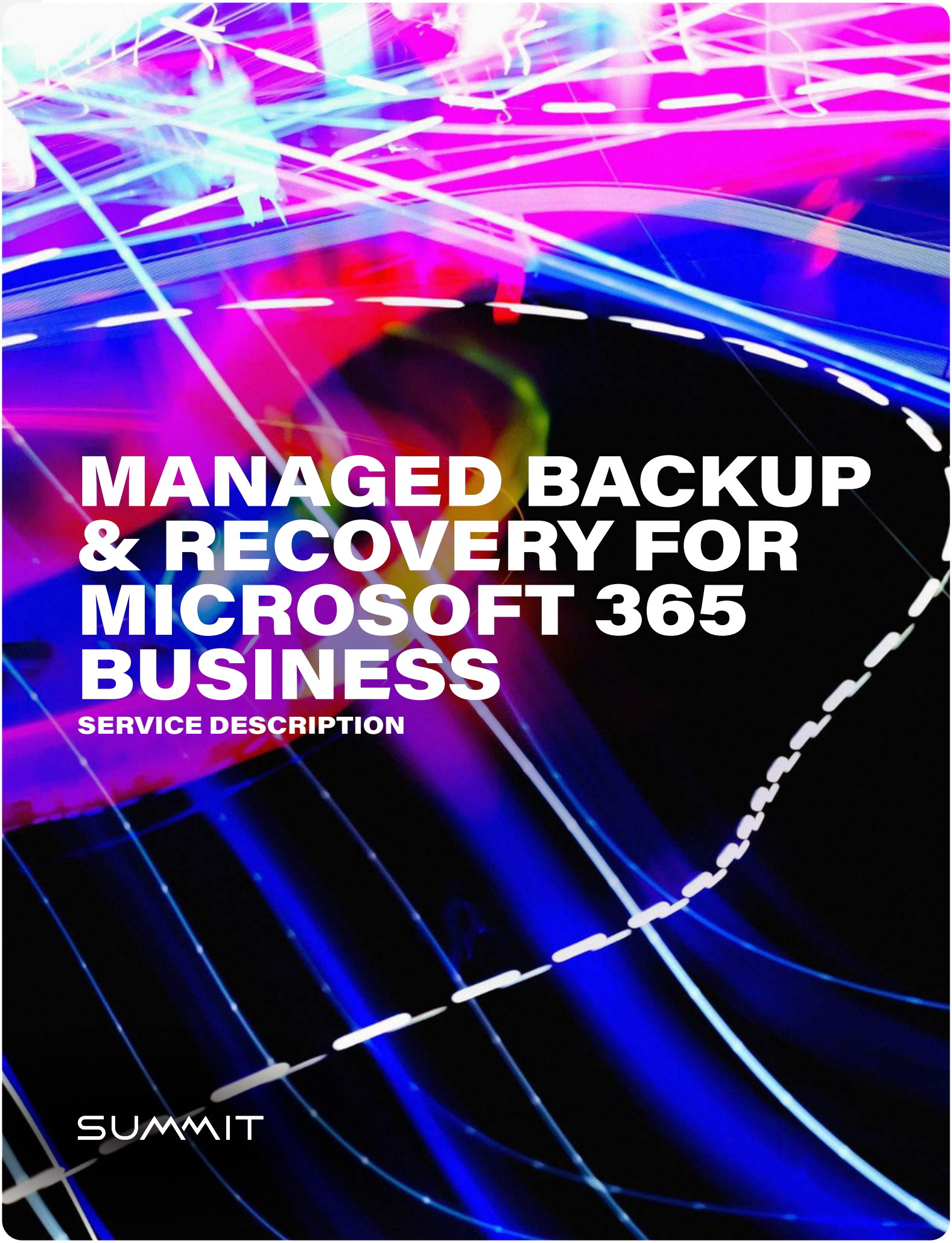


MANAGED BACKUP & RECOVERY FOR MICROSOFT 365 BUSINESS

SERVICE DESCRIPTION

SUMMIT

Service overview

Summit's Managed Backup & Recovery for Microsoft 365 Service provides protection for the data and configurations contained in your Microsoft 365 or on-premise Exchange and SharePoint environments. This includes, but may not be limited to, Exchange, SharePoint, OneDrive for Business and Teams.

Backups are performed, stored, and maintained in one of our secure, SOC 2 compliant data centers on our fully redundant, high-performance object storage platform. We utilize the industry's leading technology, Veeam Backup & Recovery for Microsoft 365, to power this service.

Managed Backup & Recovery for Microsoft 365 is a fully managed service that is configured, administered, monitored, and supported 24x7x365 by our Managed Services and Service Desk teams.

As a fully managed service, our Managed Services engineers support the underlying hardware & software tools used to deliver the Managed Backup & Recovery Service, as well as administer and monitor the backup and recovery processes. You will receive a weekly Managed Backup & Recovery Service Report detailing the status of backup jobs, completion of jobs, and any other information about the Service. To create or alter backup jobs, change data retention policies, or get any additional information about the service, you simply open a support ticket via our Customer Portal.

Default configuration and backup schedule

In the default configuration, the Service will provide daily incremental backups. The data for all backups retained for 14 days in a Summit data center on our fully redundant, high-performance object storage platform. Customers can choose to have more or less frequent backups, shorter or longer retention timeframes, or replication to a specific data center should these capabilities be required. Please note increased frequency and data retention length will have an impact on the Service cost.

For security and compliance purposes, backup to a second or third Summit-operated data center is available as an option, for an additional fee.

Encryption

The Managed Backup & Recovery for Microsoft 365 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.

Service overview

Restore processes

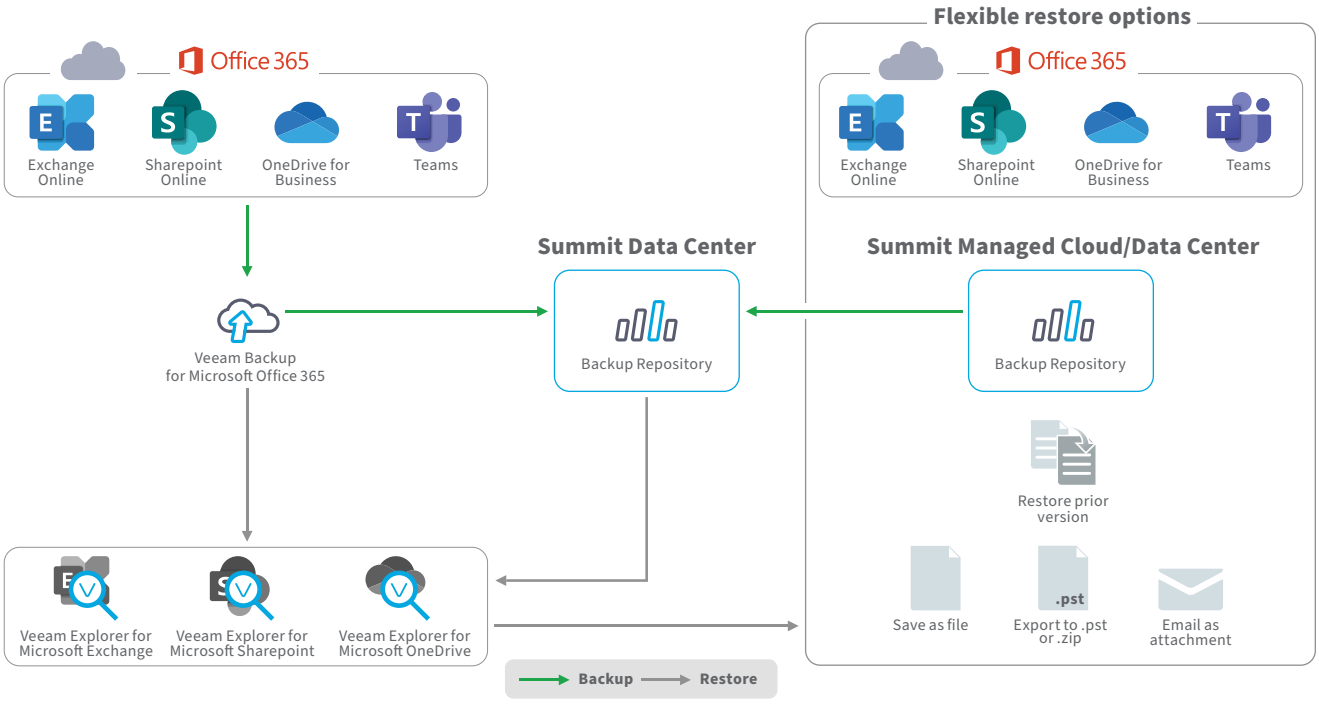
Restores for backup data are performed upon request. Restores can be made in time-based, aggregate or granular fashions with item-level restore requests supporting critical emails, files, conversations, projects, tasks and other 365 assets. You can also request security roll-backs to remove unintended permission or configuration changes.

Data is generally restored to the primary system where the data originated – your Microsoft 365 environment. The Service does support the option for Microsoft 365 data to be recovered to additional environments including a Summit Managed Cloud, a Summit Managed Colocation configuration or a Customer Premise location.

Recoveries are performed on a best-effort basis and will include additional charges for use of storage and/or cloud services as applicable. Please note, restore locations and procedures will be pre-defined and specific to your unique requirements. When restores are needed, no additional questions will need to be asked or answered unless your needs for a specific request areunique.

Sample service configuration

The Managed Backup & Recovery for Microsoft 365 Service is offered on a per-user per month basis, with a minimum of 10 user licenses required. Users are calculated as licensed Microsoft 365 or Exchange Users. Shared mailboxes are included for free.



Key features

The key features for this Service include, but are not limited to:

- Backup Microsoft 365 Exchange, SharePoint, OneDrive for Business and Teams data and configurations so you always have access to your data
- Complete configuration & administration by Summit's Managed Services Engineers
- Backup job monitoring, with regular reporting
- Flexible, tiered backup, retention, and replication schedules designed around your requirements
- Option for restore into Microsoft 365 enviroments, Summit Managed Cloud Services, Summit Managed Colocation Services and/or Customer Premise environments
- 24x7 Service infrastructure health monitoring, performance metrics, and alerting
- 24x7 Service Desk support for ticket acknowledgement, management and response

Day-to-day management

Summit's Managed Backup & Recovery for Microsoft 365 Service (MBUR) 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 environments. 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.

Monitoring & reporting

All Summit MBUR environments include comprehensive Health + Performance Monitoring. Reports including the status of backup jobs and the associated storage utilization are available.

Maintenance

For the MBUR Service, Summit provides the Maintenance of all infrastructure and backup software. This includes, but is not limited to, regularly scheduled updates to all service components, ad-hoc updates should emergency updates be necessary, communication of regularly scheduled maintenance and coordination of emergency maintenance.

Maintenance schedules

Summit maintains regular maintenance schedules, as follows:

- Production: Declared Saturday of Every Month: 4:00am - 8:00am CST/CDT
- Other Environments: Remaining Saturdays: 4:00am - 8:00am CST/CDT

Based on the Managed Backup & Recovery for Microsoft 365 Service configuration, Summit will perform scheduled maintenance activities on the infrastructure and backup software included as part of the service in accordance with the schedule noted above. 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, Summit will use commercially reasonable efforts to notify Customer upon execution of the maintenance.

Support

For the Managed Backup & Recovery for Microsoft 365 Service, Summit provides support for all necessary components of the Service, exclusing Microsoft 365 itself. This includes, but is not limited to, testing of updates and patches provided by vendors to create official, customer approved images, 24x7x365 response to customer support inquiries, and provides confirmation of all successful client Microsoft 365 environment backups.

Customers may also view real time and historical information regarding the Service via the Summit Customer Portal located at https://www.summithq.com/login-and-support/.

Customer success & Service operations

The foundation of every Summit Managed Backup & Recovery for Microsoft 365 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 & Network 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 – Customer Portal

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 ecient 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 Sumit 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.

Service & support response time

All Summit Managed Backup & Recovery for Microsoft 365 Service 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:

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 MSP 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 respond to such issues. Please note the 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

The Managed Backup & Recovery for Microsoft 365 Service is governed by Managed Backup Service Level Agreement.

The SLA for your Managed Backup & Recovery for Microsoft 365 Service will be dependent upon the configuration(s) selected by Summit and you. You can find current version of the Managed Backup & Recovery for Microsoft 365 Service Level Agreement on our website at https://www.summithq.com/.

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
- Question & Answer / 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.

Tired of tech that underdelivers?

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