphis Independent School District in the small town of Memphis, TX prides itself on being able to provide top-notch, big-city technology services to its students.

When he joined the district, David Calabrese, Technology Director, needed to replace (or renew) the antivirus solution, as well as update the content filter, prepare for email archiving regulations, manage bandwidth, and more.

David’s multiple needs led him to a single solution: Lightspeed Total Traffic Control (including Lightspeed Security Manager).

David shares his success with the solution: “Security Manager caught things that our previous antivirus didn’t. And since then, we haven’t had ANY viruses. When something is suspicious, the product alerts me (tells me what it is, where it is, and what it’s trying to do), and either quarantines or deletes the file. We haven’t had a single virus outbreak.”

Part of that success is that David rebuilt his machines from the ground up: he imaged, rebuilt, reinstalled software, and installed the Security Agent on every machine on the network in order to start with a clean slate. “I took a layered approach, starting at the bottom and getting the proper systems in place.
When those things are true, **Security Manager beats any other antivirus solution out there.** I have the control and security I need: I can customize what things to block, and set policies prohibiting users from installing software or from being administrators of their machines."

“Because the Security Agent is policy-based instead of signature based, it can run on a client machine without running everything against a database of signatures. The server knows all about the viruses, and all the agent on the computer has to worry about is staying up to date with the server, which is a quiet process in the background,” David comments.

David has also been impressed with the invisibility of the solution to the user. “The Security Agent is very light,” he says. “**It’s a small package that doesn’t interfere with the everyday processes on a machine.**” David also takes advantage of the ability to set how much of the CPU the solution should use, which is especially useful on older machines. “Because of tight budgets, I have to work with what I have,” he shared. “So I set the Security Agent CPU usage to 25% for older machines. The scan might take a few hours, but who cares? It gets done, and gets done without the user complaining that the machine is slow or that other programs can’t be used.”

David has a unique viewpoint on his job: “If you don’t know me or my face, then I’m doing my job properly,” he shares. “With the power I have through the Security Agent and Total Traffic Control, I can do everything I need—effectively, efficiently, and transparently.”

**Conclusion**

Every network faces security risks. To protect your district resources, you need to utilize an antivirus solution, properly configure it, and complement it with other tools, including content and spam filtering and Group Policy or ZenWorks controls.

Lightspeed Security Manager delivers a powerful solution to combat viruses, spyware, and malware on your network. Following best practices for installing, configuring, and updating the solution will maximize its effectiveness.

**About Lightspeed Security Manager**

*Block viruses, spyware, and malware with desktop and gateway security*

Potential threats lurking inside and outside your network can compromise safety, expose systems to harm, and lead to costly and time-consuming problems and outages. While anti-virus software can reduce exposure to known threats, unknown threats remain unblocked.

**Lightspeed Security Manager** allows you to easily maintain the health of computers across your network by stopping threats to your servers and desktops. Security Manager protects your valuable network resources from unwanted access with its advanced, stateful inspection of network traffic.
About Lightspeed Systems

Lightspeed Systems Inc., founded in 1999, develops comprehensive network security and management solutions for the education market. We are committed to helping schools operate their networks effectively and efficiently, so educators can provide safe online teaching and learning environments.

Our software is used in more than 2,000 school districts in the United States, the United Kingdom, and Australia to protect more than 6 million students. For the past several years, Lightspeed Systems has been recognized on the Inc. 5,000 list as one of the fastest-growing private companies.

www.lightspeedsystems.com

For More Information:

➢ Watch a 5-minute overview of our solutions:
  http://www.lightspeedsystems.com/resources/Lightspeed_TTC_Demo.html

➢ Get more information on these and other important topics in our Resource Center:

➢ Customers: Access this information paper in our Wiki
  http://wiki.lightspeedsystems.com/x/5xSkAQ