Seven Simple Steps to Improve your NetBackup and NetBackup Appliances Security Posture

Introduction

Veritas NetBackup and NetBackup Appliances bring together the power of NetBackup software with state-of-the-art servers and storage technology to enable our customers to deploy enterprise-class data protection with enhanced ransomware-resiliency.

Ransomware attacks are on the rise. Our intelligence channels increasingly show that attackers are using stolen credentials to gain unauthorized access to backup software and appliances. The likelihood of a successful attack increases dramatically due to the use of out-of-date software, poor password management practices, generic user ID's and/or not enabling Multi-Factor Authentication.

We highly recommend that our customers take immediate action to bolster their cybersecurity defenses by taking advantage of many of the security features in our products, including Multi-Factor Authentication (MFA), Lockdown Mode, and immutability.

Do not put your critical backup data at risk. Veritas strongly recommends that you take the time to review and secure your data protection infrastructure. These Seven Simple Steps should help to improve your NetBackup and NetBackup Appliances security posture.

Seven Simple Steps

1. Enable Multi-Factor Authentication

MFA is a system utilizing at least a second source of added verification to gain access to a resource. We utilize it today for many things, like logging into a bank account or VPN access. Enabling Multi-Factor Authentication allows you to align with your existing Identity and Access Management (AIM) policies.

How to enable MFA with your single sign-on

- NetBackup Flex Appliance
- Veritas NetBackup Appliance
- Managing user authentication with smart cards
- Application - Enable MFA using any SAML2.0 compliant Identity Provider
- Application - Smart card or digital certificate
- Application Access Management - Implement least privileges model using Role-Based Access Control (RBAC)

2. Elevate Veritas Appliance Security Level with Lockdown Mode

Veritas Appliances offer a hardened, secure operating environment right out of the box. In addition, Veritas Appliances also offer an added protection, Lockdown Mode, to prevent unauthorized access or modification to the underlying Operating System. Once Lockdown Mode is enabled, Administrators cannot make changes to the Operating System (OS) and internal components. Access to the OS for emergency operations will require quorum approval – meaning your NetBackup administrator and Veritas must agree. If a change is needed, you will need to contact Veritas support to obtain a one-time password to unlock your Veritas Appliance. This prevents unauthorized changes even if credentials were stolen by a malicious actor and Multi-Factor Authentication (MFA) was bypassed.

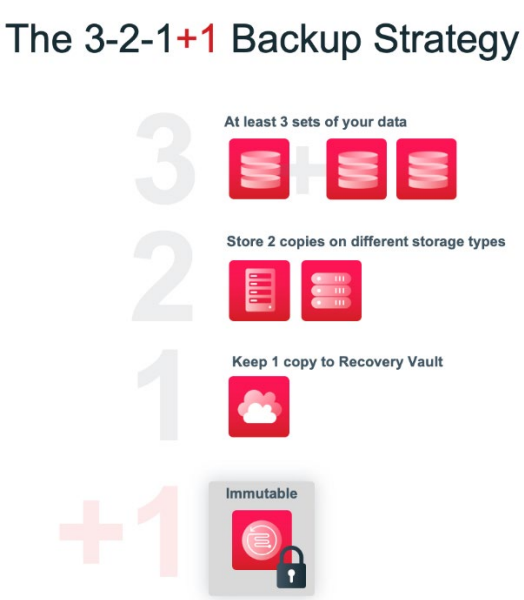
How to enable lockdown mode

- NetBackup Flex Appliance
- NetBackup Appliance
- NetBackup Flex Scale
- NetBackup Access Appliance

Access codes enable non-RBAC users to administer NetBackup operations using CLI.

3. Implement an Immutable Data Vault to Secure Data

One of the best ways to safeguard your data is to implement immutable and indelible storage, ensuring that data cannot be changed, encrypted, or deleted for a determined length of time (or at all). NetBackup Flex Appliances, NetBackup Flex Scale and NetBackup Access Appliances provide secure and tamper-resistant immutable and indelible storage, preventing data backups from being tampered with or from unauthorized access, which is vital to an effective and rapid recovery strategy. Veritas also offers the ability to immutably store data in the cloud on object storage, including our own Alta Recovery Vault and with 3rd party Open Storage Technology (OST) vendors.



Veritas recommends a new strategy for backups. In the past we recommended a 3-2-1 strategy: three copies of data, two on site on different media, and one copy offsite. The current rise in cyber threats today calls for adding an extra "1" creating a 3-2-1+1 strategy; three copies of data, two on site on different media, one copy offsite and one copy that is immutable.

Veritas Alta Recovery Vault also creates a separation of duties where the administration of the storage is managed by Veritas, providing you another layer of isolation from attack.

4. Secure Credentials with Privileged Access Management

We highlighted poor credential management practices above. Don't re-use, don't share, don't keep a file filled with passwords on any systems. It's unacceptable and it creates security, auditability, and compliance issues.

Veritas NetBackup and NetBackup Flex Appliances support external password management solutions. For example, you can deploy CyberArk Privileged Access Management (PAM) solutions to enforce password rotation policy and monitor all activity in privileged sessions. The Veritas NetBackup Appliance and NetBackup Flex Appliance plugins can be downloaded from CyberArk Marketplace.

5. Reduce Network Exposure by Implementing Network Access Controls

Network access control can ensure that only properly authorized personnel can access selected networks or network segments to access backup administrative interfaces. As an example, you can control which IP address or subnet can access NetBackup Flex Appliances via SSH and HTTPs with an allow list. All IP addresses not on the allow list are blocked by default. This is an example of network segmentation. Implement network access control today to prevent attackers from gaining system access.

Another way to isolate and protect backups is by creating an Isolated Recovery Environment (IRE). NetBackup and NetBackup Flex Appliances includes a simple, turnkey, pull-based IRE which creates a network isolated or air-gapped recovery environment. This allows you to create a vault for your data. Additionally, the proprietary

compliance secure clock provides added confidence that your storage is never subject to time-based attacks meant to expire data prematurely.

How to implement Network Access Controls

- NetBackup Flex Appliance
- NetBackup Appliance
- NetBackup Isolated Recovery Environment

6. Keep All Systems and Software Updated

Veritas has delivered many new security features in the last few years specifically to protect your data and ensure that only properly authorized personnel have access to critical systems. Examples include next generation Cyber resilience data protection platforms like NetBackup Flex Appliance, NetBackup Flex Scale, Multi-Factor Authentication, Immutability, built-in Isolated Recovery configurations, built-in malware scanning & anomaly detection, new simpler role-based access controls, SIEM/SOAR integrations, to name a few examples. If you are running out-of-date software, you can't take advantage of these important new capabilities. In addition to enhanced security features, we also release security updates on a regular basis which fix critical issues. If you aren't taking advantage of new functionality and the security updates your data could be at risk. Build a strategy to stay current and upgrade now - it's one of the best ways to safeguard your data.

Don't fight today's cyber threats with yesterday's technology or software!

Links to the latest software releases

- Veritas Download Center
- NetBackup Automated Upgrades

Register with Veritas NetInsights Console to receive proactive recommendations on product upgrades, security patches, hotfixes and maintenance releases.

7. Enable Encryption

We recommend enabling encryption at-rest and in-transit. Encryption prevents unauthorized data access and theft. If the backup data is encrypted using robust industry standards, even if data is stolen, attackers can't access it.

Use NetBackup's built-in capabilities to configure strong encryption everywhere both on-premises and in the cloud. You can use either the built in NetBackup key manager service (KMS) or configure NetBackup with a third party KMS through the NetBackup

administration console or the NetBackup command line during storage server configuration. Reduce your risk of data theft, exfiltration, and unauthorized access with strong encryption.

How to enable encryption

- NetBackup Flex Appliance
- NetBackup Flex Scale
- NetBackup Appliance
- NetBackup Security and Encryption Guide