Veritas NetBackup Isolated Recovery Environment

Reduce risk, eliminate uncertainty and disrupt the spread of ransomware with cyber-resilient, air-gapped isolated recovery.

The Evolution of Data Management Amid the Rise of Ransomware

Ransomware and malware attacks are on the rise and ransomware attacks have increased 185 percent year-to-date[1], with many analysts reporting that costs are expected to surpass $20 billion this year[2]. The threat of ransomware is evolving and so are the techniques attackers are using to bypass the most vigilant security perimeters. Today's enterprise infrastructure and applications are hybrid and geographically distributed, creating unique data management challenges. Governing all this data holistically and ensuring continued availability is a challenge for any IT team, and this problem is only exacerbated by the rise in ransomware.

Backup and recovery of data may be considered the last line of defense against ransomware attacks, but recovering from those attacks requires segmentation, redundancy and data integrity to achieve business resilience. Ransomware attacks have the power to strategically take down an organization's data protection infrastructure before conducting mass-scale encryption, exfiltration or declaring an IT lockout. Because an attack can result in emotional, financial, physical and economic tolls, having a comprehensive, multi-layered cybersecurity strategy is paramount.

Secure Business Data with NetBackup Isolated Recovery Environment

When ransomware attacks, infrastructure network segmentation plays a critical role in limiting the blast radius. Organizations can minimize ransom demands from exfiltrated data by using encryption and creating a stringent security perimeter. In addition, they need to isolate, analyze and preserve a copy of data to ensure business continuity. That is where an isolated recovery environment (IRE) is beneficial, enabling organizations to meet these needs while satisfying strict regulatory and retention requirements. Veritas customers can easily deploy an IRE using their existing Veritas NetBackup™ infrastructure as part of a multi-layered resiliency strategy. Following are the four ways the NetBackup IRE helps prevent ransomware attacks.

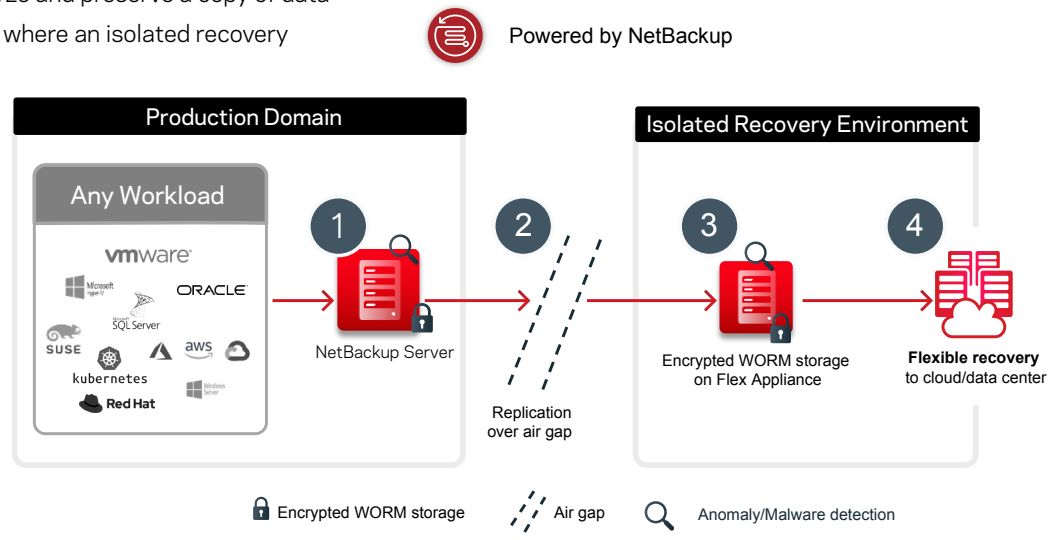
NetBackup Isolated Recovery Environment Benefits

Immediate action on malicious activity—AI-powered anomaly detection and malware scanning detect and notify you before an event can occur.

Isolate data using air gap—Logical and physical isolation from the primary data center ensures integrity of recovery.

Immutable data—Preserve and secure data to ensure data integrity and seamless recovery.

Recovery orchestration—Rehearse or execute complex business service recovery to any hybrid or multi-cloud infrastructure.



1. Leverage Real-time Anomaly Detection

If ransomware is successful in gaining entrance, having insight into your environment is key to identifying any malicious activity. You need to identify the last known good data with a combination of anomaly detection and malware scanning.

NetBackup triggers alerts for administrators to take immediate action against possible malicious activity as it evaluates backup jobs in near-real-time. It uses AI-based anomaly detection that identifies and alerts on unexpected changes to backup data before an event can occur, ensuring you can take action before a lock-out occurs. This capability is available on any NetBackup server and does not require any additional infrastructure for post-processing.

Confidently Choose NetBackup IRE vs Competing Solutions for:

- **Lower TCO**—No additional infrastructure or licensing costs
- **Real-time Anomaly Detection**—no post-processing delays
- **Flexible air gap operation**—no dependence on infrastructure
- **Recovery at scale**—Determine last known good backups

2. Preserve Data with Isolation

Isolating backups can significantly minimize the spread of ransomware. Using air gaps to separate backups from the primary data center, both logically and physically, enables data to remain secure and compliant. The automation of air gaps provides the flexibility to optimize movement of replicated data into WORM (write once, read many) storage.

The NetBackup IRE is impenetrable during data transfer due to multiple layers of security, including intrusion prevention mechanisms plus 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 having access to read or modify data. Veritas offers data isolation options both 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.

3. Stay Secure and Compliant with Data Immutability

When data arrives at its destination, it is crucial it remains secure. Considering it could be the only copy of data if everything else is compromised, making sure that copy is isolated and nothing can alter or corrupt it is vital. That is why having storage isolated from the backup application itself and adopting the "3-2-1-1" backup strategy—keeping three copies of data on two different media types, with one off-site and one copy in immutable WORM storage—prevents harm.

All NetBackup processes are digitally signed, and the hardened solution ensures only processes on the *allowed list* can execute on the system. Containerized WORM storage also prevents a rogue authorized user from compromising data. Data cannot be expired until the retention period has been satisfied using a proprietary compliance clock that is immune to OS or Network Time Protocol (NTP) hacks, providing unmatched immutability throughout the end-to-end data journey.

4. Recover to a Last Known Good State

After malicious activity is detected, having direct insights into which files to rescan or exclude during recovery is vital for business resiliency. With today's diverse workloads, understanding that recovery methods and recovery point objectives (RPOs) vary across different workloads is crucial. Business services comprise multi-tier applications, making it necessary to conduct an orchestrated, automated recovery from multiple service-level objectives (SLOs).

NetBackup lets you create data protection workflows to rehearse or execute complex business service recovery to any hybrid or multi-cloud infrastructure and recover from a backup or granular replication checkpoints based on desired RPOs. With NetBackup, you can automate disaster recovery (DR) rehearsals on a schedule using the last known good backups to achieve regulatory compliance, ensuring you are prepared for an attack.

Choose Veritas NetBackup to Deploy an Isolated Recovery Environment

NetBackup provides the industry's most comprehensive, compliant and secure ransomware resiliency solution, offering you valuable peace of mind and confidence against an inevitable attack. Air gaps are a key component of ransomware resiliency to ensure backup files remain immutable and indelible so a clean set of backups are available for recovery from any possible attacks. NetBackup provides an all-in-one solution with a Zero Trust governance model to ensure data is protected and recoverable from edge to core to cloud at scale—all while detecting any malicious activities in your system—so your organization can be ransomware resilient.

Reduce risk, eliminate uncertainty and maintain control with NetBackup. Connect with our Veritas team to learn more about how our solution can ensure your ransomware resiliency.

1. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

2. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. 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

V1466 11/21