VERITAS

Improve Data Recovery with Air Gaps and Isolation

Maintain secure copies of your data to neutralize the impact of cyberattacks.

White Paper | May 2023

Why Create a Data Vault?

Cybersecurity maintains a front row seat in business leaders' minds. Cyber threats are increasingly sophisticated, constantly refining their techniques for maximum damage. According to Gartner, by 2025, 40 percent of all boards of directors will have a dedicated cybersecurity committee to create additional reporting and strategy expectations on cybersecurity policies, execution, and recovery[1]. The exponential growth of cyber crime is costing millions of dollars and hours that organizations are fighting to reduce and recover. With a cyberattack occurring every 15 seconds in 2022[2], it has become a race against the clock to ensure you are prepared with a strategy that reduces your risk, eliminates your uncertainty, and maintains control of your environment.

Confidence in a resiliency and recovery plan comes from implementing a reliable cybersecurity framework, with the right technology and processes. Do you have a cybersecurity incident response plan that you could confidently communicate to your manager and upper management? According to Gartner[3], by 2025, 70 percent of CEOs will mandate a culture of organizational resilience from cybercrime. Now is the time to understand cybersecurity trends, and the critical components of a successful recovery plan. Be able to stop a ransomware attack dead in its tracks, and demonstrate to your board of directors with confidence that you have implemented the right tools to recover.

What is an Air Gap and Why Should I Care?

As cyberattacks become increasingly sophisticated, hackers are not only targeting your primary data storage, but also your backup data storage. It is critical to plan for this in your disaster recovery strategy. In most cases, hackers are lying dormant in your system until they can access and compromise your primary and backup data. If they can access it, they can disrupt it.

An air gap, according to the National Institute of Standards and Technology (NIST), is an interface between two systems at which (a) they are not connected physically, and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control)[4]. In the past, air gaps were the gold standard for protecting operational technology such as a thermostat or home appliance. Now that almost everything is connected via a wireless or wired network, the need for a stringent air gap process is critical to keeping a good copy of data available for recovery.

In networked environments, hackers can exploit almost any entry point, even via a system with all wireless and wired signals disabled. In the most closed systems for highly secure data, some IT departments disable all USB ports and use a Faraday cage to block all wireless transmission and prevent electromagnetic leakage.

Auto image replication (AIR) enables you to replicate backup data between backup domains that can be within the same or different sites, including public cloud. AIR also enables offline air gapped copies of your backups, to further reduce the threat of data access by unintended sources. As data expands in your owned data centers and in the public cloud, it is important to have a backup and recovery solution that implements an air gap structure to maintain a last known good copy of critical data.

Cloud Data and Air Gapping

Cloud-first is growing: 85 percent of organizations report that they will be cloud-first by 2025, with 94 percent implementing a multi-cloud strategy[5]. We have seen a sharp increase in accelerating cloud strategies, which can result in disparate tools and decision-making authority. Just as you diversify and optimize your primary data repository with different public cloud options, it is important to optimize your data recovery approach with the best built solutions to get you back up and running.

We recommend the functionality of an isolated recovery environment (IRE) as the best possible option. Air gapped solutions offered in an IRE create a secure copy of your critical data, providing administrators a clean set of files on demand to neutralize the impact from a ransomware attack within a multi-cloud environment.

Isolated Recovery Environments

Traditional network isolation solutions physically or logically break connectivity between secure locations, making all communication in or out impossible. This limits data transfer to the isolated environment and endangers recovery time objectives (RTOs) and recovery point objectives (RPOs) if the tertiary copy is needed. Commonly referred to as the pushing of replication data from the source to the target, the source domain independently processes and submits a replication job to a target domain. This traditional approach limits the time available to replicate critical data into a secure environment when the connection is down or blocked.

By contrast, the pull replication model initiates the replication request from the target. Veritas offers NetBackup's IRE solution, which optimizes data movement by offering a pull replication model whereby the request to send data comes from the IRE's media server deduplication pool (MSDP), and the reverse connection offers better control of the data flow to further secure the environment logically and physically. Replications to the IRE are now able to be fully controlled from within the IRE, including support of a specific window as defined in the IRE air gap schedule.

The NetBackup IRE is impenetrable during data transfer due to multiple layers of security, including intrusion prevention mechanisms and data encryption in-transit and at-rest. Throughout the data journey, data is secure regardless of where it resides, storage is not compromised, and there is zero risk of malicious or unauthorized users reading or modifying data. Veritas offers data isolation options on-premises and in the cloud with NetBackup Recovery Vault—a seamless cloud storage-as-a-service, air gapped for ransomware protection, optimized for scale, and ensuring data portability with predictable costs.

Veritas offers a simple workflow that allows you to transform any NetBackup—on-prem or in the cloud—into an IRE framework, providing ransomware resiliency focused on three key principles:

- **Protect**: Easily incorporate isolated recovery capability with support for multi-factor authentication (MFA) and role-based access control (RBAC) that aligns with the Veritas Zero Trust security strategy.
- **Detect**: NetBackup IT Analytics provides anomaly detection that can detect ransomware in real-time. The integrated NetBackup malware scanning capability provides malware scanning prior to recovery that can be prioritized based on anomaly scores.
- **Recover**: Orchestrate recovery of an entire data set in an isolated environment, in the cloud or on-prem, with the ability to manage a wide variety of RPO and RTO requirements.

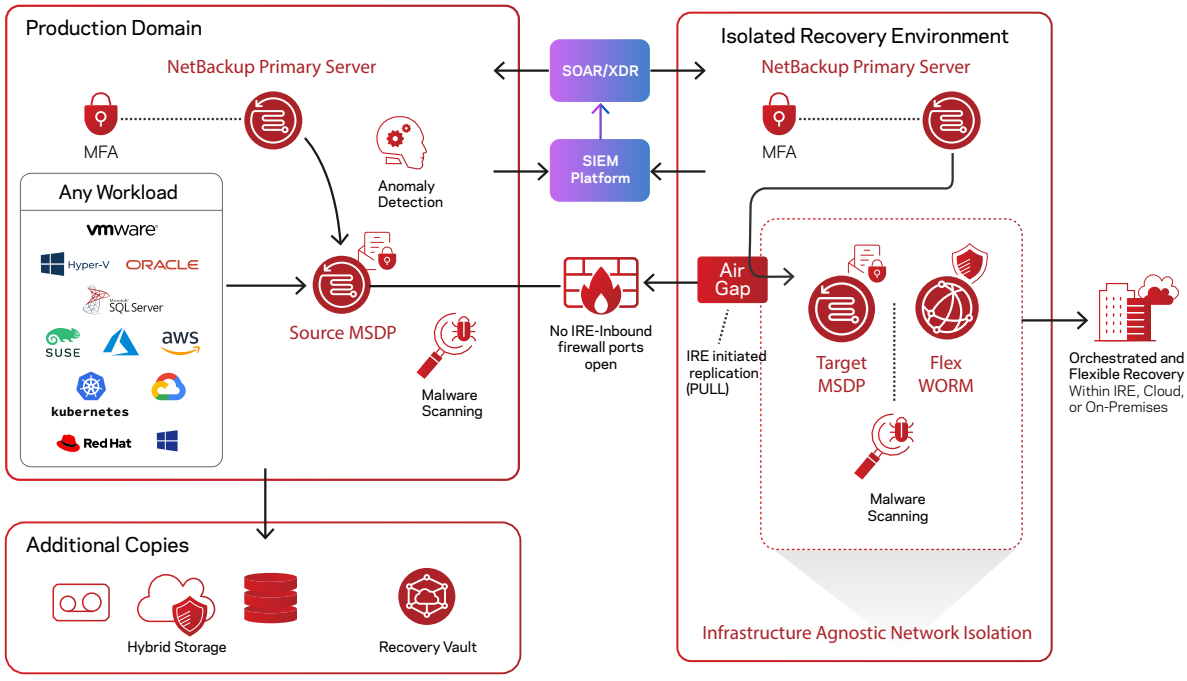

Figure 1: NetBackup Isolated Recovery Environment

An isolated environment provides another layer of resiliency to combat ransomware and malware.

Increase Protection with Zero Trust

A Zero Trust policy provides even greater protection. Adopting a companywide Zero Trust mindset has been proven to reduce the risk of a devastating attack.

Veritas IRE is based on the Flex appliances' container-based multi-tenant WORM (write once ready many) storage with hardening OS and a Zero Trust architecture. By strengthening your identity and access management (IAM) with MFA and RBAC for users, tools, and machines, you are limiting access to highly sensitive data and backups. Only users that need to access the data should be permitted. Password hygiene is also a top priority.

You can prevent access to these areas with strong IAM controls, privilege controls, hardening, and secure hardware all built on Zero Trust. If a breach occurs, it reduces the attack surface or the blast radius because it provides multiple layers of security that minimize impact. Once in your systems, cybercriminals often move across your environment searching for business-critical data, confidential information, and backup systems.

Anomaly Detection and Malware Scanning

With complete visibility, intelligent anomaly detection, and malware scanning, you can confidently know where all your data is, while reducing operational complexity and optimizing cost management. Veritas AI-powered anomaly detection recognizes out-of-the-ordinary data and user activity across your entire environment, and alerts you to suspicious activities, in near real-time. This feature ensures your data is always recoverable and enables you to take immediate action when ransomware strikes, isolating backups with malware and limiting the impact of malware on your backup data. You can either restore full images that have been scanned and validated as secure, or you can restore individual files. If a file marked for restore is infected, you can restore it from an uninfected backup. This gives you a safe and effective way to recover data without any risk of re-infecting the target machine.

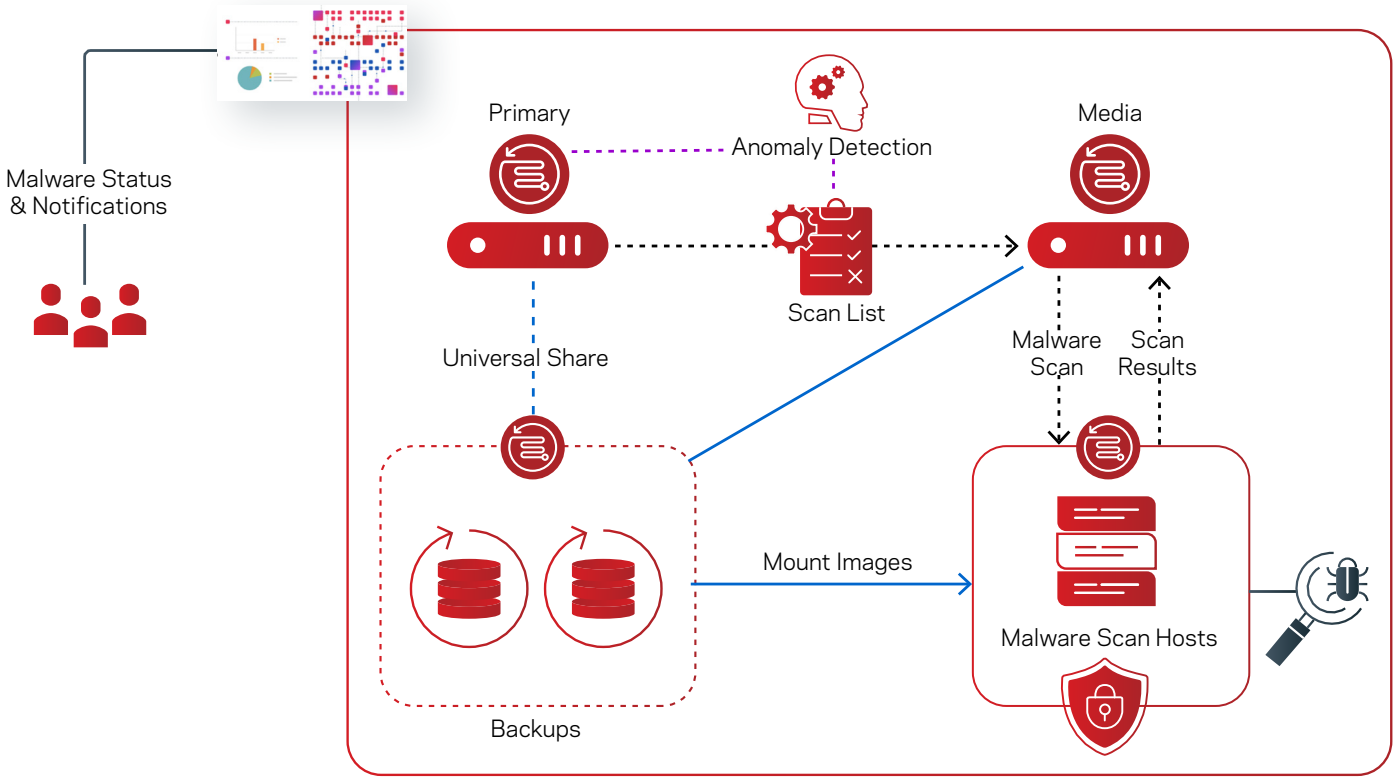

Figure 2: NetBackup integrated malware scanning

Recover Using Immutable and Indelible Storage

Immutable and indelible storage ensures that no one or nothing can change, encrypt, or delete data for a determined length of time (or at all). It also prevents data tampering and unauthorized access. As part of your IRE strategy, NetBackup Recovery Vault provides a cloud-based immutable and indelible storage solution that you can scale up or down depending on your needs.

Recover Confidently with IRE

Reduce risk, eliminate uncertainty, and maintain control with NetBackup Isolated Recovery Environment. Visit Veritas.com or connect with our team to learn more about how our solution can ensure your ransomware resiliency within your multi-cloud environment.

Close the Gaps in Your Enterprise Resiliency Strategy. Learn more >

1. www.gartner.com/en/newsroom/press-releases/2021-01-28
2. www.sonicwall.com/resources/white-papers/2023-sonicwall-cyber-threat-report/
3. www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
4. csrc.nist.gov/glossary/term/air_gap
5. www.gartner.com/en/newsroom/press-releases/2021-11-10

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

V1626 05/22