Technical Report

The NetApp solution for ransomware

Product Security Team, NetApp
November 2021 | TR-4572

Abstract

This guide covers what ransomware is; how it has evolved; and how to identify, detect early, prevent the spread, and recover as quickly as possible using the NetApp® solution for ransomware. The guidance and solutions provided in this document are designed to help organizations have cyber resilient solutions while meeting their prescribed security objectives for information system confidentiality, integrity, and availability.

TABLE OF CONTENTS

LIST OF FIGURES

Ransomware overview

Everyone knows that a ransomware attack is one of the top cybersecurity threats an organization can face. The potential damage is not just the direct associated recovery costs (which increased 241% between 2019 and 2020, according to Sophos); it is also the effect on the company's reputation and brand.

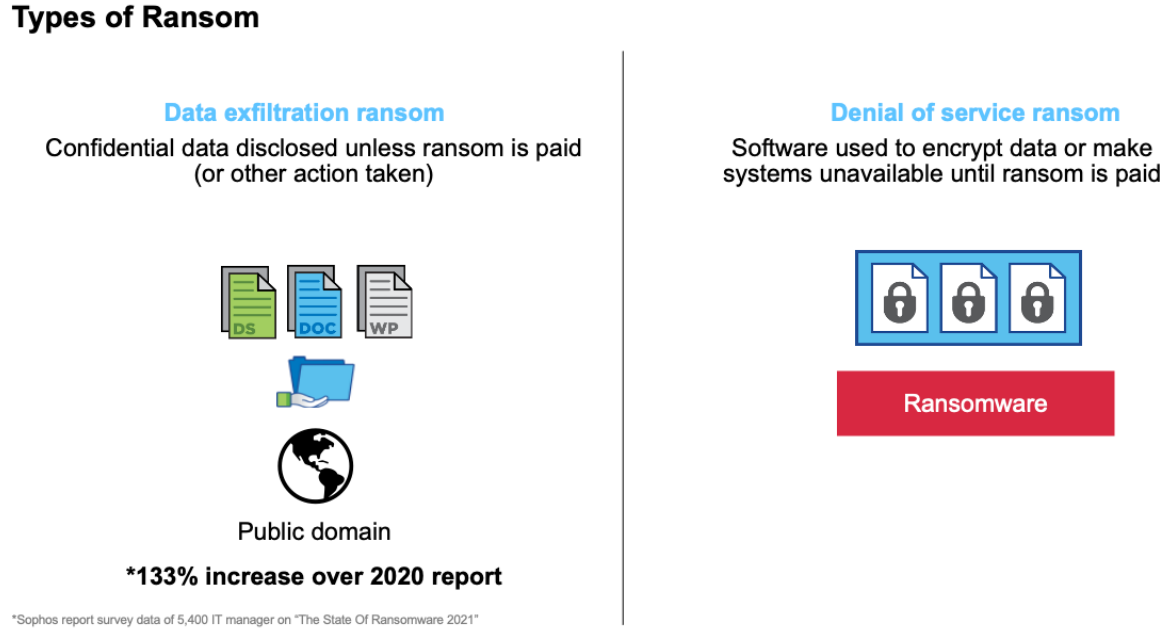
What is ransomware?

The goal of an attacker employing ransomware is simply to make money as cheaply as possible. Over the years, the strategies used by attackers have evolved. In the past, attackers typically used a distributed denial of service attack, in which a corporation's website that customers use to purchase items is made inaccessible. The denial of service remained in place until a ransom was paid. This strategy is not used much today. Another method is known as a data exfiltration. With this strategy, the attacker gains access to a company's IT systems, moving sensitive data to an unknown location outside of the company, and then threatens to publicly release that data unless a ransom is paid. Data exfiltration is on the rise again with attacks in this area up 133% compared to the previous year, according to Sophos.

The more common version of ransomware, the one that most people are familiar with, is called denial of service ransomware. In this ransomware strategy, an attacker gets you to inadvertently download an encryption program (malware). After it is installed, that malware encrypts all the local client files and every single file that it can on NFS or SMB shares on the corporate network. After the files are encrypted, the original files are deleted and there is no longer any way for you to access the data in the files. You can still see the files because they are still on your network, but you can't access them because the attacker has encrypted them.

In contrast to the earlier methods, denial of service has very low overhead for attackers because they do not have to summon an army of bots to take the corporate website offline, and they do not need to copy your data to another location. An attacker demands that you pay a ransom to obtain the decryption key so that you can regain access to your data. The size of the ransom is typically large enough for an attacker to realize a sizeable chunk of money from the attack but not so large that it is unrealistic for the organization to pay.

Figure 1) The two main types of ransomware that are used against organizations today.

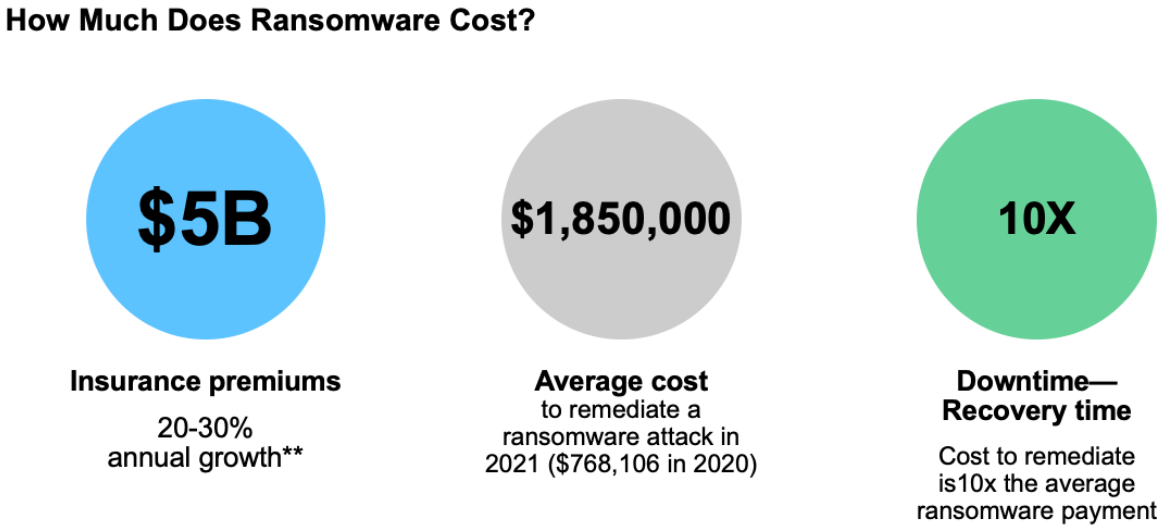


The real cost of ransomware

You might think that the ransom payment itself is the largest monetary effect on a business. However, although the payment is not insignificant (the average cost is believed to be as much as $154,108 per incident), it pales in comparison to the real cost of suffering a ransomware incident: downtime.

When an organization cannot access data that is critical to its business, productivity is severely impacted. According to a January 2020 analysis from Coveware, the average downtime from ransomware is more than 16 days, and downtime costs are typically 10 times the actual ransom amount. With an average cost of recovery in the United States at 1.8 million dollars. The effect and resulting cost of the downtime can vary from organization to organization depending on the type of business. Organizations that rely heavily on IT availability (such as e-commerce, equities trading, and health care) are looking at the 10 times cost factor. This means that the organization might face as much as $1,154,108 for the actual downtime suffered, if not more. Remember that this amount is per incident; multiple incidents can increase the costs. Cyber insurance costs also continue to rise given the very real likelihood of a ransomware attack on the insured companies.

Figure 2) The major cost of ransomware is the downtime an organization faces while recovering.



For additional information about the history and real cost of ransomware, see Fighting Ransomware: Part One — The History and Cost.

NetApp solutions for ransomware

A layered defense approach

It is important for ransomware detection to occur as early as possible so that you can prevent its spread and avoid costly downtime. However, an effective ransomware detection strategy should include more than a single layer of protection. A good analogy is the safety features of a vehicle for protection in a crash. You would not want to rely on a single feature, such as a seatbelt, to protect you in an accident. Air bags, antilock brakes, and even forward-collision warning are additional safety features that can result in a much better outcome. Ransomware protection should be viewed in the same way.

For example, NetApp FPolicy in combination with NetApp Cloud Insights, or similar capabilities from our partners, do an excellent job of detecting ransomware through user behavioral analytics (UBA). They look

for potential ransomware attacks from the aspect of an individual user's behavior. Hijacking a single user account is just one avenue a hacker might take when launching a ransomware attack; malicious actors are constantly evolving their attack techniques.

NetApp Active IQ® and NetApp Active IQ Unified Manager also provide additional layers of detection for ransomware. Active IQ checks NetApp ONTAP® systems for adherence to NetApp configuration best practices, such as enabling FPolicy. Active IQ Unified Manager generates alerts for abnormal growth of NetApp Snapshot™ copies or storage efficiency loss, which can indicate potential ransomware attacks.

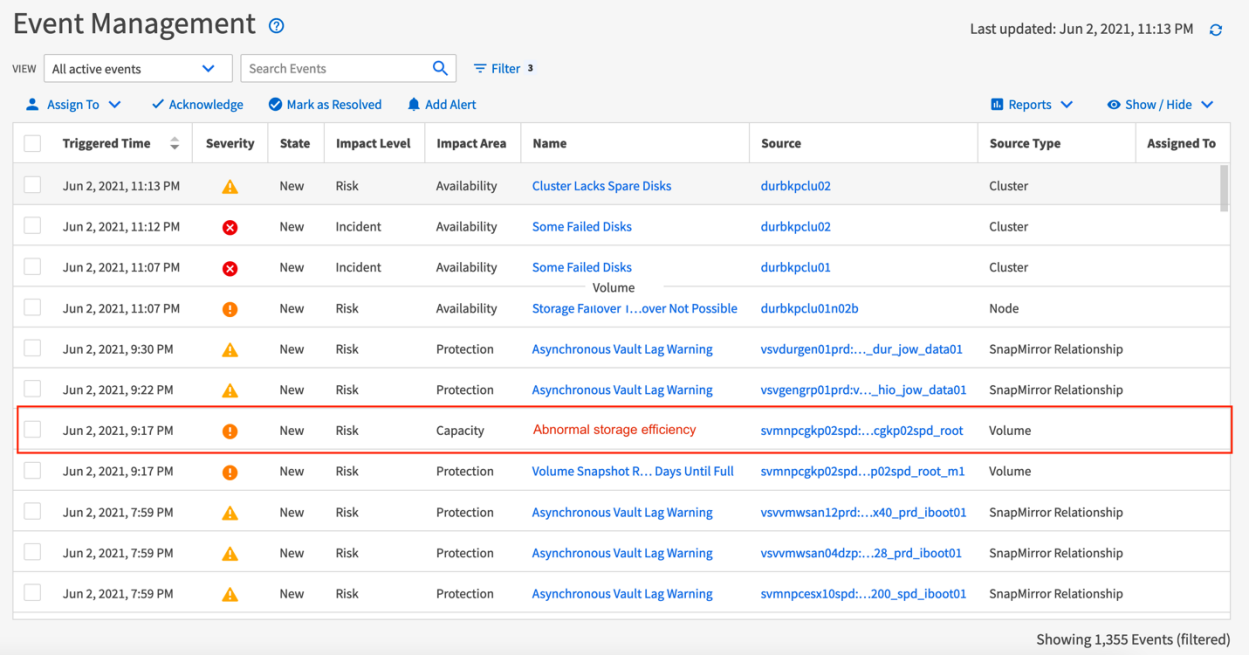
This is where the anti-ransomware feature in ONTAP 9.10.1 and later comes into play. It leverages built-in on-box machine learning (ML) that looks at volume workload activity plus data entropy to automatically detect ransomware. It monitors activity that is different from UBA, so that it can detect attacks that UBA does not.

For additional information about a layered defense approach, see the blog, Prevent ransomware spread with ONTAP automatic ransomware protection.

NetApp native detection tools

NetApp has native or built-in tools to help you detect ransomware early. For ONTAP in particular, these tools include Active IQ Unified Manager alerts for abnormal Snapshot copy and volume growth rates and loss in storage efficiency.

Figure 3) Abnormal storage efficiency alert provided by Active IQ Unified Manager.



You can also use ONTAP System Manager to look at Snapshot percent change or storage efficiency savings in real time.

To learn more about ONTAP native detection tools, see the blog, Fighting Ransomware: Part Two – ONTAP Native (aka Free) Tools for Detecting Ransomware.

Native FPolicy

NetApp FPolicy (an evolution of the name File Policy) is a file-access notification framework that you use to monitor and to manage file access over the NFS or SMB/CIFS protocol. It has been part of ONTAP for

over a decade, and it is incredibly useful in helping you detect ransomware. This Zero Trust engine is valuable because you get extra security measures beyond permissions in access control lists (ACLs).

The concept behind Zero Trust is to never trust and to always verify. You can learn more about it in another recent NetApp blog post. The key point, though, is that just because a user (or administrator) has permission to access a file or folder, they should not necessarily be able to change whatever content they want to in that location.

FPolicy was initially intended to help you block unwanted files from being stored on your enterprise-grade storage appliance. (For example, many users stored .mp3 files on their home folders before music streaming services like Spotify became popular, enabling users to stream music from their personal devices.) However, FPolicy also gives you a way to block known ransomware file extensions. The user still has full access permissions to their home folder, but FPolicy does not allow them to store whatever files your administrator marks as blocked, whether it is .mp3 files or known ransomware file extensions.

To learn more about native FPolicy, read the blog Fighting Ransomware: Part Three — ONTAP FPolicy, Another Powerful Native (aka Free) Tool.

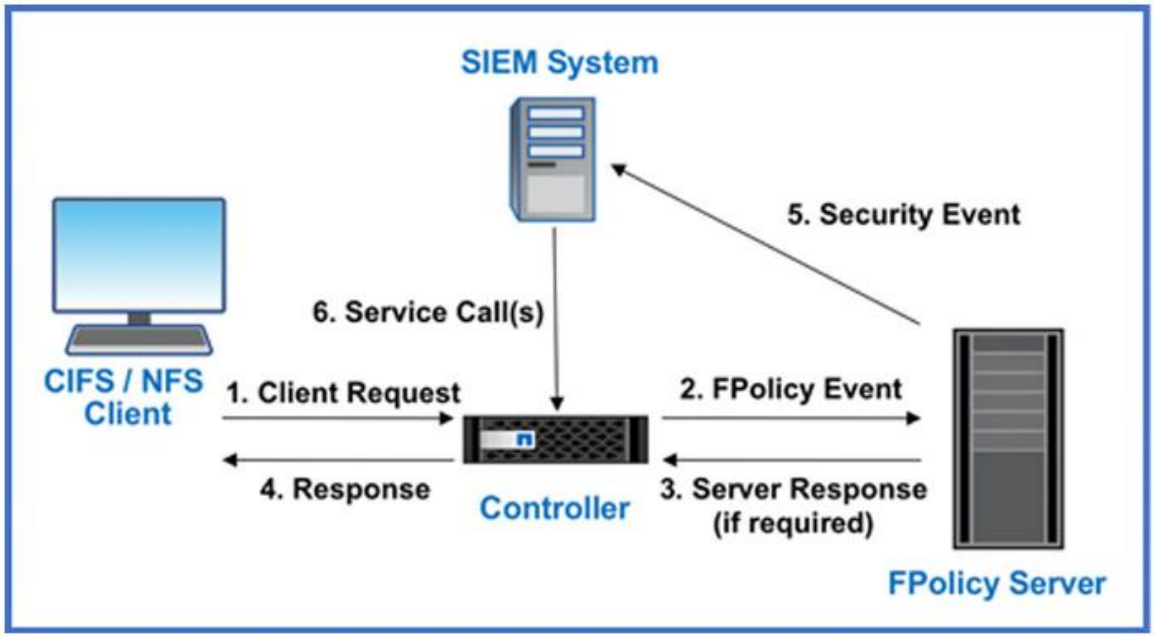
External FPolicy

FPolicy external mode in ONTAP uses UBA (sometimes referred to as User and Entity Behavior Analytics, or UEBA) as the key to stopping a zero-day ransomware attack. To understand how, you need a solid understanding of UBA.

Human beings are creatures of habit. Our habits apply to many things, including how we access and work on data. Users and groups often access particular datasets to perform their jobs. UBA tracks these behaviors, identifies typical access patterns for a user, and can report when that user's behavior differs from the pattern. Going a step further, UBA can also deny access to file data if users are doing something outside their usual patterns. FPolicy external mode integrates with an external server that uses UBA to determine when users are doing things that they do not normally do.

In the following example of a security information and event management (SIEM) system, every CIFS or NFS client request is sent to the FPolicy server, which judges whether access is allowed.

Figure 4) FPolicy in external mode integrates with external servers by using FPolicy specific APIs.



This extra level of analysis occurs even if users have file permissions to the file data they are trying to manipulate. Because permissions are hard to get right all the time, UBA with FPolicy can be a much better gauge in determining whether the user is trying to do something nefarious. You can learn more about UBA in the NetApp technical report, TR-4829: NetApp and Zero Trust.

UBA is quite powerful, but it is not the end game in fighting against zero-day ransomware attacks. Many NetApp partners and vendors have started to incorporate artificial intelligence (AI) and ML in their external FPolicy servers. Because each vendor plugs into the FPolicy feature built into ONTAP, you can harness these AI/ML enhancements right away.

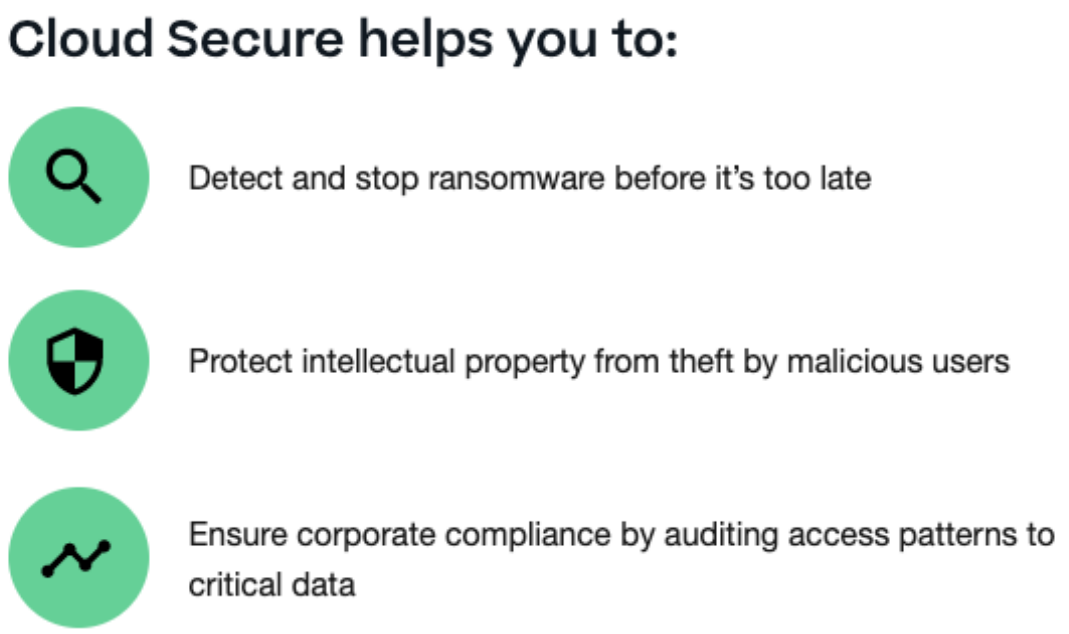
To learn about user behavior analytics and FPolicy external mode, read the blog, Fighting Ransomware: Part Four — UBA and ONTAP with FPolicy External Mode

Cloud Insights

As mentioned previously, UBA requires an external mode FPolicy server. Although NetApp has partners that provide this service, we also have our own external mode FPolicy server: Cloud Insights with Cloud Secure.

Cloud Insights is a SaaS infrastructure and service monitoring solution that works for on-premises, private cloud, and public cloud environments including AWS, Azure, and Google Cloud. Cloud Secure, a feature of NetApp Cloud Insights, analyzes data access patterns to identify risks from ransomware attacks.

Figure 5) Cloud Secure helps protect from ransomware in three key ways.



To learn more about Cloud Insights with Cloud Secure, see cloud.netapp.com.

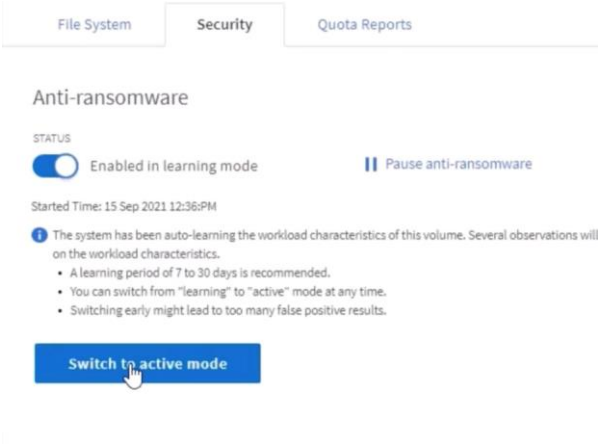
On-box anti-ransomware

ONTAP 9.10.1 and later introduces a brand new form of ransomware detection and prevention in its anti-ransomware feature. It leverages built-in on-box ML that looks at volume workload activity plus data entropy to automatically detect ransomware. It also monitors for activity that is different from UBA so that it can detect attacks that UBA does not.

ONTAP anti-ransomware protection is provided as part of the Security and Compliance software bundle. Customers who already have the bundle only need to upgrade to the latest version of ONTAP (ONTAP 9.10.1) to take advantage of the feature. It's configurable through the ONTAP built-in management interface, System Manager, and is enabled on a per-volume basis.

The anti-ransomware feature starts in learning mode. NetApp recommends a period of at least 30 days so that the ML has a chance to understand the typical workloads on the NAS volumes. When anti-ransomware is put into active mode, it starts looking for the abnormal volume activity that might potentially be ransomware.

Figure 6) Enable anti-ransomware in learning mode for a recommended 30 days before setting to active mode.



If abnormal activity is detected, an automatic Snapshot copy is immediately taken, which provides a restoration point as close as possible to the file infection. Simultaneously, an automatic alert is generated that allows administrators to see the abnormal file activity so that they can determine whether the activity is indeed malicious and take appropriate action. Or, if the activity was an expected workload, they can easily mark it as a false positive; the anti-ransomware ML notes the change in workload and no longer flags it as a potential attack. In addition, the feature does not disrupt I/O in any way. Instead, it provides administrators with native analytics, insights, and data recovery capabilities for unprecedented on-box ransomware detection. The anti-ransomware feature makes it easier than ever to enable automatic ransomware detection for your NAS workloads in ONTAP.

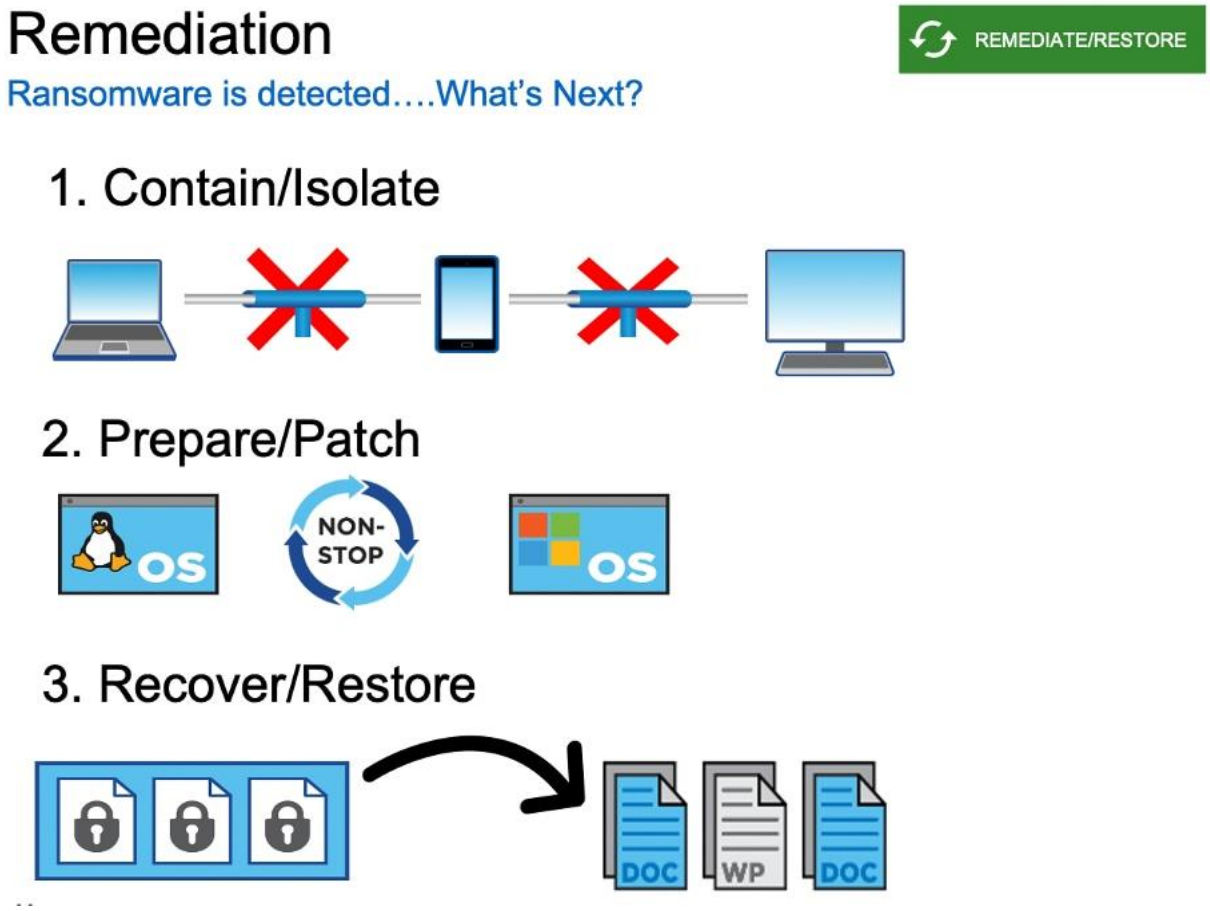
To learn more about the anti-ransomware feature, see the anti-ransomware ONTAP 9 documentation.

Recommendations for recovering from a ransomware attack

Your first instinct after a ransomware attack might be to instantly recover your data. You can certainly do this, but if you don't take other steps to make sure that the ransomware does not come back, you are likely to end up being reinfected and the effort will waste valuable time.

There are three key steps to remediate your environment properly and holistically from ransomware infection. These steps are depicted in the following graphic and are preferably completed in the order listed (although, it is not required).

Figure 7) The recommended steps to recover from an attack.



This approach is the most effective way to make sure that when you restore your data it is going to be safe from reinfection.

To learn more about ransomware recovery best practices, see the blog, Fighting Ransomware: Part Five — Smart Recovery to Avoid Reinfection.

ONTAP recovery capabilities

Everyone knows that the quickest way to recover from a ransomware attack is to restore from backup. It sounds simple enough, but the actual restore process can be complex, not to mention slow.

- Has the backup data also been encrypted?
- Are the backups that I need still there?
- How much time will it take to restore the encrypted data?
- Will restoring the data affect my production workload?

It is important to answer all of these questions to avoid extended downtime (the real cost of ransomware) during the restore.

ONTAP Snapshot technology is the key to answering all these questions and providing rapid restores (terabytes in seconds), protecting your backups from ransomware encryption, and preventing deletion of valuable backup data. You can leverage the power of Snapshot copies throughout your entire ecosystem for things such as disaster recovery, data archiving, and data tiering.

To learn more about ONTAP recovery capabilities, including how to harden your Snapshot copies against deletion and have complete backup immutability, see the blog post, Fighting Ransomware: Part Six — Recover Data Fast with ONTAP Snapshot Copies.

SnapLock, a logical air gap

A growing trend is for attackers to destroy the backup copies and, in some cases, even encrypt them. That is why many in the cybersecurity industry recommend using air gap backups as part of an overall cyber resiliency strategy.

The problem is that traditional air gaps can significantly increase restoration time, thus increasing downtime and the overall associated costs. It also generally adds complexity. A logical air gap is an excellent substitute for a traditional air gap because it has the same security protection principles while keeping the backup online. With NetApp, you can solve the complexity of tape or disk air gapping with logical air gapping, which can be achieved with immutable Snapshot copies and NetApp SnapLock® Compliance.

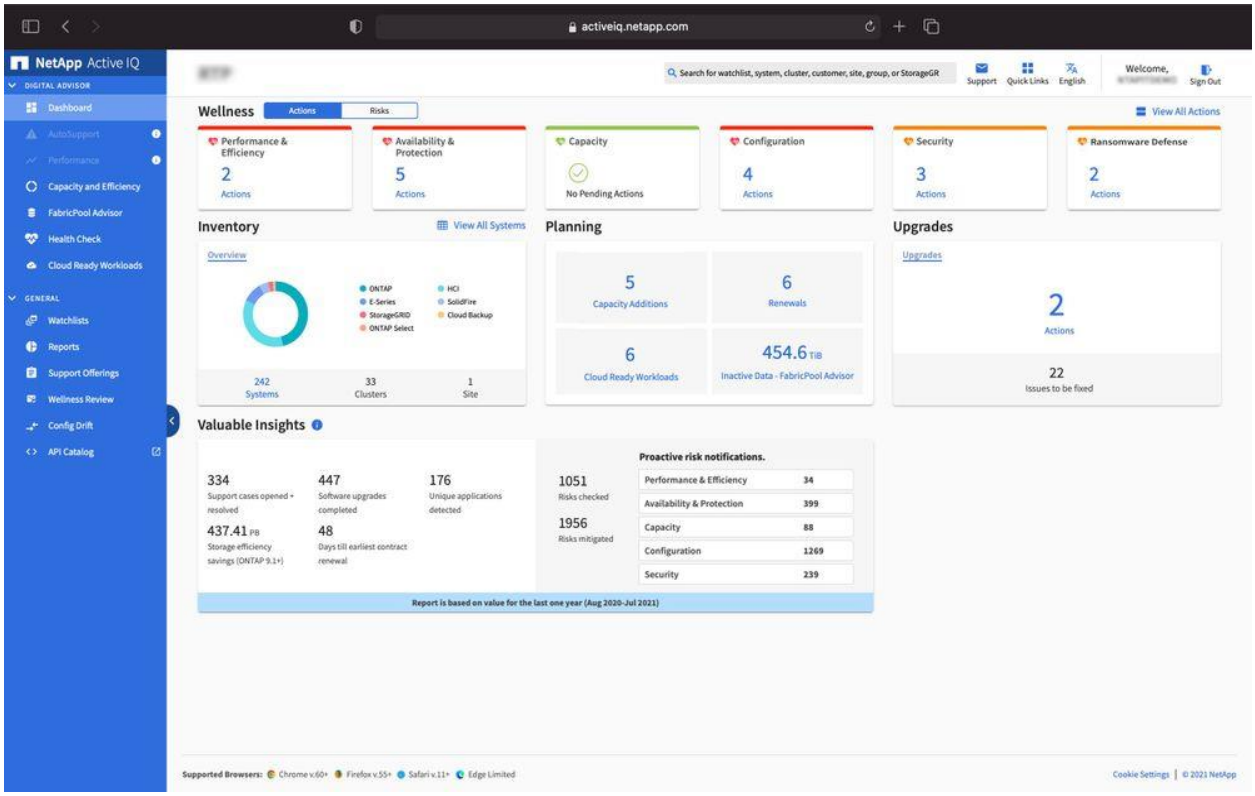
NetApp released the SnapLock feature more than 10 years ago to address the requirements of data compliance, such as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, and other regulatory data rules. You can also vault primary Snapshot copies to SnapLock volumes so that the copies can be committed to WORM, preventing deletion. There are two SnapLock license versions: SnapLock Compliance and SnapLock Enterprise. For ransomware protection, NetApp recommends SnapLock Compliance because you can set a specific retention period during which Snapshot copies are locked and cannot be deleted, even by ONTAP administrators or NetApp Support.

To learn more about SnapLock and its logical air gapping capabilities, see the blog post, Increase *ransomware* protection with SnapLock logical air gaps and technical report, TR-4526: Compliant WORM storage using NetApp SnapLock.

Active IQ — Ransomware protection best practices

When it comes to ransomware protection and ensuring your NetApp systems are conforming to best practices to fight ransomware, NetApp Active IQ plays a role as well. Not only can Active IQ help eliminate security vulnerabilities, but it also provides insights and guidance specific to protecting against ransomware. A dedicated wellness card shows the actions needed and the risks addressed, so you can be sure that your systems are meeting those best practices recommendations.

Figure 8) Wellness monitors on the NetApp Active IQ Dashboard.



Risks and actions tracked on the Ransomware Defense Wellness page include the following (and much more):

- Volume Snapshot copy count is low, decreasing potential ransomware protection.
- FPolicy is not enabled for all storage virtual machines (SVMs) configured for NAS protocols.

To see the ransomware defense of Active IQ in action, see NetApp Active IQ.

Conclusion

It is very clear that ransomware, like so many other malware threats, continues to evolve. Just as defensive methods improve, so do the attack methods and vectors. Although no single solution can thwart all attacks, using a portfolio of solutions, including partnerships and third parties, provides a layered defense.

The NetApp solution provides various effective tools for visibility, detection, and remediation, helping you to spot ransomware early, prevent this spread, and recover quickly, if necessary, to avoid costly downtime. Traditional layered defense solutions remain prevalent, as do third parties and partner solutions for visibility and detection. Effective remediation remains a crucial part of the response to any threat. The unique industry approach leveraging the immutable NetApp Snapshot technology and SnapLock logical air gap solution is an industry differentiator and the industry best practice for ransomware remediation capabilities.

Where to find additional information

To learn more about the information described in this document, refer to the following documents and/or websites:

- NetApp ONTAP Documentation Center
  http://docs.netapp.com/ontap-9/index.jsp
- NetApp Ransomware Blog Series
  https://www.netapp.com/blog/prevent-ransomware/
- NetApp Support Site Resources page
  http://mysupport.netapp.com/ontap/resources
- NetApp Product Security
  https://security.netapp.com/resources/
- NetApp Snapshot Technology
  www.netapp.com/us/media/ds-2477.pdf
- All other NetApp Product Documentation
  https://docs.netapp.com

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.

Copyright Information

Trademark Information

TR-4572 1121