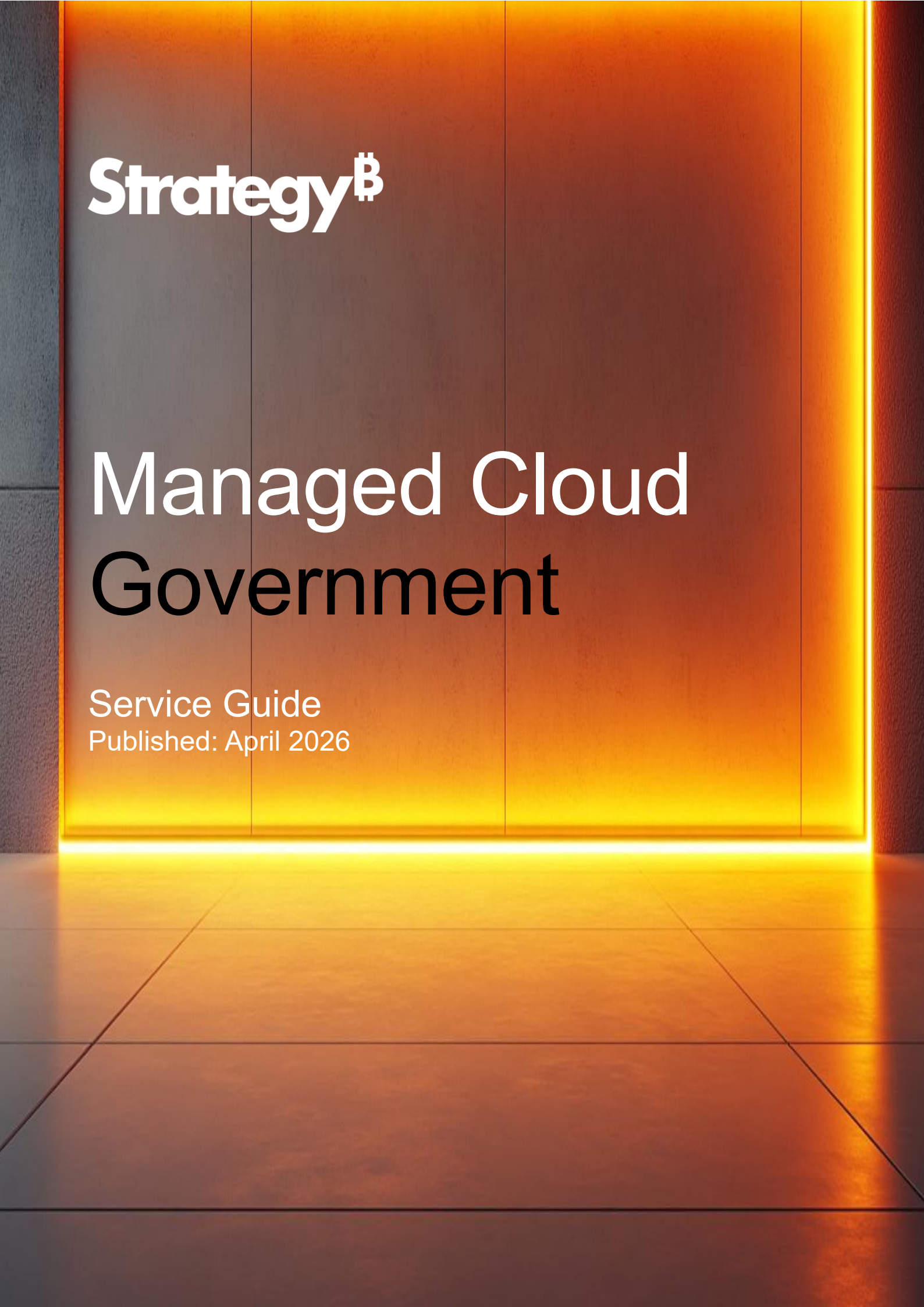

Strategy

Managed Cloud Government

Service Guide

Published: April 2026

Copyright Information

Trademark Information

The following are either trademarks or registered trademarks of Strategy Incorporated or its affiliates in the United States and certain other countries:

Dossier, Enterprise Semantic Graph, Expert.Now, Hyper.Now, HyperIntelligence, HyperMobile, HyperVision, HyperWeb, Intelligent Enterprise, Strategy, Strategy 2019, Strategy 2020, Strategy 2021, Strategy Analyst Pass, Strategy Architect, Strategy Architect Pass, Strategy Auto, Strategy Cloud, Strategy Cloud Intelligence, Strategy Command Manager, Strategy Communicator, Strategy Consulting, Strategy Desktop, Strategy Developer, Strategy Distribution Services, Strategy Education, Strategy Embedded Intelligence, Strategy Enterprise Manager, Strategy Federated Analytics, Strategy Geospatial Services, Strategy Identity, Strategy Identity Manager, Strategy Identity Server, Strategy Insights, Strategy Integrity Manager, Strategy Intelligence Server, Strategy Library, Strategy Mobile, Strategy Narrowcast Server, Strategy One, Strategy Object Manager, Strategy Office, Strategy OLAP Services, Strategy Parallel Relational In-Memory Engine (Strategy PRIME), Strategy R Integration, Strategy Report Services, Strategy SDK, Strategy System Manager, Strategy Transaction Services, Strategy Usher, Strategy Web, Strategy Workstation, Strategy World, Usher, and Zero-Click
Intelligence.

The following design marks are either trademarks or registered trademarks of Strategy Incorporated or its affiliates in the United States and certain other countries:

Other product and company names mentioned herein may be the trademarks of their respective owners.

Specifications subject to change without notice. Strategy is not responsible for errors or omissions. Strategy makes no warranties or commitments concerning the availability of future products or versions that may be planned or under development.

Table of Contents

Service Level Agreement

With Strategy's Managed Cloud Government (MCG) services, harness the power of the Strategy One platform, and allow your business to focus on data rather than cloud management. Strategy One is designed to empower businesses with cutting-edge capabilities for analytics and business intelligence in a modern, intuitive interface. Leveraging this platform, your organization can tap into powerful, built-in benefits, including seamless integration with other data sources, advanced security measures, and efficient data management.

The Managed Cloud Government service ("MCG Service") is a software-as-a-service ("SaaS") offering that Strategy manages on its customers' behalf in an Amazon Web Services environment for GovCloud that includes access to, collectively, the "Cloud Platform" version of Strategy software products (an optimized version of the Strategy software platform built specifically for deployment in AWS GovCloud) licensed by the customer. Strategy's SaaS delivery model is designed to allow businesses to consume the Strategy Analytics and Mobility platform in a single tenant architecture without the need to deploy and manage the underlying infrastructure.

As an MCG Service customer, you will receive "Cloud Service Support" (Cloud Support) in which our Cloud Support engineers will provide ongoing support over your MCG Service term to assist in maximizing the performance and agility—as well as minimizing the cost—of your Strategy Cloud Platform deployment. Cloud Support includes environment configuration (setting up customer accounts in a selected VPC), enterprise data warehouse integration (including modifying the Strategy configuration for data warehouse connections and opening any connectivity for external data warehouses), authentication (OIDC/SAML), and application integration.

If a production outage issue occurs, Strategy reserves the right to fix the issue on behalf of the customer without pre-authorization. If a support issue is logged and determined through the diagnosis that the Root Cause Analysis (RCA) that the stated issue is due to a customer-specific customization of the Strategy application, the Cloud Support team will provide the customer with available options to resolve the issue. These solutions may require the purchase of Strategy Professional Services for additional assistance depending on the complexity of the issue.

Cloud Offering

The Cloud Architecture offered as part of the MCG Service is an optimized reference architecture providing enterprise-grade data design and governance, and consists of (a) the Cloud infrastructure and architecture components required to run your SaaS environment, configured through High-Availability MCG Architecture constructs detailed below, and (b) Cloud Environment Support, the support services and components needed to successfully run the infrastructure and architecture components of the MCG Service offering.

Strategy's Enterprise MCG Architecture is built on Amazon Web Services. Each instance consists of an instance(s) for Strategy Intelligence Server, Library, Library Mobile, Modeling Service, Export Engine, Platform Analytics, and Collaboration. Additionally, a

database for the Strategy metadata and statistics is provided. Administrators have the option to purchase incremental resources as needed.

A. The cloud infrastructure provided with the Cloud Architecture - Tier 2 operating environment (designated on an order as “Cloud Platform for AWS-Tier 2-MCG”) includes the following components:
• two (2) high-availability instances (HA) with up to 512 GB RAM each;
• one (1) non- high-availability instance with up to 256 GB RAM;

B. The cloud infrastructure provided with the Cloud Architecture - Tier 3 operating environment (designated on an order as “Cloud Platform for AWS-Tier 3-MCG”) includes the following components:
• two (2) high-availability instances (HA) with up to 1 TB RAM each;
• one (1) non-high-availability instance with up to 512 GB RAM; and
• one (1) non- high-availability instance with up to 256 GB RAM;

C. The cloud infrastructure provided with the Cloud Architecture - Tier 4 operating environment (designated on an order as “Cloud Platform for AWS-Tier 4-MCG”) includes the following components:
• two (2) high-availability instances (HA) with up to 2 TB RAM each;
• one (1) non-high-availability instance with up to 1 TB RAM; and
• one (1) non-high-availability instance with up to 512 GB RAM;

Additional instances are also available to purchase, through the execution of an order, as an add-on to this offering. Each additional instance purchased is for use in either production or non-production environments. A customer may purchase additional instance to create a HA production instance (inclusive of a high-performance file system) or for use as separate, standalone environments for quality assurance or development.

Our MCG Service offers an enterprise platform architecture based on industry best practices for security, compliance, and availability. The building block of these SaaS components is an infrastructure package and optional add-ons which allow you to add high availability and extra environments if needed. The MCG Service provides a highly elastic infrastructure that can scale both horizontally and vertically. In addition, MCG Service also provides 24x7x365 system monitoring and alerting, daily backups for streamlined disaster recovery, and an environment with FedRAMP Authorization. This offering is procured on your behalf from Amazon Web Services to host the MCG. Additionally, all MCG customers will receive up to 1 TB per month of data egress. As part of the MCG quarterly service review, we will advise you if your monthly data egress usage is close to or exceeds 1 TB for each MCG environment.

The MCG Service offering is a fully managed cloud environment with each customer getting their own tenant along with a dedicated metadata database, load balancers, firewalls, data egress, and other services to ensure ease of use for customers. This also includes Strategy Workstation deployed on the client machine to enable customer administrators to perform tasks such as assigning roles and permissions to users etc.

Service Availability

The MCG Service offers a service level agreement of 99.9% availability for HA environments and 99% availability for non-HA environments. Availability is calculated per calendar month as follows:

$$\left[\left(\frac{\text{Total Minutes} * \#\text{ of Production Instances} - \text{Unavailability}}{\text{Total Minutes} * \#\text{ of Production Instances}}\right) * 100\right]$$

Service Definition

“Availability”: the access to mission critical system components including Strategy Library, APIs and Endpoints to support end users. Access is based on 24x7 for high-availability environments and 12x5 for non-high availability environments.

“Total Minutes”: the total number of minutes in a calendar month.

“Container”: a full set of MCG Container Architecture that users are running in support of an operational business process.

“Unavailability”: for each Instance, the total number of minutes in a calendar month during which (1) the Instance(s) has no external connectivity; (2) the Instance(s) has external connectivity but is unable to process requests (i.e., has attached volumes that perform zero read- write IO, with pending IO in the queue); or (3) all connection requests made by any component of the Instance(s) fail for at least five consecutive minutes. “Unavailability” does not include minutes when the MCG is unavailable due to issues referenced in section 3.5 of this document.

“Total Unavailability”: the aggregate unavailability across all Instances.
For any partial calendar month during which customers subscribe to the MCG, availability will be calculated based on the entire calendar month, not just the portion for which they subscribed.

Service Remedies

MCG offers a service level agreement of 99.9% for High Availability environments and 99.5% for non-HA environments. If the availability standards are not met in any given calendar month, customers may be eligible for a Service Credit, according to the definitions below. Each Service Credit will be calculated as a percentage of the total fees paid by customers for the MCG Service, managed by Strategy within the calendar month that a Service Credit has been accrued. This is the exclusive remedy available to customers if Strategy fails to comply with the service level requirements below.

Service Credits

HA Production Instance:

- Availability less than 99.9% but equal to or greater than 99.84%: 1% Service Credit
- Availability less than 99.84% but equal to or greater than 99.74%: 3% Service Credit
- Availability less than 99.74% but equal to or greater than 95.03%: 5% Service Credit
- Availability less than 95.03%: 7% Service Credit

Non-HA Production Instance:

- Availability less than 99% but equal to or greater than 98.84%: 1% Service Credit
- Availability less than 98.84% but equal to or greater than 98.74%: 3% Service Credit
- Availability less than 98.74% but equal to or greater than 94.03%: 5% Service Credit
- Availability less than 94.03%: 7% Service Credit

Service Credits Procedure

To receive a Service Credit, customers must submit a Strategy case on or before the 15th day of the calendar month following the calendar month in which the Service Credit allegedly accrues that includes the following information: (a) the words “SLA Credit Request” in the “Case Summary/ Error Message” field; (b) a detailed description of the event(s) that resulted in unavailability; (c) the dates, times, and duration of the unavailability; (d) the affected system or component ID(s) provided to customers by Strategy during onboarding and Intelligence Architecture delivery activities; and (e) a detailed description of the actions taken by users to resolve the unavailability.
Once Strategy receives this claim, Strategy will evaluate the information provided and any other information relevant to determining the cause of the Unavailability (including, for example, information regarding the availability performance of the Intelligence Architecture, third-party software or services, dependencies on customer-hosted or subscribed software or services, operating system, and software components of the MCG). Thereafter, Strategy will determine in good faith whether a Service Credit has accrued and will notify customers of its decision. If Strategy determines that a Service Credit has accrued, then at its discretion, it will either (1) apply the Service Credit to the next MCG Service invoice sent or (2) extend the MCG Service Term for a period commensurate to the Service Credit amount. Customers may not offset any fees owed to Strategy with Service Credits.

Exclusions

In the context of Strategy MCG managed cloud services delivered via a SaaS model, the following are considered exclusions for service as it concerns all matters of impacts to availability:

1. **Scheduled Maintenance**: Service interruptions during scheduled maintenance, announced in advance, are excluded from the SLA.
2. **Customer Configurations**: Service issues caused by customer actions, such as misconfigurations or excessive API requests, are not covered. Issues related to

applications built on the Strategy software platform, including project, report, and document issues; migration problems related to user design; downtime experienced as a result of user activity.

3. **ETL Application:** Outages caused through degradation or failure of ETL processes in the application.
4. **Database Issues and Configuration:** Improper database logical design and code issues.
5. **HyperScaler or other Third-party Services**: Downtime related to third-party services or dependencies outside control is excluded.
6. **Force Majeure**: Events beyond control of Strategy, such as natural disasters or government actions, do not qualify for SLA coverage.
7. **Unauthorized Access**: Issues not originated by Strategy like unauthorized access or credential compromised
8. **Customer-Based Migration Issues:** Migration problems and outages related to customer or user design.
9. **SSO or other Custom Security Configuration or Policies**: Implementation and management of custom security policies and compliance measures outside the pre-configured, standard security settings are not included.
10. **Network Connectivity Issues**: Issues related to the customer's internal network or internet connectivity, including VPN configurations and local firewall settings, fall under the customer's responsibility.

These exclusions ensure a clear boundary of responsibilities and help manage expectations for the scope and limits of Strategy MCG managed cloud services within a SaaS delivery model.

Support Levels

As an MCG customer, you receive "Cloud Application Support" ("Cloud Support") in which Strategy Cloud Support engineers provide ongoing management over your MCG term to assist in maximizing the performance and agility of your Strategy Cloud deployments.
If a production outage issue occurs, Strategy reserves the right to fix the issue on behalf of the customer without pre-authorization.

Support Availability

The MCG Service will provide 24x7 operations support in the customer's local time zone. These parameters may be changed based upon mutual agreement.

Service Levels

Support Detail	MCG Support
Designated Customer Success Manager (CSM)	Yes
Number of designated Support Liaisons	4
Initial response times for P1 and P2 issues **priority definitions as provided in the Technical Support Policy and Procedures	P1 < 2hr P2 < 2hr
P1 and P2 issues updates	As Status Changes
Case management meetings	No

System alert notifications	No
Quarterly service reporting	Via email
Location based 24x7 support	Yes

Root Cause Analysis (RCA)

For production outages, an RCA is generated by the Cloud Support team. For other P1 cases (outside of a production outage) that are logged, an RCA can be requested by the customer. Customers will receive the RCA report within 10 business days of the production outage or the requested RCA. The final analysis is conducted during business hours in the Eastern Time Zone to allow for management and peer approvals before formal communication of the stated issues.

Cloud Support will cover all support regarding the diagnosis of the RCA. It will also cover product defects, security updates, operating system updates, and changes. As noted in Section 3, if an RCA determines an issue to be created by a customer-specific customization, Strategy will provide options outside of Cloud Support, such as Professional Services engagements, to remedy the issue.

24/7 Cloud Help Desk

For Production system outages where system restoration is paramount, all alerts are sent to a 24x7 dedicated operations support team within the US Region for prompt resolution.

24/7 Monitoring and Alerting

Key system parameters are tagged and monitored. Strategy has alerts on CPU utilization, RAM utilization, disk space, SSL certification expiration, daily backups, host failures, application-specific performance counters, VPN Tunnel, and ODBC warehouse sources monitoring. System performance is logged over time to give the customer and Cloud Support team the ability to maintain a performant cloud platform.

Backups

Daily backups are performed for all customer systems, including system state, metadata, customizations, and performance characteristics. Strategy retains at least ninety consecutive days of backups. Backups are dispersed across availability zones to ensure multiple points of failure (for example, a single cloud data center).

Platform Analytics Strategy

Platform Analytics is set up for all Strategy customers on MCG and maintained to allow for instant access to system performance metrics. In the event the space availability is less than 20% of the allocated storage, after receiving the customer’s consent, Strategy will purge older data from the MCG Service-based Platform Analytics database in 30- day increments until the disk availability is below the 80% capacity threshold. The amount of data that the customer chooses to keep may have a corresponding cost to the customer. Contact your Account team for a cost estimate to modify the MCG Service, including increases to the data repository and/or cube memory requirements.

Intra-Region Failover

For all MCG deployments, production environments are deployed across multiple Availability Zones. This provides physical separation of compute and data and allows the service to continue running if one AZ becomes unavailable. For container-based deployments in all Tiers, failover is automatic. If capacity is available in a third AZ, replacement workloads are started there. Some active sessions or jobs on the affected AZ may be interrupted, but services are restored automatically without manual intervention. This is achieved by utilizing underlying application features and building on best practices such as clustering along with the advantage AWS allows through the splitting of the GovCloud Region into multiple Availability Zones ("AZ") to withstand AZ-wide failure. The use of multiple AZs creates a physical separation of data between the machines storing production and backup environments.

Maintenance and Updates

Maintenance windows are scheduled monthly to allow for a monthly update of Strategy and third-party security updates to be applied to the MCG platform. Updates will not include any new, unlicensed products. During these scheduled interruptions, the MCG Service systems may be unable to transmit and receive data through the provided services. Customers should plan to create a process that includes the pause and restart of applications, rescheduling subscriptions, and including but not limited to, related data load routines. When it is necessary to execute emergency maintenance procedures, Strategy will notify customer-specific support liaisons via email as early as possible—identifying the nature of the emergency and the planned date and time of execution. Customers will normally receive a minimum of two weeks' advance notification for planned maintenance windows. However, if emergency maintenance work is required, we will use commercially reasonable efforts to give 48-hour notice before applying a remedy.

Security

Various security tools are employed to perform penetration testing and remediation, system event logging, and vulnerability management. The MCG Service maintains a high security posture in accordance with the following security standards:

Federal Risk and Authorization Management Program (FedRAMP)
FedRAMP is a government-wide initiative in the United States that establishes a uniform approach to security evaluation, authorization, and continual monitoring of cloud products and services. Its governing entities comprise the Office of Management and Budget (OMB), the General Services Administration (GSA), the Department of Homeland Security (DHS), the Department of Defense (DoD), the National Institute of Standards & Technology (NIST), and the Federal CIO Council. Cloud Service Providers (CSPs) seeking to provide their Cloud Service Offerings (CSOs) to the US government are required to adhere to FedRAMP guidelines. Utilizing the NIST Special Publication 800 series guidelines, FedRAMP mandates CSPs to undergo an independent security assessment by a Third-Party Assessment Organization (3PAO) to validate compliance with the Federal Information Security Management Act (FISMA).

National Institute of Standards and Technology (NIST)

NIST Special Publication (SP) 800-53's security controls are designed for use with US Federal Information Systems. These systems must undergo a systematic assessment and authorization process for the adequate protection of data confidentiality, integrity, and availability. The MCG Service leverages these controls from the NIST SP 800-53 for its FedRAMP Moderate solution. NIST's Cybersecurity Framework (CSF) has gained acceptance across governments and businesses globally as the standard groundwork applicable to organizations of all sizes and sectors. Post 2016, metrics under the Federal Information Security Modernization Act (FISMA) have been restructured around the CSF, and pursuant to the Cybersecurity Executive Order, adoption of the CSF is mandatory for agencies.

Federal Information Processing Standards (FIPS) 199
FIPS 199 outlines a structure to evaluate potential impacts on organizational operations, assets, or individuals through three main security goals: confidentiality, integrity, and availability. This standard requires federal agencies to appraise their information systems within these categories, ranking each system as either 'Low (L)', 'Moderate (M)', or 'High (H)' impact. The highest severity level identified within any category dictates the overall security categorization of the system. According to FIPS 199 regulations, the MCG Service is categorized with a 'Moderate (M)' impact tier.

Federal Information Processing Standards (FIPS) 200
FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," is a compulsory standard issued by NIST due to FISMA. To adhere to it, organizations must categorize their information system as per FIPS Publication 199, determine the impact level according to FIPS 200, and implement tailored baseline security controls from NIST Special Publication 800-53. This standard extends the categorization framework of FIPS 199 and sets minimum security requirements across 17 cybersecurity areas like access control, incident response, and risk assessment.

Federal Information Processing Standards (FIPS) 140-2
FIPS 140-2 establishes standards for cryptographic modules, which include hardware and software components. Ensuring the confidentiality and integrity of sensitive information is vital for any cryptographic module used within a security system. This standard outlines the necessary security requirements that must be met by a cryptographic module, providing four distinct levels (Level 1 to Level 4) for a variety of use cases and environments. Covered topics involve design and construction; interfaces and physical connections; user roles, services, and authentication methods; state transition logic; physical security provisions; environmental operation scenarios; and protocols for managing cryptographic keys. MCG Service complies with encryption protocols validated by FIPS 140-2 to guarantee secure data transactions with all integrated applications.

Quarterly Service Reviews

The designated Customer Success Manager (CSM) for your MCG will conduct the Quarterly Service Reviews (QSR) with the business and technical contacts on a quarterly cadence. This may include the overview of system resources and recommendations based on observed trends.

Cloud Shared Services Components

As part of the MCG Service's platform architecture and in support of the MCG Service, we incorporate other solutions to assist in the management, deployment, and security of the environment, and to complete operational tasks. These solutions include management and detection response, cloud security posture management, compliance with FedRAMP, NIST SP 800-53, and CIS Foundations Benchmarks, adherence to AWS Foundational Security Best Practices, application and infrastructure monitoring, alerting and on-call management, and workflow and continuous integration tools.

Non-Migrated Components

Stated below are Strategy components that will not be hosted in cloud. Customers are highly encouraged to move away from legacy components and leverage newer and modern replacement of such tools:

- Strategy Narrowcast Server replaced with Distribution services
- Strategy Enterprise Manager replaced with Platform Analytics
- Web is replaced with Library
- MDX Cubes to be converted to MTDI/OLAP
- Big Data and Cloud Connectors are not supported for MCG
- Mobile is replaced with Library Mobile
- SDK/Plugins are not supported for MCG
- 32-bit Client Tools (ex. Developer, Object Manager, Command Manager, System Manager, Project Duplication, Integrity Manager) is replaced with Workstation

The following items below are supported only for connectivity to MCG. Strategy will not host them in the Cloud. These solutions may require additional assistance from Strategy Professional Services.

- ETL/Scheduling Tools

Distribution Services

All Strategy Cloud customers are required to use their own SMTP server for delivery of email and history list subscriptions. File subscriptions are pushed to AWS S3 bucket provided to the customer as part of the MCG infrastructure to all customers. Customers may pull file subscriptions from the storage locations provided during the on-boarding process with their Customer Success Manager (CSM).

AI Capabilities

The "AI Power User," "AI Consumer User," "AI Architect User," "Strategy AI," and "Strategy AI User" SKUs provide artificial intelligence capabilities as a part of your MCG Service ("AI Capabilities").

AI Capabilities are designed to accommodate various user roles, and provide AI-assisted data exploration, automated dashboard design processes, SQL generation tools, and ML-based visualization methods. The AI Capabilities within the framework of the Strategy analytics platform augment the platform's data processing and presentation capabilities. The use of AI Capabilities may have limitations which impacts the effectiveness, quality

and/or accuracy of output from your MCG Service and should not replace human decision-making. You remain responsible for judgments, decisions, and actions you make or take based on the output of your MCG Service.

Notwithstanding anything to the contrary, we may provide AI Capabilities to you from an environment that is different from the operating environment specified on your MCG Service order. You may not perform any penetration testing on the artificial intelligence service powering the AI Capabilities.

Consumption-Based Licensing and Auto-Replenishment of the Strategy AI SKU

- For each Strategy AI SKU quantity you license, you may consume up to twenty thousand (20,000) Questions (as defined below) for a period of up to twelve (12) months beginning on the order effective date and, in the case of a replenishment, from the beginning of the replenishment effective date (each period, a “Use Period”). Unconsumed Questions are automatically forfeited at the earlier of (a) the end of the Use Period, or (b) termination or expiry of the MCG Service term, and do not carry over to any subsequent Use Periods. Upon the earlier of the expiration of the Use Period or the full consumption of 20,000 Questions, we will automatically replenish your right to consume an additional 20,000 Questions for each licensed Strategy AI SKU quantity for a subsequent Use Period, each at the then current list price for such Strategy, unless you provide written notice to us that you desire not to auto-replenish (a) at least ninety (90) days before the expiration of the then current Use Period, or (b) before 18,000 Questions have been consumed, whichever occurs first. Strategy AI is otherwise non- cancelable by you, and nonrefundable.
- For the avoidance of doubt, the foregoing does not apply to the licensing of the other AI Capability SKUs, which are licensed on a named user basis, with no limit on the number of questions. Customers purchasing the Strategy AI SKU will have access to Platform Analytics, which will include your usage in its reporting.
- One “Question” is defined as any input action taken while using the Strategy AI SKU. Below are examples of a Question:
- Auto Answers (multiple consumption options):
  - One action submitted to Strategy’s Auto chatbot that returns a response constitutes consumption of one Question.
  - One click on auto-populated suggestions below Strategy’s Auto chatbot input box constitutes consumption of one Question.
  - Any subsequent selection(s) of the recommended data analysis constitutes consumption of an additional Question.
- Auto SQL:
  - One action submitted to Strategy’s Auto chatbot that returns a response constitutes consumption of one Question.
- Auto Dashboard (multiple consumption options):
  - One action submitted to Strategy’s Auto chatbot that returns a response constitutes consumption of one Question.
  - One click on auto-populated suggestions below Strategy’s Auto chatbot input box constitutes consumption of one Question.
  - Any subsequent selection(s) of the recommended data analysis constitutes consumption of an additional Question.

Customer's Responsibilities

ACTIVITY	DESCRIPTION	MCG STANDARD	CUSTOMER
Cloud Platform			
Environment Build	Automated build, security boundaries, etc.	RA	CI
Infrastructure Maintenance	Monthly/Emergency Maintenance Windows, OS Updates	RA	I
Environment Resizing	Upsizing/Downsizing of the VMs	RA	CI
Infrastructure Management	All cloud components such as VMs, Storage, DBMS (for MD/PA)	RA	
Backups	Compute Instances, cache/cubes files, MD Repository, ODBC and Config files	RA	
Restores	Compute Instances, cache/cubes files, MD Repository, ODBC and Config files	RA	CI
24x7 Support		RA	
Security & Compliance			
FedRAMP Moderate	Certifications with 3rd party audit	RA	I
FIPS 140-2	Certifications with 3rd party audit	RA	I
FIPS 200	Certifications with 3rd party audit	RA	I
FIPS 199	Certifications with 3rd party audit	RA	I
NIST Special Publication (SP) 800-53	Certifications with 3rd party audit	RA	I
NIST Cybersecurity Framework (CSF)	Certifications with 3rd party audit	RA	I
ISO27001	Certifications with 3rd party audit	RA	I
SOC2/Type 2	Certifications with 3rd party audit	RA	I
GDPR	Certifications with internal audit	RA	I
PCI	Certifications with internal audit	RA	I
HIPAA	Certifications with 3rd party audit	RA	I
24x7 Security Incident Event Management	Security logs sent to SIEM for automatic analyses	RA	I
Vulnerability Management	Scanning, remediation following the NIST standards	RA	I
Penetration Testing	Quarterly environmental external scanning	RA	I
Data Encryption at Rest	AES 256 encryption on storage volumes and MD DB	RA	I
Monitoring			
Cloud Infrastructure Components	VMs, Storage, DBMS (for MD/PA), Network components	RA	I
Application Services	Strategy Components like I-Server, WebApps, etc.	RA	I

Data Connectivity	VPN, PrivateLink	RA	CI
Intrusion Detection	SIEM	RA	I
Networking Connections	On-Premise Connectivity for internal access	RA	CI
Networking			
Logging	Load balancer logs, etc.	RA	
Data source and Databases connections	Deployment/configuration of VPN Tunnels, Private Links, Express route, etc.	RA	RA
Networking Connections	On-Premise Connectivity for internal access	RA	RA
Strategy Application Administration			
Reference Architecture	Strategy Cloud Environment Architecture	RA	I
Upgrades	Platform Upgrades via parallel environments	R	ACI
Description	Over the top Updates - no parallel environment required	R	ACI
Post Upgrade QA (Availability of the Services)	Testing and Validation of Services health/availability	RA	CI
Post Upgrade Regression Testing	Customer Regression and functional tests/certifications	I	RA
Customer Data	Customer Data		RA
Strategy Project Development	Content building and delivery		RA
Strategy Project and I-Server Configuration	Project and I-Server specific settings		RA
Customizations	Custom workflows, plugins/SDK Customizations, Strategy Webapps Customizations	CI	RA
Strategy Application User Permissions	Customer controls who has access to what reports		RA
Authentication set up	SSO Authentication Methods	R	ACI
Metadata Modelling	Building rules		RA
Platform Analytics	Initial configuration only + Monitoring of availability of the services	RA	
SMTP Server for Distribution Services	Your MCG's DS sent via your own SMTP server	CI	RA
File Subscriptions	Customer configures to send content to files on disk (S3)	RA	CI
Plugins		N/A	N/A
Pre-Prods/POC			
Project Management	Aligning internal resources to complete activities. Highlighting areas of customer responsibility (SE led)	RA	CI
Build Environment (Vanilla)	Based on the platform and region of choice	RA	CI

Strategy MD Restore	Restore MD and other artifacts	RA	CI
Environment Configuration	I-Server Settings, URL customization, Authentication setup, Webapps Deploy, Custom ODBC Drivers	RA	CI
Customizations	Custom workflows, plugins/SDK Customizations, Strategy Webapps Customizations	N/A	N/A
Testing	Testing to ensure success criteria is met (SE led with customer)	CI	RA
Migrations			
Project Management	Aligning internal resources to complete activities. Highlighting areas of customer responsibility	R	ACI
Application Upgrade	Upgrade of MD and other artifacts to the latest version	RA	CI
Strategy MD Restore/Refresh	Restore/Refresh MD and other artifacts	RA	CI
Environment Configuration	I-Server Settings, URL customization, Authentication setup, Webapps Deploy, Custom ODBC Drivers	RA	CI
Networking Connections	On-Premise Connectivity for internal access	RAC	ACI
Customizations	Custom workflows, plugins/SDK Customizations, Strategy Webapps Customizations	N/A	N/A
Post Upgrade QA (Availability of the Services)	Testing and Validation of Services health/availability	RA	CI
Post Upgrade Regression Testing	Customer Regression and functional tests/certifications	CI	RA

Terms Applicable to Processing Personal Data

This Section will apply only to the extent there is no other executed agreement in place regarding the same subject between Strategy and the customer (“Customer”), including any order(s) and/or a master agreement between the customer and Strategy (collectively, the “Governing Agreement”), and shall be considered a Data Processing Addendum (DPA). Except as amended by this DPA, the Governing Agreement will remain in full force and effect.

Definitions

“Applicable Data Protection Laws” shall include and means all applicable laws and regulations where these apply to Strategy, its group, and third parties who may be utilized in respect of the performance of the MCG Service relating to the processing of personal data and privacy, including, without limitation, the California Consumer Protection Act (Cal. Civ. Code §§ 1798.100 et. seq.), including as modified by the California Privacy Rights Act, together with any applicable implementing regulations (CCPA). The terms “Business”,

“Service Provider,” “Supervisory Authority,” “process,” “processing,” and “personal data” shall be construed in accordance with their meanings as defined under Applicable Data Protection Law.

“Customer Group” shall include and mean Customer and any affiliate, subsidiary, subsidiary undertaking, and holding company of Customer (acting as a Controller) accessing or using the MCG Service on Customer’s behalf or through Customer’s systems or who is permitted to use the MCG Service pursuant to the Governing Agreement between Customer and Strategy, but who has not signed its own Order Form with Strategy.

“MCG Service” means the Strategy Cloud for Government service, the platform-as-a-service offering that we manage as a unique FedRAMP certified offering that includes access to, collectively: (a) the “Cloud Platform” version of our Products (an optimized version of the Strategy software platform built specifically for deployment in an Amazon Web Services GovCloud environment licensed by the Customer; and (b) the Additional SaaS Components (as defined in the Strategy Software License and Service Agreement) Customer has purchased for use with such Products.

“**Personal Data**” means any information Strategy processes on behalf of Customer to provide the Services that is defined as “personal data” or “personal information” under any Privacy Law.
“**Security Incident**” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Personal Data. For the avoidance of doubt, an unsuccessful attempt that does not result in the unauthorized access to Personal Data or to any of Strategy’s or Strategy’s sub-processor’s equipment or facilities storing Personal Data including, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents shall not be considered a Security Incident.
“External Service Provider” shall include and mean any third party appointed by Strategy to process personal data.

Data Processing

As a Processor, Strategy will process the personal data that is uploaded or transferred to the MCG Service as instructed by Customer or provided by Customer as Controller (collectively, “Personal Data”) in accordance with Customer’s documented instructions. Customer authorizes Strategy, on its own behalf and on behalf of the other members of its Customer Group, to process Personal Data during the term of this DPA as a Processor for the purpose set out in the table below.

Personal Data in relation to MCG Service

Subject matter of processing	Storage of data, including without limitation personal data, provided by Customer for its business purpose
Duration of processing	MCG Service Term
Nature of processing	Storage, back-up, recovery, and processing of Personal Data in connection with the MCG Service. All data is encrypted at rest.

Purpose of processing	Provision of the MCG Service
Type of personal data	The Personal Data uploaded or transferred for processing through the MCG Service by the Customer
Categories of data subject	Employees or agents of the Customer and Customer's customers, prospects, business partners and vendors, and those individuals who have been authorized to use the MCG Service by the Customer

In processing Personal Data under the Agreement, Strategy will:

1. only process Personal Data on documented instructions from Customer which the Parties agree that this DPA is Customer's complete and final documented instruction to Strategy in relation to Personal Data (which the parties agree are reflected in full in this DPA), for the limited and specific purpose described in Annex 1, and at all times in compliance with Privacy Laws, unless required to process such Personal Data by applicable law to which Strategy is subject; in such a case, Strategy shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
2. notify Customer without undue delay if it: (i) makes a determination that it can no longer meet its obligations under Applicable Data Protection Laws or (ii) believes that the instruction of Customer infringes Applicable Data Protection Laws;
3. to the extent required by Applicable Data Protection Laws, and upon reasonable written notice that Customer reasonably believes Strategy is using Personal Data in violation of such laws or this DPA, grant Customer the right to take reasonable and appropriate steps to help ensure that Strategy uses the Personal Data in a manner consistent with Customer's obligations under Applicable Data Protection Laws, and stop and remediate any unauthorized use of the Personal Data; and
4. require that each employee or other person processing Personal Data is subject to an appropriate duty of confidentiality with respect to such Personal Data.

To the extent required by Applicable Data Protection Laws, Strategy will not:

1. sell the Personal Data or sharing the Personal Data for cross-context behavioral advertising purposes;
2. retain, use, or disclose the Personal Data outside of the direct business relationship between Strategy and Customer and for any purpose other than for the specific purpose of performing the Services; and
3. combine the Personal Data received from, or on behalf of, Customer with any Personal Data that may be collected from Strategy's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Applicable Data Protection Laws.

Confidentiality

Strategy will not disclose Customer Data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a government or law enforcement agency (such as a subpoena or court order). If a government or law enforcement agency sends Strategy a demand for Customer Data, Strategy will attempt to redirect the government or law enforcement agency to request that data directly from the Customer. As part of this effort, Strategy may provide Customer's basic contact information

to the government or law enforcement agency. If compelled to disclose Customer Data to a government or law enforcement agency, then Strategy will give the Customer reasonable notice of the demand to allow the Customer to seek a protective order or other appropriate remedy, unless Strategy is legally prohibited from doing so. Strategy restricts its personnel from processing Customer Data without authorization by Strategy, and imposes appropriate contractual obligations upon its personnel, including, as appropriate, relevant obligations regarding confidentiality, data protection, and data security.

Third-Party Processing

The customer gives Strategy permission to use its affiliate companies to deliver the MCG Service. Additionally, the customer consents to Strategy utilizing External Service Providers to meet its commitments under this DPA or to perform services on its behalf. The Strategy website at https://community.Strategy.com/s/article/MCG-External-Service-Providers provides a current list of External Service Providers hired for specific processing tasks for customers. Should Strategy employ an External Service Provider for the MCG Service, it will limit their access to Customer Data strictly for delivering the MCG Service, forbid any other use of Customer Data, bind them with a written contract, and enforce data processing obligations that mirror those placed on Strategy by this DPA.

Security of Data Processing

Strategy shall, taking into account the state-of-the-art, the costs of implementation and the nature, scope, context and purpose of the processing, implement appropriate technical and organizational measures designed to provide a level of security appropriate to the risk.
Strategy will ensure such technical and organizational measures provide the same level of privacy protection to any Customer Personal Data as provided, and required, under Applicable Data Protection Law, including the CCPA, to the extent applicable.
Customer may also elect to implement appropriate technical and organizational measures regarding Customer Personal Data, directly from Strategy's External Service Providers. Such appropriate technical and organizational measures include:

1. Pseudonymization and encryption to ensure an appropriate level of security;
2. Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services provided by Customer to third parties;
3. Measures to allow Customer to backup and archive appropriately to restore availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and
4. Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

Security Breach Notification

To the extent required by Applicable Data Protection Laws, Strategy shall without undue delay notify Customer of any Security Incident, with further information about the Security Incident provided in phases as more details become available. For the avoidance of doubt, Strategy's obligation to report or respond to a Security Incident, including without limitation, under this Section 6.6 is not and will not be construed as an acknowledgement by Strategy of any fault or liability of Strategy with respect to the Security Incident.

Assessments

Strategy will allow for and contribute to risk-based assessments (including questionnaires), conducted by Customer or other auditors mandated by Customer, provided that they give Strategy at least 30 days' reasonable prior written notice of such request. Any information disclosed during such assessments and the results of and/or outputs from such assessments will be kept confidential by the Customer. Such assessments shall be performed not more than twice every 12 months.

Return or Deletion of Customer Data

Due to the nature of the MCG Service, Strategy's External Service Providers provide Customer with controls that Customer may use to retrieve Customer Personal Data in the format in which it was stored as part of the MCG Service or delete Customer Personal Data. Up to the termination of the Governing Agreement between Customer and Strategy, Customer will continue to have the ability to retrieve or delete Customer Personal Data. For 90 days following that date, Customer may retrieve or delete any remaining Customer Personal Data from the MCG Service, subject to the terms and conditions set out in the Governing Agreement, unless (i) it is prohibited by law or the order of a governmental or regulatory body, (ii) it could subject Strategy or its Sub-Processors to liability, or (iii) Customer has not paid all amounts due under the Governing Agreement. No later than the end of this 90-day period, Customer will close all Strategy accounts. Strategy will delete Customer Data when requested by Customer through the MCG Service controls provided for this purpose.

Strategy

1850 Towers Crescent Plaza | Tysons Corner, VA 22182 |
strategysoftware.com