VERITAS

NetBackup Flex Appliance Security

Protect and easily recover backup data with a unified, multi-layered platform.

Veritas NetBackup™ Flex Appliances provide a zero-trust multilayer security solution to defend an organization’s backup data and recover in software and hardware. This white paper highlights hardware security, secure Veritas VxOS operating system, container service isolation, secure storage services and data security in the Flex Appliance with NetBackup solution.

White Paper | January 2023

Contents

Contents

Introduction

Executive Summary

In the wake of several successful and high-profile cyberattacks against banks, technology, retail, and governments, organizations want to ensure they are not the next victim reporting a devastating breach that resulted in data loss or corruption. Data protection solutions are designed to protect data from cyberattacks, but it's now common for attacks to enter an organization's primary environment and target its backups—where the majority of enterprise data is stored. Ensuring your backup data isn't compromised in a way that you won't be able to recover from a ransomware attack is a top concern for companies. SonicWall recorded a record number of ransomware attacks in 2021. In fact, they recorded a high of 78.4 million ransomware attacks in the month of June 2021 alone—over 30 attacks per second1. Ransomware volume showed massive year-to-date spikes of 185 percent in the U.S. and 144 percent in the UK

A Zero Trust security architecture is never trust and always verify. Using a Zero Trust architecture, NetBackup Flex Appliances provide a unified, multi-layered platform approach to seamlessly integrate intelligent protection, comprehensive detection, and industry-leading backup and recovery. Flex Appliances offer hardware security, secure Veritas VxOS operating system, container service isolation, secure storage services and data security. They feature (WORM) storage, STIG-compliant operating system (OS) hardening, FIPS140-2–compliant data encryption, and comprehensive security access controls. Flex Appliances provide a complete immutable and indelible storage solution to defend an organization's backup data and enable recovery in software and hardware.

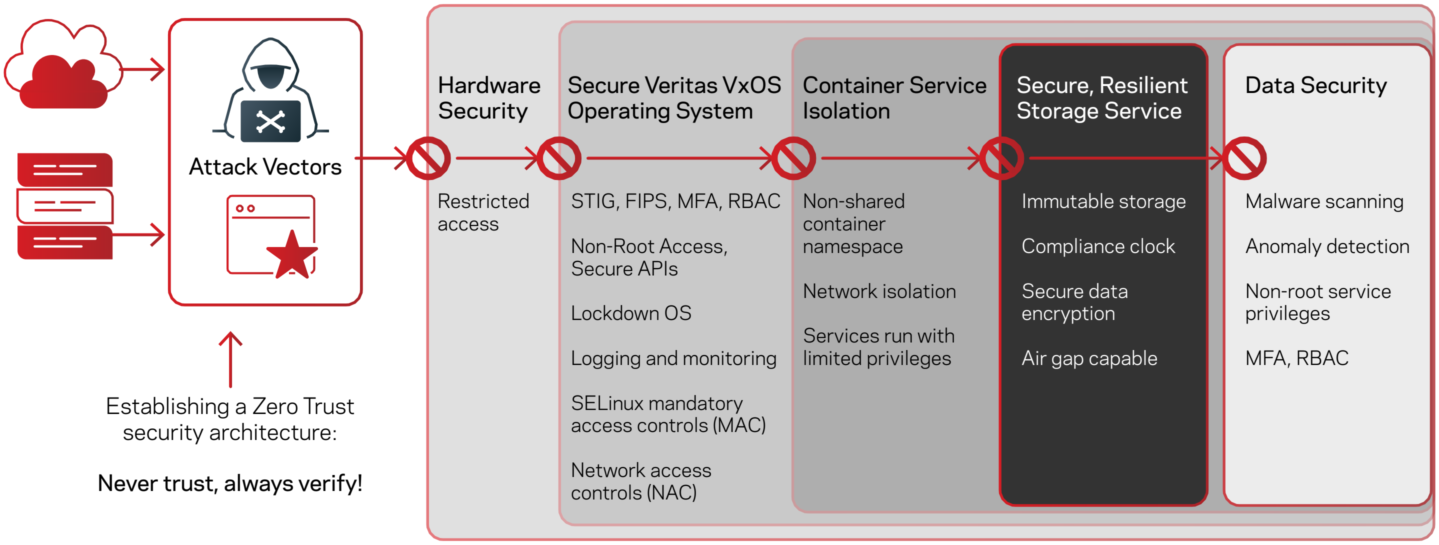

Attack Vectors
Establishing a Zero Trust security architecture:
Never trust, always verify!
Hardware Security
Restricted access
Secure Veritas VxOS Operating System
STIG, FIPS, MFA, RBAC
Non-Root Access, Secure APIs
Lockdown OS
Logging and monitoring
SELinux mandatory access controls (MAC)
Network access controls (NAC)
Container Service Isolation
Non-shared container namespace
Network isolation
Services run with limited privileges
Secure, Resilient Storage Service
Immutable storage
Compliance clock
Secure data encryption
Air gap capable
Data Security
Malware scanning
Anomaly detection
Non-root service privileges
MFA, RBAC

Figure 1. An overview of the NetBackup Flex Appliance's Zero Trust architecture.

Veritas data protection appliances include native ransomware recovery for business-critical data—at any scale—with near-zero RPO and RTO. Some key benefits include:

- Simplified IT management with immutable storage
- A secure-by-default architecture
- Integrated highly available system configurations

Scope

The purpose of this document is to provide technical details on the Flex Appliances' Zero Trust architecture and their use of OS and firmware hardening, container separation, write once, read many (WORM) storage and logging, and access controls.

Here are additional resources for Flex Appliances:

- For Air Gap Solution: SO_flex_appliance_netbackup_ire_solution_V1543.pdf

- For best practices and sizing recommendations: WP_netbackup_flex_appliance_best_practices_V1452.pdf
- For integration and API guide: NetBackup Flex API Guide
- For installation, configuration, and administration of each of the products discussed in this white paper: see the appropriate Veritas product documentation

Physical Firmware Hardening

Firmware is highly vulnerable and increasingly attractive for hackers as a place to embed malware and hide other malicious code that can ultimately compromise a system. To stop attackers, gain high privilege on firmware and device drivers, Flex Appliance eliminate implement the follow security settings:

- Boot
  - Eliminate "single user" mode / "rescue mode" boot options
  - GRUB menu editing disabled
- Storage
  - No storage reset (factory reset/reimage allowed)
  - Locked-down storage array Access

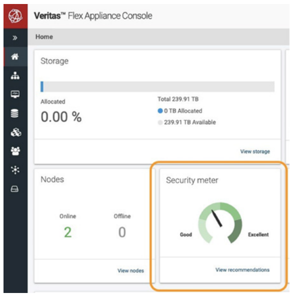
Firmware Updates

Veritas regularly provides firmware updates (SURE tool) and advisories to gain protection from firmware vulnerability.

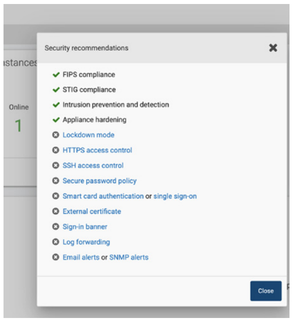
Secure Veritas VxOS Operating System

To help you fully utilize flex appliance zero-trust architecture, security meter enables you with ONE GLANCE To View, and with ONE CLICK To Configure for the security settings. Security meter can keep tracking security settings and show you a list of available security features with Quick links to configure them. The security meter can be found at Flex Appliance landing page, only the admin user can view this feature.

Security Insights

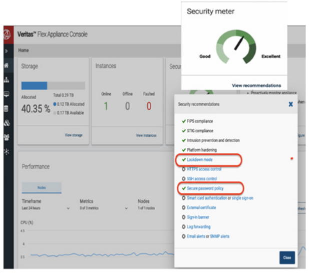


Security Recommendations


Security recommendations ✖

- ✓ FIPS compliance
- ✓ STIG compliance
- ✓ Intrusion prevention and detection
- ✓ Appliance hardening
- ⊗ Lockdown mode
- ⊗ HTTPS access control
- ⊗ SSH access control
- ⊗ Secure password policy
- ⊗ Smart card authentication or single sign-on
- ⊗ External certificate
- ⊗ Sign-in banner
- ⊗ Log forwarding
- ⊗ Email alerts or SNMP alerts

Improved Security Score



Security recommendations ✖

- ✓ FIPS compliance
- ✓ STIG compliance
- ✓ Intrusion prevention and detection
- ✓ Platform hardening
- ✓ Lockdown mode
- ⊗ HTTPS access control
- ⊗ SSH access control
- ✓ Secure password policy
- ⊗ Smart card authentication or single sign-on
- ⊗ External certificate
- ⊗ Sign-in banner
- ⊗ Log forwarding
- ⊗ Email alerts or SNMP alerts

Security Technical Implementation Guide (STIG)

Because new exploits appear on a regular basis, cybersecurity continues to be a focal point for government agencies. The Defense Information Systems Agency (DISA) has published a Secure Technical Implementation Guide (STIG) to ensure exposure to unauthorized access and resulting data loss or theft is minimized.

An intrusion detection system (IDS) protects a system from attacks, misuse, and compromise by analyzing system and network activity for unauthorized entries and/or malicious activities. An IDS can monitor and audit network activities and system configurations for vulnerabilities and analyze data integrity.

An intrusion protection system (IPS) reinforces a firewall and provides an analysis layer to select for dangerous content. An IPS actively analyzes the network and undergoes automated actions on all traffic flows that enter the network. When an IPS detects an intrusion, it blocks the traffic and prevents it from getting to its target. These actions may include dropping malicious packets, blocking traffic to a source address, or resetting a connection.

STIG is a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security. Flex Appliances meet STIG compliance at the OS (software and firmware) and appliance management by using the STIG template to meet security requirements per the DISA profile.

The STIG for Red Hat SELinux consists of more than 300 security controls over configuration settings. Flex Appliances are fully STIG compliant and have been tested at CAT I, II, and III.

Examples for CAT I:

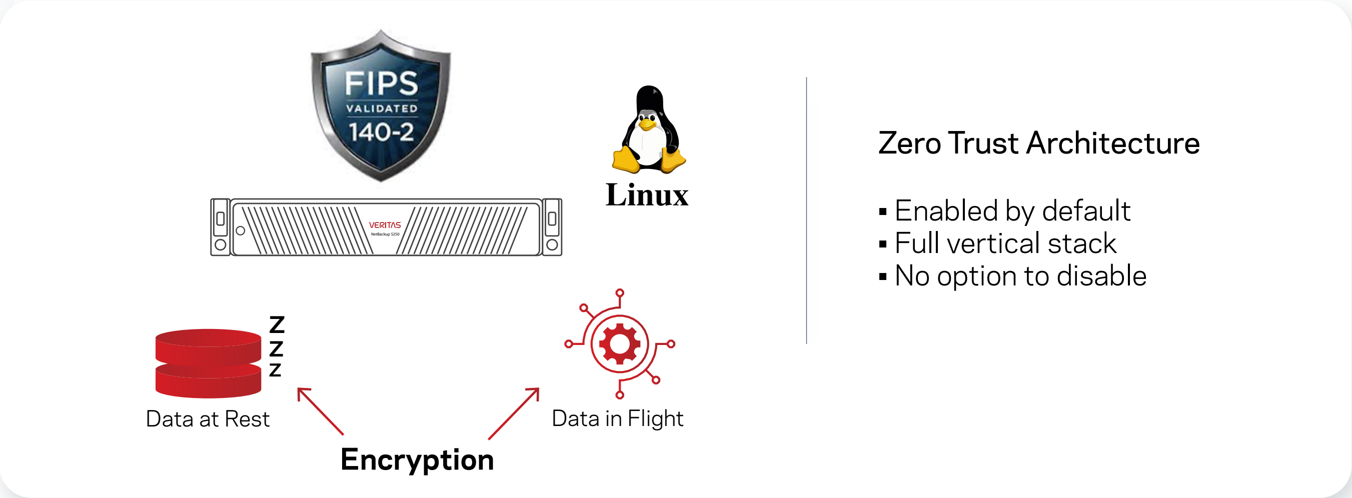
- Do not have accounts configured with blank or null passwords
- X86 Ctrl-Alt-Delete key sequence is disabled on the command line
- Red Hat RHEL version 7.2 or newer with a basic I/O system (BIOS) must require authentication on booting into single-user and maintenance modes
- Ensure gpgcheck is enabled for local packages
- Implement NIST FIPS-validated cryptography

CAT II and III:

- Ensure gpgcheck is enabled for local packages
- Ensure /home is located on a separate partition with nosuid mount option
- Add noexec option to /dev/shm, use FIPS-validated MACs and Ciphers inssh confi
- Set account expiration based on inactivity
- STIG: The Red Hat Enterprise Linux operating system must not have unnecessary accounts
- STIG: The Red Hat Enterprise Linux operating system must not allow a non-certificate trusted host SSH logon to the system
- STIG: The Red Hat Enterprise Linux operating system must use a separate file system for /var
- STIG Disable KDump Kernel Crash Analyzer (kdump)

Data Encryption

NetBackup Flex Appliances meet Federal Information Processing Standards (FIPS) 140-2 standards to keep data encrypted in transit and at rest. This certification ensures government organizations, financial, and healthcare institutions that data handled by third-party organizations is stored and encrypted securely and with the proper levels of confidentiality, integrity, and authenticity (see Figure 2).



Zero Trust Architecture

- Enabled by default
- Full vertical stack
- No option to disable

Figure 2: An overview of the FIPS 140-2 standard with which Flex Appliances comply.

FIPS is enabled on a Flex Appliance's host infrastructure instances. SSH and sshd settings are updated to support FIPS-compliant ciphers and MAC ciphers. FIPS is enabled during the Flex Appliance installation process.

User Authentication and Authorization

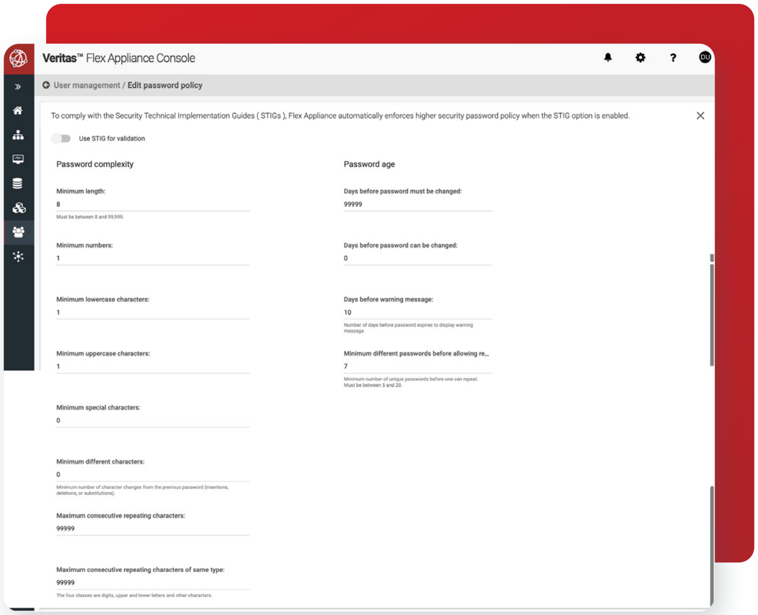
With password policy, LDAP integration, Smart Card, and SSO, Flex Appliance provides a secure and efficient enterprise identity management.

Flex Appliances Password Policy

You can use the NetBackup Flex Appliance Web GUI to edit the password policy for user passwords. To comply with the Security Technical Implementation Guides (STIGs), Flex Appliance automatically enforces higher security password policy when the STIG option is enable.

Password Policy Enhancement:

- Forced password changes during initial configuration to ensure the default password does not remain active on the system
- The ability to set your own password policy, including the option to use the Security Technical Implementation Guide (STIG) for validation
- After Three Failed Login Attempts, access to account would be gained after superadmin unlocks it and the local user changes the password
- Session timeouts that automatically sign users out of the NetBackup Flex Appliance Console and the NetBackup Flex Appliance Shell after 10 minutes of inactivity


Veritas™ Flex Appliance Console
DU
User management / Edit password policy

To comply with the Security Technical Implementation Guides (STIGs), Flex Appliance automatically enforces higher security password policy when the STIG option is enabled.

Use STIG for validation

Password complexity

Minimum length: 8
Must be between 8 and 99,999.

Minimum numbers: 1

Minimum lowercase characters: 1

Minimum uppercase characters: 1

Minimum special characters: 0

Minimum different characters: 0
Minimum number of character changes from the previous password (insertions, deletions, or substitutions).

Maximum consecutive repeating characters: 99999

Maximum consecutive repeating characters of same type: 99999
The four classes are digits, upper and lower letters and other characters.

Password age

Days before password must be changed: 99999

Days before password can be changed: 0

Days before warning message: 10
Number of days before password expires to display warning message.

Minimum different passwords before allowing re...: 7
Minimum number of unique passwords before one can repeat. Must be between 5 and 20.

CyberArk Integration for Password Management

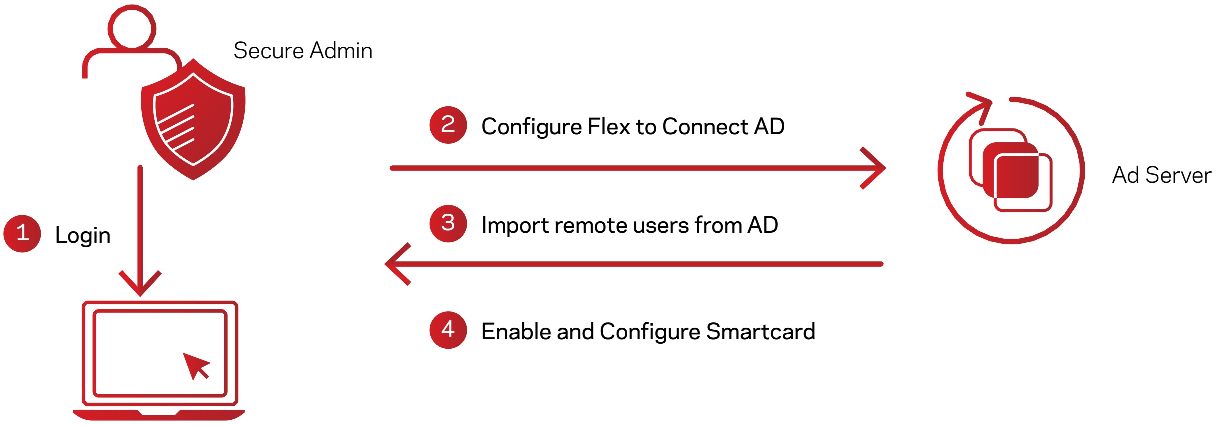
Veritas Flex Appliance supports External password management solutions. To keep unauthorized users out, detect and stop threats in real time , you can deploy CyberArk Privileged Access Manager (PAM) as-a-Service or host it in your Flex Appliance environment. You can download Veritas Flex Appliance API CPM Plugin.

LDAP User Login and Smart Card Authentication

Flex Appliance has the capability to import users from a remote AD server with Open LDAP protocol. You can seamlessly authenticate and authorize users with a global entry LDAP integration.

After you configure Flex to connect to a remote AD server and import remote users and groups, you can also enable a smart card to enable multi factor authentication. The smart cards allow user authentication with cryptographic keys, the keys are encrypted with a unique ID. The smart card feature enhances the security posture for public sectors and government.

NBU Flex Appliance


Secure Admin
1 Login
2 Configure Flex to Connect AD
3 Import remote users from AD
4 Enable and Configure Smartcard
Ad Server

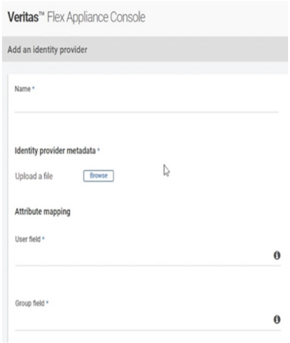
Single Sign On with SAML

With Flex Appliance Single Sign-On, you can log on Flex Appliance Web GUI after logging into the identity provider. SAML SSO provides a faster and seamless user experience. The user only needs to log in once. SAML SSO provides the following benefits:

- Secure systems and narrows attack surfaces
- Reduce costs by saving Improves user productivity and less helpdesk tickets
- Reduces the helpdesk password reset requests,
- Simpler user management and integration with B2B partners

The diagram below shows you how to configure SSO on Flex Appliance:

Add an Identity Provide



Veritas™ Flex Appliance Console

Add an identity provider

Name *

Identity provider metadata *

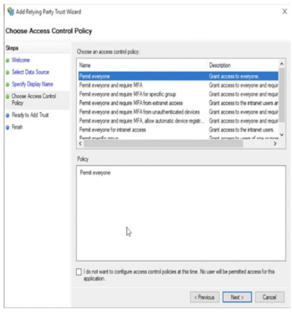
Upload a file

Attribute mapping

User field *

Group field *

Connect SP with IdP



Choose Access Control Policy

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Choose an access control policy:

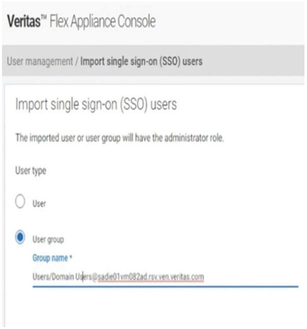
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

Policy

Permit everyone

□ I do not want to configure access control policies at this time. No user will be permitted access for this application.

Import Users or Groups



Veritas™ Flex Appliance Console

User management / Import single sign-on (SSO) users

Import single sign-on (SSO) users

The imported user or user group will have the administrator role.

User type

○ User

● User group

Group name *

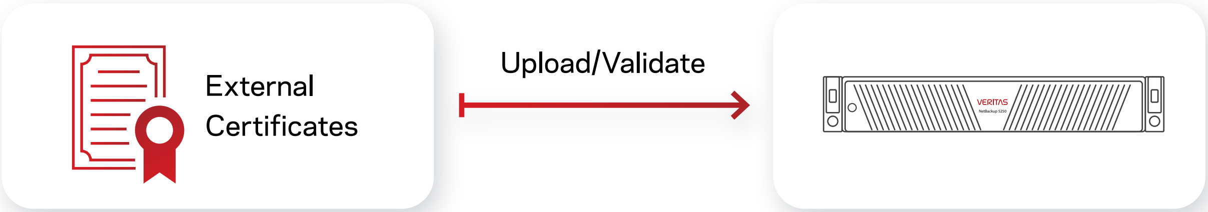
Users/Domain Users@sadie01vm082ad.rsv.ven.veritas.com

Customizable Login Banner

You can set a text banner that appears before a user sign into the NetBackup Flex Appliance web UI, Shell, and Console. The typical use cases for login banners are legal notices, warning messages, and company policy information. The security banner can provide legal protection if an unauthorized user violates any access restrictions, such as Terms of Use, and accesses the system anyway.

External Certificate Authorization

Flex Appliance provides the flexibility to use certificates from an external certificate authority (ECA). You can upload and validate the ECA using the Flex web UI. Without an EC, the Flex Appliance will use the default self- signed certificates.



To use an external certificate, you must have the following:

- **Host certificate**—An X.509 certificate for the appliance, in PEM format. This certificate is different from the certificate for your NetBackup primary and media servers.
- **Private key**—The RSA private key of the host certificate.
- **Passphrase**—The passphrase of the private key if the key is encrypted.

Non-Root Access

Follow Zero Trust Principal, Flex Appliance uses non-root user in CLI, API and platform. Non-root access prevents malicious code from gaining permissions to the systems and run undesired processes, change the UID especially in a multi-tenant domain. Access to the root filesystem is restricted even for admin account which prevents accidental or malicious damages root filesystem . Direct Access to data and filesystem is prohibited by restricting mount or unmount operations of devices and installation or uninstallation of packages are not allowed.

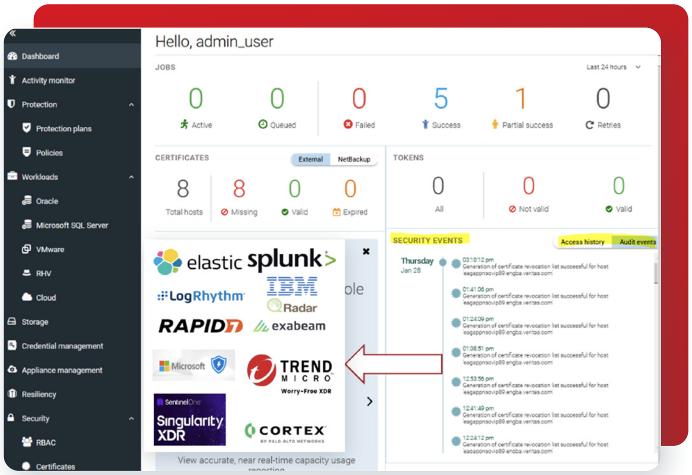
All the CLI commands, API executions are logged in a separate file and forwarded to syslog for security incident investigation.

Access tokens allow an application to access an API. After a user successfully authenticates and authorizes access, the application receives an access token and then passes the access token as a credential when it calls the target API. TLS is required and OAuth is enabled.

Track Threats and Monitor User Activities with Logging and Auditing

To detect and prevent threats, organizations need to promptly spot malicious insiders, compromised accounts, malware infections and other problem.

With Flex Appliances, you can view the events at WebUI or forward syslog and audit logs including elevated shell commands to a syslog server or **SIEM - Security information and event management**. The log has consistent timestamp formats across all event logs which are necessary for accurate and efficient event correlations and log analysis



03:10:12 pm
Generation of certificate revocation list successful for host 'eagappnsovip89.engba.veritas.com'

01:41:06 pm
Generation of certificate revocation list successful for host 'eagappnsovip89.engba.veritas.com'

01:24:09 pm
Generation of certificate revocation list successful for host 'eagappnsovip89.engba.veritas.com'

01:08:51 pm
Generation of certificate revocation list successful for host 'eagappnsovip89.engba.veritas.com'

12:53:56 pm
Generation of certificate revocation list successful for host 'eagappnsovip89.engba.veritas.com'

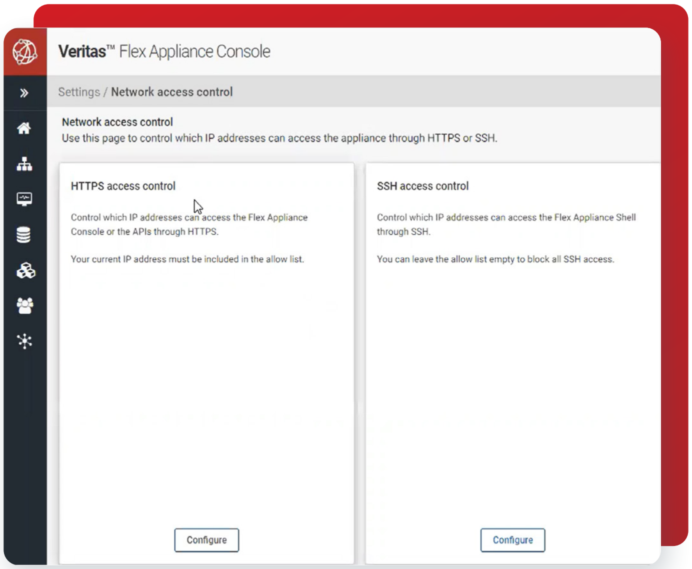
12:41:49 pm
Generation of certificate revocation list successful for host 'eagappnsovip89.engba.veritas.com'

12:24:12 pm
Generation of certificate revocation list successful for host 'eagappnsovip89.engba.veritas.com'

Flex Appliance offers UDP and TCP options. You can also use TLS log transmission, a cryptographic protocol that provides end-to-end security of data sent between applications over the network. You need a CA certificate and the client private key to configure TLS log transmission.

NetInsights Console Integration

The Veritas NetInsights Console lets you leverage accurate reporting to uncover the total amount of backup data involved and develop proactive budget decisions. By integrating Flex Appliances with the NetInsights Console, you can determine key risks and improve operational efficiency, reduce unplanned maintenance and downtime, and increase ROI with global insights and monitoring.



Veritas™ Flex Appliance Console

Settings / Network access control

Network access control
Use this page to control which IP addresses can access the appliance through HTTPS or SSH.

HTTPS access control

Control which IP addresses can access the Flex Appliance Console or the APIs through HTTPS.

Your current IP address must be included in the allow list.

SSH access control

Control which IP addresses can access the Flex Appliance Shell through SSH.

You can leave the allow list empty to block all SSH access.

Restricted Appliance Platform Network Exposure

Network access control mitigate the risk of information being accessed without the appropriate authorization. You can control which IP address or subnet can access Flex Appliances via SSH and HTTPs with an allow list. All IP addresses are not on the allow list are blocked by default.

Restricted Application Platform Network Exposure

To reduce SSH exposure on Flex Application instances customization, you can change default SSH port or restrict interface use for SSH connection by editing **/etc/ssh/sshd_config**.

Reducing SSH exposure for AD or LDAP users

You can connect a Flex Appliance **primary or a media server instance** via System Security Services Daemon (SSSD) with LADP or AD for authentication and authorization.

You can restrict access to specific users or groups with sssd.conf file by using **ldap_access_filter** or **ad_access_filter**. Check the detail at Flex Appliance product document.

Container Service Isolation

Namespaces Isolation

The VxOS kernel provides namespaces, control groups, and secure computing mode to control processes and resources at the OS level. NetBackup Flex Appliances use these features to control access and manage resources.

The concept of namespace is a feature of the VxOS kernel that provides fundamental support for containers in VxOS. Namespaces ensure a group of processes only sees its own set of assigned resources and another group of processes only has access to its own, discrete services. Neither group of processes can see the resources assigned to the other group.

Control Groups

Control groups (cgroups) provide resources management for the CPU, memory, disk I/O, and networking. Using cgroups protects an appliance from being taken down by a single container consuming all available resources on the physical system. Cgroups are help defend against denial-of-service (DoS) attacks on NetBackup Flex Appliances.

Multiple NetBackup Domains

Flex Appliances tightly integrate with NetBackup and simplify your environment by providing a common platform for Veritas data protection. You can consolidate multiple NetBackup and MSDP-C deployments (domains) on a single Flex Appliance, substantially reducing data center costs and complexity.

The Docker container software runs directly on the appliance VxOS, which is a Linux-based OS. VxOS provides the Flex Appliance kernel, runtime library, and container engine. The Flex Appliance uses container isolation and security technology to ensure users are kept separate from one another when using different instances of NetBackup on a single appliance. Between the kernel features built into the VxOS and the network and data segregation, users of NetBackup services are effectively firewalled from one another. This multi-domain architecture simplifies your NetBackup environment by allowing multiple NetBackup domains to run on this common platform (see Figure 3).

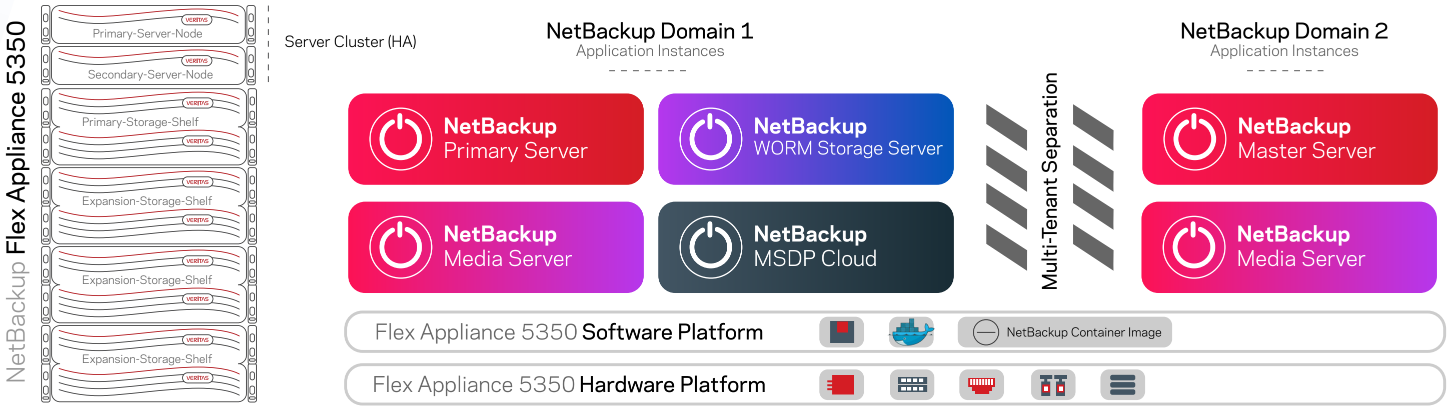


Figure 3. An overview of the NetBackup Flex Appliance's multi-domain architecture.

All application containers running on Flex Appliances need to share the hardware resources of the host such as CPU, memory, disk I/O, and network. Flex Appliance containers use Linux Control Groups (cgroups) resource management and namespaces to isolate the processes (see Figure 4). The network and data segregation and the Veritas Optimized Operating System (VxOS) security features provide secure NetBackup multi-domain implementation and reduce the potential of security exploits. You can consolidate multiple NetBackup and Media Server Deduplication Pool Cloud Tier (MSDP-C) deployments (domains) on a single Flex Appliance, substantially reducing data center costs and complexity.

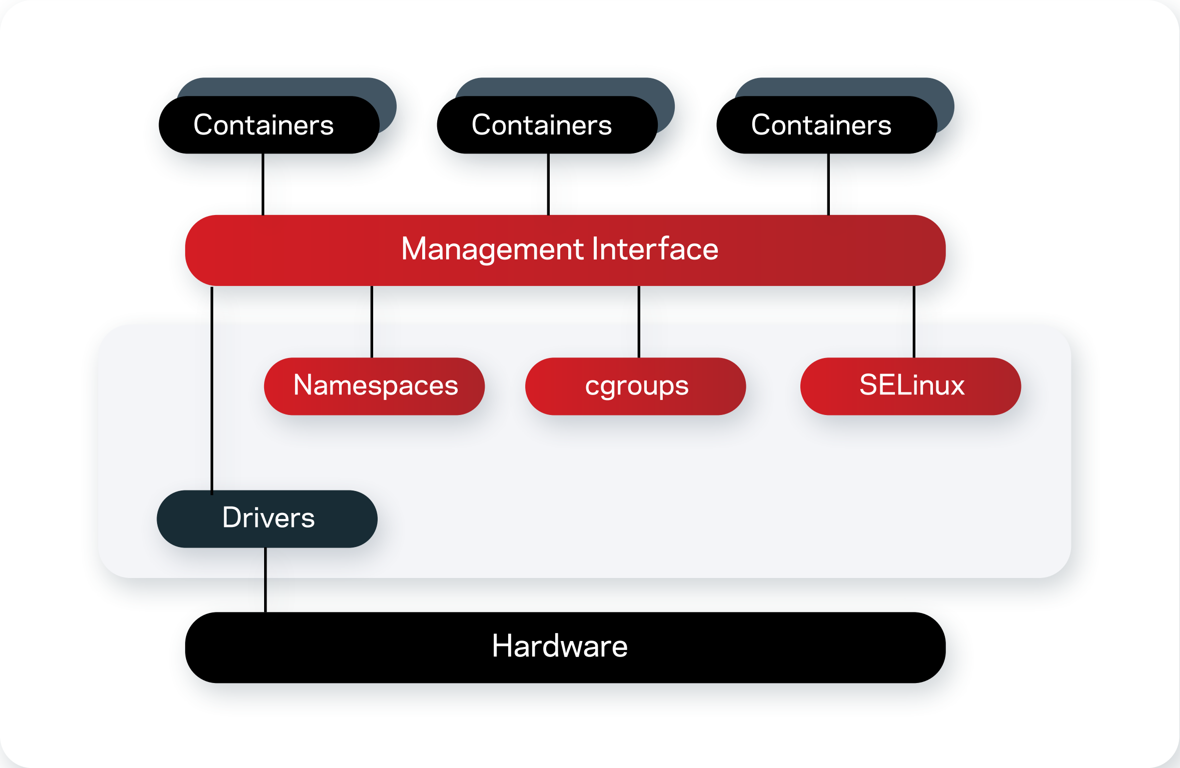


Figure 4. An overview of how Flex Appliance containers isolate processes.

Network Segregation

NetBackup Flex Appliances use the Macvlan network driver to assign a MAC address to each container's virtual network interface; each MAC address is bound directly to a physical network interface. This approach provides external connectivity to and from the containers as well as network isolation between them.

Flex Appliances use the VEPA Macvlan type; data from one Macvlan instance to the other on the same physical interface is transmitted over the physical interface. Either the attached switch needs to support hairpin mode or there must be a TCP/IP router forwarding the packets to allow communication (see Figure 5).

In addition to Macvlan, Flex Appliances have separate internal networks for network isolation. Internal network bridges use reserved subnets for security boundaries

The separate internal networks ensure the container networks cannot have direct access to each other—even when running in the same host. This design prevents containers-to-container attacks: If one container is exploited, it cannot harm other containers.

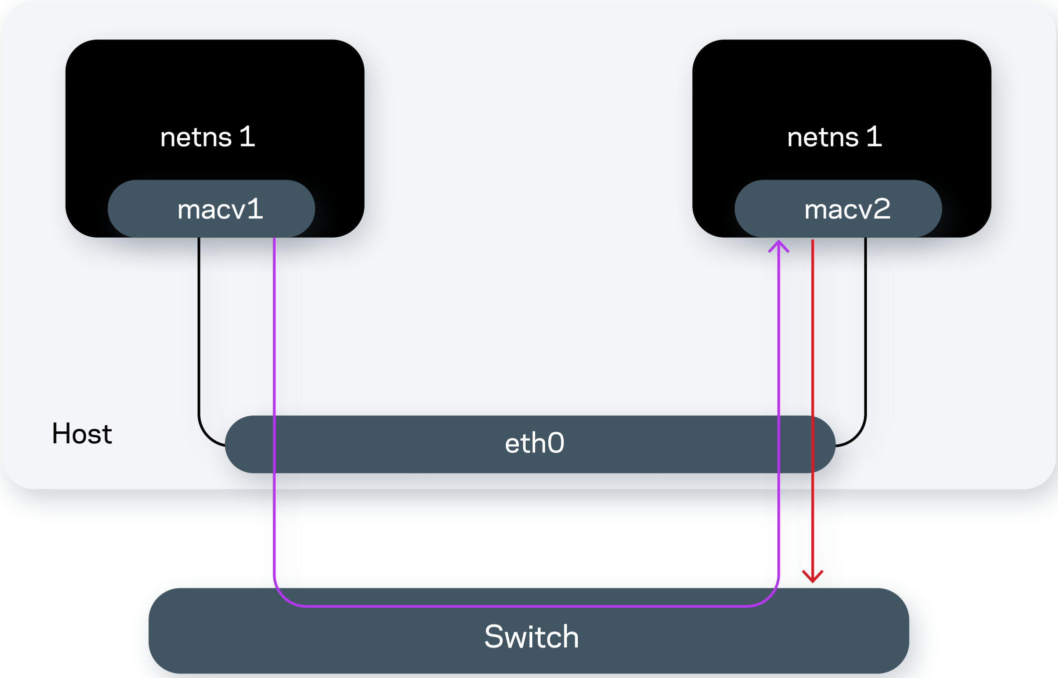


Figure 5. An example of how Flex Appliances use Macvlan to ensure network segregation.

SELinux for Limited-Service Privilege

The VxOS kernel secure computing mode (seccomp) feature limits the number of system calls a process can make through secure, one-way transactions. NetBackup Flex Appliances use seccomp to control the security of the NetBackup containers with a seccomp profile. Each profile represents a list of privileged system calls that are blocked within the container.

SELinux Multi-Category Security (MCS) allows users to label files with categories for further constraining Discretionary Access Control (DAC) and Type Enforcement (TE) logic.

In Flex Appliances, applications and services are containerized and they run with MCS turned on for exclusive data access. The Docker engine assigns a unique category pair (C1, C2) to provide isolation between the containers. Flex Appliances present dedicated file systems mounted with security context for exclusive access to each container. Each service container has a unique SELinux MCS category and resource limits.

Immutable Storage

Flex Appliances provide a complete immutable storage solution to defend your backup data and recover in software and hardware. NetBackup Flex WORM storage provides immutability and indelibility for your data. Immutable and indelible data cannot be changed for a determined length of time to protect data against cybercriminal intrusion and internal threats. This property protects the backup image from being deleted before it expires to ensure your data is protected from malicious deletion. Flex Appliances provides instant access to WORM storage to maintain business continuity or minimize downtime in case of a cyber-attack. Through restricted shell commands, you can configure and enable instant access services on the WORM storage. You can change the content of the instant mount but not the original WORM storage.

Cohasset Associates evaluated NetBackup's capabilities against compliance regulations and showcased how NetBackup with WORM-capable storage meets the requirements. NetBackup WORM capability is vendor-agnostic and will run on devices with immutable storage. Flex Appliances offer a hardened solution with immutable storage that prevents access to backup data by malicious invaders. We provide organizations with hardened solutions while also securely protecting their most important asset—their data.

NetBackup and Flex Appliance immutability solutions have completed the Cohasset Associates' immutability assessment (in compliance mode), specifically:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c)
- Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d)

To see the full assessment, visit Veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup.

Lock-Down Mode

The NetBackup primary server communicates with the storage unit to gather the immutability and indelibility capability and WORM retention period (min/max) settings. The primary server sets up immutability controls on the storage unit and applies the WORM retention period policy. NetBackup provides backup image management with visual representation of the immutable lock, image deletion after the WORM retention period (via the command line interface [CLI]), and honors legal hold on the catalog. (See Figure 6.)

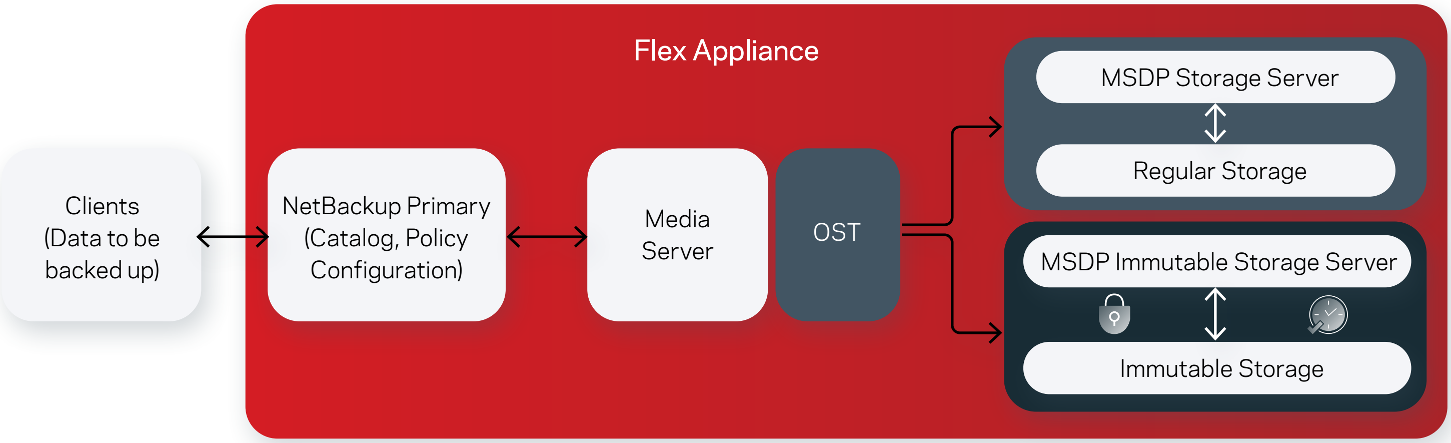

Flex Appliance
Clients (Data to be backed up)
NetBackup Primary (Catalog, Policy Configuration)
Media Server
OST
MSDP Storage Server
Regular Storage
MSDP Immutable Storage Server
Immutable Storage

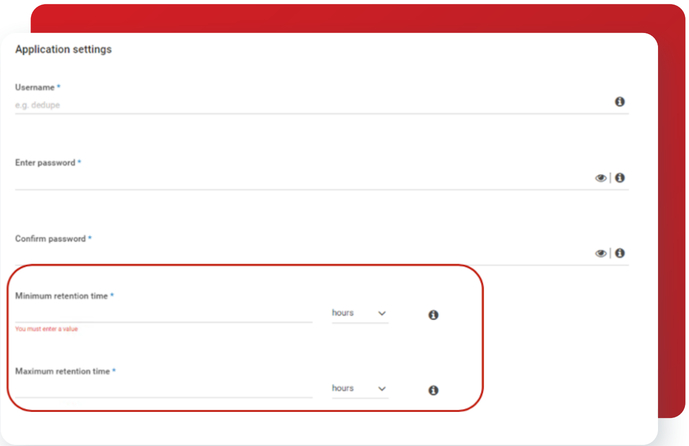
Figure 6. An overview of the FIPS 140-2 standard with which Flex Appliances comply.

NetBackup Flex Appliances have an immutable storage server to provide WORM capability, retention locks, and platform hardening to protect against malware infiltration and ransomware attacks. A specially designed secure Compliance Clock is used to manage retention periods and is independent from the OS time. NetBackup Flex Appliances have two lock-down immutability modes—Enterprise and Compliance. You can enable the appliance lock-down state at any time. You can choose either Compliance mode or Enterprise mode for an MSDP storage instance, but you cannot mix the two modes. Table 1 lists the differences between Enterprise mode and Compliance mode.

	Enterprise Mode	Compliance Mode
WORM storage instance creation	Can create WORM storage instances.	Can create WORM storage instances.
WORM storage instance deletion	Any administrator can delete WORM storage instances if there is no immutable data. However, only the default admin user can delete them if immutable data is present.	Any administrator can delete WORM stor-age instances if there is no immutable data. No one can delete WORM storage instance if there is immutable data.
Lock deletion	Deleting an Enterprise lock with the Flex/ MSDP solution is a two-step process: 1. The storage "security admin" removes the retention period (the existing storage admin is not authorized). 2. The NetBackup admin requests image deletion via the catalog.	N/A
Security level change	To change from Enterprise mode to Normal mode, you must first delete all WORM storage instances.	To move down to Enterprise or Normal mode, you must first expire all data on the WORM storage instances and then delete the instances.

Table 1: Enterprise and Compliance Mode Comparison

During the MSDP immutable storage server creation, you will be prompted to enter the minimum and maximum retention times. The minimum retention period is the shortest amount of time a WORM file can be retained in a storage unit. The maximum retention period is the longest retention period a file can have at the time it is committed to WORM. The retention period configuration can be changed via the CLI (see Figure 7).



Application settings

Username *
e.g. dedupe

Enter password *

Confirm password *

Minimum retention time * hours
You must enter a value

Maximum retention time * hours

Figure 7. The process of setting the retention period for a WORM file in the Flex Appliance web UI.

Isolated Recovery Environment

For enhanced ransomware resiliency, it is important to not only secure your backup data on immutable storage but also to maintain an isolated copy of your backup data.

This is often referred to as an air gapped copy. An Isolated Recovery Environment (IRE) enables air-gapped backup copies by disabling network connectivity to a secure copy of your critical data, providing administrators a clean set of files on demand to neutralize the impact from a ransomware attack.

The NetBackup Flex IRE solution:

- Stores an isolated copy of the data ensuring it stays unaltered until it's no longer needed
- Ensures data is immutable and indelible – minimizing threats from both ransomware and rogue users
- Detects ransomware infections within the protected data to prevent re-infection when restoring data

- Enables recovery operations at scale so business services can meet service level objectives
- Enables predictable recovery processes that can be rehearsed to on-premises or cloud infrastructure

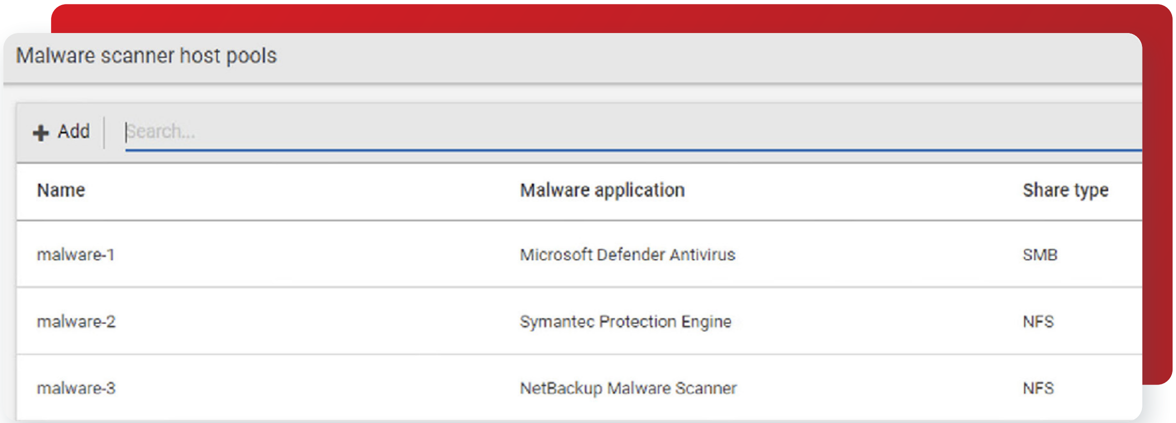
Unlike traditional IRE solutions, the NetBackup Flex IRE solution offers a unified, scalable solution with immutability and indelibility. In addition, the Veritas IRE is based on the Flex appliances' container-based multi-domain WORM storage with hardening OS and a zero-trust architecture without additional license cost. NetBackup Anomaly and Malware Detection provides another line of defense against malware propagating in the environment. NetBackup IRE provides a simple means to determine Service Lifecycle Policy (SLP) windows and configure an Air-Gapped schedule for maximum protection with a simple streamlined approach.

To help you understand more and leverage Veritas NetBackup IRE to defend against ransomware, check "NetBackup Isolated Recovery Environment" white paper.

Data Security with NetBackup Malware Scanning and Anomaly

NetBackup Malware Scanning provides greater control in the detection and recovery portions of the workflow. NetBackup offers two malware scanning methods to protect your data's integrity and the backup image: on-demand scans and scans automatically triggered by high anomaly scores.

The integrated NetBackup malware engine allows you to perform on-demand scans of backup images for latent threats. Additionally, integration with leading malware scanners such as Microsoft Defender and Symantec Protection Engine was made available in the NetBackup 10.0 release.



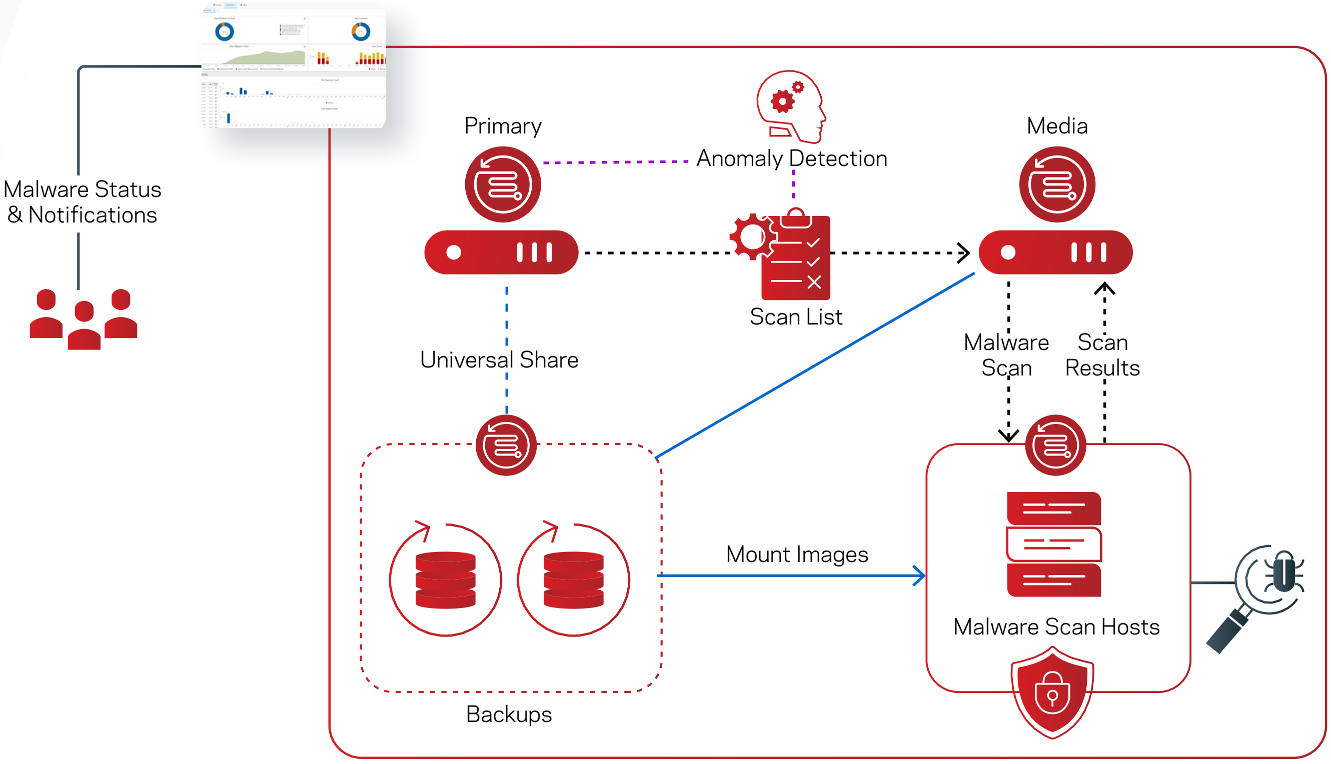
Name	Malware application	Share type
malware-1	Microsoft Defender Antivirus	SMB
malware-2	Symantec Protection Engine	NFS
malware-3	NetBackup Malware Scanner	NFS

Malware scanners can be deployed on one or more hosts, depending upon concurrent scanning requirements. These scan hosts are grouped together into a scan pool that can inspect unstructured data of either MS-Windows or Standard data types.

Malware scanning can be initiated using the WebUI or launched automatically when a high anomaly score is generated from Anomaly Detection activity. You can also create custom data protection workflows using our powerful APIs. Scan pools should be configured with a common malware application along with the desired protocol and you should not mix engines or protocols when adding additional scan hosts.

Malware Detection leverages Universal Shares, so you don't need to configure a specific share for scanning. NetBackup Flex appliances have all the pre-requisites for Malware Detection and support SMB and NFS shares.

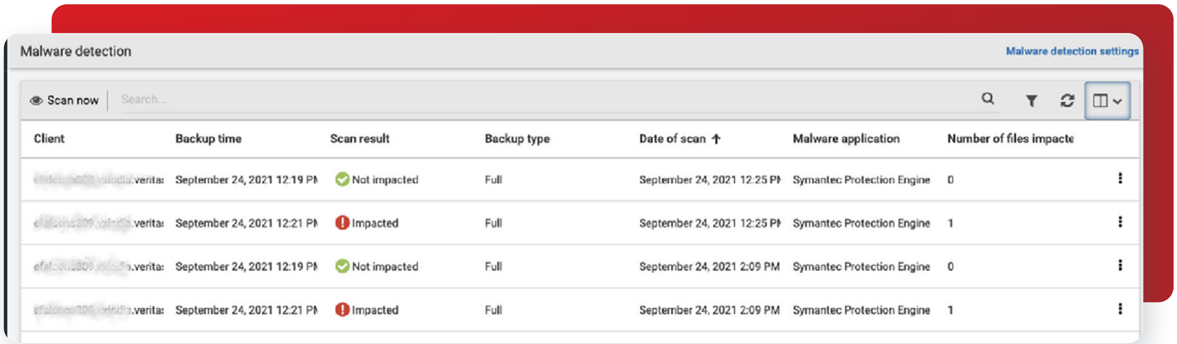
The MSDP host exposes the image to the scan host as a read-only share so there is no additional risk to read a potentially infected image. As an image passes through its Storage Lifecycle Policy (SLP), you can scan images once they reside on MSDP without interrupting the secondary SLP operations.



An on-demand scan model in the NetBackup WebUI is focused on periodic inspection of images, with the option of enabling automatic scanning for images with high Anomaly Detection scores. Focus your on-demand scans against the high-risk hosts—hosts interfacing with the public internet, Internet-of-Things (IoT) devices, and other edge machines.

On-Demand scanning targets images within a specific range for a specific host and each image will be scanned in a single job. The scan's output status is stored with the image and offers common remediation actions, which also triggers an alert in the top right of the WebUI.

Once an impacted image is detected, you can view the impacted files list, expire all copies, or leave the image in place where the scanning status tag will alert when the backup image is selected in a recovery workflow in the future. The last-known-good image will be clearly visible in the recovery workflow and selecting an impacted image will present several warnings to the user.



Client	Backup time	Scan result	Backup type	Date of scan ↑	Malware application	Number of files impacte	
[redacted].verita	September 24, 2021 12:19 PI	✓ Not impacted	Full	September 24, 2021 12:25 PI	Symantec Protection Engine	0	⋮
[redacted].verita	September 24, 2021 12:21 PI	! Impacted	Full	September 24, 2021 12:25 PI	Symantec Protection Engine	1	⋮
[redacted].verita	September 24, 2021 12:19 PI	✓ Not impacted	Full	September 24, 2021 2:09 PM	Symantec Protection Engine	0	⋮
[redacted].verita	September 24, 2021 12:21 PI	! Impacted	Full	September 24, 2021 2:09 PM	Symantec Protection Engine	1	⋮

Veritas makes sure security is not compromised when working on support issues and evidence collection. Data Collect sanitization is on by default and must be manually disabled. Appliances Data Sanitization features removes the sensitive information such as PII or other contact details like email addresses, usernames, passwords, host names and IP and MAC addresses.

Summary

Veritas Flex Appliance provides a multi-layered zero trust appliance platform covers infrastructure security and data security. Veritas solution ensures your data resiliency by immutable storage and encryption, data observability by malware scanning, anomaly detection and File Analytics and Classification and data remediation by isolating Malware and mass recovery. As an industry leader in data protection, Veritas provides the technological depth and experience to safeguard your business-critical data across physical, virtual, and cloud environments.

References

- Flex Appliance Product Documents
- NetBackup Product Documents

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact