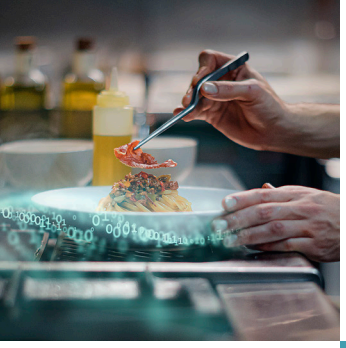
EBOOK

# Ransomware in the Cloud: Prevention and Remediation with NetApp Cloud Volumes ONTAP



## Introduction

A recent wave of severe ransomware attacks have targeted major US governmental IT platforms, costing those municipalities and the federal government billions of dollars in order to recover their systems.

Ransomware is an increasingly popular form of modern cyber attacks that can have a crippling effect on any organization. While all cyber attacks can be damaging, Ransomware attacks could be more damaging due to the fact that they target the most valuable property of these modern organizations: their data. Not being able to access critical data can wreak havoc for any organization and the impact could be severe not just for the organization itself but also on their end customers.

With the increasing adoption of public cloud IT platforms to underpin IT operations by many organizations, it is important to understand the threat of ransomware in the cloud and considerations for preventing and mitigating against such attacks.

In this guidebook, we'll take a closer look at the impact of ransomware attacks and how organizations such as governmental bodies can keep their data in the cloud safe and out of harm's way through the use of NetApp Cloud Volumes ONTAP.

# Table of Contents

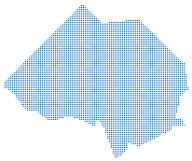
# What Is Ransomware?

Ransomware is a malware program created with malicious intent, for the purpose of restricting or preventing the use of a business's system, application, or solution until a ransom is paid. Out of the two main types of ransomware commonly seen, crypto ransomware (a.k.a. encrypted ransomware) has easily become the most popular type of attack used against various enterprises in the recent past. A crypto ransomware typically encrypts system resources such as valuable files or the entire content of a disk drive to prevent users from accessing it. The organization affected would typically have to resort to paying a ransom to regain access to the data or recover their data files from backups. This can be extremely costly and time consuming, or at times even be impossible if a well implemented backup and data protection solution was not in place.

Many organizations across all sectors have become increasingly reliant on digital assets and that has been providing an ever-increasing target market for ransomware attackers. The evolution of ransomware has significantly increased over the last five years, and in Q2 of 2019 alone, the average ransom payment has increased by 184% based on research carried out by ransomware recovery experts CoveWare.

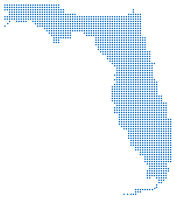
## A Serious Uptick in the Ransomware Threat

Ransomware has been a threat that enterprises have been hearing about for years, but a recent string of high profile attacks on major governmental and enterprise operations demand some renewed attention be paid to this potential threat.



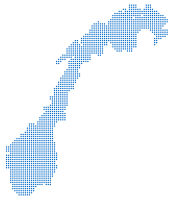
### $400,000 paid by Georgia's Jackson County

In March 2019, hackers locked out the local Georgia county government from their IT systems using Ryunk, a variant strain of the widespread Ryuk ransomware, taking crucial county services entirely offline. Luckily, the attack did not affect the 911 system, but nearly all other systems were offline, forcing officials to return to a paper-only record based system, slowing operations to a crawl. To regain their systems, Jackson County decided to pay the ransom of $400,000 to the hackers.



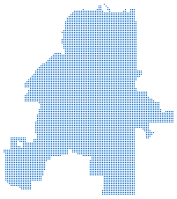
### Florida Cities Pay Combined Ransoms of Over $1 Million

In one week in June 2019, both Lake City and another city in Florida paid hackers a combined $1.1 million to release their frozen IT systems infected with ransomware. Lake City's equivalent $600,000 payment in Bitcoins was one of the highest ransoms that has ever been paid out to free an impacted system, a devastating sum for the small city.



## Norweigian Industrial Firm Attacked

Major industry can be as important to a nation as its governmental services. Such is the case with Norsk Hydro, the Norweigan aluminum manufacturer, which was recently the target of a vicious ransomware attack that has cost the company over $57 million. The ransomware that targeted Norsk Hydro originated within the United States. While this attack has been a huge financial blow to the company, what Norsk Hydro didn't do—give in to the ransom demands—has garnered them praise. Norsk Hydro had to resort to manual processes to function, and it's insurance has not covered anything close to the total losses.

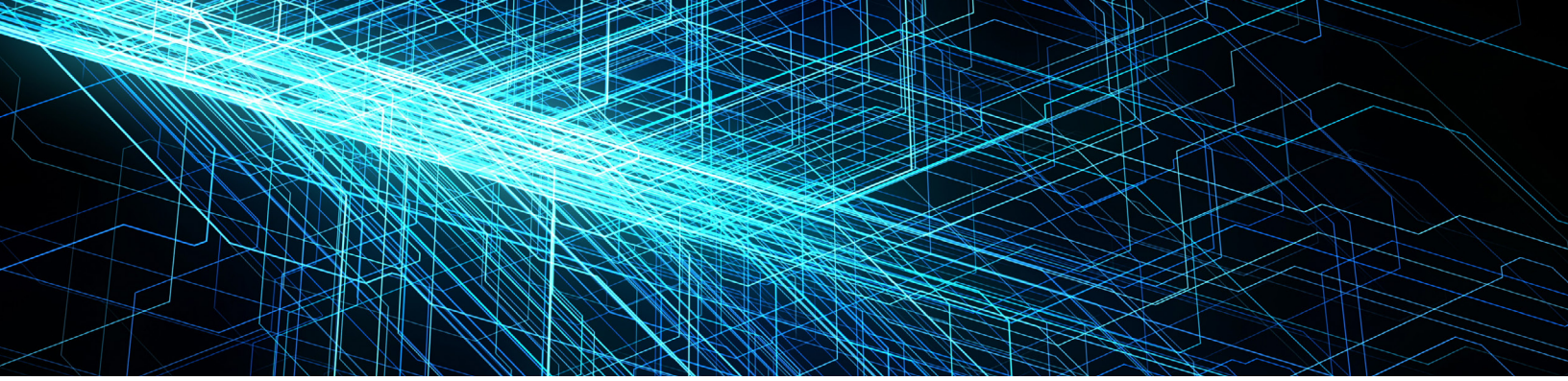


## Major US Metropolis Atlanta Opts to Recover and Pays

Atlanta was struck by the SamSam ransomware in March 2018, but unlike the smaller municipalities that have recently been hit by ransomware attacks, the administration decided that they would not pay the ransom of close to $50,000, considering it to be akin to negotiating with terrorists. However, due to inefficiently configured recovery systems, restoring their full operations has not been possible and costs have run into the millions of dollars. At the same time, hundreds of the city's systems remained offline months after the lockout and may never be fully recovered.

By nature, most governmental organizations are under high level of public visibility and also subject to more public and political scrutiny. Many of these organizations such as health or security services are not just organizations but are a part of a critical public infrastructure. If these organizations are unable to provide these critical public services effectively due to a ransomware attack crippling their core IT infrastructure, the impact of that can be felt rapidly and can have lasting political impacts. While there has been a recent push to avoid making ransom payments, recovery costs have skyrocketed, as in the case of Atlanta (see above).

The financial impact of a ransomware recovery can also be felt significantly more severely by these government bodies in comparison to enterprises. IT departments of government bodies are often cash strapped due to various reasons such as reduced federal funding and other budget priorities. Ransom payments such as those forced to pay by Jackson County and Lake City in Florida as well as the additional recovery costs incurred by the city of Atlanta can have a lasting impact on the budget priorities and has the potential to deprive their many of their citizens of vital public services as a potential consequence.



# The Impacts of a Ransomware Attack

The true impact of a wide-spread ransomware attack is difficult to be quantified accurately. The infamous NotPetya ransomware that affected a number of global organizations such as Maersk, Saint-Gobain, Mondelez International, Merck & Co., and others in 2017 was estimated to have cost over $10B in various damages in total.
However, at a high level, some of the key impacts of a wide scale ransomware attack can be grouped into the following categories.

COST OF DOWNTIME | COST OF RECOVERY | REPUTATIONAL DAMAGE

## COST OF DOWNTIME

Some of the most significant costs to any organization undergoing a ransomware attack are due to loss of revenue due to systems being offline. For example, the 2017 global cyber attack that caused the spread of the ransomware Wannacry reportedly estimated to have cost the UK government's National Health Service up to £20m ($25m) worth of lost revenue.
This was due to 19,000 cancelled appointments as a result of 200,000 infected computers not being accessible for over seven days.

In an increasingly digital world, where enterprises are starting to rely on digital technologies to offer always on revenue streams, the potential for such downtime can raise these costs significantly higher. When it comes to organizations such as governmental, medical, and emergency services, such downtime has the potential to cause damages beyond just a financial loss and into physical damages, affecting the normal operation of major cities or even states.

## COST OF RECOVERY

In relative terms, a major organization might consider this the smallest portion of the overall cost of a ransomware attack. Recovery costs will include the cost of ransom payments as well as other additional recovery activities related costs. Ransom demands can vary depending on the type of the ransomware and the nature of the attackers, resulting in thousands of dollars to millions of dollars in some cases such as this local government organization example.

Better prepared organizations can sometimes avoid this cost altogether by opting to restore affected data from backups and not paying the ransom demands. Recovery costs can include forensic investigation costs, data recovery costs, and subsequent increased IT support costs during the whole recovery process which in itself can run into hundreds of thousands of dollars, depending on the size of infection.

## REPUTATIONAL DAMAGE

On one level, this might be the most significant cost an affected organization will have to endure due to a ransomware attack. Organizations with established brands will often incur public reputational damages and the financial impact of such damage can be often difficult to be quantified upfront. It was estimated that during the 2017 NotPetya ransomware cyber attack, UK based consumer goods conglomerate Reckitt Benckiser lost around 2% of its share price value within a day after the news of the attack broke out. Customer's as well as Investor's trust of these global brands can take a severe toll if they are deemed to be ill equipped to avoid, or recover from such malicious attacks swiftly.

When it comes to governmental bodies that lose control of their operational abilities, this loss of confidence can be less financial and more dangerous to consider, which may be in line with the goals of the initial attack.

# Ransomware and Cloud Storage

With the implosion of public clouds over the recent years, many enterprise organizations have started building in cloud computing as a key part of their IT strategies. Due to the inherent nature of public cloud IT, where the underlying infrastructure is secured and managed by the cloud service provider, many customers somewhat incorrectly assume that the threat of ransomware in the cloud is less than in a private data center that is managed by the end users themselves.

When it comes to the majority of cloud workloads that operate on Infrastructure as a Service (IaaS) today, this is far from the truth.

All major cloud platforms operate on the basis of a shared responsibility model when it comes to security and compliance of the services they offer.

The AWS shared responsibility model for example, clearly declares the boundaries of security responsibilities: AWS maintains the security of the underlying cloud platform itself, while the users who subscribe to their services are still held responsible to maintain their own security measures to safeguard their data.

Microsoft Azure has a similar shared responsibility model for Azure Cloud which clearly advise that ensuring data accountability, end-point protection, identity and access management and application level controls for a safe computing environment on Azure is the responsibility of the customers.

Similarly, Google Cloud also advises customers to ensure that customers of Google Compute Engine and Google Kubernetes Engine are responsible to maintain the VM operating systems and applications up to date in order to avoid potential infections such as ransomware, as a part of their shared responsibility model.

This shared responsibility model is especially relevant when customers consume IaaS services such as Azure Virtual Machines or AWS EC2 resources to run virtual data centers in the cloud by provisioning virtual machines. Similar to a private data center, customers have unrestricted access to the VM's and their guest operating systems which means issues such as patching are just as important, yet just as complicated as in a private data center.

Due to this situation, all IaaS compute platforms in the public cloud are equally susceptible to ransomware infections and prevention and remediation remains the sole responsibility of the customer and not the cloud service provider.

Furthermore, most of these IaaS compute subscriptions aren't managed by local IT teams and are instead owned by various line of business owners or developers. This shadow IT can not only increase the chance of inadvertent ransomware infections on the cloud platform of their infrastructure, but can also run the risk of introducing these back into the corporate data centers during various data synchronization between the two platforms.

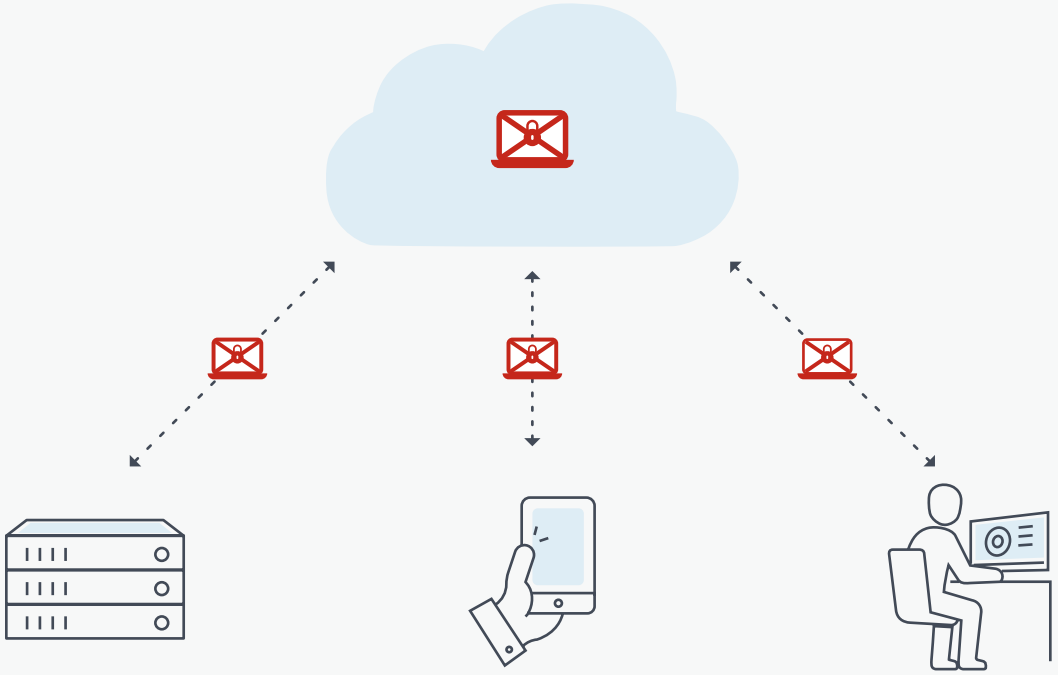
## Shadow IT

Also known as stealth IT or Client IT, Shadow IT refers to IT technologies signed up to, deployed and in use within an organization by someone other than the designated IT department. Shadow IT has become a serious problem in large governmental and enterprise organizations in particular, especially since the widespread use of cloud technologies where anyone, such as a developer or a line of business owner (LOB) can easily sign up to and consume these services, bypassing corporate IT teams and their policies.

- Easily signed up for or implemented by any team member.
- Carry the risk of not being compliant of security and best practice policies.
- Often unsupported by the IT and information security teams.
- Potential additional costs and resource use.

In 2016, a Netskope security report identified that 43.7% of malware found in the cloud is carrying a ransomware. Preventing ransomware infections on these cloud platforms require similar laborious tactics as in the corporate data center, such as installing ransomware protection software on all virtual machines. In addition, customers would also need to ensure that dedicated backup and recovery solutions and processes are in place to protect and secure the cloud data in order to swiftly recover from a possible ransomware infection.

Even some of the cloud-based Software as a Service (SaaS) solutions such as Google Drive, Microsoft OneDrive, or Dropbox are not immune to the threat of ransomware. These services relies on synchronization of data from across multiple platforms, from on-premises data centers to end-user devices and cloud platforms, and if ransomware encrypted data enters into that synchronization chain, the same unreadable data will now run the risk of being propagated across the cloud backend too.



In summary, most prevention, detection and remediation requirements for ransomware applies equally to public cloud as in the customer owned data center environments. Therefore, customers must seriously consider having appropriate preventive, detection, and remediation measures in place using native solutions available via the cloud platforms or third-party solutions via cloud marketplaces to ensure the safety of their critical data from ransomware infections.

# How to Prevent and Remediate Ransomware Attacks

In order to understand how to prevent and remediate ransomware attacks, it is important to understand how and when these infections commonly occur. Ransomware infections typically happen to an organization via various vectors such as URL downloads, direct ransomware files, exploit kits, and infected USB flash drives.
Once the ransomware has entered the system using these means, one of the most common exploits include unpatched servers and workstations.


URL Downloads

Direct Ransomware Files

Exploit Kits

Infected USB Flash Drives

The most effective way for an organization to counter this threat is through a complex, layered defense (a.k.a. Defense in Depth). Such a layered defense would typically begin with preventive measures to reduce the attack surface and prevent known and unknown infections. These would typically include steps such as:

**Define** organizational processes, policies, and procedures to enforce information security and up to date defense mechanisms.

**Equip** with specialist endpoint protection solutions such as antivirus solutions with malware protection capabilities.

**Harden** networking security solutions such as firewalls, intrusion detection and prevention systems, as well as web and URL filtering solutions.

**Enable** access control solutions that perform actions such as dual-factor authentication, role-based access control, accounting for visibility, etc.

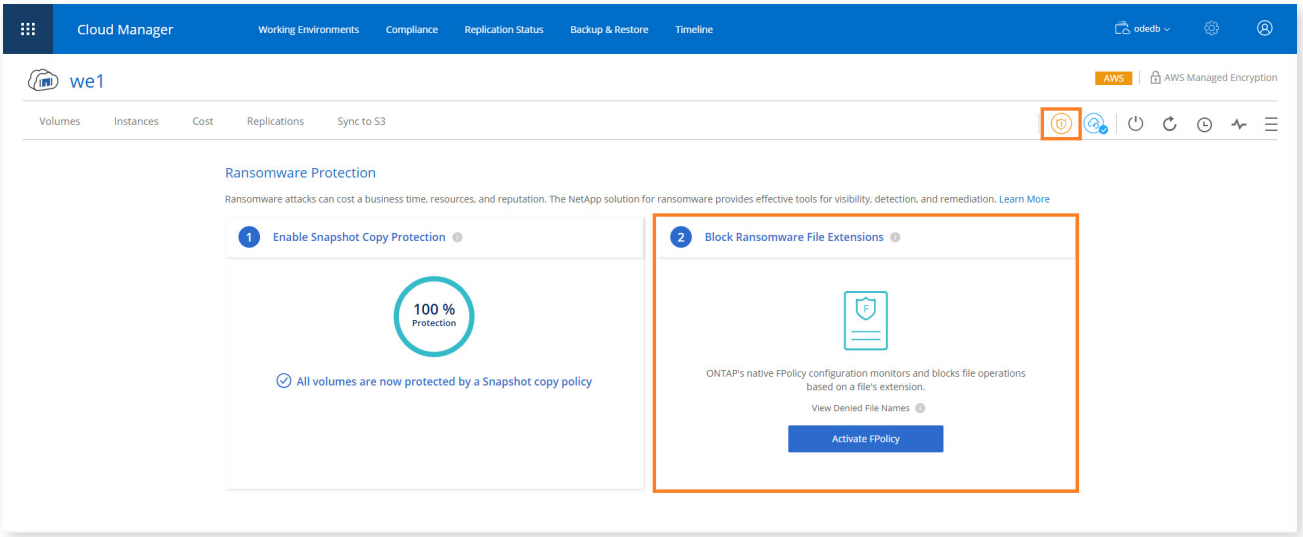
After establishing preventive measures, it is also important for any organization to ensure that resources exist for ransomware visibility and detection and tools for subsequent remediation, should all preventive measures fail to safeguard against an infection.

# NetApp Solutions for Ransomware Protection in the Cloud

NetApp offers a number of security solutions, some native, some developed with alliance partners to help enterprises bolster their defenses against costly ransomware infections in the cloud.

## Prevention with FPolicy

NetApp FPolicy is a solution that is integrated into Cloud Volumes ONTAP. With FPolicy, file operations can be monitored and blocked. This can act as a proactive preventive solution to limit ransomware and other malware infections for Cloud Volumes ONTAP customers.




FPolicy provides a native file blocking mechanism that proactively denies executing operations on selected file extensions (as defined by an administrator policy). This can be leveraged by an organization to proactively block the execution of operations on known, common ransomware file extensions such as .mcro, .encrypted, .crypto, .crypt, .CBTL, .CBT2, .SUPERCRYPT, .pzdc, .LOL!, .OMG!, and others.

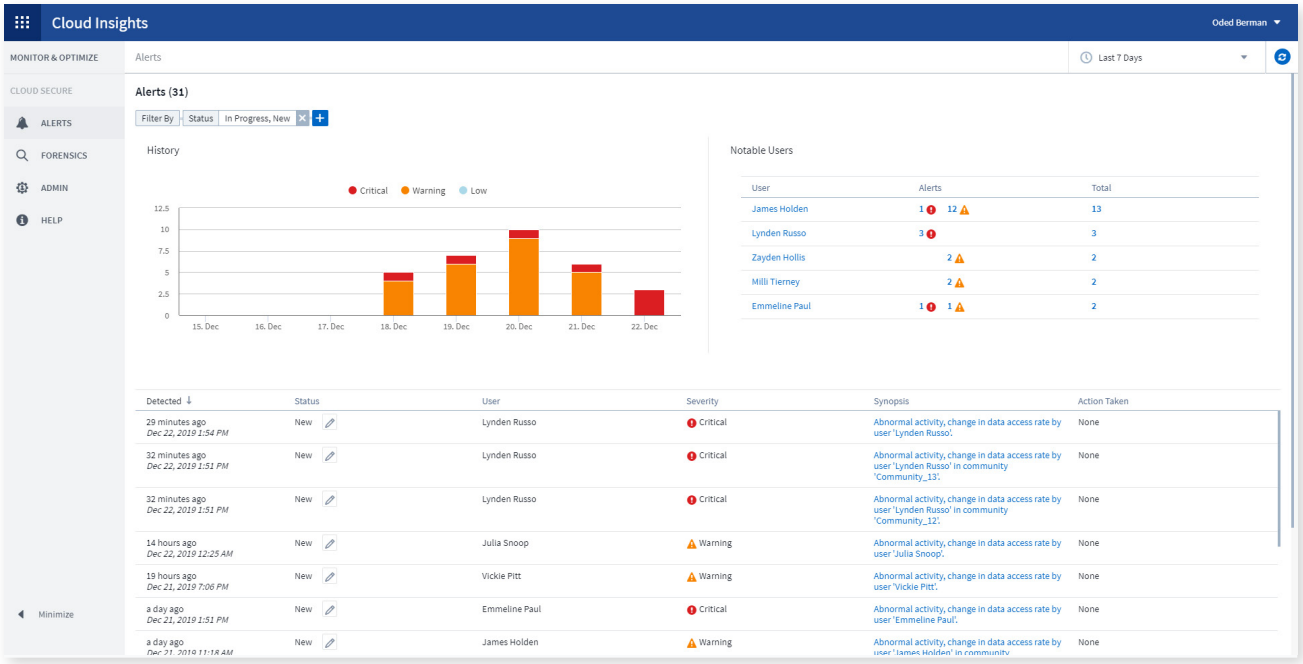
FPolicy provides an even richer set of use cases when working with NetApp partner technologies such as Varonis, STEALTHbits, Veritas, etc. to identify and prevent possible ransomware attacks. FPolicy's ability to use external FPolicy servers such as Varonis DatAdvantage enables organizations to view, understand, and manage who's using data and enforce compliance through data usage policies, proactively minimizing the chance of malware infections including ransomware on data volumes.

# Visibility and Detection

NetApp partner technologies also enable customers to detect and respond to potential ransomware infections through analyzing file system activities via the integration with Cloud Volumes ONTAP API. Ransomware infections typically would have an impact on block level change rates, abnormal user activity rate, as well as the underlying NetApp deduplication rates due to encryption of data at the file system.

Specialist solutions such as Varonis DatAlert can capture these symptoms to detect when attacks are underway and alert customers to take immediate actions. In some cases, these solutions can also automatically respond by shutting down compromised accounts automatically to reduce the potential damage to customers IT systems in the cloud.

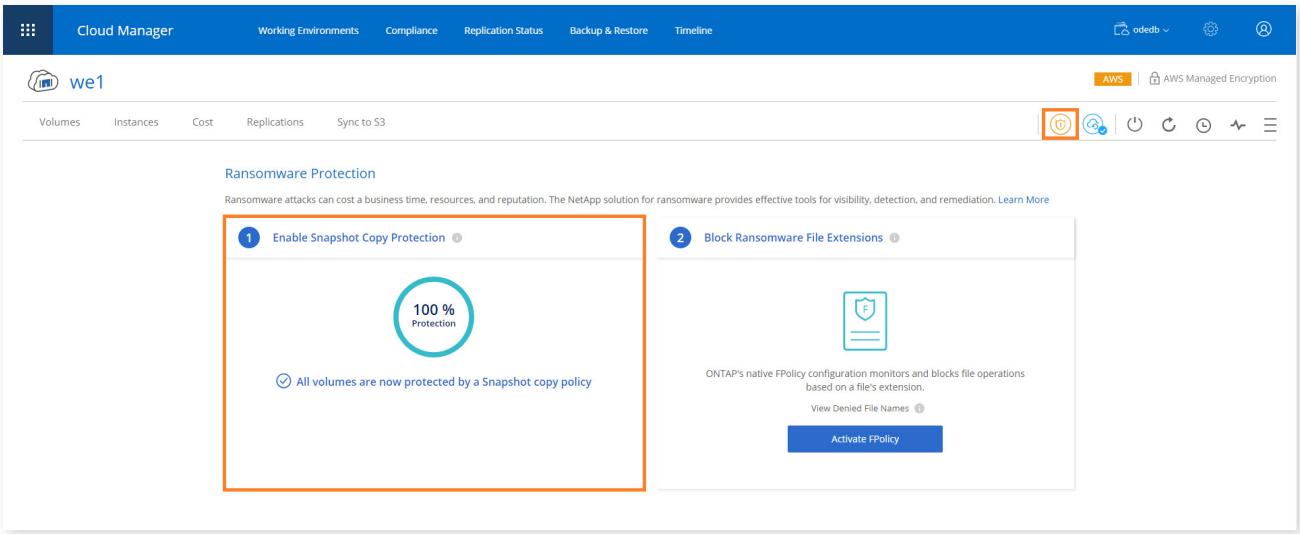
NetApp also has native tools that complements Cloud Volumes ONTAP's capabilities to help customers gain visibility of the health and security of their cloud infrastructure. NetApp Cloud Insights is one of those key solutions that is specifically designed for cloud-based infrastructure and deployments, offering advanced analytics and security assessment of various connections and inter dependencies of resources.




This visibility Cloud Insights provides can be in the form of real-time dashboard visualizations providing performance statistics of your cloud infrastructure as well as Cloud Secure information that provide information around potential security breaches and compromised accounts, such as are seen in ransomware infections, across the hybrid multi-cloud infrastructure.

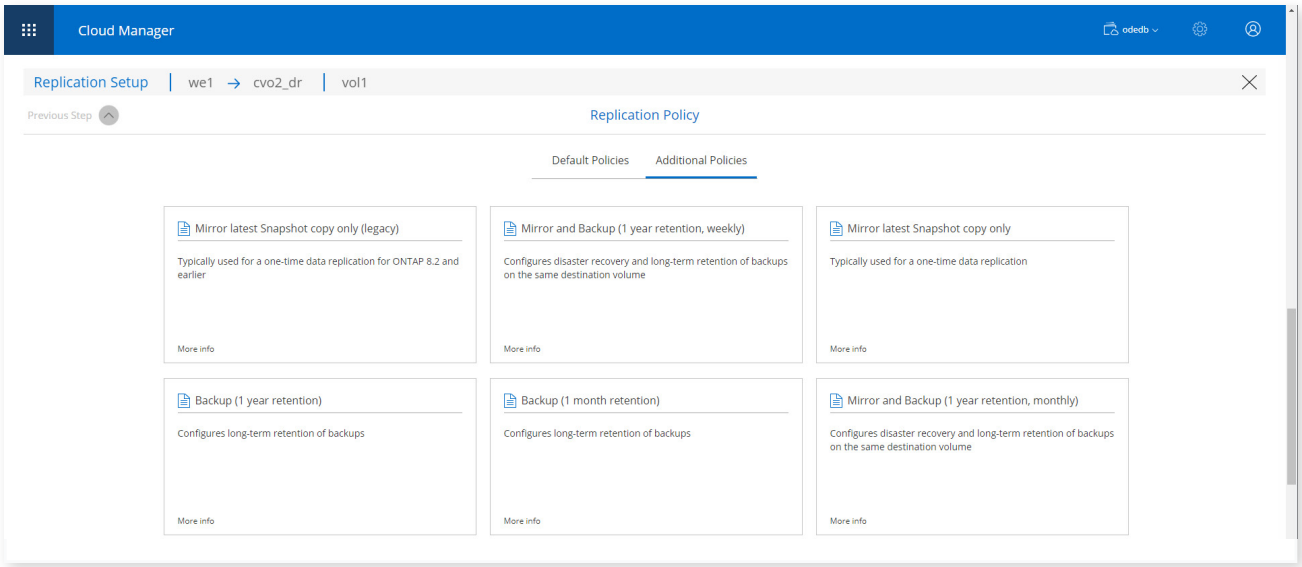
# Remediation

Ransomware remediation with Cloud Volumes ONTAP is centered on the availability of the proven NetApp Snapshot™ technology. The key to a successful ransomware recovery is to have uninfected backups and the ability to restore from them. The NetApp Snapshot technology built into Cloud Volumes ONTAP provides a great solution for customers to restore their uninfected data.

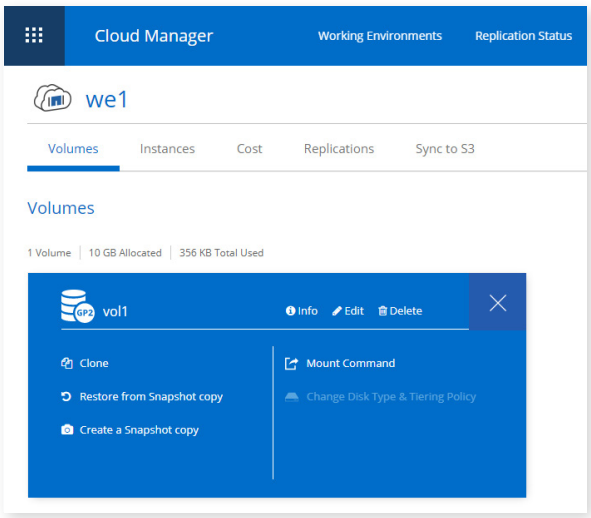


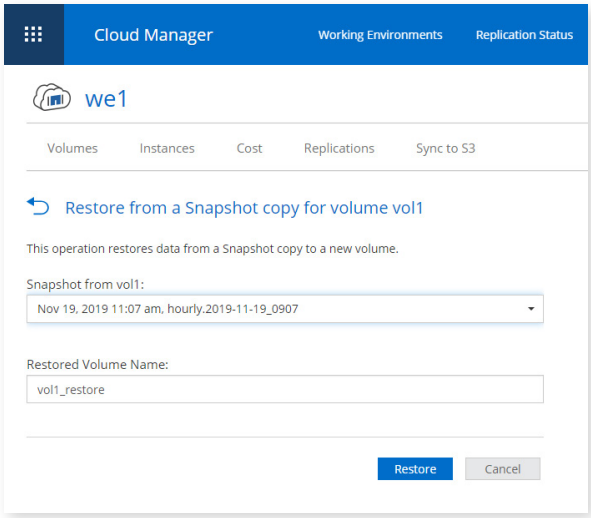

NetApp Snapshot copies are point-in-time copies of data that can be instantly created at any interval, kept for as long as needed, and are **immutable**—i.e., they are read-only by design and cannot be altered. These copies can protect data with no performance effects and minimal cloud storage footprint. They also provide the granularity to restore individual files or an entire data volume depending on the severity of the ransomware infection.

NetApp Cloud Volumes ONTAP users have the option to automate and streamline the recovery point objectives (RPO) from uninfected data points through the scheduling of automated Snapshot copy creation. These copies can be local to each Cloud Volumes ONTAP instance or can be offloaded for 3-2-1 type of retention requirements using remote replication to another Cloud Volumes ONTAP instance in a different cloud region or a different cloud platform all together.

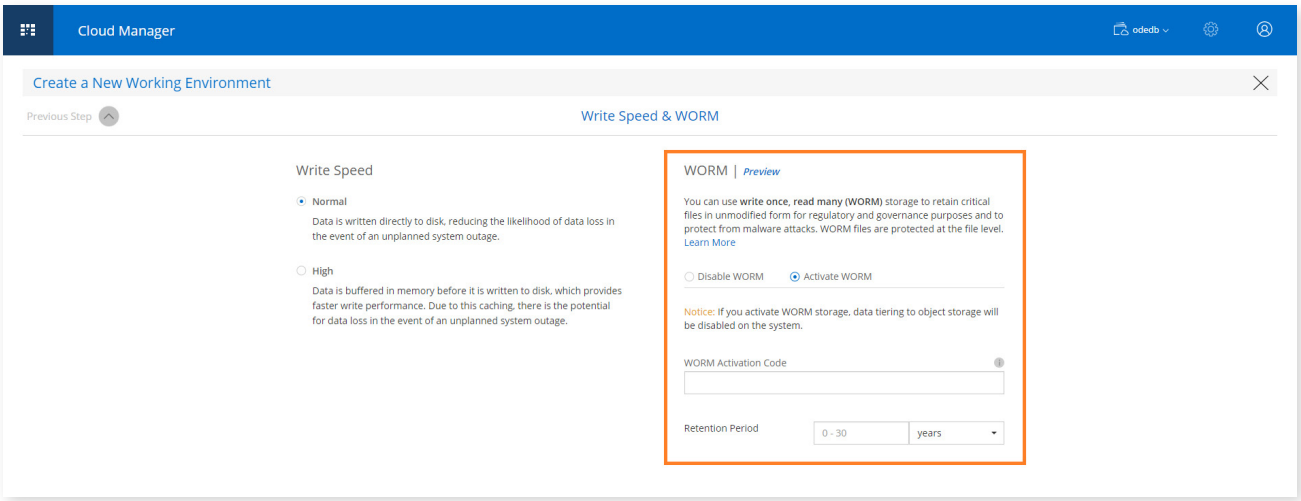


NetApp Snapshot copies also enable Cloud Volumes ONTAP users to perform rapid recovery in a matter of seconds, given the instantaneous nature of the underpinning SnapRestore® technology and FlexClone® technology. This improves recovery time objective (RTO) during a ransomware infection, ensuring the cost of downtime (described earlier) for an organization during a ransomware restore is kept to a minimum.




In addition to immutable Snapshot copies, NetApp Cloud Volumes ONTAP customers can also activate Cloud WORM (Write Once Read Many) feature during the provisioning of a new Cloud Volumes ONTAP instance. Powered by the high performance compliance solution NetApp SnapLock® (Enterprise mode) behind the scenes, this enables a Cloud Volumes ONTAP system to retain files and snapshots in unmodified form for a specified retention period for regulatory and compliance purposes. Snapshots stored in a Cloud WORM enabled system cannot be renamed or deleted until they are no longer needed or have aged out (based on an administrator configured WORM policy). Additional details can be found here.




In the case of using specialist partner solutions such as Varonis, users can also utilize Cloud Volumes ONTAP Snapshot technology to pinpoint specific files affected by ransomware attacks based on NetApp FPolicy information and enable a speedy recovery by restoring the specific files from the Snapshot copies of that data.

# Don’t Get Locked Out of Your System

It is clear that ransomware has become an ongoing threat that all organizations have to be prepared for. The threat of ransomware is no longer just limited to private, on-premises data centers as the infections can happen on cloud platforms too. It is important for customers to have an appropriate layered defense against threats such as ransomware, that consist of prevention, detection and remediation technologies, along with appropriate organizational policies and procedures.

NetApp Cloud Volumes ONTAP provides a number of built-in ransomware prevention, detection and remediation options for enterprise customers to use to mitigate against, as well as to efficiently recover from ransomware infections on the cloud. Immutable NetApp Snapshot technology is one of the significant parts of these options, providing highly efficient, read only, automated point in time copies of data for customers to restore from with a click of a button.

In addition to this, Cloud Volumes ONTAP also work hand in hand with various other NetApp and third-party tools and solutions to provide an extended, layered defense mechanism for maximum protection against ransomware and other malware attacks.


Additional information can be found in the following documents:

- NetApp ransomware solution TR
- NetApp ransomware solution brief
- Improving ransomware protection (blog)
- Varonis and NetApp solution whitepaper
- STEALTHbit auditing and reporting for NetApp storage
- SnapLock documentation
- NetApp FPolicy introduction
- FPolicy solution guide for Varonis DataAdvantage
- FPolicy solution guide for STEALTHbit File Activity Monitor
- FPolicy solution guide for Veritas Data Insight

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.



NA-287-0218