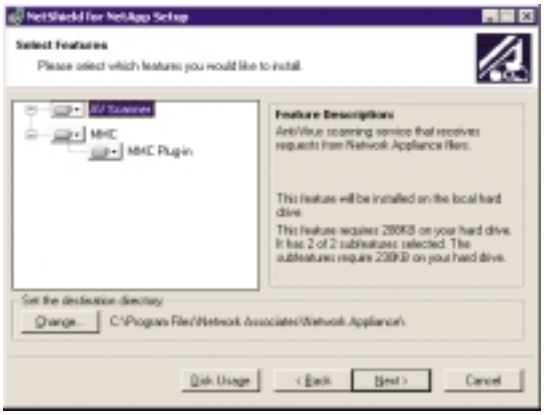
NetShield 4.5 for NetApp®

Superior Virus and Malicious Code Protection for NetApp® Filer Storage Appliances

The requirements placed on network availability by e-business take the threat of virus outbreaks to the next level, no longer are such outbreaks simply a nuisance. Today a virus outbreak that disrupts the flow of an organization's e-business activity will actually affect profitability. In fact, 2000 saw more than $17.1 billion in damages as a direct result of virus infections.

Minimizing the threat of virus attacks on storage systems is what NetShield for NetApp® is all about. This NetShield product combines the award winning NetShield for Microsoft NT product with advanced virus-scanning technology and unmatched management capabilities. It detects virus-infected files that users are trying to access in real-time as well as files that are being written to the Filer. Once detected, the infected file can be automatically cleaned, quarantined, or deleted. McAfee's effectiveness in detecting viruses and other malicious code is demonstrated time and time again in independent tests and NetShield for NetApp® provides continuous protection for your storage systems.

The powerful central management console of NetShield for NetApp® give you complete control over all protected servers from any server or workstation. Enterprise-wide, all monitoring configuration and installation functions can be performed from the convenience of a single console. NetShield for NetApp® working in conjunction with ePO gives true enterprise-wide reporting from one central location, allowing you to understand what is occurring on your network like never before.



Configuring and installing NetShield for NetApp®

Flexible Scanning Options

NetShield provides comprehensive protection for network file servers, capturing both known and new viruses before they infect multiple users. The award-winning scanning engine delivers high-speed scans of all files as they are accessed in real-time. All major file compression formats are supported. Detected viruses can be automatically cleaned, deleted, or even quarantined for future analysis and origin tracing. Never the less, with more than 55,000 known viruses in existence, and more than 300 new ones cropping up every month, a virus security solution is only as good as its most recent update. NetShield's AutoUpdate functionality provides incremental updating, making the process of keeping your virus security state of the art faster than ever before.

Key Features

- Continuous Protection
  On-access scanning protects Filer users in real-time when they are accessing files, plugging the security holes that exist with older on-demand or scheduled scanning methods.
- Detection and Cleaning
  NetShield's award winning scanning and cleaning engine is proven effective time after time as it is continually awarded 100% in independent detection and cleaning tests.
- Load Balancing
  Because the NetShield for NetApp product allows you to bring the power of multiple instances of NetShield to bear on one filer, the scanning load can be balanced across several servers ensuring optimum performance as well as high availability or fail-over at all times.
- Intuitive File Scanning
  File status is cached as an initial scan is performed ensuring clean files are not rescanned unless they get modified giving optimum server performance.
- Infection Reports
  Working in conjunction with ePolicy Orchestrator, NetShield for NetApp® provides detailed infection and trend analysis reports. These reports will show all virus activity on the filer enabling you to trace outbreaks to their sources, detecting users whose virus protection needs to be updated.

McAfee

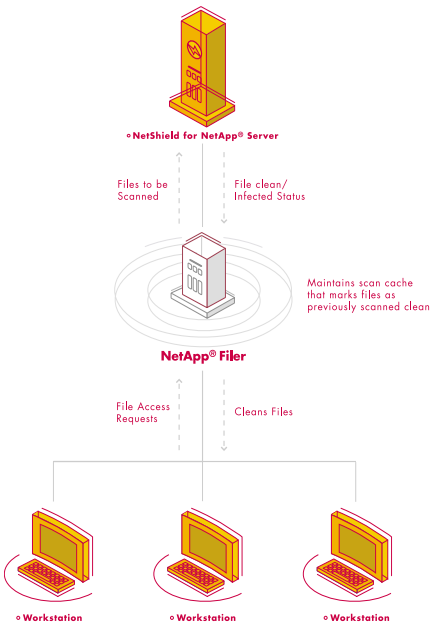
A Network Associates Business

Real-time Scanning

When an end-user attempts to either access or save files stored on the Filer, the Filer signals NetShield to scan the file. The file is then opened by NetShield and scanned. If the file is clean, NetShield signals the Filer that the file is clean, and the end-user is granted access or the file is saved to disk.

If a virus is detected, NetShield will clean or delete the file. If the option to automatically clean all infected files has been selected, NetShield will clean the file and signal the Filer that the user may be granted access. If the option to quarantine or delete infected files has been selected, or a virus is detected that cannot be cleaned, the appropriate action will be taken on the file and the end-user will be denied access.

Any time a virus is detected, regardless of the product configuration, the administrator will receive an alert message. Alert Messages can be sent via email or by utilizing McAfee's Alert Manager functionality, which allows alerts to be sent via pager, SNMP, SMS and Tivoli.



Shows the NetShield for NetApp® scanning process

Load Balancing and High Availability

Multiple NetShield for NetApp® servers can be configured to support one Filer. Giving administrators the peace of mind and security of knowing they have a solid fail-over system in the event of a hardware failure. This also allows the scanning load to be balanced across several servers, ensuring optimum performance at all times.

Advanced Enterprise Reporting

The most difficult aspect of implementing and proactively managing a virus security policy is getting the visibility you need to evaluate your policy's effectiveness and find your network's weak points. Tracing an outbreak to its source or determining effectiveness of virus security policies is effortless with ePolicy Orchestrator's wide array of pre-defined reports. Information on update deployments and virus activity is at your fingertips. Customizing reports to suit your specific needs is just as easy, making ePolicy Orchestrator your most powerful tool in the battle to keep viruses out of your network. There will also be clear justification for the expenditures required in maintaining a proper virus security solution. Administrators may select from a variety of printable and exportable chart types including three-dimensional bar charts, pie charts, line graphs, and tables. ePolicy Orchestrator integrates Seagate Crystal Reports technology and Microsoft's MSDE/SQL 7.0 server for a balance of simplicity and power that suits every size of company – from the corner store to the largest corporations.

Protection from the Newest Threats

There are many Anti-Virus products on the market today, but not all products have 100% detection and cleaning. In today's connected world we're witnessing the constant onslaught of new malicious code threatening corporate security. Virus writers are always there behind the scenes creating new attacks such as ActiveX and Java applets, worms, and Remote Access Trojans (RATs). To combat this never-ending threat and achieve the world's market leading detection and cleaning, McAfee NetShield uses advanced heuristic technologies called ViruLogic to seek out previously undiscovered viruses. ViruLogic has the intelligence to know what characteristics viruses do and do not exhibit; something other scanners cannot achieve. The result is unparalleled detection of new viruses with the fewest possible false alarms. When a new virus is confirmed, the cure is generated and distributed to infected systems.

System Requirements

Note: The following are minimum system requirements only. Actual requirement will vary depending on the nature of your environment.

System

- F85, F720, F740, F760, F820, F840

Disk Space

- 128MB RAM

Other Hardware

- Pentium II 450 MHz
- Dedicated 100MB connection to NetApp" filer

Other Software

- Data ONTAP 6.1 operating system using CIFS protocol
- NT 4.0 SP4+ or Windows 2000 SP1Server

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

1-AVD-NAP-001 8/01