



This Fixed Price-Fixed Scope Service Description describes the **Ransomware Data Protection Assessment (24595)** (the "Service"). This Service Description is part of any Services Instrument that incorporates this Service Description by reference (collectively, the "Agreement"). **"Services Instrument"** means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Veritas certificate, or a written statement of work or similar document, between Customer and Veritas with associated terms and conditions, that references this Service Description.

Service Overview

This Service is a Fixed Price-Fixed Scope Service engagement to review data protection capability against ransomware attacks and provide comprehensive advice on how to protect backup data and backup systems in the customer organization.

Delivery Details

Scope of Service

Veritas will conduct the Ransomware Data Protection Assessment and provide comprehensive advice on how Customer can protect its backup data and backup systems against the threat of Ransomware. Veritas uses a comprehensive strategic approach. We look at the issues surrounding the threat as well as the response to them, with practical mitigating solutions to meet the business demands, beyond simply a theoretical discussion.

This project will include the following areas of focus:

- Facilitate focused program discussions around areas of Data Protection against Ransomware attacks
- Identify Customer's current Data Protection capabilities and issues against Ransomware attacks, utilizing the Veritas Ransomware Protection Model
- While on-site, Veritas will conduct a cooperative Data Protection review during which Veritas Consultants will work with staff, in the form of interviews and process document reviews, to identify practices and procedures
- Based on the Veritas Ransomware Protection Model, provide recommendations for enhancement, when applicable
- Create an action plan which includes prioritization of short-term and long-term recommended objectives based on Best Practices

Phases of Work:

Veritas shall perform the following tasks using a phased approach.:

- Phase 1: Off-site Alignment and Planning
- Phase 2: Interviews and Data Collection
- Phase 3: Analysis and Completion of the Final Assessment Report



Any Service and Deliverable(s) not specifically written below are out of scope.

Phase 1: Off-site Alignment and Planning

- Veritas conducts an initial Meeting with the Customer
- Veritas Project Manager, in coordination with the Customer Manager, schedules a workshop and (/or) interviews with Customer representatives to discuss Ransomware Protection as identified in the five (5) focused areas outlined in the Veritas Ransomware Protection Model
- Veritas provides a Document List to be reviewed and recommended Interviewee List to the Customer
- Customer shall arrange the time, place, and attendees for interviews and prepare documents to be reviewed
- Veritas shall conduct an On-site Kickoff Meeting

Phase 2: Interviews and Data Collection

- Veritas conducts on-site interviews, discussions, and/or workshops with Customer representatives, up to 5 sessions.
- Customer shall gather requested documents, and hand them to Veritas
- Veritas reviews the existing Data Protection policies and processes of the customer organization, up to 10 documents.
- Veritas to assess the current Data Protection policies and architecture to identify gaps against identified best practices and notable industry standards such as the ISO27001, COBIT 5, ITILv3, and Veritas Best Practices as applicable for the domains.
- Veritas to assess the implemented Data Protection and recovery processes working with Information Security to identify gaps and issues.
- Veritas conducts a technical architecture review of NetBackup.
- Veritas shall review security configurations of NetBackup, on up to two servers.

Phase 3: Analysis and Completion of the Final Assessment Report

- Veritas conducts a review and analysis of Customer's current Data Protection capabilities and readiness against Ransomware attacks compared with the Veritas Ransomware Protection Focused Areas
- Veritas prepares a draft Ransomware Data Protection Assessment Report as outlined in the Deliverables section.
- Veritas develops recommendations based on Veritas Best Practices on Data Protection with action items to reach the desired level of Data Protection.
- Veritas completes the final deliverable document.
- Veritas conducts final meetings to present findings.



Deliverable

Veritas, through the interviews and workshops conducted with the Customer will perform the required analysis and document all findings and recommendations in the Ransomware Data Protection Assessment Report. The recommendations will be prioritized and placed into an effective “roadmap” for management agreement and subsequent implementation by Customer.

The Ransomware Data Protection Assessment Report will contain the following sections based on key findings and information gathered during the project and (/or) Veritas Best Practices:

- An introduction of Veritas Best practices and a model for Data protection
- An observation on the current Data Protection capabilities and issues against Ransomware attacks
- A high-level recommendation for improvements in Customer’s Data Protection strategy, policies, processes, architecture and technologies in order to mitigate the risk of Ransomware, and achieve the desired state of Data Protection capability
- A prioritized action plan of short-term and long-term recommendations for Customer intended to enhance its Data protection and reduce the risk of Ransomware

Key Dependencies & Customer Responsibilities

- All tasks shall be performed at the Customer’s site and remotely
- Work is conducted during Normal Work Hours.

Customer Responsibilities. Veritas can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following prerequisites, assumptions, or dependencies, Veritas’ performance of the Service may be delayed, impaired or prevented:

- Implementation of any of the recommendations made in the Service and/or Deliverable is out of scope of this Service and is the responsibility of Customer
- For any time that the Veritas consultant is onsite, additional applicable fees are required for travel and expenses.
- Veritas strongly recommends that the Customer back up all critical hosts in Customer’s environment before Service commencement. Veritas does not accept responsibility or liability for any loss of data incurred by Customer during the delivery of this Service
- Provide the necessary staffing resources (e.g., LAN, SAN, OS Platforms, DBA, etc.) to enable the Service to be performed.
- Allocate any necessary space, power, cooling, networking, security measures, and wire/cable management for the Service.
- Provide any necessary network access for Veritas, SNMP and email address requirements for alert notifications, and open the necessary network ports to enable the Service to be performed.



- Provision a contiguous range of physical IP addresses and a contiguous range of virtual IP addresses. All IP addresses (both physical and virtual) must be part of the same subnet and use the same netmask as the node's access IP.
- Customer must have active Veritas NetBackup licenses and active maintenance/support if NBU is part of the scope of the engagement.
- Any additional Customer Responsibilities set forth in this Services Description and the Services Instrument.

Acceptance Schedule

This Service is pre-paid, and payment is not contingent upon acceptance of any deliverable. Veritas shall invoice Customer or its Reseller in advance of delivery of Services.