SOLUTION BRIEF

NETAPP RANSOMWARE RESILIENCE

Detect ransomware attacks in real time, prevent data loss, recover fast, and minimize the impact on your business

Are you prepared for a ransomware attack?
A critical aspect of being prepared for a ransomware attack is protecting your workload data at the storage layer—the last line of defense. With attacks becoming more sophisticated, automated, and costly, preventing a ransomware attack is unrealistic. You must be ready when attackers get in.

Backups alone are not enough. You need to be able to assess the risks to your critical workload data and to detect threats and respond in real time. You also need recovery plans in place that can be executed quickly and easily. However, achieving effective resilience against a ransomware attack is an operational burden, with many error-prone manual tasks and too few staff who have the necessary expertise.

If you don't have a program in place, attacks on your workloads will go undetected, and your responses will be delayed. Workload recovery will be complex—taking an average of 7 days[1]—and your data may not even be fully recovered. That's too little, too late!

Get comprehensive protection at the last line of defense
The NetApp® Ransomware Resilience service enables you to quickly and easily execute your program, from prevention through detection, response, and recovery.

Ransomware Resilience provides a single interface to intelligently orchestrate your workload-centric ransomware defense. With a few clicks, you can identify and protect your critical workload data at risk. The service also accurately and automatically detects and responds to potential attacks and limits their impact. And you can recover workloads, free from malware, within minutes, safeguarding your valuable data and minimizing damage and the cost of disruption to your business.

Ransomware Resilience merges the powerful features of NetApp ONTAP® software with NetApp Data Services, adding intelligent recommendations and guidance with automated workflows to:

- **Identify.** Automatically identify workloads (VMs, file shares, popular databases) and their data in your NetApp storage, map data to the workload, and determine data sensitivity, importance, and risk.
- **Protect.** Get recommendations for workload protection policies and apply them with one click.
- **Detect.** Detect suspicious file and user behavior activity in real time which could signal potential data exfiltration attempts, as well as file encryption and mass deletion attempts.
- **Respond.** Protect workloads by automatically creating NetApp Snapshot™ copies and blocking users when a potential attack is suspected. The service also integrates with industry-leading security information and event management (SIEM) solutions.
- **Recover.** Quickly restore workloads and their associated data through a simple, orchestrated recovery process. And by using the isolated recovery environment, you get a clean, malware-free restoration of your data.
- **Govern.** Implement your ransomware protection strategy and policies, and monitor outcomes.

Prepare for an attack: Save time and improve effectiveness

Ransomware Resilience automatically identifies the types of data in your NetApp storage, maps the data to specific workloads, assesses data sensitivity and criticality, and analyzes risk. This process reduces your reliance on complicated manual analysis, additional third-party tools, and specialized expertise.

KEY BENEFITS

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 revenue, and business damage.
- Get data for forensic analysis and recommendations to improve your security posture.

Ransomware Resilience then proposes intelligent protection policies using ONTAP features, including NetApp Autonomous Ransomware Protection with AI (ARP/AI) anomaly detection, FPolicy malicious extension blocking, and tamperproof Snapshot copies. Ransomware Resilience also tailors protection recommendations to the sensitivity and criticality of your data assets.

With just one click, protection policies are seamlessly and consistently applied to your workload data. Ransomware Resilience works in the background to configure ONTAP and NetApp Data Services capabilities and to orchestrate protection workflows across each data volume, reducing the need for repetitive manual tasks.

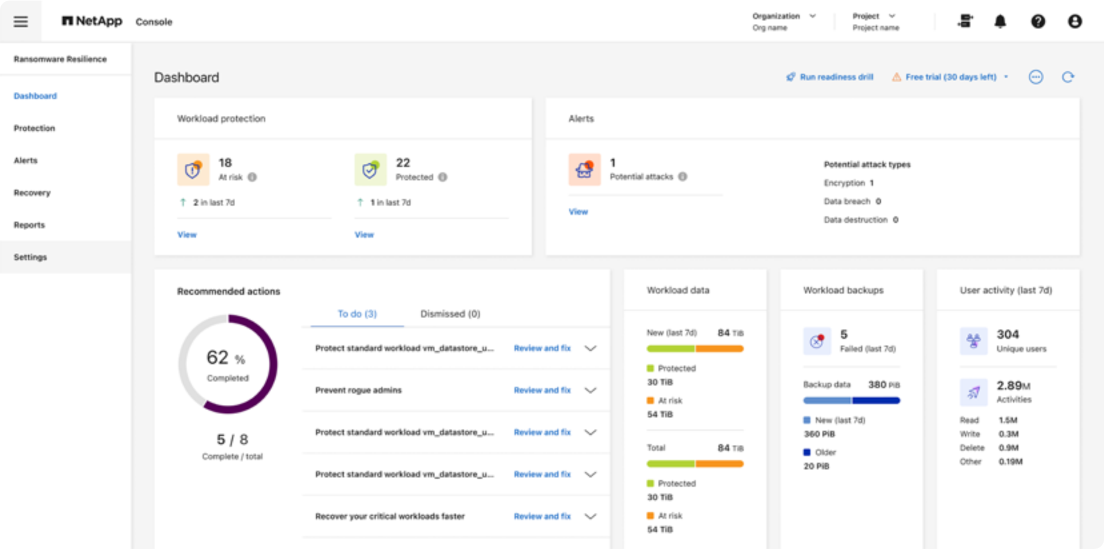
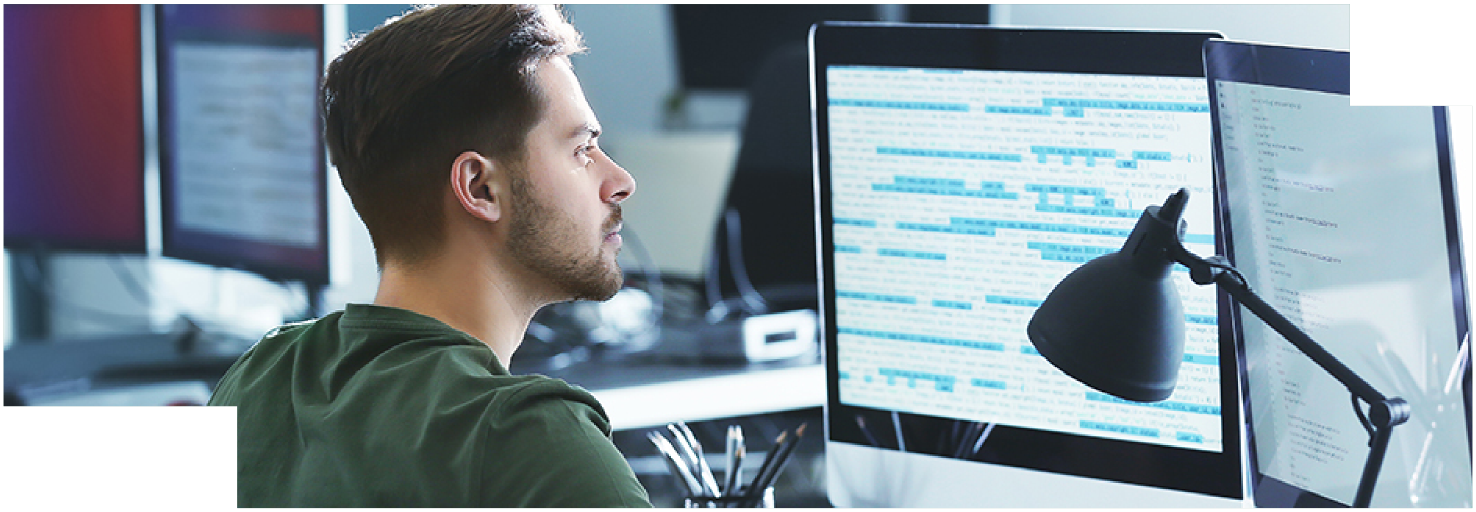


Figure 1: NetApp Ransomware Resilience service provides comprehensive, orchestrated workload-centric ransomware defense from detection to recovery via a single control plane.



Detect and respond to threats in real time
Ransomware Resilience continuously monitors for suspicious file and user behavior anomalies. It can detect data breaches by identifying early user behaviors which could signal potential data exfiltration attempts, as well as file encryption and mass deletion attempts. When an attack is suspected, Ransomware Resilience creates a Snapshot copy to prevent data loss, and it enables blocking of the user who is perpetrating the attack to stop them and to prevent further attacks.

This service uses innovative, advanced AI-based ransomware detection on your primary storage. This approach means that potential attacks can be found quickly and can be mitigated immediately.

Ransomware Resilience provides incident reports to support forensics and it integrates with the industry-leading SIEM solutions.

Recover workloads easily, within minutes
Ransomware Resilience orchestrates the workflow for application-consistent recovery of all the associated workload data, and it gives you visibility into the process and status in real time. Snapshot copies can be restored at the workload level or more granularly at the volume or file level.

As part of the recovery process, Ransomware Resilience provides an isolated recovery environment that isolates infected workloads, removes malware, recommends a recovery point, and guides the user through an intuitive restoration process. This approach delivers a clean malware-free restoration and prevents reinfection of your data.

Minimize business disruption
Ransomware Resilience removes the burden and anxiety of protecting your workloads from ransomware-related downtime and data loss. It delivers a comprehensive service that improves your readiness, responds to attacks, and guides you through recovery. Only with NetApp can you have peace of mind knowing that when an attack occurs, you will be alerted immediately, your valuable workload data will be protected, and recovery will be fast and easy—minimizing the disruption to your business.

Get NetApp Ransomware Resilience today

[1] ESG, 2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation, November 2023.

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 or follow us on X, LinkedIn, Facebook, and Instagram.

NetApp

SB-4278-0925