VERITAS

Fortify Your Perimeter: Stop the Spread of Ransomware Dead in its Tracks

Technical Brief | August 2022

Contents

Ransomware Attack - It is no Longer "If", but "When

Today, organizations of all types and sizes face similar problems: defending against ransomware attacks, responding to rapidly changing business environments, and ensuring they meet critical backup and recovery service level agreements (SLAs). Unfortunately, it's commonplace for malware attacks to enter your primary environment and target your backup data.

SonicWall reported more than 623.3 million attacks globally in 2021, doubling the number of attacks in just a year. In June 2021 alone, SonicWall recorded a record high of 78.4 million ransomware attacks—more than 30 attacks per second.

The meteoric rise in cyber threats continues to fuel concerns about an organization's ability to reliably and quickly recover from a ransomware attack.

What is an Isolated Recovery Environment?

For enhanced ransomware resiliency, it is important to secure your backup data on immutable storage and maintain an isolated copy of your backup data, also called an air gapped copy. An Isolated Recovery Environment (IRE) enables air-gapped backup copies by disabling network connectivity to a secure copy of your critical data, providing administrators a clean set of files on demand to neutralize the impact from a ransomware attack.

NetBackup's Isolated Recovery Environment Solution

Traditional network isolation solutions physically or logically break connectivity between secure locations. 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.

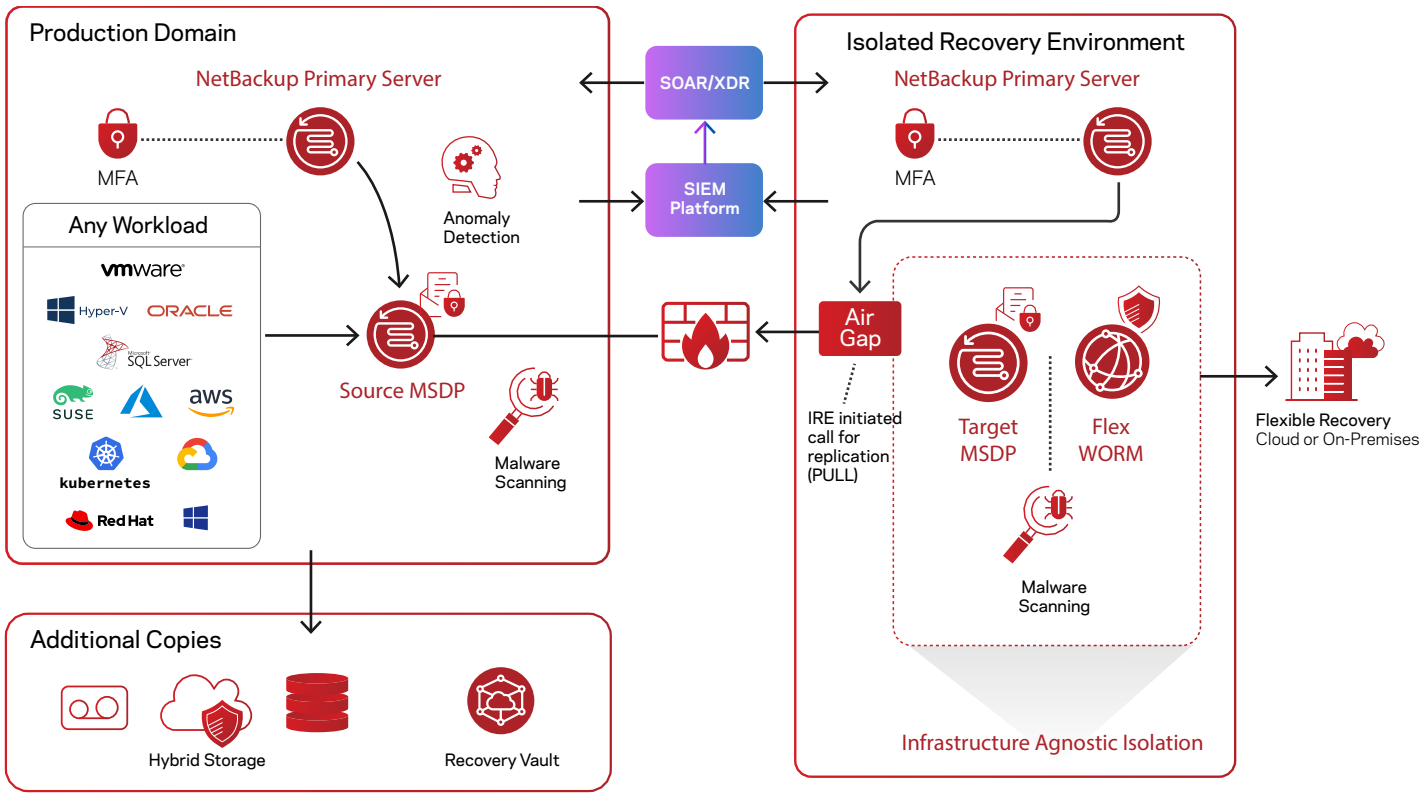

Figure 1. NetBackup's Isolated Recovery Environment architecture

By contrast, the "pull" model pulls the replication request from the source through a specific window as defined in the IRE air-gap schedule. As of version 10.1, NetBackup's IRE solution optimizes data movement by offering a pull replication model, where the request to send data comes from the IRE side, the MSDP reverse connection, to better control data flow and further secure the environment both logically and physically.

NetBackup's Isolated Recovery Environment minimizes threats from ransomware and rogue users by:

- Storing an isolated copy of the data, ensuring it stays unaltered until it is no longer needed
- Detecting ransomware within the protected data to prevent reinfection when restoring data
- Providing scalable recovery operations, so business services can meet service-level objectives
- Enabling predictable recovery processes that can be rehearsed to on-premises or cloud infrastructures

Additional Components to Consider with an IRE

Tertiary storage solutions are an excellent addition to any IRE, which aligns with the ideal of multiple copies of backup images stored in multiple locations, cited as 3-2-1-1. For additional resiliency and security, consider NetBackup Recovery Vault as a tertiary duplication task that offers a secure, deduplicated, cloud-based storage location.

Manage Network Access to the IRE environment with NetBackup

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. Customers can optionally add a physical air-gap as an additional layer of protection. By empowering the 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.

Zero-Trust Architecture with NetBackup Flex Appliance

NetBackup Flex Appliance is designed with security at the forefront, and provides a complete immutable and indelible storage solution to ensure your system and data are recoverable.

NetBackup Flex Appliance offers an easier, more streamlined way to deploy a secure, isolated recovery environment. Built-in features support a zero-trust architecture and provide comprehensive security access controls, including FIPS 140-2-compliant data encryption, a hardened OS, and immutable storage.

NetBackup Flex Appliance uses msdpadm to access restricted shell commands to configure IRE. For container-based architectures, NetBackup Flex Appliance offers multi-domain isolation, network segregation, and limited-service privileges, as well as an immutable (WORM) container as a complete storage solution.

NetBackup Recovery Vault streamlines multi-cloud storage processes—account creation, access tier definition, and protection policy selection. All resources are provisioned and managed from within NetBackup's locked-down security and role-based authentication policies, eliminating separate accounts and user interfaces across cloud providers, and ensuring security and compliance policies are in check. You can run a recovery vault in the cloud while deploying an air-gapped IRE on premises with NetBackup Flex Appliances. This hybrid cloud approach provides stronger resilience and security while lowering your total cost of ownership, by eliminating the unexpected data ingress and egress fees and paying for only what's used with a "pay-as-you-go" subscription service.

NetBackup Malware Scanning and Anomaly Detection

NetBackup Malware Detection provides additional control in the detection and recovery portions of the workflow. NetBackup offers two malware scanning methods to protect your data's integrity and the backup image: on-demand scans and scans automatically triggered by high anomaly scores.

The integrated NetBackup malware engine allows you to perform on-demand scans of backup images for latent threats. Additionally, integration with leading malware scanners such as Microsoft Defender and Symantec Protection Engine were made available in the NetBackup 10.0 release.

Storing the scan's status in the NetBackup catalog empowers you to restore confidently with visibility into the malware scan status. Add your malware scanning engine to NetBackup for added resistance to the growing cyber-terror threats.

An IRE that is Flexible and Easy to Set Up

You can configure an isolated recovery environment (IRE) on a NetBackup BYO media server or Flex Appliance WORM Storage server to create an air-gap between your production environment and a copy of the protected data. The air-gap restricts network access to the data except during the timeframe when data replication occurs, providing further protection against ransomware and malware.

To configure an IRE, you need a production NetBackup environment and a distinct NetBackup IRE environment with an MSDP server configured. The production environment does not require any additional steps for this feature. Enabling IRE functionality is performed within IRE itself, desinating trusted sources and a schedule.

Conclusion

Veritas continues to strengthen NetBackup's Isolated Recovery Environment controls to easily secure a replication target from ransomware and malware. With NetBackup's granular controls for an IRE and the SLP operations, you no longer have to sacrifice your organization's security posture for data flow.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 95 percent of the Fortune 100—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

V1600 08/22