VERITAS

NetBackup Flex Appliance Security

Elevated data protection.

White Paper | December 2023

Introduction

Data security is as important as data availability. The Mid-Year Update to the 2023 SonicWall Cyber Threat Report shows 2.7 billion malware and 140 million ransomware attacks. Cryptojacking attacks grew by 399% reaching 323 million by the end of June 2023. According to Cybersecurity Ventures, by 2031 a business will fall victim to a ransomware attack every two seconds—and the attacks will cost more than $265 billion annually.

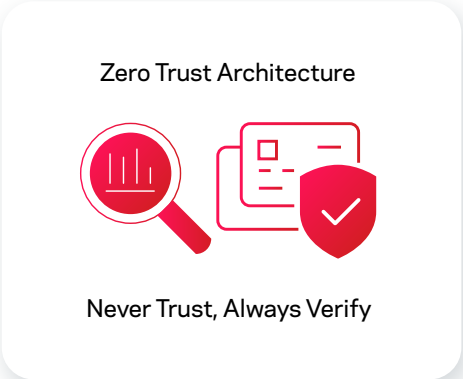
Successful, high-profile cyberattacks frequently resulting in multi-million dollar losses have raised the importance of secure and reliable data protection. Backup as a last resort for organizations' data recovery has also become the main target for cybercriminals.

This document describes security measures and enhancements implemented on Veritas NetBackup Flex appliances. The objective is to emphasize Flex appliances' high security features and how they benefit customers in guarding backup data and the data protection environment against ransomware, cryptojacking, and intrusion attacks.

Flex Appliance Security

Overview

The Zero Trust security model or architecture based on the never trust, always verify principle has been the primary design guideline for Flex appliances from their inception. With Zero Trust by default, users, devices, services, and processes are not trusted and require identity verification along with the least privilege resource access. The Zero Trust model is instantiated on Flex appliances on multiple levels, starting at restraining system access, and culminating with blocking access to the data destruction operations.



The main cyber resiliency barriers may be grouped into the following objectives:

- Restricting system network access
- Preventing unauthorized user login
- Limiting user and process permissions at the operating system and applications
- Restricting access to destructive storage operations

As each barrier is penetrated, the appliance security controls become more restrictive at every stage to reduce the risk of damage to the backup data. For example, if a bad actor gains network system access due to an incorrectly configured firewall and lax network access controls, the appliance—and consequently backup data—is still secure, since the unauthorized user login controls are in place to prevent cybercriminals from logging in.

We will examine each control in greater detail and describe its advantages from the security perspective and the corresponding benefits. See Figure 1 for an outline of appliance security measures.

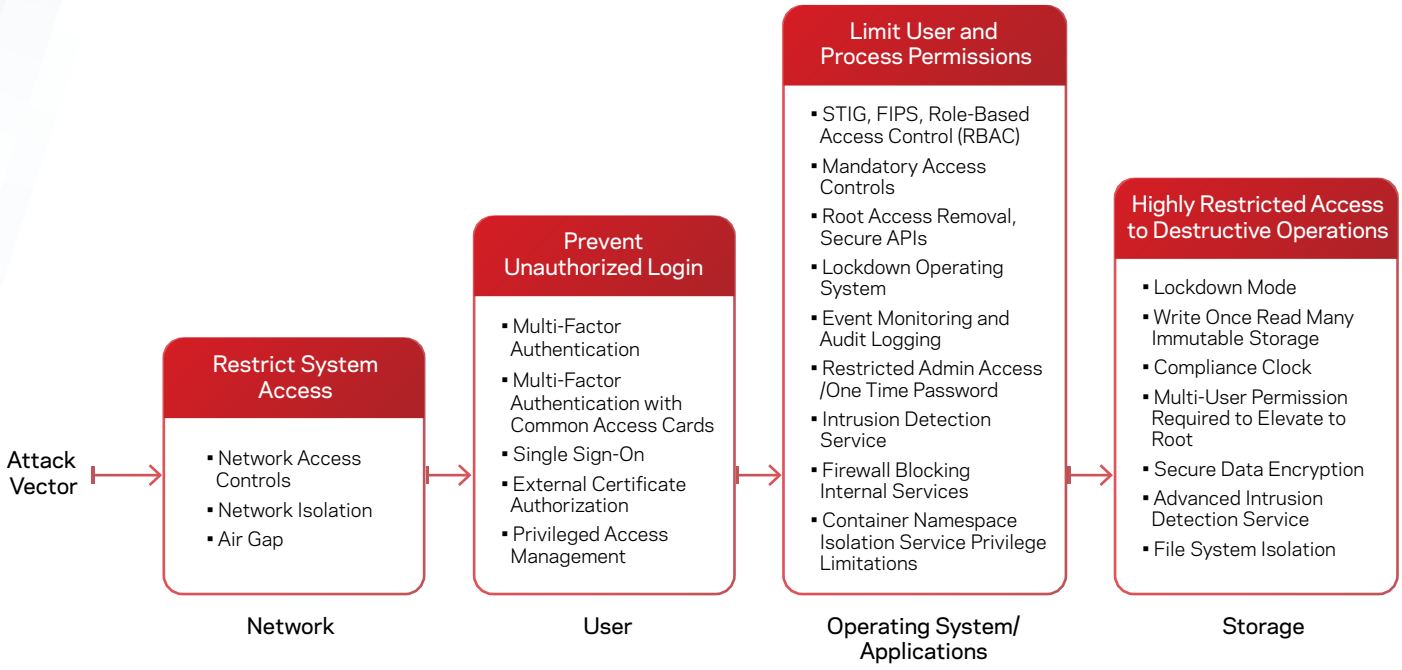


Figure 1. Flex Appliance Security Barriers

Restricting System Access

Modern computers provide multiple potential system entry points that can be exploited by hackers. Flex appliances restrict system access using the following techniques:

- Network Access Controls
  Administrators can manage appliance access by creating separate lists of IP addresses allowed to connect using Secure Shell (SSH) and HTTPS protocols. Connection requests from IP addresses and subnets not listed in network access controls are automatically rejected. For increased security, the default SSH port 22 can be modified.
- Network Isolation
  All applications running on Flex appliances, including NetBackup primary and media servers, are deployed as containers and are network segregated. Appliances deploy MACVLAN type VEPA technology, where the network traffic between the containers is transmitted over the physical interface even if all instances (containers) are connected to the same NIC. This network implementation prevents direct inter-container communication and container-to-container attacks.
- Air Gap
  One of the security features of NetBackup is its ability to maintain an isolated copy of backup data, referred to as an air-gapped copy. This air-gapped copy is in an isolated recovery environment (IRE) that is created on a write once, read many (WORM) storage device. The network access to data in an isolated recovery environment is available only during the replication window, otherwise the air-gapped copy is protected against malware and ransomware attacks.

Preventing Unauthorized Login

Once system access is gained, user authentication (login) is required. Multiple authentication options are available to prevent unauthorized appliance login:

- Multi-factor Authentication
  Multi-factor authentication requires at least two factors (elements) of authentication before user is granted access to the resources. Multi-factor authentication on Flex appliances can be configured by individual users however, once enforcement is activated multi-factor authentication cannot be disabled.

- Multi-Factor Authentication with Common Access Cards (CAC)
  Common access cards provide two-factor authentication, where access to the resources is granted upon the card possession, as well as knowledge of the personal identification number (PIN).
- External Certificate Authority-Issued X.509 Certificate
  By default, Flex appliances use a self-signed certificate. Users may be able to gain appliance access by importing the X.509 certificate issued by an external certificate authority. Only users in possession of the X.509 certificate will be allowed to log in. This certificate is different from the NetBackup primary and media servers.
- Single Sign-On
  Single sign-on (SSO) is supported, however only identity providers using Active Directory or LDAP are supported with SAML 2.0-compliant identity providers.
- Privileged Access Management
  Flex appliances support external password management, such as CyberArk Privileged Access Management, to enforce password rotation policy and privileged session activity and monitoring.
- Intrusion Protection System
  The Intrusion Protection System analyzes system and network activity and logs any unauthorized access attempts.

Limit User and Process Permissions

If bad actors manage to successfully gain access and login to the appliance, additional restrictions implemented compliant with well-defined security standards provide further protection for the backup data and prevent system damage.

- Security Technical Implementation Guides (STIG) Compliance
  STIG is a cybersecurity configuration standard and methodology for securing protocols. Flex appliances are STIG compliant at the operating system (software and firmware) and appliance management level by using the STIG template to meet security requirements per the Defense Information Systems Agency (DISA) profile. Some examples of Flex appliance Security Technical Guides implemented for operating system hardening include:
  - Audit logging of cluster and appliance events—operations that are initiated by users such as login, add node, and configuration changes
  - Auditing is enabled for low-level operations such as operating system commands and system calls
  - Ctrl-Alt-Del (soft) reboot is disabled
  - SSH root login is disabled
  - Interactive/login session idle timeout enforcement
  - Limited number of concurrent login sessions
  - Forced password changes during initial configuration (default password change)
  - Logging of incorrect login attempts
  - Appliance console lock after three incorrect login attempts
  - Customizable password policies—the ability to set customized password policy, including the option to use STIGs for validation
  - Restricted access to GRUB (boot loader) menu
  - Conformance to the Federal Information Processing Standards (FIPS) 140-2
- Federal Information Processing Standards (FIPS)
  FIPS are National Institute of Standards and Technology standards for computer security and interoperability. Flex appliance operating system, platform software, and the NetBackup container conform to FIPS 140-2. Flex also takes advantage of the Security Enhanced Linux (SELinux) framework to create and enable proprietary security policies that conform with STIG guidelines (DISA RHEL7 profile) to further harden the operating system from malicious attacks.

- Role-Based Access Control (RBAC)

  Role-based access control is a security control mechanism where system and resource access are managed based on roles. Flex appliance has three roles: Super administrator, Administrator, and Security administrator. The Administrator role is assigned to all users, but only users with the Security administrator role can manage users and security of the appliance. The Super administrator role is assigned to the default user admin. This role and user cannot be changed.

- Mandatory Access Control

  Mandatory access control constrains processes and threads from accessing and taking certain actions on system resources, such as shared memory segments, file system objects, network ports, and IO devices. The Flex operating system explicitly denies access to all resources—only programs and activities specifically requiring resource access are granted the right to use them, regardless of their system privileges.

- Root Access Removal

  The Linux security model allows the root to bypass security checks; however, the Flex appliance operating system eliminates console root account access. Only the hostadmin user is allowed to log in via SSH to the compute nodes.

- Secure APIs

  Veritas provides a set of secure rest API calls to programmatically manage and monitor the appliances. API access tokens are required for appliance access. The Administrator]can generate a Metrics token for the third-party analytics application, and a Support token for Veritas technical support personnel, to grant permissions to create, download, and clean up log packages. Appliance administration via API also requires credentials to create an X-AUTH-TOKEN for any management tasks. API executions are logged.

- Lockdown Operating System

  Flex appliances can lockdown the operating system. Once the operating system is locked down, modification to operating system services, network, and device drivers is not permitted. The lockdown mode prevents unauthorized changes, even in situations where appliance authorization has been compromised (stolen credentials). For the emergency operations, a one-time password is required. The one-time password can be obtained from Veritas technical support to temporarily unlock the appliance.

- Event Monitoring and Audit Logging

  Flex appliances monitor and analyze system events. All CLI commands and API executions are logged in a separate file and forwarded to the syslog for possible security incident investigation. Appliance system and audit logs can be forwarded to an external log management server. For improved security, TLS log transmission is also available.

- Restricted Admin Access/One-Time Password

  When in lockdown mode, the user admin (Super administrator) has restricted access which does not allow operating system and volume modifications such as deletion, mounting, and unmounting. Installation and uninstallation of software packages is also forbidden. In cases where restricted actions are required, dual authentication and participation from Veritas technical support is necessary to generate a one-time password for access to the appliance.

  Appliance hostadmin and application (NetBackup) appadmin users are forced to change the initial default password upon the first successful login.

- Intrusion Detection

  NetBackup Flex helps protect the system from an attack, misuse, or compromise with its built-in intrusion detection system (IDS), including an advanced intrusion detection environment (AIDE) and an intrusion prevention system (IPS). Intrusion detection isolates each application by allowing access only to assigned resources and processes.

- Firewall Blocking Internal Services

  The built-in firewall blocks all access except ports required for backup and management. All other internal services are blocked.

- Container Namespace Isolation and Service Privilege Limitations

  Flex appliances feature a highly secure, hardened Linux-based VxOS operating system that serves as a hosting platform for containerized services such as NetBackup, appliance management, and a metrics collection time series database, among others.

Containers are inherently more secure than traditionally-executed applications because of the separate resource allocation and logically independent configuration. Applications are packaged in binary bundles which undergo checksum verification before the execution. This approach assures immutability of the binaries and applications included in the container image. The logical independence is derived from the separation of various NetBackup functions (services) into different containers that can only access their own discrete resources. Moreover, NetBackup services are also separated from the backup images stored in WORM storage.

As mentioned earlier, the MACVLAN type VEPA architecture provides containers with network segregation. Sharing the host network with containers is also blocked to prevent snooping on communication between the services.

Containers are also assigned limited-service privileges to define intra-container executables and which system calls are allowed without the need for elevated system privileges.

Highly Restricted Access to Destructive Operations

For sensitive data, additional controls may be configured, virtually eliminating access to damaging operations such as volume formatting and deletion. Entry to hardware-based utilities is also protected. These controls are organized into lockdown modes. Different lockdown modes and corresponding restrictions are described below, along with additional security features:

- Lockdown Mode
  Flex appliance lockdown mode offers additional security levels to protect your appliance and data—it is a core component of the appliance immutable architecture. Lockdown mode sets the appliance into a heightened security level to protect data and the storage infrastructure. When in lockdown mode:
  - Administrators cannot make changes to the operating system, operating system services, and hardware device drivers.
  - WORM storage instances can be created only in lockdown mode. Any data written to WORM storage is immutable, which means it is marked as read only and cannot be modified, corrupted, or encrypted. Moreover, the data on WORM storage is also indelible, making it impossible to delete before the retention period expires.

  Flex appliance supports the following lockdown modes:

- Normal Mode
  This mode is the default mode of the appliance. Normal mode does not support WORM storage.
- Enterprise Mode
  - You can create WORM storage instances and delete them, including volumes with existing data
  - 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
  - When you delete a WORM storage instance as the default admin user, the instance can be running or stopped; when you delete a WORM instance as any other user, the instance must be running so that the system can verify that there is no immutable data present
  - To change from enterprise mode to normal mode, you must first delete all WORM storage instances
- Compliance Mode
  - You can create WORM storage instances; you can delete the instances only if there is no immutable data present
  - Any administrator can delete WORM storage instances if there is no immutable data
  - When you delete a WORM storage instance, the instance must be running so that the system can verify that there is no immutable data present
  - To change from compliance mode to enterprise mode or normal mode, you must first wait for all data on the WORM storage instances to expire and then delete the instances

See Table 1 for a summary of possible actions based on the lockdown mode.

Action	Normal Mode	Enterprise Mode	Compliance Mode
Create WORM Storage	No	Yes	Yes
Delete WORM Storage—No Data	N/A	Yes	Yes
Delete WORM Storage—Data Present	N/A	Yes	No
Storage Reset	Yes	No	No

Table 1. Lockdown Modes

- WORM Immutable Storage
  WORM storage provides data immutability and indelibility. The primary server sets up immutability controls such as mandatory data retention policy. WORM storage is available only when appliance is in lockdown mode.
- Compliance Clock
  The central attribute of WORM is the ability to accurately measure elapsed time to ensure minimum and maximum data retention duration. The immutable clock is independent of the operating system time, and the Network Time Protocol (NTP) is a function of the compliance clock. The compliance clock is tamper-proof—even the NetBackup administrator does not have the ability to modify it.
- Multi-User Permission Required to Elevate to root
  Before root access is granted to the shell, a separate password from a different user—external to the appliance—is required.
- Secure Data Encryption
  Data selected for backup, restore, and duplication, as well as corresponding metadata are encrypted over a secure TLC channel while in transit between NetBackup entities (primary and media servers). Encryption for data at rest is also available, including client-side, multi-server deduplication pool, cloud, tape drive, and AdvancedDisk destinations.
- Advanced Intrusion Detection Service
  As part of STIG rules, the Advanced Intrusion Detection Service keeps track of file systems and generates alerts if any new software is deployed, or if any changes are made to the operating system files. This feature provides enhanced visibility into important user and system actions to ensure a valid and complete audit trail that addresses compliance regulations such as Payment Card Industry as a compensating control.
- File System Isolation
  Access to the root filesystem is restricted to read only operations—even for the admin account—to prevent accidental or malicious damage. Host-level services are also blocked from accessing the container file systems. Additionally, dedicated filesystems mounted with security context are available for container-exclusive access, where file system sharing is not permitted. This makes each file system visible and accessible only by a single, specific container.

Security Updates

The dynamic nature of the security landscape, with discoveries of new vulnerabilities and more sophisticated attack techniques, requires frequent and regular appliance updates. Veritas is committed to delivering hotfixes for critical exploitable vulnerabilities within 30 days or as mandated by the Cybersecurity Information Security Agency. Maintenance releases are to be delivered about every 90 days, with fixes for medium, high, and critical vulnerabilities.

Security Meter

To simplify the process of securing the platform, Flex appliances include a Security Meter, which is a tachometer-style widget. The Security Meter evaluates the current state and recommends required actions to change the protection ranking from Good to Excellent. Some settings are enabled by default and cannot be modified, whereas recommendations are linked to the appropriate configuration section where they can be easily changed. The Security Meter is available only to the Super administrator (admin) user.

Summary

Veritas invests significant research and engineering resources in the development of Flex appliances to deliver a stable, reliable, and highly secure data protection solution. With each product release and regular product updates, new security features are added, and existing ones are enhanced to lower the risk ofcurrent and future threats. This highly secure platform, combined with the unbeatable NetBackup reputation, makes for an ideal solution for customers seeking an easy-to-deploy, flexible, scalable, and secure data protection environment.

References

NetBackup and Veritas Appliances Hardening Guide

Veritas Flex Appliance Getting Started and Administration Guide

VERITAS

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

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

V1108 12/23