SERVICE DESCRIPTION

Ransomware Protection and Recovery Service

NetApp

NetApp

Service background and overview

The customer has requested NetApp to provide NetApp® Managed Professional Services, NetApp Ransomware Protection and Recovery Service (hereinafter referred to as "Ransomware Protection and Recovery Service" or "Professional Services") as described in this document. NetApp technical resources will deliver the skills, knowledge, and expertise that are needed to meet specific customer objectives and to maximize the investment that the customer has made in NetApp technology.

NetApp Professional Services provides operational excellence and optimization for customers' NetApp solutions in hybrid cloud environments. The NetApp Ransomware Protection and Recovery Service is remotely delivered as a 1-year minimum fixed-price subscription service with options for local delivery. The service is built around NetApp anti-ransomware software solutions, which provide proactive detection of ransomware attacks and the ability to recover data quickly by using protected NetApp Snapshot™ copies. When customers combine the Professional Services with the NetApp ONTAP® anti-ransomware solutions, they are assured of strong ransomware protection. Although no technology vendor can guarantee that customers will not be impacted by a ransomware event, NetApp can assist in minimizing business disruptions by protecting customer data where ransomware viruses are targeted—at the data layer.

The NetApp Ransomware Protection and Recovery Service includes implementation and administration services for the following solutions:

- Cloud Insights and Cloud Secure
- SnapLock® compliance software
- SnapMirror® replication software
- Multi-Key Management/Advanced Data Encryption
- Active IQ® and Active IQ Unified Manager
- SnapCenter® software
- FPolicy

These operational services are delivered remotely as standard practice and can be customized with on-premises and/or on-shore delivery via a custom statement of work (SOW).

With these services, customers can rely on NetApp or an authorized partner to perform implementation, management, and data recovery tasks to ensure the continuous health of the ransomware solutions by making sure that the tools are connected, receiving data, and issuing ransomware warnings and alerts on a 24/7/365 basis. Tasks include 24/7 monitoring, triage and remediation, periodic software upgrades (including ONTAP), and ransomware file allowed-listing and block-listing, as well as ensuring that backups are immutable and logically air gapped to assist with quick recovery from clean data.

Key benefits

Although all customers need to have a ransomware strategy, many are not aware of their data protection gaps or knowledgeable about what solutions are available. The NetApp Ransomware Protection and Recovery Service begins with a Discovery and Design phase to identify gaps in data protection as well as to understand how the NetApp solution can coexist with existing ransomware efforts.

Another key benefit of the service is that NetApp monitors and responds to ransomware alerts 24/7, because most attacks are launched outside of normal business hours.

Effectively, the service is designed to bring together NetApp's ransomware software solutions into a cohesive solution to protect against and recover from ransomware events.

Scope of Managed Services
NetApp will provide a qualified team to deliver the Ransomware Protection and Recovery Service. If this service description does not meet the customer's requirements, a statement of work (SOW) is necessary. The service will be delivered remotely, unless the customer specifies otherwise. NetApp will assign a shared Project Manager (PM) or Service Delivery Manager (SDM) in accordance with the scope of the service. The SDM or PM will be responsible for managing the service delivery process and will be the primary interface between the customer and the NetApp teams.

Service delivery
The Managed Services will be delivered in distinct phases. During the Discovery and Design phase, NetApp will collect the necessary data from the customer's environment, including the existing data protection policies, ransomware risks, and ability to recover from a ransomware event. NetApp will also discover the current ONTAP version and the potential gaps in anti-ransomware tools (NetApp native) to be configured. In addition, NetApp will review and define communication plans, escalation procedures, and onboarding expectations.

During the Project Implementation phase, NetApp will begin configuring the anti-ransomware tools, configure data protection and SnapMirror relationships, and begin monitoring and managing the defined elements of the customer's environment, including the anti-ransomware solutions listed above.

During the Project Closeout phase, NetApp will review deliverables and begin the final acceptance process.

Service tasks
In preparing to deploy the Ransomware Protection and Recovery Service, NetApp performs the following tasks:

- Conduct an engagement kickoff meeting of up to 1 hour to review the scope of the engagement and to gather details necessary to provide the service.
- Review which clusters or nodes the anti-ransomware solutions will be deployed on.
- Test the credentials necessary to perform the service.
- Establish communication plans.
- Create a deployment schedule.
- Review existing documentation, if provided by the customer.
- Document roles and responsibilities of customer contacts, if required.
- Review support status (customer's existing support contracts and end-of-support dates).
- Establish or review escalation procedures.

When these tasks are complete, the Managed Service is delivered in three phases: (1) Discovery and Design, (2) Project Implementation, and (3) Project Closeout.

Discovery and Design phase
The Discovery and Design phase involves the following tasks:

- Review the customer's environment and determine which nodes the NetApp anti-ransomware suite will be installed on.
- Determine the current version of ONTAP and upgrade to 9.10.1 or later if necessary.
- Document SnapLock policy definitions.
- Review the current retention period of the source SnapLock Compliance files.
- Review available Cloud Insights devices and services that Cloud Insights can collect data and report on (known as data collectors) for the environment.

- Review available Cloud Insights acquisition units for the environment.
- Review ransomware protection and recovery reporting requirements.
- Review customer RPO and RTO requirements.
- Review existing ransomware software status, including NetApp and third-party software.
- Configure alert settings.
- Review reporting requirements.
- Review communication and escalation procedures.
- Review deployment schedule and activation planning activities.
- Review roles and responsibilities.
- Create and review an ONTAP Upgrade Plan.

Project Implementation

The Project Implementation phase involves the following tasks.

Implementation and administration tasks

Multi-key management:

- Install multi-key management/advanced data encryption license to enable encryption of data at rest.

Cloud Insights and Cloud Secure implementation:

- Verify Cloud Insights portal.
- Deploy acquisition units (if needed).
- Configure collectors.
- Configure allotted annotations.
- Configure allotted dashboards.
- From the Cloud Insights menu:
  - Deploy Cloud Secure User Agents.
  - Deploy Cloud Secure Active Directory Data Collector.
  - Deploy Cloud Secure Lightweight Directory Access Protocol (LDAP)Data Collector.
  - Deploy Cloud Secure SVM Data Collector.

Cloud Insights and Cloud Secure administration:

- Monitor health and connections of Cloud Insights and Cloud Secure.
- Make sure that the Cloud Secure environment is healthy and is able to receive data from Customer volumes.
- Send alerts to contacts provided by the customer for joint remediation.
- Monitor availability of Snapshot copies and capacity for Snapshot copies.
- Set up monitoring to view snap count and volume capacity to make sure that Cloud Secure is able to take and store Snapshot copies of Customer volumes.

SnapLock implementation:

- Install SnapLock.
- Initialize the ComplianceClock.
- Create SnapLock aggregates or volumes (FlexVol® volumes) or mount volumes.
- Set the retention time
- Verify SnapLock settings.

SnapLock administration:

- Administer SnapLock Log via existing APIs.
- Administer SnapLock ComplianceClock via existing APIs.
- Administer Event Retention via existing APIs.
- Administer File Retention and Privileged Delete via existing APIs.
- Administer File Fingerprint via existing APIs.
- Administer Legal Hold via existing APIs.

Snapshot and SnapMirror configuration:

- Enable Snapshot and SnapMirror policies based on recommendations from the Design and Discovery phase.
- Create and initialize Snapshot Schedule, Policy, Relationships, and Destination volume (up to six policies or relationships).

Snapshot and SnapMirror administration:

- Manage, triage, and resolve Snapshot, SnapMirror, and SnapVault® alerts 24/7/365.
- Manage the NetApp SnapMirror replication software and the NetApp SnapVault storage backup feature of ONTAP: Configure data protection (DP) and extended data protection (XDP) relationships, creating replication policies and job scheduling, and converting DP relationships.
- Configure destination volumes, restoring files from destination volumes, making the destination volumes writable, resynchronizing replication relationships, managing SnapMirror root volume replication, and updating load-sharing mirror relationships

SnapCenter implementation:

- Install SnapCenter server.
- Perform SnapCenter configuration
- Add storage connections (licensing).
- Configure RBAC.
- Add Run As credentials.
- Prepare storage for SnapMirror and SnapVault replication, if necessary.
- Create policies and backup schedules.
- Create resource groups.
- Back up the resources or resource groups and SnapCenter server repository.

SnapCenter administration:

- Add or modify users or groups and create or assign roles and assets.
- Monitor, triage, and remediate failed backup jobs and SnapCenter events.
- Monitor licensed capacity alerts.
- Provide SnapCenter reports: Backup, Clone, Restore, and Protection reports.
- Manage SnapCenter policies.

FPolicy configuration and administration:

- Determine mode: Native or External mode.
- Create FPolicy event.
- Create FPolicy policy.
- Configure the policy.
- Enable the policy.
- Modify FPolicy configurations per customer's requirements.

Active IQ and Active IQ Unified Manager configuration:

- Perform initial setup.
- Add clusters, if required.
- Configure remote authentication.
- Add users and alerts (if required).

ONTAP upgrades

- NetApp upgrades ONTAP systems to the designated version, according to the ONTAP Upgrade Plan.
- Update service processors.
- Verify that corresponding firmware is upgraded, as required.
- Confirm upgrades of any SAN host drivers and firmware to designated versions.
- Validate end-to-end configuration.
- Install the qualification package and the latest disk firmware.
- Roll the system back to an earlier version, if required.
- Perform post-upgrade tasks: Verify the cluster version, verify cluster health, and reenable features.

Data recovery

- Recovery activities must be performed in conjunction with customer participation. NetApp and customer will develop a RACI chart to identify customer and NetApp teams to participate in recovery activities.
- Assist in making sure that data is in place to meet the customer's recovery needs.
- Assist in confirming that ransomware spread is contained (NetApp assistance with customer interaction).
- Restore data protected under the ransomware solution using SnapCenter operations (NetApp primary, customer secondary).
- Assist with data recovery testing and continue monitoring during and after recovery.
- NetApp and customer confirm that the ransomware event is contained, business continuity is recovered, and root cause analysis (RCA) assistance is performed. (Provide input to the customer from the ONTAP anti-ransomware solution to assist with any customer RCA of the ransomware attack.)
- Snapshot and/or volume rollback to data available prior to attack.
- Volumes restored based on Customer-communicated priority.

Operational reporting

NetApp Managed Services will produce reports on the environment for review of the services being delivered by the NetApp Managed Services team. Reports will include a selection of those shown in Table 1.

Report type	Report details	Frequency
Alert Executive Summary		Monthly
Service Operations report	• Incidents including service level metrics • Changes • Problems and service risks • Service improvement review and recommendations • Open Issues	Monthly
Cloud Secure reports	NetApp will provide historical reporting of Cloud Secure alerts (attacks and warnings).	Monthly
SnapCenter reports	Backup, Clone, Restore, and Protection reports	Monthly
Post-incident report (High Severity only)		As occurred
Post-implementation review		As occurred
Root cause analysis (High Severity only)	Environmental operational status	As needed
Health check	Custom reporting is limited to small efforts, under 2 hours of labor required for both compiling and preparing the data. Larger reporting requirements are considered a project and are out of scope. Additional reporting services can be purchased under separate agreement.	Daily
Custom (ad hoc) reports	Custom reporting is limited to small efforts, under 2 hours of labor required for both compiling and preparing the data. Larger reporting requirements are considered out of scope. Additional reporting services can be purchased under separate agreement.	Upon negotiation

Table 1) Environmental reports.

Project Closeout

- Review project deliverables with the customer.
- Obtain Certificate of Completion and customer acceptance.

Deliverables

In connection with the Managed Services, NetApp will provide the following tangible materials (the "Deliverables") to the customer in a format or method mutually agreed upon between the parties:

- ONTAP Upgrade Plan
- Daily Health Check report
- Notification of exceptional events as they occur
- Monthly Alert Executive Summary report
- Monthly Service Operations report
- Post-Incident report, as required
- Monthly SnapCenter reports
- Root cause analysis, as needed

- Post-implementation review, as needed
- Custom reports as needed, upon negotiation

Project-specific assumptions and customer responsibilities

The following assumptions are hereby acknowledged by the parties and apply to the performance of the Managed Services.

Managed Service: General

- If the customer fails to implement any of NetApp's recommendations or requirements, or makes changes to the customer equipment being managed by the NetApp Managed Services team, NetApp will not be held responsible for failures of performance of the Managed Services.
- Customer will maintain and upgrade, as necessary, its equipment to the minimum required versions as specified in the NetApp Interoperability Matrix.
- Customer will maintain an active SupportEdge Premium Support agreement (if applicable) throughout the Managed Services term for the customer equipment in scope for the Ransomware Protection and Recovery Service.
- NetApp Managed Services requires remote access to the customer equipment and uses the following steps and technologies:
  - NetApp uses a virtual appliance (gateway) to function as a monitoring device that collects monitoring data from the customer equipment.
  - The gateway needs outbound internet connectivity to the cloud, via ports 443, 22.
  - The gateway needs DNS access to resolve *.api.opsramp.io.
  - Managed devices are configured via the web portal for remote access to the device's service processor or switch service port via SSH.
  - All activity through the gateway is logged and can be recalled for auditing as required.
  - The gateway processes SNMP events and traps locally and sends resultant alerts to the remote monitoring portal via a secure channel. The gateway does not collect, and has no means to collect, any customer data that it processes.
  - No ongoing management is required for the gateway. For any troubleshooting purposes, NetApp will log into the gateway though remote shell by launching a console and will contact the customer if required.
  - Gateway requirements for up to 25 devices: 2 virtual CPUs, 4GB RAM, 40GB disk, 1 NIC.
  - Gateway requirements for up to 100 devices: 4 virtual CPUs, 8GB RAM, 40GB disk, 1 NIC.
  - Supported hypervisors: VMware ESXi, Citrix XenServer, Microsoft Hyper-V, and KVM.
- If the management agent machine residing at the customer site is down or off line, preventing monitoring of the customer equipment, NetApp will contact the customer for assistance in power cycling or other troubleshooting.
- NetApp has the right to share the customer reports with its subcontractors assigned.
- Customer will provide contact lists for 24/7/365 incident escalation.
- Customer will provide a static public IP address on the firewall.
- Customer must resolve all alarms before live operations commence.
- Customer must provide 24 hours' notice of planned maintenance involving any configuration items, such as CI record, controller, volume.
- Customer must provide an administrator for remote support utility sessions, as required.
- Customer must maintain compatibility of interacting external systems or environments at all times.

Managed Service: NetApp Ransomware Protection and Recovery Service

- For Cloud Secure scope, customer must have purchased one or more enterprise-level Cloud Insights license.
- During data restoration, NetApp will work alongside the customer, using the SnapCenter platform.
- Prior to recovery, the customer will isolate, patch, and test users impacted by ransomware. NetApp will make sure that this step is completed prior to restoration activities.
- In addition to storage teams, additional personnel from the customer's application, compute, and network teams may be required to conduct a successful DR test.
- Customer will grant the NetApp team proper access to the managed environment to perform administration and management tasks.
- NetApp Professional Services will deploy the ONTAP anti-ransomware solution or components required to perform the service.
- The Discovery phase of the project requires tools for data collection (Cloud Insights, Active IQ Unified Manager) and can begin after tool configuration.
- For each cluster that the anti-ransomware solutions will be installed on, the minimum ONTAP release required is 9.10.1.
- The customer will upgrade any SAN host drivers and firmware to designated versions.
- The ONTAP upgrade service includes up to two upgrades annually for two nodes.
- Recovery activities must be performed in conjunction with customer participation. NetApp and the customer will develop RACI to identify customer and NetApp teams to participate in recovery activities.

Project exclusions and out of scope activities

Project exclusions are any items that are not expressly included below:

- NetApp and the NetApp Ransomware Protection and Recovery Service do not guarantee that (a) the customer will not be impacted by a ransomware attack; or (b) the Recovery Services will be successful in recovering any or all lost customer data. Further, NetApp will not be held responsible for any data loss suffered as a result of a ransomware attack.
- Purchase of hardware, licensing of software, and any associated support services. (Any hardware and software and support requested or needed by customer, in relation to the Managed Services, will be purchased separately by customer.)
- Relocation of customer equipment.
- Installation of customer equipment.
- Development of customer-requested automation routines.
- Data migration planning and execution services.
- Development of designs to address new customer requirements.
- Transformational consulting services: service improvement planning, business process engineering, data analytics, custom software development, and systems integration.
- Logical and physical decommissioning services: data eradication, disk degaussing, hardware destruction, and recycling services.
- Design activities in relation to SnapCenter for a new implementation or expansion of use.
- Configuration of new applications for SnapCenter.
- Application configuration. Any linkage between SnapCenter and an application is configured within the SnapCenter application.
- Knowledge transfer is not included as part of this scope. Training is available through NetApp Learning Services.

Service level objectives

NetApp Managed Services service level objectives (SLO) is a policy that governs the delivery of the Managed Services; it applies only to components within the NetApp managed environment that are within the control of the NetApp defined service. NetApp will use reasonable commercial efforts to adhere to SLOs (as defined below).

Incident response time

NetApp will record and categorize incidents and respond based on the priority of the issue. The priority of incidents is defined by impact and urgency. Any discrepancies in the incident classification are escalated to the Service Delivery Manager. Impact considers the size, scope, and scale of an issue. Urgency defines the criticality, such as Critical, Important, Normal, or Low.

Definitions

- **Time to Respond** is defined as the elapsed time between the Receipt of Call about an incident and:
  - If the Incident is managed by the customer, the time that NetApp's representative who will perform the related incident management tasks contacts the incident resolution team or nominated contact; or
  - The time NetApp that allocates a representative to work on the incident and contacts the authorized user reporting the incident.
- **Receipt of Call** means the earlier of:
  - NetApp becoming aware of the incident via automated notification from its monitoring systems;
  - NetApp becoming aware of the incident via notification from the customer or other service providers; or
  - the time the service desk notifies NetApp of the incident.

SLO: Incident response time

Priority	Time to respond	Definition
P1	15 minutes	**Priority 1: Critical.** Severe business impact, data availability affected, or a state of degraded performance sufficient to prevent normal business operations. At this level, both NetApp and the customer must commit to around-the-clock action and involvement by all necessary and appropriate personnel and systems until a mutually agreeable workaround is provided and the priority level is downgraded.
P2	30 minutes	**Priority 2: Important.** Experiencing infrequent, isolated, or intermittent service interruptions, or in a state of degraded performance that allows business operations to continue but at an inconsistent or less than optimal rate. At this level, NetApp is committed to a commercially reasonable best effort to provide a workaround and/or to restore normal operations as quickly as possible.
P3	45 minutes	**Priority 3: Normal.** Noncritical operational impact with no direct impact on service availability, inflicts little or no business impact, and a viable and mutually agreeable workaround or hardware or software upgrade exists to mitigate the problem.
P4	120 minutes	**Priority 4: Low.** Noncritical requests with no business impact or financial impact.

Table 2) NetApp incident response times by priority.

SLO assumptions

- All service levels presented will be aligned with the technology and workflow and service level tiers being offered to the customer.
- Service level objectives may be offered as part of Managed Services offerings that do not include service level agreements (SLAs). NetApp will perform Managed Services in a professional and workmanlike manner in accordance with industry standards. The customer will not receive any credits, discounts, fee adjustments, and/or other concessions based on the performance of standard Managed Service offerings.
- Service level measurements exclude the following:
  - Any delays caused by customer, such as obtaining change approval.
  - Operational errors, accidents, negligence, abuse, misuse, unauthorized alteration, or modification by customer or its third-party contractors.
  - Movement of hardware or software without NetApp's prior written approval.
  - Customer's failure to provide an installation environment or product configuration in accordance with the documentation.
  - Use of the hardware or software for other than the specific purpose for which such hardware or software is designed.
  - Any third-party hardware or software installed in the system.
  - Issues related to nonimplementation of any required corrective actions for which NetApp has provided prior written notice of such requirement.
  - Any mutually agreed schedule for activities that may fall outside the service level.
  - Any issues caused by third parties for support.
  - A security intrusion or virus attack for which NetApp is not responsible.
  - Any network outage or data center outage.
  - If NetApp is unable to access or customer has not provided on-site access and/or remote access is prohibited or not made available to NetApp.

Schedule of performance

The estimated Ransomware Protection and Recovery Service start date is approximately 2 weeks from the date of the customer's approved purchase order. If performance of the service does not begin within 1 year of the purchase order date, and there is no written change request, the order is automatically terminated. Services must be delivered during consecutive months after the actual start date. The number of consecutive months is identified in the Managed Services Implementation Details document that NetApp provides.

Information and expertise

The Customer will make available to NetApp staff:

- Accurate, complete, and up-to-date documentation and information.
- Knowledgeable staff and system administrators who can be contacted by pager, telephone, or cellphone. These contacts will provide background information and clarify information that is required to perform the Ransomware Protection and Recovery Service.

Communication

The Customer is responsible for all communication to their internal users, including notification of maintenance and migration windows, as required.

Licenses
The customer must obtain from third parties any and all permissions and licenses that are necessary for NetApp or a NetApp subcontractor to successfully perform the Ransomware Protection and Recovery Service. The customer hereby grants these licenses to NetApp and its subcontractors.

Fee description and payment
Before performing the Ransomware Protection and Recovery Service, NetApp requires an approved purchase order from the customer or from an authorized reseller that is acceptable to NetApp. NetApp will invoice upon receipt of an approved purchase order. Payments are nonrefundable, with no right to refund or credit. If the customer requires any additional time, a new NetApp sales quote and purchase order will be required.

Change process
- Changes to this service description will be documented in a change request.
- Any renewals or scheduling adjustments that affect the fees will require a new NetApp sales quote.
- Implementation of any additional services that affect the pricing will require an approved customer change order to the customer's existing purchase order or an additional purchase order.

Acceptance
- Upon completion of the engagement, the customer will receive a Certificate of Completion form to sign.
- If the Certificate of Completion form is not signed within 5 business days from the customer's receipt, the work will be deemed accepted unless the customer submits a written notification of a service performance issue.

Incorporated terms
In the absence of an effective written agreement between the parties expressly governing the Ransomware Protection and Recovery Service, this service is governed by the standard NetApp Professional Services terms, posted at www.netapp.com/us/how-to-buy/stc.html, as of the sales quotation date. The standard NetApp Professional Services terms are incorporated herein by reference. If the customer wants to negotiate any of these terms, a NetApp statement of work (SOW) is required.

NetApp