OpSus|Live

Implementation and Configuration Assumptions

Functionality.

The OpSus Live service includes the provision and management of compute and storage resources that power, secure, and connect the customer to the application environment. The OpSus team performs daily operational tasks such as routine backups and disaster recovery replications, facilitating end-user access, and managing system performance. Upper service tiers offer snapshot backups and automatic restoration of the backup copy to a DR site for even faster recovery in the event of a disaster.

Onboarding and Implementation

Service Initiation and Customer Requirements.

CloudWave and Customer work together in the design and delivery of the managed service. Customer has additional administrative, technical, and device configuration responsibilities to enable the environment.

- Readiness Assessment- An onsite assessment of the Customer environment is performed to review scope, service level objectives, and technical and integration considerations prior to commencement of the service.
- Assessment Remediation- Describes specific areas of improvement or modification needed prior to the start of the service, as observed during the Readiness Assessment.
- Operations Coordinator- A primary and secondary Customer point of contact is needed to schedule planned downtime, participate in quarterly rounding calls, and coordinate infrastructure changes when required.
- Onsite Connectivity- Customer is responsible for providing and managing adequate and redundant network and internet bandwidth and services at the Customer site to access the service.
- End User Device Requirements- Customer user devices, including thin clients, PCs, and mobile devices must support the applicable protocol of their contracted configuration for secure access to the OpSus environment.
- Authentication and Access Control- Customer is responsible for providing appropriate levels of access to CloudWave to assist in environment setup, migration, monitoring, and service operations, including:
    - Domain / Active directory,
    - EHR Client / Service login,
    - Any applicable backup technologies.
- User Accounts- Customer is responsible for maintaining user accounts, security controls, and authorization (additions, terminations, role changes, etc.) for Windows and EHR accounts.
- EHR Application Support- Customer is responsible for EHR application support, monitoring, and management of the application environment including application upgrades.
- Vendor License Responsibility- Customer may be required to financially and administratively provide some

application licenses or software to enable the EHR environment, as described in the Proposal.

Environment Components and Configuration.

CloudWave will provide necessary compute, storage and replication services determined by service level to ensure successful delivery of the OpSus Live environment. Customer participation and environment management is also required.

- Virtual Desktop Infrastructure- The Proposal includes the Virtual Desktop Infrastructure (VDI) Service which runs from thin client devices or PCs. The underlying technology may be Horizon View or Citrix.
    - For Horizon View, Microsoft requires the Microsoft Virtual Desktop (MS VDA) to access the Windows OS License. Microsoft does not provide Service Provider Licensing for MS VDA and this must be provided by and paid for by Customer.
    - For Citrix, Microsoft requires Remote Desktop Services Client Access Licenses (RDS CALs) to access the remote desktop services running on the Microsoft OS. This may be provided by Customer or may be provided by CloudWave for an additional fee.

      NOTE: If RDS user CALs are not purchased through CloudWave, the following must be met:
        - Customer must provide CloudWave the required RDS User CALs with Software Assurance purchased under a Microsoft Volume Licensing Agreement.
        - Customer must complete, and Microsoft must accept, the Microsoft License Mobility Verification Form to allow CloudWave to use the RDS User CALs.

- Virtual Private Networking- CloudWave provides secure, virtual private networking (VPN) to Customer site for non-client-based traffic such as interfaces, background printing, and other specific communication needs.

- Internet Connectivity- CloudWave provides secure, diverse, and redundant internet connectivity into CloudWave data center facilities.

- OpSus License Responsibility- CloudWave is responsible for software licensing and maintenance of hypervisors, operating systems, utilities, and embedded support agents to manage and present the service, as described in the Proposal.

- Data Backups for Operational Recovery- CloudWave provides data backups in accordance with the chosen service level, a minimum of once per day for operational recovery. Daily data backups are retained as specified in the Service Level Agreement or Proposal.

- Backup and Replication for Disaster Recovery- CloudWave will replicate data, or transfer backup data to an alternate data center a minimum of once per day to facilitate the recovery process in the event of a Disaster Declaration at the primary data center. CloudWave provides hardware, software, and services to accommodate full restoration of supported components in the event of a Disaster Declaration by CloudWave of the primary site.

Disaster Testing.

CloudWave will coordinate initial and periodic testing with Customer as specified by the Proposal.

- Test Coordination and Frequency- The service includes one planned disaster recovery test each year, extra planned tests are available for an additional fee. Tests must be scheduled a minimum of thirty (30) days in advance.

- Testing Duration- Upon test scheduling, Customer will be allocated a five to seven-day window for resource allocation and testing.

- Post Test Assessment and Report- CloudWave will conduct a Post Test Assessment with Customer to review results, and to assess the need for improvements for future tests. CloudWave will provide a report to document the success, failure, and any improvement opportunities.

Operations and Support

Support Functions and Change Management.

CloudWave provides managed support and the hours of support as specified in the Proposal. Support includes incident investigation with EHR application providers and other third-party vendors as needed and available.

- Monitoring Services- CloudWave will provide capacity, performance, and availability monitoring of critical compute, storage, networking, and virtual desktop services and components 24x7, as described in the Proposal.

- Service Desk and Portal- CloudWave will provide support and service desk access via telephone (855-28-OPSUS) and the MyOpSus Customer portal (https://myopsus.opsuscloud.com) for reporting and tracking incidents, service requests, and access to the OpSus monitoring portal.

- Incident Management and Response- CloudWave will provide incident management and response for issues associated with the service as described in the OpSus Live SLA.

- Quarterly Rounding Calls- CloudWave will schedule periodic rounding calls with Customer no less than once per quarter for the purpose of evaluating customer satisfaction with service and performance, and to discuss upcoming changes for either party, and/or any issues that need addressing.

- Patch and Maintenance Windows- CloudWave provides patch and customer specific maintenance windows for security and operational patches, upgrades, and other system maintenance a minimum of quarterly.
    - CloudWave will schedule patch and customer-specific system maintenance windows at a time mutually agreeable between Customer and CloudWave.
    - Customer is responsible for notifying and coordinating downtime with its own end users and conducting application related functions, such as stopping and re-starting application or application services and verifying application and interface functionality.

- Change Management- To minimize the adverse impact of changes to the operating environment, CloudWave will provide appropriate change controls to ensure the integrity of production computer resources.
    - Single Customer Changes: CloudWave will coordinate and schedule changes with Customer that may impact a single customer's production environment a minimum of five (5) business days in advance.
    - Multiple Customer Changes: CloudWave will provide change notification that may affect multiple customer's production environments a minimum of five (5) business days in advance.
    - Emergency Changes: CloudWave reserves the right to conduct emergency changes when the integrity, confidentiality, or availability of the service are at risk for any reason, with limited notification to customers.

- Customer Change Management. In order to protect both availability and monitoring of the service, Customer agrees to notify CloudWave's Service Desk five (5) business days in advance for the following activities:
    - EHR Application Upgrades and/or Application Downtimes: Any activity that may impact Customer owned/managed software running on covered machines.
    - Network Changes: Activities that may potentially disrupt or change the path for internet, VPN, client SSL, or private network communications to the service environment.
    - Other Major Changes: Any hardware, software or configuration change that may alter the performance of the services or service environment.