VERITAS

NetBackup Flex Appliance Security

Elevated ransomware and data protection

Introduction

Data security is as important and paramount as data availability. The 2024 SonicWall Cyber Threat Report shows 6.06 billion malware (11% year-over-year increase) and 317.6 million ransomware attacks (36% year-over-year decrease) in 2023. Cryptojacking attacks grew by 659% over 2022 reaching 1.06 billion. 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 multimillion 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 cyber criminals.

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 data protection environment against ransomware, cryptojacking and intrusion attacks.

Flex Appliance Security

Overview

Zero trust security model or architecture which is based on "never trust, always verify" principle has been the primary design guideline for Flex appliances from the 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. Zero trust model is instantiated on Flex appliances on multiple levels starting at restraining system access and ending with blocking access to the data destructive operations.

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

- Restricting system access
- Preventing unauthorized user login
- Limiting user and process permissions
- Restricting access to destructive 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 instance, if a bad actor gains system access because of 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 preventing cybercriminal from logging in.

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

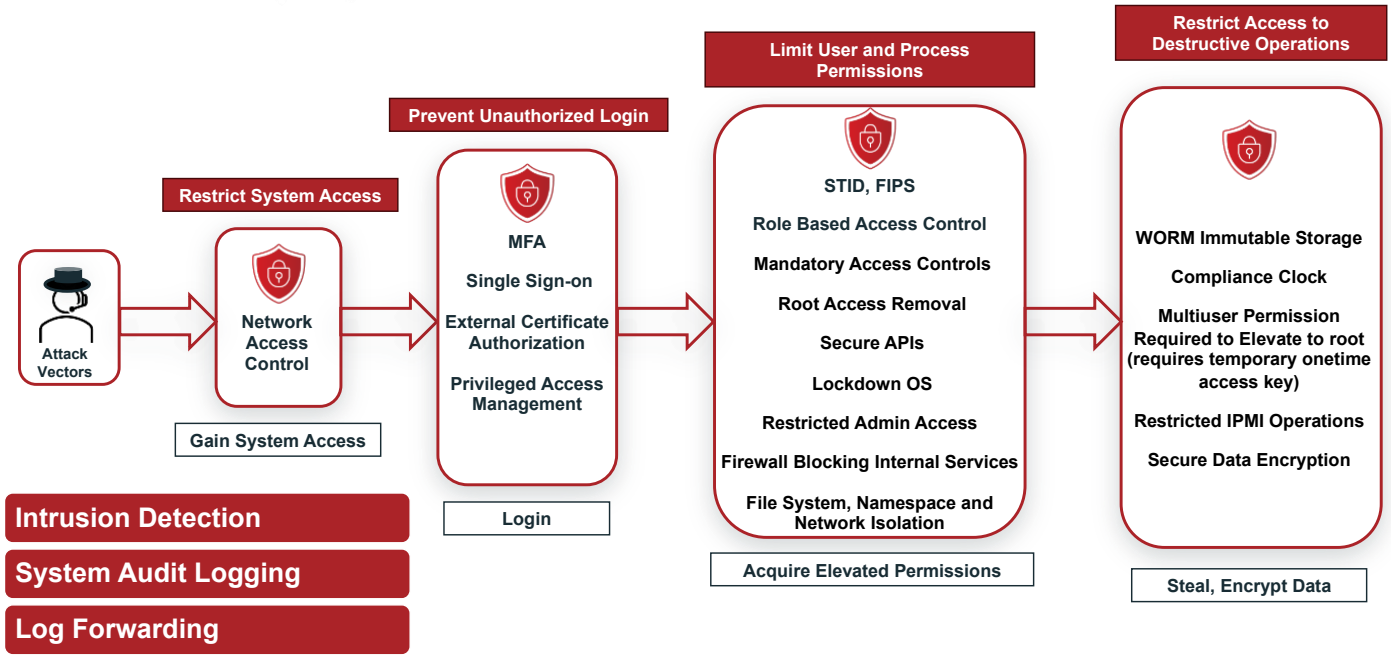

Figure 1. Flex Appliance Security Barriers

Restricting System Access

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

- **Network Access Controls**
  Administrator 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 defined in network access control list are automatically rejected. For increased security the default SSH port 22 can be also modified.

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. Once enforced, 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 appliance uses self-signed certificate. Users may be able to gain appliance access by importing X.509 certificate issued by 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 provider.

- **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.

Limit User and Process Permissions

If bad actors manage to successfully gain access and login to the appliance, additional restrictions implemented and compliance with well-defined security standards provide additional 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, configuration changes
  - Auditing enabled for low-level operations such as operating system commands and system calls
  - Ctrl-Alt-Del reboot disabled
  - SSH root login disabled
  - Interactive/login session idle timeout
  - 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 your own 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 NetBackup container conform to FIPS 140-2. Flex also takes advantage of the SELinux (Security Enhanced Linux) framework to create and enable proprietary security policies that conform with STIG guidelines to further harden the operating system from malicious attacks.

- **Role Based Access Control**

  Role Based Access Control (RBAC) is a security control mechanism where system and resource access are managed based on roles. Beginning with Flex 5 there are four basic roles: Super administrator, Administrator, Security administrator and Observer. The Super administrator role is assigned to the default user admin. This role and user cannot be changed and deleted. The user with Administrator role can manage appliance and application instances. User with Security administrator role is able to manage appliance security aspects such as local user accounts and roles. The Observer is a read only role assigned by default to all newly created users. The user with the Observer role can be promoted to Security administrator, Administrator or both Administrator and Security administrator roles. Furthermore, three new extended roles have been also introduced: application operator, security observer and support. The extended roles add greater flexibility in user account management. Application operator role, which can be assigned only to the user with Observer role, allows application instances to be stopped, started and relocated. Security observer appends Administrator as well as the Observer role with the option to view the security appliance's security information. The Support role allows management of diagnostic data such as appliance logs. This role can be also assigned to the Security administrator and Observer roles.

Mandatory Access Controls

Mandatory Access Controls constrain 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. Flex operating system explicitly denies access to all resources and only programs and activities specifically requiring resource access are granted the right to use them regardless of their system privileges.

- **Root Access Removal**

  Linux security model allows root to bypass security checks however, the Flex appliance eliminates console root account access. Only the hostadmin user is allowed to login via SSH to the compute nodes.

- **Secure APIs**

  Veritas provides a set of secure rest API calls to programmatically manage and monitor the appliance. API access tokens are required for appliance access. Administrator (admin) can generate Metrics token for the third-party analytics application and 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 X-AUTH-TOKEN for any management tasks. Additionally, Flex 5 customers have an option to convert any local user account to a service account. The service account is not allowed to connect to the appliance using Web UI, only REST API login and management calls are permitted. When user account is changed to a service account, the maximum time-to-live (TTL) for an associated API token must be defined. The service account inherits all the privileges of the original user account. When service account is utilized for appliance login, the TTL for a requested X-AUTH-TOKEN needs to be defined and be less than maximum TTL specified during the account conversion process. The service account API token is not revocable. Also, starting with Flex 5, customers can create a personal API token associated with any local user account. Similarly to the service account token, personal token inherits all the associated account privileges but unlike the service account token, login API is not required. Personal token's TTL can be decreased, increased and the token can be revoked. API executions are logged.

- **Lockdown Operating System**

  Flex appliance can lockdown the operating system. Once the operating system is locked down, modifications to Veritas Flex operating system including operating system services, network and device drivers are not permitted. The lockdown mode prevents unauthorized changes even in situation when appliance authorization has been compromised (stolen credentials). For the emergency operations one time password is required which can be obtained through Secure Quorum portal to unlock the appliance.

- **Restricted Admin Access/One Time Password**

  When in lockdown mode the user admin (Super administrator) has also restricted access which does not allow operating system and volume modifications including deletion, mounting and unmounting. Installation and uninstallation of software packages is also forbidden. In cases when restricted actions are required multi person authorization is necessary where one time password is generated for access to the appliance. Additionally, appliance hostadmin and application appadmin users are forced to change the default password upon the first successful login.

- **Firewall Blocking Internal Services**

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

- **Container Namespace Isolation and Service Privilege Limitations**

  Flex appliances feature highly secure, hardened Linux based VxOS which serves as a hosting platform for containerized services such as NetBackup, appliance management, and metrics collection time series database

among others. Containers are inherently more secure than traditionally executed application 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 which can access only their own discrete resources. Moreover, NetBackup services are also separated from the backup images stored in Write Once Read Many (WORM) storage.

Containers are also assigned limited-service privileges to define intra container executable 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. Additionally, entry to hardware-based utilities is also protected. Different lockdown modes and corresponding restrictions are described below.

- **Lockdown Mode**

  Flex appliance lockdown mode offers additional security levels to protect your appliance and data and it is a core component of the appliance's immutable architecture. Lockdown mode sets appliance into a heightened security level to protect data and storage infrastructure. When in lockdown mode administrators cannot make changes to the operating system and the internal components.

  

  Write Once Read Many (WORM) storage instances can be created only in enterprise and compliance lockdown modes. Any data written to WORM storage is immutable which means 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 the 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.

- **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 independent of the operating system time and the Network Time Protocol (NTP) is a function of compliance clock. Compliance clock is tampered proof and even the NetBackup administrator does not have right to modify it.

- **Multiuser Permission Required to Elevate to root**

  Before root access is granted to the shell a separate password from a different, appliance external user is required.

- **Secure Data Encryption**

  Data selected for backup, restore and duplication and corresponding metadata are encrypted over 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.

- **File System Isolation**

Access to the root filesystem is restricted to read only operations even for admin account to prevent accidental or malicious damages. Host level services are also blocked from accessing the container file systems. Additionally, dedicated files system mounted with security context are available for container exclusive access where file system sharing is not permitted making each file system to be visible and accessible only by a single, specific container.

Intrusion Detection

The Intrusion detection analyzes system and network activity and logs for any unauthorized access attempts. The system keeps track of file systems and generates alerts if any new software is deployed or if any changes are made to the file system containing the operating system. This feature provides enhanced visibility into important user or system actions to ensure a valid and complete audit trail that addresses compliance regulations such as Payment Card Industry as a compensating control.

System Audit Logging

Flex appliances monitor and analyze system events. All the CLI commands, API executions are logged in a separate file and forwarded to syslog for possible security incident investigation. Appliance system and audit logs can be forwarded to an external log management server and third-party plug-ins and add-ons such as Splunk are supported. For improved security TLS log transmission can be enabled.

Log Forwarding

Appliance and NetBackup instance logs can be forwarded to a syslog server. To simplify log analysis and to provide better user behavior analytics, plugins for the popular Security Information and Event Management (SIEM) applications such as Splunk and Securonix are also available.

Security Meter

To simplify the process of securing the platform, appliances include Security Meter which is a tachometer style widget. The Security Meter evaluates 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.

Conclusion

Veritas invests significant research and engineering resources in development of Flex appliances to deliver stable, reliable and highly secure data protection solution. With each product release and regular product updates the new security features are added and existing ones are enhanced to lower the risk against current and future threats. This highly secure

platform combined with the unbeatable NetBackup reputation makes an ideal solution for customers seeking easy to deploy, flexible, scalable and well protected data backup environment.

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 veritas.com. Follow us on Twitter at @veritastechllc.

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

For specific country offices
and contact numbers,
please visit our website.