

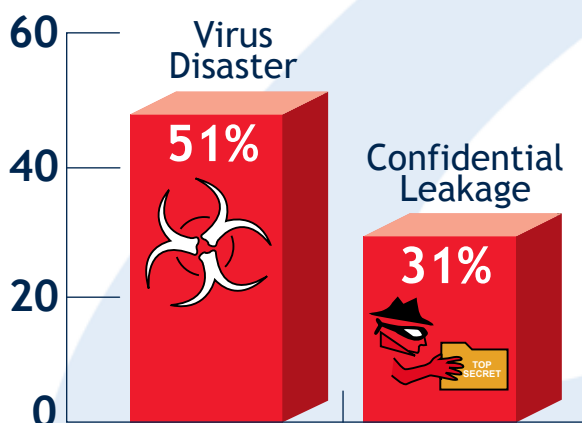
SuperScout®

Email Filter

Managing Content Security

In today's workplace, email use has skyrocketed. Businesses are increasingly recognizing the benefits of providing email as the primary means of communicating with customers, partners, and the rest of the world. Businesses are now faced with serious threats to their organization's content security if email use goes unmanaged.

Security Threats



51% of companies reported virus disaster.
Source: 2000 Virus Prevalence Survey - ICISA.net

31% of respondents admitted to intentionally or accidentally sending confidential information outside the organization.
Source: PC Week Survey - 1999

While many companies are taking care to monitor network use, too few pay attention to **what** comes and goes across their virtual company boundary. SuperScout Email Filter allows you to flexibly define rules, as well as implement and enforce an email Acceptable Usage Policy (AUP), fully customized to your organization's needs.

Increase Security

- Provide Anti-Virus Scanning at the Gateway** - Use your current anti-virus solution, giving you the choice of best of breed products, for enhanced virus protection.
- Prevent Confidential Data Loss** - Block, isolate, or delay until approved, the unauthorized transmission of email containing intellectual property or other confidential data.
- Implement Encryption Policy** - Block, isolate, allow, or strip desktop encrypted messages from unauthorized personnel within the organization.

Limit Legal Liability

- Prevent Sexual Harassment** - Provide a safe and productive work environment for employees, by filtering out offensive/inappropriate email from the Internet.
- Avoid Libel Litigation** - Protect company image and liability with corporate disclaimers, where appropriate, or by preventing internal users from sending offensive or otherwise inappropriate email to the outside world.

Improve Productivity

- Enhance Email Server Productivity** - Schedule non-essential email to transmit after normal business hours, ensuring priority to business-critical email during the workday.
- Improve Employee Productivity** - Prevent spam and other junk email, as well as minimize, delay, or discourage excessive personal use of email depending on your organization's specific email policy.

SuperScout®

Email Filter

• Increase Security

Features and Functionality:



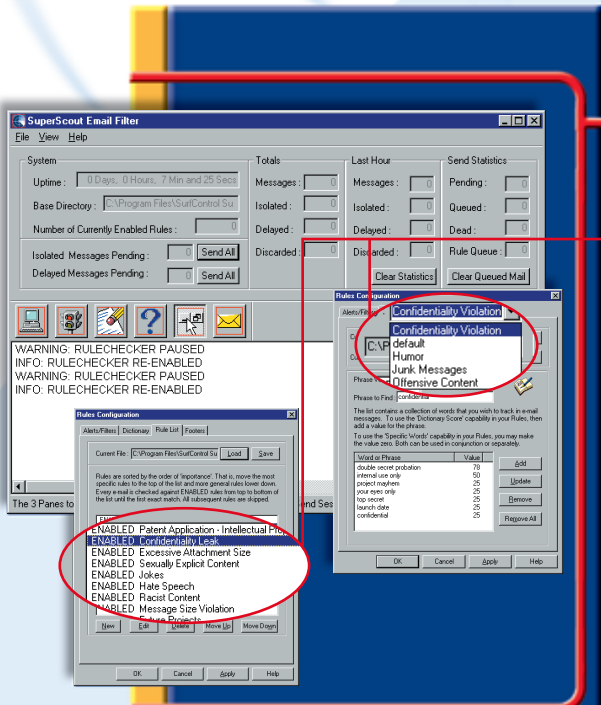
Intelligent Rules Processing

Multiple policy actions allow you to effectively manage the flow of information traveling into and out of your organization through email.

▶ Unlimited email rules can be simply enforced, and are fully customized to your organization's needs, using multiple content dictionaries.

▶ Allow, delete, isolate, or delay any email that breaks your organization's email policy rules.

▶ Flexible notification options allow you to copy the appropriate manager based on the content of the policy violation. This feature also allows for notification to the sender and/or recipient that the email has violated the corporate Internet email policy.



Email Access Policies

SurfControl encourages you to define, implement, and use a corporate email Acceptable Usage Policy (AUP) that clearly explains what is and is not acceptable email usage. Developing an AUP that is tailored to your corporate culture and needs is a team effort, and SurfControl can help.



Secure Remote Management

Allows for multiple administrators, such as HR and IT managers, to remotely monitor, receive, and review notice of security breaches and policy violations based on content type.

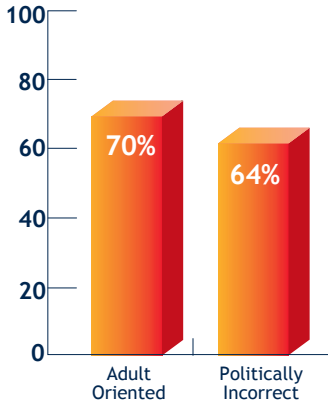
▶ Secure Access for remote managers enables multiple actions to be taken on isolated messages.



• Limit Legal Liability • Improve Productivity

Extensive Reporting

Where are emails coming from, who is sending the largest volume, who is sending the largest attachments, and are they work-related? Who is breaking your corporate email policy? With SuperScout Email Filter, you can report on all email usage and policy violations.

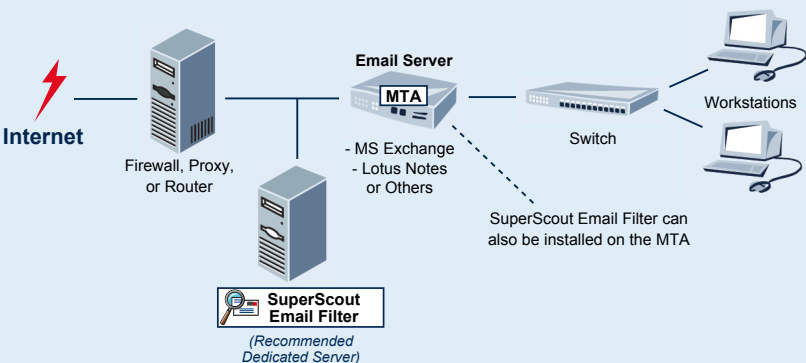
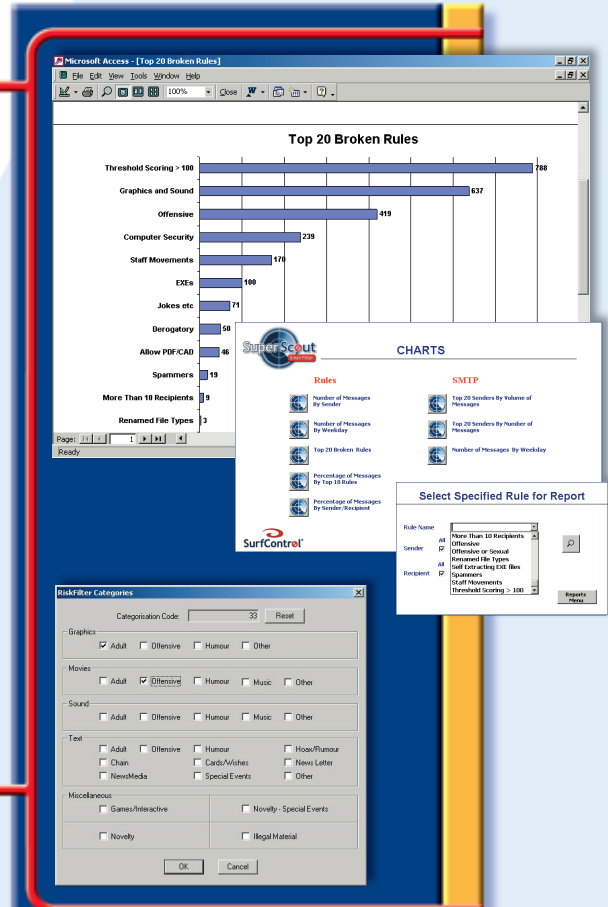


According to *BusinessWeek*, 70% of employees say they have received adult oriented emails, and 64% have received politically incorrect or offensive emails in the office.

RiskFilter™

A unique feature that provides a pre-categorized database of content that automatically protects the organization from nuisance emails such as chain letters, get-rich-quick schemes, joke lists, as well as GIF's, JPEG's, and MPEG's containing offensive material that have spread like wildfire through the Internet and email.

How SuperScout Email Filter Works:

Top 20 Broken Rules

Rule Category	Count
Threshold Scoring > 100	188
Graphics and Sound	837
Offensive	419
Computer Security	239
Staff Movements	174
EXEs	100
Jokes etc	71
Berogatory	50
Allow PDF/CAD	46
Spammers	19
More Than 10 Recipients	9
Renamed File Types	3

RiskFilter Categories

- Graphics: Adult, Offensive, Humour, Other
- Moves: Adult, Offensive, Humour, Music, Other
- Sound: Adult, Offensive, Humour, Music, Other
- Text: Adult, Offensive, Humour, Hoax/Rumour, Chain, Cards/Wishes, News Letter, NewsMedia, Special Events, Other
- Miscellaneous: Games/Interactive, Novelty - Special Events, Novelty, Illegal Material

Additional Features:

- ▷ Scan inside the subject line of the message, the body of the message, as well as inside attachments.
- ▷ Real-Time Monitor offers quick view into email volume and status.
- ▷ Add customizable footers to any or all emails.
- ▷ Scan for viruses using your preferred anti-virus tool.
 - Mc Afee
 - Sophos
 - Norton
 - Others
 - Trend

 Download your FREE trial version from
www.surfcontrol.com

▶ Try SuperScout Email Filter FREE Today!



System Requirements:

Operating System:

- Microsoft® Windows NT4® with Service Pack 6a
- Microsoft® Windows 2000 Server with Service Pack 1
- Microsoft® Windows 2000 Advanced Server with Service Pack 1

Processor:

- Pentium® II 400 mHz processor or higher
- Pentium® III recommended

Memory:

- 128 MB
- 256 MB recommended

Disk Space:

- 1 GB disk space

Other:

- Microsoft® Data Access Components (MDAC) 2.5 or higher
- TCP/IP installed and configured
- Dedicated Internet Connection
- Internal and External DNS configured
- Email system with SMTP gateway or MTA installed
- Browser Access
Microsoft Internet Explorer 5.0 or higher
Netscape Communicator 4.75

The volume of Internet traffic and topology has an impact upon the number and size of machines required.

Works with the following Mail Servers, either on the same machine or on separate machines:

- Microsoft® Exchange
- Lotus Notes®/Domino
- Netscape® Mail Server
- Sendmail and others

 Email emailinfo@surfcontrol.com to request a CD-ROM

 Call SurfControl:
US and Canada: **1-800-368-3366**
UK: **+44-(0)-1260-296150**
Austria: **+43-(1)-513-4415**
Germany: **+49-(69)-972 64 105**
BENELUX: **+31-10-402-00-00**
Asia Pacific: **+61-(2)-9882-0039**
Australia: **1-800-73-22-44**

Our technology partnerships and affiliations include:



CISCO SYSTEMS
Verified

Microsoft Certified
Solution Provider



▶ About SurfControl

SurfControl plc (London:SRF/EASDAQ:SRFC), is a world leader in Internet filtering solutions, offering a complete line of Web and Email filtering products for home, education, business and OEM use.


SurfControl®
The Filtering Company

US Headquarters:

SurfControl, Inc. 100 Enterprise Way, Suite A110, Scotts Valley, California 95066, USA
Tel: 1-831-431-1300 Fax: 1-831-431-1800

International Headquarters:

SurfControl plc, Riverside, Mountbatten Way, Congleton, Cheshire, CW12 1DY, England
Tel: +44 (0) 1260 296200 Fax: +44 (0) 1260 296151

www.surfcontrol.com