

## Spyware *Interceptor*™

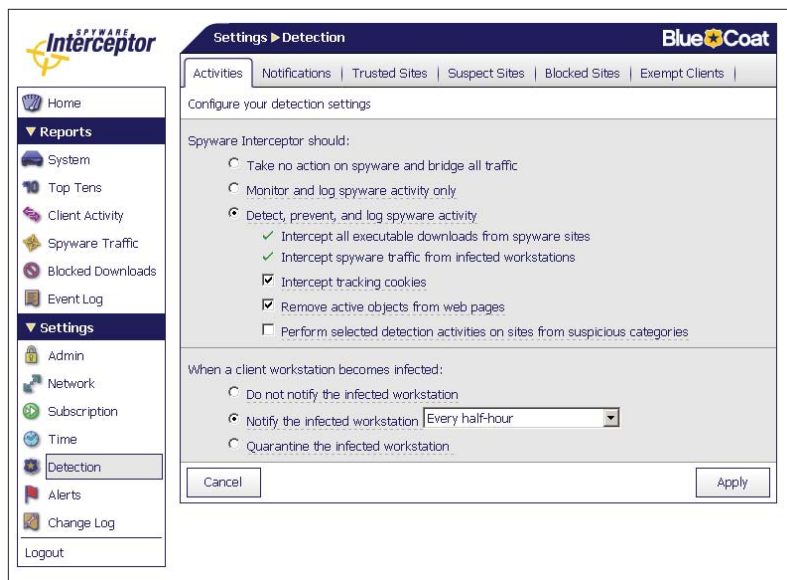
**Easy. Effective. Affordable.**



Blue Coat Spyware *Interceptor*™ is an easy-to-deploy anti-spyware appliance for networks of up to 1000 users. Interceptor prevents known and unknown spyware while enabling legitimate applications via proven proxy technology. Interceptor's patent-pending SCOPE™ anti-spyware engine optimizes its ten methods of protection continuously to minimize the need for cleaning spyware, keyloggers and adware from your desktops.

Spyware Interceptor gateway benefits include:

- Easy, affordable, and effective at preventing spyware
- Automatically updates spyware profiles, policies, and prevention techniques
- Backed by world-leading experts in web proxy performance and security at Blue Coat Labs™



*Point-and-click policy setting for fast, easy administration*

***“Blue Coat's Spyware Interceptor will enable us to stop spyware before it reaches our desktops, and it is so easy and affordable, it should pay for itself in about six weeks.”***

Tom Trumble, network administrator for Merrimack County, New Hampshire.

### Spyware *Interceptor*™

#### **Stops Spyware**

Provides gateway prevention to reduce cost and hassle of cleaning spyware off networked PCs

#### **8-Step Installation Wizard**

Transparently installs in line with firewall in minutes, with fail-open architecture

#### **Proxy-based**

#### **Anti-spyware Appliance**

Powerful policy control over web traffic with point-and-click web-based policy settings

#### **Strips Unauthorized Installers, Executables and Active Content**

Configurable to prevent spyware downloads from known, suspicious, and potential sources while allowing page views and legitimate applications

#### **Prevents Spyware From “Phoning Home”**

Protects your confidential information, and reports which PCs may be infected

#### **Monitor-Only Mode**

Assess how much undesirable and unknown executable content is being downloaded onto your users' PCs

#### **Block Unknown Spyware**

Optional suspect-file, unknown file, and rules-based filtering techniques can prevent many new and unknown spyware types

#### **True-File-Type Identification**

Detect file type spoofing to block deceptive executable downloads

[www.spywareinterceptor.com](http://www.spywareinterceptor.com)

**Venture capitalists invested \$140 Million in spyware startups**

*Advertisers pay spyware producers to serve behavior-based ads, by paying web site operators to host spyware installers. Venture capital has helped spyware get more sophisticated.*

**Spyware Growth**

### The Spyware Problem:

**Spyware degrades PC performance, wastes employee and help desk time, and puts confidential information at risk. And it's everywhere.**

- IDC estimates 67% of all computers have some form of spyware. <sup>(1)</sup>
- Microsoft estimates more than half of all Windows operating system failures are caused by spyware. <sup>(2)</sup>
- Gartner says as much as 25% of corporate help desk calls are coming from end users whose systems are overwhelmed with spyware. <sup>(3)</sup>

**Desktop prevention tools and cleaners are of limited effectiveness, difficult to centrally administer, and typically treat only symptoms—not the problem.**

- 72% of IT professionals surveyed in February 2005 said desktop cleaners were ineffective in preventing spyware. (339 people surveyed) <sup>(4)</sup>
- 39% was the average detection and removal score of 20 leading desktop scanners against 425 spyware samples in an October 2004 review. The best scored only 72% in this SpywareWarrior review. <sup>(5)</sup>
- 74% of IT professionals re-image some or all of their desktops as a way to completely clean infected systems, and that still leaves them vulnerable to the next infection. <sup>(6)</sup>

**Existing network defenses (e.g., Firewalls, IDS/IPS) are ineffective against application level threats like spyware, and often block critical business web applications with crude on/off controls.**

(1) [http://www.idc.com/getdoc.jsp?containerId=pr2004\\_11\\_23\\_102854](http://www.idc.com/getdoc.jsp?containerId=pr2004_11_23_102854)  
(2) [http://www.wired.com/news/technology/0,1282,63345,00.html?tw=wn\\_story\\_page\\_prev2](http://www.wired.com/news/technology/0,1282,63345,00.html?tw=wn_story_page_prev2) (Wired News 5/7/04)  
(3) <http://computerworld.com/softwaretopics/software/groupware/story/0,10801,98226,00.html> Dec. 13, 2004.  
(4) <http://informationweek.com/story/showArticle.jhtml?articleID=159402838>  
(5) <http://spywarewarrior.com/asw-test-guide.htm>  
(6) <http://informationweek.com/story/showArticle.jhtml?articleID=159402838>

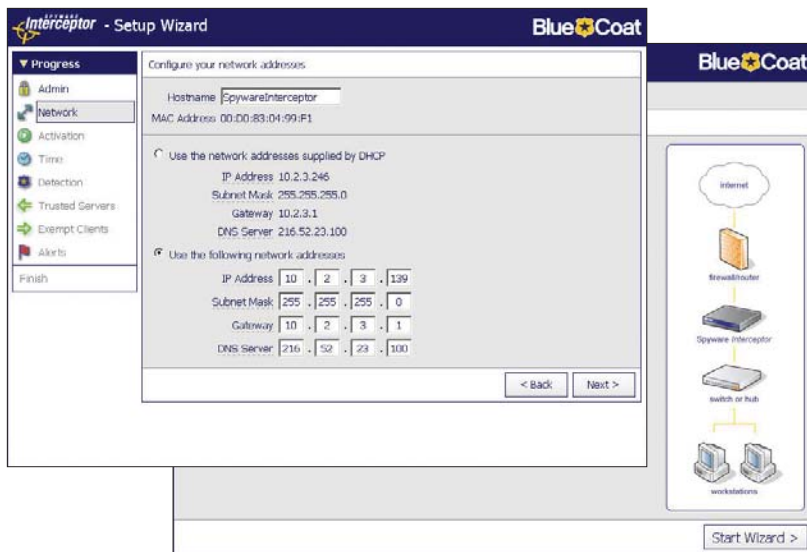
## Why is the spyware problem so difficult to solve?

- Spyware is rapidly recompiled so that signature-based systems are unable to keep up with the numerous, easily generated, original spyware files from web servers, rendering signature-based approaches ineffective.
- Packet-based systems cannot recognize the difference between appropriate executables and spyware, hence they are not accurate enough to be effective.
- Simple URL filtering systems are binary. They block the entire web page, sometimes inhibiting legitimate business usages, or do not block at all allowing spyware downloads to the entire organization.
- Spyware desktop cleaning utilities only report when a PC is already infected, and then only for known spyware infections. Tests show they can not completely remove 30-60% of the spyware, leading many IT professionals to simply reimage infected PC's.

## What makes Blue Coat Systems' approach unique?

While spyware executable code changes every few days or hours, the sites that push spyware are much more constant. Once a website has taken money for pushing spyware, it is highly likely they will continue to do so. Blue Coat prevents spyware by tracking those sites known or highly likely to push spyware, and then removing the potential spyware code in downloads from those sites.

Blue Coat's optimized and streamlined proxy appliance delivers the best balance of spyware prevention and business process enablement for a uniquely real-world solution. Only Blue Coat Systems has the necessary combination of world-class proxy expertise (20,000+ installations) to understand Web objects, plus the depth of content filtering expertise (over 8.0 million web sites analyzed) required to identify known and likely spyware sources, strip out spyware downloads, yet enable needed page views. This combination delivers effective, sustainable and usable gateway spyware prevention.



## Spyware Interceptor: The Right Choice

Spyware Interceptor is easy, effective and affordable. Spyware Interceptor incorporates the Blue Coat patent-pending SCOPE (Spyware Catching Object Protection Engine) technology with 10 methods of preventing known and unknown spyware at the gateway. Spyware Interceptor leverages Blue Coat Labs' expertise with proxy and web traffic to ensure necessary executables, installers, and active content can continue to function.

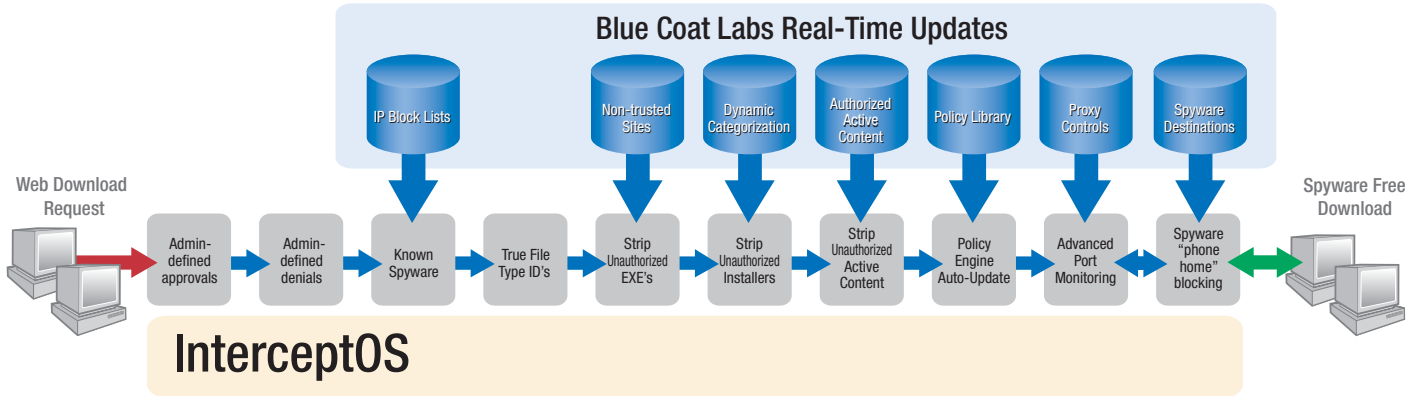
*An installation wizard helps you configure and deploy Spyware Interceptor in as little as a few minutes.*

## Blue Coat Spyware Interceptor Features and Benefits

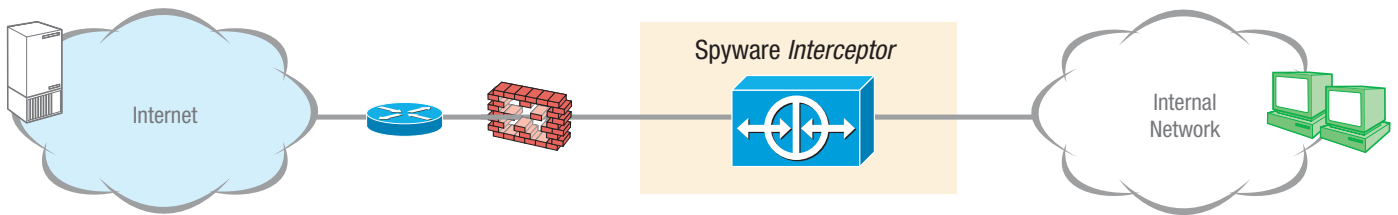
Feature	Benefit
Dedicated anti-spyware appliance	Easy. Effective. Affordable.
<b>Easy</b>	
8-step installation wizard	Set up in as little as 10 minutes
Point-and-click policy setting	Saves administrator time and effort
In-context help	Quickly learn terms and implications of features
Monitor-only mode	See likely effects before implementing policy for smoothest possible deployment
User-proof architecture (no end-user cooperation needed)	Maximum reliability and simplicity
Dedicated appliance with automatic updates	Short learning curve for quick success with minimal administration
<b>Effective</b>	
Strips spyware but permits page views	Supports required business processes
Prevents unknown spyware	Future-proof design delivers highest protection rates
Strips unauthorized EXEs and "drive-by" Installers	Minimizes time and cost of cleaning spyware from desktops
Protects against port-agile spyware (e.g., CoolWebSearch)	Blocks even the most challenging spyware types
Blocks spyware from "Phoning Home" & identifies infected PCs	Protects your data, minimizes financial liability
Customizable "allow list" & "block list"	Ensure legitimate web applications function
True file type identification for better security	Blocks spyware pretending to be harmless file types
Patent-pending SCOPE™ anti-spyware engine	10 methods deliver strongest current and future protection
<b>Affordable</b>	
Optimized hardware/software bundle	High value package
Prevents spyware from reaching desktops	Reduces help desk costs, performance problems, and idle workers
Single appliance to deploy and manage	Least administrative load for lowest Total Cost of Ownership (TCO)
Policy engine with automatic, continuous updates	Stays flexible and secure for year(s) with minimal administrator involvement

## The SCOPE engine provides unmatched spyware prevention

Blue Coat's patent-pending Spyware Catching Object Protection Engine (SCOPE) intercepts and analyzes all executable web traffic, then implements preset policy preferences to remove known, likely, or simply potential spyware. SCOPE allows viewing the non-executable portions of web pages whenever possible. SCOPE uniquely evaluates risk based on characteristics of the executable code and a comparison of the referring site to more than 8 million analyzed sites. SCOPE uses 10 methods of spyware prevention that can be configured with a simple GUI. SCOPE blocks known and unknown spyware both inbound and outbound, while enabling page views and legitimate applications.



Blue Coat's patent-pending SCOPE technology utilizes 10 methods of preventing known and unknown spyware at the gateway.



Spyware Interceptor installs transparently inline behind the firewall for the easiest possible installation, and includes an ethernet bypass card for maximum robustness.

### Spyware Interceptor Specification Chart

	Model SI-1
<b>System</b>	
Disk drives	40 GB
RAM	512 MB
Network Interfaces	(2) integrated; 10/100 on-board port, plus pass-through card for fail open stance
<b>Operating System</b>	InterceptOS
<b>Operating Environment</b>	
Power	AC power 100-240V, 65 watts
Temperature	5°C to 35°C (41°F to 94°F)
Humidity	Less than 90% relative humidity, non-condensing
Altitude	Up to 2000 M (6,561 feet)
<b>Dimensions and Weight</b>	
Enclosure	19" Rack-mountable with mounting kit
Height	44 mm (1.72 in); 1 rack units
Width	191 mm (7.5 in), 442 mm (17.4 in) with rack kit
Depth	356 mm (14 in)
Weight	2.3 Kg (5.1 lbs), 3.3Kg (7.3 lbs) with rack mount
<b>Regulations</b>	
Emissions	FCC Class A, EN55022 Class A, VCCI, BSMI, NOM
Safety	UL 60950 3rd Edition, EN60950 CSA C22.2 No. 950 M95
<b>Support</b>	Standard warranty: 90-day software & phone support with 1-year hardware support; extended and upgraded support plans available

### Blue Coat Support Services

Blue Coat supports its products with an outstanding customer support program. All Blue Coat products come with a 90-day software and one-year hardware warranty. Support services include a WebPower password enabling access to the following:

- Online access to open technical support cases, review open cases, and add comments to existing cases
- Exclusive support documentation, installation notes, and FAQs
- Blue Coat Instant Support provides an online self-service portal for your technical needs

\* Hardware will be shipped same day when RMA Requests are received during regular business hours and deemed necessary by Technical Support before the RMA cut off time.