**Account Information:**

| **Service Opportunity Type** | License subscription and implementation services |
| --- | --- |
| **Company Name** | **ETPI-Network** |
| **Project Name** | Full implementation of ManageEngine Endpoint Central (Security) solution - On-Premise |
| **SDP Reference No.** |  |
| **Account Manager** | Shane Lopez |

**Product profile:**

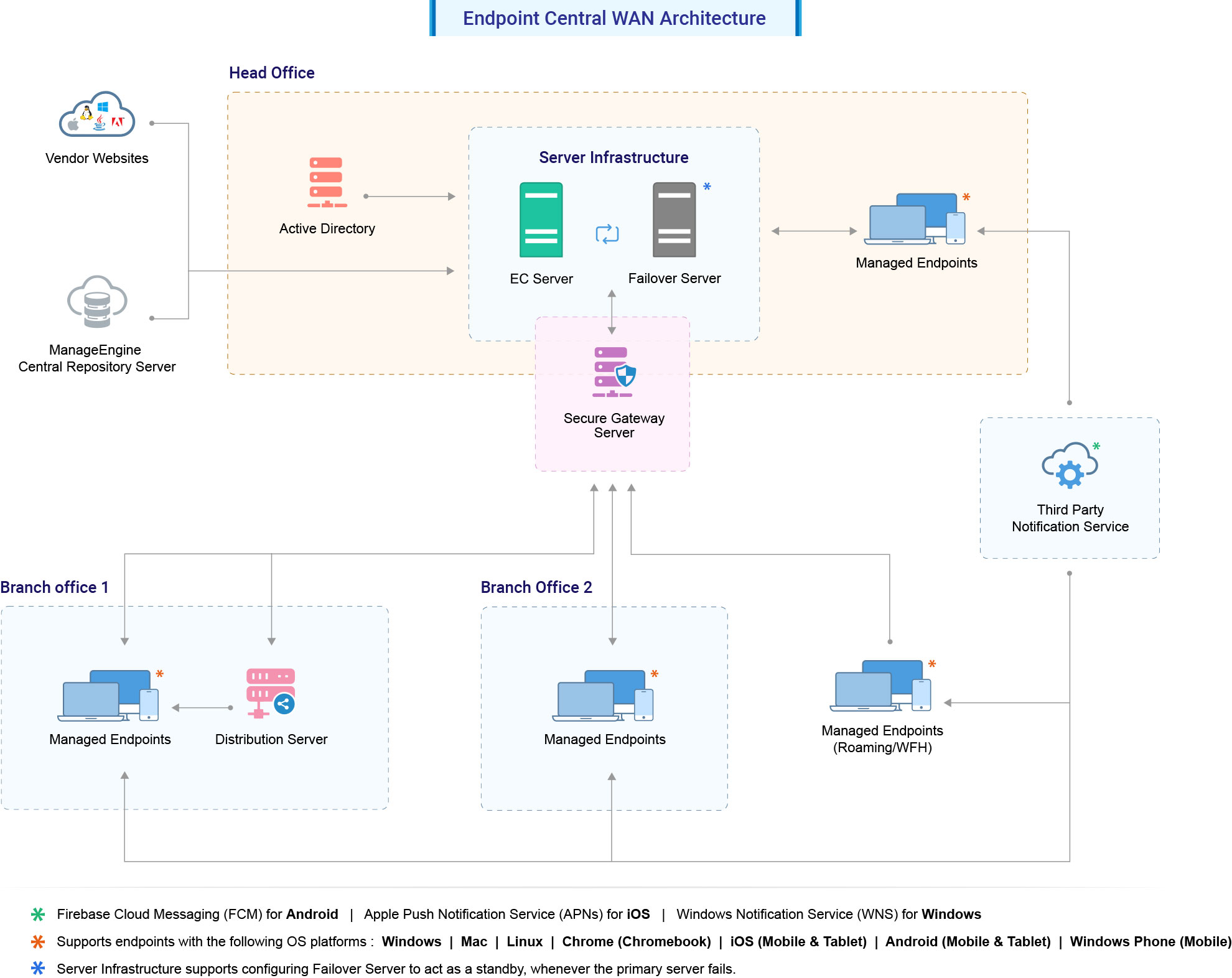
| **Product Name** | Endpoint Central |
| --- | --- |
| **Product Platform** | On-Premise |
| **Product Edition** | Endpoint Central: Security |
| **Standard License Details** | **Endpoint Central**   * Edition: Security * Number of endpoints: 30 * Number of servers: 150 * Number of technicians: 6 * Client is requesting for an additional 10% count of total assets to be included in the license count) |
| **Add-ons / Plug-ins** | **Endpoint Central**   * Security Gateway server * Anti-Ransomeware * Failover Services |

**PAIN POINTS**

| **Pain points / Challenges** | **Recommended Solutions** | **Product/Services to Offer** | **Modules to Emphasize** | **INTERNAL NOTES)**  **Next Step Actions/Remarks** |
| --- | --- | --- | --- | --- |
| Client is in need of an enterprise Endpoint management solution | ME Endpoint Central - Security | License and implementation | Endpoint Management and Patch management |  |

**Endpoint Central**

**Proposed Architecture:**



**Hardware Requirements:**

| **Server** | **Parameter** | **Minimum Requirement** |
| --- | --- | --- |
| **Endpoint Central Server** | Processor information | Physical Machine: Intel Xeon (8 core/16 thread) 2.6 GHz  Virtual Machine: 16 virtual processors (2.6 Ghz) |
| RAM size | 16 GB |
| Hard disk space | 60 GB\* |
| **Endpoint Central Agents** | Processor | Intel Pentium |
| Processor Speed | 1.0 GHz |
| RAM size | 512 MB |
| Hard disk space | 3 GB\*\* |
| **Network requirement** | Network card speed | Minimum 1 GBPS Network Interface Card (NIC) |
| Bandwidth | Minimum 1 MBPS (T1 connection) |
| **SQL Server** | Processor information | Physical Machine: Intel Xeon (8 core/16 thread) 2.6 GHz 20 MB cache  Virtual Machine: 16 virtual processors (2.6 GHz 20 MB cache) |
| RAM size | 16 GB |
| Hard disk space | 250 GB\* |
| Edition | Standard/Enterprise |
| \* May increase dynamically according to the frequency of scanning | | |
| \*\* May increase dynamically depending on the operations performed on the client computer | | |

**Distribution server**

| **No. of Computers Managed Using the Distribution Server** | **Processor Information** | **RAM Size** | **Hard Disk Space** |
| --- | --- | --- | --- |
| 1 to 500 | Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache | 4 GB | 6 GB\* |
| 501 to 1000 | Intel Core i3 (2 core/4 thread) 2.9 Ghz 3 MB cache | 4 GB | 12 GB\* |
| 1001 to 3000 | Intel Core i5 (4 core/8 thread) 2.3 GHz | 8 GB | 16 GB\* |
| 3001 to 5000 | Intel Core i7 (6 core/12 thread) 3.2 GHz | 8 GB | 20 GB\* |

\* May increase depending on the number of software applications and patches that are deployed

**Note** : It is highly recommended to install a Distribution Server for every 1000 computers.

**Operating System**

| **Windows OS** | **Windows Server OS** | **macOS** | **Linux OS\*** |
| --- | --- | --- | --- |
| Windows 11 | Windows server 2022 | macOS 14 Sonoma | Ubuntu 10.04 & later versions |
| Windows 10 | Windows server 2019 | macOS 13 Ventura | Debian 7 & later versions |
| Windows 8.1 | Windows server 2016 | macOS 12 Monterey | Red Hat Enterprise Linux 6 & later versions |
| Windows 8 | Windows server 2012 R2 | macOS 11 Big Sur | CentOS 6 & later versions |
| Windows 7 | Windows server 2012 | macOS 10.15 Catalina | Fedora 19 & later versions |
| Windows Vista | Windows server 2008 R2 | macOS 10.14 Mojave | Linux Mint 13 & later versions |
| Windows XP\* | Windows server 2008 | macOS 10.13 High Sierra | OpenSuSE 11 & later |
| [\*Conditional Support](https://www.manageengine.com/products/desktop-central/securing-legacy-os-communication.html) | Windows server 2003\* | macOS 10.12 Sierra | SuSE Enterprise Linux 11 & later versions |
|  | [\*Conditional Support](https://www.manageengine.com/products/desktop-central/securing-legacy-os-communication.html) | macOS 10.11 EI Capitan | Pardus 17 and 19 |
|  |  |  | Oracle Linux Server 6,7,8 and 9 |
|  |  |  | Oracle Linux 6 and later versions |
|  |  |  | Rocky Linux 8 and later versions |
|  |  |  | \*Kernel versions above 2.6.33 |

**Port requirements**

**Note:** The ports mentioned under 'Server' must be enabled at all times irrespective of your license edition. Refer the ports required for specific modules and enable them as per your requirement.

**Server**

| **Port** | **Purpose** | **Type** | **Connection** |
| --- | --- | --- | --- |
| 8383 | For communication between the agent or distribution server and the Endpoint Central server.  **Source:** Agent/Distribution server  **Destination:** Endpoint Central server | HTTPS | In bound to server |
| 8027 | The notification server port is responsible for communicating on-demand operations from the server to the agent.  **Source:** Agent  **Destination:** Endpoint Central server | TCP | In bound to server |

**Tools and Remote Control**

| **Port** | **Purpose** | **Type** | **Connection** |
| --- | --- | --- | --- |
| 8444 | For Sharing remote desktops, System Manager, Chat  **Source:** Agent  **Destination:** Endpoint Central server | HTTP | In bound to server |
| 8032 | For transferring files  **Source:** Agent  **Destination:** Endpoint Central server | HTTP | In bound to server |
| 8443 | For Sharing Remote Desktops, System Manager, Chat  **Source:** Agent  **Destination:** Endpoint Central server | HTTPS/UDP (for voice & video chat) | In bound to server |
| 8031 | For transferring files  **Source:** Agent  **Destination:** Endpoint Central server | HTTPS | In bound to server |

**Distribution Server**

| **Port** | **Purpose** | **Type** | **Connection** |
| --- | --- | --- | --- |
| 8384 | For communication between (remote)agent and distribution server  **Source:** Agent  **Destination:** Distribution Server | HTTPS | In bound to Distribution Server |

**MDMP**

| **Port** | **Purpose** | **Type** | **Connection** |
| --- | --- | --- | --- |
| 9020 | ME MDM app and server communication. | HTTP | Inbound to Server |
| 9383 | ME MDM app and server communication. | HTTPS | Inbound to Server |
| 443 | Should be open on the firewall/ proxy for Endpoint Central server to reach GCM/APNs service  **Source:** Endpoint Central server  **Destination:** Apple server, Google server Ex: \*.push.apple.com | HTTPS | Outbound from Corporate Network Firewall |
| 5223 | Should be open, if the mobile device connects to the internet through the Corporate WiFi, it is recommend to configure the IP range 17.0.0.0/8.  **Source:** Endpoint Central server  **Destination:** Apple server, Google server | HTTPS | Outbound from Corporate Network Firewall |
| 5228 | For the GCM to reach the managed mobile device  **Source:** Endpoint Central server  **Destination:** Google Playstore server | HTTPS | Outbound from Corporate Network Firewall |
| 5229 | For the GCM to reach the managed mobile device  **Source:** Endpoint Central server  **Destination:** Google Playstore server | HTTPS | Outbound from Corporate Network Firewall |
| 5230 | For the GCM to reach the managed mobile device  **Source:** Endpoint Central server  **Destination:**Google Playstore server | HTTPS | Outbound from Corporate Network Firewall |
| 2195 | Should be open on the firewall/ proxy for Endpoint Central server to reach APNs. Host Address: gateway.push.apple.com  **Source:** Endpoint Central server  **Destination:** gateway.push.apple.com-Apple server | HTTPS | Outbound from Server |
| 5235 | For Firebase Cloud Messaging  **Source:** Endpoint Central server  **Destination:** Google server | HTTPS | Outbound from Corporate Network Firewall |
| 5236 | For Firebase Cloud Messaging  **Source:** Endpoint Central server  **Destination:** Google server | HTTPS | Outbound from Corporate Network Firewall |

**OSD**

| **Port** | **Purpose** | **Type** | **Connection** |
| --- | --- | --- | --- |
| 8444 | For communication between the OS Deployer Components and the server  **Source:** Target machine  **Destination:** Endpoint Central server | HTTP | In bound to server |
| 8443 | For communication between the OS Deployer Components and the server  **Source:** Target machine  **Destination:** Endpoint Central server | HTTPS | In bound to server |
| 8383 | For communication between the OS Deployer Components/Distribution Server and the OS Deployer server in secured mode | HTTPS | In bound to server |
| 8384 | For communication between the OS Deployer Components and Distribution server | HTTPS | In bound to server |
| 69, 4011 | TFTP PXE Communication between the target machine and Server  **Source:** Target machine  **Destination:** Endpoint Central server | UDP | In bound to server |

**Note**: Ports 135,139 and 445 should also be kept open for pushing agent installation on both agent and server.**You can use Endpoint Central to manage the computers running on the below mentioned operating system:**

**For Managing Mobile Devices**

* Android: Android devices running on version 4.0 or above
* iOS (incl. iPhone, iPad and iPod): iOS devices running on version 4.0 or above
* Windows Smartphones: Devices running on version Windows Phone 8.1 or above
* Windows laptops (incl. Surface Hubs and Surface Pros): Devices running on Windows 10
* Chrome OS: Devices running on version 57.0 or later
* tvOS: Devices running on version 7.0 or above

macOS: Devices running on version 10.11 or later

**Reference links:**

* **Endpoint Central system requirements:** [**https://www.manageengine.com/products/desktop-central/system-requirements.html**](https://www.manageengine.com/products/desktop-central/system-requirements.html)
* **Port requirements:** [**https://www.manageengine.com/products/desktop-central/desktop-central-wan-architecture.html**](https://www.manageengine.com/products/desktop-central/desktop-central-wan-architecture.html)

**ITG Project Members:**

| **Project Member** | **Headcount** | **Role / Responsibilities** |
| --- | --- | --- |
| Project Consultant / Team Lead | 1 | * Guide the implementation team to fulfill project activities. * Final Arbiter of key design and implementation decisions. * Managing the technical staff and delivering training if necessary * Supervising work and solving all technical problems that arise and ensuring that any necessary changes are reported and resolved. * Escalating and resolving technical issues to the product support/dev team. |
| Project Manager | 1 | * Deciding what methodology and model is going to be followed to develop the project * Define project assumptions, scopes and objectives. * Create/define project timeline * Assign tasks and finalizes work breakdown structure * Risk assessing the whole project and individual stages and then managing these risks * Bringing together the work completed by different teams and ensuring that this cohesion goes smoothly * Project communication and coordination * Keeping the project on schedule and managing the time and resources that are spent on it * Monitoring the project at all times to ensure that it will achieve its desired outcomes and that a product or system is completed that meets client or customer requirements |
| Implementation Engineer | 1 | * Conducts admin and user training * performs Installation/Configuration of the product. * Conduct product or function testing. * Solving all technical problems that arise and ensuring that any necessary changes are reported and resolved. * Assist in escalating and resolving technical issues to the product support/dev team. * Support end users’ inquiries |

**EndUser Project Members:**

| **Project Member** | **Headcount** | **Role / Responsibilities** |
| --- | --- | --- |
| Project Coordinator / SPOC | 1 | * Internally manages and coordinates the possible requirement changes, project deadlines/targets, prerequisites, dependencies, and internal support needed. |

**Baseline/Core Configuration:**

| **Configurations that can be covered on the Mandays Allocated** | **Mandays Allocated** |
| --- | --- |
| **Project Management and Business Analysis**   1. Kick-off meeting 2. Workshop: Understanding User Stories 3. System Walkthrough – DGF session 4. Business requirement definition/acceptance | 5 |
| **Configuration and Build-up**  **Start of configuration**  **Endpoint Central**   1. **Instance installation**    1. Server installation       1. Client to provide the host server where the solution will be implemented    2. Secondary Server installation (Failover setup)       1. Client to provide the host server where the secondary server will be implemented on       2. MSSQL database will be required for implementing the failover services          1. Client will provide the MSSQL server to be used by the solution.    3. Distribution server setup (As needed)       1. Only 2 distribution servers will be configured.          1. Additional distribution servers will entail additional billable mandays for implementation       2. Client to provide host server for distribution servers       3. All distribution servers will be implemented remotely.    4. Secure Gateway Service       1. Installation of certificate       2. Client to provide hosting server resources for the server       3. Client shall provide FQDN details for configuration. 2. **Replication Policy setup**     1. \*Maximum of 2 Distribution Server only 3. **Mail Configuration**    1. Mail server details and credentials shall be provided by the client 4. **User and Permission Setup**    1. Enrollment of Technician/s       1. Up to 6 technicians only    2. Technician Role creation       1. Up to 2 roles only 5. **Network dependency configuration**    1. FQDN       1. Client to provide FQDN information as well as public IP to be used.    2. Network dependencies shall be handled by client network admin please refer to links mentioned above. 6. **Domain Setting**     1. Adding domain or workgroup       1. Client to provide domain details to include in the solution          1. This is a prerequisite for GPO deployment of agents. 7. **Agent settings configuration** 8. **Device enrollment**    1. Through GPO enrollment(Windows) or Manual method (**Choose one option**)       1. Agent deployment via GPO (Option 1)          1. GPO deployment will be done by the client’s team but will be assisted by the vendor’s team.          2. Trigger deployment up to a maximum of 180 Windows devices only             1. Monitoring for enrolled devices will only be for 10 days only due to device availability dependency.   Any devices not enrolled during the declared days on 12.1.1.2.1, the client will continue the enrollment and monitoring   * + 1. Manual (Option 2)        1. Up to 180 devices only           1. 30 workstations only           2. 150 servers only           3. Deployment and monitoring will be up to 10 days only due to device availability.   Any devices not enrolled during the declared days on 12.1.2.1.1, the client will continue the enrollment and monitoring.  If the client will require more devices to be enrolled, this will be subject for review and approval. This may require additional billable mandays.   1. **Asset Management Configuration**    1. Scan settings    2. Trigger file scan only to selected devices       1. Device scope will depend on the number of endpoints scanned (Refer to item number 12 for the total number of endpoints enrolled)          1. Any additional endpoints not part of the scan, shall be subject for additional billable mandays.    3. Scheduled scan       1. Up to 1 schedule only    4. File scan rules       1. 1 configuration only    5. Configure Inventory alerts       1. Up to 2 alerts only    6. Configuration of Software metering rules       1. Up to 2 rules only 2. **Creation of device groupings - Custom groups\***    1. Maximum of 5 custom groups only 3. **Patch Management**    1. Configuration of Patch Database settings    2. Creation of Deployment Policies       1. Up to 4 policies only    3. Configuring Test and Approval Environment       1. Up to 4 configurations only    4. Configuration of Declined patches       1. Up to 2 patches only    5. Configuration of Automated Patch Deployment Tasks       1. Up to 2 deployment tasks only 4. **Configuration Settings (Users and Computers)**     1. Setting up Computer or User Configurations for domain or workgroup users (Windows)       1. Up to 2 configurations only    2. Creating configurations for Mac or Linux Systems (as needed)       1. Up to 2 configurations only 5. **Software Management**    1. Configuring Software Repository (Network Share or via HTTP) - *optional*       1. Shared folder’s directory shall be provided by the client    2. Configuration of Self-Service Portal Settings - *optional*    3. Creating Software Packages from the templates       1. Up to 2 packages only    4. Creation of Deployment Policy/Policies       1. Up to 2 deployments only    5. Remote installation of Software from the created packages for Users or Computers (As needed)       1. Up to 2 configurations only       2. Up to 1 group/device target only 6. **Reports**    1. Configuration of Schedule for Pre-Defined Reports       1. Up to 5 reports only    2. Configuration of Custom Reports and adding schedule       1. Maximum of 5 records to be configured 7. **Remote Control settings configuration**     1. General Settings    2. Screen Recording    3. User Confirmation (optional)   **Add-ons**   1. **Vulnerability Management**    1. Deployment of software vulnerability patches       1. Up to 5 patch deployment only.    2. Detected CVE fix       1. Up to 5 fixes only          1. Up to 5 target devices only    3. Zero-Day Vulnerability management       1. Up to 2 vulnerability fix deployment only    4. System Misconfigurations       1. Up to 2 fix only          1. Up to 1 target device per fix only    5. Software Vulnerability       1. Up to 2 reports only in the summary view    6. Web Server Misconfigurations management       1. Up to 2 report only    7. Port audit       1. Up to 2 report only 2. **Device Control Plus**    1. Enrollment of trusted devices       1. Up to 3 devices only    2. Group creation       1. Up to 3 groups only    3. Policy creation       1. Up to 3 policy creation only    4. Policy assignment       1. Up to 3 policy assignments only 3. **Application Control Plus**    1. Creation of blacklist and whitelisting of applications       1. Up to 2 blacklisted and whitelisted applications only    2. Group creation       1. Up to 2 group only    3. Policy creation       1. Up to 2 policy creation only    4. Policy assignment       1. Up to 2 policy assignments only 4. **Bitlocker management**    1. Bitlocker Management       1. Creation of Policy          1. Up to 2 policies only       2. Deployment of policy for the encryption          1. Up to 1 target device only 5. **Browser Security Plus**    1. Group creation       1. Up to 2 groups only    2. Creation of Policy       1. Up to 2 policies only    3. Deployment of policy to device groups.       1. Up to 2 group associations only 6. **Data classification**    1. Creation Data Rules       1. Custom content pattern creation (Up to 2 options and 5 configurations only)          1. Data content pattern shall be provided by the client’s team             1. Option 1: Regex Pattern             2. Option 2: Keyword matching             3. Option 3: Document matching             4. Option 4: File extension matching       2. Up to 2 rule configurations only    2. Policy Deployment       1. Up to 2 policy associations and configurations only       2. Up to 180 endpoint targets only    3. Reports       1. Up to 4 reports only          1. Option 1: Sensitive Email Audit          2. Option 2: Keyword matching          3. Option 3: Document matching          4. Option 4: File extension matching 7. **Anti-Ransomware**    1. Detection Settings    2. Clean-up Policy    3. Endpoint management scope       1. Configuration is only limited to up to 30 endpoints only   **Final deployment** | 50 |
| **Quality Test, Errors and Fixes**   1. Functional test cases creation 2. Functional Testing 3. User Acceptance Test | 5 |
| **Project Handover and Release Management**   1. Knowledge Transfer for:    1. Admin    2. Technicians (Train the Trainer)    3. User (as required - Train the Trainer) 2. Project Completion    1. Business requirement acceptance (As-built)    2. Project Sign-off    3. Turn over to support | 5 |

**Project Summary:**

| Total Billable Work Efforts | 65 Mandays |
| --- | --- |
| Premium Support Manhours | N/A |
| Project Resource | 1-Project Consultant | 1-Project Manager | 1-Implementation Engineer |

**Assumptions and Limitations**

**FULL IMPLEMENTATION**

ITG will be implementing the ManageEngine Endpoint Central Security On-Premise. ITG recognizes that all parties must use all reasonable endeavors to meet agreed schedules and deadlines. ITG shall not be liable for any delays or failures in performance due to circumstances beyond its control. We have made the following overall assumptions in the development of this implementation methodology:

* In the performance of our work, we will not be assuming the role of management and we will report to you. It is understood that implementation of our recommendations will be at your sole discretion. Refer to project roles and responsibilities.
* It is assumed that a Client representative working on this effort would be existing staff doing this work as part of their normal work assignments.
* Scope of the project will only focus on the following items:
  + Endpoint Central
    - Edition: Security
    - Number of technicians: 6
    - Number of endpoints:
      * Endpoints: 50
      * Servers: 150
    - Add-ons
      * Secure Gateway Services
      * Anti-Ransomware endpoints: 50
      * Failover services
* Assuming all the prerequisites and required data are available at the time of implementation
* The configuration shall ONLY cover the default administration module of the product with no customization, backend configuration, or third-party integrations. If needed, ITG will reassess and plot additional man-days and scope as needed.
* As ITG adapts to the new normal, the actual configuration and setup will be done remotely.
  + The client and ITG may require a conference tool (i.e., Zoom, MS teams, or if there’s any preferred conference tool) to use for collaboration during the remote implementation.
* Endpoint Central will be hosted on client’s provided server
  + Client will provide the resources (physical or virtual server) for the installation of main server and distribution servers for asset management.
  + Up to 2 sites only.
  + All distribution server implementation will be done remotely.
* The end-user shall provide and maintain a fully operational technical environment that allows the implementation team to meet the required project deliverables on time.
* System requirements, architecture, and hardware resources for the product to operate shall be available/fulfilled/prepared by the end user as needed.
* Local environment, platform, and network-related configuration will be implemented by the end-user team with the support from the ITG implementation team
* The project deliverables will be implemented ONLY within the agreed stated scope of work and man-days allocated.
* Functionalities of the system that require information or resources from the end user need to be provided on or before the defined target date, else will be set to default.
* Should a CSV/XLS import is necessary, the client shall build the CSV/XLS file/s.
  + For CSV import for IT assets, clients must ensure the service tags are correct to avoid duplication of records.
* Undelivered tasks dependencies of the project will be considered as task closed and default configuration will be established.
* In the event of a change request, ITG will re-assess and scope as needed and will be subject to the approval of the stakeholders.
* The project shall be considered completed once the following criteria
  + Business requirement definition documentation has been completed
  + Agreed configuration has been completed
  + Passed Functional Criteria
  + Training has been provided:
    - Admin
    - Technicians (Train the Trainer)
    - User (as required - Train the Trainer)
* Add-ons not included in the initial proposal and if requested by the client, vendor will have to re-assess and provide a new proposal that may include additional cost for license and/or mandays for implementation.
* All OS-related configuration will be done by the client’s system administrator(s).
* All network-related configurations will be done by the client’s network administrator(s).
* The client should fix the network issues if any.
* Should the project finish ahead of the plotted man-days, the client has the privilege to divert the unused man-days to other services related to the client’s requirements. Or the client can add it on the support man-hours.

**SIGN-OFF AND ACKNOWLEDGEMENT**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: 10/21/2024

Michael Ernest Sanchez

Subject Matter Expert, ESD-ITMS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_/\_\_\_/\_\_\_

**Rommel Joseph Bernabe**

Practice Head, ESD-ITMS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_/\_\_\_/\_\_\_

Shane Lopez

Business Development Officer