Technical Validation

Ransomware Defense and Remediation With Pure Storage

Pure Storage Ransomware Solution

By Craig Ledo, IT Validation Analyst

July 2022

This ESG Technical Validation was commissioned by Pure Storage and is distributed under license from TechTarget, Inc.

Introduction

This ESG Technical Validation documents the detailed evaluation of the Pure Storage solution for ransomware mitigation and recovery. We evaluated how Pure Storage provides ransomware protection before, during, and after an attack, including offline restoration for malware cleansing, rapid recovery for priority systems, and support for forensics with space-efficient snapshots.

Background

Ransomware attacks continue to be top of mind for business and IT leaders—and for good reason; they compromise access to an organization's lifeblood—data. The recent rash of ransomware attacks has had tremendous costs, including downtime, people time, device costs, network cost, lost opportunity, ransom paid, and so on. With millions of dollars spent annually to guard entry points to data, many organizations still underestimate the strategic value of augmenting data protection. ESG research shows that 36% of survey respondents said their organization experienced such probing attacks on at least on a monthly basis over the past 12 months, including 9% that were targeted daily and 12% that were attacked weekly (see Figure 1).[1]

Figure 1. Recurring Ransomware Attacks Are Common

Source: ESG, a division of TechTarget, Inc.

Another 27% of respondents experienced ransomware attacks more sporadically. With so many organizations experiencing attempted ransomware attacks, it's critical for organizations to implement strong defenses to address attacks before, during, and after to prevent them from succeeding, especially since victims can and often will be revisited by these criminals.

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021. All ESG research references and charts in this technical validation are from the research report.

Pure Storage Ransomware Solution Overview

Pure Storage provides three pillars of ransomware lifecycle best practices:

- **Pillar 1 – Before an Attack (Preventive Maintenance):** The first pillar simplifies management of system hygiene and patching, implements SIEM and speeds up processing to identify threats, and sets up multi-factor authentication.
- **Pillar 2 – During an Attack (Mobilize the Response):** The second pillar locks down application data, backups, and systems with always-on encryption at rest, identifies attack and severity, and prevents snapshots from modification or deletion.
- **Pillar 3 – After an Attack (Recovery Effort):** The third pillar provides rapid recovery for priority systems, offline restoration for malware cleansing, and support for forensics with space-efficient snapshots.

Pure Storage has three key backup technology partners to help address ransomware attacks (see Table 1).

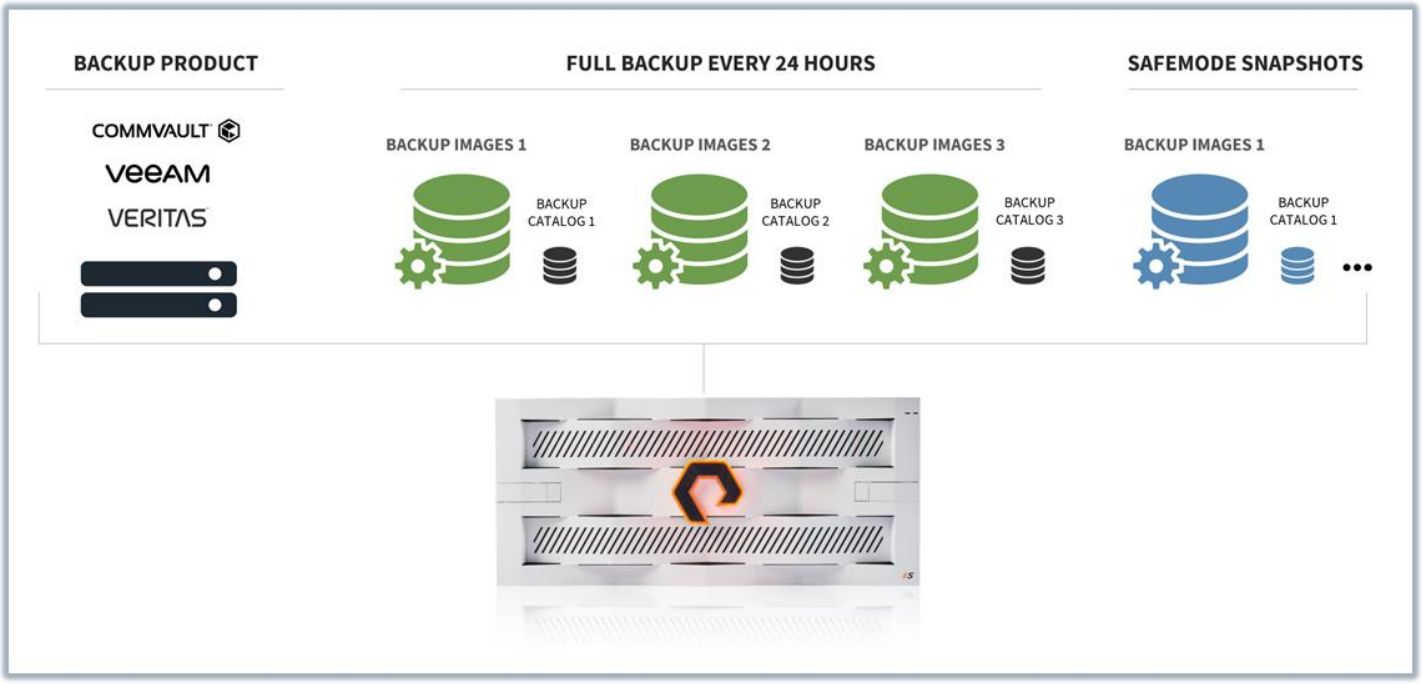
Table 1. Pure Storage Ransomware Solution Matrix

	FlashArray//C	FlashBlade//S	FlashRecover
TAP Partner	Veeam	Commvault	Cohesity
Footprint	3U for chassis, 3U per shelf, up to 2.3 PB raw in 9U (with Purity 6.3.2 or later)	5U chassis, up to 1928 TB raw	Scaling from 4 RU with 64 TB usable scaling to 40 RU with 9 PB usable Right size compute with disaggregated architecture in 2 RU increments with no limits to meet any rapid restore needed
Performance	Up to 10 TB per hour restore	Restore scales based on number of blades and data movers can be 10 TB per hour	Restore scales on number of blades and data movers can be 10 TB per hour
Connectivity	Block, IP	IP	IP
Protocol	Block, NFS	S3	NFS

Source: ESG, a division of TechTarget, Inc.

With Pure Storage, organizations can mitigate ransomware attacks with Pure SafeMode, which is a built-in feature of the Purity operating environment that powers FlashBlade and FlashArray. This enables organizations to create read-only snapshots of application data, backups, and associated metadata catalogs after a full backup is performed with Commvault, Veeam, or Veritas data protection software. SafeMode snapshots cannot be altered, encrypted, or deleted. To manually access or eradicate SafeMode-enabled copies, only authorized personnel, in conjunction with Pure Storage Support, can delete or alter the copies, providing a virtual air gap that is automated and simple to set up and that provides a clean copy to recover from (see Figure 2).

Figure 2. Pure Storage Ransomware Solution Overview



Source: ESG, a division of TechTarget, Inc.

SafeMode provides the following benefits:

- **Enhanced Protection:** Ransomware can't eradicate (delete), modify, or encrypt SafeMode snapshots.
- **Backup Integration:** Backups utilize the same snapshot process regardless of the backup product or native utility used to manage data protection processes.
- **Secure Application Data**: Protects backups of native databases and applications.
- **Flexibility:** Snapshot cadence and eradication scheduling are customizable and easy to set up.
- **Rapid Restore:** Restores leverage a massively parallel architecture and elastic performance that scales with data to speed backup and recovery.
- **Investment Protection:** FlashBlade and FlashArray both include SafeMode at no extra charge. Pure Storage subscription or maintenance support contracts cover enhancements.
- **Compatibility:** SafeMode seamlessly integrates with a variety of data protection solutions from Commvault, Rubrik, Veeam, and Veritas.

ESG Technical Validation

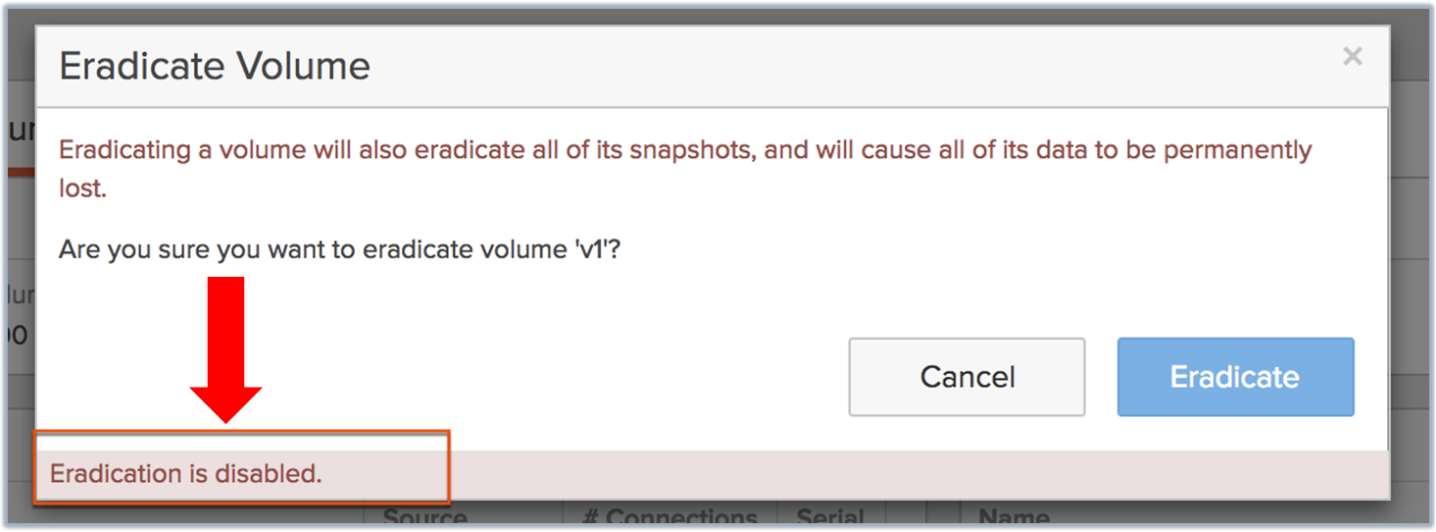
ESG performed a technical validation of the Pure Storage ransomware solution with a focus on recovery after a ransomware attack, including offline restoration for malware cleansing, rapid recovery for priority systems, and support for forensics with space-efficient snapshots.

Offline Restoration for Malware Cleansing

During an attack, organizations should isolate, disconnect, and clean up compromised network systems. Once the attack is over, organizations should fully audit all the systems on the network to make sure no artifacts or malware remain. The previous step helps to prevent a situation where an organization shut down multiple systems, performed migrations, restored data, and got the network back online only to have the automated ransomware reactivate. So, organizations need to make sure to sanitize the environment before restoring data from backups and going live.

Pure Storage ensures data is safe from encryption by ransomware attackers, that it's stored in a protected manner, and that it leverages a multi-factor authentication approach to ensure that people or processes with administrative access cannot fully delete data without manual interaction and intervention from Pure Storage support. For example, in Figure 3, snapshot deletion (i.e., eradication) is disabled.

Figure 3. Disabled Deletion of Snapshots



Source: ESG, a division of TechTarget, Inc.

Why This Matters

ESG research shows that the top cybersecurity areas for planned spending increases in 2022 are cloud application security (62% of respondents) and data security (58%), followed by cloud infrastructure security (56%). This points to the importance of taking a holistic approach to cybersecurity to help protect organizations against the growing number of security threats they face, including the ongoing spike in ransomware attacks.

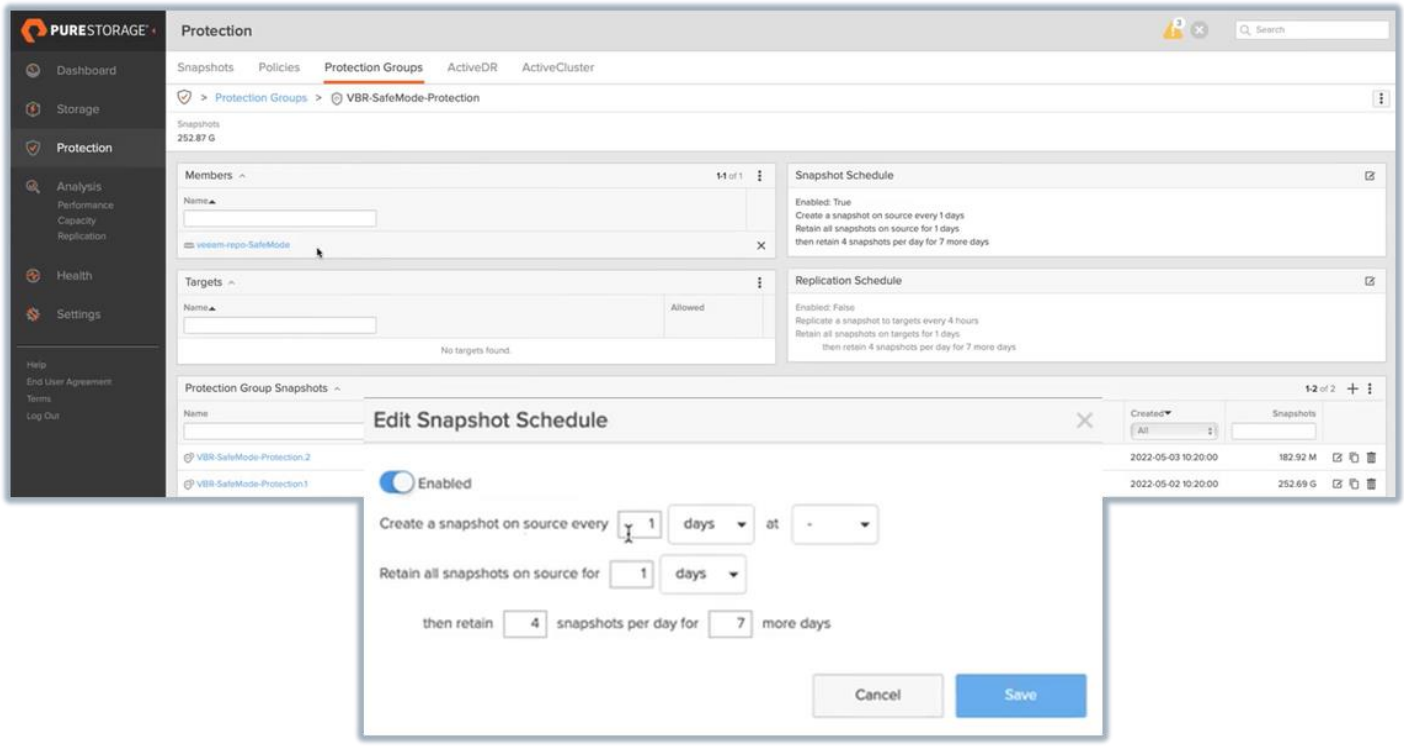
Rapid Recovery for Priority Systems

Pure Storage SafeMode with Pure FlashArray, Pure FlashBlade, or Pure FlashRecover prevents permanent loss of data due to admin mistakes or malicious attack including unalterable/immutable snapshots.

In addition, Pure FlashArray provides immutable protection (10 to 30+ days of production) and immediate snapshot rollback of production data or up to 8.7 TB per hour restore per FA//C. Pure FlashBlade provides immutable file system protection (0 to 400 days of database dumps and backups) and immediate file system snapshot rollback or up to 270 TB per hour restore at scale. And Pure FlashRecover, powered by Cohesity, provides immutable protection and recovery of 1000+ VMs in 3.5 hours or more than 1 PB per day.

Figure 4 shows the Pure Storage Protection screen where admins can setup SafeMode Protection Groups and add Members (in this case a Veeam repository). Next, admins can setup a snapshot schedule, including creating a snapshot source every day(s), etc., and retain all snapshots on source for X number of days.

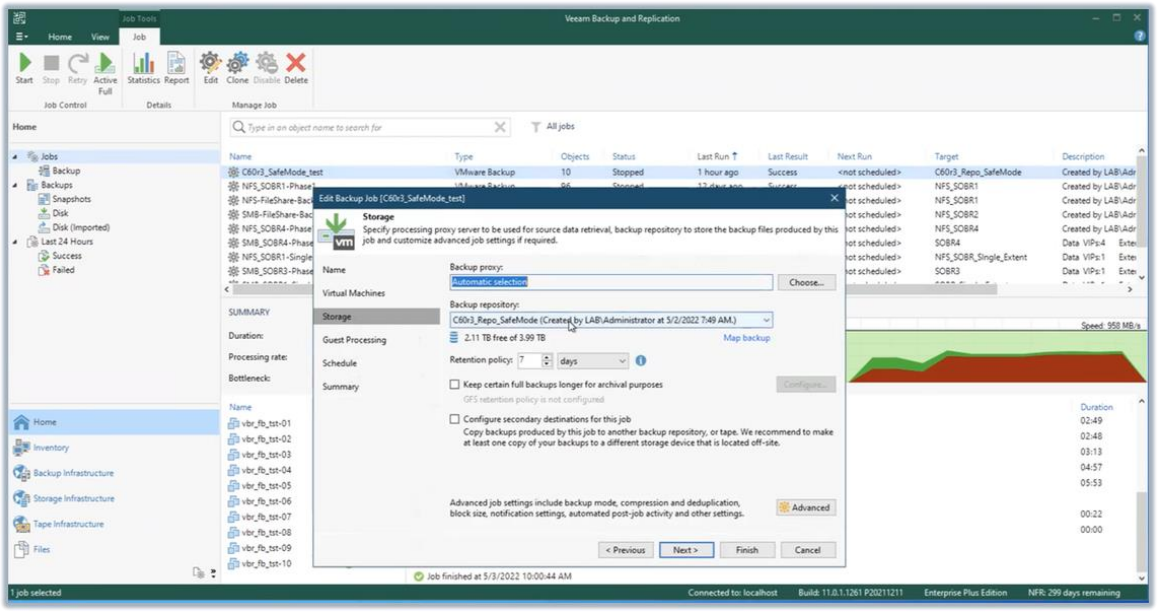
Figure 4. Setup of SafeMode Protection Groups



Source: ESG, a division of TechTarget, Inc.

Figure 5 shows the Veeam backup, including the backup proxy, backup repository, and retention policy (in this case seven days).

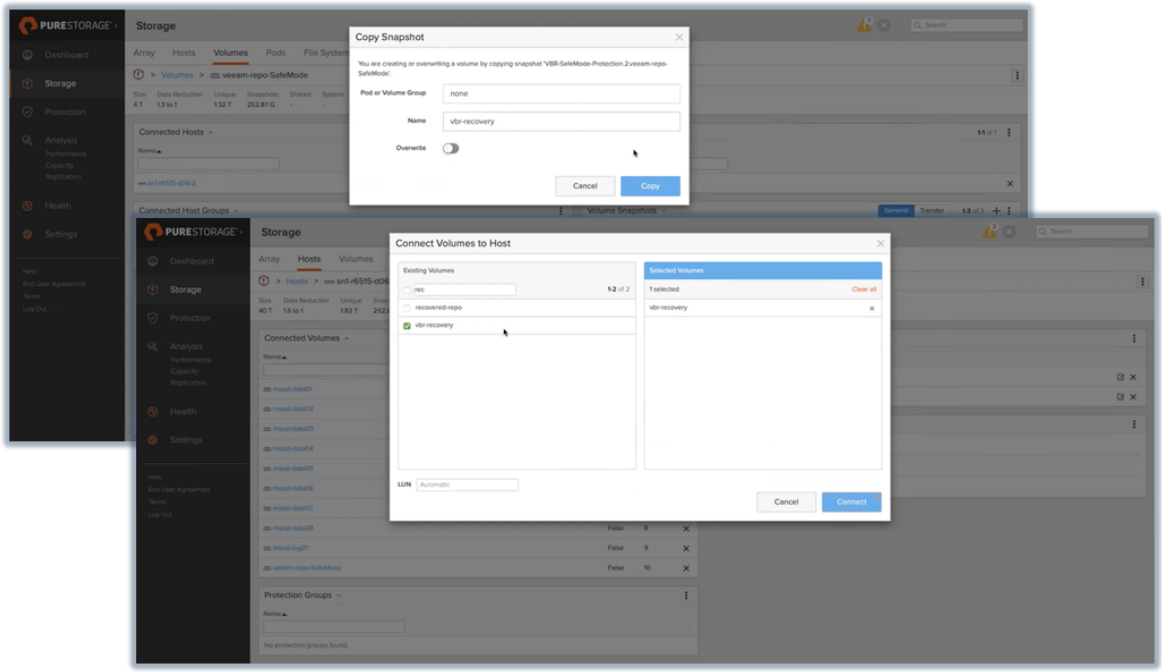
Figure 5. Veeam Backup Job



Source: ESG, a division of TechTarget, Inc.

For a ransomware scenario, Figure 6 shows how organizations can rapidly copy a snapshot to a regular volume and connect it to the host.

Figure 6. Rapid Recover Copy and Connect



Source: ESG, a division of TechTarget, Inc.

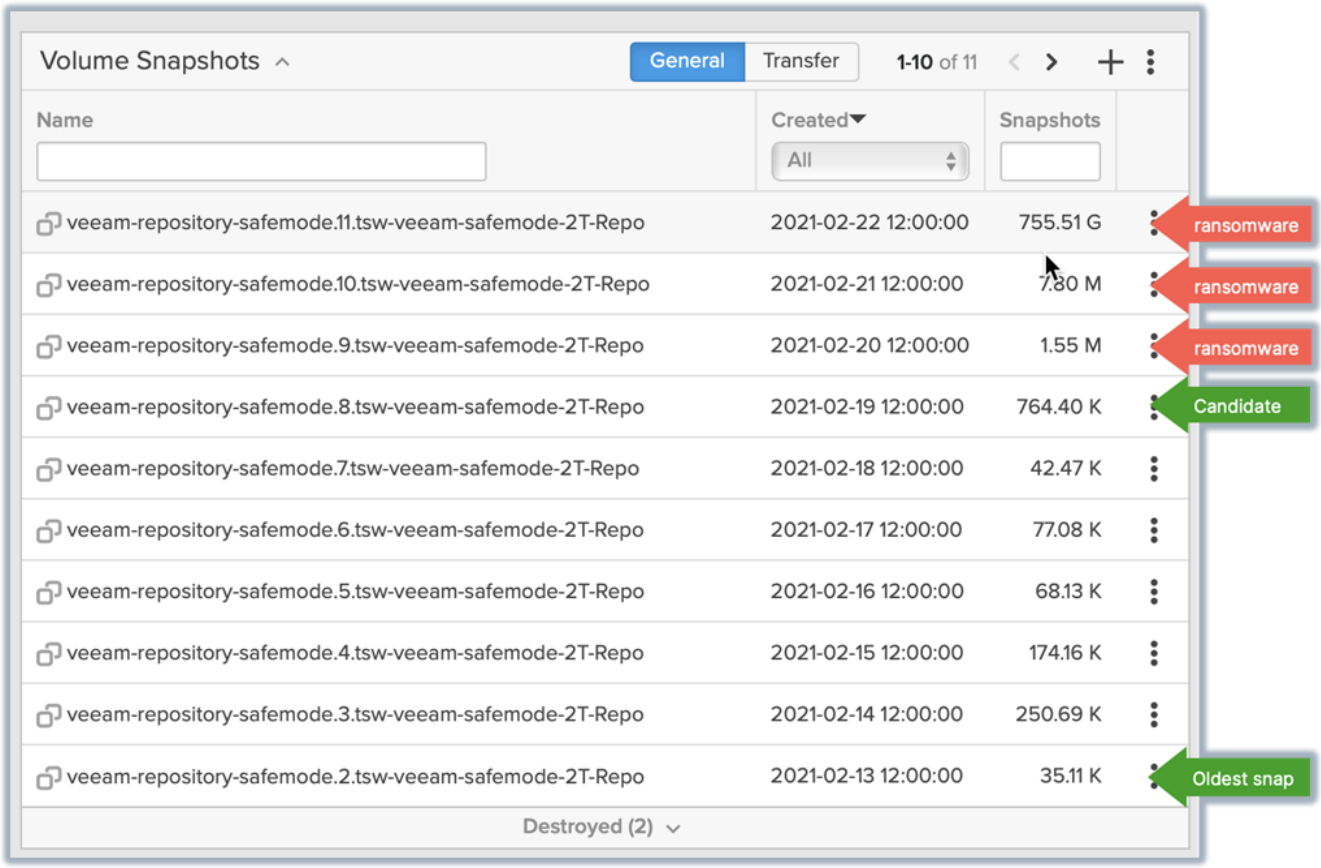
Why This Matters

Given the unabated increase in security threats, it's no surprise that improving cybersecurity was by far the most commonly cited response among research survey respondents (44%) when asked about the most important considerations for justifying IT investments in 2022. Pure Storage helps improve cybersecurity by providing rapid recovery for priority systems.

Support for Forensics with Space-efficient Snapshots

It is also important to have the appropriate sandbox environment available for forensic analysis of snapshots and backup data. Organizations can't just restore directly without performing a forensic review and cleansing to remove identified indicators of compromise left behind by the attacker. Having a solid logging environment in place that delivers the proper visibility will be critical through the restoration process. Pure Storage ensures that organizations have a starting point for recoverability and provides a fast recovery solution to get systems back up and running quickly (see Figure 7).

Figure 7. Analyzing Daily Repository Snapshots



Source: ESG, a division of TechTarget, Inc.

Why This Matters

The gravity of ransomware attacks makes blocking them a top business priority. After an organization is back up and running, it's important to review what happened, learn from it, and modify systems and policies accordingly so the organization can move on in an educated manner. This postmortem evaluation should look not only at technology, but also at people and processes. Pure Storage provides the capability to perform a forensic review to identify and remove any malware left behind by the attacker to enable a successful restore.

The Bigger Truth

Organizations should understand why and how ransomware attacks occur, including what to do before, during, and after an attack. This should help organizations be better prepared to prevent an attack from occurring or to recover quickly. These actions should also include using the right people, processes, and technologies. In addition, organizations should ensure that strong passwords are set and managed properly, as well as inventory software and assets to protect them and minimize the attack surface.

ESG's analysis of the Pure Storage ransomware solution demonstrated the capabilities to provide protection before, during, and after an attack, including offline restoration for malware cleansing, rapid recovery for priority systems, and support for forensics with space-efficient snapshots.

ESG a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188

© 2022 TechTarget, Inc. All Rights Reserved.