VERITAS

The Fastest Way to Achieve Cyber-Resilient Data Protection

NetBackup™-Powered Appliances

NetBackup Flex Scale, Flex, and Access Appliances.

White Paper | July 2023

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 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 Sonicwall, in 2022 there were 15 ransomware attacks per second[1], and IBM reported that those attacks cost victims on average $4.35 million[2], making ransomware the fastest-growing type of cybercrime. Your last line of defense is being able to quickly restore your data from prior to the attack.

$4.35 MILLION

Average cost of a data breach.

Cyberattackers know this, so they target your backup systems. They try to gain access to your backup infrastructure and acquire administrative passwords, elevate credentials to gain access to your system shell or filesystem, look for security holes in software—anything that can give them access to your backup environment and remove your ability to recover. Attackers will try to gain access via APIs, the OS, and hardware consoles. This is why it is essential to protect your backup data and ensure your backup infrastructure is highly secure. That's why we designed NetBackup-powered appliances to be highly secure by default.

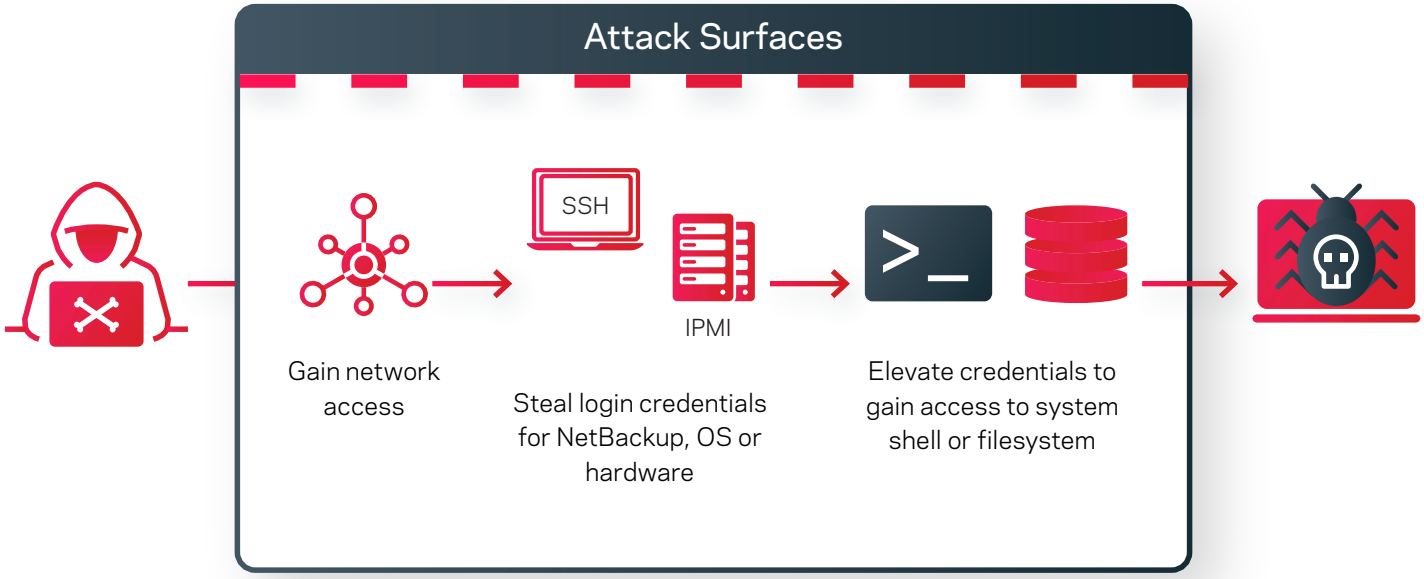


Figure 1. Attack surfaces a cyberattacker targets

The easiest way to get the most secure backup infrastructure is with NetBackup-powered appliances, including NetBackup Flex Scale, Flex Appliance, and Access Appliance.

NetBackup provides secure mechanisms to prevent unauthorized access, including:

- Data encryption
- Support for an external certificate authority
- Support for privileged access management
- Role-based access control (RBAC)
- Support for multi-factor authentication (MFA)

NetBackup safeguards against the malicious use of stolen user logins by eliminating operations requiring operating system administrator access, removing root permissions for executing binaries, and minimizing the number of required open network ports.

Malicious actors also target the backup infrastructure through the operating system, infrastructure management access points, and the system shell.

While protecting against stolen NetBackup credentials is crucial, it is important to remember that malicious actors do not stop there. They also target the backup infrastructure through the operating system, infrastructure management access points, and system shell. For instance, they may exploit the OS or remote console credentials to gain unauthorized access and potentially compromise your disks by formatting or encrypting them. That's why it is essential to implement additional layers of security for the servers, storage, services, and operating systems that run your data protection software.

To protect your infrastructure, people often believe that storing backups on immutable write once, read many (WORM) storage is all that's needed, but that's only part of the solution. There is no silver bullet to protect your data. Instead, there are several factors involved in protecting your backup data in addition to storing it on immutable WORM storage. These include encryption, firewalls, access controls, security scanning, and intrusion detection and protection to name a few, but these can be extremely challenging to set up and even harder to maintain.

NetBackup-powered appliances deliver security by default, with an architecture that provides enterprise scalability with immutable and indelible infrastructure security protection through:

- System hardening and a Zero Trust architecture
- Immutable and indelible storage with an integrated secure compliance timer
- Network isolation
- Container isolation

This architecture was designed specifically to secure data protection environments. It works against multiple attack vectors including:

- **Network:** Prevents network access to backup systems and provides an isolated environment that stores an additional backup copy of essential data.
- **Users:** Adds an extra layer of protection from password theft to prevent unauthorized login, which is the easiest method for attackers to gain access to a system.
- **Application and OS:** Strictly limits user and process permissions and isolates service access permissions so that even if an attacker is able to enter a system via a stolen password, they would have limited rights to any action.
- **Storage:** Highly restricts access to your filesystem and destructive operations.

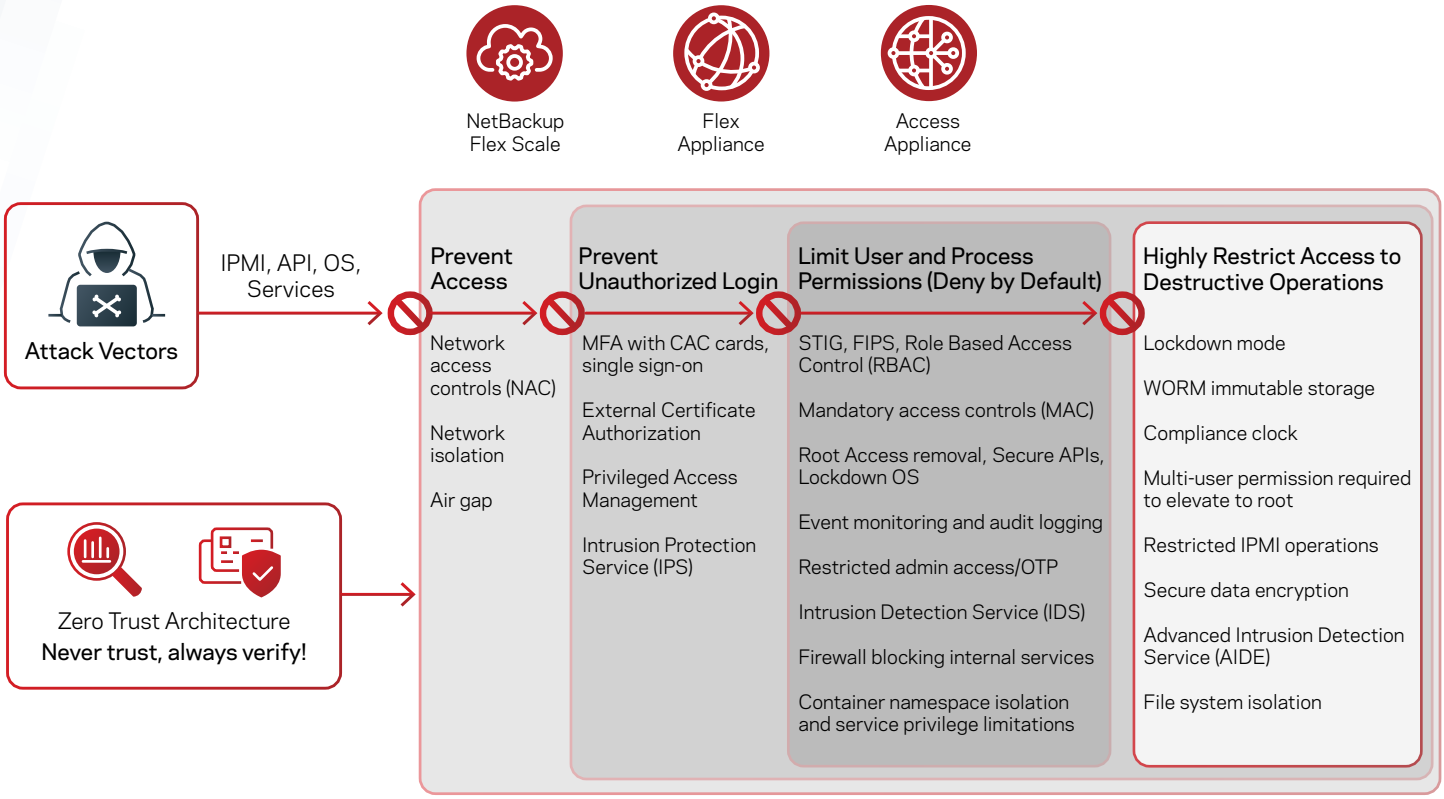


Figure 2. NetBackup-powered appliances protecting from multiple attack vectors

Prevent Access to the System

The best way to prevent a cyberattacker from compromising your backups is to prevent them from accessing the backup systems. NetBackup-powered appliances utilize containers that deliver network segregation between containers and the host, ensuring containers can't affect other containers if compromised. Additionally, Veritas recommends implementing network access controls and storing a secure air-gapped backup copy of your critical data in an isolated recovery environment.

Reduce Network Exposure by Implementing Network Access Controls

One way to prevent infection is to implement network access controls for your backup environment. You can control which IP address or subnet can access NetBackup-powered appliances via SSH and HTTPs with an allow list. All IP addresses not on the allow list are blocked by default.

Secure an Air-Gapped Copy of Critical Data in an Isolated Recovery Environment (IRE)

An IRE disables network connectivity to a secure copy of your backup data, providing administrators a clean set of files on demand to neutralize the impact from a ransomware attack. For more detail, please review the Veritas Isolated Recovery Environment white paper.

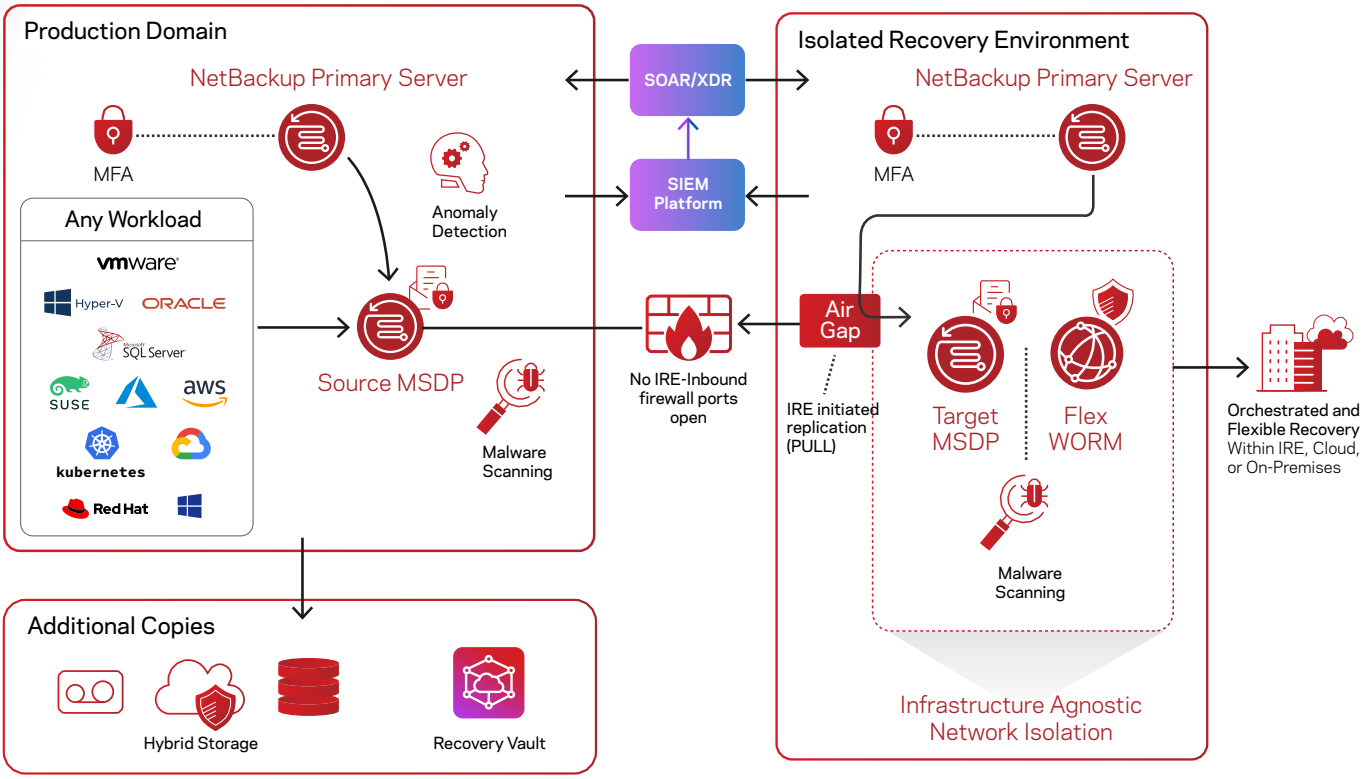


Figure 3. Isolated recovery environment (IRE)

Preventing Unauthorized Login

The most important thing to protect is your login credentials. These should always be highly secure passwords, unique to individuals, not accessible to others, and changed frequently. Unfortunately, IT administrators commonly share root, built-in accounts, and many other privileged credentials for convenience, so workloads and duties can be seamlessly shared as needed. However, this creates security, auditability, and compliance issues. External hackers covet privileged accounts and credentials, knowing that once obtained, they provide a fast track to an organization's most critical systems and sensitive data. Therefore, it is essential to not share or reuse credentials whenever possible.

NetBackup-powered appliances support multiple options to prevent unauthorized logins to the appliances, OS, and NetBackup service containers. These include secure login options, privileged access management, and intrusion protection services.

Secure Login Options

NetBackup-powered appliances support multiple authentication methods including single sign-on and multi-factor authentication with smart cards.

Privileged Access Management

To increase security on important NetBackup and appliance credentials, NetBackup-powered appliances support privileged access management services such as CyberArk. This helps to keep unauthorized users out, and detect and stop threats in real time. Check out this demo video to see how easy this integration is and how it works.

External Certificate Authorization

NetBackup-powered appliances provide the flexibility to use either internal certificates or certificates from an external certificate authority (ECA).

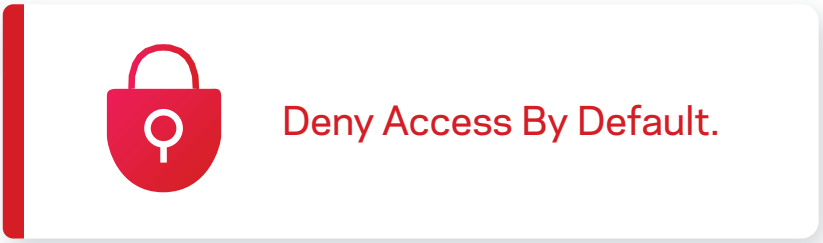
Intrusion Protection Service (IPS)

The integrated Intrusion Protection Service (IPS) analyzes system and network activity and logs any unauthorized access attempts.

Limiting User and Process Permissions

If a malicious actor were to gain access to administrative credentials, the NetBackup-powered appliances have multiple security features to limit the actions that can be performed.

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. Instead, NetBackup-powered appliances explicitly deny 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.

It 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.

Root Access Removal

Root access has 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 from being able to make system changes such as deleting volumes.

Secure APIs

NetBackup-powered servers authenticate incoming API requests based on a JSON Web Token (JWT) that needs to be provided in the Authorization HTTP header.

Firewall Blocking

NetBackup-powered appliances include an internal firewall that only exposes backup and management ports required by NetBackup admins. All other internal services are blocked.

Intrusion Detection Service

NetBackup-powered appliances help protect the system from an attack, misuse, or compromise with a built-in intrusion detection system (IDS). In essence, the IDS sandboxes applications, restricting each access only to processes and resources specifically assigned to them.

Event Monitoring and Audit Logging

NetBackup-powered appliances provide audit logging of cluster and appliance events—operations that are initiated by users—such as login, and config changes. These logs are regularly rotated and retained for 90 days.

Container Namespace Isolation and Service Privilege Limitations

One of the key design choices needed to build the most secure immutable architecture for protecting backup data from a ransomware attack is containerizing 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-powered appliances, all NetBackup services run in different containers. This design provides many layers of additional security, including:

- **Limited-service privileges per container:** Defines which system calls a container can run, and grants control of what runs inside the container, eliminating the need for elevated system privileges. NetBackup-powered appliances employ seccomp security profiles to restrict container privileges and remove unnecessary system call access for the container processes.
- **Blocking host network sharing with containers:** Ensures that anyone able to access the host network won't be able to see communications between services.
- **Namespace isolation:** Ensures processes only have access to their own discrete set of resources.

Highly Restrict Access to Your Filesystem and Destructive Operations

By necessity, every system has certain operations that, in the wrong hands, can be destructive to the backup data. In order to prevent malicious actors from accessing these operations, it is essential to restrict these destructive operations. NetBackup-powered appliances have a hardened OS built with multiple layers of security based on a Zero Trust architecture.

Write Once, Read Many (WORM) Storage

NetBackup-powered appliances include 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.

Most importantly, there is an 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 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 instantiated by the filesystem layer.

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-powered appliances' 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 the 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
- Your data is protected from being encrypted, modified, and deleted using WORM properties
- The NetBackup administrator's ability to delete images stored in WORM storage is removed

NetBackup-powered appliances support three different lockdown modes, each providing a different level of granularity for WORM and retention: Normal Mode, Enterprise Lockdown Mode, and Compliance Lockdown Mode (see Figure 4).

Normal Mode disables WORM and retention capabilities.

To configure WORM storage and retention capabilities, a user with the appropriate rights must enable either Enterprise or Compliance lockdown mode during initial config or after. The differences are:

Enterprise Lockdown 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/security 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 Lockdown 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 rentention locking	✕	✓	✓
Deletion of immutable data before expiry by the Backup Administrator	✓	✕	✕
Backup image retention lock deletion	—	✓	✕
Access to Remote Management Platform	✓	✕	✕
Appliance Administrator access to node operating system	✓	✕	✕
Appliance immutability mode upgrade	✓	✓	—
Appliance immutability mode downgrade	—	✕	✕
Retention lock extension	—	✓	✓

Figure 4. An overview of the three lockdown modes in NetBackup-powered appliances

Once a system 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 an appliance when it is set to either Enterprise or Compliance mode include:

- Lockdown modes are retained during upgrades
- The appliance nodes are prevented from being factory reset
- In a scale-out cluster, newly added or replacement nodes are automatically placed in the existing lockdown mode of the cluster

Multi-User Permission Required to Elevate to Super User

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 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 remote console, 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).

Secure Data Encryption

NetBackup-powered appliances include 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.

Filesystem Isolation

NetBackup-powered appliances utilize dedicated file systems that are mounted with a security context for exclusive access to each container. This blocks container file system sharing, allowing each file system to only be visible from—and accessible to—one specific container. As an example, it prevents host-level services such as the web UI from accessing the container file systems.

The container file systems are also isolated to necessary services within a container, thus limiting other services from seeing and accessing 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 dedupe 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.

Advanced Intrusion Detection Service (AIDE)

As part of STIG rules, NetBackup-powered appliances also have 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.

Security Standards

FIPS Compliance

The NetBackup containers, OS, and platform software meet stringent security standards and are Federal Information Processing Standard (FIPS) 140-2–compliant. NetBackup-powered appliances leverage FIPS validated crypto modules (by NIST) for all cryptographic operations. These modules are sourced from external vendors such as RedHat and SafeLogic.

Security Technical Implementation Guide (STIG)

STIG is a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security. NetBackup-powered appliances use the STIG template to meet security requirements per the Defense Information Systems Agency (DISA) profile for the OS and the application security and development (ASD). They use the security framework within Linux, SELinux, to create and enable proprietary security policies that conform with STIG guidelines (DISA RHEL profile) to further harden the OS from malicious attacks. For example, it removes admin access to superuser and includes an internal software firewall that blocks external access to internal services.

Some examples of NetBackup-powered appliances 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 or unauthorized 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, config changes; these logs are rotated daily and retained for 90 days.

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 regularly performed.

Appliance Software Lockdown

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

Summary

Using NetBackup-powered appliances adds the additional layers of infrastructure immutability and indelibility that are needed to provide the most comprehensive and robust security protection for your backup data. With integrated container isolation, a security-hardened OS, and a Zero Trust security model, NetBackup-powered appliances are proven to help prevent data loss due to malware infiltration and ransomware attacks, while providing the flexibility to recover from an isolated recovery environment. So your data stays secure and always available.

References

For more information about the security built into each appliance, check out these white papers:

- NetBackup Flex Scale: Secure by Default
- NetBackup Flex Appliance Security

1. 2023 Sonicwall Cyber Report
2. www.ibm.com/

VERITAS

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

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

V1960 07/23