SOLUTION BRIEF

# Ransomware Protection & Recoverability for Cloud-Native Environments

## THE TRILIOVAULT DATA PROTECTION PLATFORM APPROACH ALIGNS WITH THE NIST CYBERSECURITY FRAMEWORK FOR COMPREHENSIVE RANSOMWARE PROTECTION

Cyber attacks are on the rise, painfully impacting governments, corporations and individuals around the globe. One recent ransomware attack led to the complete shutdown of the major US pipeline that delivers 45% of the fuel to the East Coast. The aftereffects of the attack went far beyond just fuel shortages, resulting in reputation loss, a fuel price surge, loss of revenue and countless other issues. Safeguarding against these attacks needs to be a top priority for all organizations today — and that's not something that can be accomplished with a single, one-size-fits-all approach.

The objectives of this solution brief are to:

- **Highlight** what ransomware is
- **Show** how ransomware attacks have matured over time
- **Provide** an overview of the NIST Cybersecurity Framework
- **Demonstrate** how Trilio aligns with NIST in its solution offering and technology approach

Ransomware attacks are a type of cyber attack where malicious actors and organizations use software to gain unauthorized access to data, encrypt it and then hold it ransom. The attackers then demand a fee, typically paid in crypto currency, before they'll release the data back to its owners. However, there's no guarantee that the attackers will hand over the data when they get paid. As a result, any ransomware attack could lead to permanent loss of vital data.

The threat of ransomware is not new. The first recorded ransomware attack was in 1989 and ever since then, the attacks have become increasingly prolific, specialized, hard to detect and hard to evade. Ransomware attacks mostly focus on enterprises where they have a much higher chance of a significant payout (though they frequently start off by compromising individuals with useful credentials in order to gain access to a larger organization).

The sheer number of ransomware attacks that happen each year is enormous — close to 300M cases. According to the 2021 Unit 42 Ransomware Report, the average cost of a single ransomware attack has increased 171% to $312,493 in 2020. As the Coronavirus pandemic accelerated businesses' digital initiatives, the number of ransomware attacks have rapidly increased as well. During the first few months of the pandemic, attacks were up by 72%. The increased access to business data over mobile devices during the pandemic drove mobile vulnerabilities up by 50%. The opportunity for ransomware attacks keeps growing, as does the damage in terms of proprietary information, reputation and revenue lost on a regular basis.

Enterprises and organizations alike understand the damage caused by ransomware and have come up with various strategies to mitigate and facilitate recovery. However, the attacks have become smarter and more specialized over the years. Based on a recent Gartner report, ransomware attacks generally start with network penetration. After gaining entry, attackers patiently wait inside the networks to capture privileged credentials that will give them access to sensitive accounts and domains. Keeping backup copies of data and "point-in-time captures" is the most effective means of thwarting ransomware attacks, since there's no need to pay to recover data if there's another copy of the data safe and sound. However, attackers can also target the backups.

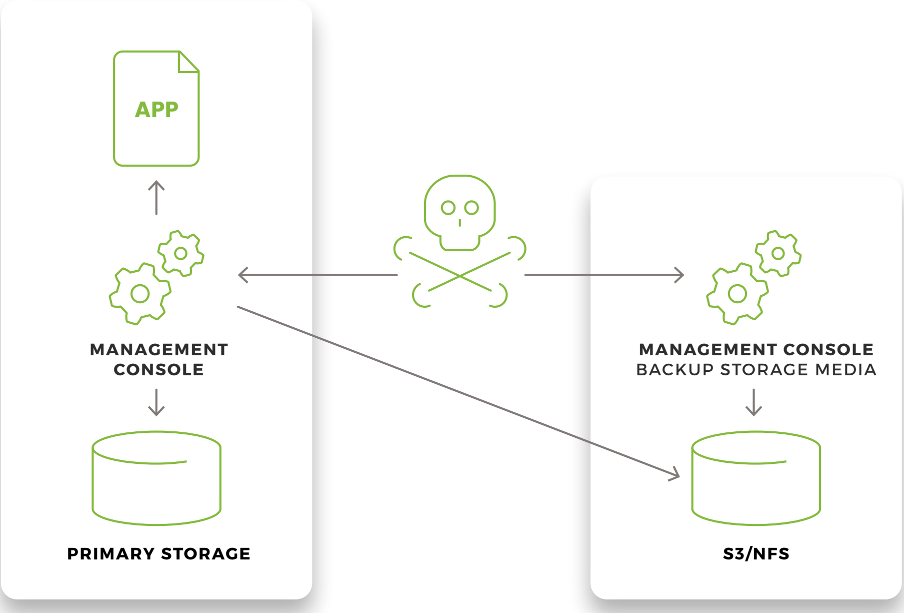
Attackers frequently try to penetrate the backup system either through the administrative console or the storage media itself in order to access and delete point-in-time data. This greatly inhibits an enterprise's ability to restore business operations after their data is held ransom. With the push to machine learning and AI, the data itself is now being stolen from organizations via primary and secondary storage domains. As a result, organizations can lose data and not even know about it until later.

### 2 Entry Points of Attack

1. From the K8s/backup management console

2. From the storage media (where backups are stored) console

**Ensuring data cannot be altered in the S3/NFS storage if a malicious user gains access via the primary or backup infrastructure is the immutability goal of TrilioVault for Kubernetes (TVK)**



TrilioVault safeguards secondary (backup) storage while also detecting issues at the primary storage level.

## TRILIOVAULT'S CLOUD-NATIVE APPROACH TO RANSOMWARE

With the threat of ransomware rising, Trilio has listened to the needs of its customers and partners and decided to take on the challenge of ransomware protection. Trilio will enhance it's TrilioVault cloud-native data protection platform to offer users a comprehensive approach to ransomware protection and recoverability.

Trilio recognizes that ransomware protection is more than just a single software feature. It's a set of features, tools and processes that organizations need to adopt and follow in order to stay safe. Consequently, Trilio will provide nothing less than a comprehensive ransomware protection strategy enabled by its TrilioVault technology platform.

Trilio is leveraging the NIST (National Institute of Standards and Technology) Cybersecurity Framework to align it's capabilities and approach. The NCCoE (National Cybersecurity Center of Excellence) at NIST "data integrity project" details ransomware protection best practices aligning to the NIST framework. Trilio is aligning its technology to those best practices in order to meet NIST standards.

The main components of the NIST Cybersecurity Framework are Identify and Protect, Detect and Mitigate and Recover. Here is what they require from a backup perspective:

- **Identify and Protect**: Organizations must create an inventory of all of the assets they need to protect and ensure that there are no potential vulnerabilities in the environment. This means making sure that all applications are discovered and protected and that there are no zero-day exploits hidden in the management domain that could compromise the storage behind it. It also means instituting Role-Based Access Control (RBAC) to reduce the attack surface and protect the backup storage media from being altered or compromised from outside.

- **Detect and Mitigate**: Organizations must be able to identify when attacks happen and mitigate them before they propagate through the environment. The backup technology must be able to identify or flag as early as possible any scenario where the data might be compromised. Once detected, any further data manipulation or theft needs to be stopped through access controls.

- **Recover**: Once an attack has been identified, an organization must be able to recover from it. This means being able to quickly point to uncompromised backups and use them to restore business operations. This should occur first in an isolated environment to validate and then within the production environment.

With this framework and best practices, Trilio has mapped a comprehensive set of features essential to minimizing and completely eliminating ransomware attacks within an organization. Some features are available today, while other features will arrive in the coming months as part of the TrilioVault for Kubernetes roadmap.

TrilioVault for Kubernetes features and descriptions are outlined in the chart below:

## Identify & Protect

- **Application Discovery**: Discover all applications to make sure they're protected.
- **Security Validation**: New technology validated by industry leaders.
- **Backup Immutability**: TVK supports multiple platforms that store data to support WORM.
- **RBAC**: Control user access to shrink penetration surface.
- **Encryption**: All backup data is encrypted.
- **2FA/MFA**: Authentication requirements to prevent manipulation of backups via backup management console.

## Detect & Mitigate

- **Abnormal Events**: Deep analytics on top of backup data to help understand abnormal events.
- **Containment**: Revocation of service accounts when abnormal events are detected.
- **Malware Scanning**: Automatic scanning of backup images to check for malware on production data.
- **Notifications and Alerts**: Automatic notifications directly integrated into popular platforms.

## Recover

- **Deep Logging**: Faster backup and identification using keyword-based triggers.
- **Isolation Testing**: Single workflow for testing backups in isolation prior to recovery.
- **DR Workflow**: Single workflow for restoring applications and data to production.
- **Multiple Targets**: Increase recovery surface by storing multiple backups on multiple target types and on multiple targets.

Trilio takes the security of its products and the protection of customer data seriously. Trilio is committed to the challenge of solving the exponentially growing problem of ransomware attacks — and intends to do so in the most complete manner possible.

TrilioVault for Kubernetes offers features that enable protection and recovery from ransomware. Trilio will continue hardening and enhancing this platform with additional features to better align with NIST and the NCCoE framework and best practices guidelines. By leveraging these industry standards, Trilio will give its customers the peace of mind that comes from knowing that Trilio's enterprise-class technology is running continuously to keep their environments safe and protected across potential attack vectors.

## About Trilio

Trilio is a leader in cloud-native data protection for Kubernetes, OpenStack and Red Hat Virtualization environments. Our TrilioVault technology is trusted by cloud infrastructure operators and developers for backup and recovery, migration and application mobility. Customers in telecom, defense, automotive and financial services leverage TrilioVault to recover from disasters, migrate workloads, move workloads to new infrastructure and migrate to new software distributions.

WWW.TRILIO.IO