

# RainbowShield

## Total Virus Protection for Linux e-mail Servers

Taking into account the market needs and requests, the development and research department of SolviT Networks has made a smooth integration of worldy renowned antivirus with mail servers: thus RainbowShield is the software solution for integrating Trust Antivirus, Norton Antivirus, Sophos, Clamav the mail servers on Linux. This solution confers to security administrators the opportunity to protect their Sendmail, Qmail and Postfix mail servers on the following Linux distribution: RedHat, SUSE, Slackware, Fedora and Debian.

### Value Proposition

Computer viruses are the most prevalent security risk threatening computer users today. In a heterogenous IT environment, mitigating the risk of business interruption is not accomplished with just desktop antivirus alone, but instead requires a comprehensive threat management approach. RainbowShield offers:

### Return on Investment

- Provides global antivirus protection at an excellent quality-price ratio.
- Maximize the level of security across the whole enterprise.
- Helps reduce damage and costly downtime from virus infections and untrustworthy, non-productive traffic.
- Scans, identifies and isolates viruses before they can enter the network.

### Reduce Business Risk

- Superior manageability helps ensure the availability of critical business systems.
- Provides layers of security for any enterprise, including virus scanning at the gateway, as well as antivirus software on desktops, servers and mail servers.

### Use Your Existing Resources

- RainbowShield is available for Linux: RedHat ( 7.2, 2.1), SUSE ( 8.0), Slackware ( 8.2), Fedora and Debian.
- When used for mail server protection, RainbowShield Server complements existing antivirus desktop and server software.

### Key Features

#### Proactive Protection against Unknown Threats.

With RainbowShield, antivirus protection is proactive and extremely efficient. In addition to known viruses, the product recognizes new, unknown viruses based on typical features of viruses. You can also protect your network by specifying potentially dangerous files to be automatically dropped from the email traffic.

### **Automatic Virus Definition Updates.**

Updating of virus definition databases is automatic and secure.

### **Ease-of-Use and Deployment.**

RainbowShield is easy to set up and administer. Your administrator is constantly aware of what is happening in the network.

### **Outbreak Management.**

Your administrator is able to react faster to virus outbreaks with outbreak management. The product notifies the administrator if an infected email enters the system.

The administrator can also configure the program to notify the recipients and/or the sender.

## **Distinctive Functionalities**

### **Global Protection.**

RainbowShield protects your company globally, by scanning all incoming and outgoing emails. Both the message body and attachments are being scanned with eTrust Antivirus. The archived files .zip, .arj, or similar files are scanned as well. For building and maintaining a stable IT environment, the network administrator can define its own security policy against viruses or malicious codes in emails or attachments (cure, delete, warning, ignore). File extensions can be also defined and automatically deleted.

### **Flexibility.**

Easy to install, configure and deploy, RainbowShield is a typical "out of the box" software solution, but optionally it can work in different architectures (such as, the scanner server can be installed on a server and the reports can be sent to another server or more than one client can send messages to one server).

### **Superior Manageability and Scalability.**

The multi-tiered architecture and hierarchical organization of RainbowShield provide deployment flexibility and powerful management tools to administer antivirus protection throughout your enterprise. An extremely flexible and scalable solution, RainbowShield shall offer you the possibility to implement it on different client-server architectures: server-multi client and client-multi server as well.

### **Real-time Reporting**

Powerful reports can be created to provide relevant information on the status of an antivirus implementation. Statistical reports regarding the scanned traffic can be obtained either from the kept logs, or by integration with specific tools. The server having been scanned can optionally (or according to predefined politics) send figures and reports to another server that processes in real-time the incoming data (message size, scanning time, number of detected viruses).

Implicitly by integrating it with RRD tool (a specific tool for graphic reporting under GPL free license), the administrator is able to monitor the scanning server

### **Backed by the Security Expertise of SolvIT Networks Support.**

As a CA's Regional Competence Center, SolvIT Networks provides technical support according to the highest standards of professionalism. Accordingly trained and qualified, our specialist can offer you around-the-clock support and expertise.

## **Supported Environments**

### **Operating System**

- RedHat ( 7.2, 2.1)
- SUSE ( 8.0)
- Slackware ( 8.2)
- Fedora
- Debian

### **Mail Servers**

- sendmail ( 8.10)
- qmail (1.03)
- postfix ( 1.1)