

i-Filter Managed Services

The i-Filter is a security appliance that doubles as a web filter and total network protection solution. It is designed to provide enterprise level security while fitting the needs and budget of a small business. It keeps your employees more productive and cuts IT costs and downtime by preventing problems before they happen. Unlike traditional security monitoring software, the i-Filter protects **all** of the devices on your network in real time and does not require individual PC and server maintenance. You can think of it as a coffee filter for your entire network, filtering all communications and data transmissions.

Standard Package – Starting at \$39.00 Per Month

Web Filter	Firewall
Spam Blocker	Routing & QoS
Ad Blocker	Intrusion Prevention
Attack Blocker	Protocol Control
Phish Blocker	Reports
Spyware Blocker	

Server Integration Package – Starting at \$30.00 Per Month

Active Directory Connector
Policy Manager

Optional Add-Ons – Starting at \$8.00 Per Month

eSoft Web Filter	Kaspersky Virus Blocker
CommTouch Spam Booster	PC Remote
WAN Balancer	WAN Failover
Remote Access Portal	

Web Filter

Control Web Content at the Gateway

(Internet filter) enables administrators to enforce network usage policies and monitor user behavior. Powerful features such as Zero client installation and category block lists make it easier for administrators to:

- Protect the network from malware on the web
- Block time-wasting sites like MySpace
- Conserve bandwidth by blocking audio/video downloads

According to an industry study, at least 90 percent of large enterprises and 50 percent of small companies in the United States now monitor and filter their employees' Internet access.

The primary reasons companies' use Internet filtering and monitoring is to block inappropriate content (44%), control productivity (32%) and preserve network bandwidth (23%).

Now you can easily monitor, set and enforce your own web usage policy with our Web Filter application—without the hassles of outsourcing it. Whether you want to use our blocklists or set your own policies for hosts, domains and files types, you can block access to inappropriate sites. Reporting enables you to view a big picture of the kind of Web browsing behavior occurring on your network.

Key Features:

- Pass, Block, and Logging options for all categories, such as gambling, webmail, shopping, and pornography
- Categories update automatically
- Add your own URLs and file types to block, log, or pass
- No proxy settings required
- Local database ensures fast web browsing
- Set time and user based policies (e.g. allow shopping during lunch and outside business hours)
- Reporting and event logs help monitor web browsing behavior

Spam Blocker

Block Spam at the Network Gateway

Our Spam Blocker uses an advanced **spam filtering** system to block spam at the gateway before it ever reaches the users. Zero client installations make it easy for administrators to:

- Leverage the best spam filtering techniques including Bayesian Filters, Razor, real-time block lists (RBLs), OCR(Optical Character Recognition) for image spam and Tarpitting
- Provide individual quarantines for each mailbox
- Filter SMTP, POP & IMAP

Spam is the bane of small businesses' existence. It can not only bring viruses onto your network, but it can take over your computers and send spam to other computers.

And it impacts you in other ways. According to a recent study, the cost of spam messages to U.S. companies—in terms of productivity and the equipment, software and manpower to combat it—was upwards of \$10 billion in 2004.

So the key is to stop spam before it stops you.

Our powerful Spam Blocker protects you with top-notch spam scanning and blocking at the edge of your network—before it can do damage or slow you down. Using the latest technologies, Spam Blocker transparently scans for spam, marks messages and intercepts emails. It requires no alteration of your network's mail configuration and is constantly updated to guard against any refinements in trickery or techniques that senders create to get around other solutions.

Key Features:

- Quarantine Digest—our Spam Blocker is optimized to make sure “good” mail is never mistaken for spam. However, if a “good” mail is ever identified as spam, our Spam Blocker gives each team member in your company their own personal “quarantine” list. They can find that email without having to track down an administrator
- Personal Passlist—users can designate certain email addresses as “good” without having to bother your IT person
- Image based filtering — scans images within emails to stop this new type of spam
- POP, IMAP & SMTP support
- Reports give a comprehensive view of the spam environment on your network, including the source of the spam and how much spam is received in aggregate and by user

Ad Blocker

Eliminate Annoying Ads and Improve Page Download Times

Ad Blocker enables administrators to block web ads at the gateway by transparently removing them from web pages. Benefits include:

- Easier to read web pages without distracting ads
- Improved page download times
- Reduced traffic on the network

Key Features:

- Create custom rules and exceptions
- Automatic updates
- Event log details all blocked ads

Attack Blocker

Keeping DOS Attacks at Bay

Attack Blocker stops denial of service (DOS) attacks. Pre-configured settings make it easier for administrators to:

- Provide 24/7 network protection from DOS attacks
- Sort good traffic from bad with reputation-based heuristics
- Put legitimate users with intensive bandwidth needs on Pass lists

Prevent Denial-of-Service attacks—and keep your network focused on legitimate uses

“Unfriendly” machines earn bad reputations and are limited, dropped and rejected. Attack Blocker can also quickly identify unauthorized use of network resources and stop those resources from being allocated to unauthorized users.

Key Features:

- Dynamically blocks flood attacks based on reputation based heuristics
- Carefully allocates network resources to legitimate users if network is under attack
- Create exception list of users allowed to behave aggressively
- Event Logs and reports show limited, dropped, and rejected events

Phish Blocker

Block Phishing & Pharming at the Gateway

Identity thieves are becoming increasingly sophisticated with email and website spoofs that are nearly impossible to discern from the real thing. Phish Blocker makes it easier for administrators to:

- Protect users from email phishing attacks and fraudulent pharming websites
- Protect multiple protocols, including HTTP, SMTP, POP & IMAP
- Ensure that signatures are always current with automatic updates

Identity theft can compromise your business, and your accounts, as well as create turmoil in the lives of your employees. None-of-which is good for business.

Maintain the highest level of protection for you and your employees with our Identity Theft Blocker. This application protects your network against “phishing” attacks—emails that direct users to fraudulent websites with the intent to steal personal identity, credit card information and more.

Identity Theft Blocker marks phishing emails and puts them in a user’s quarantine. Transparent, powerful and easy to use, it requires no alteration of your network’s mail configuration.

Key Features:

- Block phishing email on SMTP, IMAP, and POP
- Event log of phish caught
- Reports show how many fraud emails were stopped, who they were targeting, and from where they were sent

Spyware Blocker

Block Spyware at the Network Gateway

Spyware Blocker enables administrators to block spyware at the network gateway before it reaches users desktops. Zero client installations make it easy for administrators to:

- Protect users from browsing websites that install malware
- Scan network traffic to block spyware before users can install it
- Ensure that signatures are always current with automatic updates

Is your IT guy spending too much time going from machine to machine getting rid of spyware only to have it show up again a week later?

The battle with spyware is constant, and its infection is insidious—you may not even know you have it until its doing real damage to your network. Weird settings, an abundance of pop-up ads (even when you're not on the Web), clicking hyperlinks that don't work and a sluggish system are just a few of the symptoms to look out for.

Stop spyware, adware and malware before it makes it to your network—and find already infected computers with our powerful Spyware Blocker. We use a wide range of cutting-edge technologies, including URL blocking, cookie blocking, ActiveX blocking of bad vendors and subnet logging, to protect you from attacks and infections.

Key Features:

- Manage your Block and Pass Lists
- Special "request pass" button makes it easy for a user when blocked to request the site to be white listed at the administrator's discretion
- Event log shows real-time spyware detected and blocked
- Reports track violations in summary, detail, and by user

Firewall

Your First Line of Defense

Firewalls draw the line which separates internal and external networks. Firewall filters traffic based on IP address, protocol and ports that allow administrators to:

- Designate which systems and services (http, ftp, etc.) are publicly available
- Create a DMZ and perform NAT (with Router)
- Run as a transparent bridge to complement existing hardware

The Firewall is the most basic security element to hide your network from the outside and control all external access points (also known as ports). It lets you block unwanted activity and protect your network.

You can build a list of rules that meets your unique needs—control traffic by protocol, source address or port, destination address or port, and set default actions.

Firewall evaluates traffic traveling across your network by applying your rules until a block/pass verdict is reached or a default action is taken.

Key Features:

- Easily blocks sessions based on simple rules
- Rules can be based on a variety of attributes

Routing & Quality of Service (QoS)

Networking's Blocking & Tackling

Routing capabilities enable administrators to:

- Provide the basics like NAT, DMZs, DHCP & DNS
- Get fancy with multiple NAT spaces, routing tables and configurable MTU
- Prioritize traffic with QoS
- **Support SIP & IAX VoIP traffic**

Our web filter device allows all hosts to share internet access via Network Address Translation (NAT), and also provides DHCP and DNS services and advanced routing capabilities. The administrator can configure NAT, as well as related redirect rules, and DMZ host settings. The administrator can also add static DHCP and DNS entries, as well as custom routes to support more complicated networks.

QoS is a great way for administrators to improve VoIP call quality and ensure that critical apps have priority access to bandwidth. QoS enables administrators to create a pool of bandwidth that is reserved for critical apps. Administrators can decide what percentage of their bandwidth to reserve depending on the size/type of their connections and the intensity of critical apps they intend to run concurrently. By segmenting services into high, medium and low priority queues, administrators can minimize interruptions to sensitive apps (VoIP, SSH, VNC, RDP, etc.) from bandwidth intensive downloads or websites (YouTube, etc.) that may be lower priority.

Intrusion Prevention

Stopping Hackers at the Gateway

Intrusion Prevention blocks hacking attempts before they reach internal servers and desktops. Pre-configured signature-based IPS makes it easier for administrators to:

- Provide 24/7 network protection from hackers
- Minimize annoying false positives
- Ensure that signatures are always current with automatic updates

Most hackers are looking for computer networks that they can hijack and exploit. They cast wide nets using automated programs that sniff out exposed networks. This makes small businesses, with more limited IT budgets, particularly vulnerable.

Our Intrusion Prevention software intercepts attacks in their tracks. Working transparently on your network, this innovative application uses thousands of signatures to detect, block and log intrusion attempts, using industry-standard rules.

Plus, we simplify the process by setting reasonable defaults for you on thousands of signatures—or you can change defaults and add new rules based on your company's specific needs.

Key Features

- Thousands of signatures for a variety of attacks
- New attack signatures automatically downloaded to your device

Protocol Control

Block Port Hopping Applications

Protocol Control lets administrators take back control of their networks from disruptive port-hopping applications like peer-to-peer applications or online games. Signature based layer 7 filtering makes it easy for administrators to:

- Conserve bandwidth by blocking applications like peer-to-peer that open multiple TCP ports
- Improve productivity by blocking IM & online games that evade firewall rules
- Write custom signatures for any protocol

Protocol control covers a broad set of applications, such as Instant Messaging, Peer to Peer activity, online games and streaming media, which can clog your network, reduce productivity, and infect computers with spyware, malware, and viruses.

These applications are extremely aggressive and will sneak out on ports used for other vital network traffic such as web and email, making it nearly impossible to control them with firewall rules.

Protocol Control takes a different approach to log and/or block these applications using their signatures. This allows you to lock down the unwanted activity.

Key Features:

- Protocol control lets you select the protocol signatures to log or block
- Custom rules can be added for any unsupported protocols
- Time based policies let you decide when and if these applications are permitted
- Reporting lets you see which protocols are active on your network and who is using them

Reports

Network Visibility & Monitoring

Reports provide administrators the visibility and data necessary to investigate security incidents and enforce acceptable network usage policies.

- Monitor behavior at the user, client and incident level
- Understand traffic flows and network usage patterns
- Share reports in PDF or HTML formats

Visibility is the first step in controlling your network, identifying misuse, and enforcing your network usage policy. Reports provide this visibility and are also a great tool for troubleshooting.

You'll get daily, weekly and monthly reports about the activity in your network and each application. How many viruses and spam were blocked? Which phish were caught? What Websites were visited?

Reports can be delivered via email

Key Features:

- Summary, detail, and per user reports
- Automated email report delivery
- Report archive

eSoft Web Filter

Filter Web Content Dynamically

eSoft Web Filter enables administrators to block inappropriate web content in real-time. eSoft's dynamic URL categorization engine makes it dead simple for administrators to:

- Block 100M+ classified websites in [53 categories](#) and [20+ languages](#). **Great for:** Traditional sites like **porn, gambling, social networking** & more.
- Block new and unknown sites as users browse to them with eSoft's dynamic filtering and *Distributed Intelligence Architecture* (DIA). **Great for:** Rapidly changing sites like **proxies, phishing, IM, P2P** & more.
- Leverage eSoft's *Threat Protection Team* for best-in-class online security. **Great for:** **Spyware, phishing** and **virus distribution** sites.
- Block encrypted sites by IP address. **Great for:** **Proxies** and other sites that use **https** to obfuscate themselves.
- [eSoft vs. Web Filter comparison](#) available below

The web is a rapidly evolving place and the pace of change increases every day. For all the positive content created online, the fastest changes take place in the murkiest corners of the web. In fact, most proxy and phishing sites are online for less than 24hours. Yet, highly organized search, social and email campaigns drive massive numbers of unsuspecting users to them before they get shut down. The traditional malware protection companies just can't write signature fast enough to keep up... but this is precisely where eSoft excels.

eSoft's web filter was originally built to combat online security threats where rapid reaction to emerging threats was paramount. eSoft's Distributed Intelligence Architecture leverages the power of its wide implementation by verifying and classifying every new website and webpage that its user base browses to with algorithmic triggers and a team of 70 professionally trained multilingual web analysts. While 99.9% of users browse sites that are already classified within eSoft's 100M+ database, the new sites that users find are classified and updated to the hosted database in real-time so that all eSoft customers benefit instantly.

Key Features of eSoft Web Filter:

- Best-of-breed performance from the leading web filtering technology
- Block lists updated in real-time based on sites that users actually browse to
- DIA architecture ensures blocklists are updated in real-time with the latest proxy or social networking before your users even know about them
- 100M+ website database categorized by content

- 53 content categories
- 20+ languages supported
- Database maintained by 70 professionally trained multi-lingual web analysts
- Hosted database ensures updates are received instantaneously
- Pass, Block, and Log options for all categories, such as porn, gambling, social networking, proxy, webmail, shopping etc.
- Add your own URLs and file types to block, log, or pass
- No proxy settings required
- Set time and user based policies (e.g. allow shopping during lunch and outside business hours)
- Reporting and event logs help monitor web browsing behavior

Below is a list of Content Categories in which eSoft Web Filter can block or allow access.

Content Categories



Adware	Government	Portal Sites
Alcohol	Hate Speech	Proxy/ Anonymizer
Anonymizer/ Proxy	Health	Real Estate
Art	Home/Leisure	Religion
Business/ Services	Humor	Restaurants
Cars/ Transportation	Illegal Drugs	Search Engines
Chat/IM	Job Search	Shopping

Community Sites	Mature	Social Networking
Compromised	Military	Spammed
Computers & Technology	Miscellaneous	Sports and Recreation
Criminal Skills/ Hacking	Music	Spyware & Malicious Sites
Dating	News	Tobacco
Download Sites	Non-profits	Translator
Education and Reference	Nudity	Travel
Entertainment/ Videos	Personal WebPages	Violence
Finance	Pharmacy	Weapons
Gambling	Phishing/ Fraud	Web-based Email
Games	Politics & Law	
	Pornography/ Sex	

Supported Languages

Arabic	French	Polish
Catalan	Frisian	Portuguese
Chinese	German	Romanian
Czech	Hungarian	Russian
Danish	Italian	Spanish
Dutch	Japanese	Swedish
English	Korean	& more!

Web Filtering Comparison

		
	Web Filter	eSoft Web Filter
Price	Included	Refer to Price List
Website database	1M+	100M+
Content categories (porn, gambling, etc.)	15	53
Block https	No	Yes
Dynamic categorization	No	Yes
Database maintenance	Community	Professional analysts
Block by URL	Yes	Yes
Block by file extension (.exe, mp3, etc.)	Yes	Yes
Block by MIME type	Yes	Yes

Kaspersky Virus Blocker

Cutting Edge Anti-Virus Protection at the Gateway

Stopping viruses at the Internet gateway is critical. Virus threats have shifted dramatically from email to the web. Malware outbreaks have scaled exponentially, from 200,000 in 2006, to 2 million in 2007, to 20 million in 2008. Kaspersky Virus Blocker is a best-of-breed anti-virus application for businesses, schools and homes that want the reassurance of robust virus protection. It's a commercial application that:

- Blocks viruses at the gateway before they even touch the PCs or servers
- Protects users in real time from viruses over HTTP, SMTP, POP, IMAP & FTP
- Updates automatically with new signatures every hour

We're always looking for the best applications to offer our customers. Every time we've tested anti-virus software Kaspersky comes out on top... and we're not alone in singing Kaspersky praises, they've won numerous awards from CNET, SC Magazine, PC World and many others! AV-Comparatives, an independent company, ranked Kaspersky #1 in both On-Demand Scanning and Rootkit Detection. Kaspersky tied for first place on the Fastest Response Time to malware threats.

Kaspersky Lab's success stems from their international team of the world's leading virus researchers and developers. Kaspersky's research team works round the clock to stay ahead of the game with new virus blocking techniques and ensure rapid response to new threats as they emerge.

Kaspersky is offer cutting edge virus blocking technology starting at just

Key Features:

- Award winning best-of-breed virus protection from the leading anti-virus vendor
- Kaspersky Virus Blocker sits at the network gateway so there is only one application to keep up-to-date
- Protection on the most common email protocols SMTP, IMAP, and POP
- Protection for webmail and file transfer via HTTP and FTP protocols, an increasingly common route for infection
- Reports and event logs show you what viruses are being blocked on the network

Commtouch Spam Booster

Best-of-Breed Spam Blocking Technology

Commtouch Spam Booster is a premium extension to Spam Blocker that adds an enterprise-class layer of protection against annoying, offensive and time-wasting unsolicited bulk email. Commtouch Spam Booster enables administrators to:

- Detect over 98% of spam messages in SMTP, POP & IMAP
- Minimize false positives with the industry's highest accuracy levels (Osterman Research)
- Detects spam outbreaks in real-time with patented Recurrent Pattern Detection™ technology

Recurrent Pattern Detection™ technology

Commtouch's Recurrent Pattern Detection™ (RPD) technology is a service "in the cloud." Rather than evaluating each individual message, RPD technology analyzes large volumes of Internet traffic in real-time. New spam and malware outbreaks are identified as soon as they emerge, and recorded in the Commtouch Detection Center. Commtouch Spam Booster then queries the Commtouch Detection Center and receives message classification in real-time. The result is instant protection from new outbreaks – far ahead of signatures or software updates. Esteemed analysts agree that Commtouch achieves the industry's best detection/accuracy performance (Osterman Research) and "detects and blocks spam in the first few minutes of an outbreak, unlike other anti-spam approaches" (IDC).

Key Features:

- Integrates seamlessly with Spam Blocker
- Blocks any Spam outbreak with 98% detection and near zero false positives
- High accuracy in any format or language
- Quarantine Digest— Commtouch's technology is highly optimized to make sure "good" mail is never mistaken for spam. However, if a "good" mail is ever identified as spam, the quarantine digest gives each user their own personal "quarantine" list that they can manage on their own
- Personal Passlist—users can designate certain email addresses as "good" without having to bother your IT person
- Image based filtering — scans images within emails to stop this new type of spam
- PDF based filtering — protection from spam leveraging PDF attachments
- POP, IMAP & SMTP support
- Reports give a comprehensive view of the spam environment on your network, including the source of the spam and how much spam is received in aggregate and by user

Active Directory (AD) Connector

Integrate Apps & Reporting with Active Directory

The AD Connector is designed to leverage your Microsoft Active Directory server to simplify policy management and enrich reporting. Active Directory can be used for:

- Reporting by user name
- Enforcing policy, such as web content restrictions, by user name

Microsoft's Active Directory is an identity management tool that is popular with many businesses. By integrating with Active Directory, i-Filter makes it easy for administrators to leverage the rights and privileges they've already established for users on their networks. Users also benefit because they don't have to remember any additional passwords. Even management loves the integration because leveraging Active Directory usernames in reporting makes it easier to understand who is doing what on the network.

Key Features:

- Leverage existing Active Directory deployments
- Authenticate by AD username
- Logging & reporting by AD username
- Automatic software updates & upgrades
- Installs on the i-Filter platform with in seconds after download
- Guaranteed to integrate seamlessly with other i-Filter apps
- Runs at the gateway with no client software to install
- Reporting (PDF & HTML) and logging to monitor network, system & user behavior

Policy Manager

Customize Network Access by Time or User

Policy Manager enables administrators to fine tune network privileges. Policy Manager's intuitive GUI and "virtual rack" metaphor makes it easy for administrators to:

- Create network access policies by username
- Create network access policies by time or day of the week
- Assign permission to users for applications such as instant messenger, gaming, and video streaming.

Policy Manager is for administrators with complex networks where one size doesn't fit all. Many organizations need to provide unique privileges to different sets of users like schools (teachers vs. students), libraries (librarians vs. public Internet terminals) or businesses with different departmental requirements (engineering vs. sales.) Policy Manager even makes it possible to block access to common productivity-killing websites like Myspace or Facebook during working hours, but keep it available during lunch and after hours.