

# Security at the Desktop – Your First and Last Line of Defense

This Defense in Depth Report  
discusses the results of a survey  
conducted in September, 2007



Blended Systems, LLC • 8240 Blackfoot Trail • Jonesboro, GA 30236  
770-603-0300 • [www.blendedsystems.com](http://www.blendedsystems.com)

# Table of Contents

Executive Summary . . . . .	<a href="#">3</a>
General . . . . .	<a href="#">4</a>
Impact of Malware on Organizations . . . . .	<a href="#">4</a>
Attack Fronts . . . . .	<a href="#">4</a>
Viruses vs. Spyware . . . . .	<a href="#">4</a>
Trouble Making vs. Economics . . . . .	<a href="#">4</a>
Telling the Difference - I've stopped viruses, isn't that enough? . . . . .	<a href="#">5</a>
Survey Results - Comparison . . . . .	<a href="#">6</a>
Virus vs. Spyware Infestation . . . . .	<a href="#">6</a>
Virus vs. Spyware Infestation Recovery . . . . .	<a href="#">7</a>
Virus vs. Spyware Feelings of Security . . . . .	<a href="#">8</a>
Spyware Best vs Need to Add Protection . . . . .	<a href="#">9</a>
Virus Infection . . . . .	<a href="#">10</a>
Virus Damage Recovery . . . . .	<a href="#">11</a>
Anti-Virus Defense Tools . . . . .	<a href="#">12</a>
Confidence Level - Virus Protection . . . . .	<a href="#">13</a>
Spyware Infection . . . . .	<a href="#">14</a>
How Much Work Was It to Stop the Spyware Infestation? . . . . .	<a href="#">15</a>
Confidence Level - Spyware Protection . . . . .	<a href="#">16</a>
Best Protection Against Spyware . . . . .	<a href="#">17</a>
Where to Add Protection - Spyware . . . . .	<a href="#">19</a>
Conclusions & Recommendations . . . . .	<a href="#">20</a>
Recommendations . . . . .	<a href="#">20</a>
Reference vendors . . . . .	<a href="#">20</a>

## **Executive Summary**

To provide the best security for a network, the rings of defense (Firewall, Email & Desktop) must be tuned to optimize the balance of risk of loss, criticality of data at risk against the budget.

This report focuses on the mechanisms of data loss at the desktop. Blended Systems offered a survey (co-sponsored by Webroot) to over 7000 organizations. The sizes of these organizations range from less than 100 to significantly over 1000 workstations.

The results show that most organizations have been infected by both viruses and spyware. This in itself is not unexpected. The status after the infection, perception of security and perceived needs are what we find interesting.

Most organizations have been infested with either viruses or spyware. Many workstations now bristle with anti-virus and/or anti-spyware tools. We have some concern about these tools stepping on each other and impacting performance at the desktop. With all the defense tools respondents reported, many still don't feel secure against the next attack and feel they need to add protection at each level.

## General

### Impact of Malware on Organizations

- Financial Fraud is #1 source of financial loss in businesses, government agencies and universities (12th Annual Computer Crime and Security Survey)
- Malware is #2 source of financial loss in businesses, government agencies, and universities (12th Annual Computer Crime and Security Survey)
- Cybercrime is #3 priority for the FBI, following counter-terrorism and counter-intelligence
- More than 20% of all companies do NOT have adequate protection against online viruses and spyware
- Cybercrime in its various forms – computer crime, identity theft and phishing – costs the U.S. economy more than \$117 billion each year (Government Accountability Office/GAO)

### Attack Fronts

Attacks at the desktop come from three fronts: infected email, browsing to an infected website and infected files transferred from other workstations or files available from the desktop. To fully secure a workstation, the IT department must have a strong defense at all three levels. However, as the Gartner Report: *Magic Quadrant for Secure Web Gateway, 2007* says, "...the primary challenge is demonstrating significant diversity between client and gateway malware detection techniques..."

Since the workstation is an endpoint device, it is the both the first and last defense line against security attacks. It is the last line of defense when some malicious item gets through the firewall during a browser session or when someone opens a piece of mail with some malicious item in it. It is the first line of defense when a user plugs in a USB drive with a malicious file on it.

### Viruses vs. Spyware

Viruses started as a bragging gimmick to show how clever the creator was at programming. They soon became destructive as each copycat virus creator wanted to show that their skills were better than their peers. Virus payloads now include spyware such as keyloggers, rootkits, malware and spam generators. Viruses may also spread adware and browser pop ups. While the latter category are probably less destructive than the former group, they may act as a channel leading to spyware containing websites.

### Trouble Making vs. Economics

The primary difference between viruses and spyware is the motivation behind them. Viruses are primarily designed for bragging rights. Spyware has behind it an economic incentive.

While there are still destructive viruses in the wild, most viruses in the wild contain some sort of spyware.

**Telling the Difference - I've stopped viruses, isn't that enough?**

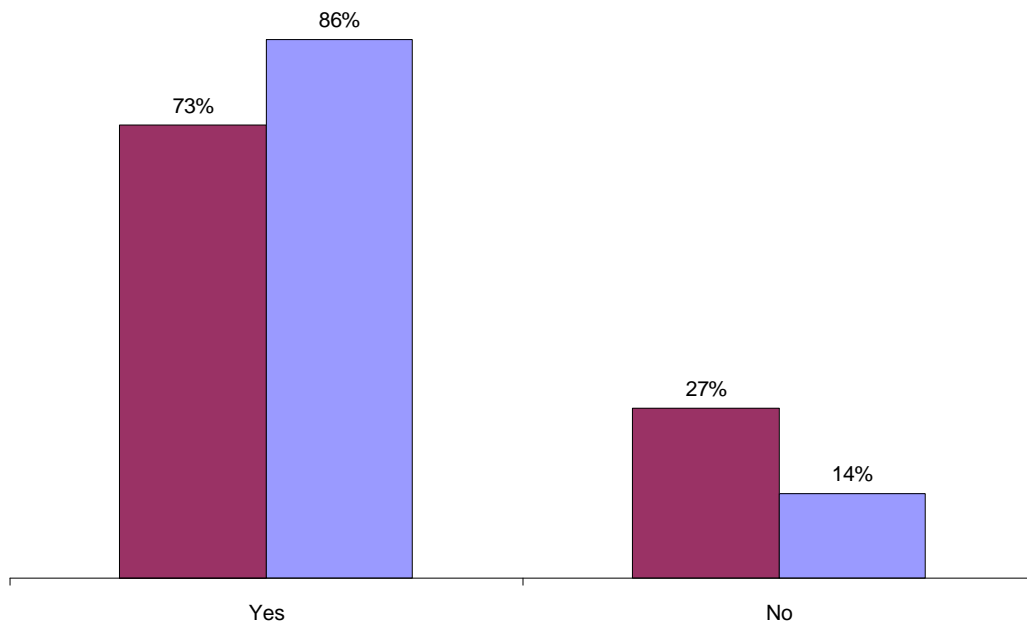
If spyware were only spread by viruses, yes. However, spyware comes in via three channels now: via the web through an weak firewall, via email messages coming through a weakness in email protection, and directly to or through the desktop by means of direct file transfer.

Defense in Depth means protecting all three fronts. While this survey covered are three areas, we focused the questions on the desktop in the interest in brevity for the volunteer survey takers.

## Survey Results - Comparison

### Virus vs. Spyware Infestation

While we asked about virus and spyware infestation separately, it is interesting to compare the results.

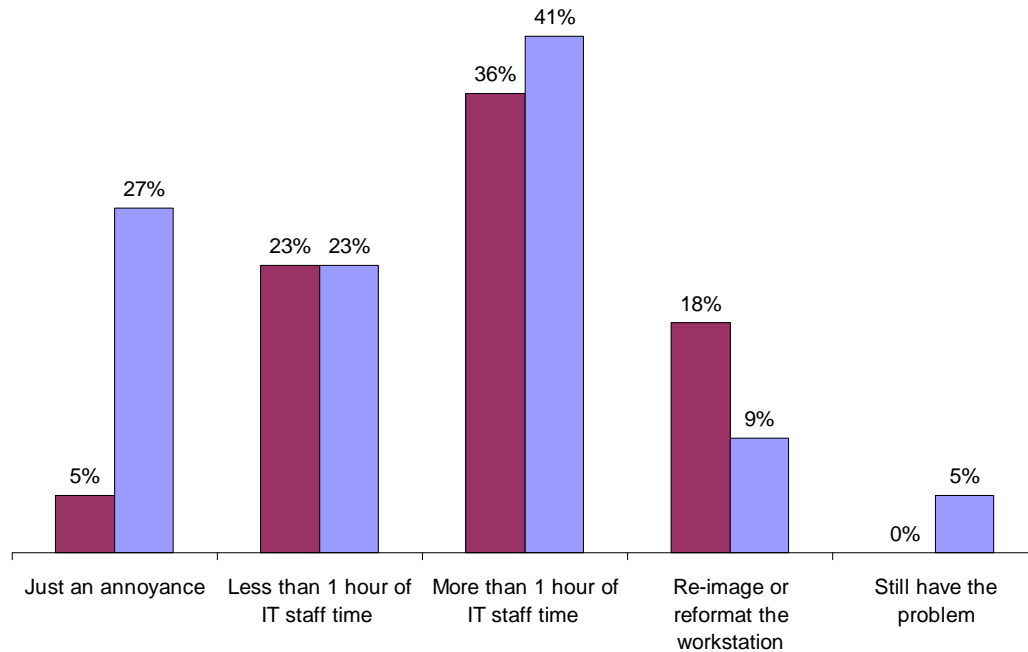


**Figure 2** - Have any of the workstations in your business been infested with a **virus** (spyware)?

No surprise here. Most organizations who responded to our survey have experienced both a virus and a spyware attack. Note that more respondents indicated they have had a spyware infestation than had a virus attack.

## Virus vs. Spyware Infestation Recovery

The recovery effort shows the difficulty in removing spyware in contrast to viruses.



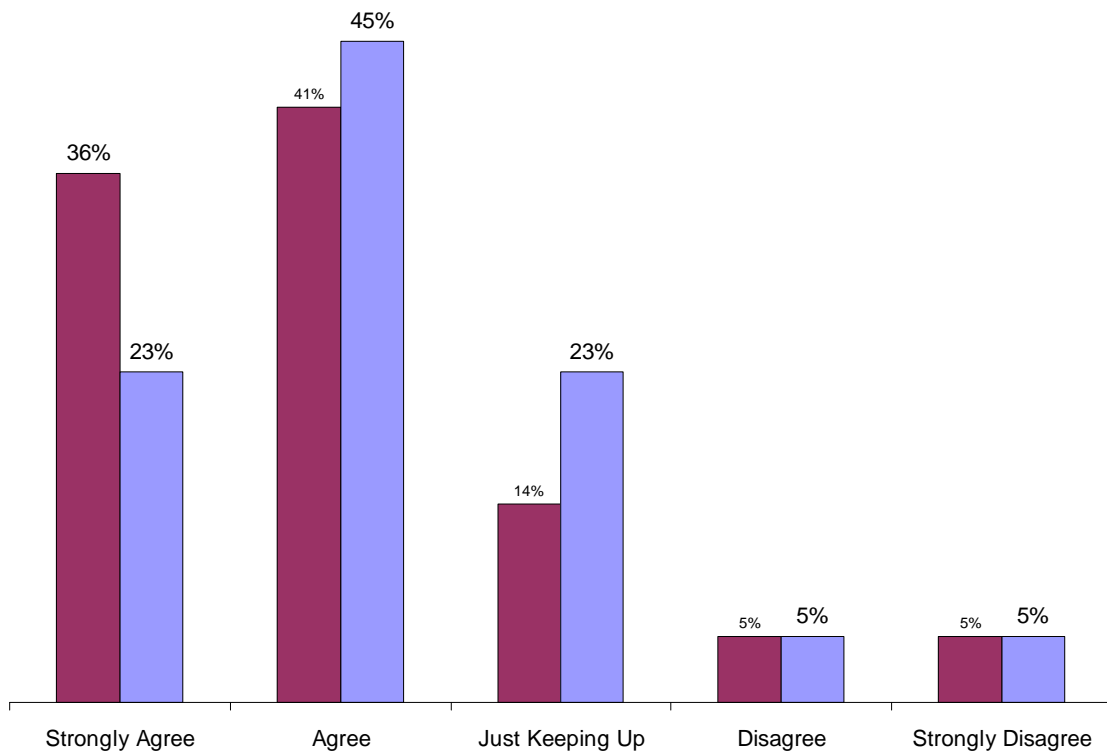
**Figure 3** - How much trouble was it to remove the **virus** (**spyware**) infestation?

What is interesting is the report of how much work it was to recover from these attacks. The difference between recovery from a virus and from a spyware attack shows several things. Recovery from a virus attack is generally easier than from a spyware attack. Different kinds of spyware are easier to deal with than others. Defense against Cookies and pop-up ads are often built into browsers now and are easier to remove than are keyloggers, trojans and rootkits. Fully 55% said recovery from a spyware attack took longer than 1 hour, required a re-image or reformatting of the workstation or the problem was still in place.

Because of the economic component to spyware, the spyware propagator wants to protect their "investment" in the infected workstation once the spyware is entrenched. It takes an excellent anti-spyware engine to remove spyware components such as rootkits and some keyloggers.

## Virus vs. Spyware Feelings of Security

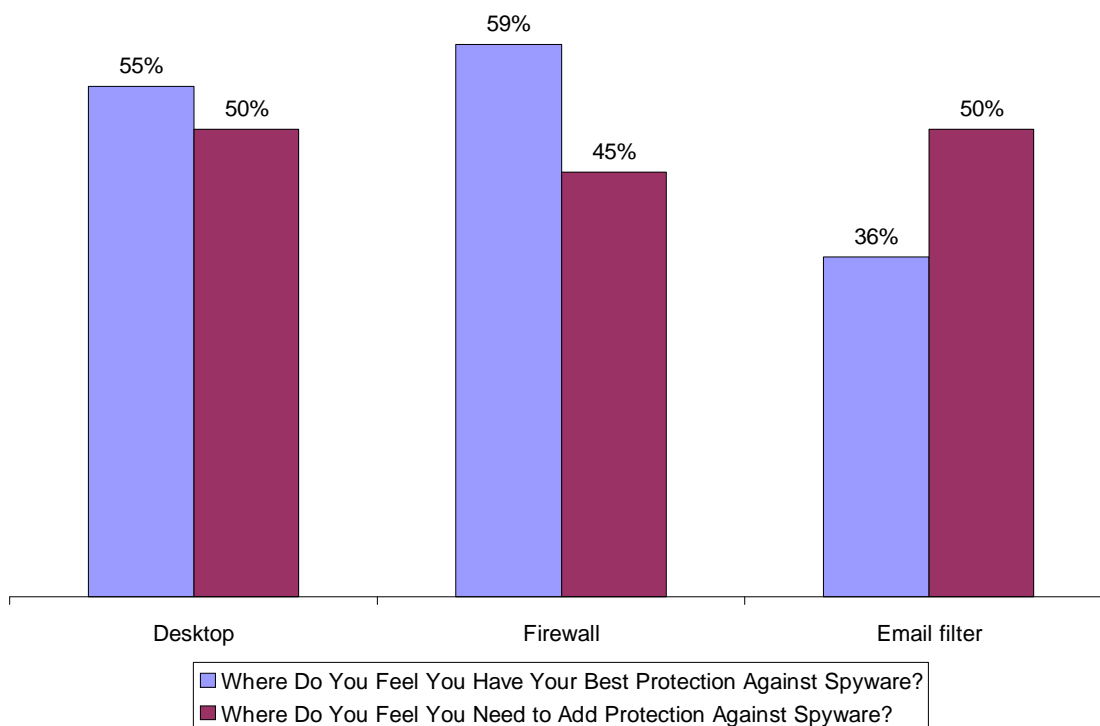
We asked our survey takers how secure they felt against future infestation.



**Figure 4** - I feel secure in our defense against **virus** (**spyware**) infestation.

With virus and spyware protection in place, more respondents feel vulnerable against spyware (34%) than they do against virus (24%) infestation. The next chart shows where they feel vulnerable.

## Spyware Best vs Need to Add Protection



**Figure 5** - **Best** existing vs Need to **Add** protection against spyware.

Every respondent wanted to add protection in at least one position and a few wanted to add protection in all three locations. The question is where is the best place to add protection?

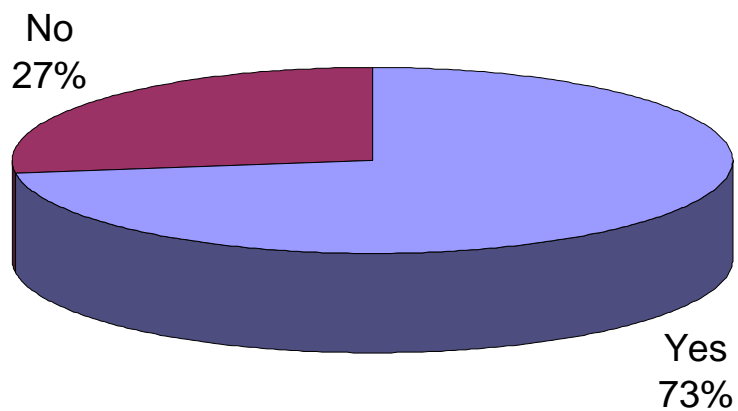
Email filters usually include an anti-virus engine as well as an anti-spam engine. Unless spyware rides in a message not seen as spam or containing a virus, you are unlikely to be hit with spyware via an email message. From the standpoint of spyware, it's good to beef up this channel but, email is not the major route for incoming spyware. Most spyware comes in via a browser (through the firewall) or by direct file transfer.

Unless a firewall contains web content protection, it cannot do much in the way of preventing spyware via a browser. It must contain some content filtering intelligence to be of use at this critical outer ring. We will be offering a survey and webinar on this critical point in November, 2007.

Regardless of the source of the infestation, the workstation is the First and Last Line of Defense. First line against direct file transfer from files available via shares or portable storage devices. Last line against incoming infestations that have gotten through email and firewall filters.

## Virus Infection

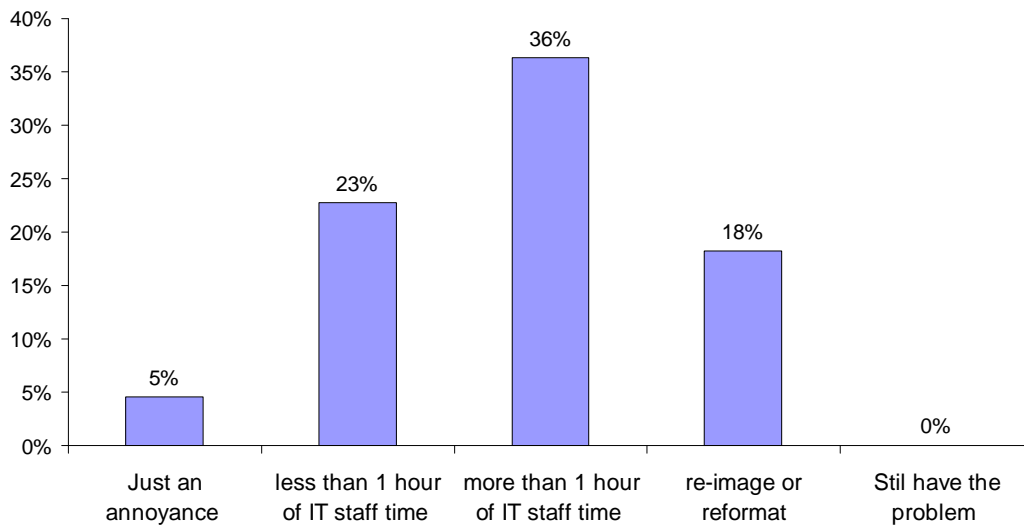
We asked our survey takers about their experience with virus outbreaks on their organization's workstations. It came as no surprise that almost three quarters of them said that they have had a virus infection. Virus attacks have been going on since the 1980s and most organizations have anti-virus defense in place.



**Figure 6** - Have Any of the Workstations Been Infested with a Virus?

## Virus Damage Recovery

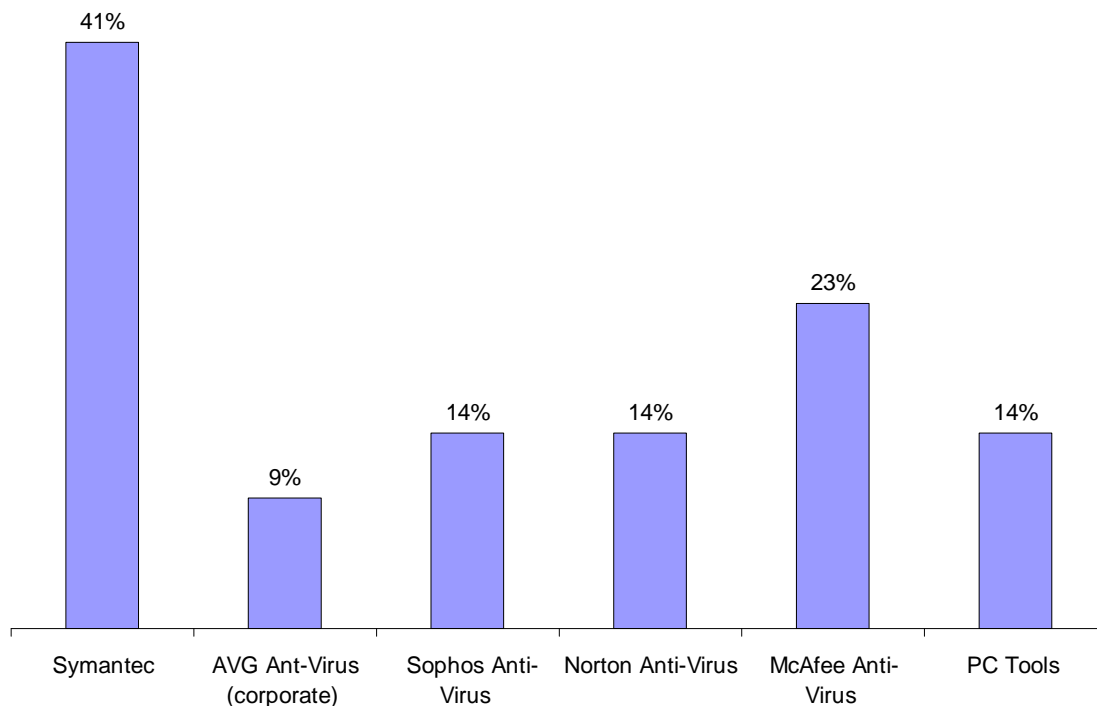
These attacks did some damage but, that damage was limited as seen in the following graph. Fully 54% of respondents reported that it took more than 1 hour of staff time or they had to re-image or reformat the workstation to recover from the virus infection.



**Figure 7** - How Much Work Was It to Stop the Virus Infestation?

## Anti-Virus Defense Tools

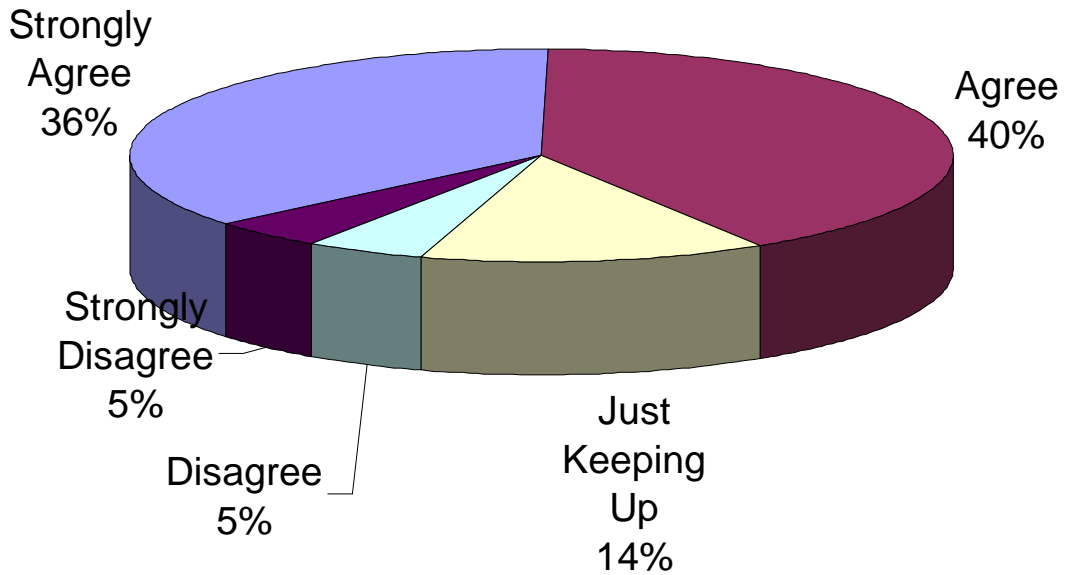
The collection of tools the respondents have in place is varied. As one would expect, the leaders are Symantec/Norton Anti-Virus with an 41% aggregate representation and McAfee with 23%.



**Figure 8** - What tools do you have in place to stop viruses at the desktop?

## Confidence Level - Virus Protection

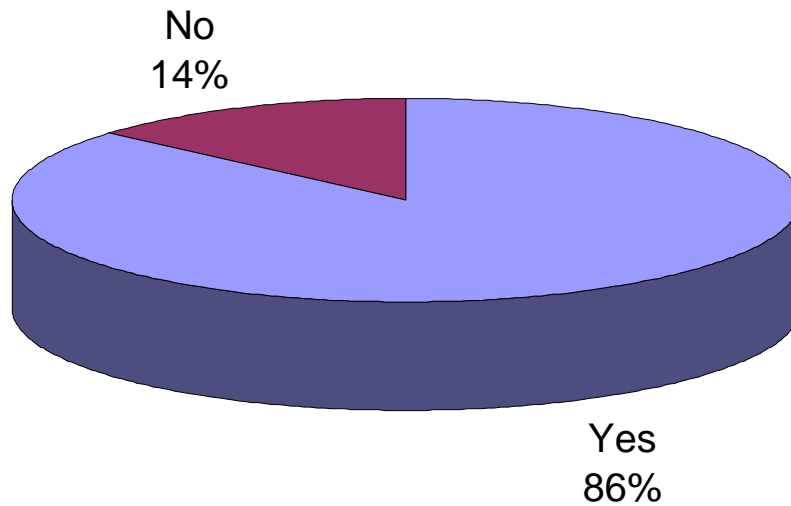
When asked their confidence level against future virus attacks, 24% of the respondents felt they were just keeping up or did not feel confident on their ability to fend off the next virus attack. Clearly, those organizations are concerned about infestation.



**Figure 9** - I Feel Secure in our Defense Against Infestation by Viruses

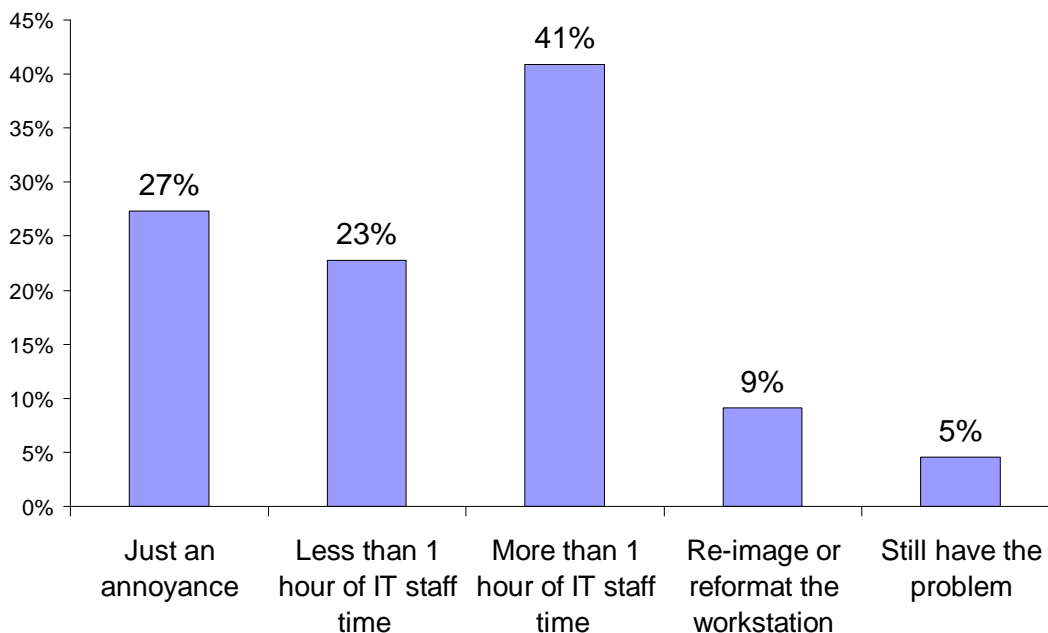
## Spyware Infection

We asked our survey takers about their experience with spyware outbreaks on their organization's workstations. It came as no surprise that 86% of them said that they have had a spyware infection.



**Figure 10** - Have Any of the Workstations Been Infested with Spyware?

## How Much Work Was It to Stop the Spyware Infestation?



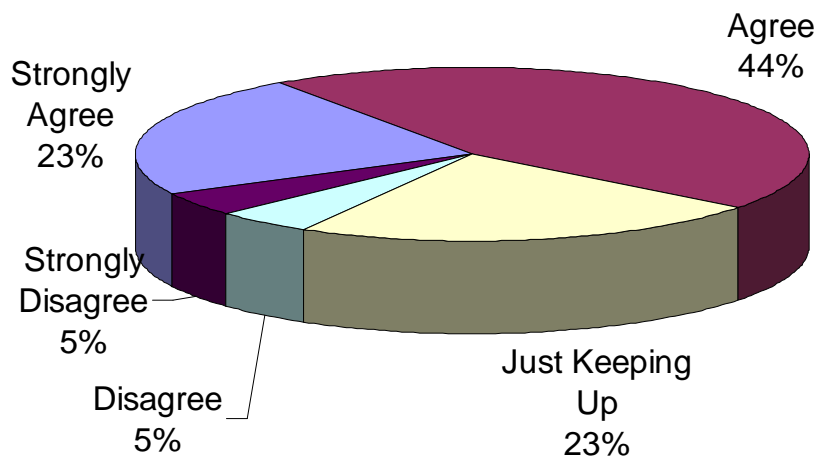
**Figure 11** - How Much Work Was It to Stop the Spyware Infestation?

This survey did not differentiate among various kinds of spyware. Defense against Cookies and pop-up ads are often built in to browsers now and are easier to remove than are keyloggers, trojans and rootkits. Fully 55% said recovery from a spyware attack took longer than 1 hour, required a re-image or reformatting of the workstation or in a few cases, the problem was still in place.

Because of the economic component to spyware, the spyware propagator wants to protect their "investment" in your workstation once it is entrenched. It takes an excellent anti-spyware engine to remove spyware components such as rootkits and some keyloggers.

## Confidence Level - Spyware Protection

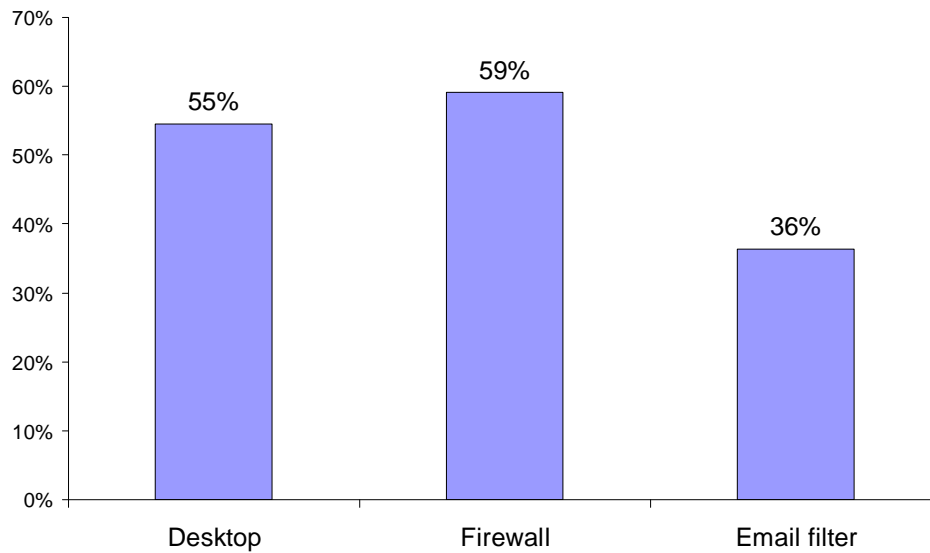
When asked their confidence level against future spyware attacks, 33% of the respondents felt they were just keeping up or did not feel confident on their ability to fend off the next spyware attack. This is a higher percentage than those that do not feel confident about their ability to fend off virus attacks.



**Figure 12** - I feel secure in our defense against Spyware attacks.

## Best Protection Against Spyware

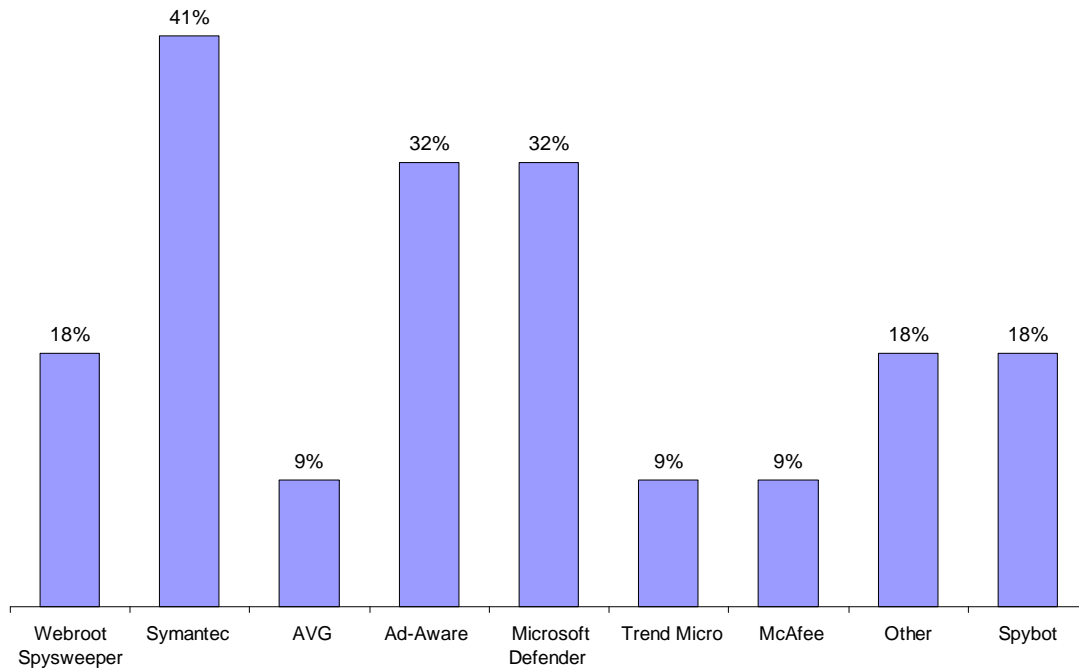
The respondents obviously recognize that spyware has three main vectors for infiltration. What's interesting is their view of their strongest lines of defense are the firewall and the desktop. Contrast this with where they feel the need to add protection against spyware below.



**Figure 13** - Where do you feel you have your best protection against Spyware?

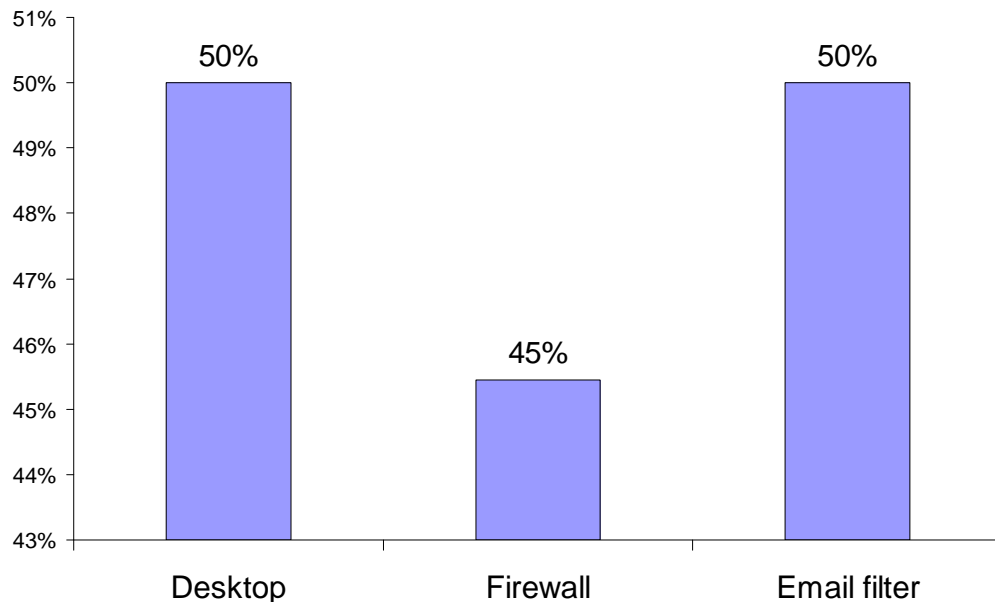
## Anti-Spyware Defense Tools

The spyware defense tools are more varied than are the virus tools. We grouped all responses below 5% in the "other" category. Several of the respondents reported having several tools at the desktop under the theory that different suppliers have better tools than others. They feel that they need to have a "team" approach in dealing with spyware.



**Figure 14** - What Tools to You Have in Place to Stop Spyware at the Desktop?

## Where to Add Protection - Spyware



**Figure 15** - Where Do You Feel You Need to Add Protection Against Spyware?

Every respondent wanted to add protection in at least one position and a few wanted to add protection in all three locations. The question is where is the best place to add protection?

Email filters usually include an anti-virus engine as well as an anti-spam engine. Unless spyware rides in a message not seen as spam or containing a virus, you are unlikely to be hit with spyware via an email message. It's good to beef up this channel but, email is not the major route for incoming spyware. Most spyware comes in via a browser (through the firewall) or by direct file transfer.

Regardless of the source of the infestation, the workstation is the First and Last Line of Defense. First line against direct file transfer from files available via shares or portable storage devices. Last line against incoming infestations that have gotten through email and firewall filters.

## **Conclusions & Recommendations**

Almost every organization has been hit by a virus or spyware attack. Recovery from these attacks have often been painful for the IT staff. They are planning by deploying multiple tools at the desktop to prevent and ameliorate the effects of the next attack. While their confidence level is generally good, some respondents are feeling vulnerable against the ever present probing of the spyware generator.

Regardless of the source of the infestation, the workstation is the First and Last Line of Defense. 1st line against direct file transfer from files available via shares or portable storage devices. Last line against incoming infestations that have gotten through email and firewall filters.

### **Recommendations**

- Be sure the multiple tools for anti-virus or anti-spyware are not interfering with the performance of the workstation. Often multiple tools looking for the same problem significantly degrade the workstation's performance. It is better to have one fully-capable tool than a several less capable tools attempting the same task.
- Investigate where the enterprise can get the greatest value for the security budget. To do this, find out if you still have a problem at the desktop. Blended Systems will perform a spyware audit on as much of your network as you wish. You will receive a report showing what problems are found where. From this information you can make an informed decision as to whether your existing tools are in fact doing the job you wish.
- If you are not pleased at the level of protection at the email or firewall security ring, ask for a demo of technologies where you feel weak. They are free and can be implemented in parallel or series with your existing systems.

### **Reference vendors**

Blended Systems partners with several vendors which specialize in data defense. Here is a list and description of each.

#### **Defense at the Desktop – Webroot**

Administrators need a desktop tool that handles both virus and spyware infestation in a centralized administration point. It must not only detect but prevent infestation as well as repair after an infestation. Webroot has two primary products of interest for enterprises. Webroot AntiSpyware Corporate Edition and Webroot AntiSpyware Corporate Edition with AntiVirus. <http://www.blendedsystems.com/webroot>

### **Defense at the Email Gateway – NEMX Technologies**

Among other things, NEMX SecurExchange provides inbound, outbound and internal email content filtering using software running on an Microsoft Exchange server. All email can thereby be protected, not just inbound messages. <http://www.blendedsystems.com/nemx>

### **Defense at the Email Gateway -- Mirapoint**

Mirapoint produces both full email appliances as well as email security appliances. The RazorGate email security appliance has a throughput of over 2.4 million messages per day with full Anti-Spam and Anti-Virus protection. <http://www.blendedsystems.com/mirapoint>

### **Defense at the Firewall – Astaro**

Astaro produces three kinds of firewall Unified Threat Management appliances: hardware, software & VMware™. Each appliance can be a point solution (eg., email security, network protection, SSL-VPN or Web protection only) or combine these solutions in a device or devices. <http://www.blendedsystems.com/astaro>

For more information on Blended Systems'  
services and products or  
if you have any questions about  
this report please contact us at:

Blended Systems  
8250 Blackfoot Trail  
Jonesboro, GA 30236  
877-603-0301

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

Email: [info@blendedsystems.com](mailto:info@blendedsystems.com)



© 2007 Blended Systems, All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Blended Systems, LLC, nor may it be resold by any entity other than Blended Systems, LLC, without prior written authorization of Blended Systems, LLC.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.