SOLUTION BRIEF

NetApp

PROTECT. DETECT. RECOVER.
A DATA-CENTRIC APPROACH TO RANSOMWARE PROTECTION

Protect: Secure your environment.
Detect: Anticipate threats.
Recover: Bounce back quickly.

The challenge
Ransomware attacks are an increasingly prevalent and sophisticated threat to organizations of all sizes. These malicious attacks encrypt valuable data and demand payment for its release, often causing significant financial losses and operational disruptions.

- Cyberincidents are the number one business risk globally.
- Ransomware is expected to strike every 2 seconds by 2031.
- 59% of organizations were affected by ransomware last year.
- Ransomware attacks increased by 73% from 2022 to 2023.

Although many businesses focus on network and endpoint security, it's crucial not to overlook the importance of securing the storage layer where data resides. By implementing robust security measures at the storage level, such as encryption, access controls, and immutable backups, you can create an additional line of defense against ransomware.

This approach helps protect data at its source, making it more difficult for attackers to encrypt or corrupt critical information. Secure storage solutions can aid in faster recovery times and minimize data loss in the event of a successful attack, underscoring the importance of a comprehensive security strategy that includes fortifying the storage infrastructure.

NetApp cyber resilience: A data-centric approach to ransomware protection

Protecting against cyber incidents encompasses multiple layers of defense to protect against a wide range of threats. A strong cyber defense begins at the **identity security** layer that along with the outermost layer, **perimeter security**, acts as the first line of defense.

Network security builds on this foundation to protect data in transit and detect anomalous activities within the internal network. **Endpoint security** adds a layer of defense for individual devices connected to the network. **Application security** focuses on protecting software applications from vulnerabilities and attacks.

Finally, at the core of the security posture lies **data security**, which safeguards an organization's most valuable asset—its data and the most mission-critical assets. This layer typically includes data protection with robust backup and recovery solutions.

Together, these interconnected layers of security create a comprehensive defense strategy that is designed to protect the enterprise's digital assets from the perimeter to the data center, addressing threats at every level of the IT infrastructure.

Protection at the data layer for mission-critical assets is even more important and has unique requirements. To be effective, solutions at this layer must offer these four critical attributes:

- Secure by design to minimize the chance of a successful attack against your organization
- Real-time detection and response to minimize the impact of a successful attack
- Air-gapped write once, read many (WORM) protection to isolate critical data backups
- Simple control plane for comprehensive ransomware protection and rapid recovery

NetApp can detect, protect, and recover at the data layer.

Secure by design: ONTAP built-in ransomware protection native in storage
NetApp ONTAP software provides robust ransomware protection through a secure-by-design approach. Core capabilities include immutable and indelible Snapshot copies, so that data remains unalterable and cannot be deleted, even by administrators, creating a reliable fallback point for recovery. The ONTAP FPolicy feature enhances security by blocking malicious files, preventing the spread of threats within the system.

KEY BENEFITS

- **Secure by design.** Built-in data protection at the storage layer.
- **Real-time detection and response.** AI-powered ransomware defense.
- **Cyber vaulting.** Immutable and indelible backups.
- **Simple control plane.** Intelligent orchestration from detection to recovery.
- **Recovery guarantee.** No data loss with NetApp Snapshot copies.

To fortify access controls, multiadmin verification requires multiple administrators to approve critical actions, reducing the risk of insider threats or compromised credentials. And multifactor authentication adds an extra layer of security, which means that only authorized personnel can access sensitive data and systems.

Real-time detection and response
Adding to our robust ransomware protection, NetApp provides real-time detection with 99% accuracy and near-instant response capabilities, leveraging AI-powered autonomous technology built directly into ONTAP. This advanced detection continuously monitors for suspicious activities and anomalies, swiftly identifying potential ransomware attacks as they unfold on file, block, and native cloud in Amazon FSx for ONTAP. When a threat is detected, the system can automatically isolate affected data and prevent further spread, minimizing potential damage.

NetApp Data Infrastructure Insights (DII) offers an additional layer of defense against insider threats. It detects potential anomalous user behavior and takes immediate action such as blocking user access to storage systems and taking snapshots. Furthermore, DII provides detailed analytics for forensic analysis and auditing. This comprehensive approach combines proactive threat detection, rapid response mechanisms, and detailed user activity monitoring, offering a multifaceted shield against both external ransomware attacks and internal threats.

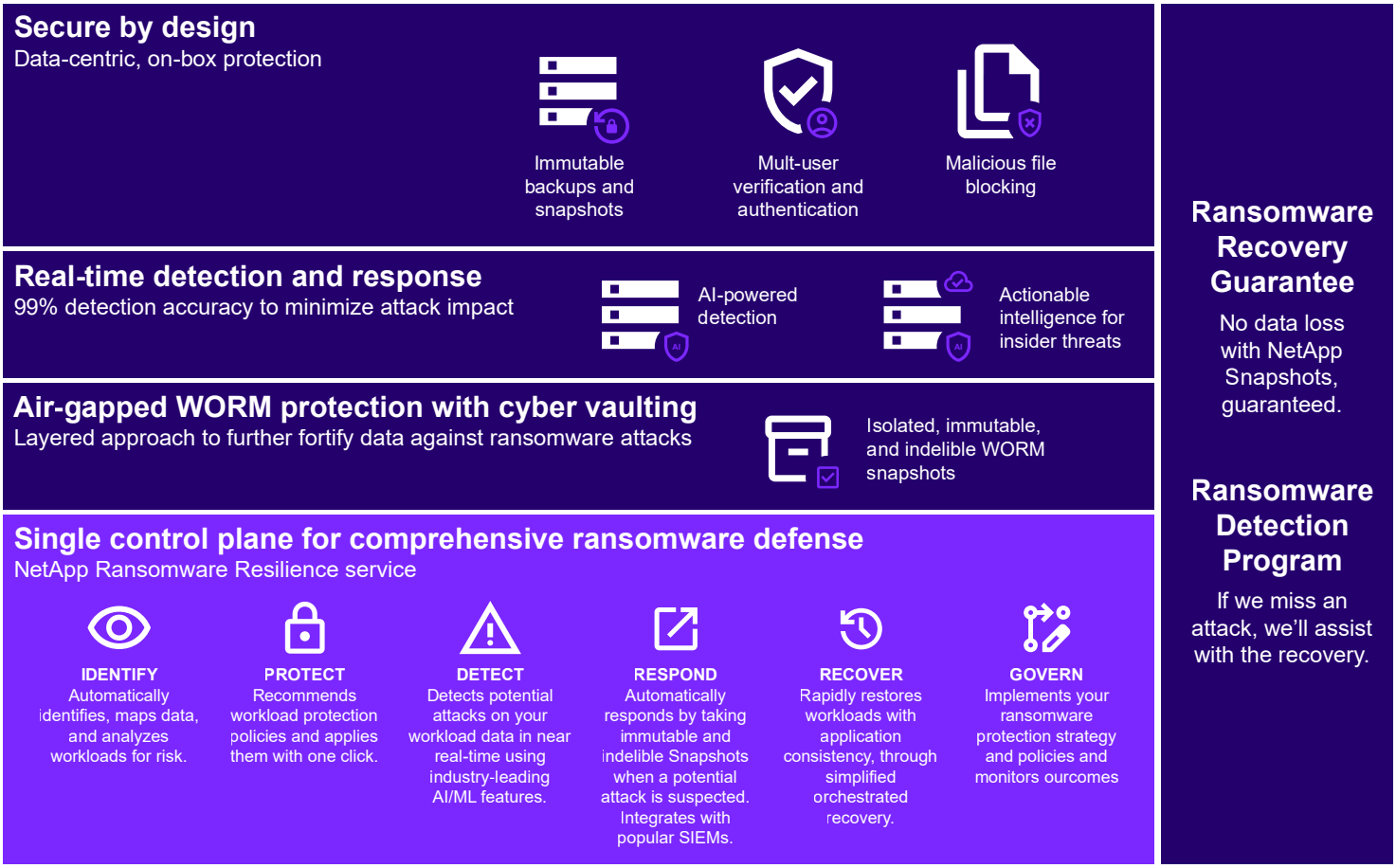

Figure 1: NetApp delivers the most secure data storage on the planet, with multilayered defenses to intelligently and efficiently protect your data, including data access through end-to-end encryption, multifactor authentication, and role-based access.

Isolated backups for cyber vaulting

NetApp cybervaulting, powered by SnapLock® compliance software, gives organizations a comprehensive and flexible solution for protecting their most critical data assets. Logical air-gapping with robust hardening methodologies for ONTAP enables you to create secure, isolated storage environments that are resilient against evolving cyberthreats. With NetApp, you can have confidence in the confidentiality, integrity, and availability of your data while maintaining the agility and efficiency of your storage infrastructure.

For greater security, NetApp enables you to create an additional layer of data protection:

- Secure, isolated storage infrastructure (for example, air-gapped storage systems)
- Backup copies of your data that are both immutable and indelible
- Strict access controls and multifactor authentication
- Rapid data restoration capabilities
- By applying WORM technology, SnapLock prevents encryption and deletion of data with indestructible and efficient data copies

Simple robust, control plane

The NetApp Console gives you one intuitive interface to intelligently coordinate and execute end-to-end workload-centric ransomware defense technologies. With these technologies, you get enterprise-grade control of storage and data services in your NetApp systems—simplifying operations, delivering insights, and safeguarding every action with a secure-first design.

NetApp Ransomware Resilience merges the powerful features of NetApp ONTAP with NetApp Data Services, adding artificial intelligence and machine learning based recommendations and guidance with automated workflows to help you:

- **Identify.** Automatically identify workloads and their data in your NetApp storage, map data to workload, determine workload importance, and analyze workload risk.
- **Protect.** Recommend workload protection policies and apply them with one click.

- **Detect.** Detect potential attacks on your workload data with industry-leading ML-based detection that operates in near real time.
- **Respond.** Automatically respond in near real time by making immutable Snapshot copies when a potential attack is suspected.
- **Recover.** Identify the best recovery point and rapidly restore workloads and their associated data through simplified orchestrated recovery.

"ARP detected a ransomware attack, responded in real-time, and we were able to recover quickly with the ARP snapshot data."

U.S. based Commercial Design Firm

Ransomware Resilience removes the burden and anxiety of defending workloads from ransomware-related downtime and data loss by providing a comprehensive solution that assists you with ransomware preparedness, responds to attacks, and guides you through recovery. Only NetApp offers peace of mind that when an attack does happen, you'll know about it immediately, your valuable workload data will be protected, and recovery will be easier and rapid so that business disruption is minimized.

Ransomware Resilience helps you identify and protect data where it resides, accurately and automatically detect and respond to limit the impact of potential attacks, and recover data within minutes, not days or months. This capability helps to preserve your valuable data and minimize costly disruption for cyber resilience.

Ransomware can debilitate enterprises that don't take it seriously. Only NetApp's data-centric cyber resilience approach offers comprehensive, integrated security and protection for primary and secondary data with a guarantee to help you recover.

Learn more about NetApp Ransomware Resilience

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.

NetApp