VERITAS

NetBackup Flex Appliance Security

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

Veritas NetBackup™ Flex Appliances provide a complete immutable storage solution to defend an organization's backup data and recover in software and hardware. This white paper highlights the intrusion detection and prevention, OS hardening, and multi-tenancy security features in the Flex Appliance with NetBackup solution.

White Paper | July 2022

Contents

Introduction . . . 3

Executive Summary . . . 3

Scope . . . 3

Infrustructure Immutability and Indelibility Protection . . . 4

Container Isolation . . . 4

Network Segregation . . . 4

Namespaces Isolation . . . 5

Control Groups . . . 5

SELinux for Limited-Service Privilege . . . 5

Multiple NetBackup Domains . . . 5

OS Hardening . . . 6

Software Hardening with RBAC . . . 6

Software Hardening . . . 7

Physical Firmware Hardening . . . 7

Appliance Management Hardening . . . 7

Security Technical Implementation Guide . . . 8

Data Encryption . . . 9

Immutable Storage . . . 10

Lock-Down Mode . . . 10

Isolated Recovery Environment . . . 11

External Certificate Authorization . . . 12

Log Forwarding . . . 12

LDAP User Login and Smart Card Authentication . . . 13

NBU Flex Appliance . . . 13

Customizable Login Banner . . . 13

Summary . . . 13

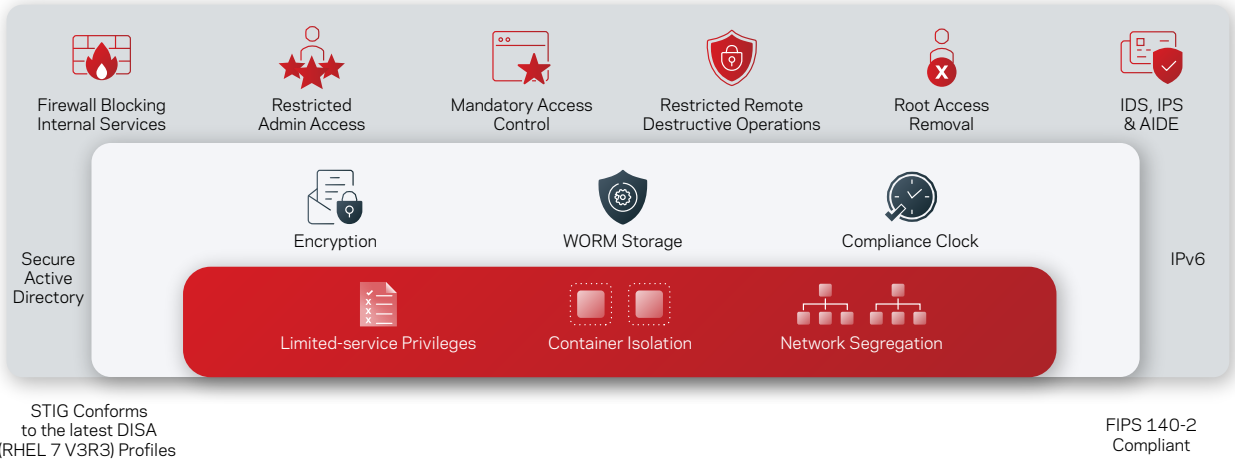
References . . . 14

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 architecture is to use the least privileges needed to complete a particular task based on roles and permissions, combined with robust user authentication, authorization, and policy-based data protection. 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 multi-domain isolation, network segregation, and container separation. 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.



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: NetBackup Isolated Recovery Environment Solution
- For best practices and sizing recommendations: NetBackup Flex Appliance Best Practices
- 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

Infrastructure Immutability and Indelibility Protection

With the combination of a hardened OS, container isolation and Zero Trust security model, Flex Appliances provide the multi-layered infrastructure immutability and indelibility necessary for ransomware protection (see Figure 1).

NetBackup Flex Appliances Zero Trust Architecture

Container Isolation
- Namespace Isolation
- Network Segregation
- Limited-service Privileges

Hardened OS
- Software Hardening with RBAC
- Firmware Hardening
- Appliance Management Hardening
- STIG Compliance
- Integrated IDS/IPS

Encryption
- FIPS 140-2 Compliant

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

Container Isolation

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 2). 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.

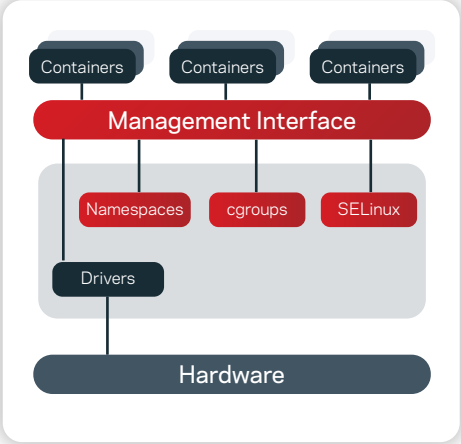


Figure 2. An overview of how Flex Appliance containers isolate processes.

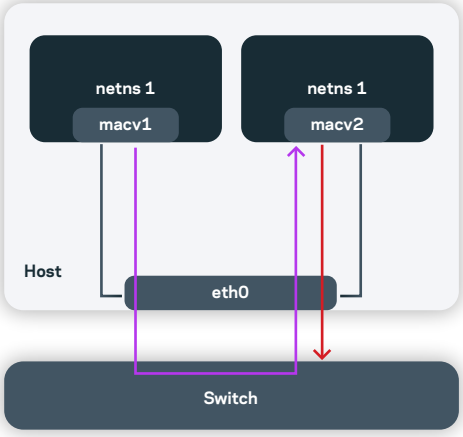


Figure 3. An example of how Flex Appliances use Macvlan to ensure network segregation.

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 3).

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.

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.

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.

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 4).

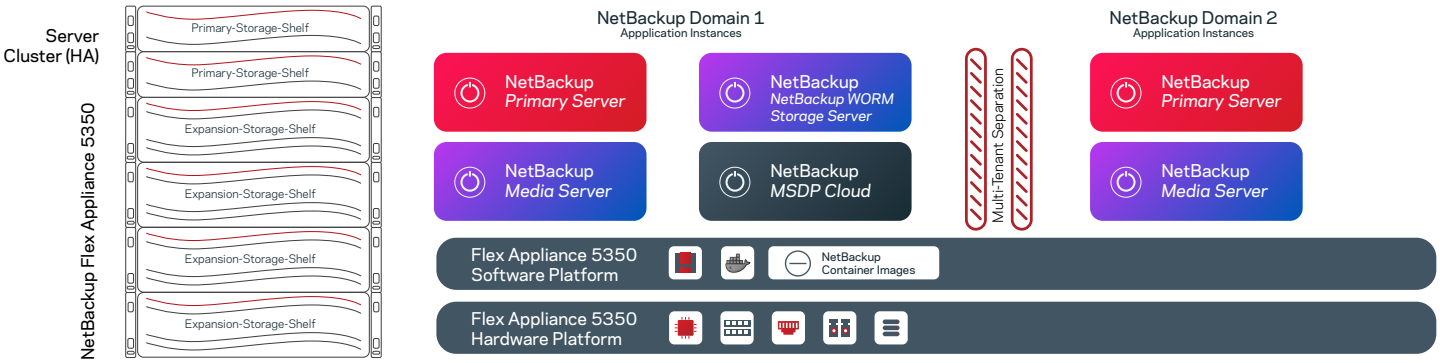


Figure 4. An overview of the NetBackup Flex Appliance's multi-domain architecture.

OS Hardening

Secure by default

The overall hardened solution on Flex Appliances provides the following features:

- Hardened Linux OS components
- Prevents or contains malware from harming the integrity of the underlying host system in the event of OS vulnerabilities
- Data protection that tightly limits access to only those programs, process and resources that need access, regardless of system privileges
- Hardened appliance stack
- Locked-down appliance application binaries and configuration settings so that changes are tightly controlled by the application or trusted programs and scripts
- Expanded detection and audit capabilities
- Enhanced visibility into important user or system actions to ensure a valid and complete audit trail that addresses compliance regulations (such as PCI) as a compensating control

Flex Appliances use the integrated Security-Enhanced Linux (SELinux) functionality supported by Red Hat to protect roles, platform, services, and applications with full Security Technical Implementation Guide (STIG) compliance. SELinux is a set of kernel modifications and user-space tools that gives administrators more control over who can access the system. It separates the enforcement of security decisions from the security policy and streamlines the amount of software involved with security policy enforcement. In Flex Appliances, each service container has unique SELinux MCS category and resource limits to enhance security and availability.

SELinux is also used in the context of container separation to prevent containers from attacking the host file system and also to prevent container-to-container attacks. The standard Linux security model allows the superuser "root" to bypass all security checks, including the possibility of using the setuid bit to allow users to run an executable file with the permissions of the executable file owner. This model can cause security issues. SELinux is a labeling system and views each object on the system with a SELinux label—a file, directory, socket file, symlink, shared memory, semaphore, or FIFO file—and also every subject such as a running process or Linux user entity. This deep inspection of object requests by the object manager and security server permits SELinux to deny access to unexpected requests for system resources.

Software Hardening with RBAC

ole-based access control (RBAC) refers to the idea of assigning permissions to users based on their roles within an organization. Flex Appliances use SELinux RBAC to authorize users to achieve OS hardening. User permissions are granted through roles to gain rights. A Flex Appliance login account is mapped to an SELinux user. Figure 5 shows that the Flex Appliance accounts HostAdmin, Root user, and Any user accounts are mapped to SELinux user staff_u and guest_u with staff_r and guest_r roles, respectively.

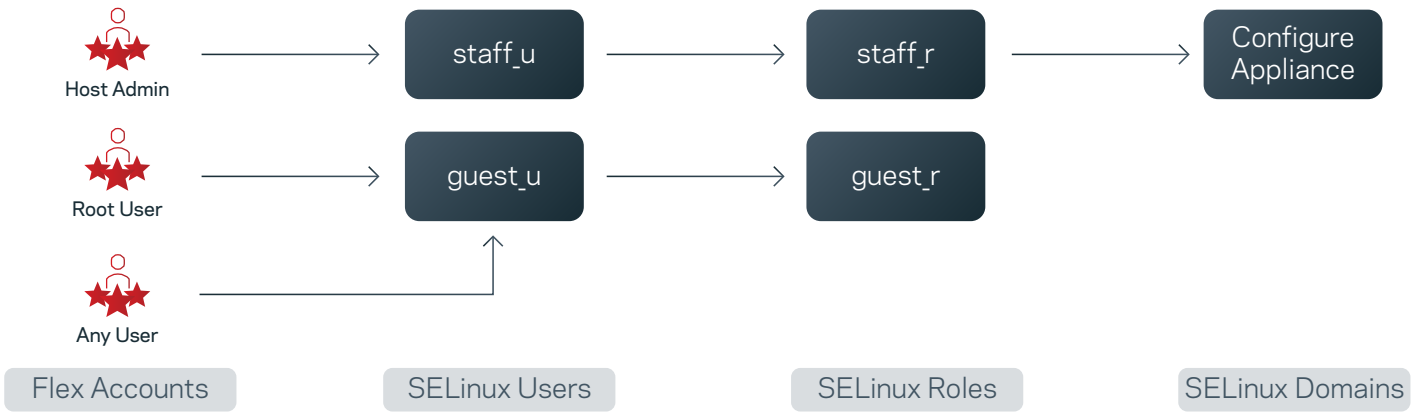


Figure 5. An overview of how Flex Appliance login accounts are mapped to SELinux users and roles.

SELinux has two modes: enforcing and permissive. Flex Appliances enable SELinux in enforcing mode to set the following policy rules:

- Root user account privileges are significantly limited. Only the hostadmin account can log in to compute nodes
- Flex Appliances keep IPS enabled even upon elevation, and the elevated user has most of the privileges
- Policies to allow all Flex Appliance Shell and web UI operations
- Policies to allow elevated users certain additional administrative commands
- File labeling for platform certificates, tokens, logs, and the compliance clock device
- Confine each of the instances and infra-services with exclusive access to their storage
- Policies to enable instances to run systemd and NFS services, access FUSE device, and mount NFS/CIFS shares

Note:

- The Flex Appliance root account and any customized accounts are reduced to SELinux user guest_u that has next to no-privileges
- An SELinux user is allowed one or more roles, restricting which roles a particular user can have
- Roles are mapped to permissions and allowed certain domains, runtime privileges for one or more applications.

Flex Appliance have integrated hardening of the software OS, physical firmware, and appliance management. Following are some additional details on how the system has been hardened.

Software Hardening

- Auditing enabled for low-level operations such as OS commands and system calls
- Ctrl-Alt-Delete reboot disabled
- SSH root login disabled
- Maximum 10 concurrent login sessions for the hostadmin account
- Interactive/login session idle timeout is 10 minutes
- Account lockout for 15 minutes after three consecutive incorrect login attempts in the Flex Appliance Shell within 15 min
- Account policies allow an elevated user certain administrative commands and access to the Shell

Physical Firmware Hardening

- 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

Appliance Management Hardening

You can use the NetBackup Flex Appliance Console to edit the password policy for user passwords. The password policy is enforced for local Flex Appliance Console users and the **hostadmin** user in the Flex Appliance Shell.

- 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

- Session timeouts that automatically sign users out of the NetBackup Flex Appliance Console and the NetBackup Flex Appliance Shell after 10 minutes of inactivity

Security Technical Implementation Guide

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. (See Figure 6.)

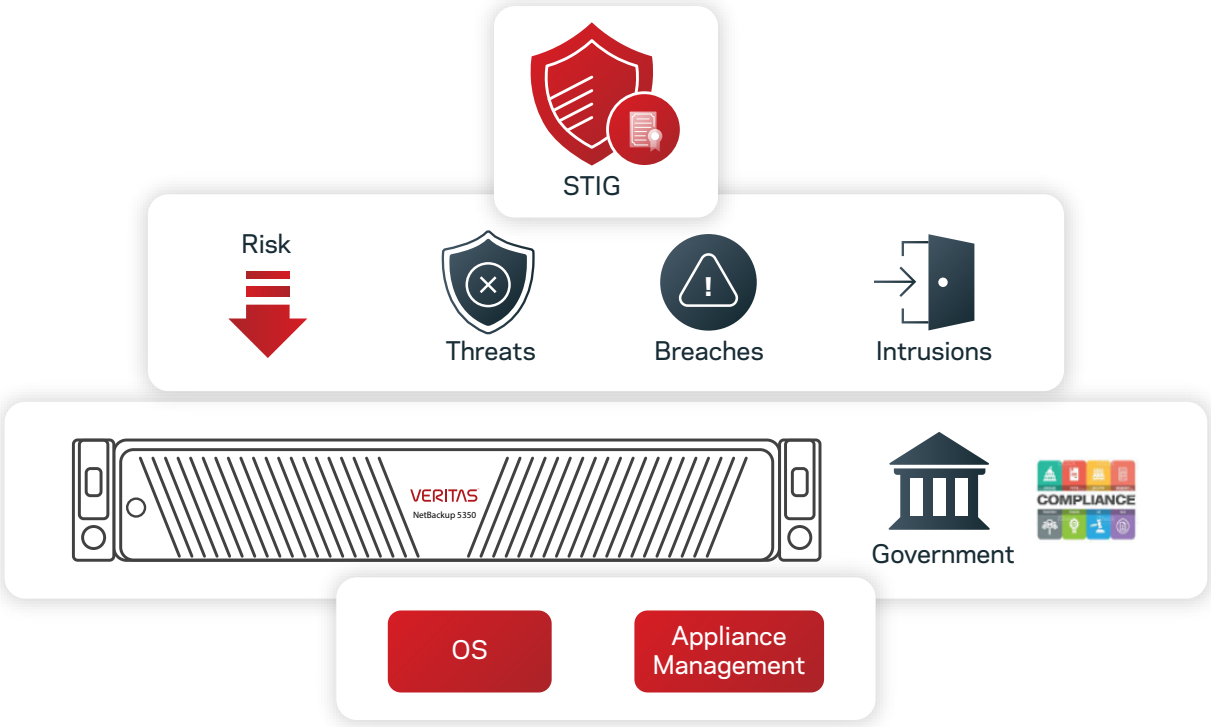


Figure 6. An overview of the STIG rules with which Flex Appliances comply.

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 7).

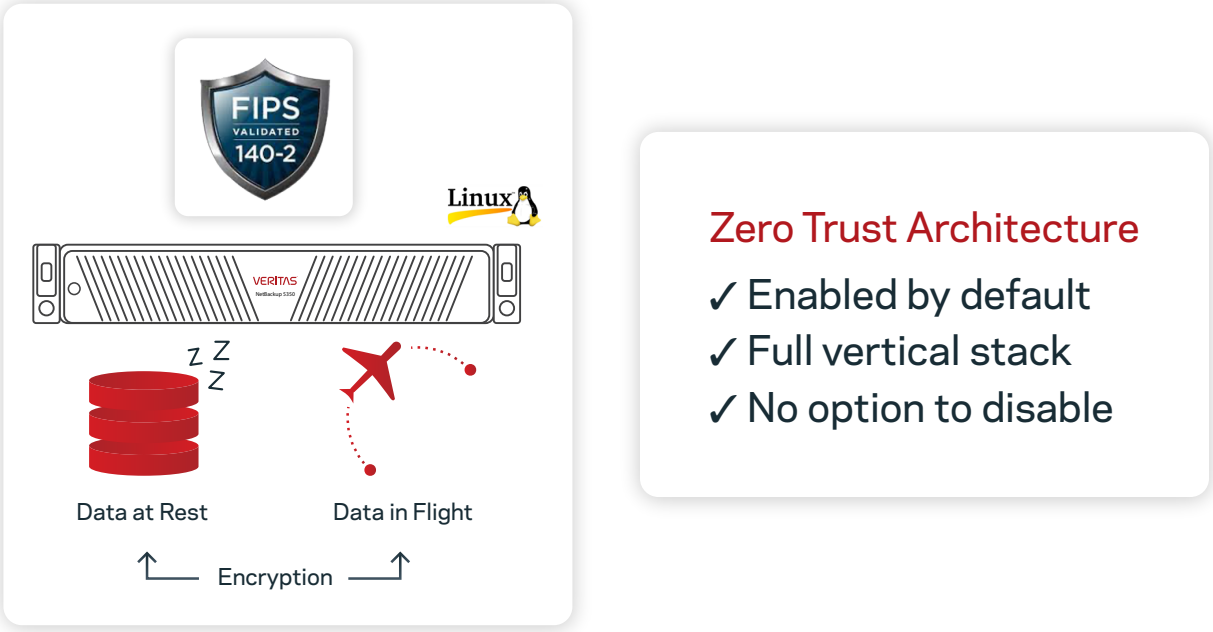


Figure 7: An overview of the FIPS 140-2 standard with which Flex Appliances comply.

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.

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 8.)

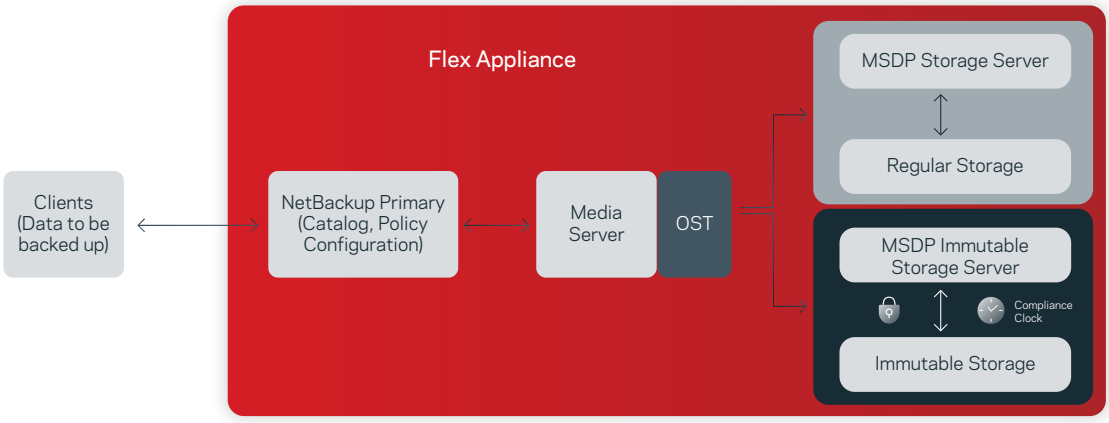


Figure 8: An overview of the FIPS 140-2 standard with which Flex Appliances comply.

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 storage 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 9).

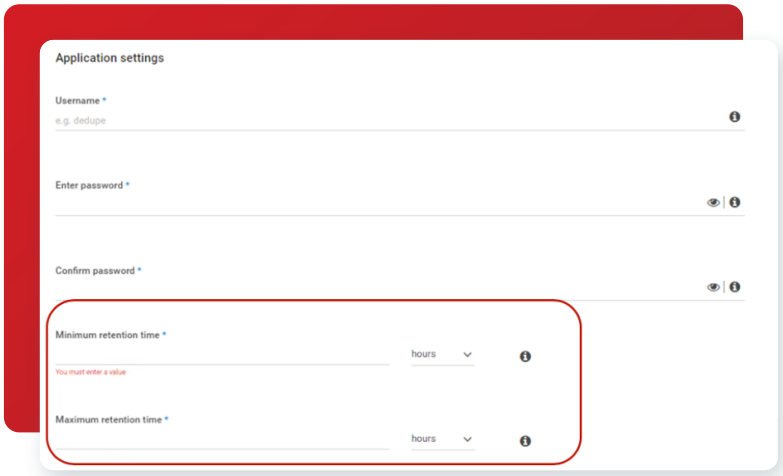


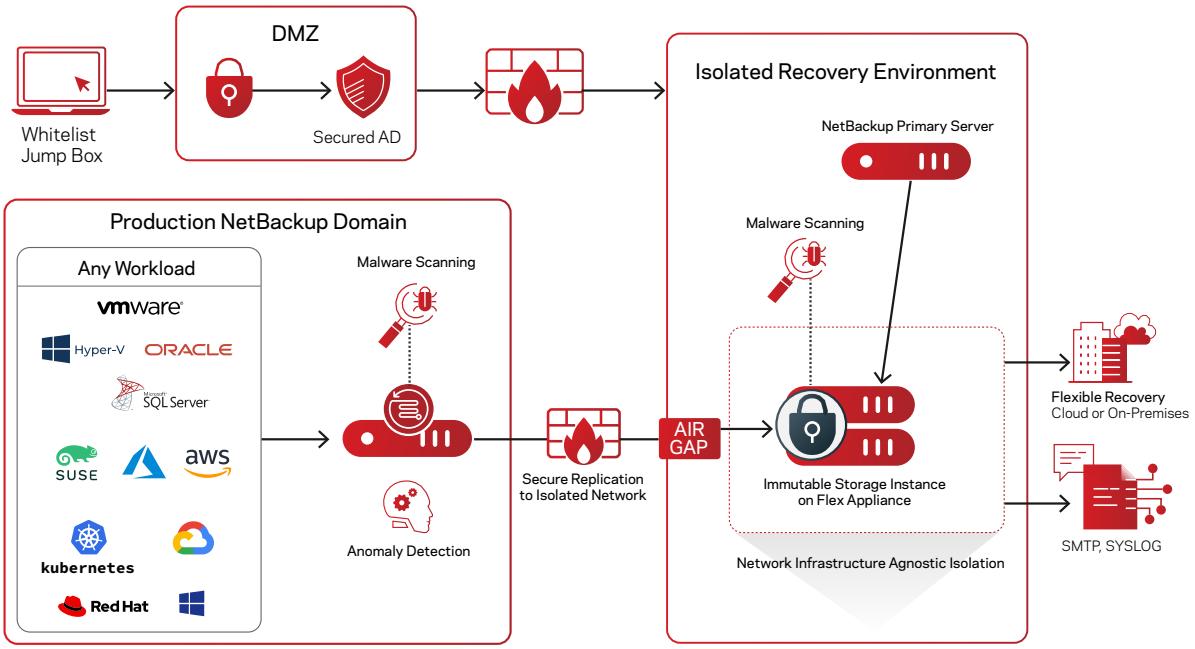
Figure 9: The process of setting the retention period for a WORM file in the Flex Appliance web UI.

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

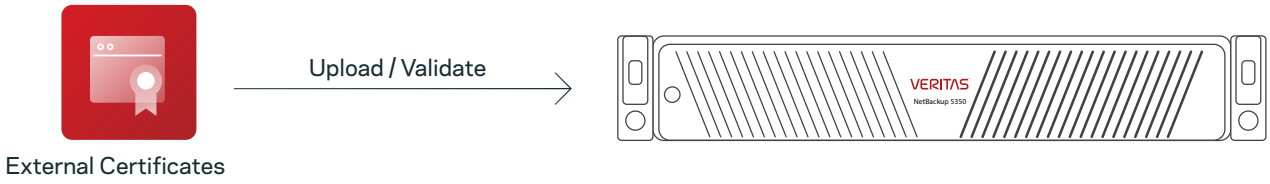


Unlike traditional IRE solutions, the NetBackup Flex IRE solution offers a unified, scalable solution with immutability and indelibility. In addition, the Veritas IRE is based on the Flex appliances' container-based multi-domain WORM storage with hardening OS and a zero-trust architecture without additional 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.

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.



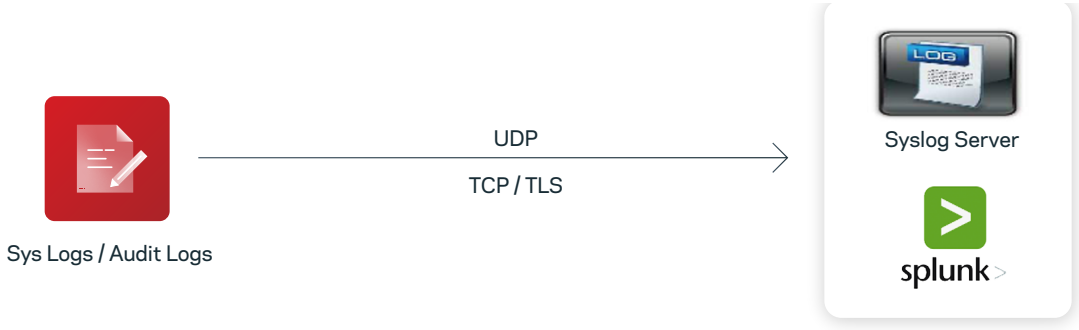
To use an external certificate, you must have the following:

- **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.

Log Forwarding

Log forwarding provides many benefits and can be used for compliance management, redundancy, data and operational analytics, centralized monitoring, and reviewing threat behaviors and long-term patterns. With Flex Appliances, you can forward logs including elevated shell commands to a syslog server or Splunk, expanding support for external log management platforms and offering the flexibility for organizations to leverage their current investment areas.

You can choose UDP or TCP protocols. You can also use TLS log transmission, a cryptographic protocol that provides end-to-end security of data sent between applications over the network (see Figure 10). You need a CA certificate and the client private key to configure TLS log transmission.

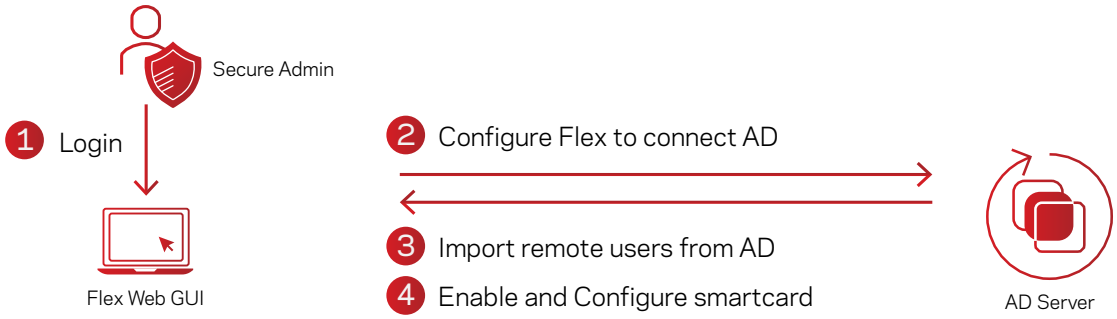


LDAP User Login and Smart Card Authentication

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



Customizable Login Banner

You can set a text banner that appears before a user signs in to 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.

Summary

Veritas provides a unified, multi-layered, hardened and secure appliance platform that optimizes operational efficienty and seamlessly integrates comprehensive protection and malware detection into an industry-leading backup and recovery solution. 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 global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

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

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

Copyright © 2022 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

V1516 07/22