McAfee Active Virus Defense

Viruses Are Not Passive

The threat from viruses changes constantly. More than 300 new viruses are discovered each month. To make matters worse, today's most prevalent threats are worms and mass-mailing viruses that can spread around the world in a matter of hours. Since the virus threat is actively shifting, shouldn't your defense strategy be active too?

The Best Defense is an Active Defense

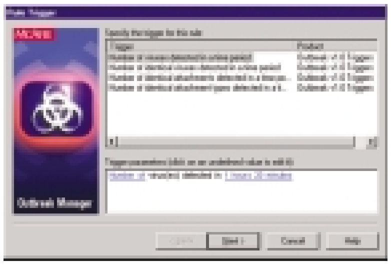
To effectively combat the ever-changing virus threat, you should establish an active anti-virus policy. Most companies today understand the need for virus protection. Many have established formal policies defining what form that protection should take, and how it should be used. But very few take the necessary next step to make their policies active. Making a policy active isn't as simple as just changing it occasionally.

First, Measure

Before you can know what changes should be made to a policy, you need to know which parts of it are working and which are not. Is the virus protection software on all computers being updated according to policy? Are the configuration settings dictated by the policy still applied? Is virus protection even installed on all machines? To know, you need a tool like McAfee's ePolicy Orchestrator. The heart and soul of McAfee Active Virus Defense, ePolicy Orchestrator can help anyone answer all these questions—which will enable administrators to intelligently adjust their policies to the changing virus threat.

Ensure Total Coverage

Once you know where the weak points in your defense are, you can take action to correct the problems. Having world-class virus detection and cleaning software on all computers on the network is a good start. Most companies need protection at the desktop, file server, groupware server, and Internet gateway. Active Virus Defense offers industry-leading protection for each of these four network tiers. Once all the computers on the network are fully protected, ePolicy Orchestrator's policy enforcement features can ensure they stay that way. ePolicy Orchestrator also enables administrators to make configuration changes to handle new virus types or changes in virus prevalence trends.



It's Called A Gateway

There's a reason the point at which a corporate network connects to the Internet is called the Internet gateway: it's a point beyond which some things must not pass. That goes for inbound as well as outbound traffic, and it's just as useful in fighting viruses as in preventing intrusions. As anyone who has administered desktop virus protection software can attest, it's nearly impossible to get all the desktops on a network 100% protected with updated anti-virus software. With today's fast-moving worms, all it takes is one out-of-date machine to start a virus outbreak. If there are other vulnerable computers on the network, the result is a costly clean-up effort. Even if every other computer is well protected, the result can be hundreds of helpdesk calls from users asking if the message they just saw saying a virus was cleaned is correct. McAfee's WebShield Internet gateway virus protection solution can stop Internet email borne viruses before they get to even one user on the network, preventing those costly problems. With McAfee's unique Outbreak Manager technology, WebShield can identify and stop outbreaks even when the virus instigating them is new and unknown. And content filtering capabilities can help kill time-wasting spam and virus hoaxes.

Key Features

- Superior detection and cleaning
  Because that's what it all comes down to, in the end.
- Policy Management
  ePolicy Orchestrator enables administrators define, implement, and enforce a standard anti-virus policy.
- Enterprise-wide Reporting
  ePolicy Orchestrator gives you unprecedented visibility into the state of virus protection on your network.
- Expertise
  AVERT is standing by to help you recover from virus emergencies 24x7, worldwide.
- Support
  There's a McAfee PrimeSupport offering for everyone, from online forums to 24x7 named contact.
- Multi-tier defense
  McAfee products at every level of the network provide a bulletproof defense.

MCAFEE

A Network Associates Business

Groupware Protection

Of course, not every piece of data on a network enters through the Internet gateway. For keeping those emails and collaborative environments virus free, McAfee's GroupShield products are just the ticket. With support for both Lotus Domino and Microsoft Exchange environments, GroupShield stands guard with an arsenal of anti-virus defenses. Outbreak Manager stops outbreaks before they start. Content filtering allows spam and hoax blocking, and can also help keep confidential data from leaving the network. Because it's remotely manageable, GroupShield is well suited to even the largest and most distributed enterprise environments.

The Petri Dish of Computer Viruses

File servers are extremely useful, productive tools. Their utility in collaboration and file storage makes them indispensable. But it also makes them a favorite hiding place for viruses. When Jane User's out-of-date desktop virus protection allows her to upload a virus infected document, all the other users who access that file can become infected. And if the IT team backs up the data on the server regularly, even the backups can wind up infected if they're not careful. McAfee's NetShield server protection can eliminate these potential headaches. It offers both real-time scanning to detect and clean known viruses as files are accessed and on-demand scanning that allows scheduled deep-down bug scrubs of the entire system.

Popular Desktop Protection

Every desktop on the network represents several vectors of infection, or ways for viruses to enter the network. Floppy disks, CDs burned at home, personal email accounts, and PDAs are just a few of the routes a virus might take onto the network. That's why comprehensive, manageable desktop virus protection is essential. VirusScan is the protection of choice for desktops. It's tight integration with McAfee's ePolicy Orchestrator management console makes it a manageable desktop anti-virus solution on the market today. And a host of installation and customization features make it a favorite of enterprise customers.

It's All About Detecting And Cleaning Viruses

At the end of the day, all the manageability and policy enforcement in the world won't stop a virus, if the anti-virus solution can't detect and clean viruses. All the McAfee Active Virus Defense components use the award-winning McAfee virus scanning engine. With unique double heuristic scanning technology, generic variant detection capabilities, and industry-leading compressed file handling, the McAfee engine is one of the best money can buy.

Backed By AVERT

Active Virus Defense is more than just software. It's a partnership with McAfee. It's the support of the McAfee PrimeSupport organization, which can put advice and help from a live person at your fingertips 24 hours a day, 7 days a week. It's the expertise of the McAfee Anti-Virus Emergency Response Team (AVERT). AVERT researchers stationed all around the world combine their expertise and skill to consistently make McAfee one of the first to detect new viruses. When the Anna Kournikova and Homepage viruses were ravaging networks worldwide, McAfee customers were relaxed and doing business as usual, because AVERT researchers had produced products that were capable of detecting and cleaning the viruses months before they were discovered.

Active Virus Defense Includes:

VirusScan

- Runs on Windows 95, 98, Me, NT, 2000; DOS; Linux; HP-UX; SCO; AIX; Solaris

VirusScan Thin Client

- Runs on Windows 95, 98, NT, 2000

NetShield

- Runs on Windows NT and 2000; Netware

GroupShield

- Supports Microsoft Exchange and Lotus Domino

WebShield SMTP

WebShield for Solaris

ePolicy Orchestrator

For more information on products, worldwide services, and support, contact your authorized McAfee sales representative or visit us at:
3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (888) 847-8766
Fax (888) 203-9258

www.mcafeeb2b.com

McAfee
A Network Associates Business