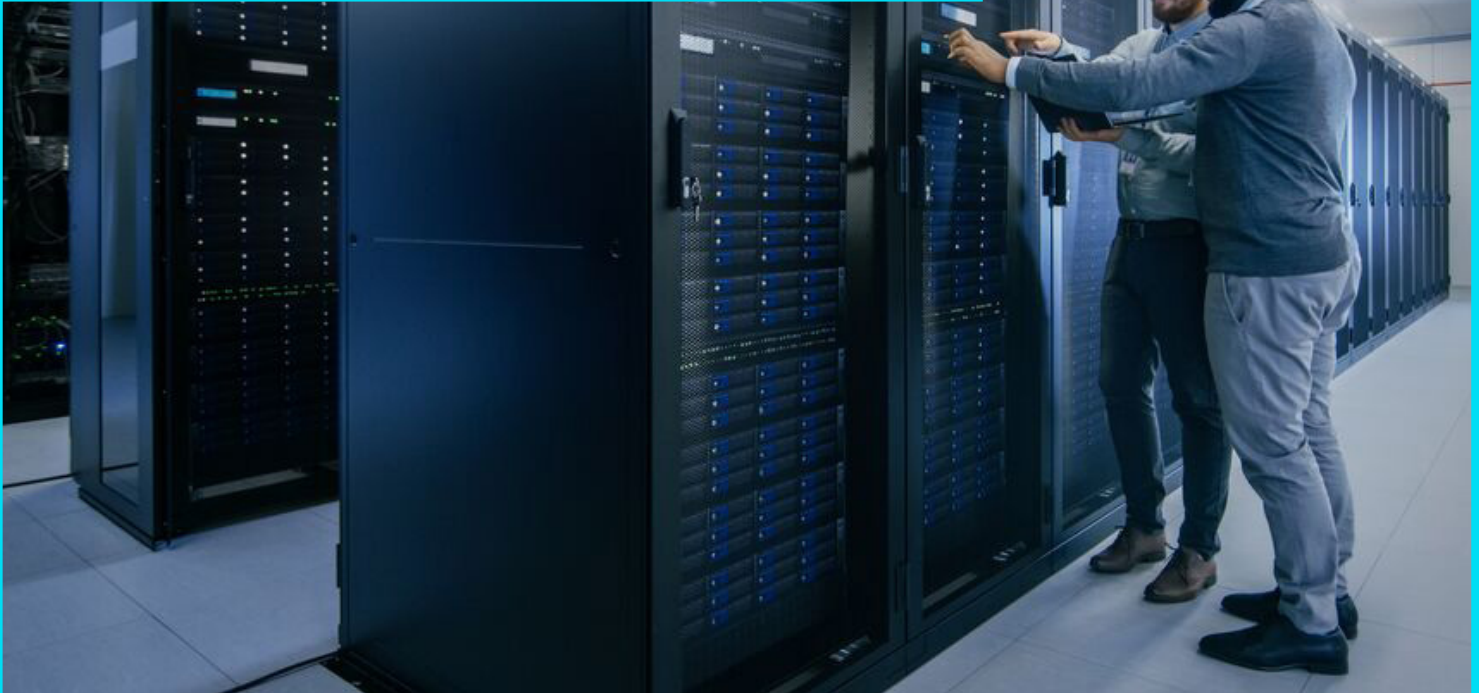


# STRENGTHENING CYBER RESILIENCE: A STORAGE ADMINISTRATOR'S GUIDE TO RANSOMWARE PROTECTION



## How to detect, respond and recover from ransomware attacks

Is your organization prepared for a ransomware attack? It could take up to 5 days to detect ransomware and 7 days to recover - resulting in business downtime, operational disruptions and financial impact.

Storage systems are the last line of defense against ransomware attacks. Many strategies, however, focus only on snapshots and backups to protect against ransomware attacks neglecting the need to address detection, response, and data recovery. Storage administrators play a key role in closing these defense gaps with the right tools and processes.

This solution brief provides guidance to help storage teams prepare for, defend against and recover from ransomware attacks, quickly and easily.

# CHALLENGES IN RANSOMWARE PROTECTION

Ransomware attacks are increasingly sophisticated and nearly impossible to prevent, posing significant risks to businesses worldwide.



Preparation



Resilience

---

### Sophistication of ransomware attacks

Ransomware attacks are becoming smarter in both methods and targeting. Attackers are using sophisticated social engineering tactics to gain initial access and advanced techniques such as double extortion, where they not only encrypt data to prevent access, but also steal it and threaten to release it publicly.

---

### Human error and insider threats

Human error remains one of the most significant vulnerabilities to any cybersecurity strategy. Employees may fail to follow security protocols, and storage or security teams may fail to apply controls or fix vulnerabilities, leading to successful ransomware attacks. Additionally, insider threats, whether intentional or accidental, can also compromise security.

---

### Inadequate ransomware protection strategies

Many organizations still rely on outdated or insufficient defense strategies, such as simply backing up their data. The National Institute of Standards and Technology (NIST) recommends a six-step framework to protect against ransomware attacks: identify, protect, detect, respond, recover, and govern. However, this approach entails a significant operational overhead.

---

Given the sophistication and velocity of attacks and tenacity of attackers, 100% attack prevention is unrealistic. Cyber criminals are always going to get in one way or another, so organizations need to focus on building a ransomware defense based on preparation and resilience that aligns with the NIST framework.

## REAL-WORLD SUCCESS STORIES

# PROTECTING PATIENT DATA

A major healthcare provider uses NetApp® Ransomware Resilience to safeguard patient data, resulting in zero data loss during a recent attack.

# 1

### Increased security

NetApp Ransomware Resilience automatically discovered and prioritized workloads within the customer's NetApp storage. It specifically identified an application containing critical patient information that was at risk. Ransomware Resilience then provided recommendations for better protection, and through its orchestration capabilities applied protection policies to this high-priority workload, with one click. Additionally, Ransomware Resilience detected a Common Vulnerabilities and Exposures (CVE) vulnerability and recommended a fix thereby improving data protection and reducing the risk of a ransomware attack.

# 2

### Efficient detection

Ransomware Resilience accurately detected a ransomware attack on the patient application in real time, mapped the attack to a suspicious user, automatically created a tamperproof NetApp Snapshot™ copy, and sent an alert. An additional alert with forensic details was sent to the customer's Splunk security information and event management (SIEM), so the Security Operations team could investigate further. Overall, Ransomware Resilience's rapid detection capabilities effectively minimized the impact of the attack.

# 3

### Fast recovery

Ransomware Resilience rapidly restored all the affected workloads through a simplified, orchestrated recovery process, minimizing downtime and data loss.



“Our patient application remained intact and available, thanks to NetApp’s robust ransomware protection.”

IT Director, Healthcare Provider



## HOW NETAPP HELPS

### Protecting your data at the storage layer

NetApp Ransomware Resilience makes protecting and recovering your ONTAP workloads easier, faster, and more effective. You get a comprehensive, orchestrated workload-centric ransomware defense from detection to recovery via a single control plane.

Prepare for an attack by identifying and protecting critical workloads with a single click. AI-powered detection automatically uncovers and responds to potential attacks and data breach attempts to minimize data loss. And, if an attack does occur, clean, malware-free restore points and guided restoration help you recover affected workloads within minutes.

Get comprehensive, orchestrated protection at the last line of defense:

- Gain complete visibility into your workload protection posture
- Detect an attack early and prevent data loss
- Recover entire workloads fast and malware-free to minimize disruptions, costs, lost revenues and business damage
- Get data for forensic analysis and recommendations to improve your ransomware protection



#### Comprehensive, unified protection

Ransomware Resilience manages NetApp ONTAP® cyber resilience capabilities and NetApp Data Services from a central console, streamlining operations and enhancing efficiency. Through this single control plane you can boost your ransomware resilience by orchestrating an effective, time-sensitive detection, response and recovery to ransomware attacks.



#### Intelligent defense

Using AI for intelligent insights and orchestrated actions, Ransomware Resilience detects and responds to attacks quickly and accurately. This automation limits the need for human intervention, reduces application downtime, and enables fast restoration of critical business operations.



#### Fast, clean restoration

Ransomware Resilience enables fast, clean, malware-free workload restoration. It uses AI-powered forensics to identify and remove malware, and recommends a recovery point for the workload. It then guides you through an intuitive restoration process to ensure a clean, safe recovery to minimize data loss while preserving application states and data.

When paired with NetApp Ransomware Resilience, ONTAP delivers the most secure storage platform for safeguarding your organization's critical data.

Ransomware Resilience integrates with SIEM systems to support incident reporting and analysis. Your security team now has the data to quickly respond to potential attacks and make informed decisions based on a comprehensive picture of the security posture.



## NEXT STEPS

# STRENGTHEN YOUR RANSOMWARE RESILIENCE



### Assess your ransomware preparedness

1. I know what my most critical workloads are.
2. My critical workloads and their data are protected from ransomware.
3. If there was an attack, I would know immediately and receive forensic details.
4. My team has an attack response plan.
5. In the event of an attack, I'm confident I would know which files were impacted.
6. My team knows which files to recover in the event of an attack.
7. I know how long it would take to recover our workloads after a ransomware attack.
8. My team has a plan for recovering all data related to our workloads.
9. My team regularly updates and tests our ransomware protection program.
10. I would be comfortable demonstrating my team's ransomware attack plan to leadership/CISO/CSO/CIO, showing that all areas are covered to protect data at the storage layer.

### Next steps: Act now

See room for improvement? Here are some recommendations for enhancing your ransomware resilience today:

#### Review your ransomware protection posture

- Take advantage of the Ransomware Resilience 30-day free trial to review your current security posture.

#### Fix gaps in protection

- Assign Ransomware Resilience policies to protect your critical workloads and sensitive data, all with one click.

#### Detect attacks as soon as they occur

- Monitor alerts and investigate potential attacks using detailed forensics from Ransomware Resilience

#### Recover workloads fast

- Use Ransomware Resilience for fast, clean malware-free restoration of all your impacted files after an attack.

#### Report your protection posture to stakeholders

- Use the Ransomware Resilience dashboard to highlight your real-time security posture to leadership.

# BECOME YOUR ORGANIZATION'S DATA DEFENDER

Ready to take an active role in defending your organization from ransomware attacks?

Protect against ransomware attacks with NetApp Ransomware Resilience.

See it in action

Start your free trial



Contact Us

## About NetApp

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data, operational and workload services to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry's best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our operational and workload services provide continuous optimization of performance and efficiency for infrastructure and workloads through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities. Learn more at [www.netapp.com](http://www.netapp.com) or follow us on X, LinkedIn, Facebook, and Instagram.



© 2025 NetApp, Inc. All rights reserved. NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners. NA-1158-0925