



National Instruments® Ensures Productivity & Network Availability with Mirage NAC™



National Instruments, a global technology pioneer and leader in virtual instrumentation, implemented Network Access Control (NAC) from Mirage Networks® to protect its networks from day-zero worms and viruses and other rapidly propagating threats.

THE NETWORK ENVIRONMENT

National Instruments has direct operations in nearly 40 countries with more than 3,500 employees and a very diverse PC environment that includes Windows XP, Windows 2000, Windows 9x, Linux, MacOS, and Solaris. At its Austin, Texas-based corporate campus alone there are nearly 6,000 IP devices on the network - ranging from office productivity machines to software development and test machines to PCs used to run its manufacturing line. This large, varied environment makes keeping all systems up to date and properly configured difficult at best.

National Instruments has always taken a layered approach to security, which includes active patch management programs and centrally managed antivirus software. Inevitably, some systems fall behind and allow worms and viruses to propagate in its environment. In the past, the National Instruments IT staff spent a significant amount of time cleaning up machines that became infected, especially given the rate at which new worms are released. These worms and viruses also had a direct impact on productivity.

BUSINESS CHALLENGE

The primary need was protecting employee productivity as well as data and information assets, and reducing the Help Desk staff workload required to repair infected machines. In addition to the impact from various worms, National Instruments realized the existence of the very real potential for the release of much more destructive worms. Of greatest concern: a rapidly propagating worm that carries a destructive payload and deliberately destroys data. The results of such a threat entering the network environment — while “in the wild” (not yet detected by the National Instruments antivirus solution) — could be very serious. National Instruments believed it was critical to add another layer to its security model that would help stop such a threat.

Ease of deployment and maintainability were also important considerations. The company was reluctant to deploy yet another piece of software to every machine in its environment, increasing operational burden of managing additional updates and upgrades and the risk of software incompatibilities or performance impacts.

» executive summary

Industry:

- » Technology/Manufacturing

Business Challenges:

- » Maintain network integrity and availability, and protect employee productivity
- » Secure network from day-zero worms and other threats, from 6,000+ endpoints across multiple operating systems
- » Accomplish the above while lessening impact on IT resources

Security Solution:

- » Deploy Mirage Network Access Control on corporate campus network
- » Roll out deployment in European and Asia-Pacific offices

Business Value:

- » Reduction in operational costs and lost productivity due to virus outbreaks
- » Reduction in IT workload due to easy deployment and maintenance
- » ROI of up to 122% over 3 years, not including intangibles such as opportunity cost

SECURITY SOLUTION

National Instruments deployed Mirage Networks' NAC security appliances on its corporate campus in Austin, Texas. The company also scheduled deployments in seven of its international branches.

The Mirage NAC security appliances provide an agentless solution to stop worms that manage to get past other layers of the National Instruments defenses. The devices watch the internal network without needing to sit inline, negating any potential detrimental impact on network performance or reliability. The appliances use a unique behavior-based monitoring technique that does not require virus definition updates like traditional antivirus products. This means that they can identify and react to day-zero threats. Once an infected machine is identified by the Mirage NAC appliances, it is instantly "cloaked" (removed from the network), preventing the worm from propagating. The appliances send a notification to the National Instruments Help Desk so IT staff can work with the owner of the cloaked machine to clean it and bring it up to date on patches and antivirus software.

Implementation was quick and easy. First brought up in "audit mode," the Mirage appliances simply watched the network and identified potential threats without actually taking any action. Once the Mirage appliances proved successful in identifying infected machines, the company put the devices into "attack mode" and allowed them to begin actively defending the network. This defense includes stopping the rash of new mass-mailer worms that lately have been plaguing the Internet.

BUSINESS VALUE

National Instruments realized a reduction in operational costs associated with IT response to virus outbreaks as well as a reduction of lost productivity costs due to virus outbreaks.

Ease of implementation was also a strong driver. Because the Mirage solution is agentless, the company did not need to add another piece of software that would have to be managed on thousands of PCs and servers.

THE BENEFIT

National Instruments began seeing benefits immediately. The Mirage solution identified infected machines and stopped worms from propagating on its network. In addition, the company believes that it has a good insurance policy in place to protect itself against any destructive worms that may be released. Given that a truly destructive worm in the wild could cause significant damage to the company's productivity, National Instruments is happy to have the Mirage appliances in place as a layer of defense.

The result of the Mirage implementation is that only one or two machines are infected by any given threat, instead of tens or even hundreds, dramatically reducing IT cleanup time and lost productivity. In 2005 alone, National Instruments has seen six instances of worms introduced into its enterprise environment before its antivirus solution could detect them. The Mirage solution stopped the worms from propagating throughout its environment and limited their impact. Portions of the enterprise not yet protected by a Mirage appliance were infected and required labor-intensive IT attention and clean-up.

ROI

Based on historical data, National Instruments estimates that the Mirage appliances will stop between six and 10 average worm outbreaks per year (that may not have been prevented or stopped by other components of its security infrastructure). As the rate of new viruses/worms increases, this estimate will increase.

This means the company will save between a projected \$78,000 and \$130,000 annually (depending on the number of potential outbreaks) in IT response costs and lost productivity. There are significant additional considerations that may make this savings number higher:

- Even average outbreaks in its international branches cause wide area network performance problems that adversely affect the productivity of all staff at that branch, not just the infected PC. These productivity costs are hard to estimate, but are significant and have real business impact.
- Not included in these ROI numbers are the lost "opportunity costs" of IT personnel around the globe not free to expend effort on productive tasks because of the clean-up required after virus outbreaks.
- Also not included in these numbers are any large outbreaks that the Mirage appliances would stop.
- Finally, these ROI numbers are based on nondestructive outbreaks (worms that do not destroy any of the company's corporate data that would then either have to be restored or recreated). If such a worm propagated, it would be caught and stopped by the Mirage appliances, thus resulting in even greater savings because of the dollar cost associated with the restoration or recreation of that data. Thus, the Mirage solution offers additional "insurance policy" value to National Instruments above and beyond the current operational savings.

Mirage Networks
6801 North Capital of Texas Highway
Building 2, Suite 200
Austin TX 78731

phone: 866.869.6767
fax: 512.874.7806
email: info@miragenetworks.com
web: <http://www.miragenetworks.com>

©2005-2006 Mirage Networks, Inc. All rights reserved. Mirage Networks, the Mirage Networks logo, CounterPoint, Full-Cycle NAC, and You can't control people. Control what's on your network., are trademarks or registered trademarks of Mirage Networks, Inc. All other names and marks may be trademarks of their respective companies.