Tintri VMstore Ransomware Recovery: Immutable Before It Was Cool

by DCIG Lead Analyst Storage, Ken Clipperton

Tintri

COMPANY

Tintri
9351 Deering Ave
Chatsworth, CA 91311
+1.650.810.8200

tintri.com

INDUSTRY

Data Storage

SOLUTION

Tintri VMstore

FEATURES

- Granular Data Protection
- Intelligent Integrated Analytics
- VM-level Management

BENEFITS

- Mitigates Ransomware Attacks
- Returns Applications to Service ASAP

This report focuses on the ways that the Tintri VMstore storage platform helps organizations recover from successful ransomware attacks.

These days, many people are concerned about supply chain disruptions. Indeed, this affects numerous businesses. Nevertheless, when it comes to protecting an organization from disruptions, ransomware is top-of-mind for many leaders. This is quite reasonable.

For many years, the most common cause of data loss or disrupted access to data was human error: the accidentally deleted file or folder, the botched upgrade, or a typo in a configuration script, for example. This includes even recent disruptions to major Internet-based services.

However, over the last several years ransomware attacks have increased to such an extent that they now comprise the greatest threat to an organization's data.

Assume a Ransomware Attack Will Succeed

Every organization needs to assume that ransomware attacks will succeed in evading the organization's cybersecurity protections. As with many aspects of security, protecting an organization requires successfully thwarting all attacks.

Protection that thwarts 999 out of a thousand attacks is a failure. For cybercriminals, the opposite ratio is true. Getting through an organization's cyber-defenses a single time after 999 failures is still a success.

> ***"Organizations must be prepared for the likelihood that their cybersecurity defenses will eventually fail."***

As news headlines suggest (and statistics from security organizations confirm), ransomware attacks have become a significant threat to nearly every organization. Therefore, business and IT leaders need to plan for this cyber-protection failure and implement a plan for recovering from such an attack. The right data storage technology will play an important role in successfully recovering and resuming normal operations.

Company Downtime is the Largest Ransomware Cost

The ransoms demanded by cybercriminals can reach into the millions of dollars. These ransom demands certainly make headlines. However, the largest cost associated with such an attack is actually application downtime that leads to business interruption.

Added up, the average total expense for operation recovery from a ransomware attack: $1.85 million.[1] And the largest expense, greater than the payout itself, is the median 21-day business interruption costs.[2]

On top of all of this, it is not uncommon for a business to lose C-level talent, lay off employees, or even close completely due to a successful ransomware attack. No wonder that nearly a quarter of all C-level IT leaders rank protecting their company against such things as their top priority.

Happily, the Tintri VMstore platform incorporates many technologies that reduce ransomware's impact.

Ransomware 2021

600%	Increase in malicious emails since COVID-19[3]
$170,404	Average mid-sized corporation payout[4]
$1.85M	Average organizational cost to recover
21 Days	Average company downtime from a ransomware attack

The largest cost—**Business interruption**

[1] https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 Referenced 8/12/2021
[2] https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 Referenced 8/12/2021
[3] https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542 Referenced 8/12/2021
[4] https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 Referenced 8/12/2021

Intelligent Integrated Analytics Reduce Ransomware Impact

A hallmark of the VMstore platform is its in-depth storage analytics. These analytics are not merely a management and visibility add-on. Rather, these analytics are inherent to the operation and adaptive autonomous management capabilities of VMstore.

The autonomous management capabilities were originally used to guarantee consistent sub-millisecond performance of every application. Now, they are being used to assist in identifying an attack, understanding its scope, and facilitating a rapid, precise recovery.

Tintri VMstore incorporates multiple capabilities that work together to facilitate rapid application recovery.

These capabilities include:

- VM-level Management
- Role-based access controls
- Attack identification through analytics
- Inherently invisible snapshot pointers and metadata
- Sophisticated snapshots
- Flexible replication options
- Granular policy-based data protection and recovery
- Near-instant recovery at the primary or DR sites

> *"Tintri's focus is to return applications to service as quickly as possible."*

VM-level Management Enables Applications to be Recovered ASAP

A key differentiator between Tintri VMstore and other storage products is that VMstore is uniquely designed to enable management at a per-VM level. Thus, the name "VMstore."

The significance of VM-based management is readily apparent to experienced storage administrators, and yet challenging to keep in mind. VMstore management is far more granular than managing LUNS, yet it is far less time intensive. And Tintri has now extended that management construct to include SQL databases and plans to do the same for containers.

When it comes to recovering from a data loss or cyberattack, this VM-based management infrastructure enables data to be protected and recovered on a per application basis. The key outcome from this difference is that it enables IT staff to return applications to service as quickly as possible.

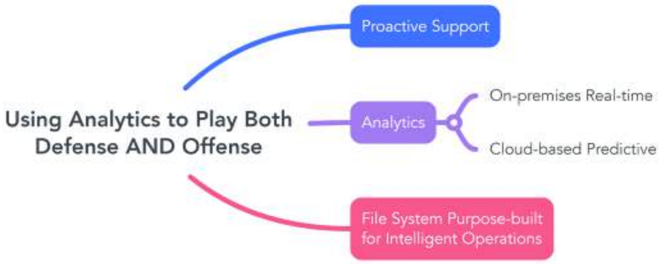
Role-based Access Controls

VMstore's Role-based access controls (RBAC) reduce the scope of a successful attack within the storage system. Rather than granting all or nothing access to the storage infrastructure, RBAC grants each individual or business process only the permissions it requires in order to carry out its tasks.

Supported roles include:

- Read Only
- Service Account
- Storage Administrator
- Super Administrator
- Database Administrator

Properly assigning these roles enables effective day-to-day delegation of responsibilities and empowers departmental personnel to accomplish their tasks. It also limits the impact of a breach of any of those individual's credentials.


Using Analytics to Play Both Defense AND Offense
Proactive Support
Analytics
On-premises Real-time
Cloud-based Predictive
File System Purpose-built for Intelligent Operations

Attack Identification

VMstore provides granular visibility into the performance and capacity used by individual virtual machines and SQL Server databases. Analytic views can easily be configured to show performance and capacity "movers" among an organization's applications. These views also make changes that fall outside the normal trend line readily visible.

Tintri Global Center (TGC) already uses this data for workload placement in multi-VMstore environments. It periodically analyzes the data that is always being generated by the running workloads and the available VM store resources. TGC then provides recommendations for moving workloads from one VM store to another. Along with the recommendations, TGC provides an "Execute" button that an administrator can click to implement the recommended changes.

Few, if any, other storage systems provide this granular level of visibility. In keeping with Tintri's intelligent infrastructure focus, Tintri plans to add alerts based on anomaly detection.

Inherently Immutable Snapshots

Some storage vendors are now adding features to their solutions to make them less prone to ransomware infection. Not so for VMstore. This protection is inherent to the VMstore architecture.

The metadata that VMstore collects in order to enable it's AIOPS capabilities is stored separately from the data. Due to the unique Tintri file system, snapshots are based on metadata pointers. This metadata is stored in a way that Ransomware is unable to make changes to it. The metadata and snapshots are also invisible to ransomware. Thus, VMstore was immutable before it was cool.

Sophisticated Snapshots

Many enterprise storage systems use snapshots as a data protection mechanism. So does VMstore, and VMstore snapshots are more capable than those of many other storage solutions.

Fast, non-workload-impacting snapshots. VMstore is among an elite group of enterprise storage arrays that provide fast, non-workload-impacting snapshots. These snapshots facilitate low-RPO backups and replication. In Tintri's case, they also enable rapid recovery of applications.

VMstore snapshots provide object-level granularity. The snapshots can be global, per-VM, and per-SQL Server Database. Per-VM snapshots make each vDisk individually actionable for cloning and restoring.

Being able to manage snapshots at this level of granularity is useful for many day-to-day operations. It is especially useful in providing targeted data restoration after a successful ransomware attack.

In most LUN-based environments, multiple VMs and applications share a single LUN. If one application's data must be restored, the entire LUN must be restored back to that same point in time. This consumes more time and affects more data than necessary as compared to restoring only the affected VMs.

Restore to any point in time, and even multiple points in time. VMstore supports more than 100 snapshots per protected object, and SyncVM allows recovery from multiple snapshots. With SyncVM, IT staff can test multiple recovery points to determine the best snapshot to use in recovering the application.

VMstore's space-efficient, time-stamped snapshots are pointer and metadata-based. Organizations that have experienced a successful ransomware attack can leverage these snapshots to enable forensic analysis after operations return to normal.

Policy-based data protection at scale. Many Tintri environments support more than 100,000 VMs, databases, or containers. The Tintri Global Center management application provides policy-based scheduling of snapshot and replication tasks. This enables an organization to apply consistent application-level protection by associating VMs with the appropriate policy. Enterprises can also manage data protection dynamically and at scale via PowerShell and REST APIs.

Efficient copy data management enhances agility. Enterprise can leverage VMstore's VM-centric, fast snapshot technology to accelerate application development. SyncVM can refresh production data to multiple development servers with minimal data movement.

SyncVM can eliminate the cumbersome, time-consuming, and difficult task of providing application developers with a complete and reasonably current data set against which to develop. In addition, VMstore's auto-QoS gives developers access to fast storage without putting the performance of production applications at risk. Thus, organizations can use VMstore to eliminate multiple overhead costs from the application development process, while improving development cycles and quality.

Invisible to ransomware. TxOS, the operating system that powers VMstore, internally reserves storage space for metadata. This metadata repository is not visible to applications, hosts, or clients. Thus, TxOS' pointer and metadata-based snapshot architecture is invisible to ransomware. This is important, because many ransomware attacks try to thwart data protection mechanisms and encrypt backups early in their attacks.

Flexible Replication

Tintri VMstore supports asynchronous replication with RPO/RTO via ProtectVM as frequently as 1-minute periodic intervals. VMstore supports high frequency snapshots for up to 200 key VMs with a 1 minute RPO; standard intervals are typically as frequent as 15 minutes. Additional replication capabilities include synchronous replication, one-to-one, one-to-many, and many-to-one. These replication options are primarily about enabling disaster recovery and business continuity.

Another replication option that most relates to ransomware protection is the VMstore's ability to replicate to S3 storage on multiple public clouds. Tintri has support in place with AWS, IBM, and Wasabi. The Wasabi option is interesting due to Wasabi's focus on performance, as well as the absence of charges associated with using or exporting the object data.

Replicating to S3 gets the snapshots out of the primary storage system, adding another layer of protection. Snapshots that have been replicated to S3 storage can then be restored to any VMstore appliance.

Granular Policy-based Data Protection Enables Near-instant Recovery

Because VMstore is architected from the ground up to manage VMs—and now SQL databases and containers—it is able to provide policy-based data protection and recovery at that same level of granularity. This enables Tintri VMstore infrastructures to resume normal operations in minutes or hours, not the 21-days of downtime that most companies endure following an effective ransomware attack.

Due to the prevalence of these attacks, Tintri added tools to automate recovery via scripts. This further accelerates application recovery, while reducing the likelihood of human error during said process.

Beyond Current Ransomware Mitigation Capabilities

Multi-factor authentication. In addition to existing role-based access controls discussed above, Tintri plans to further enhance security through multi-factor authentication. Multi-factor authentication (MFA) prevents bad actors from logging into the VMstore infrastructure, even if they have acquired the username and password of an administrator. It requires an additional mechanism to authenticate a login attempt, often by requiring a physical security key or phone with an authenticator application. MFA is a security best practice.

Alerting based on anomaly detection. Tintri plans to extend its intelligent infrastructure capabilities to include alerting based on anomaly detection. VMstore provides a robust core set of AIOPS capabilities that monitor and automatically optimize quality of service for each application. Detecting anomalies associated with cyberattacks and ransomware infection represents a natural extension of these AIOPS capabilities, addressing a concern that reaches all the way to the boardroom.

Tintri VMstore Provides Outstanding Ransomware Mitigation and Recovery

Ransomware attacks are getting measurably more sophisticated and accomplished each year. Thus, every organization needs to assume it will be the next target and plan accordingly. Those plans should focus on containing the ransomware infection, identifying affected applications, and then restoring those applications to normal operational status as rapidly as possible.

Tintri combines a full complement of enterprise-class data protection features that build on its inherent per-VM management construct to deliver exceptional ransomware mitigation and rapid recovery of applications.

Some might say that Tintri customers have an unfair advantage in sustaining their operations in the face of this ransomware threat. I don't call that advantage unfair. Rather, I suggest that Tintri offers its customers an intelligent advantage.

To learn more about how Tintri can advantage your organization, visit the Tintri website at www.tintri.com or contact your preferred Tintri value-added reseller. ■

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. More information is available at **www.dcig.com.**

DCIG

DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552