VERITAS

NetBackup™ Flex Scale Secure by Default

Providing the building blocks for ransomware protection.

White Paper | March 2024

Contents

Executive Summary . . . 3

Secure by Default . . . 4

- Network Access Controls . . . 4
- Container Isolation . . . 4
- Hardened Operating System (OS) . . . 5
  - Mandatory Access Control . . . 5
  - Intrusion Detection and Prevention . . . 5
  - Security Technical Implementation Guide . . . 5
  - Continuous Security Scanning . . . 6

Write Once, Read Many (WORM) Storage . . . 7

- Lockdown Mode . . . 7

Air Gap . . . 9

Zero Trust . . . 9

- Superuser Rights Removal . . . 9
- Restricted Admin Access . . . 9
- Restricted Access to Remote Management Platform . . . 9
- Authentication Methods . . . 10
- Multi-factor Authentication . . . 10
- Single Sign-on (SSO) . . . 10
- Privileged Access Management . . . 10
- Appliance Software Lockdown . . . 10
- Internal Firewall . . . 10
- Encryption . . . 10
- External Certificate Authorization . . . 10
- Customizable Login Banner . . . 11

Compliance . . . 11

Summary . . . 11

Executive Summary

With ransomware attacks occurring at an alarming rate and demands becoming outrageous, it's no surprise that securing data is top of mind for all companies. When the first known ransomware attack happened back in 1989 the demands were minimal, and if you paid, your data was restored. Nowadays, the demands are increasingly excessive and there is no guarantee you'll get your data back intact. According to Cybersecurity Ventures, by 2031, a business will fall victim to a ransomware attack every two seconds, and those attacks will cost victims more than $265 billion annually, making ransomware the fastest-growing type of cybercrime. Your last line of defense is being able to quickly restore your data to the way it was prior to the attack. This requirement makes protecting your backup data, and ensuring your backup infrastructure is highly secure, even more critical.

People often believe that storing backup data on immutable write once, read many (WORM) storage is all that's needed, but that's only part of the solution. Unfortunately, there is no silver bullet to protect your data because there are many attack vectors cyber criminals use to wreak havoc on your systems, including server IPMI, application and system APIs and GUIs, filesystems, and operating systems. For each of these attack vectors, you need to be able to prevent system access and unauthorized logins, ensure that you limit user and process permissions, and restrict access to destructive operations. Building your own secure infrastructure is extremely challenging to set up, and even harder to maintain as newer vulnerabilities are identified. The easiest way to get the most secure backup infrastructure is with Veritas appliances, including NetBackup Flex Scale, which delivers security by default, with an architecture that provides enterprise scalability with both immutability and indelibility. It was designed from its inception with the zero trust security model, which is based on the never trust, always verify principle. With its zero trust architecture, 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 Scale 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.

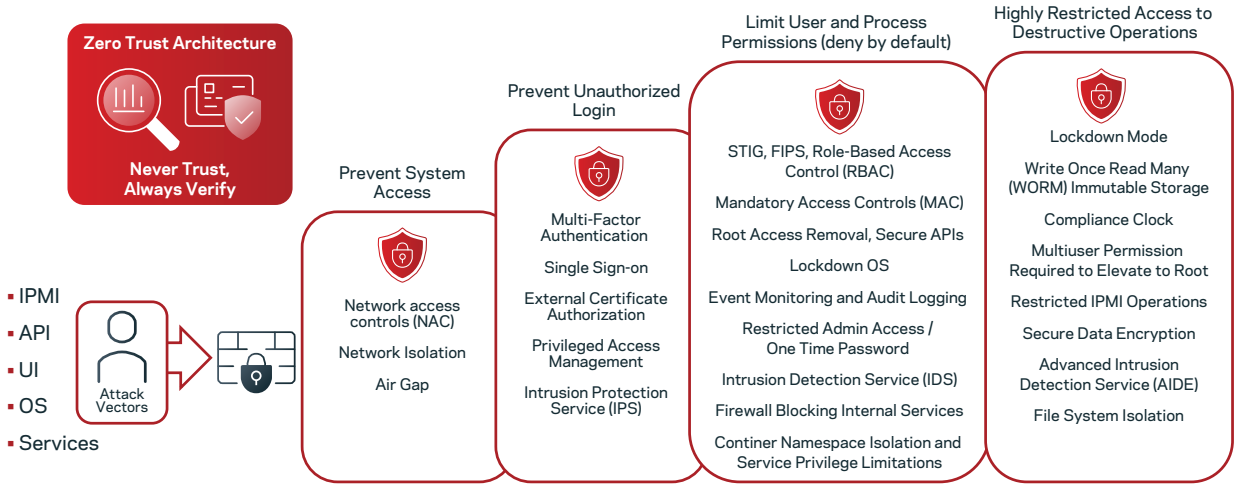


Figure 1. NetBackup Flex Scale's zero trust model, providing multiple layers of protection from ransomware attacks

Secure by Default

The NetBackup Flex Scale architecture was built with security as its primary objective. It uses containers to provide service isolation, a hardened OS, and a zero trust security model. There are many layers required to provide a zero trust architecture, including access controls that limit or remove root access to users and services, secure communication including management controls, and enhanced data infrastructure security. Let's get into each of these in more detail.

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.

Container Isolation

One of the key design choices needed to build the most secure immutable architecture to protect backup data from a ransomware attack is to containerize the software. This approach is inherently more secure due to the isolated nature of container resource allocation and namespaces, and their logically separated configurations. Starting a container-based service is subject to security constraints and checks: Rather than being read and executed from a node's operating system files, a container's contents are bundled together in binary form and a checksum comparison is carried out before execution to ensure program contents are immutable. In NetBackup Flex Scale, all NetBackup services run in different containers. This design provides many layers of additional security, including:

- **Separation of backup images from NetBackup services**: Removes the NetBackup admin's ability to delete images stored in WORM storage (see the lockdown section for details on when deletion is possible).
- **Namespace isolation**: Ensures processes only have access to their own discrete set of resources.
- **Limited-service privileges per container**: Defines which system calls a container can run and grants control on what runs inside the container, eliminating the need for elevated system privileges.
- **Network isolation**: All NetBackup services running on Flex Scale, 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.
- **Blocking host network sharing with containers**: Ensures that anyone able to access the host network won't be able to see communications between services.
- **Preventing access to container file systems:** Keeps host-level services such as the web UI from accessing container file systems.
- **Dedicated file systems mounted with security context for exclusive access to each container**: Blocks container file system sharing, allowing each file system to only be visible from and accessible to one specific container.
- **Isolation of container file systems to necessary services**: Limits other services within a container from seeing and accessing container file systems they are not specifically assigned. For example, there is a secure dedupe (MSDP) data store that eliminates users and NetBackup processes from accessing the MSDP data store where the backup images lie. It works by the dedupe filesystem only being visible to the dedupe (MSDP) service, but it is hidden from file system services such as CIFS and NFS that are used for Instant Access and Universal Shares, even though they run from the same container (see Figure 2).

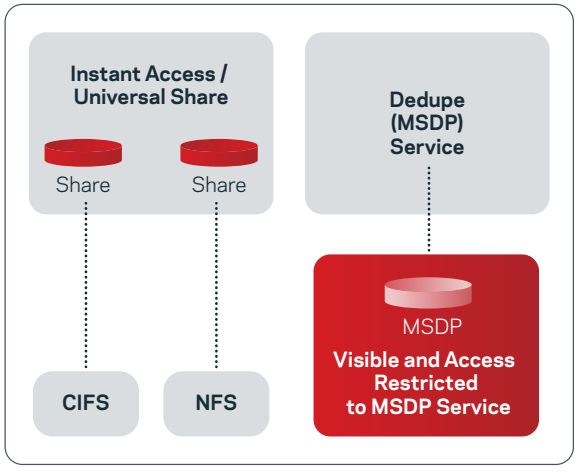


Figure 2. An overview of container file system isolation in NetBackup Flex Scale

Hardened Operating System (OS)

NetBackup Flex Scale includes a customized version of Linux OS called VxOS that removes all unnecessary services and software packages to eliminate the ones that could potentially result in vulnerabilities. The VxOS kernel provides namespaces, control groups, and secure computing mode to control processes and resources at the operating system (OS) level. NetBackup Flex Scale uses these features to control access and manage resources.

The NetBackup containers, OS, and platform software meet stringent security standards and are Federal Information Processing Standard (FIPS) 140-2–compliant. NetBackup Flex Scale also uses the security framework within Linux, SELinux, to create and enable proprietary security policies that conform with STIG guidelines (DISA RHEL7 profile) to further harden the OS from malicious attacks. For example, it removes admin access to superusers, and includes an internal software firewall that blocks external access to internal services.

Mandatory Access Control

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. Doing so could cause serious security issues on systems. Instead, NetBackup Flex Scale explicitly denies access by default to all resources and tightly limits data access to only those programs and activities that need access, regardless of their system privileges.

NetBackup Flex Scale works by using SELinux labels that view each object on the system — every file, directory, socket file, symlink, shared memory, semaphore, or FIFO file — and every subject, running process or Linux user entity — with an SELinux label. It uses these labels to specifically assign access permissions for individual resources to each service.

Intrusion Detection and Prevention

NetBackup Flex Scale 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).

In essence, the IDS sandboxes applications, restricting each to access only to processes and resources specifically assigned to them. As part of STIG rules, it also has AIDE, which 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 OS. 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 PCI as a compensating control.

The IPS analyzes system and network activity, and logs any unauthorized access attempts.

Security Technical Implementation Guide

Security Technical Implementation Guides (STIGs) are a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security. NetBackup Flex Scale uses the STIG template to meet security requirements per the Defense Information Systems Agency (DISA) profile.

Some examples NetBackup Flex Scale implemented for OS hardening with the DISA STIG include:

- Auditing enabled for low-level operations such as OS commands and system calls
- SSH root login disabled
- Interactive/login session idle timeout
- Forced password changes during initial configuration, ensuring the default password does not remain active on the system
- Logging of incorrect login attempts

- Customizable password policies: The ability to set your own password policy, including the option to use STIGs for validation. For example, the admin can set the password complexity, age, password lockout, and login-retry enforcement policy with or without STIG being enabled.
- Audit logging of cluster and appliance events — operations that are initiated by users — such as login, add node, and configuration changes. These logs are rotated daily and retained for 90 days.
- You can forward system logs, which contain event and notification messages, from a NetBackup Flex Scale cluster to an external log management server. Forwarding the appliance syslogs to an external log management server provides system administrators a centralized location for viewing logs, and for further analysis and troubleshooting.

Continuous Security Scanning

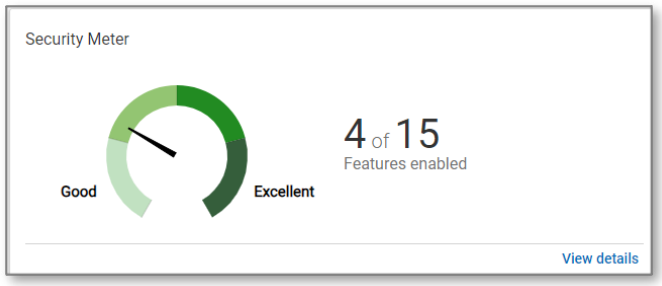
As part of product development, each element of the appliance, including its Linux OS, drivers, appliance software, patches, and the core NetBackup application is continuously tested for vulnerabilities using industry-standard advanced security products such as Tenable, Qualys, Black Duck, and OpenSCAP. External penetration (PEN) testing is also performed regularly.

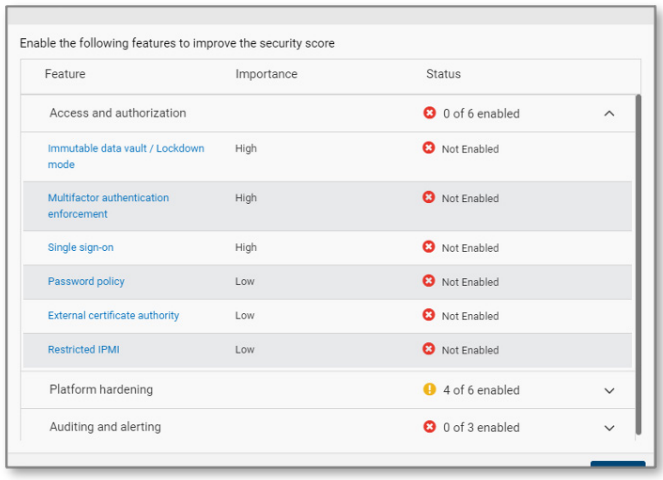
Security Updates

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, NetBackup Flex Scale 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 easily be changed. The Security Meter is available only to a user with the *Appliance* administrator role.





Write Once, Read Many (WORM) Storage

NetBackup Flex Scale includes WORM storage that provides immutable and indelible data protection, ensuring data cannot be changed for a determined length of time to protect data against cybercriminal intrusion and internal threats. Any data saved on WORM storage is protected with the following security measures:

- **Immutability**: Ensures the backup image is read-only and cannot be modified, corrupted, or encrypted after backup.
- **Indelibility**: Protects the backup image from being deleted before it expires. The data is protected from malicious deletion.

WORM storage also works with Instant Access and Universal Shares.

Lockdown Mode

Immutability support for backup images requires locking down the appliance and disallowing any operations that could lead to data destruction. Lockdown mode is a core component of NetBackup Flex Scale's immutable architecture, and it means that in addition to being able to provision WORM-based storage, the appliances hosting this storage in their distributed cluster move into a heightened security level to protect data and storage infrastructure. When the appliance is placed in lockdown mode:

- Administrators are prevented from making any changes to the OS and the internal components
- All the external endpoints are secured from unauthorized access, protecting your cluster data from internal and external threats
- Access to all services is protected and authenticated
- Data is protected from being encrypted, modified, and deleted using WORM properties
- Appliance administrators can choose to prohibit disruptive operations via the HP iLO

NetBackup Flex Scale supports three lockdown modes, each providing a different level of granularity for WORM and retention: Normal Mode, Enterprise Mode, and Compliance Mode (see Figure 3). Normal Mode disables WORM and retention capabilities. To configure WORM storage and retention capabilities a user with the appliance admin role must enable either Enterprise or Compliance lockdown mode for the cluster either during initial config or after. The differences are:

- **Enterprise Mode** images stored in a WORM-enabled storage unit can be deleted prior to expiration; however, it involves a two-step, two-persona action.
    1. Users with the **appliance admin role** can remove the retention lock on an image-by-image basis using the MSDP restricted shell, then
    2. Users with the **backup admin role** can expire the unlocked images.
- In **Compliance Mode**, images stored in the WORM-enabled storage unit can't be deleted early.

Properties	Standard Protection	Immutable Protection	
	◉ Normal	○ Enterprise*	○ Compliance*
Immutable data support with retention locking	X	✓	✓
Deletion of immutable data before expiry by the Backup Administrator	✓	X	X
Backup image retention lock deletion	—	✓	X
Access to Remote Management Platform	✓	X	X
Appliance Administrator access to node operating system	✓	X	X
Appliance immutablility mode upgrade	✓	✓	—
Appliance immutablility mode downgrade	—	X	X
Retention lock extension	—	✓	✓

Figure 3. An overview of the three lockdown modes in NetBackup Flex Scale

*Exclusions may apply. refer to documentation here

Once a cluster has entered lockdown mode, it cannot be exited as long as data is stored with an active retention period, nor can the lockdown mode be changed from Compliance lockdown mode to the less-restrictive Enterprise version.

However, users with the appliance admin role can increase the mode; supported changes include:

- Normal Mode to Enterprise Mode
- Normal Mode to Compliance Mode
- Enterprise Mode to Compliance Mode

Other security enhancements for a cluster when it is set to either Enterprise or Compliance mode include:

- Lockdown modes are retained during upgrades
- The cluster nodes are prevented from being factory reset
- Newly added or replacement nodes are automatically placed in the existing lockdown mode of the cluster

Figure 4 shows the WORM storage configuration in NetBackup Flex Scale.

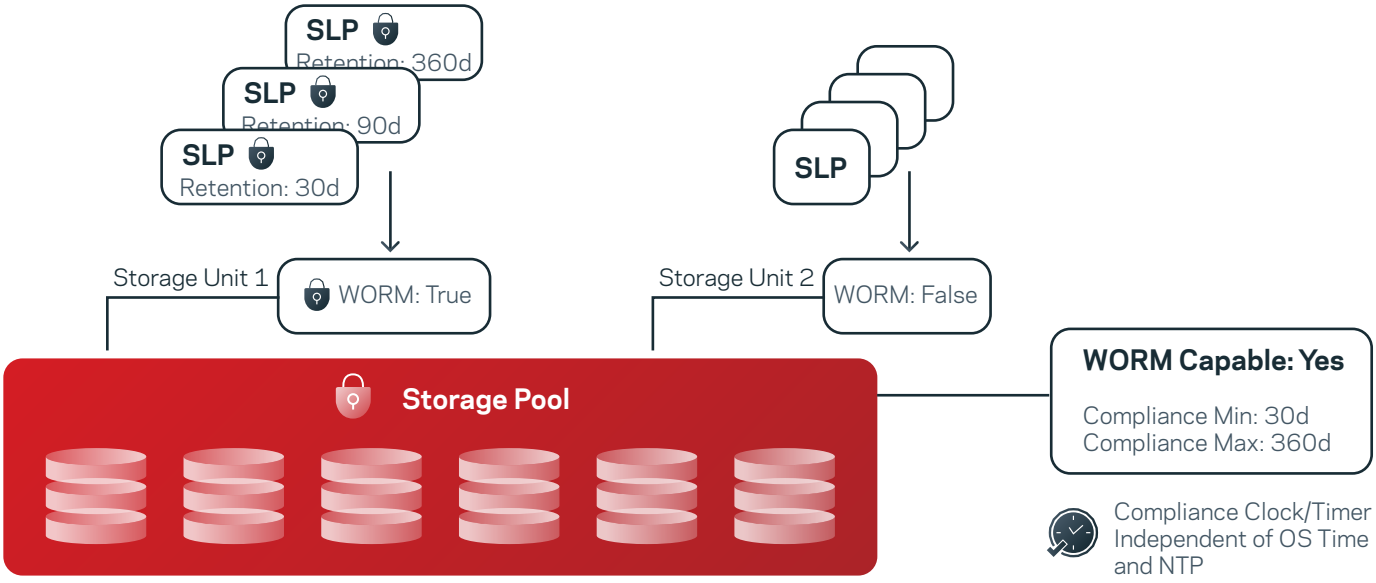


Figure 4. The WORM storage configuration in NetBackup Flex Scale

1. The disks inside the nodes are automatically configured in a single storage pool that can be configured to be WORM-capable by selecting a lockdown mode. If lockdown is selected, the admin sets a compliance minimum and maximum duration for data retention of between one hour and 60 years. The appliance admin can change this setting at any time, but it will only affect future backup images. Any changes to compliance mode or duration will generate an event and be logged.
2. The storage pool is automatically presented to NetBackup with a single storage unit. After the admin enables Enterprise or Compliance lockdown mode, this default storage unit is automatically enabled for WORM. If desired, the backup admin can configure additional storage unit(s); typically, admins add a storage unit with WORM set to False in addition to the default one that has WORM set to True.
3. Then, when you create backup policies or storage lifecycle policies (SLPs), you can select to have the data written to the appropriate storage unit. If you don't want to set a retention period on a particular backup policy, you send it to the storage unit with WORM set to False. If you want the data to be retained for a set retention period, then you configure the policy to write to the storage unit with WORM set to True. Each policy/SLP can have a different retention period, but it must fall within the compliance minimum and maximum range set at the storage pool layer.

Most important, there is a cluster-based immutable compliance clock/timer that is independent of OS time and the Network Time Protocol (NTP), and can't be tampered with by the appliance or the NetBackup admin. This compliance clock is used to determine whether a retention period on backup data has actually expired or not, thus ensuring the data written to WORM storage is retained for the proper duration and isn't affected if an attacker or ransomware tries to modify the system or NTP time. The compliance clock/timer is implemented at the cluster level and instantiated by the filesystem layer.

NetBackup provides backup image management with a visual representation of the immutable lock and image deletion after the WORM retention period.

Air Gap

One of the security features of NetBackup is its ability to maintain an isolated copy of backup data, referred to as a virtual air-gapped copy. This air-gapped copy is in an isolated recovery environment (IRE) that is created on a WORM storage device. The network access to data in an IRE is available only during the replication window, otherwise the air-gapped copy is protected against malware and ransomware attacks. Unlike traditional push replication methods, NetBackup Flex Scale works by utilizing a pull model which means the replication request comes from the IRE during an admin-specified replication window. By empowering the IRE destination environment to request the data from the source environment — by invitation only — we can support 24x7 data movement while isolating the stored data from any potential threats.

You can deploy the tertiary copy of the backup images behind a firewall to an isolated environment without opening any inbound firewall ports to NetBackup. This keeps the environment secure, allowing a sandbox approach to perform malware scans or test recovery procedures before recovering at a larger scale. Optionally, you can add a physical air gap as an additional layer of protection.

Zero Trust

The zero trust architecture model means that NetBackup Flex Scale is designed to inherently trust no person, service, or process. This model ensures there is no implicit trust granted to users or resources. By default, NetBackup Flex Scale assigns the least privileges possible, thereby minimizing the impact of a breach. For example, if a malicious user were able to gain access to the system using admin credentials, because of the zero trust architectural design implemented in NetBackup Flex Scale, they can only see the infrastructure details, but not cause any harm such as encrypting or deleting data, wiping a system, or changing a config. There are many design elements that are included in the zero trust design. In addition to the inherent network segregation between applications — NetBackup and appliance software — plus the container isolation and hardened OS attributes previously mentioned, NetBackup Flex Scale also includes the following enhancements to align with the zero trust security model.

Superuser Rights Removal

Superuser rights have been removed, ensuring users and appliance services have limited permissions. Unlimited privileges are not granted.

Restricted Admin Access

Restricted admin access limits what access administrators have, including removing admin access to the OS and preventing them access to make system changes such as deleting volumes. Any access to superuser-level appliance commands requires dual authentication and participation from the system admin and Veritas support, thus ensuring system-level activities are closely supervised.

Restricted Access to Remote Management Platform

Appliance administrators can choose to restrict access to destructive operations via the remote management platform — HPE ILO — when either Enterprise or Compliance lockdown mode is selected. This feature adds an additional level of data security and limits the privileges and operations that can be done remotely. Once this is enabled, a sysadmin user with the IPMI role will only be allowed to log in to the iLO, view settings, and perform power-related operations. Physical access to the system will be required to log in to the console. This is a critical security feature to prevent anyone from remotely changing the boot device and gaining access to the underlying OS and data, or wiping and repartitioning the disks from the remote management interfaces/Intelligent Platform Management Interface (IPMI).

Authentication Methods

NetBackup Flex Scale supports single sign-on and multi-factor authentication (MFA) for an additional layer of security to the authentication process used to log in for local and domain users.

Multi-factor Authentication

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

Single Sign-on (SSO)

SSO is supported for any SAML 2.0 compliant identity providers.

External Password Management

NetBackup Flex Scale supports external password management, such as CyberArk Privileged Access Management, to enforce password rotation policy and privileged session activity and monitoring.

Appliance Software Lockdown

All appliance software is signed and installed at the factory; any new additions must contain Veritas signatures.

Internal Firewall

NetBackup Flex Scale includes an internal firewall that only exposes backup and management ports required by NetBackup admins. All other internal services are blocked.

Encryption

NetBackup Flex Scale includes in-flight and at-rest encryption. Management access — web UI, SSH shell, and REST APIs — are encrypted using TLS 1.2 and 2048 bit+. The backups are stored on disk using AES 256-bit encryption.

External Certificate Authorization

NetBackup Flex Scale provides the flexibility to use internal certificates or certificates from an external certificate authority (ECA). The ECA can be uploaded and validated using the NetBackup Flex Scale web UI. To make it simple to manage with the ECA, the entire cluster and all its components are represented with one certificate, meaning once you deploy the external certificate, all NetBackup Flex Scale components will use them, including the NetBackup services, management gateway, and web services.

Customizable Login Banner

If STIG is disabled, you can create a customized text banner that appears before a user signs in to the NetBackup Flex Scale web UI, system console, or NetBackup UI. 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. If STIG is enabled, then it sets its own login banner, which can't be modified.

Compliance

NetBackup Flex Scale's immutability solution has been assessed by the Cohasset Immutability assessment (in Compliance mode) and found to be compliant by third parties such as:

- 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)

Summary

NetBackup provides anomaly detection, policy-based image retention, and KMS encryption. Using NetBackup Flex Scale as the deployment option adds additional layers of infrastructure immutability and indelibility that are needed to provide ransomware protection. With integrated container isolation, a security-hardened OS, and a zero trust security model, NetBackup Flex Scale is a proven platform that helps prevent data loss due to malware infiltration and ransomware attacks, while allowing you to recover more efficiently.

To see some of these security features in action, watch this video.

VERITAS

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

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

V1517 03/24