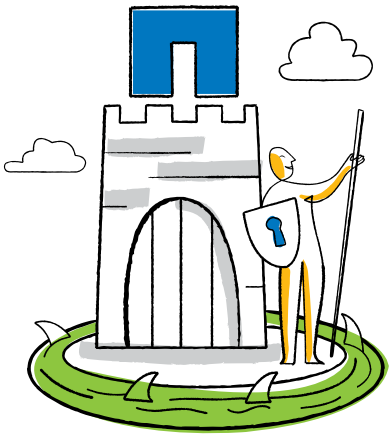

Datasheet

Integrated Virus Protection: Safeguarding Your Data Center

Select from on-board or off-box antivirus scanning solutions

KEY BENEFITS

Antivirus scanning is a must-have feature to protect your organization from cyberattack. Integrated antivirus software can kill viruses at the source, helping to protect data on your NetApp® storage devices from compromised computers.

Whether scanning is performed on board within the storage device using Cluster-Mode or off box using dedicated AV servers, the antivirus functionality is tightly integrated within the NetApp storage device's Data ONTAP® operating system, offering maximum performance and centralized management.

The Challenge

Evolving threats

Corporate networks are under constant siege from attackers using a plethora of weapons, making antivirus scanning a must-have feature. Network-attached storage is constantly exposed to malware if it remains unprotected. In its simplest form, an infected file could get onto the networked storage and spread to client computers throughout the environment. What if you could stop infection at its source, before an infected file can be read or written to your storage environment?

The Solution

Choose what works for your organization

NetApp has partnered with leading AV vendors to offer combined solutions designed to detect and prevent the spread of malicious virus code before data is compromised. This tight integration means that the antimalware solution works in lockstep with the storage system. NetApp supports both on-board and off-box AV scanning, and the choice is yours, because both are deeply integrated within the NetApp Data ONTAP operating system.

If you are running Data ONTAP 8.1 in Cluster-Mode, you have access to on-board scanning from selected AV vendors. If you are running earlier releases of Data ONTAP or in 8.1 7-Mode, then off-box scanning from multiple industry-leading AV vendors is meant for you.

On-board antivirus scanning allows the antivirus engines to directly access the data by using a fast native storage controller protocol, reducing the overhead seen in traditional off-box antivirus solutions. Off-box AV servers use remote procedure calls and an authenticated CIFS connection. Multiple servers can be configured to support one or more NetApp storage devices for redundancy and performance.

Whether on board or off box, AV scanning stops malware in its tracks before it ever reaches your mission-critical data. The AV engine scans files in real time when they are added or modified on the storage system. Scanned file information is persistent in on-board mode, eliminating processing load during on-access scanning as only modified files are scanned. If an infected file is detected, it can be quarantined or immediately deleted per the organization's policy, safeguarding the massive amounts of data stored in the data center.

On Access, On Demand, and After Hours

Complete control of your AV environment

On-access scanning activity is transparent to end users and occurs just after the file is committed to disk (write requests) or before it is delivered to the requesting user or application (read requests). NetApp storage devices will send a scan command to the AV engine and await a reply. When running in on-board mode, the NetApp storage device keeps track of recently scanned files. This improves performance by minimizing redundant scanning activity.

On-demand scanning can scan a single file or the entire storage system and anything in between and can be run manually before a backup and after a restore or on a schedule such as nights and weekends.

Scalability is a key design consideration in clustered storage systems. On-board AV takes advantage of the NetApp cluster architecture to support failover of multiple scan engines. Although not necessary, at least two off-box antivirus servers are recommended for redundancy and higher availability, and the NetApp storage devices will automatically distribute scanning activity among them using a round robin scheme.

The NetApp storage device does not determine the action taken on an infected file. The settings that affect how a virus is handled are determined by the administrator and stored as part of the AV software's configuration. If it is determined a file is infected, the virus software will typically take one of three actions: it will clean, quarantine, or delete the file. The choice is yours based on your risk profile.

Automatic Updates Mean Continuous Protection

Antivirus scanning engines are designed to identify specific viruses by using the information contained in definition files and by recognizing characterized behavior. Antivirus software vendors release new virus definitions when they find new viruses.

When a new virus definition becomes available, the definition update might occur automatically through the Internet or be installed by an administrator. In either case, once a new definition is applied, the virus software will notify the NetApp storage device that a new definition exists. The current scan status is reset, and all subsequent file accesses are scanned with the new virus definition. This makes sure that new viruses are properly identified and removed by the antivirus software.

For More Information

AV technology is constantly improving, and NetApp has made several best practices documents available to you. To download them, or to get the latest information, visit *www.netapp.com* and search for "antivirus" or contact your local NetApp sales representative.

About NetApp

NetApp creates innovative storage and data management solutions that deliver outstanding cost efficiency and accelerate business breakthroughs. Discover our passion for helping companies around the world go further, faster at *www.netapp.com*.

Go further, faster®

NetApp®

www.netapp.com