TACTICAL BUYERS GUIDE

NetApp

NETAPP RANSOMWARE RESILIENCE

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

THE PROBLEM

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, prevention of 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 protection against a ransomware attack is an operational burden, with many error-prone manual tasks and too few staff who have the necessary expertise.

THE SOLUTION

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.

7 reasons NetApp Ransomware Resilience makes protecting and recovering workloads more effective, easier, and faster

1. **Save time and effort:** Automate complex and time-consuming manual tasks.
2. **Improve consistency and accuracy:** Reduce errors with automated and guided actions.
3. **Detect threats early:** Automatically monitor and alert on file and user behavior anomalies.
4. **Respond immediately:** Instantly act on potential attacks to limit data loss. Integrate with the most popular SIEM solutions.
5. **Recover faster and more easily:** Recover entire workloads fast and malware-free, to minimize disruptions, costs, lost revenues and business damage.
6. **Save money:** Align protection policies to workload sensitivity and criticality for optimal ROI.
7. **Be more effective:** Speed and improve decision-making and actions using AI.

NetApp Ransomware Resilence encompasses activities that span all six functions of the National Institute of Standards and Technology (NIST) cybersecurity framework: identify, protect, detect, respond, recover, and govern.

Manage the risk of a ransomware attack	The NetApp approach
Identify	Automatically identify workloads and their data in NetApp storage, map data to the workload, and determine workload 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 that typically indicate an attack, as well as early indicators of compromise (IoC) that could signal potential data exfiltration 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.

NetApp provides the most secure storage on the planet

Comprehensive

- Orchestrates the powerful, industry-leading cyber-resilience features of NetApp ONTAP and NetApp Data Services.
- Provides comprehensive ransomware protection at the last line of defense. Goes beyond backup and covers all six areas of the NIST cybersecurity framework.
- Delivers industry leading storage with ransomware protection from a single vendor.

Easy to use

- Automatically identifies workloads, analyzes their sensitivity, criticality, and risk, and offers prioritized, intelligent recommendations for protection policies.
- Provides automated and guided actions to protect and recover data workloads without needing specialized skills or time-consuming manual tasks.
- Does not require complex configurations, tuning, or integrations.

Fast

- Uses advanced AI to detect and to respond to potential attacks early.
- Rapidly recovers entire application-consistent workloads with just a few clicks—minimizing costly downtime. Includes the option to restore data granularly by volume or file.

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

Additional resources

Get NetApp Ransomware Resilience today. ›

Contact Us

About NetApp

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data services, and CloudOps solutions 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 CloudOps solutions provide continuous optimization of performance and efficiency 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. www.netapp.com

NetApp