NetApp solution for ransomware

ONTAP Technical Reports

NetApp
January 23, 2026

Table of Contents

NetApp solution for ransomware

Ransomware and NetApp's protection portfolio

Ransomware remains one of the most significant threats causing business interruption for organization in 2024. According to the Sophos State of Ransomware 2024, ransomware attacks affected 72% of their surveyed audience. Ransomware attacks have evolved to be more sophisticated and targeted, with threat actors employing advanced techniques like artificial intelligence to maximize their impact and profits.

Organizations must look across their entire security posture from perimeter, network, identity, application, and where the data lives at the storage level and secure these layers. Adopting a data-centric approach to cyber protection at the storage layer is crucial in today's threat landscape. Although no single solution can thwart all attacks, using a portfolio of solutions, including partnerships and third parties, provides a layered defense.
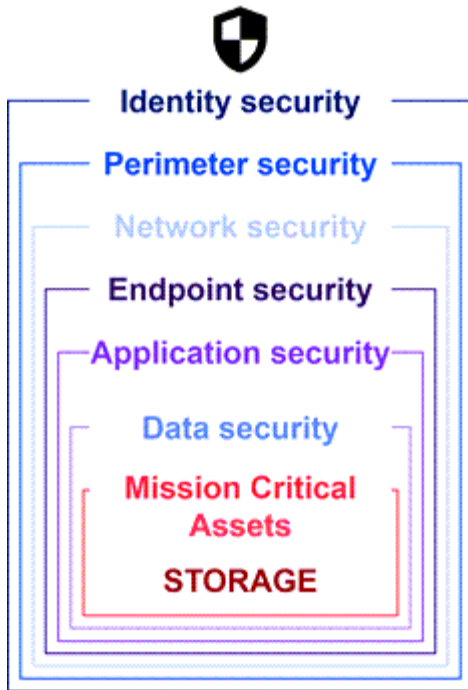
The NetApp product portfolio provides various effective tools for visibility, detection, and remediation, helping you to spot ransomware early, prevent spread, and recover quickly, if necessary, to avoid costly downtime. Traditional layered defense solutions remain prevalent, as do third parties and partner solutions for visibility and detection. Effective remediation remains a crucial part of the response to any threat. The unique industry approach leveraging immutable NetApp Snapshot technology and SnapLock logical air gap solution is an industry differentiator and the industry best practice for ransomware remediation capabilities.

> (i) Beginning in July 2024, content from the technical report *TR-4572: NetApp Ransomware Protection*, which was previously published as a PDF, is available on docs.netapp.com.

Data is the primary target

Cybercriminals increasingly target data directly, recognizing its value. While perimeter, network, and application security are important, they can be bypassed. Focusing on protecting data at its source, the storage layer, provides a critical last line of defense. Gaining access to production data and encrypting or rendering it inaccessible is the objective of ransomware attacks. To get there, attackers must have already pierced existing defenses deployed by organizations today, from perimeter to application security.

Unfortunately, many organizations don't take advantage of security capabilities at the data layer. This is where NetApp ransomware protection portfolio comes in, protecting you at the last line of defense.

The real cost of ransomware

The ransom payment itself is not the largest monetary effect on a business. Although the payment is not insignificant, it pales in comparison to the downtime cost of suffering a ransomware incident.

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024 organizations reported a mean cost to recover from a ransomware attack of $2.73M, an increase of almost $1M from the $1.82M reported in 2023 according to the 2024 Sophos State of Ransomware report. For organizations that rely heavily on IT availability, such as e-commerce, equities trading, and health care, costs can be 10 times higher or more.

Cyber insurance costs also continue to rise given the very real likelihood of a ransomware attack on insured companies.
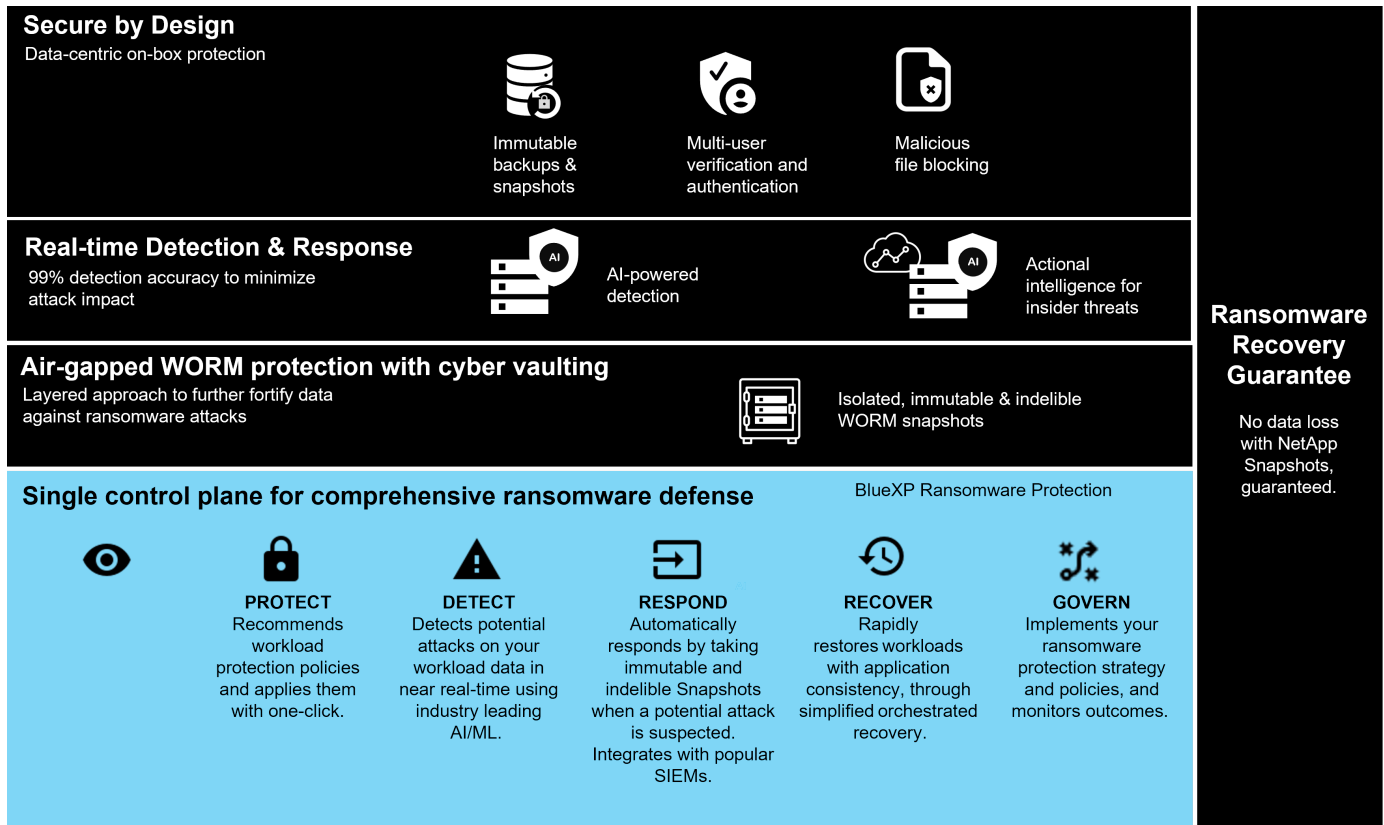
Ransomware protection at the data layer

NetApp understands your security posture is wide and deep across your organization from the perimeter to the where your data lives at the storage layer. Your security stack is complex and should provide security at every level of your technology stack.

Real-time protection at the data layer is even more important and has unique requirements. To be effective, solutions at this layer must offer these critical attributes:

- **Security by design** to minimize chance of successful attack
- **Real-time detection and response** to minimize impact of a successful attack
- **Air-gapped WORM protection** to isolate critical data backups
- **A single control plane** for comprehensive ransomware defense

NetApp can deliver all of this and more.

Secure by Design
Data-centric on-box protection

Immutable backups & snapshots

Multi-user verification and authentication

Malicious file blocking

Real-time Detection & Response
99% detection accuracy to minimize attack impact

AI-powered detection

Actional intelligence for insider threats

Air-gapped WORM protection with cyber vaulting
Layered approach to further fortify data against ransomware attacks

Isolated, immutable & indelible WORM snapshots

Single control plane for comprehensive ransomware defense

BlueXP Ransomware Protection

Ransomware Recovery Guarantee

No data loss with NetApp Snapshots, guaranteed.

PROTECT	DETECT	RESPOND	RECOVER	GOVERN
Recommends workload protection policies and applies them with one-click.	Detects potential attacks on your workload data in near real-time using industry leading AI/ML.	Automatically responds by taking immutable and indelible Snapshots when a potential attack is suspected. Integrates with popular SIEMs.	Rapidly restores workloads with application consistency, through simplified orchestrated recovery.	Implements your ransomware protection strategy and policies, and monitors outcomes.

NetApp's ransomware protection portfolio

NetApp's built-in ransomware protection delivers real-time, robust, multi-faceted defense for your critical data. At its core, advanced AI-powered detection algorithms continuously monitor data patterns, swiftly identifying potential ransomware threats with 99% accuracy. Reacting quickly to attacks allows our storage to quickly snapshot data and secure the copies ensuring rapid recovery.

To further fortify data, NetApp's cyber vaulting capability isolates data with a logical air gap. By safeguarding critical data, we ensure rapid business continuity.

NetApp NetApp ransomware protection reduces operational burdens with a single control plane to intelligently coordinate and execute an end-to-end workload-centric ransomware defense, so you can identify and protect critical workload data at risk with a single click, accurately and automatically detect and respond to limit the impact of a potential attack, and recover workloads within minutes, not days, safeguarding your valuable workload data and minimizing costly disruption.

As a native, built-in ONTAP solution for protecting unauthorized access to your data, multi-admin verification (MAV) has a robust set of capabilities that ensure that operations such as deleting volumes, creating additional administrative users, or deleting snapshots can be executed only after approvals from at least a second designated administrator. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data. You can configure as many designated administrator approvers as you want before a snapshot can be deleted.

> (i) NetApp ONTAP addresses the requirement for web-based multi-factor authentication (MFA) in System Manager and for SSH CLI authentication.

NetApp's ransomware protection offers peace of mind in an ever-evolving threat landscape. Its comprehensive approach not only defends against current ransomware variants but also adapts to emerging threats, providing long-term security for your data infrastructure.

Learn about other protection options

- Digital Advisor ransomware protection
- Data Infrastructure Insights Storage Workload Security
- FPolicy
- SnapLock and tamperproof snapshots

Ransomware recovery guarantee

NetApp offers a guarantee to restore snapshot data if a ransomware attack occurs. Our guarantee: If we can't help you restore your snapshot data, we'll make it right. The guarantee is available on new purchases of AFF A-Series, AFF C-Series, ASA, and FAS systems.

Learn more

- Recovery guarantee service description
- Ransomware recovery guarantee blog.

Related information

- NetApp Support site resources page
- NetApp product security

SnapLock and tamperproof snapshots for ransomware protection

A vital weapon in NetApp's Snap arsenal is SnapLock, which has proven highly effective in safeguarding against ransomware threats. By preventing unauthorized data deletion, SnapLock provides an additional layer of security, ensuring that critical data remains intact and accessible even in the event of malicious attacks.

SnapLock Compliance

SnapLock Compliance (SLC) provides indelible protection for your data. SLC prohibits data from being deleted even when an administrator attempts to re-initialize the array. Unlike other competitive products, SnapLock Compliance is not vulnerable to social engineering hacks through those products' support teams. Data protected by SnapLock Compliance volumes is recoverable until that data has reached its expiration date.

To enable SnapLock, an ONTAP One license is required.

Learn more

- Snaplock documentation

Tamperproof snapshots

Tamperproof Snapshot (TPS) copies provide a convenient and fast way to protect data from malicious acts. Unlike SnapLock Compliance, TPS is typically used on primary systems where the user can protect the data for a determined time and left locally for fast recoveries or where data does not need to be replicated off of the primary system. TPS uses SnapLock technologies to prevent the primary snapshot from being deleted even by an ONTAP administrator using the same SnapLock retention expiration period. Snapshot deletion is prevented even if the volume is not SnapLock enabled, although snapshots do not have the same indelible nature of

SnapLock Compliance volumes.

To make snapshots tamperproof, an ONTAP One license is required.

Learn more
- Lock a snapshot for protection against ransomware attacks.

FPolicy file blocking

FPolicy blocks unwanted files from being stored on your enterprise-grade storage appliance. FPolicy also gives you a way to block known ransomware file extensions. A user still has full access permissions to the home folder, but FPolicy doesn't allow a user to store files your administrator marks as blocked. It doesn't matter if those files are MP3 files or known ransomware file extensions.

Block malicious files with FPolicy native mode

NetApp FPolicy native mode (an evolution of the name, File Policy) is a file-extension blocking framework that allows you to block unwanted file extensions from ever entering your environment. It has been part of ONTAP for over a decade and is incredibly useful in helping you protect against ransomware. This Zero Trust engine is valuable because you get extra security measures beyond access control list (ACL) permissions.

In ONTAP System Manager and the NetApp Console, a list of over 3000 file extensions is available for reference.

> ⚠ Some extensions might be legitimate in your environment and blocking them can lead to unexpected issues. Create your own list that is appropriate for your environment before configuring native FPolicy.

FPolicy native mode is included in all ONTAP licenses.

Learn more
- Blog: Fighting Ransomware: Part Three — ONTAP FPolicy, another powerful native (aka free) tool

Enable user and entity behavior analytics (UEBA) with FPolicy external mode

FPolicy external mode is a file activity notification and control framework that provides visibility of file and user activity. These notifications can be used by an external solution to perform AI-based analytics to detect malicious behavior.

FPolicy external mode can also be configured to wait for approval from the FPolicy server before allowing specific activities to go through. Multiple policies like this can be configured on a cluster, giving you great flexibility.

> ⚠ FPolicy servers must be responsive to FPolicy requests if configured to provide approval; otherwise, storage system performance might be negatively impacted.

FPolicy external mode is included in all ONTAP licenses.

Learn more
- Blog: Fighting Ransomware: Part Four — UBA and ONTAP with FPolicy external mode.

Data Infrastructure Insights Storage Workload Security

Storage Workload Security (SWS) is a feature of NetApp Data Infrastructure Insights that greatly enhances the security posture, recoverability, and accountability of an ONTAP environment. SWS takes a user-centric approach, tracking all file activity from every authenticated user in the environment. It uses advanced analytics to establish normal and seasonal access patterns for every user. These patterns are used to quickly identify suspicious behavior without the need for ransomware signatures.

When SWS detects a potential ransomware, or data deletion, it can take automatic actions such as:

- Take a snapshot of the affected volume.
- Block the user account and IP address that is suspected of malicious activity.
- Send an alert to admins.

Because it can take automated action to quickly stop an insider threat as well as track every file activity, SWS makes recovery from a ransomware event much simpler and faster. With advanced auditing and forensics tools built in, users can immediately see what volumes and files were affected by an attack, which user account the attack came from, and what malicious action was performed. Automatic snapshots mitigate the damage and accelerate file restoration.

Total Attack Results

5	0	1,488
Affected Volumes	Deleted Files	Encrypted Files

1,488 Files have been copied, deleted, and potentially encrypted by **1 user account**.

This is potentially a sign of Ransomware Attack.

The extension ".wanna" was added to each file.

Alerts from ONTAP's Autonomous Ransomware Protection (ARP) are also visible in SWS, providing a single interface for customers using both ARP and SWS to protect from ransomware attacks.

Learn more

- NetApp Data Infrastructure Insights

NetApp ONTAP built-in on-box AI-based detection and response

As ransomware threats become more and more sophisticated, so should your defense mechanisms. NetApp's autonomous ransomware protection (ARP) is powered by AI with intelligent anomaly detection that is built in to ONTAP. Turn it on to add another layer of defense to your cyber resiliency.

ARP and ARP/AI are configurable through the ONTAP built-in management interface, System Manager, and enabled on a per-volume basis.

Autonomous Ransomware Protection (ARP)

Autonomous Ransomware Protection (ARP), another native built-in ONTAP solution since 9.10.1, looks at NAS storage volume workload file activity and data entropy to automatically detect potential ransomware. ARP provides administrators with real-time detection, insights, and a data recovery point for unprecedented on-box potential ransomware detection.

For ONTAP 9.15.1 and earlier versions that support ARP, ARP starts in learning mode to learn typical workload data activity. This can take seven days for most environments. After learning mode is complete, ARP will automatically switch to active mode and start looking for abnormal workload activity that might potentially be ransomware.

If abnormal activity is detected, an automatic snapshot is immediately taken, which provides a restoration point as close as possible to the time of attack with minimal infected data. Simultaneously, an automatic alert (configurable) 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.

If the activity is an expected workload, administrators can easily mark it as a false positive. ARP learns this change as normal workload activity and no longer flags it as a potential attack going forward.

To enable ARP, an ONTAP One license is required.

Learn more

- Autonomous Ransomware Protection

Autonomous Ransomware Protection/AI (ARP/AI)

Introduced as a tech preview in ONTAP 9.15.1, ARP/AI takes NAS storage systems on-box real-time detection to the next level. The new AI-powered detection technology is trained on over a million files and various known ransomware attacks. In addition to the signals used in ARP, ARP/AI also detects header encryption. The AI power and additional signals allow ARP/AI to deliver better than 99% detection accuracy. This has been validated by SE Labs, an independent test lab that gave ARP/AI its highest AAA rating.

Because training the models continuously happens in the cloud, ARP/AI does not require a learning mode. It is active the moment it is turned on. Continuous training also means that ARP/AI is always validated against new ransomware attack types as they arise. ARP/AI also comes with auto-update capabilities that deliver new parameters to all customers to keep ransomware detection up to date. All other detection, insight, and data recovery point capabilities of ARP are maintained for ARP/AI.

To enable ARP/AI, an ONTAP One license is required.

Learn more

- Blog: NetApp's AI-based real-time ransomware detection solution achieves AAA rating
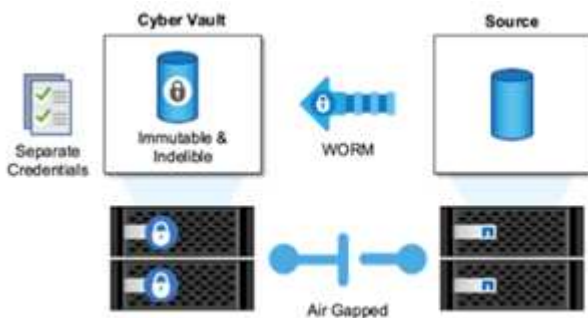
Air-gapped WORM protection with cyber vaulting in ONTAP

NetApp's approach to a cyber vault is a purpose-built reference architecture for a logically air-gapped cyber vault. This approach takes advantage of security hardening and compliance technologies, such as SnapLock, to allow for immutable and indelible snapshots.

Cyber vaulting with SnapLock Compliance and 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 (tape and offline media) can significantly increase restoration time, thus increasing downtime and the overall associated costs. Even a more modern approach to an air-gap solution can prove problematic. For example, if the backup vault is temporarily opened to receive new backup copies and then disconnects and closes its network connection to primary data to once again be "air gapped", an attacker could take advantage of the temporary opening. During the time the connection is online, an attacker could strike to compromise or destroy the data. This type of configuration also generally adds unwanted complexity. A logical air gap is an excellent substitute for a traditional or modern 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 snapshots and NetApp SnapLock Compliance.

NetApp released the SnapLock feature more than 10 years ago to address the requirements of data compliance, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, and other regulatory data rules. You can also vault primary snapshots 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 snapshots are locked and cannot be deleted, even by ONTAP administrators or NetApp Support.

Learn more

- Blog: ONTAP cyber vault overview

Tamperproof snapshots

While leveraging SnapLock Compliance as a logical air gap provides the ultimate protection in preventing attackers from deleting your backup copies, it does require you to move the snapshots using SnapVault to a secondary SnapLock-enabled volume. As a result, many customers deploy this configuration on secondary storage across the network. This can lead to longer restoration times versus restoring a primary volume Snapshot on primary storage.

Beginning in ONTAP 9.12.1, tamperproof snapshots provide near SnapLock Compliance level protection for your snapshots on primary storage and in primary volumes. There is no need to vault the snapshot using SnapVault to a secondary SnapLocked volume. Tamperproof snapshots use SnapLock technology to prevent the primary snapshot from being deleted, even by a full ONTAP administrator using the same SnapLock retention expiration period. This allows for quicker restore times and the ability for a FlexClone volume to be backed up by a tamperproof, protected snapshot, something you cannot do with a traditional SnapLock

Compliance vaulted snapshot.

The major difference between SnapLock Compliance and tamperproof snapshots is that SnapLock Compliance does not allow the ONTAP array to be initialized and wiped if SnapLock Compliance volumes exist with vaulted snapshots that have not yet reached their expiration date. To make snapshots tamperproof, a SnapLock Compliance license is required.
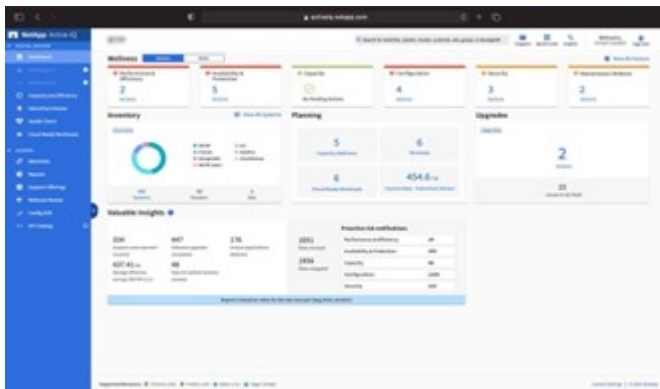
Learn more

- Lock a snapshot for protection against ransomware attacks

Digital Advisor ransomware protection

Digital Advisor powered by Active IQ simplifies the proactive care and optimization of NetApp storage with actionable intelligence for optimal data management. Fueled by telemetry data from our highly diverse installed base, it uses advanced AI and ML techniques to uncover opportunities to reduce risk and improve the performance and efficiency of your storage environment.

Not only can NetApp Digital Advisor 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.

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

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

To see ransomware protection in action, see Digital Advisor.

Comprehensive resilience with NetApp ransomware protection

It is important for ransomware detection to occur as early as possible so that you can prevent the spread and avoid costly downtime. An effective ransomware detection strategy, however, should include more than a single layer of protection. NetApp's ransomware protection takes a comprehensive approach that includes real-time, on-box capabilities extending to data services using the NetApp Console and an isolated, layered

solution for cyber vaulting.

NetApp ransomware protection

The NetApp Console is a single control plane to intelligently orchestrate a comprehensive, workload-centric ransomware defense. NetApp ransomware protection brings together the powerful cyber-resilience features of ONTAP, such as ARP, FPolicy, and tamperproof snapshots, and NetApp data services, such as NetApp Backup and Recovery. It also adds recommendations and guidance with automated workflows to provide an end-to-end defense through a single UI. It operates at the workload level to ensure that the applications that run your business are protected and can be recovered as quickly as possible in case of an attack.

Customer benefits:

- Assisted ransomware preparedness reduces operational overhead and improves efficacy
- AI/ML-powered anomaly detection delivers greater accuracy and faster response to contain risk
- Guided application-consistent restoration allows you to recover workloads more easily and within minutes

NetApp ransomware protection makes these NIST functions easier to achieve:

- Automatically **discover** and prioritize data in NetApp storage **with a focus on top application-based workloads**.
- **One-click protection** of top-workload data backup, immutable, secure configuration, malicious file blocking, and different security domain.
- **Accurately detect** ransomware as **quickly** as possible using **next-generation AI-based anomaly detection.**
- Automated response and workflows and integration with top **SIEM and XDR solutions.**
- Rapidly restore data using a simplified **orchestrated recovery** to accelerate application uptime.
- Implement your ransomware protection **strategy** and **policies**, and **monitor outcomes**.