MIT Backup Solution for Virtualization RFP:

MIT is seeking a comprehensive enterprise backup solution to support their current infrastructure. The proposed solution should include the following components:

1. Backup Software Requirements:

- Support for up to **60 virtual machines (VMs)** subscription for **5 years**.
- Coverage for **9 physical servers**, subscription for **1 year**

2. Backup Target Appliances:

- Two appliances required: one for **primary (main)** site and one for **disaster recovery (DR)** site.

Backups should be replicated to DR either by Backup software or by the backup appliances native replication feature.

Backup Software:

The proposed solution must be present as a Leader in the latest Gartner's Magic Quadrant for backup software for at least 5 consecutive years
Technology provider should have a customer satisfaction rating of 95% and above in the backup / recovery space (Validated through third party). Please provide the evidence
The proposed solution must be a complete data protection solution supporting all major operating systems, applications, and databases on virtual and physical servers, NAS shares and cloud-based infrastructures including support for multiple protection methods like backup and archive, snapshot management, replication, and content indexing for eDiscovery.
The proposed solution must include a centralized web-based unified console for the administration, configuration, monitoring and reporting of all data management tasks across the enterprise. The console must include dashboards and guided wizards.
The proposed solution must have efficient storage management capabilities using built-in deduplication with support for the following : a) Client-side dedupe b) Storage-side dedupe c) Global dedupe
The proposed solution must be a single pane of glass management without operating multiple instances / consoles for different functionalities.
The proposed solution shall support agentless backup and restore operations for the following hypervisors and more : - Vmware - Hyper-V - Nutanix Acropolis Hypervisor - Oracle VM - OpenStack - RHEV - Citrix XenServer

The proposed solution should support Application protection using application-aware backup agents to provide consistent point-in-time protection for application data
The proposed solution should support Database protection using application aware agents to provide a simplified end-to-end backup solution for database environments of any size. Database agents intelligently quiesce databases when needed, and provide robust and comprehensive backup and recovery with significant speed and performance, and efficient use of disk and tape drives
The proposed solution must support back up of Oracle databases, the control file, log files, the server parameter file, or Oracle datafiles and tablespaces. You can back up the database when it is online or offline and with or without a RMAN catalog
The proposed solution architecture should be based on a 3-tier architecture consisting of : a) Backup Management Server - central management component of the backup environment. It coordinates and executes all operations, maintaining a Microsoft SQL Server database that contain all configuration, security, and operational history for the environment. b) Media Servers with Disk Library - provides high performance data movement and manages the data storage libraries c) Clients - logical grouping of the software agents that facilitate the protection, management, and movement of data associated with the client
The proposed solution shall be able to perform automatic job restart for any workload (Filesystem and DBs)
The proposed solution must provide data validation features to ensure data integrity by validating data integrity during backup, when data is at rest, and during data copy operations.
The proposed solution must support Global deduplication to allow data from multiple copies to be deduplicated against each other, eliminating redundant data between the copies
The proposed solution will allow automated orchestration of snapshots with global deduplication and compressions.
The proposed solution must support Full, Incremental, Differential, Synthetic Full and Block-level backup capability
The proposed solution must support Synthetic full backups by consolidating data from the latest full backup or synthetic full backup together with any subsequent incremental backups, instead of reading and backing up data directly from the client computer
The proposed solution must allow full and partial restoration of objects from the backup images.
The solution must support recovery of data to a certain point in time
The proposed solution must support the automatic creation of secondary copies and allow to delay the creation of the auxiliary copies
The proposed solution will allow Flexible Retention policy implementation options with the ability to define different retentions for each secondary copy
The proposed solution must support optimized secondary copy creation to a remote site where only unique data blocks is sent over the network

The proposed solution should support the following replication capabilities : - Block-Level Replication - Database Replication - Periodic Replication - Continuous Replication - Replication Monitor - Snapshot Replication - Virtual Machine Replication
The proposed solution should natively provide a) Physical to Virtual recovery b) Virtual to Physical recovery c) Bare metal recovery d) Virtual to Virtual recovery across different Hypervisor (Cross Hypervisor Restore)
The proposed solution must support in-place to same location or out-of-place to different location restores
The solution will be API Enabled to allows flexible integration.
The solution will allow Centralized Management through a flexible UI, Centralized Security Policy enforcement and Audit including Encryption, Access control, and role separation.
The proposed solution must provide feature rich reporting including executive level dashboards, data analytics and capacity trending reports through the single UI managing backup and restore.
The proposed solution must provide data encryption at rest and in transit. Including the following encryption algorithms : - AES 256-bit - 3-DES 192-bit - Blowfish 256-bit
The proposed solutions software encryption must be externally validated as FIPS-2 certified and evidence must be provided
The proposed solution must provide file anomaly detection on client computers to monitor and alert administrators in real time.
The proposed solution should have the ability to protect mount paths to Media Servers from Ransomware attacks by write-protecting mount paths from all processes except the backup software processes
The proposed solution should be able to automatically detect the presence of Ransomware on your client computers using the honeypot file method
The proposed backup solution must include advanced security capabilities to limit access to critical data, provide granular management capabilities, and provide single sign on access for Active Directory users.
The proposed solution must support secure replication of data to an isolated environment with air gap capabilities
The proposed solution should provide a workflow framework that executes and controls the scripts, API requests, or command line operations to orchestrate air gapping.
The proposed solution should support network traffic QoS adjustments on clients
The proposed solution should support network bandwidth throttling

Licensing

The proposed backup software solution should cover below workload :

- **Cover up to 60 virtual machines (VMs) subscription for 5 years.**
- **Coverage for 9 physical servers with total capacity of 9TB , subscription for 1 year:**
- Support and Maintenance agreement for the full term of the license should be Production level with **24x7 .**

Official Training

Official Training (abroad) for **two persons by a certified instructor in certified Training Center .**

Backup Appliance Qty (2):

Main & DR Site:

- Offered Disk to disk backup device shall be a purpose-built backup appliance and shall be certified to work with at-least 3 Backup application vendor ISV like HPE Zerto, Veeam and Commvault etc.

- Offered device shall be offered minimum with useable capacity **50 TB before deduplication and compression.**

- Offered device shall be protected with hardware raid 6 from the factory so that no raid configuration is required in field.

- Offered device shall be shipped with at-least **two** hot spare disks.

- Offered device shall support emulation of both VTL and NAS target like NFS & CIFS.

- Offered Device shall integrate and utilize customer's current backup infrastructure in the following aspects

    - Compatibility with the offered backup server (if required) / media servers.
    - Compatibility with the offered backup software.

- Offered device shall have integrated de-duplication license, low bandwidth replication license so that only unique non-duplicated block transfers to remote / DR location.

- Offered device shall have intelligence to understand both sources based and target based de-duplication and shall be integrated with all well-known backup ISVs. **At-least 3 ISVs shall be supported.**

.

- Offered device shall have Minimum of 4 x 10/25Gbps SFP IP ports. License and SFP+ transceivers for all ports shall be offered and configured.

- Offered disk-based backup device shall also support **encryption functionality**.

- Offered disk-based backup device shall also support dual authorization for preventing disruptive operations so that hackers shall not be able to execute or complete all critical operations like deletion of backup store, changing system time etc.

- Dual authorization shall be approved by two separate accounts or entities instead of a single responsible account / entity so that all malicious actions such as ransomware attacks can be effectively prevented.

- **The data inside the backup appliance must be isolated and protected against any ransomware attacks.**

- Bidder should provide an official white paper from the vendor about the methodology of ransomware protection.

- The backup appliance must effectively isolate critical data where attackers cannot have impact on it without resorting to direct physical interactions that ultimately would result in the destruction of some or all of the hardware itself

- Offered disk-based backup device shall also support Secure erase feature for protecting against unauthorized recovery of deleted data.

- Offered disk-based backup appliance shall support VLAN tagging. Offered IP ports of same type shall also support Port bonding in Adaptive Load balancing as well as in Active-backup mode.

- Offered device shall support rated write performance of at-least **25TB per hour.**

* ملاحظة: يتم دفع كامل المستحقات بعد الانتهاء من الاستلام النهائي وخلال 3 شهور من الاستلام

Backup Server:

5 years support from mother and local company with below specs:

Server Specifications Qty (1)		Comply (Yes / No)	Notes
Form Factor	2U Rack mount Server		
Processor	Dual Intel® Xeon® Gold 6448Y 2.1G, 32Cores, 16GT/s with 60M Cache		
Generation	4th generation Intel® Xeon® Scalable processors		
Memory	**1TB**, DDR5 RDIMMS up to 4800 MT/sec		
Storage Capacity	2 x 960GB SSD SATA Mix Use 6Gbps for OS		
	8 x 1.92TB SSD SATA Mix Use 6Gbps for Data		
RAID	RAID controllers support 0,1,5,6 With 8GB Cache.		
Management	Enterprise Remote Management		
Interfaces	Dual Port 10Gb Base-T network card		
	Dual Port 32Gb Fiber Channel HBA with Transceivers		
PCI slots	support up to available 6 PCIe slots,		
Security	Cryptographically signed firmware Data at Rest Encryption (SEDs with local or external key mgmt.) Secure Boot Secure Erase Secured Component Verification (Hardware integrity check) Silicon Root of Trust System Lockdown TPM 2.0 FIPS, CC-TCG certified		
OS support	Microsoft Windows Server with Hyper-V Red Hat Enterprise Linux SUSE Linux Enterprise Server VMware ESXi Canonical Ubuntu Server LTS		
Power Supply	Dual, Hot-Plug, Redundant Power Supply		
Mount Kit	Rack mounted kit with cable management		
Accessories	All the required cables and all power connectors should be provided.		