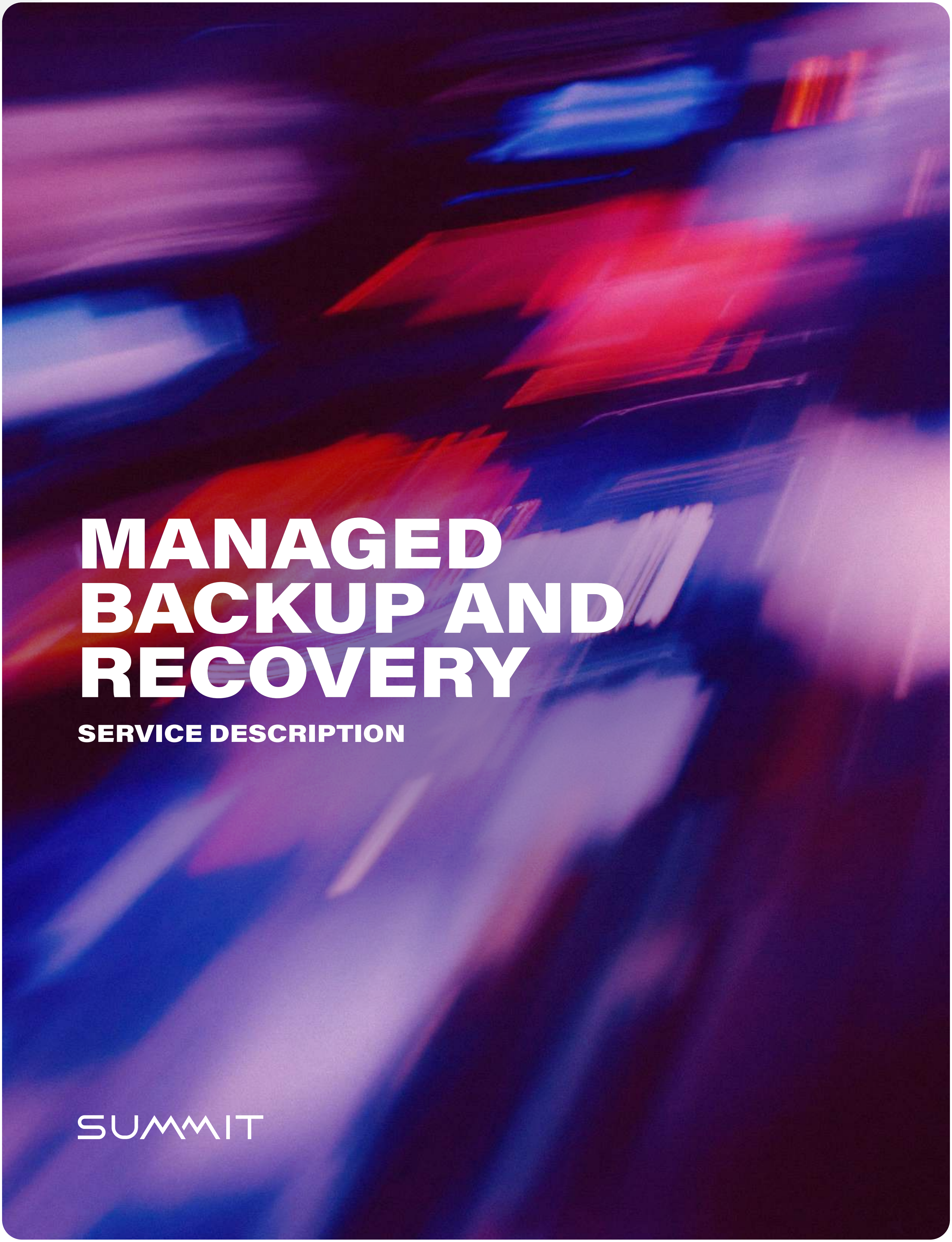

MANAGED BACKUP AND RECOVERY

SERVICE DESCRIPTION

SUMMIT

Service Overview

Summit’s Managed Backup & Recovery (MBUR) provides end-to-end protection for applications, files, and virtual or physical servers. Backups are securely stored and maintained in our SOC 2-compliant data centers, powered by industry-leading platforms including Rubrik, Veeam, and Zerto.

MBUR is a fully managed service — configured, monitored, and supported 24x7x365 by our Managed Services and Service Desk teams. Restore requests can be made on-demand by submitting a ticket through our Customer Portal, with flexible options for restoring data into Summit’s cloud environments.

Our engineers manage the hardware, software, and tools behind the scenes, ensuring data is backed up, protected, and recoverable when you need it. You’ll also receive weekly reports detailing backup job status, completions, and retention policy details so you’re always in the loop.

Default Configuration and Backup Schedule Summit's MBUR service delivers industry best practice configurations for Backup & Recovery operations. This includes: maintaining a Synthetic Full Backup + 6 Days Forward Incremental Backups in a Performance Storage Tier and maintaining a Full Backup for a rolling 28 days on a Capacity Storage Tier. This provides two benefits for our Clients 1/ Clients have the most needed data readily available in case of a restore request and; 2/ lower the total costs of the Managed Backup service by aging out older data to the Capacity Storage Tier.

Note: The Capacity Tier data is maintained in a physically separate data center providing the air gap necessary for maximum data protection and recoverability.

Should there be unique compliance, backup, or archival requirements, Summit will work with each Client to understand their data protection needs and configure the MBUR service parameters, including the frequency of backups, retention policy, encryption methods, and data locations, accordingly.

Encryption

The Managed Backup & Recovery Service enables encryption of data by default. The Service will generate the encryption keys necessary to protect the data. Data is encrypted as it is written to the Backup Repository, and the resulting encrypted data blocks are stored. The Service includes encryption-at-rest so data remains encrypted while stored in any Summit-operated data center.

Restore request processes

Restores for backup data are performed upon request on a best-effort basis. Data is typically restored to the primary system where the data originated. MBUR also supports the option for virtual machines or data to be recovered manually to a different target system. Target systems can include a new virtual machine created in Summit's Enterprise Cloud or Managed Private Cloud environment. Manual recoveries are performed on a best-effort basis and will include additional charges for use of storage and/or cloud services. If specific SLAs are required for data restore processes, Summit also offers comprehensive DRaaS services.

Service overview

A managed service

Summit's Managed Services team supports the underlying hardware, software and network connectivity used to deliver the MBUR Service, as well as administers and monitors the backup and recovery processes put in place. Customers receive a weekly Managed Backup & Recovery Service Report detailing the status of backup jobs, completion of jobs, and any other information about the jobs. Customers open support requests to create or alter backup jobs, change data retention policies, or get any additional information about the service.

Application-aware, image-based backups

MBUR creates application-consistent, image-level VM backups with advanced, application-aware processing which includes transaction log truncation.

Synthetic full backups

MBUR's support of Synthetic Full Backups eliminates the need for periodic full backups by creating forever-incremental backups that save time and storage space.

Performance & capacity tier storage

MBUR delivers a two-tier storage architecture enabling the most recent data to be quickly and easily accessible with nominal latency (miliseconds). The Performance Tier maintains a Synthetic Full Backup + 6 Days Forward Incremental Backups while the Capacity Tier maintains a Full Backup for a rolling 28 days.

Multi-tier protection

MBUR's Capacity Tier is located in a physically separate data center from the Performance Tier providing an extra level of security and data protection.

Deduplication, compression & swap exclusion

MBUR decreases backup storage requirements and network traffic with built-in deduplication. Additionally, multiple compression options are used to balance storage consumption with performance and backup proxy load. Swap exclusion reduces backup footprint and improves performance.

Recovery

MBUR Recovery On-Demand can occur at the VM level, File level, Virtual Disk level or Item level.

Guest file system indexing

A catalog of guest files enables quick search and identification of individual files to find and restore a file without knowing the precise file location, or the time when it was deleted.

Changed block tracking for VMware

MBUR minimizes backup time with Changed Block Tracking. This allows for more frequent backups.

vCloud Director support

MBUR provides native vCloud Director support which enables the backup of vApp and VM metadata and attributes and restore vApps and VMs directly to vCloud with full support for fast provisioned VMs and direct restore to vCloud.

Day-to-day management

Summit's Managed Backup & Recovery Service delivers consistent operations management and predictable results by following industry-standard and proven, internal best-practices. The specific services / management functions offered by Summit as part of the Service include:

Change management

MBUR provides simple and efficient means to make controlled changes to Client environments. System changes are serviced by the Managed Services Team through support requests. Changes follow a well-defined approval process, and most changes can be executed quickly by Summit's Managed Services Team.

Incident management

MBUR includes the monitoring of the overall health of the Backup & Recovery platform and the handling of the daily activities of investigating and resolving alarms or incidents. Summit creates pre-defined playbooks that are used to rectify alarms and incidents in a way that minimizes disruption to each Client's environment.

Provisioning management

Designed to meet a Client's specific needs, MBUR allows Clients to configure backup parameters and allocate additional resources to support rapidly changing enviroments. These changes are managed through the timely handling of submitted support requests by our Managed Services Team.

Patch management

MBUR takes care of all infrastructure system patching activities to help keep resources current and secure. When updates or patches are released from infrastructure vendors, Summit applies them in a timely and consistent manner to minimize the impact on Client business.

Access management

MBUR enables clients to securely connect to the Service in the manner they require — be it API access, HTTPS, Cross Connects or Dedicated Physical Connectivity. Our team will make sure that the connection is maintained.

Security management

MBUR protects Client information assets and helps keep all MBUR infrastructure secure. All systems are logically separated and only available to the appropriate MBUR environment. All Summit MBUR services have encryption at rest and in-flight enabled by default for all Clients.

Continuity management

Summit can provide Restore / Recover services as an additional, on-demand service. In the event of a failure or outage that impacts the Client's business, or at their request, Summit can perform a restore of these backups as needed. Summit also offers comprehensive Disaster Recovery as a Service capabilities which introduces formal SLA and automation to the Restore / Recover processes.

Monitoring and reporting

All Summit MBUR environments include comprehensive Health and Performance Monitoring. Weekly or monthly reports, including the status of backup jobs and the associated storage utilization, are available.

What makes this service unique?

Tailored to your use case

We work with you to understand your data protection needs and configure the Managed Backup & Recovery Service parameters to support your unique business, financial, and technological requirements.

Custom backup and recovery policies

You can adjust the frequency of back-ups, retention policies, encryption methods, and data locations to fit these requirements.

Custom replication strategies

You may also choose to have backup data replicated to a second Summit-operated data center to provide physical redundancy should security, governance or compliance requirements dictate.

Roles, responsibilities and process

Successful Managed Services are the result of transparency and collaboration. Clearly defined processes and a detailed outline of roles and responsibilities are where this collaboration begins.

Our Managed Backup & Recovery Service is preceded by defined Consult and Plan, Design and Build processes. These critical steps establish the foundation for the execution of the Service and align these critical processes with your unique business needs.

Consult

We follow a proven, structured process of automated data collection and personal interviews with key business stakeholders, IT infrastructure, and application teams to successfully complete the Discovery process.

The outcome of these efforts includes identification of identification of business drivers and the discovery / analysis of your existing environment including Business and IT Governance processes, Infrastructure configurations and Networking and Security policies.

Discovery sessions are conducted with your company’s subject matter experts (SMEs) and our Managed Services team. This collaboration helps us prioritize your goals and ensure that all critical success factors are met.

Plan, design and build

The data gathered and objectives defined in Consult inform the configuration and process requirements for your Service. Plan, Design and Build brings these to life.

During this phase we will deliver the official, comprehensive analysis of the current environment. This documentation includes, but is not limited to, Infrastructure Diagrams and network connectivity requirements – identifying how is accessed, used and managed today – and where risks are present.

We will also develop and deliver a Remediation Plan for the current environment or a Development Plan for a net-new environment to ensure industry and Summit best practices are in place to support your business today and tomorrow.

Once the recommended Remediation Plan / Development Plan has been vetted and approved, we will move on to complete the Remediation / Development Process using the documentation and decisions identified, and agreed upon, by both parties.

Run and operate

Now that your environment is successfully configured and verified as ready for production, the official Managed Backup & Recovery Service can begin. This is where we begin delivery of proactive day-to-day management, administration, monitoring, and support for your backup and restore environment and processes.

Optimize and evolve

The final component of our Managed Backup & Recovery Service for is the ongoing optimization and evolution of your environment. This phase has us focused on infrastructure performance and cost management. Monthly or quarterly reviews provide updates and opportunities for additional environment optimizations based upon changing business requirements and environment performance. Any opportunities identified are shared directly with your IT and leadership teams to inform strategy and decisions.

Customer success and service operations

The foundation of every Summit Managed Backup and Recovery Service is collaboration. All customer success and service operations workflows have been designed to minimize response time, mitigate risk and optimize collaboration so knowledge transfer occurs when and where necessary.

We recognize your business, and your customers, operate 24x7x365. We have designed and operate our business to be here for you, whenever and however necessary to ensure your success.

Customer success team

Summit provides each customer with comprehensive resources to deliver ongoing service and support for your cloud environment. From sales, solution architecture and certified engineer support on our Service Desk, to customer success and executive management sponsorship, you will have experts with you every step of the way.

How to contact Summit support

Summit uses cases to identify incidents and provide support to our clients until the incident is resolved. Case identification and review is conducted using the Summit Customer Portal. Each Summit client is supplied with accounts that are permissioned to create, update and view their cases.

Case Creation – Customer Portal

Support cases submitted to Summit are submitted using the Summit Customer Portal. The portal is accessible at: https://www.summithq.com/login-and-support/.

To create a support case:

- Log into the Summit Customer Portal.
- Select “Create Case”.
- You receive an automatic confirmation of the successful case creation, including the case number.
- Summit Service Desk staff review the case for accuracy, confirm the Severity Level, and send acknowledgement of case receipt to you.
- Summit Service Desk agent & Cloud Services Engineer work to resolve the support case.
- Case updates are provided at set intervals as determined by the Severity Level.
- Case is Resolved & Marked for Closure.

Case Creation – Telephone

We recognize there may be times when a support case required the immediacy only a phone call can provide. Support cases may be created by calling the Summit Service Desk at +1 312-829-1111, Ext. 2. Telephone submitted support cases utilize a similar support operation, with a few modifications.

To create a support case:

- Call the Summit Service Desk at +1 312-829-1111, Ext. 2.
- Summit Service Desk Agent verifies caller identity, captures relevant information, creates the support case, and assigns a Severity Level.
- Summit Service Desk agent & Cloud Services Engineer work to resolve the support case.
- Case updates are provided at set intervals as determined by the Severity Level.
- Case is Resolved & Marked for Closure.

Case Escalation Paths

Summit provides several, formal options for support case escalation. Escalations occur to set a support case to a desired Severity Level, as outlined below.

Primary Escalation Path - This method is preferred as it is the most efficient method for raising the Severity Level of a case. To create a support case, you will:

- Log into the Summit Customer Portal.
- Navigate to the appropriate case.
- Click the “Escalate Case” link.
- Select the desired Severity Level and submit.

Alternate Case Escalation Path(s) - Additional Case Escalation paths are also available. However, it is important to note that Alternate Case Escalation Paths will not be as expedient as the Preferred Escalation Path.

Alternate Escalation – Case Response

You may submit a response to an existing case and simply request an escalation to the desired Severity Level. The Severity Level will be raised once a Service Desk Agent has reviewed and processed the request.

Alternate Escalation Path - Phone Support

- You may call the Summit Service Desk at +1 312-829-1111, Ext. 2.
- The Summit Service Desk Agent will verify the caller’s identity and the support case number. You verbally request escalation to the desired Severity Level.
- The Summit Service Desk Agent updates the case accordingly.

Response time

All Summit customers can set the severity level of their support cases. The severity level you select will determine the response time. You can select the following severity levels when submitting a support case:

Infrastructure Administration (Proactive Services)

Severity Level	Description	Response Time SLA
Critical / Level 1	Critical Issues include business-critical system outages or issues causing extreme business impact.	15-minute response time
High / Level 2	High Severity Level issues include the impairment of production systems, impaired application performance, and moderate business impact.	30-minute response time
Normal / Level 3	Normal Severity Level issues include standard service issue requests and minimal business impact.	1-hour response time
Low / Level 4	Low Severity Level issues include general information requests, questions and guidance from Summit team members, arranging prescheduled maintenance activities.	4-hour response time
Informational / Level 5	Informational Issues include general questions, how-to style requests, or reports.	24-hour response time

As standard business practice, Summit's Service Desk acknowledges all support cases within 15 minutes of case creation. The response times identified in the table above represent the average time required to remediate such issues. Please note the response time to resolution of your issue may vary based upon circumstances and configurations unique to your business and your cloud architecture. Any support cases created without a severity level selected will be set to "Level 3 – Normal" by default.

Service level agreements

Summit provides two Availability SLAs for Managed Backup and Recovery customers.

Availability SLA

For Summit's Managed Backup Service, Summit provides the following uptime SLA: one hundred percent (100%) availability of the Summit-owned and managed infrastructure supporting the service. If the infrastructure supporting the Managed Backup and Recovery Service disrupts the ability of the service to complete Backup jobs, Customer shall be eligible for a Credit as set in the SLA.

Restoration SLA

Customer is required to submit each Backup Restoration Request via Summit's Customer Service Portal. For providing restoration of data from a completed Backup Job, Summit commits to initiating the restoration process within twenty-four (24) hours of receiving the Restoration Request.

The SLA for MBUR will be dependent upon the configuration(s) selected by Summit and you. You can find current version of the Managed Backup and Recovery SLA on our website.

Account reviews

Summit offers quarterly and annual Account Reviews for all Managed Service Partnerships. These collaborative sessions aim to provide greater visibility into the technical, operational, financial and business aspects of your company and your Cloud. Account Reviews also provide you with a way to offer direct feedback, including areas of improvement, on the status of your Partnership with Summit.

- An Account Review agenda includes:
- Introductions
- Technical, Operational, Business Updates
- Service & Performance Metrics/Dashboard Review
- Optimization Recommendations
- SLA Adherence & Support Ticket Review
- Access Control List (ACL) Review Q&A/Discussion

Upon completion of each account review, you should be confident that we are flexing our services and approach to meet you where you are and have a plan to take you where want to go so that you can focus on what matters most for your customers and your business.

Responsibility matrix

We are committed to solving your Backup and Recovery challenges so you can focus on what matters most.

Each Summit Managed Services Partnership operates with the understanding that there are two parties involved in supporting your environment: your in-house experts and ours.

The MBUR Service, including all Summit-operated hardware and software, is monitored by our Managed Services Team and Service Desk. Should any issues or anomalies be detected with the Service, a member of the Summit Managed Services Team or Service Desk team will take corrective action as planned and notify the customer.

From time to time, we will perform scheduled maintenance activities on the infrastructure supporting the service. Customers will be notified in advance for all scheduled maintenance. Emergency maintenance may be required and performed without advance notice. Should a service-impacting emergency maintenance be required, we will use commercially reasonable efforts to notify Customer upon execution of the maintenance.

The following responsibility matrix defines the roles and responsibilities for each phase:

Consult responsibilities

Managed Service	SUMMIT	Customer
Identify Business Drivers	Y	Y
Align Business Drivers with Project	Y	Y
Current Infrastructure	Y	Y
Current Applications	Y	Y
Application Dependency Mapping	Y	Y

Plan, design and build responsibilities

Plan and Design Managed Service	SUMMIT	Customer
Greenfield Architecture	Y	N
Total Cost of Ownership	Y	N
Migration Plannning	Y	N
Security and Compliance Requirements	Y	N

Build Managed Service	SUMMIT	Customer
Proof of Concept / Pilot Environment	Y	N
Environment Build-Out (New)	Y	N
Environment Remediation (Existing)	Y	Y
Environment Migration	Y	Y

Run and operate responsibilities

Configuration Managed Service	SUMMIT	Customer
Backup Infrastructure Patching and Updates	Y	N
Backup Infrastructure Configuration Management Automation	Y	N
Backup Infrastructure and Environment Audit Logging	Y	N
Credential Management and Resets	Y	N

Monitoring and Alerting Managed Service	SUMMIT	Customer
Backup Network Performance	Y	N
Backup Storage Performance	Y	N
Backup Application Performance	Y	N
Infrastructure Alert Response and Triage	Y	N
Environment Alert Response	Y	N

Security Managed Service	SUMMIT	Customer
Backup Network Configuration and Security Protection	Y	N
Data Encryption Enforcement	Y	N
Key Management	Y	N
Compliance Support	N	Y

Run and operate responsibilities continued

Support Managed Service	SUMMIT	Customer
Support / Incident Portal	Y	N
Incident Response	Y	N
Request Response	Y	N
Custom Dashboard and Reporting	Y	N
On-Demand Recovery Support (Items Outside of Service)	Y	N

Optimize and evolve responsibilities

Change Management Managed Service	SUMMIT	Customer
Backup and Recovery Infrastructure Resources	Y	N
Backup and Recovery Application Configuration	Y	N
OS-Level UAC	Y	N

Audit Trails Managed Service	SUMMIT	Customer
Backup and Recovery Infrastructure Logs	Y	N
OS-Level Logs	Y	N
Application-Level Logs	Y	N
Platform Compliance Initiatives	Y	N

Tired of tech that underdelivers?

Let’s fix that. Get IT infrastructure that works at summithq.com.