intego

VirusBarrier Server
Antivirus Protection for Mac OS X Servers

The threat of viruses and malware affects Macintosh computers, just as it affects computers running other operating systems. Companies running servers with Mac OS X must protect these servers from viruses that infect files or e-mail attachments. This is important not only to protect the servers and Mac clients on the network, but also to protect against malware that can infect computers running other operating systems. Using a strong, reliable server-side antivirus solution for Mac OS X servers can provide the first level of protection for networks with Macs. This white paper will examine how companies running a Mac OS X server can benefit from using Intego VirusBarrier Server and VirusBarrier Mail Gateway.

Working with a Mac OS X Server

Macintosh computers are increasingly popular in enterprise environments because of their ease-of-use, their reliability, and the creative software they offer. Especially popular in the publishing and design industries, Macs are making inroads into other sectors. Mac laptops—the MacBook and MacBook Pro—offer compelling feature sets that make them among the more popular choices for portable computers.

In addition to using Macs as client computers and workstations, more and more companies are building networks around Macs running Mac OS X Server, the robust Unix-based server operating system that runs either on Xserves or on other Macs. But as always with servers, the virus threat increases exponentially by the number of files that are stored on the server, that pass through it, or that transit via its mail server.

System administrators are well aware of the threat of viruses on a server. While a virus on a client computer or server can damage files on that computer, and eventually propagate throughout a network via files that are emailed or sent over a network, a virus on a server could damage all the computers on the network. Viruses on a file server that don't affect the server itself, if it is running a different operating system from client computers, can still propagate as users copy files to their computers. Beyond viruses, many types of malware, such as worms and Trojan horses, can infect servers, granting remote access to malicious users.

Mac OS X servers are used in a variety of environments, from Mac-only networks to networks containing a mixture of Macs, Windows PCs and Unix or Linux workstations. Protecting a Mac OS X server against viruses requires that not only Mac viruses be detected, but also Windows viruses, Word and Excel macro viruses and Linux viruses.

The Macintosh Virus Threat

Macs have been historically less vulnerable to viruses, though history shows us that the first computer virus that appeared in the wild was one that affected an Apple computer. Called "Elk Cloner", this 1982 virus, intended to be nothing more than a joke, and causing no serious damage, affected computers running Apple's DOS 3.3 operating system and spread via floppy disks.

While Windows computers now claim the majority of viruses, the threat to Macs is growing. As Apple's market share increases, hackers will augment the amount of malware they disseminate that targets Macs.

Recent events have shown that hackers are working hard to develop Mac viruses and malware, with consequences that can range from simply infecting and damaging applications (the Leap.A malware[1]) to deleting all the files in a user's home folder (the AS.MW2004.Trojan[2]). In addition, a number of exploits that have recently been made public affect Apple's Safari web browser, its QuickTime media software, and its Bluetooth software. Some of these exploits can lead to file damage, and others may provide access to remote users who can then copy or alter files on infected computers, or take control of them completely.

Macs, like all computers, are at risk from viruses, malware, hackers and vandals, and require reliable protection. IT administrators need to consider the most effective and efficient ways to protect not only the Macs in their companies or institutions, but also to ensure that Macs do not become vectors for malware that can harm other computers. In addition to the possibility of Macs becoming infected by viruses, or being compromised by other forms of malware, Mac users may share documents with others, which, while not dangerous to Macs, could compromise computers running other operating systems.

It is therefore necessary to have a server-side solution to protect servers running Mac OS X servers from viruses and malware. Not only does this protect the servers, but also ensures that files that transit through these servers do not

the time one of these people finds out that the file contains a virus, it's too late to stop its spread, and an entire network may be compromised.

But even if a server-side antivirus solution is used, Macs on the network may still get infected. Many users have portable storage devices, such as USB key drives, iPods or mobile phones, that they use to carry files between their home and the office. They may bring CDs or DVDs to work with files they have modified at home; if their home computers are not protected, these files may be infected. And users of laptops are constantly, when traveling, connecting to unprotected networks in hotels, airports, coffee shops and more. When working on these networks, they may become prey to malicious users who sniff IP traffic in search of computers they can attempt to plunder or control.
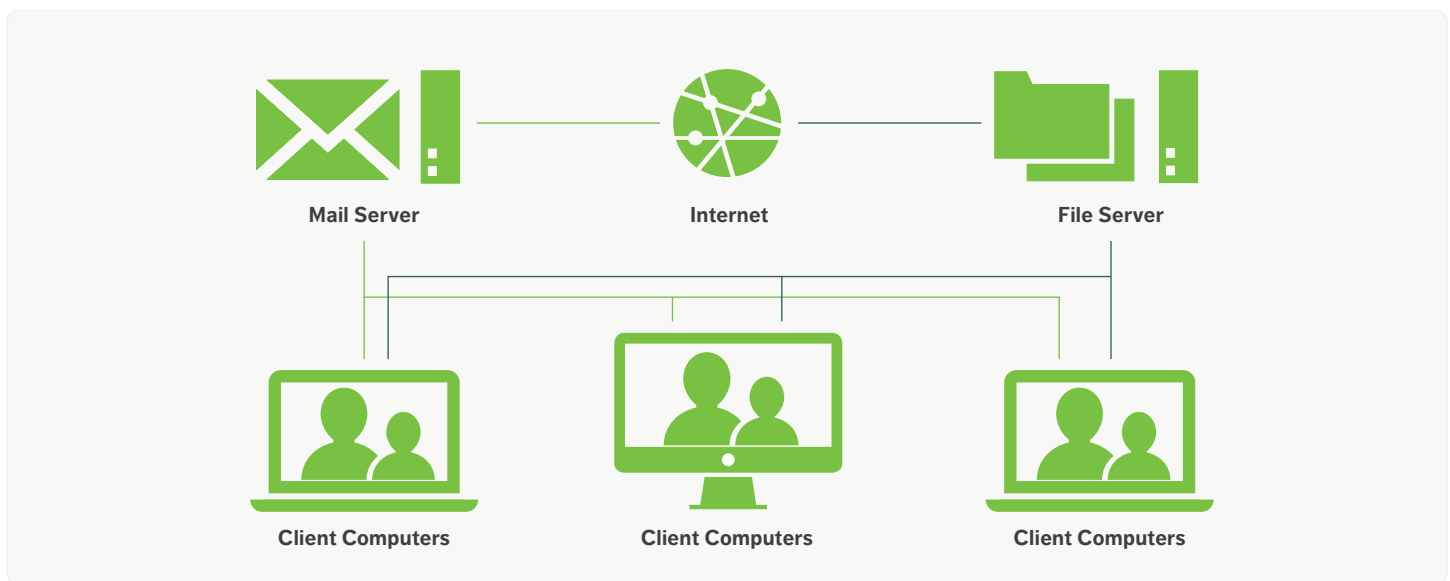
Both file servers and mail servers can spread viruses and malware to client computers on a network.

contain potentially dangerous payloads that could affect client computers.

Protecting Macs from Viruses in an Enterprise Environment

Viruses and malware can infect Macs in many different ways. The most common vectors are e-mail and web sites. Users receive e-mail messages with attachments, or they visit malicious websites and their Macs become infected with malware via exploits that can affect a web browser, or simply by downloading files or applications. Users may install an application downloaded from the web, unaware that this software may in fact be a Trojan horse. Or they may deposit an infected file on a file server, which may then be copied by dozens or hundreds of other people. By

For this reason, it is also essential that a desktop antivirus program, such as Intego VirusBarrier X4, also be installed on all Macs in enterprise environments to protect against these many means of contagion.

Intego VirusBarrier Server: The Ideal Solution for Mac Virus Protection

The virus and malware threat to Macs demands appropriate solutions to protect both Macs and other computers in any company, institution or school. While this danger will inevitably increase, solutions exist that can ensure not only total protection from all known Mac viruses, but ease-of-use, transparency for end users, and trouble-free management and maintenance for network administrators and IT managers.

Benefits of VirusBarrier Server

- A GUI administration console
- Full quarantine zone to isolate infected files
- Detailed logs of all infected files sent to administrators
- Scans of all files written to or opened on the server
- Scheduled scans of local and network volumes
- Self-protection to ensure that VirusBarrier Server doesn't get infected
- Heuristic and behavioral analysis
- Full quarantine zone to isolate infected e-mails
- Infected e-mails can be repaired and disinfected in the quarantine zone
- Notifications of infected e-mails sent automatically to administrators
- Scans of all e-mail sent and received via the Mac OS X Server e-mail server

VirusBarrier Server and VirusBarrier Mail Gateway are based on Intego VirusBarrier X4, a proven antivirus solution, recognized by users and the Macintosh press: Macworld magazine rated it the best antivirus program for Mac[3].

VirusBarrier Server automatically scans every file that is copied to a Mac OS X server where it is installed, as well as any files that are launched on the server. If viruses are found, infected files are quarantined, and administrators can determine which actions to take. VirusBarrier Server can also be set to run scheduled scans of both local and network volumes.

VirusBarrier Mail Gateway offers full protection for all e-mail that is sent or received via Mac OS X Server's built-in e-mail server. It automatically scans all e-mail messages that pass through the server, checking e-mails for infected attachments. If viruses are found, the e-mails are quarantined, and notifications can be sent to administrators informing them of this activity.

VirusBarrier Server and VirusBarrier Mail Gateway include a copy of VirusBarrier X4 offers additional features and give access to certain functions on the server.

VirusBarrier Server requires Mac OS X or Mac OS X Server 10.2.8 or later, running on an Xserve or any Mac configured as a server. VirusBarrier Mail Gateway requires Mac OS X Server 10.4 or later, running on an Xserve or any other Mac configured as a server, running the built-in e-mail server.

The Intego Answer

VirusBarrier Server is the ideal server-side solution for protecting a Mac OS X server, and for ensuring that viruses don't propagate to Macs on a network. VirusBarrier Mail Gateway offers full protection from Mac viruses and malware received as e-mail attachments, for servers running Mac OS X and the included e-mail server. These two programs are ideal choices for businesses of all sizes, schools and institutions that need to protect Macintosh computers and ensure that Macs don't serve as conduits for malware that affects other operating systems as well. Easy to use, reliable, and offering simple maintenance and management, VirusBarrier Server and VirusBarrier Mail Gateway are the antivirus programs of choice for Mac OS X servers.

For more information about VirusBarrier Server, VirusBarrier Mail Gateway, and other Intego Mac security software, visit the Intego web site, **www.intego.com.**

See also Intego's white papers about other enterprise software solutions: Remote Management Console a tool for managing Intego software on multiple Macs, and VirusBarrier X4, the endpoint antivirus solution.

---

[1] **www.intego.com/news/pr77.asp**
[2] **www.intego.com/news/pr43.asp**
[3] **Macworld magazine, July 2006**

---

intego

Intego
10900 NE 8th Street, Suite 1000
Bellevue, WA 98004   USA
Tel: (512) 637.0700
Fax: (512) 637.0701
sales@intego.com
www.intego.com

Intego
41 rue Condorcet
75009 Paris   France
Tel: +33 (1) 55 07 27 27
Fax: +33 (1) 55 07 27 28
eurosales@intego.com