

MAY 2024

ExaGrid Retention Time-Lock for Ransomware Recovery

Craig Ledo, IT Validation Analyst

Abstract

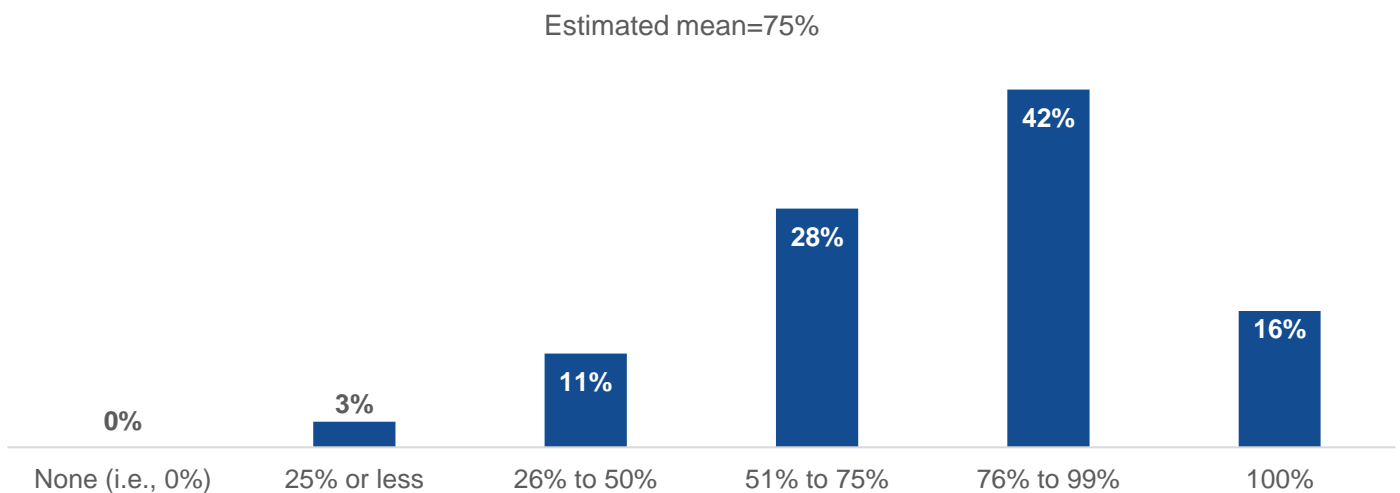
TechTarget’s Enterprise Strategy Group reviewed ExaGrid’s Retention Time-Lock (RTL) for Ransomware Recovery solution. We focused on the benefits RTL offers to organizations in terms of their readiness for ransomware attacks and security policies for data protection and recovery, including immutability (i.e., prevention of any deletion or alteration of volume, application, or database data).

The Challenges

Ransomware attacks continue to be pervasive, disrupting organizations operationally and financially. Three-quarters of organizations reported experiencing an attempted ransomware attack within the past 12 months, with 27% indicating that attacks happened on a weekly basis or even more frequently. Unfortunately, the current reality is bleak, as only 16% of organizations that were the victims of at least one successful ransomware attack reported that they were able to fully restore their data after a successful ransomware attack (see Figure 1). This highlights the need to reengineer recovery processes for ransomware attacks.¹

Figure 1. Typically, Not All Data Is Recovered After Ransomware Attacks

Approximately what percentage of your organization’s data was it able to recover after the ransomware attack? (Percent of respondents, N=354)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

¹ Source: Enterprise Strategy Group Research Report, [Ransomware Preparedness: Lighting the Way to Readiness and Mitigation](#), December 2023. All Enterprise Strategy Group research references and charts are from this research report.

This Enterprise Strategy Group Technical Review was commissioned by ExaGrid and is distributed under license from TechTarget, Inc.

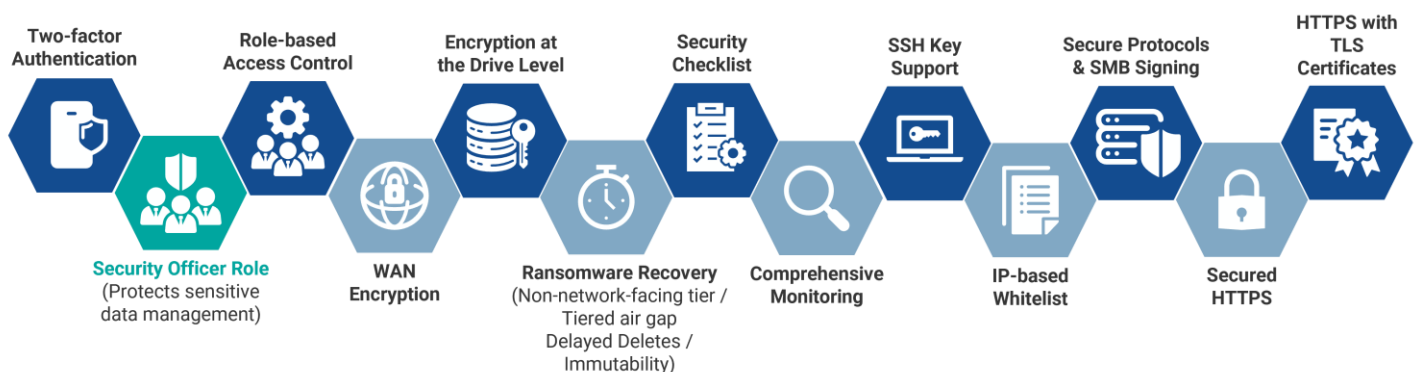
The Solution: ExaGrid Retention Time-Lock for Ransomware Recovery

ExaGrid’s ransomware recovery approach, RTL, prevents the threat of cybersecurity hackers maliciously deleting backups while still allowing for retention points to be deleted as normal based on backup application settings. ExaGrid provides Tiered Backup Storage with a front-end disk-cache Landing Zone and separate Repository Tier containing all retention data. Data is written directly to the ExaGrid disk-cache Landing Zone and is tiered into an immutable, non-network-facing, long-term retention repository where it is stored as deduplicated data objects. As data is stored to the Repository Tier, it is deduplicated and stored as immutable objects and metadata. ExaGrid objects and metadata never change, allowing only for the creation of new objects or deletion of old objects when retention is reached. Some ExaGrid key capabilities include:

- The ability to manage a single system instead of multiple systems for both backup storage and ransomware recovery.
- A unique and immutable second retention tier that is only visible to ExaGrid software—not the network—providing a tiered air gap between the backup infrastructure and the backup data.
- Delayed deletion of backup data by a configurable number of days, ready to be recovered after a ransomware attack is detected.
- Weekly, monthly, yearly, and other deletions to keep storage costs consistent with the retention periods set in the backup applications.
- A 10-day default policy for delayed deletes that only takes an additional 10% of repository storage space.
- Storage that does not grow forever and stays within the backup retention period set to keep storage costs down.
- Preservation of all retention data.
- Notification of unusual amounts of backup data deletion and notification of a reduction in deduplication ratio due to malicious encryption of enterprise or backup data.

Figure 2 shows the ExaGrid solution, which, in addition to its ransomware recovery capabilities, provides a comprehensive set of security measures to further protect backup data, including HTTPS with transport layer security (TLS) certificates, secured HTTPS, secure protocols and server message block (SMB) signing, IP-based whitelist, secure shell (SSH) key support, comprehensive monitoring, security checklist, encryption at the drive level, WAN encryption, role-based access control (RBAC), security officer role, and two-factor authentication.

Figure 2. ExaGrid Solution Overview



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group Validated

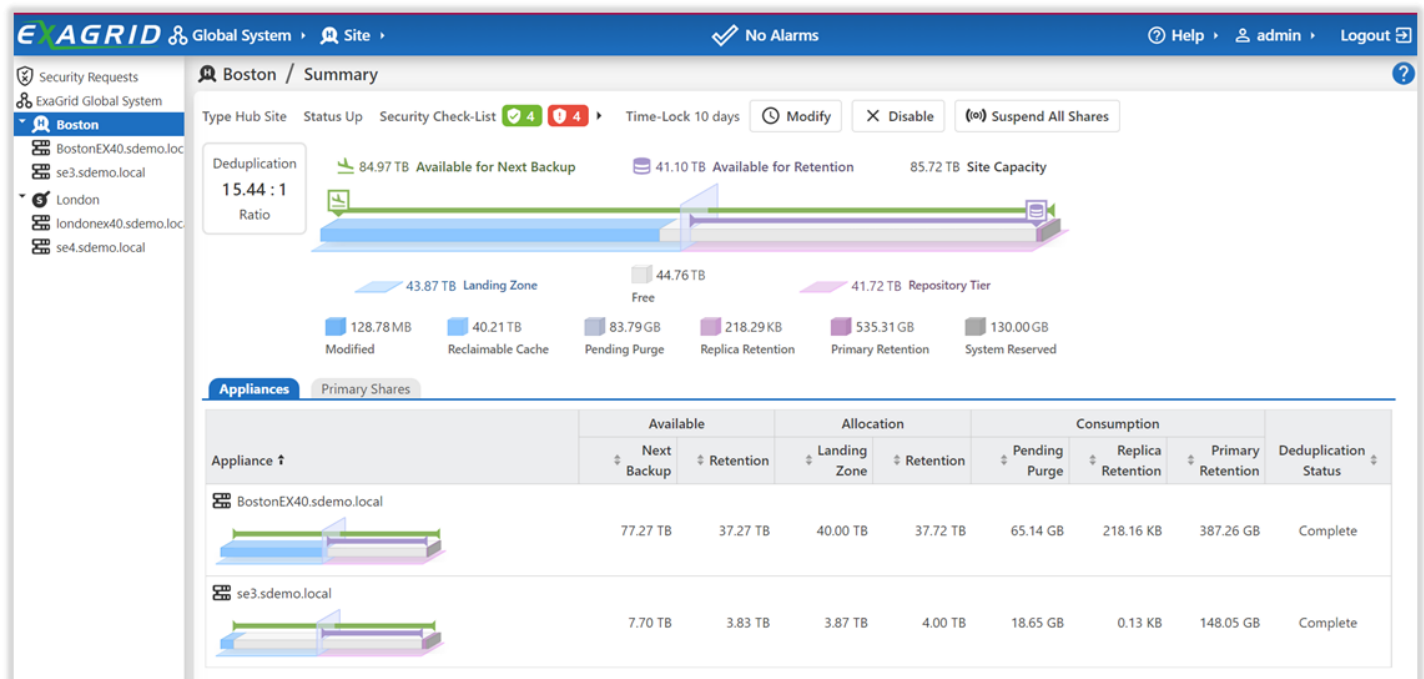
Enterprise Strategy Group validated ExaGrid’s RTL for Ransomware Recovery solution, specifically regarding the benefits RTL offers to organizations in terms of their readiness for ransomware attacks and security policies for data protection and recovery, including immutability.

Ensuring the security of data is crucial, and two key measures to achieve this are air-gapping and immutability. Depending on an organization’s needs, immutable backup/recovery solutions can be deployed on premises, in the cloud, or both. On-premises topologies offer a first line of defense and faster large restores because they leverage local networking and storage infrastructure. Additionally, compliance-related regional requirements may influence this trend. Organizations seem to increasingly favor a first line of defense for on-premises environments.

Specifically, we reviewed how organizations can recover from a ransomware attack when using ExaGrid and the Veeam Backup & Replication application, but the same steps are used with any of the leading backup applications supported by ExaGrid, including Acronis, Arcserve, Bacula, BridgeHead, Commvault, Dell NetWorker , HYCU, IBM, Oracle RMAN, Veeam, Veritas NetBackup, etc. ExaGrid supports over 25 backup applications and utilities listed on its [website](#).

Figure 3 shows the ExaGrid Summary screen. After logging into the solution, this screen shows how the capacity of ExaGrid is being utilized, including the available space left for backups, retention, and the overall site capacity. In addition, users can see their tiered backup storage capacity, including the disk-cache Landing Zone and long-term retention repository. The disk-cache Landing Zone allows for fast backups and restores, and the retention Repository Tier offers low-cost, long-term retention. This screen also shows that the “Time-Lock” is set to 10 days (the default setting). “Time-Lock” refers to the amount of time an organization has to detect a ransomware attack and then initiate a point-in-time recovery and restore.

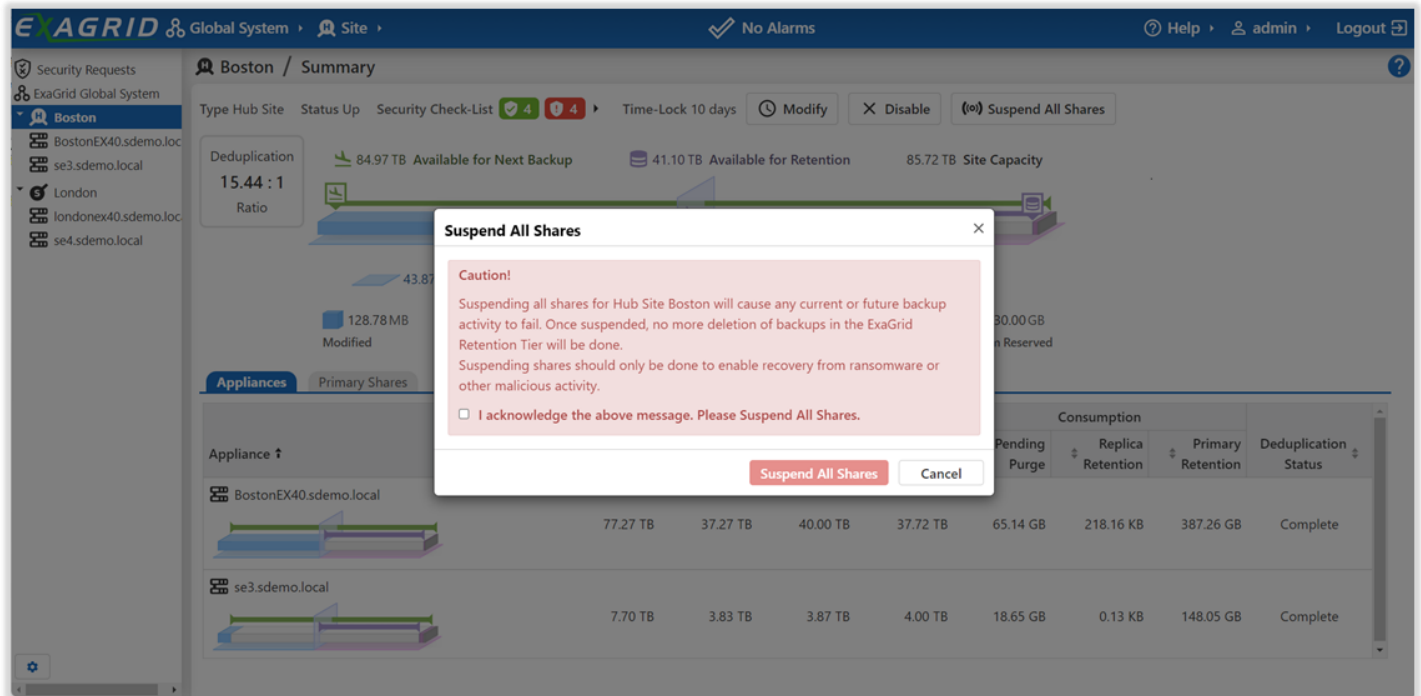
Figure 3. ExaGrid Summary Screen



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 4 shows ExaGrid suspending all shares at the point of a ransomware attack. This is based on the scenario where all the VMware backups were deleted on the Veeam Backup & Replication solution. In other words, there are no backups within Veeam that a user can do any restores from. In this scenario, the first step would be to “Suspend All Shares” to enable recovery from the ransomware attack.

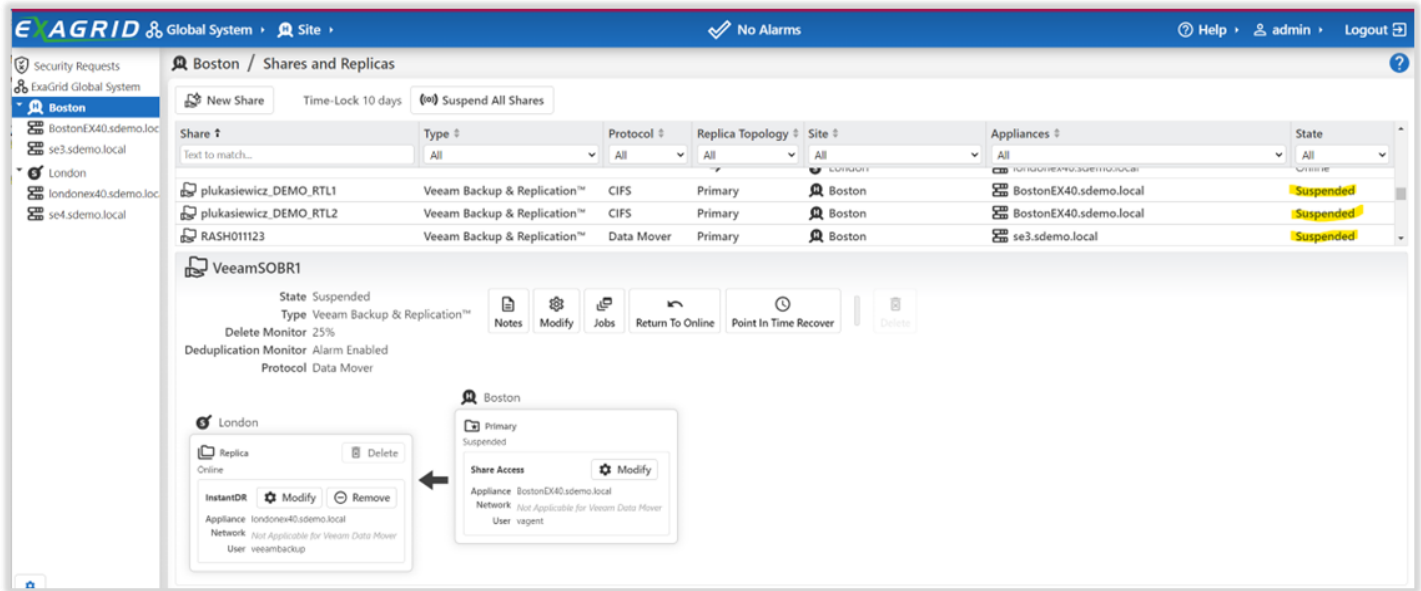
Figure 4. ExaGrid – Suspend All Shares



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 5 shows the ExaGrid Shares and Replicas screen. This screen now shows that all shares have been successfully suspended, which means they have been taken offline, giving the user time to assess, plan, and then start the recovery.

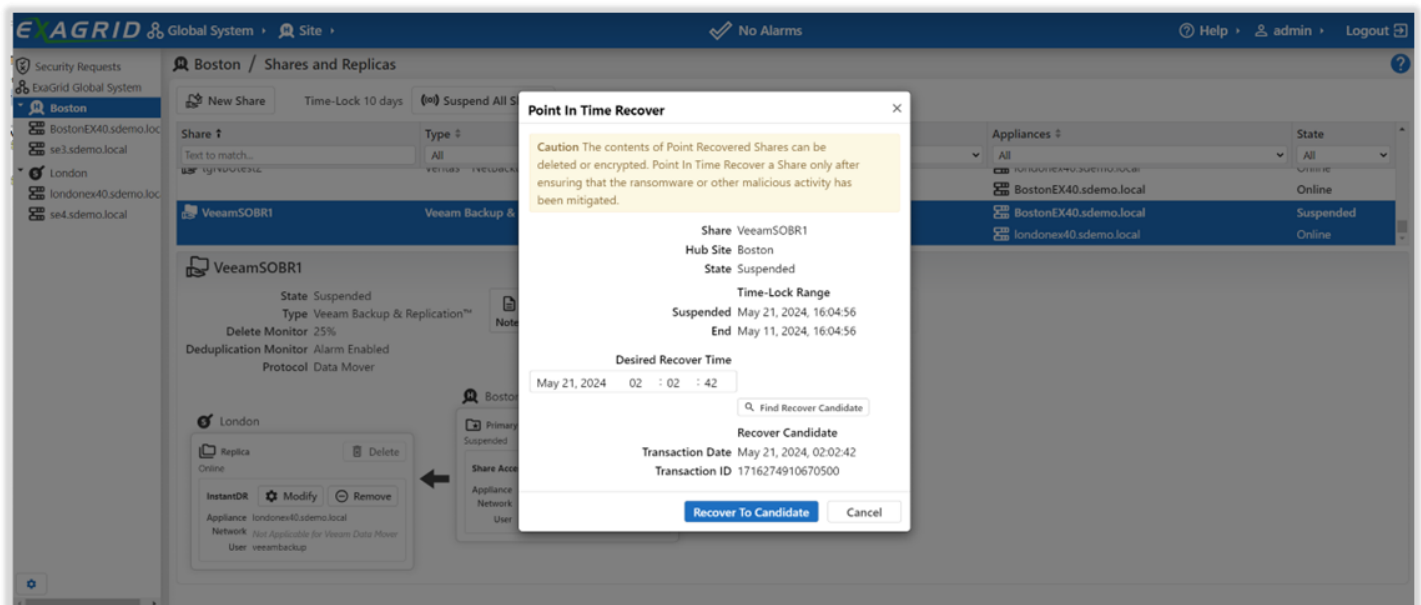
Figure 5. ExaGrid – Shares and Replicas



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 6 shows the ExaGrid Point in Time Recover window. Now that the point in time that the ransomware attack hit has been determined, a point-in-time recovery operation can be initiated by specifying the appropriate date and time. Please note that users should do this only after ensuring that the ransomware attack has been mitigated. In this scenario, we found an immutable backup in the retention tier that we could restore from.

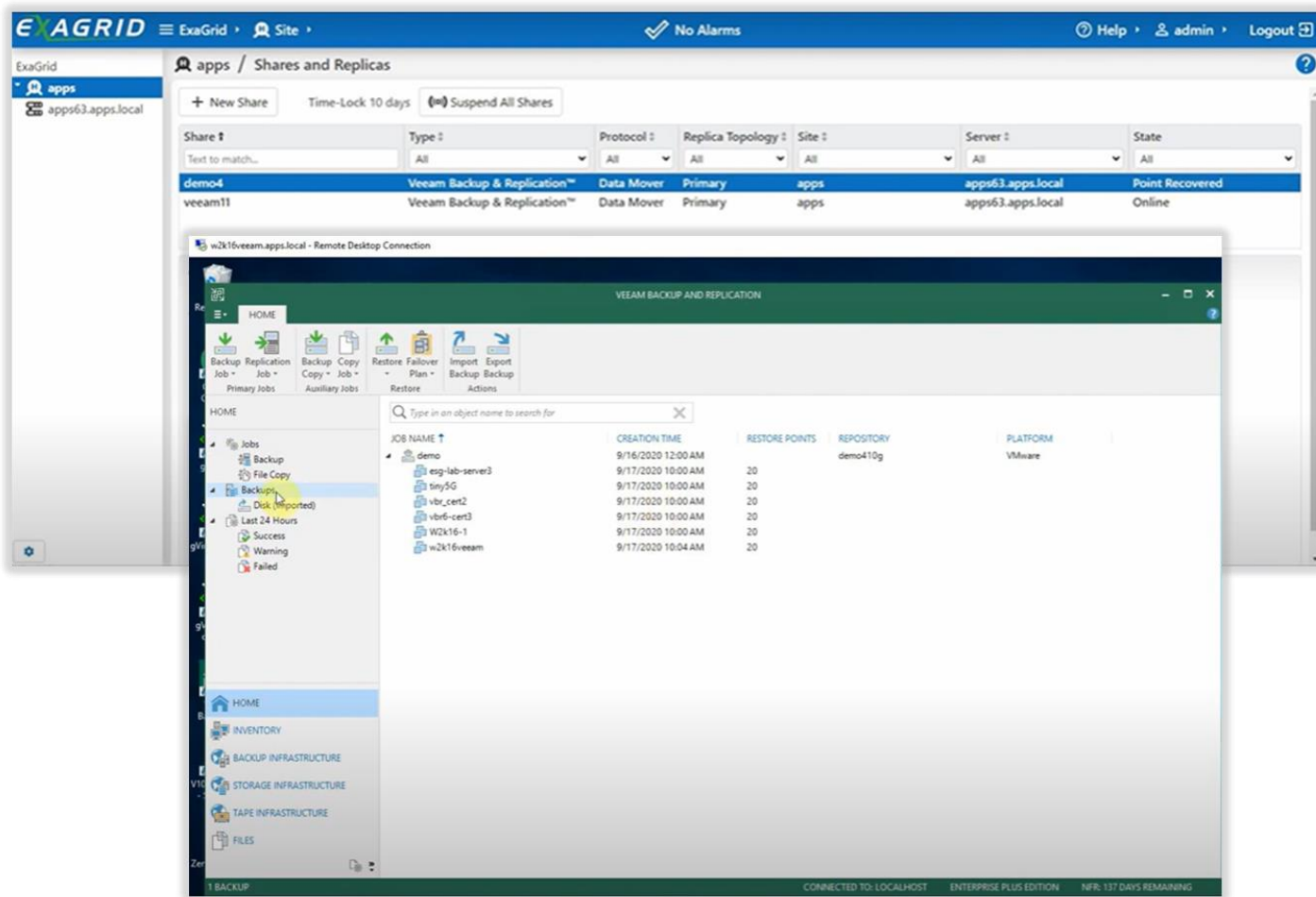
Figure 6. ExaGrid – Point in Time Recover



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 7 shows the ExaGrid Point in Time Recovered and also the Veeam backups recovered. ExaGrid enables backup applications to recover any backup data from any point in time prior to the ransomware attack. At this point, the user can go ahead and perform all of the Veeam operations, such as a boot or full restore. In addition, a user can restore other items and get the entire environment back up and running.

Figure 7. ExaGrid – Point in Time Recovered and Veeam Backups Recovered



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

Currently, 40% of organizations are protecting all their backup copies, while 77% of organizations use detailed backup scanning. Additionally, 58% have deployed air-gapping solutions to date, with another 30% either planning for or interested in this technology. When considering the technology and features currently needed to defend against ransomware, it is apparent that any solutions implemented must have a wide range of capabilities across many disciplines. In addition, ransomware attacks are on the rise, becoming highly disruptive and very costly to businesses. Quite often, these attacks encrypt primary data, take control of the backup application, and delete the backup data.

Enterprise Strategy Group validated that ExaGrid's immutable data deduplication objects and RTL approach prevents cybersecurity attackers from deleting backups. As we saw in this example, ExaGrid provides a strong data protection and recovery solution at a very low cost of storage. ExaGrid's approach to ransomware enables organizations to set up a "Time-Lock" period that controls the processing of any delete requests in the non-network-facing Repository Tier, which is not accessible to attackers. The combination of a non-network-facing tier, a delayed deletion of backup data, and immutable object storage are the key capabilities of the ExaGrid RTL solution.

Conclusion

Ransomware attacks pose a significant threat to organizations, yet in 2023, most organizations were not adequately prepared to deal with them. Enterprise Strategy Group research has shown a considerable gap between the average organization's preparedness level and that of the best-prepared ones. A closer look at readiness, prevention, detection/response, recovery, and business continuity reveals that organizations excel in prevention and response strategies but still lag in recovery strategies. For example, few organizations can successfully restore all of their data, and minimal progress has been made in the past 18 months on this front.

Data restoration difficulties are mainly due to the wide-ranging impacts of ransomware, which go beyond data-related issues, such as data exposure and data loss, to fundamentally affect business processes and operations with significant compliance exposure ramifications and the potential of financial and reputational loss. Cybercriminals are constantly adapting and targeting valuable or regulated data, as well as underlying infrastructure, to optimize their chance at extortion. This effort includes targeting backups.

Enterprise Strategy Group validated that ExaGrid's RTL for Ransomware Recovery solution offers organizations increased readiness for ransomware attacks, including security policies for data protection and recovery. Specifically, we validated how organizations can recover from a ransomware attack when using ExaGrid RTL and the Veeam Backup & Replication application. We validated the steps to recovery, which would apply to any backup application supported by ExaGrid, including suspending all shares at the point of a ransomware attack, determining the point in time that the ransomware attack hit, initiating a point-in-time recovery operation by specifying the appropriate date and time of an immutable backup in the Repository Tier that we could restore from, and then seeing that all backups were recovered.

In summary, ExaGrid Tiered Backup Storage, with its front-end disk-cache Landing Zone and separate Repository Tier, contains all retention data. All backups are written directly to the network-facing ExaGrid disk-cache Landing Zone, which provides fast backup performance, and the most recent backups are kept in their full undeduplicated form for fast restores. In addition, ExaGrid's immutability and RTL approach ensures recovery from a ransomware attack. If your organization is looking to increase its ransomware readiness, prevention, detection/response, and recovery, Enterprise Strategy Group recommends looking closely at the ExaGrid RTL for Ransomware Recovery solution.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.


Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com