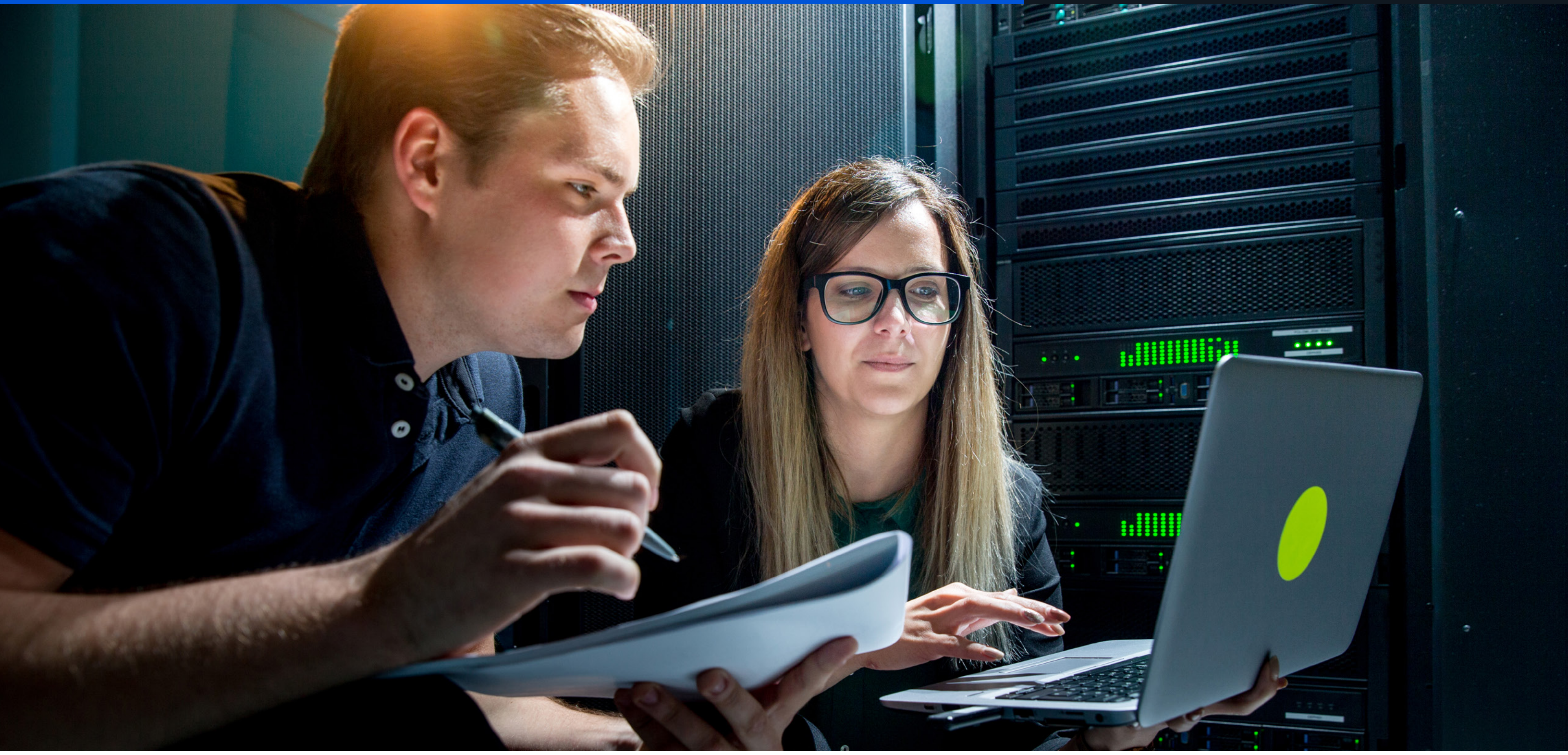
SERVICE DESCRIPTION

NetApp Ransomware Recovery Assurance Service

NetApp



Service background and overview

The customer has requested NetApp to provide NetApp® Managed Professional Services, to support the NetApp Ransomware Recovery Guarantee Program (hereinafter referred to as “Ransomware Recovery Assurance 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 NetApp solutions in hybrid cloud environments. The NetApp Ransomware Recovery Assurance Service is remotely delivered as a fixed-price subscription service with options for local delivery. The service is built around NetApp’s anti-ransomware software solutions that provide an immutable data vault for critical data and the ability to recover data quickly by using protected NetApp Snapshot™ copies. When customers combine the Ransomware Recovery Assurance Service with NetApp ONTAP® anti-ransomware solutions, customers recover data quickly. Although no technology vendor can prevent customers from being affected by a ransomware event, NetApp can assist in minimizing business disruptions by protecting NetApp assets where ransomware viruses are targeted—at the data layer.

The Ransomware Recovery Assurance Service includes implementation, validation, data recovery testing, and 24/7/365 recovery services for the rapid recovery of protected data.

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

Key benefits

By performing this service, NetApp Professional and Managed Services ensures that customers meet the terms of the NetApp Ransomware Recovery Guarantee Program. Additionally, the service provides critical services such as data recovery testing so that the customer has confidence that, working with NetApp, data can be recovered quickly.

Scope of managed services

NetApp will provide a qualified team to deliver the service as defined in this service description. If this service description does not meet the customer's requirements, a 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/PM will be responsible for managing the service delivery process and will be the primary interface between the customer and the NetApp teams.

Service tasks

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

- Conducting an engagement kickoff meeting (if necessary) of up to 1 hour to review the scope of the engagement and to gather details necessary to provide the service
- Reviewing which systems/nodes the anti-ransomware solutions will be deployed on.
  The program requires the purchase of a new ONTAP FAS, AFF, or ASA system
- Testing the credentials necessary to perform the service
- Establishing communication plans
- Creating a deployment schedule
- Reviewing existing documentation, if provided by the customer
- Documenting roles and responsibilities of customer contacts, if required
- Reviewing support status (customer's existing support contracts and end-of-support dates)
- Establishing or reviewing escalation procedures
- Reviewing NetApp SnapLock® Compliance policy definitions
- Reviewing the current retention period of the SnapLock Compliance files (if required)

Project implementation
In preparing to deploy the Ransomware Recovery Assurance Service, NetApp performs the following tasks:

- **Implementation phase: SnapLock Compliance implementation/validation**
  Snaplock Compliance: The customer can choose to do the SnapLock Compliance implementation themselves or have NetApp perform this work. If the customer chooses to do the configuration themselves, the NetApp Services team will validate the configuration, performing tasks that may include:
  - Installing SnapLock Compliance
  - Initializing the compliance clock
  - Creating SnapLock aggregates/volumes (NetApp FlexVol®)/Mount volume(s)
  - Setting the retention time
  - Verifying SnapLock settings
  - Enabling the SnapLock for NetApp SnapMirror® vault (NetApp SnapVault®) configuration

- **Implementation phase: SnapLock Compliance volume configuration report**

  The SnapLock configuration report is provided to the customer and the NetApp teams managing the participation in the NetApp Ransomware Recovery Guarantee Program. The report identifies which SnapLock Compliance volumes have been validated to meet best practices for configuration and therefore acceptance in the program. The report may contain the following details:

  - SnapLock Compliance volume names that have been validated
  - The name of the aggregate that contains the volume
  - The default/maximum/minimum retention period for the volume(s)
  - The volume retention period expiry date/time
  - The system model and serial number

- **Implementation phase: Data recovery testing**

  Data recovery testing is limited to in-scope ONTAP controllers and designated volumes. NetApp will participate in one annual recovery test (additional tests may be added).

  NetApp responsibilities for data recovery testing:

  - Providing input to the customer business continuity plan (BCP) and disaster recovery (DR) plan
  - Participating in customer-driven BCP and DR testing
  - Maintaining the BCP and DR plan for the NetApp managed environment
  - Coordinating cross-functional BCP and DR testing of the managed environment
  - Undertaking BCP and DR testing as negotiated with the customer

  Customer responsibilities for data recovery testing:

  - Defining and producing customer BCP and DR plans
  - Prioritizing the services to be recovered via business impact analysis
  - Validating whether IT service continuity strategies can continue to meet the customer's business requirements
  - Testing, reviewing, and revising the plan on a regular basis

- **Implementation phase: Data recovery**

  Data recovery may involve the following activities:

  - Recovery activities must be performed in conjunction with customer participation. NetApp and the customer will develop RACI (responsible, accountable, consulted, and informed) processes to identify the customer and NetApp teams that will participate in recovery activities.
  - NetApp will assist in ensuring that data is in place to meet customer recovery needs.
  - NetApp and the customer will verify that the threat is an actual ransomware attack and not a false positive or some other intrusion.
  - NetApp and the customer will restore volumes and/or files protected by SnapLock Compliance in either FlexVol volumes, ONTAP FlexGroup volumes, or storage virtual machines (SVMs). Snapshot and/or volume rollback to data available prior to the attack. Volumes will be restored based on the priorities designated by the customer.
  - NetApp and the customer will mount Snapshot copies for restore by using NetApp SnapCenter® plug-ins or native host tools, then copy to the data restore directory.

- **Project closeout**

  To close out the project, NetApp will:

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

Deliverables

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

- SnapLock Compliance volume configuration report
- Certificate of Completion

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 Services—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.
- NetApp Professional Services will provide recovery support and consulting for up to one recovery event in any 12-month period in which the customer is engaged in the NetApp Ransomware Recovery Guarantee Program. A recovery event may span across mutliple nodes and volumes that are covered under the Guarantee Program. Additional recovery services may require additional fees.
- The customer will maintain and upgrade, as necessary, its equipment to the minimum required versions as specified in NetApp`s interoperability matrix.
- The customer will maintain an active NetApp SupportEdge Premium support agreement throughout the Managed Services Term for the customer equipment in scope for the Ransomware Recovery Assurance Service.
- The customer will confirm that all in-scope customer equipment is remotely accessible to NetApp resources through remote VPN or alternative gateway access. The customer will provide virtual desktop infrastructure ("VDI") with VPN or alternative gateway access to NetApp resources for purposes of performing activities and tasks defined. For on-site resources, security passes to customer site locations identified will be provided to NetApp resources.
- The customer must resolve all alarms prior to live operations commencing.
- The customer must notify NetApp of critical incidents and ransomware attacks.
- The customer must provide an administrator for remote support utility sessions, as required.
- The customer must maintain compatibility of interacting external systems or environments at all times.

Managed services—NetApp Ransomware Recovery Assurance Service

- During data recovery, NetApp will work alongside the customer, using the SnapCenter platform if necessary.
- Prior to recovery, the customer will isolate/patch/test users affected by ransomware. NetApp will ensure that this step is completed prior before starting restoration activities.
- In addition to storage teams, additional customer personnel from application, compute, and network teams may be required to conduct a successful DR test.
- The customer will grant the NetApp team proper access to the managed environment to perform administration and management tasks.
- For each cluster that the anti-ransomware solutions are to be installed on, the minimum ONTAP release required is:
  - For NetApp FAS, AFF A-Series, and AFF C-Series: ONTAP 9.12.1 P1 or later
  - For NetApp ASA A-Series: ONTAP 9.13.1 P2 or later
  - For NetApp ASA C-Series: ONTAP 9.13.1 P2 or later
- Recovery activities must be performed in conjunction with customer participation. NetApp and the customer will develop RACI processes to identify the customer and NetApp teams that will participate in recovery activities.
- Data recovery testing is required only during the 12-month term of the Ransomware Recovery Assurance Service.

Project exclusions and out-of-scope activities

The following items are excluded or out of scope for the NetApp Ransomware Recovery Assurance Service.

- NetApp and the NetApp Professional Services for the Ransomware Recovery Guarantee Program does not guarantee that the customer will not be affected by a ransomware attack.
- Monitoring and incident management for ransomware alerts and the ONTAP controllers is outside the scope of this schedule of performance but may be added at an extra cost.
- Purchase of hardware, licensing of software, and any associated support services (any hardware, software, and support requested or needed by the customer, in relation to the managed services, will be purchased separately by the customer.
- Relocation of customer equipment.
- Installation of customer equipment.
- Development of customer-requested automation routines.
- Data migration planning and data migration execution services.
- Development of designs to address new customer requirements.
- Transformational consulting services, such as service improvement planning, business process engineering, data analytics, custom software development, and systems integration.
- Logical and physical decommissioning services, such as data eradication, disk degaussing, hardware destruction, and recycling services.
- Design activities in relation to SnapCenter for a new implementation or expansion of use is not covered as part of this engagement.
- 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

The NetApp Managed Services Service-Level Objectives ("SLO") is a policy governing the delivery of the managed services and 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 and restoration time

As part of incident management, 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 SDM. Impact considers the size, scope, and scale of an issue; urgency defines the criticality, such as Critical, Important, Normal, and Low.

Definitions

- Time to Respond is defined as the elapsed time between the Receipt of Call of an incident and:
  - If the incident is managed by the customer, the time at which the NetApp representative (who will perform the related incident management tasks) contacts the incident resolution team or nominated contact; or
  - The time at which NetApp 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 notification from the customer or other Service Providers; or
  - The time at which the customer notifies NetApp of the incident.

SLO: Incident response time

Table 1 provides the Time to Respond for each incident type. This applies to storage only and not to any customer storage-dependent components, such as servers connected to the storage.

Priority	Time to Respond	Definition
P1	Business hours: Within 15 minutes Non-business hours: 4 hours	**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	Business hours: Within 30 minutes Non-business hours: 8 hours	**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 restore normal operations as quickly as possible.
P3	Business hours: Within 45 minutes Non-business hours: 24 hours	**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/software upgrade exists to mitigate the problem.
P4	Business hours: Within 120 minutes Non-business hours: 72 hours	**Priority 4: Low.** Noncritical requests with no business impact or financial impact.

Table 1) SLO incident service levels by priority.

Assumptions

- All service levels presented will be aligned with the technology and workflow/service-level tiers being offered to the customer.
- Service-level objectives may be offered as part of Managed Services offerings that do not include 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 Services offerings.
- Service-level measurements exclude the following:
  - Any delays caused by the customer (for example, obtaining change approval)
  - Operational errors, accidents, negligence, abuse, misuse, unauthorized alteration, or modification by the customer or its third-party contractors
  - Movement of hardware or software without NetApp's prior written approval
  - The 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 where NetApp has provided prior written notice of such requirement
  - Any mutually agreed schedule for activities that may fall outside the session 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
  - Situations in which NetApp is unable to access, the customer has not provided on-site access, and/or remote access is prohibited or not made available to NetApp

NetApp

+1 877 263 8277