

Anti-Virus Solution Survey

To be removed for release

V 0.1	11/9/20 initial draft

Contents

1	Introduction	3
2	Antivirus in Enterprise Storage	3
2.1	DELL EMC Isilon Solution	4
2.1.1	Overview	4
2.1.2	Capability	4
2.2	Netapp Solution	5
2.2.1	Overview	5
2.2.2	Capability	6
2.2.3	Limitations	7
2.3	HP Solution	7
2.3.1	Overview	7
2.3.2	Capability	7
2.3.3	Limitations	8
2.4	Other vendors and Trends	8
2.5	Comparison Chart	10
3	AntiVirus in Huawei Storage	11
3.1	OceanStor9000 Solution	11
3.1.1	Overview	11
3.1.2	Capacity	12
3.1.3	Scalability	13
3.2	OceanStor V5 Solution	13
3.2.1	Overview	13
3.2.2	Capability	14
3.2.3	Limitations	15
4	Antivirus Requirements	15
4.1	Key Requirements	15
4.2	Gaps	16
4.3	Strategy for existing solutions	16
4.4	A Different Perspective For Data Center Antivirus Strategy	17
4.5	Trends for Antivirus Solutions	18
5	References	18

1 INTRODUCTION

Security and compliance are always top priorities for enterprise business. Many enterprises generally enforce strict security policies in place regarding virus detection, removal or quarantine. There are several level of security policies that can be applied:

1. Individual user level with per system antivirus solution from 3rd party security vendor
2. Storage system level solutions integrated with 3rd part security vendor

As storage technologies are ubiquitous, most of enterprises utilize large, centralized storage platform or distributed scale out platform to store user home directories, group project deliverables. These files are exactly same type of files stored on end user systems. It is strongly desirable to make sure that viruses are not resident on any of those storage systems. Therefore, storage vendors are well positioned to provide those integrated anti-virus solutions.

Conventionally, there are several approaches. NAS vendors may use 3rd party software designed to scan storage system itself during end user access(user access triggered) or based on manually scheduled policies from a central antivirus scan server. There are methods to do this via RPC or with SMB and NFS. There are drawbacks to these, such as proprietary solutions and non-centralized scanning using NAS protocols. However, a common and simple way to implement this is via the Internet Engineering Task Force (IETF)-ratified, publicly accessible, Internet Content Adaptation Protocol, or [ICAP \(ICAP RFC 3507\)](#).

There are several ways to “trigger” a security scanning. One is defined as “on-access”, in which a file is send to antivirus scan engine when the file is requested by the end user. It is scanned and appropriate actions are taken. The other way is policy driven. Storage administrators can choose different policies that files are scanned proactively by scan engine based on different schedules, file types and system workload etc. Most of organizations generally choose a combination of these two approaches.

In this white paper, we will first introduce major storage vendors’ anti-virus solutions. Then we come up some key requirements for those features. At last, we are proposing an alternative for anti-virus storage features with standalone solution.

This document mainly addresses key requirements for File and Object storage. However, any storage system which can expose similar granularity protocol can be applied too (For example, HDFS).

2 ANTIVIRUS IN ENTERPRISE STORAGE

In this chapter, anti-virus features from various storage companies are elaborated.

2.1 DELL EMC ISILON SOLUTION

2.1.1 Overview

Dell EMC Isilon anti-virus solution enables scanning of the file system for viruses, trojans, malware and other security threats on an EMC Isilon cluster by integrating with third-party scanning services through the Internet Content Adaptation Protocol (ICAP). OneFS sends files via ICAP, to a server running third-party antivirus scanning software. These servers are referred to as ICAP servers. Files are scanned for threats on ICAP servers, not the cluster itself. Figure 1 below shows the typical file request flow when an ICAP-enabled cluster is configured to scan for these threats.

The end user requests a file from the cluster (step 1). The cluster, which is configured to be AV-aware, sends the requested file to the scan engine via ICAP (step 2) where the engine examines the file and determines if it needs repair or quarantine. Antivirus Solutions with EMC Isilon Scale-out NAS 5 If the file is clean, or has been cleaned, it is then returned to the cluster (step 3), marked as “safe”, and then the cluster serves the file to the end user (step 4).



After an ICAP server scans a file, it informs OneFS if the file is a threat. If a threat is detected, OneFS creates an event, displaying near real-time summary information and includes the threat in an antivirus scan report. OneFS can be configured to allow the ICAP server to attempt to repair infected files, or it can also be configured to protect users against potentially dangerous files by truncating or quarantining infected files. Before OneFS sends a file to be scanned, it ensures that the scan is not redundant. If a file has not been modified, OneFS will not send the file to be scanned unless the virus database on the ICAP server has been updated since the last scan.

There are several key functionalities available for Isilon antivirus solution:

2.1.2 Capability

2.1.2.1 On-access scanning

OneFS can be configured to send files to be scanned before they are opened, after they are closed, or both. Sending files to be scanned after they are closed is faster but less secure. Sending files to be scanned before they are opened is slower, but more secure.

2.1.2.2 Antivirus policy scanning

Antivirus scanning policies can be created that send files contained in a specific directory to be scanned. Antivirus policies can be run manually at any time or configured to run according to a schedule. They are handled by the OneFS job engine and behave the same as any system job.

2.1.2.3 Individual file scanning

Specific files can be sent to an ICAP server to be scanned at any time.

2.1.2.4 Antivirus scan reports

OneFS generates a report about antivirus scans. Each time that a policy is run, OneFS generates a report for that policy. Every 24 hours, OneFS generates a report that includes all on-access scans that occurred during that day.

2.1.2.5 Antivirus threat responses

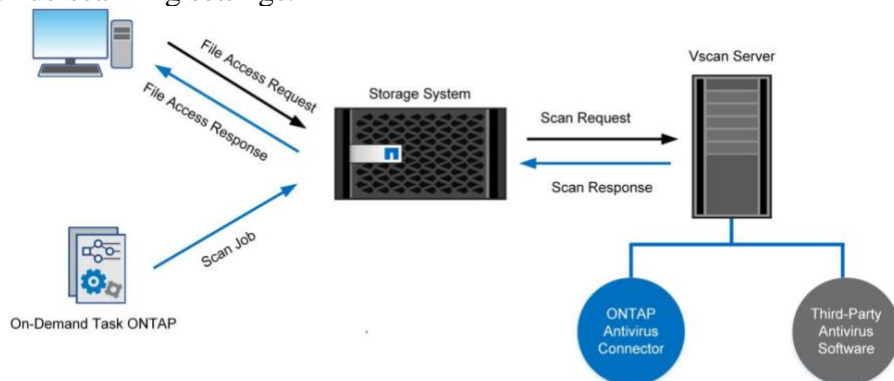
If an ICAP server detects a threat, the system can be configured to repair, quarantine, or truncate the infected files to eliminate the problem.

2.2 NETAPP SOLUTION

2.2.1 Overview

Netapp uses Netapp virus scanning, or Vscan, to protect data from being compromised by virus or other malware.

The antivirus solution consists of the following components: the third-party antivirus software, clustered Data ONTAP Antivirus Connector, and the clustered Data ONTAP virus-scanning settings.



Storage systems offload scanning operations to external servers (Vscan Server) hosting third-party antivirus software. Both the antivirus software and Antivirus Connector must be installed on the Vscan server. The antivirus software is installed and configured on the Vscan server to scan files for viruses or other malicious data. Antivirus Connector is

installed on the Vscan server to process scan requests and provide communication between the antivirus software and the storage virtual machines (SVMs; formerly called Vservers) in the storage system running clustered Data ONTAP.

Components of the storage system include:

- **Scanning Pool:** A scanner pool is used to validate and manage the connection between the Vscan servers and the SVMs. You can create a scanner pool for an SVM to define the list of Vscan servers and privileged users that can access and connect to that SVM and to specify a timeout period for scan requests.
- **Scanner Policy:** A scanner policy defines when the scanner pool is active. A Vscan server is allowed to connect to an SVM only if its IP address and privileged user are part of the active scanner pool list for that SVM.
- **On-Access Policy:** An on-access policy defines the scope for scanning files when they are accessed by a client. You can specify the maximum file size for files to be considered for virus scanning and file extensions and file paths to be excluded from scanning. You can also choose from the available set of filters to define the scope of scanning.
- **On-Demand Task:** The on-demand scan, introduced in ONTAP 9, runs the AV scanning job on files/folders in a specific path through a scheduled job whenever required.
- **Vscan File-Operations Profile:** The Vscan file-operations profile parameter (-vscan-fileop-profile) defines which file operations on the CIFS share can trigger virus scanning. You must configure this parameter when you create or modify a CIFS share.

2.2.2 Capability

The off-box antivirus feature provides two modes of scanning:

- **On-access scanning.** Triggers in-band notifications to the external virus-scanning servers during various file operations, such as open, close, rename, and write operations. Due to the in-band nature of these notifications, the client's file operation is suspended until the file scan status is reported back by the virus-scanning server, a Windows Server instance that is referred to as Vscan server.
- **On-demand scanning.** Introduced in ONTAP 9, this feature enables AV scanning whenever required on files/folders in a specific path through a scheduled job. It leverages the existing AV servers configured for on-access AV scanning to run the scanning job. The on-demand job updates the "scan status" of the files and reduces an additional scan on the same files when accessed next unless the files are modified. It can be used to scan volumes that cannot be configured for on-access scanning, such as NFS exports.

The Vscan server, upon receiving a notification for a scan, retrieves the file through a privileged CIFS share and scans the file contents. If the antivirus software encounters an infected file, it attempts to perform remedial operations on the file. The remedial operations are determined by the settings that are configured in the antivirus software. After completing all necessary operations, the Vscan server reports the scan status to clustered Data ONTAP. Depending on the scan status, clustered Data ONTAP allows or denies the file operation requested by the client.

Currently, Netapp antivirus solution supports McAfee, Symantec, Sophos and Trend Micro.

2.2.3 Limitations

On-access scan for clustered Data ONTAP is currently available only for the CIFS-related traffic.

The user can create a maximum of 10 on-access policies per SVM (only one active). The user can exclude a maximum of 100 paths and file extensions from virus scanning in one on-access policy.

2.3 HP SOLUTION

2.3.1 Overview

HP 3PAR NAS storage system use Sophos anti-virus scan engine for its protection, it has following components:

Sophos virus scan engine (VSE)

The Sophos virus scan engine executes the file scanning and virus and threat detection functions. Scans are relayed to the scan server through SAV-DI via ICAP providing real-time protection. Multiple scan servers can be configured to increase scan performance and reliability.

Sophos Antivirus Dynamic Interface (SAV-DI)

The Sophos Antivirus Dynamic Interface enables communication between HPE 3PAR File Persona and the Sophos antivirus scan server via the ICAP standard. SAV-DI relays the scan requests to the Sophos antivirus scan server installed on the same server. SAV-DI is a general-purpose interface to the Sophos antivirus scan server providing a single copy of the malware database for efficiently increased protection.

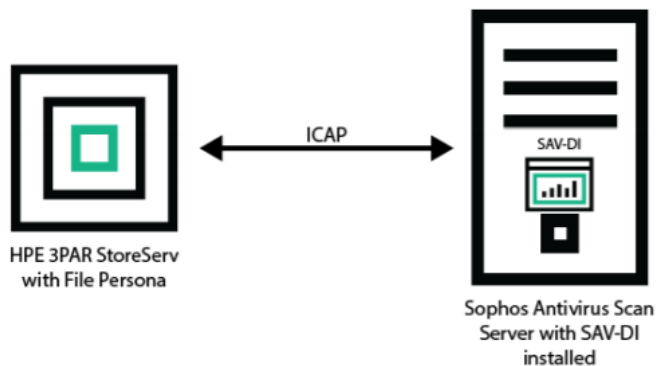


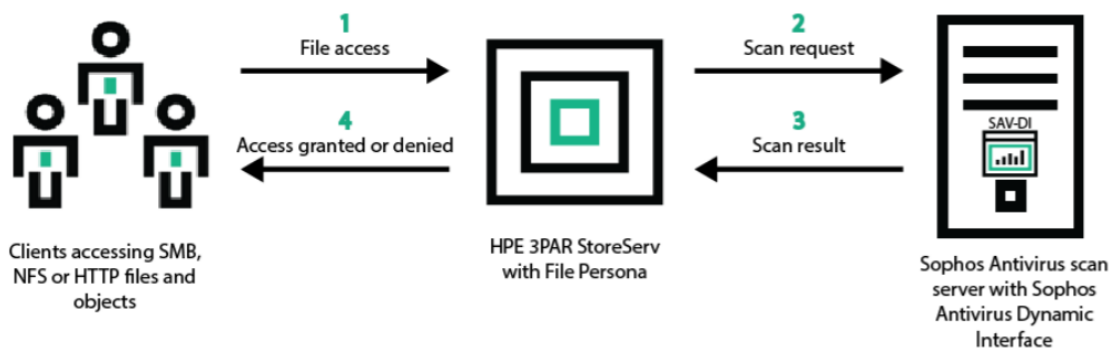
Figure 1. Sophos antivirus software with SAV-DI architecture

2.3.2 Capability

Figure below illustrates the following flow of information between HPE 3PAR File Persona and Sophos antivirus software for NAS devices:

1. The client requests an open (read) or close (write) of an SMB file, or read of an NFS or HTTP file.

2. HPE 3PAR File Persona determines if the file needs to be scanned based on the policies that have been set and notifies the Sophos antivirus servers. The file is then sent to the Sophos Antivirus Dynamic Interface (SAV-DI) via ICAP. Then requests are relayed to the Sophos antivirus scanner that's installed on the same server.
3. Sophos antivirus software scans the file and reports the scan results back to HPE 3PAR StoreServ system.
4. If no virus is found, access will be allowed to the file. If a virus is found, then there will be an "Access Denied" to an SMB client, a "Permission Denied" to an NFS client, or "transfer closed" to an Object Access API client. HPE 3PAR File Persona then quarantines the file and logs the scan messages.



SAV-DI has a single logger for logging events and messages. The log can be sent to the console, a file or on Linux/Unix, the syslog. You can also specify the level of logging.

2.3.3 Limitations

You can tune parameters in the SAV-DI configuration file to achieve optimal performance. If the parameters are not tuned (threadcount, maxqueuedsessions and Allow204), the scan server can be reported as DOWN in the HPE 3PAR StoreServ Management Console (SSMC).

The following parameters need to be changed:

- Channel: ICAP
- Port: 1344
- Service: AVSCAN
- Allow204: Yes
- Keepalive: Yes
- Threadcount: 32
- Maxqueuedsessions: 1200 (value between 1024 ~ 1280)

2.4 OTHER VENDORS AND TRENDS

Many software vendors have antivirus products running on file storage. For example, McAfee, Sophos, and Kaspersky provide antivirus protection and on-demand scanning for several storage vendors. These antivirus service vendors commonly install their

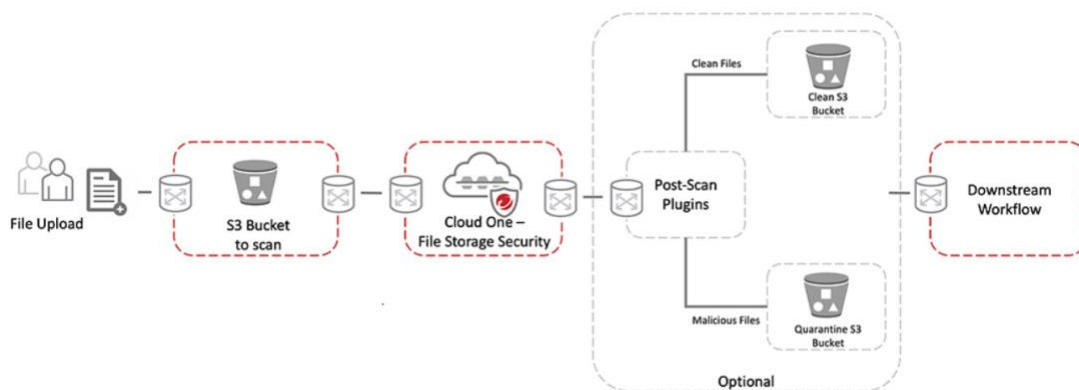
products on independent servers and be integrated with agents provided by storage vendors. The integration can be based on ICAP or storage vendors' proprietary protocols, but ICAP is the most popular one. In other words, if a customer's storage system is adopting ICAP, there will be several antivirus solutions available by different vendors. For a customer who owns NAS product from different vendors, the customer can choose a single antivirus vendor for different storage systems. For example, McAfee lists all the supported storage products on its web site [6].

Not all storage vendors choose to integrate their file sharing platforms with antivirus software using the ICAP protocol. Any CIFS server can be scanned by these antivirus products. But this setting will not be able to provide the on-access (aka real-time) virus scan feature. Some platforms may deem it as a lower-priority feature than others. For example, we are not able to find a confirmation that Pure FlashBlade is using ICAP to integrate with any anti-virus vendors. Instead, snapshots can be used to protect against ransomwares. Snapshots will help protect customers' data including virus protection, but it's in a different dimension. The virus scan is still valuable to users.

Most other vendors support ICAP based antivirus integration. The vendor list includes Hitachi, IBM, Nutanix, and many others. Therefore, several antivirus vendors can be used for their products. Apparently, each antivirus software has its pros and cons, such as virus scanning effectiveness, performance, etc. But the evaluation of that perspective is outside of this market report.

Cloud vendors are also facing the same challenges. Azure, GCP, and AWS all provide several anti-virus options, many of them from third party products on the marketplace. They can be used to scan files uploaded into user's object storage. Many of the cloud-based products can also be used across multiple cloud platforms.

Here is an example of antivirus solution for cloud file/object services from Trend Micro. Open source software such as Lambda and ClamAV also exists for scanning S3 buckets. The evaluation of cloud-based vendors is also outside of this report.



2.5 COMPARISON CHART

To compare different products on the market, we compiled a table to show the differences among them. Note that we are not comparing among different antivirus vendors, rather we are comparing the integration between storage products with these antivirus vendors.

	Scanner protocol	Third party software	Scan Policy	Scan granularity	Scan Filters	Security	Single-pane management
Dell EMC Isilon	ICAP	Symantec, Trend Micro, Kaspersky Anti-Virus, McAfee	On Access, On Schedule, Manually	File, directory	Based on file size and location and extension name.		Trigger and check Virus DB update from Isilon GUI
Netapp Clustered Data Ontap	Netapp scanner	McAfee, Symantec, Sophos and Trend Micro	On Access, On demand	File, directory	*Scan filter based on file type, extension. *Scan only when the files are modified. *Exclude filter by file type, pattern and file age. *Exclude files based on file size and location (path), or to scan only files opened with execute permissions	the connection request is compared to the privileged users and IP addresses	Upgrade antivirus software from Netapp GUI
HPE Sophos	ICAP	NA	On Access, On Schedule, Manually	File, directory	NA	NA	Integrated into HPE 3PAR File Persona Integrated with HPE 3PAR File Persona
Pure FlashBlade	No (or unknown)	NA	NA	NA	NA	NA	NA
IBM StoreWize V7000 unified system, IBM Sonas	ICAP	McAfee, Kaspersky, Symantec, and Trend Micro	On access, On demand	File, directory (subtree)	Enable or disable scanning for a specified scope. If the include list is empty or not specified, the default is that all extensions are included in scans. In this case, the exclude list can be used to create exceptions.	NA	Log on to the GUI and select Files > Services > Antivirus
Hitachi VSP-G unified storage, HNAS	ICAP/Netapp scanner	McAfee, Trend Micro, Sophos, Kaspersky	On access, On demand	File, directory	Inclusion list and exclusion list are used. Also one can set the max file size to scan	NA	Log on to the GUI and Home > Data Protection > Virus Scanning

Other than Pure, other storage vendors are using the same set of antivirus software vendors and provide a similar set of virus protection functionalities. The easy-to-use, integrated single-pane management, and extra security besides CIFS will separate the products apart.

The configuration of servers hosting antivirus software is decided by different antivirus vendors. It is commonly decided by CPU limits, antivirus software limits, and network limits. Multiple servers can be used to speed up and load balance the scanning process. Antivirus software vendors recommend adding more servers when scanning performance

is showing signs of performance degradation. The actual scanning load is determined by the total number of files, file size, and requirements of finishing time.

The antivirus software for storage has system requirements. The following is a list of requirements for McAfee VirusScan Enterprise for Storage 1.1.0:

Component	Requirement
Hardware	An Intel dual-core processor or compatible architecture
CPU speed	2.6GHz (or greater)
Memory	Minimum 4GB RAM
Disk space	Minimum 70MB to install the software Additional 5GB for ICAP scanner files and temporary files
Operating system	<ul style="list-style-type: none">• Windows Server 2008 32-bit and 64-bit• Windows Server 2008 R2• Windows Server 2012

3 ANTIVIRUS IN HUAWEI STORAGE

3.1 OCEANSTOR9000 SOLUTION

3.1.1 Overview

InfoScanner is an antivirus feature. OceanStor 9000 provides Huawei Antivirus Agent and interconnects with third-party antivirus software installed on external antivirus servers, thereby protecting shared directories from virus attacks. The third-party antivirus software accesses shared directories using the CIFS protocol and scans files in the directories for viruses (in real time or periodically). If viruses are detected, the third-party antivirus software kills the viruses based on the configured antivirus policy, providing continuous protection for data in OceanStor 9000.

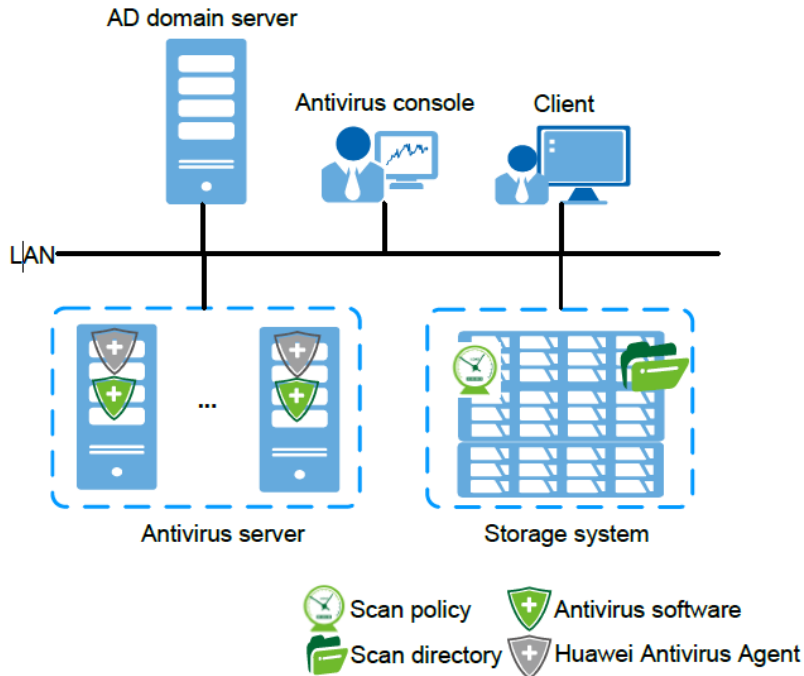
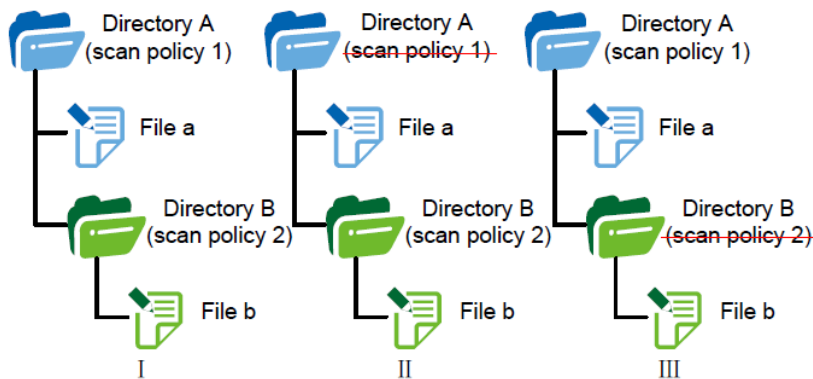


Figure 1. InfoScanner network structure

Scan Policy Configuration Guidance

OceanStor 9000 allows a scan directory and its sub-directories to be of different scan types (real-time and periodical). OceanStor 9000 allows different scan policies for a scan directory and its sub-directories (scan policies can set different Non-scan period, excluded file types in scan, max file size for scan), as shown in [Figure 2](#).

Figure 2 Scan policy configuration example



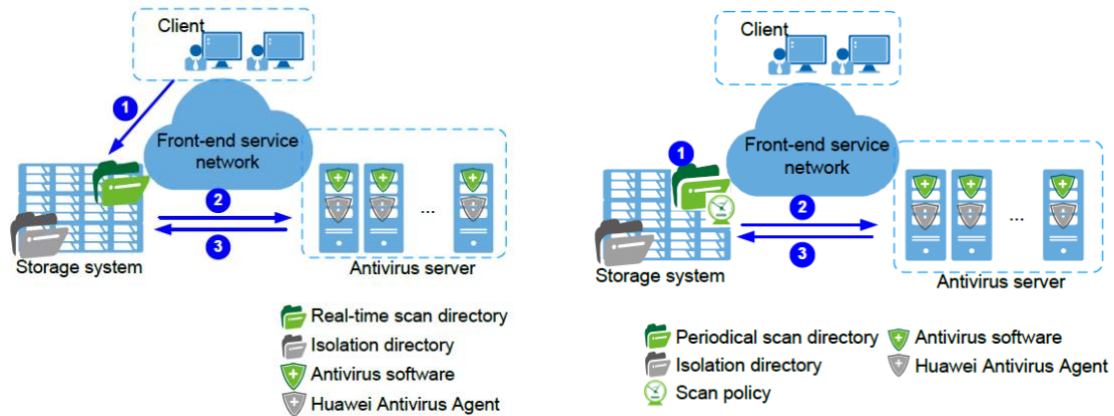
Directory A is the parent directory of directory B. Scan policy 1 is configured for directory A, whereas scan policy 2 is configured for directory B.

3.1.2 Capacity

InfoScanner offers both real-time scan and periodic scan, the processes are shown below:

Figure 3 Real-time scan process

Figure 4 Periodic scan process



3.1.3 Scalability

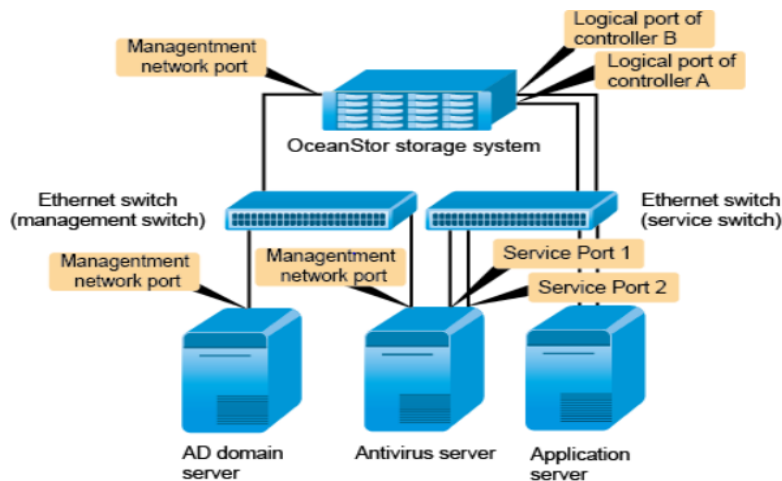
Parameter Value	Value
The maximum number of directories that can be scanned in real time	128
The maximum number of directories that can be scanned periodically	256
The maximum number of scan policies that can be configured	32
The maximum number of antivirus servers that can be configured per cluster	32

3.2 OCEANSTOR V5 SOLUTION

3.2.1 Overview

When the storage system runs a file system and shares the file system with clients through CIFS, third-party antivirus software can be used to trigger virus scanning and delete virus-infected files, improving storage system security.

The process for configuring the antivirus service includes adding the antivirus server and storage system to an AD domain, configuring the antivirus server (including the antivirus agent and antivirus software), and configuring the antivirus service on the storage system.



The file antivirus feature of the storage system supports two virus scanning modes: shareopen and ICAP protocol. The table below shows the scanning procedure and supported third-party software under each scanning mode.

Scanning Mode	Procedure	Applicable Third-Party Antivirus Software
shareopen	<ol style="list-style-type: none"> 1. The storage system sends a virus scanning request. 2. The antivirus agent opens the file after receiving the request. 3. The antivirus Engine intercepts the file and triggers virus scanning. 	<ul style="list-style-type: none"> • Symantec Endpoint Protection • Trend Micro ServerProtect • McAfee VirusScan Enterprise • Sophos Endpoint Protection • (Applicable to V500R007C20 and later versions) Kaspersky Endpoint Security 10 for Windows
ICAP protocol	<ol style="list-style-type: none"> 1. The storage system sends a virus scanning request. 2. The antivirus agent sends the file to be scanned to the antivirus engine using the FILEMOD of ICAP protocol. 3. The antivirus engine triggers antivirus scanning. 	Symantec Protection Engine

3.2.2 Capability

The antivirus service can be configured on storage systems with non-vStore scenarios and vStore scenarios.

By default, the storage system will configure a scan policy named default. A user can create or modify scan policies with followings parameters:

Parameter	Description	Value
Name	Name of a scan policy.	[Value range] <ul style="list-style-type: none"> • Contains 1 to 127 characters. • Contains only letters, digits, underscores (_), periods (.), and hyphens (-). • Must be unique. [Example] AVScanPolicy
Non-scan Period:	Period when no scan is performed.	[Example] 00:00-01:00
Excluded File Types in Scan	Types of files that do not require virus scan.	[Example] .txt
Max. File Size for Scan	Maximum size of a file that must be scanned. NOTE If the value is set to Not restricted , files of any size are scanned.	[Example] 40 MB

Antivirus service also supports real-time scan policies. When a CIFS shared file is closed, the antivirus server will scan the file immediately based on the configured scan policy. A file system can use only one real-time scan policy.

For security purposes, you are advised to periodically reset the pre-shared key. Using the pre-shared key, you set and the system's secure key generation algorithm, the system generates a new authentication certificate. This certificate is used to authenticate the session between the storage system and antivirus (AV) agent.

3.2.3 Limitations

The storage system and antivirus servers should be in the same AD domain.

For the 5000, 5000F, 6000 and 6000F series storage systems, an antivirus server supports a maximum of eight logical ports. For the 18000 and 18000F series storage systems, an antivirus server supports a maximum of sixteen logical ports.

4 ANTIVIRUS REQUIREMENTS

4.1 KEY REQUIREMENTS

After carefully analyzing features from various major storage vendors, we come into conclusion some key requirements which bring more values to customers for anti-virus feature in storage system.

1. ICAP integration support

Most of vendors opt to support standard ICAP servers with 3rd party anti-virus software integration. It ensures maximum flexibility and compatibility for customers and storage vendor. The following requirements are considered differentiating factors:

- a. Support ICAP protocol (ICAP client)
- b. multiple ICAP server support, load balancing etc.
 - i. Sizing based on current user storage configuration
 - ii. Load balancing across ICAP servers
 - iii. Different scan policy ICAP server configuration (At least one server for each controller for on-access scan, minimum of 2 for policy scan)

2. Flexible policy engine

- a. Support on-access, on-schedule, and on-demand
- b. Support a variety of scan filters

3. Easy to use

- a. Simplified steps to configure the solution (e.g., scan with a few clicks)
- b. Integrated console for feature management

4. Broad 3-party antivirus vendor support and certification

Symantec, Trend Micro, Kaspersky Anti-Virus, McAfee, etc.

4.2 GAPS

Given that Dorado NAS product is still under development, we are not able to assess anti-virus feature for Dorado. Based on 9000 and V5 features, we are only going to propose what we believe the most important requirements for competitive anti-virus feature.

Scan Policies: on-demand policy. The on-demand job updates the “scan status” of the files and reduces an additional scan on the same files when accessed next unless the files are modified. It can be used to scan volumes that cannot be configured for on-access scanning, such as NFS exports.

Granular scan exclusion: the ability to exclude files from virus scanning based on file size and location (path) or to scan only the files that are opened with execute permissions. OceanStor 9000 allows excluded file types in scan, max file size for scan)

Security: ONTAP validates incoming connection requests sent by the Vscan server. Before the server is allowed to connect, the connection request is compared to the privileged users and IP addresses defined in the scanner pools to verify that it is originating from a valid Vscan server.

Management Integration: Single pane management from the storage side to query/control Anti-virus software states, including virus definition etc.

Sizing: Provide various configurations for ICAP servers based on various requirements for virus scan (on access scan latency, time of full scan, size of storage, workload of storage system etc.). The following metrics shall be included in order to get a correct sizing model.

1. Single file scan time
2. Single file size
3. System capacity
4. System scan time
5. Number of ICAP servers
6. Number of threads per ICAP servers per Anti-virus software
7. Scan types
8. ICAP server bandwidth
9. Storage server scan capability (CPU, memory and other resources dedicated to scan agent)

It is recommended to have at least one server for each controller for on-access scan, minimum of 2 for policy scan.

4.3 STRATEGY FOR EXISTING SOLUTIONS

A storage system anti-virus feature, generally speaking, offers better integration with following benefits:

1. On access virus detection, quarantine and removal. It eliminates or reduces window of infection. It is one of the major driving forces for a storage integrated anti-virus feature.
2. Lower bandwidth consumption. Storage scanner usually has configuration and capability to hand pick certain files based on directory, extension, file size, modified time etc. It only sends file request to scan engine deemed necessary. It

also can choose to send digest or partial data to scan engine to identify possibility of scan. Therefore, it reduces certain unnecessary operations by scan engine.

3. Workload balancing. Storage system generally is configured to support multiple ICAP servers to share workload among them. It also can share them with better decisions based on storage characteristics. For example, storage system knows current workload, capacity of its NAS storage, it may choose to share them with file or folder granularity or schedule it later time if storage system is serving heavy customer workload. It maximizes ICAP server capability and minimize user impacts.

For storage systems that have not implemented the on-access virus scanning feature, customers can still integrate with Antivirus software to have virus protection using a standalone antivirus solution to be integrate antivirus features into customer data center (without storage system involvements or just simple CIFS configuration). Standalone antivirus solutions as mentioned in section 2.4, also can be configured in such way what storage filters can do (like scan only certain types of files). Those features have become ubiquitous for anti-virus software solution. A selective scan does not significantly add overall system bandwidth.

Standalone antivirus solution can also be configured as a cluster with each server serving portion of data store.

Finally, standalone antivirus solution can also configure certain sensitive folder or file types with increasing frequency scanning. It further eliminates the need for a storage side anti-virus feature.

Standalone antivirus solution can also support ICAP therefore, a storage side anti-virus solution when storage system feature is available to protects customer investment.

4.4 A DIFFERENT PERSPECTIVE FOR DATA CENTER ANTIVIRUS STRATEGY

Let's take a look at another perspective for data center antivirus strategy – Leveraging storage system continuous data protection or backup solution against common scenarios such as disasters, data corruption, or accidental deletions. Below list all the key requirements for a CDP based antivirus solution:

1. Secure Data Protection: A CDP or snapshots with protection features shall be a good starting point for antivirus or ransomware protection. Virus or ransomware can't eradicate, modify, or encrypt snapshots, even with admin credentials. In an unpredictable world, you're covered 24x7x365.
2. Ease of use: Snapshot scheduling and retention are fully customizable. Easy to deploy. Expand and upgrade without disruption. And there's no need to change your backup software. Simply set it and forget it.
3. Faster Recovery: Data recovery solutions shall be fast with lower RPO and RTO similar goals as DR. Most backup systems are not architected for restoring a large percent of a customer environment within a short timeframe. Some customers impacted by virus and ransomware may take months to recover.

In summary, a good CDP based backup recovery solution with standalone or storage integrated antivirus solution is another perspective that security expert and administrator shall not overlook.

4.5 TRENDS FOR ANTIVIRUS SOLUTIONS

First, rather than using only a traditional file-based antivirus approach, we may need other techniques such as:

- behavior-based
- reputation-based
- network-based protection techniques

Those techniques may come with the third-party software, or we may need to develop them on our own or adapt to new solutions.

Second, because of specific requirements like PCI DSS and HIPAA, many of the large vendors are starting to address risk management and compliance, in addition to just antivirus software.

Third, continued rise of AI and machine learning has big impact on antivirus industry. Antivirus solutions may need changes to reflect the impact.

Fourth, global spending for cloud computing antivirus programs has reached 1 billion. The market for automotive antivirus is projected to reach \$713 million by 2020. **This means new antivirus solutions for new storage market are needed.**

5 REFERENCES

1. [Dell EMC PowerScale: Antivirus Solutions \(delltechnologies.com\)](https://www.delltechnologies.com)
2. [Antivirus Protection for NetApp Clustered Data ONTAP | NetApp Blog](#)
3. [Antivirus Solution Guide for Clustered Data ONTAP - McAfee | TR-4286 | NetApp](#)
4. [Antivirus Solution Guide for Clustered Data ONTAP - Symantec | TR-4304 | NetApp](#)
5. [HPE Sophos Antivirus for 3PAR File Persona and Sophos antivirus software for NAS devices](#)
6. [Supported platforms for VirusScan Enterprise for Storage \(mcafee.com\)](#)
7. [Managing Antivirus Settings \(Non-vStore Scenarios\) - OceanStor V5 Series V500R007 Security Configuration Guide - Huawei](#)
8. [Cloud One File Storage Security \(trendmicro.com\)](#)