Immutable Backups are Crucial to Enterprise Hybrid Cloud Security

White Paper | December 2022

Introduction

Imagine you work for an oil and gas company that transports fuel, or a hospital with patient data—blood types, allergies, and medication lists—stored on servers.

Now imagine that ransomware has hit your company. A cybercriminal is demanding millions or else data will be released. You've lost track of fuel transportation data; how much is still in transport? Where is it? Has it been delivered? Worse; you have 20 surgeries being performed and in the middle of surgery your doctors can no longer access patient records. Do you stop surgery or keep going? Even if you paid the ransomware, would it be restored on time to save lives?

It's not enough to have storage and backup. Traditional backup and recovery systems are no longer able to help organizations quickly resume operations after an attack. Cybercriminals have learned that they can target a company's production systems and infrastructure, but they can also target backups. They can delete or encrypt repositories and snapshots, so they are unusable. How do you ensure that backup data is not vulnerable?

Despite best efforts by admins and staff to protect corporate data, ransomware, malicious insiders, and accidental deletion still happens. Having a holistic, comprehensive, and multi-layered strategy is essential and the best way to protect your business.

Many consider backup and recovery to be the last line of defense, but Veritas believes it should be considered a first-line part of your cybersecurity strategy. Security attacks and corruption are not a matter of if, but when. While detect and protect is important, at the end of the day, there is nothing more essential or infallible than knowing you have a copy of your operations tucked away in a safe place. Our goal is to make your backup and recovery process easier and more efficient.

Ransomware and corrupt data backups can disable a business quickly. Having your operations go down costs a significant amount of time and money to resolve. The use of network sharing within the company elevates the risk of spreading malware and corruption quickly once the system is breached.

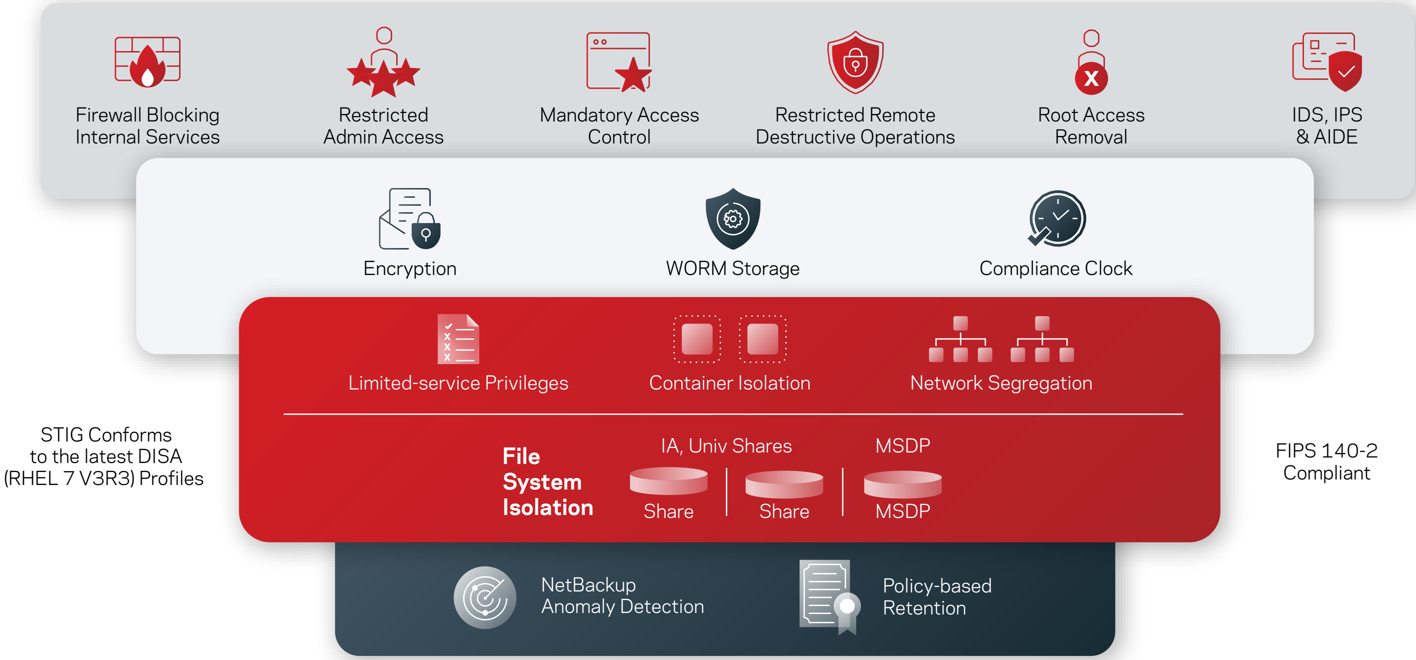

Figure 1. NetBackup Flex Scale's Zero Trust model providing multiple layers of protection from ransomware attacks

Enterprise Cloud Risks

The cloud storage option of backing up data has become a critical conversation within the enterprise business community. Many organizations debate the cost benefit, disadvantages, and risk of on-premises versus cloud storage. Regardless of location, these backup options do not guarantee data authenticity. Veritas NetBackup™ provides autonomous data management with AI-powered machine learning to provide anomaly detection, air gapping, and immutable vaults in a public cloud from a single management point.

While cloud is great for being able to access data across multiple devices from anywhere at any time, there are dangers that come with it. If systems are compromised, data recovery may not be possible. Immutable storage may be the only solution to ensure safety and security of your data. With information being on-demand via cloud-native apps and data at the edge, Veritas can protect your data regardless of where it lives.

Immutable backup from a data protection perspective is data that cannot be changed or deleted after creation. It offers the highest level of data protection for your business. This assures a business that your backup data was isolated, corruption is non-existent, and that you can move forward with a clean restore of the data.

Data permanence is an integral part of immutable storage, and backups must be made in a way that ensures data remains unchanged. When an immutable backup is created, Veritas Alta™ Data Protection for cloud and Veritas NetBackup for on-prem does it in a write once, read many (WORM) format. This means that the snapshot is read only when it is done.

Any business that handles sensitive or critical data has concerns about having a reliable backup method. If or when a data breach occurs, how can a business be assured that the backup is not corrupt? Depending on when the breach occurred, the last set of backups may have executed impartially or with corruptions. With anomaly detection on backups, immutable lockdown mode (retention lock) combined with air gapping makes a key difference in data protection solutions, regardless of the hardware you are using.

The immutable storage story is one that fits into your business continuity plan and cybersecurity strategy. A company's ability to contain and mitigate breaches and corruption as soon as they are identified is imperative. Being able to isolate, segregate, and secure successfully depends on your company's plan and backup requirements; how often does it take a snapshot and backup, and where is the backup (or multiple backups) stored?

Data can be corrupted for a multitude of reasons. While ransomware and hacking are at the top of many businesses' concerns, data can be manipulated through unattended access, unintended or accidental deletion, or even natural disasters such as flooding and power outages. The benefit of immutable storage, or immutable backup from our perspective, is that no matter what your reason is to restore and rebuild, you will have clean, reliable data.

The question then turns to timing. There is a period of time between corruption and the detection of corruption. If you consider a ransomware attack, a malware breach may occur weeks ahead of detection because it can infiltrate the system and lay low collecting information, data, and passwords. What if you replicate the breach into your isolated backup?

This is where having proper data governance and building a successful infrastructure (whether you choose on-prem or cloud) is critical. Creating data separation across multiple layers, where the layers can be isolated, is one way to have comprehensive recovery. This means that backup and recovery can be segmented and applied as needed, where needed, saving time and cost. The challenge is making sure that these layers are automated without too much interference from manual human touch, which can cause error.

Veritas NetBackup allows you to configure and automate these backups when you want them, where and how you want them. If a restore is needed, Veritas Alta™ Data Protection allows you to recovery quickly and smoothly in the cloud and NetBackup; on-premises. With containers you can additionally create immutable infrastructure; critical failure can be addressed with a rollback on a particular container instead of an entire system, and instances can be replaced quickly.

How Veritas Creates Ultimate Immutability

Enterprise cloud infrastructure should offer a technical interface that is well-optimized with an automated deployment strategy that supports segmented rollback, snapshot, and backup and restore capability to maintain a Zero Trust architecture. By eliminating the manual touch and access, servers and other resources can be centrally managed and audited. This allows for uniformity in patching and software versions across all servers and can help prevent errors.

NetBackup and NetBackup Flex use OpenStorage Technology (OST) API; a flexible, storage-agnostic immutable backup manager. Using Veritas or any third-party storage, your company can support primary, secondary (deduplication), and cross-domain replication with auto image replication (AIR), giving you unlimited configuration options across any backup storage tier. It keeps your data secure and compliant both on-prem and in the cloud, and can be used with Amazon (AWS) S3 Object Lock. Businesses can manage immutable image policies, leverage third-party immutable appliances, and remain vendor-agnostic.

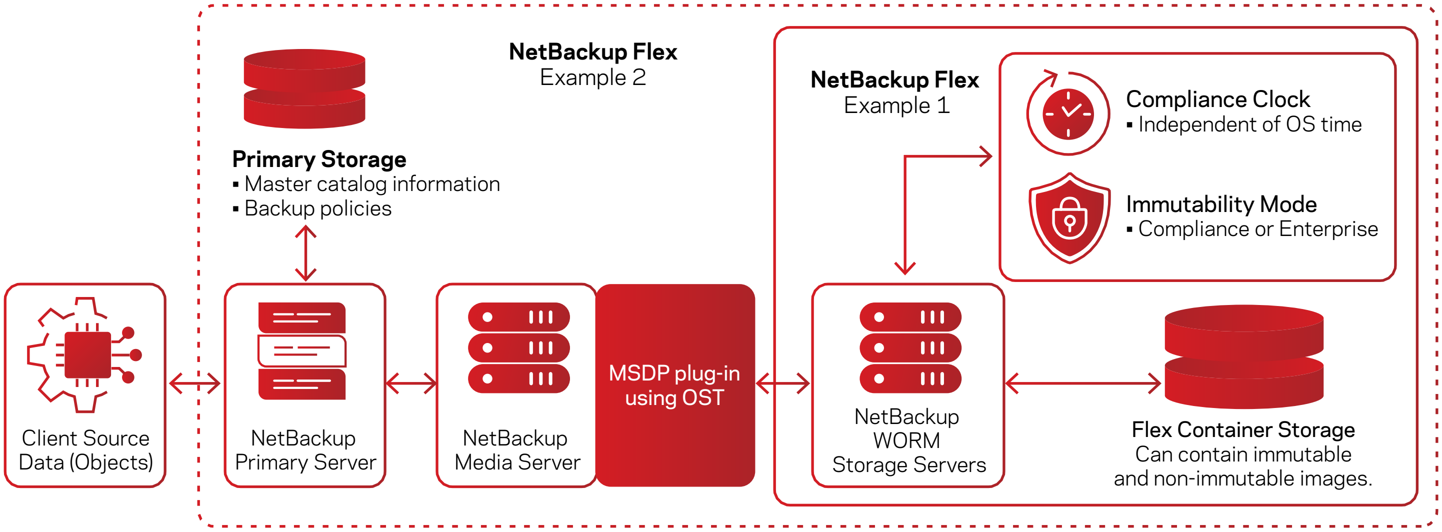

Figure 2. Veritas Flex Appliance comes with a wide variety of security features

NetBackup Flex and NetBackup Flex Scale are based on container technology, extending data protection with multi-tenant capabilities to reduce data center costs, improve management efficiency, and provide resiliency against ransomware and security threats. This affords companies comprehensive recovery to maintain business continuity, reduce downtime and lost revenue, minimize risk, and meet regulatory and corporate governance policies. It offers an air gapped solution with multi-point backup repositories including cloud; has policy-based retention locks, role-based access control, and password policy management; and Security Technical Implementation Guide (STIG)-hardened cybersecurity.

Enterprise and compliance lockdown modes allow you to choose the right immutability strength for your organization. Compliance mode enables immutable storage in which no user (including the root user) can delete the data during a predefined retention period. Enterprise mode protects data from being deleted during a predefined retention period, and only users with special permissions can alter the retention settings or delete the data through dual authorization. Two individuals with different appropriate role-based access control (RBAC) levels must agree to make any changes to retention time, modify the data, or delete the data.

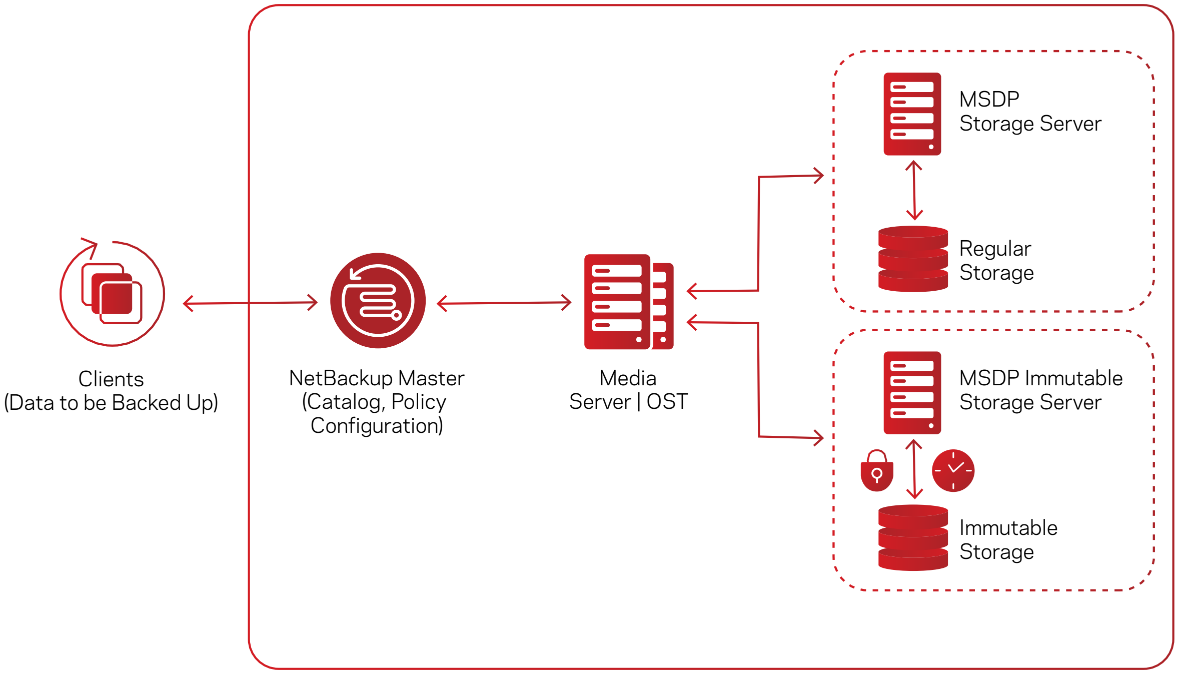

Figure 3. How Veritas protects your IT services against Ransomware attacks.

One Size Fits Many

Enterprises rarely utilize a one-size-fits-all architecture. With the amount of applications present and the multitude of variance within the environment, companies are constantly seeking a way to unify the structure so they can rest assured their data protection strategy covers the entire infrastructure stack. When immutability is required, Veritas supports immutability/WORM on-premises and in the cloud. Pair that with the intrinsic malware scanning that allows you to utilize third-party scanning, and you have an immutable vault with malware detection.

You can also configure an isolated recovery environment (IRE) on a Flex WORM storage server to create an air gap between your production environment and a copy of the protected data on the media server deduplication pool (MSDP) WORM storage server in the IRE. The production environment does not require any additional steps for this feature. All of the commands are executed on the MSDP WORM storage server shell.

Immutable backups guarantee that the data backup is authentic, accurate, and preserved. NetBackup Flex Appliances also meet Federal Information Processing Standards (FIPS) 140-2 to keep data encrypted in transit and at rest. This certification ensures government, financial, and healthcare organizations that data handled by third-party organizations is stored and encrypted securely, with the proper levels of confidentiality, integrity, and authenticity. Additionally, NetBackup and Flex Appliance immutability solutions have completed the Cohasset Associates immutability assessment[1] (in compliance mode), specifically:

- 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)

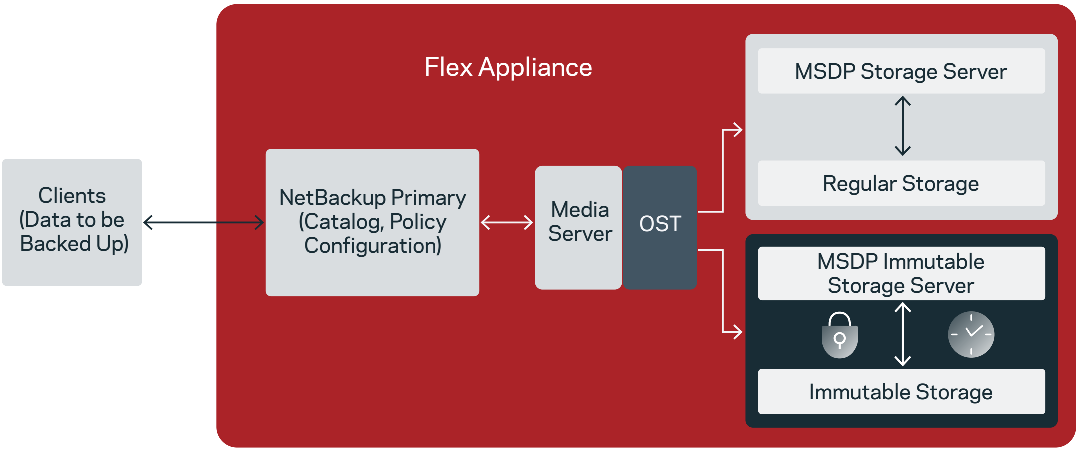
Flex Appliance
Clients (Data to be Backed Up)
NetBackup Primary (Catalog, Policy Configuration)
Media Server
OST
MSDP Storage Server
Regular Storage
MSDP Immutable Storage Server
Immutable Storage

Figure 4. NetBackup Lock Down Mode

Veritas NetBackup supports disaster recovery (DR) at scale across on-premises, hybrid, and multi-cloud environments to meet specific recovery time objectives (RTOs) and recovery point objectives (RPOs). Because NetBackup supports a wide range of recovery options, businesses can choose methods that best suit their recovery needs, such as recovery at scale Veritas Alta™ Application Resiliency for cloud and NetBackup Resiliency for on-premises..

Prevent gaps or siloed work with visibility into—and reporting of—the entire data infrastructure, with Veritas Alta™ Analytics for cloud and IT Analytics for on-prem. Whether on-premises or cloud, Veritas NetBackup integrates every point in the technology stack to maximize reliability and performance. Veritas NetBackup Flex Appliances also have a specially-designed intrinsic compliance clock based on the Veritas File System (VxFS) used for managing retention periods that is independent from the OS, which administrators are unable to change.

Conclusion

With the combination of a hardened OS, container isolation, and a Zero Trust security model, Veritas provides the multi-layered infrastructure immutability and indelibility necessary for protection. We take the complexity of the issue and make it easier for you to navigate and handle.

Even if your company is diligent about backup up data, there is still the risk of human error and equipment failure. The risk of accidental deletion or modification is high. Files that are stored in immutable storage can help you avoid the stress of corruption and cyberattacks. Veritas NetBackup ensures files are not altered by accident or on purpose, creating a more efficient and effective process within your cybersecurity strategy and can helping you avoid financial loss and downtime.

Visit veritas.com/solution/cloud-data-security to learn more.

1. veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup

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

VERITAS

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

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