



Since network misuse is widespread and can have a significant impact on network performance, we asked the survey respondents to indicate how they monitor for abuse. Just under forty percent of the survey respondents indicated that they do not actively monitor for network abuse.

Fifty-three percent of the survey respondents use a variety of somewhat informal techniques to monitor for network misuse. One example of this is having end users or managers report abuse. Another example is to identify misuse by exception; i.e., when troubleshooting a network problem. The respondents tended to use these techniques roughly equally at the headquarters and data center, as well as at remote sites.

In addition, over seventy percent of the survey respondents use multiple active measures to identify network misuse, including the use of content filtering (72%), network monitoring systems (64%), and firewalls or other security programs (81%). However, the use of these measures varies widely based on the type of site. For example, over three quarters of the survey respondents use these techniques in a data center and roughly two thirds of the survey respondents use these techniques in a headquarters site. However, under half of the survey respondents use these techniques in remote locations.

The fact that a relatively small percentage of IT organizations use active measures to identify network misuse at remote locations is somewhat disturbing in part because over the last few years the role of the branch office has changed dramatically. For example, up until a few years ago it was common to have the majority of a company's employees reside in a headquarters site and access applications locally. In addition, if an employee at a headquarters site wants to access the Internet, they typically do so over a high speed WAN link. Today most of the employees at the typical company do not reside in a headquarters site and they use the WAN to access a growing number of applications - both ones that are approved and appropriate and ones that are not. Given the number of employees that reside at remote locations and the ability of just one or two of these employees to congest a relatively low-speed WAN link by streaming internet radio, it is time for more IT organizations to actively monitor remote locations for network misuse.

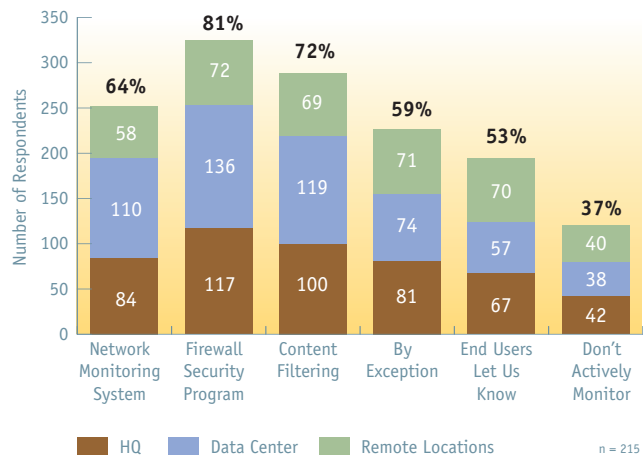


Figure 2 depicts the specific techniques that companies use to monitor for abuse as well as where they apply these techniques. To explain Figure 2, it is helpful to realize that 215 members of the NetScout community responded to the survey question that asked how they monitored for network abuse and that they could select multiple monitoring techniques and implement those techniques at multiple locations. For example, one hundred and seventy four (81%) of the survey respondents indicated that they use firewalls and security programs to monitor for network abuse in one or more components of the network - 117 in headquarters, 136 in data centers and 72 in remote locations.

### Conclusion

Up until a few years ago, few networking professionals had any responsibility for application performance. Now, it is becoming increasingly common for the network organization to be held responsible for application performance.

Ensuring acceptable application performance is not easy. The first step is to understand what applications are running on the network. The second is to make sure that network misuse is minimized and that few if any WAN vicious applications are deployed, and the third and final step is to be able to do proactive alarming to identify, and hopefully resolve, issues prior to their impacting the users.

For more information on this topic and others like it

**CLICK HERE**

or visit [www.netscout.com](http://www.netscout.com)



NetScout Systems, through its *nGenius*® Performance Management System, offers large organizations cohesive views into application services delivered over today's complex, global networks, helping IT professionals optimize network and application performance and prevent misuse of critical enterprise resources. Based on granular, flow-based

performance information gathered across the enterprise, the *nGenius* System delivers key performance management functions, including application and network monitoring, capacity planning, troubleshooting, and user experience assurance, in a single integrated solution.

For more information visit [www.netscout.com](http://www.netscout.com).