



Wyeth

Customer profile

One of the largest research-based pharmaceutical and healthcare-product companies in the world. Wyeth's R&D budget in 2007 was more than \$3.2 billion

Industry

Healthcare

IT environment

Wyeth supports more than 54,000 desktops globally with about 25 percent running Windows 2000. The company maintains four desktop ePO servers with 30 file repositories and 140 Zen servers with 560 Network Application Launcher (NAL) objects

Challenges

Deliver reliable protection for Wyeth's more than 54,000 desktops

McAfee solution

- McAfee Total Protection (ToPS) for Endpoint
- McAfee ePolicy Orchestrator (ePO)
- McAfee VirusScan Enterprise for Linux
- Resident Onsite Support Account Manager

Results

- Provides comprehensive spyware and anti-virus protection to more than 54,000 desktops
- Simplifies IT and security management with easy-to-create scheduled and ad hoc reports
- Scans millions of files and registry keys every day
- Thwarts buffer overflow attacks

Wyeth Enlists McAfee to Protect Global IT Environment from Pervasive Threats

Wyeth, headquartered in Madison, New Jersey, is one of the largest research-based pharmaceutical and healthcare-product companies in the world, dedicated to solving the world's most critical health problems through substantial investments in research and development.

As a global company, Wyeth faces pervasive security threats. For example, Wyeth scans more than 66 million files and 100 million registry keys every day. Using McAfee technology, Wyeth detected more than 2,000,000 malware infections and 16,000 unique malware items in the past year.

Constant vigilance

At Wyeth, McAfee VirusScan® Enterprise is the sole desktop protection product, augmenting the company's network and border-level security and monitoring solutions. Several times per month, through the use of firewall logs and malware report analysis, Wyeth's IT security team identifies desktop and laptop devices that exhibit behavior associated with worm, virus, or spyware activity. In most cases, this behavior stems from an executable file located on the infected device. During an outbreak, McAfee tools are essential in planning mitigation.

"Most of the time, our McAfee software can detect the malware and remove it," explains Ed Carroll, associate director of Global Client Computing for Wyeth. "In fact, the day-to-day protection works so well without impairing the user experience that it's taken for granted. Sometimes we need to submit a file to McAfee and they provide a .DAT signature file update. We use that to clean and protect Wyeth's entire desktop environment from further infection."

Buffer overflow attacks are another significant and all-too-common concern. The malicious code that executes as a result of a buffer overflow runs with administrator-level privileges, and can do virtually anything—none of it good—to a server.

"These attacks are easy to mount," adds Greg Stewart, Wyeth's IT security consultant. "That's why buffer overflow protection was a driving factor in selecting VirusScan Enterprise over other products. We also appreciate other features like the mini-firewall, root kit scanner, and email scanner."

ePO: The key to managing a large, diverse IT ecosystem

Wyeth relies on McAfee ePolicy Orchestrator® (ePO™) to produce regular and ad hoc reports on the status of devices managed by the company's ePO servers. Project managers use routine status updates on the health of the desktop environment to support various upgrade projects. ePO reports also provide critical information on the scope and spread of infections during any type of outbreak. And, ad hoc reporting enables IT security to make on-the-fly vulnerability assessments during newly discovered attacks.

“ePO limits the number of employee hours spent on deployment, management, and monitoring,” Carroll says. “When we upgrade to 4.0, we’ll be able to manage a diverse group of client machines with different organizational policies—corporate, manufacturing, research laboratory, and sales laptops—from one server.”

According to Carroll, this capability aligns with Wyeth’s goal of global server consolidation. The upgrade also supports easier delegation of reporting functions because it is browser-based and does not require client software.

“I’ve spoken with people who have worked with the McAfee product at Wyeth for seven years,” says Carroll. “And they cannot think of a significant outbreak in that time. We just haven’t had any outbreaks worthy of mention, like many other companies have, because McAfee has prevented them.”

Resident Onsite Support Account Manager

With annual revenue of over \$20 billion and a large cross section of McAfee solutions (ePO, Total Protection (ToPS) for Endpoint and VirusScan® Enterprise for Linux) protecting its 54,000 nodes globally, Wyeth has recently opted for a 3.5 year McAfee Resident Onsite Support Account Manager to assist in the safeguarding of its business.

The Resident Onsite Support Account Manager (SAM) is Wyeth’s personal security advocate and is thoroughly familiar with Wyeth’s McAfee deployment and support history. The Resident Onsite SAM becomes a critical contributor within Wyeth’s team by attending staff meetings and planning sessions. He has a sound understanding of Wyeth’s plans and strategic direction and provides 24/7/365 proactive product support and planning assistance, operational advice, and direct intercession with other McAfee teams on Wyeth’s behalf.

Being onsite also enables the SAM to see any issues first-hand and be able to quickly resolve them.

With easy-to-manage McAfee solutions, Wyeth no longer had need for a full-time security contractor. With the savings, Wyeth was able to offset a large portion of the cost of the Resident Onsite Support Account Manager.

Most of the time, our McAfee software can detect malware and remove it. It works so well, it’s taken for granted.

Ed Carroll
Associate Director
Global Client Computing
Wyeth

