General Requirements

1. The solution shall provide enterprise-grade antivirus and anti-malware protection for physical and virtual servers.
2. The product shall support centralized management and monitoring through a web-based management console.
3. The solution shall be licensed for server operating systems.
4. The OEM should be an established cyber security vendor with proven deployment in government, public sector, or enterprise environments.

2. Platform Support

1. Support for Microsoft Windows Server .
2. Support for Linux server distributions such as Red Hat Enterprise Linux, CentOS, Ubuntu Server, Oracle Linux, and SUSE Linux Enterprise Server.

3. Security Features

1. Real-time malware protection with on-access scanning.
2. On-demand and scheduled scanning capabilities.
3. Protection against viruses, worms, trojans, ransomware, spyware, rootkits, and other malware.
4. Behavioral analysis and heuristic detection capabilities.
5. Web and network threat protection.
6. Exploit prevention and ransomware protection mechanisms.
7. File integrity monitoring and suspicious activity detection.
8. Quarantine and remediation features for infected files.

4. Management and Administration

1. Centralized policy management for all protected servers.
2. Remote deployment and configuration capabilities.
3. Centralized alerting, reporting, and audit logs.
4. Role-based access control (RBAC) for administrators.
5. Dashboard showing security status, incidents, updates, and compliance status.
6. Email notifications for critical security events.

5. Updates and Threat Intelligence

1. Automatic signature and engine updates.
2. Frequent threat intelligence updates from the OEM.
3. Ability to receive updates through internet-connected and offline update mechanisms.
4. Protection shall continue even during temporary loss of internet connectivity.

6. Performance Requirements

1. Minimal impact on server performance and resource utilization.
2. Optimized scanning for server workloads.

3. Configurable exclusions for applications, processes, files, and directories.
4. Support for scan throttling and scheduled scans during maintenance windows.

7. Reporting and Compliance

1. Comprehensive reporting on malware detections, updates, scans, and security incidents.
2. Exportable reports in PDF, CSV, or equivalent formats.
3. Audit trail of administrative activities.
4. Compliance reporting capabilities.

8. Support and Warranty

1. Minimum one-year subscription including antivirus engine updates, malware signature updates, and technical support.
2. OEM support through email, web portal, and telephone.
3. Access to product documentation, knowledge base, and software updates throughout the subscription period.

9. Delivery

1. Supply, installation assistance, configuration support, and deployment guidance shall be included.
2. Necessary licenses and activation keys shall be provided.
3. Product shall be genuine, licensed, and sourced through authorized channels.