# TABLE OF CONTENTS

MicroStrategy Cloud Platform Overview..................................................................................5  
Overview of Operations ........................................................................................................5  
What is MicroStrategy Cloud Platform?..................................................................................5  
Primary Configuration Options ..............................................................................................6  
Cloud Service Responsibilities ...............................................................................................8  
Microstrategy Cloud Business Intelligence Services...............................................................9  
MicroStrategy Business Intelligence Platform Features .........................................................9  
Supported MicroStrategy Cloud Versions .............................................................................11  
Data Integration .....................................................................................................................13  
MicroStrategy Cloud And Customer Responsibility .............................................................13  
Tools Partner ..........................................................................................................................13  
Service Options ....................................................................................................................14  
MicroStrategy Cloud Data Warehouse Services..................................................................16  
Service Options ....................................................................................................................16  
Warehouse Connectivity .......................................................................................................17  
MicroStrategy Cloud And Customer Responsibility .............................................................18  
Performance and Configuration.............................................................................................19  
Services ................................................................................................................................19  
Data Warehouse Management and Access ............................................................................19  
Data Management and Loading .............................................................................................20  
MicroStrategy Cloud Infrastructure as a Service ..................................................................20  
MicroStrategy Cloud Initial Environment Setup ....................................................................21  
Cloud Platform Security Overview .......................................................................................22
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Management</td>
<td>22</td>
</tr>
<tr>
<td>MicroStrategy Control Environment</td>
<td>22</td>
</tr>
<tr>
<td>MicroStrategy Certifications and Accreditations</td>
<td>22</td>
</tr>
<tr>
<td>Security Policies</td>
<td>23</td>
</tr>
<tr>
<td>Shared Security Responsibility</td>
<td>30</td>
</tr>
<tr>
<td>Certain User Obligations</td>
<td>31</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>33</td>
</tr>
<tr>
<td>Network Security</td>
<td>33</td>
</tr>
<tr>
<td>Physical Security</td>
<td>34</td>
</tr>
<tr>
<td>Data Retention &amp; Destruction Policy</td>
<td>35</td>
</tr>
<tr>
<td>MicroStrategy Employment Practices</td>
<td>36</td>
</tr>
<tr>
<td>Data Breach Policy</td>
<td>37</td>
</tr>
<tr>
<td>MicroStrategy Cloud Platform Service Level</td>
<td>39</td>
</tr>
<tr>
<td>MicroStrategy Upgrade Policy and Process</td>
<td>40</td>
</tr>
<tr>
<td>Maintenance Planning</td>
<td>41</td>
</tr>
<tr>
<td>Cloud Support</td>
<td>42</td>
</tr>
<tr>
<td>Business and Support Operations</td>
<td>42</td>
</tr>
<tr>
<td>Support Liaisons</td>
<td>43</td>
</tr>
<tr>
<td>Contact Support</td>
<td>43</td>
</tr>
<tr>
<td>Logging a Cloud Support Case</td>
<td>43</td>
</tr>
<tr>
<td>Types of Cloud Support Cases</td>
<td>43</td>
</tr>
<tr>
<td>Providing Data to MicroStrategy Cloud Support</td>
<td>45</td>
</tr>
<tr>
<td>Domain URL Definition</td>
<td>46</td>
</tr>
<tr>
<td>Accessing the MicroStrategy Cloud</td>
<td>46</td>
</tr>
<tr>
<td>Developer Access</td>
<td>46</td>
</tr>
</tbody>
</table>
MICROSTRATEGY CLOUD PLATFORM OVERVIEW

OVERVIEW OF OPERATIONS

MicroStrategy is a global provider of enterprise software platforms for business intelligence (BI), mobile intelligence, and social intelligence applications. MicroStrategy provides integrated reporting, analysis, and monitoring software that enables companies to analyze the data stored across their enterprise or in the Cloud to make better business decisions. MicroStrategy Cloud is a division of MicroStrategy responsible for delivering MicroStrategy cloud based services. MicroStrategy Cloud offers both a Platform as a Service (PAAS) known as MicroStrategy Cloud Platform, and Software as a Service (SAAS) models known as MicroStrategy Cloud Personal and MicroStrategy Cloud Express and a small scale Infrastructure offering to support business intelligence applications in the cloud.

WHAT IS MICROSTRATEGY CLOUD PLATFORM?

MicroStrategy Cloud Platform delivers a complete business analytics platform-as-a-service, including business intelligence, data integration and data warehouse capabilities. MicroStrategy Cloud Platform is a public cloud service that offers the following services:

- MicroStrategy’s business intelligence platform for both mobile and web;
- Data hosting capabilities on a variety of database management systems. Data hosting is used primarily for the purposes of building a data warehouse or data marts, but can be extended to include a variety of other database needs.
- Data integration services which allows for extraction, transformation and loading data into data sources in the MicroStrategy Cloud environment
- Infrastructure Services to allow customers to install, manage, and run business intelligence related applications not natively hosted within the MicroStrategy Cloud Platform.
MicroStrategy Cloud Services are designed to transform and simplify the manner in which analytics solutions are built and delivered within an organization. They are designed to provide customers an environment to host, transform, analyze, and report data through the MicroStrategy Business Intelligence framework and cloud hosting services. The services offering provides a menu of data warehouse, data integration, and reporting capabilities. As subscribers to the MicroStrategy Cloud Platform customers are required to use the Business Intelligence Services, but the other Platform Services are available as options.

The MicroStrategy Cloud is centered on the MicroStrategy Business Intelligence Services. It provides customers’ access to the MicroStrategy Business Intelligence products as a hosted cloud service. Customers can select from a list of product options which are hosted on a shared infrastructure.

MicroStrategy Cloud Data Warehouse Services (MCDW) provides access to relational database capabilities. A tiered set of services are available from small transactional databases to complex enterprise data warehousing environments.

The MicroStrategy Cloud Data Integration Service (MCDIS) is designed to move data into the MicroStrategy Cloud Data Warehouse environment. The service provides capabilities that support data acquisition from varied multiple data sources including; data extraction, validation, transformation and loading.

**PRIMARY CONFIGURATION OPTIONS**

There are two primary configuration options with MicroStrategy Cloud. The first is a BI-only, “Direct Connect” service. In this case, the primary data warehouse or data mart(s) reside on-premise (or in another public or private cloud). The MicroStrategy Cloud BI layer operates directly against the on-premise database(s). Data integration capabilities in this scenario are also maintained by the customer alongside the data warehouse. Such a configuration is ideally suited to companies that have established data warehouse solutions or made recent investments in database or data integration platforms.
The second is a BI with data services configuration. With this setup, the primary data warehouse and data integration software, resides within the MicroStrategy Cloud along with the BI server itself. This configuration has the added benefit of having components of the analytics platform in a single infrastructure. The MicroStrategy Cloud service level agreement will correspondingly apply to this entire stack.

While these are the two primary configurations, customers often have specific requirements which do not conform precisely to either setup. These configurations are not exclusive with MicroStrategy multi-source a standard component of the MicroStrategy Cloud BI Service. This enables connecting Direct Connect and Cloud Warehouse Services to the same customer environment.
CLOUD SERVICE RESPONSIBILITIES

The MicroStrategy Cloud Platform Services are designed to make it quicker, easier, and more cost effective for our customers to implement business intelligence solutions. With MicroStrategy Cloud Platform Services, business users are able to take advantage of the MicroStrategy Business Intelligence Services to analyze their data, IT Professionals are able to focus on building out valuable business intelligence solutions, and the MicroStrategy Cloud Team is focused on managing, monitoring, optimizing, and running the MicroStrategy Cloud Platform Services.

To support our offering, MicroStrategy has deployed a dedicated organization focused on supporting the MicroStrategy Cloud environment. This organization is responsible for managing environment setup, configuration, monitoring, as well as additional responsibilities designed to provide high availability and performance of the environment. MicroStrategy is responsible for managing the physical implementation of the MicroStrategy Cloud Platform infrastructure and restricts customer access to the server instances running the MicroStrategy Cloud, outside of the Infrastructure as a Service offering. As part of Cloud Platform services, MicroStrategy manages patching the environments at the server and application level, excluding IaaS customer installed applications.

Customers are responsible for the configuration, development, change management, administration, and support of the business intelligence application, data warehouse, and data integration transformations. In addition, application performance tuning and optimizations are the responsibility of the customer. If desired, MicroStrategy Professional Services can be contracted to provide or assist with system tuning. Data loading, data quality, and cleansing also are responsibilities of the customers. MicroStrategy offers various Data Integration service options that can be leveraged to load and validate data in the customer environment.
MICROSTRATEGY CLOUD BUSINESS INTELLIGENCE SERVICES

MICROSTRATEGY BUSINESS INTELLIGENCE PLATFORM FEATURES

At the core of the MicroStrategy Cloud is the MicroStrategy Business Intelligence Services. The Business Intelligence Services provide customers’ access to the MicroStrategy Business Intelligence product catalog hosted as a cloud service. Customers can select from a list of product options which are hosted on a shared infrastructure. Customer environments are configured in a single-tenant virtualized environment pre-configured and optimized for use at start-up. As a result of pre-configuring the various products, customers can take advantage of the MicroStrategy capabilities immediately when starting with the MicroStrategy Cloud Business Intelligence Service, with additional capabilities enabled at the customer request. Additional configuration post setup may be required after your Cloud environment is released (e.g. VPN, metadata restores, data warehouse backups).

MicroStrategy has engineered its platform to help deliver an integrated architecture that scales to support enterprise level business intelligence. This enterprise scale integrated architecture is well suited for the Cloud, and the MicroStrategy Cloud ™ service offering takes advantage of the platform to build, scale, and manage the Cloud service. Management services like clustering, security, user management, and resource management help provide a highly available environment that can scale up or out to meet the most demanding business intelligence requirements.

MicroStrategy platform features that are part of the standard cloud offering, as well as optional choices and a Professional Services offering, are shown in the table below:

MICROSTRATEGY CAPABILITIES FOR CLOUD SERVICES

<table>
<thead>
<tr>
<th>Cloud User Types</th>
<th>Mobile User</th>
<th>End User</th>
<th>Desktop Designer</th>
<th>Architect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligence Server w/Clustering</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Distribution Services</td>
<td>*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Multi-Source</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OLAP Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Report Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>I-Server Universal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web Reporter</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web Universal</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mobile</td>
<td>✓</td>
<td>O</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Office</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Transaction Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web Analyst</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web Professional</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Desktop Designer**</td>
<td>☒</td>
<td>☒</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Architect</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>✓</td>
</tr>
<tr>
<td>MicroStrategy SDK - look and feel or security customization</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>✓</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>MicroStrategy SDK - other customizations</td>
<td>☒</td>
<td>☒</td>
<td>☒</td>
<td>O</td>
</tr>
</tbody>
</table>

*Mobile-Only licenses may receive Mobile-only push subscriptions only.

** MicroStrategy Desktop is a development only tool in the MicroStrategy Cloud used by architects and report developers to deliver reports via web, mobile, office, or distribution services. The tool is hosted via a webVPN in a virtual desktop.
SUPPORTED MICROSTRATEGY CLOUD VERSIONS

MicroStrategy Cloud keeps customers on current stable versions of the MicroStrategy platform. Currently supported versions of MicroStrategy in the cloud include:

- MicroStrategy 9.2.1m
- MicroStrategy 9.3.x
- MicroStrategy 9.4.x

MicroStrategy builds new Cloud environments with the most recently released MicroStrategy version.

Business Intelligence Services and Customer Responsibility

Cloud Business Intelligence customers are responsible for developing their own custom business intelligence and mobile applications using the Business Intelligence Services. This development can be performed through customer’s internal development resources, third party consulting services, or MicroStrategy Professional Services. While customers are able to focus on developing solutions that provide business value, the MicroStrategy Cloud service provides the monitoring, management, and optimization of the Business Intelligence environment. Customers are able to configure various components of their cloud environment or work with the MicroStrategy Cloud team to set configuration values.

MicroStrategy Professional Services consultants are granted Cloud user accounts at a privilege level decided upon by the customer without counting against the customer’s number of purchased MicroStrategy licenses.

The table below breaks down major categories of services and activities related to management of a MicroStrategy Cloud Platform environment. Premium services are available for an additional charge. Optional managed services are delivered by MicroStrategy’s Professional Services organization and are not part of the standard MicroStrategy Cloud Platform offering. As customers are responsible for the application design and implementation, the MicroStrategy Cloud team cannot guarantee performance of the finished applications. Services may be engaged to make recommendations on application design, database design, or other performance design optimizations. The MicroStrategy Cloud team will ensure that the infrastructure is optimized.

<table>
<thead>
<tr>
<th>Service</th>
<th>Customer Responsibility</th>
<th>Cloud Platform Team*</th>
<th>Optional - Managed Services**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managing MicroStrategy Groups and Users</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Controlling access to application functionality</td>
<td>□</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Controlling access to data</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring user access</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintaining report schedules and subscriptions</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced application performance tuning - reports, caches, cubes, etc.</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Testing and Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up front customized Cloud performance assessment</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring system usage</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyzing system usage and application performance</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MicroStrategy Architect Metadata Development</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>Creating logical business model / metadata</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>objects</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MicroStrategy Report and Dashboard Development</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating reports</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Designing dashboards</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Defining metrics</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Defining filters</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Creating templates</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change Management and Change Control</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing MicroStrategy objects</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>MicroStrategy Project and Object Migration</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

* The Cloud Platform Team consists of Cloud Support and Cloud Platform BI, Database, Network, and Operations engineers.

**Managed Services are an optional service in which MicroStrategy Professional Services are engaged to assist with MicroStrategy development.
DATA INTEGRATION

The MicroStrategy Cloud Data Integration Service (MCDIS) is an optional service that enables customers to move data into the MicroStrategy Cloud Data Warehouse environment. The service provides a wide array of options to support data acquisition from varied data sources, data movement, data transformation, and data loading. The service is configured to work with MicroStrategy Cloud Data Warehouse Service (MCDWS), with the Data Integration service tied to only loading data into the MicroStrategy Cloud Data Warehouse Services.

The service options can be selected based on the features required to extract, transform, validate, and load data. Options can be included depending on the type of connectivity between you and the MCDWS environment. The MicroStrategy Cloud team will assist in reviewing the options to help determine the tiers of service that would be required to support customer needs. Please consult with your Account Executive for available 3rd-party Data Integration products and tiers.

Customers that opt to maintain their data integration solutions on-premises can use these solutions alongside MicroStrategy Cloud, as long as proper connectivity between the customer network and MicroStrategy can be established.

MICROSTRATEGY CLOUD AND CUSTOMER RESPONSIBILITY

MicroStrategy provides management, monitoring, and physical environment administrative functionality for the data integration capabilities purchased through MicroStrategy. The administration offerings include environment setup, configuration, monitoring, as well as additional services designed to maintain high availability of the data integration environment. MicroStrategy is responsible for managing the physical implementation of the Data Integration Services and restricts access to the server instances running the data integration services. As part of the warehouse services, MicroStrategy manages patching the environments at the server and database level.

MicroStrategy customers are responsible for logical administration and development of data integration transformations, tasks, and jobs in the MicroStrategy Cloud including development of ETL transformation, data profiling, data quality and validation, managing schedules, and monitoring of ETL process execution. In addition, ETL performance tuning and optimizations are the responsibility of the customer. MicroStrategy customers are also responsible for implementing security as part of the ETL process. If encryption or additional data security is required as part of the transformation process, the customer is responsible for implementing security practices as part of their design and implementation. MicroStrategy personnel will have limited access to customer environments and data with only critical administrators and support person specifically granted access by the customer. As a result, customers are responsible for all data they place in the MicroStrategy Cloud Data Warehouse service.

TOOLS PARTNER

MicroStrategy has partnered with a preferred 3rd-party data integration provider to deliver data integration tools that support both ease of use and full-featured transformations. Various performance tiers are available to suit your needs. These capabilities can be used separately or be combined to support various data integration requirements.

Some of the Data Integrations services provided in the MicroStrategy Cloud are provided directly by our 3rd-party partner. As a result, our partner will be responsible for the management, monitoring, and maintenance of the data integration metadata services. MicroStrategy will have responsibility for the cloud agent services which are maintained within the MicroStrategy Cloud customer environment.
For higher tiered performance options, the MicroStrategy Cloud Data Integration capability is hosted and managed by the MicroStrategy Cloud team. These services are managed, monitored, and maintained by the MicroStrategy Technical Operations team.

SERVICE OPTIONS

MCDIS provides multiple options to support customer requirements. The service options can be selected based on the features required to extract, transform, validate, and load data. Options can be combined depending on your type of connectivity with the MCDWS environment. The MicroStrategy Cloud Platform team can help determine the tiers of service required for your needs.

CLOUD SERVICES OPTION

The Cloud Services Option is ideal for situations when you are moving from an on-premises data source or third-party cloud data source, and the data warehouse requires simple transformations or direct replication of data structures between the source and destination databases. This solution requires that connectivity be established between the customer data source and the MicroStrategy Cloud.
DATA INTEGRATION IN MICROSTRATEGY CLOUD

Data integration in MicroStrategy Cloud uses an ETL instance to manage transformations. This instance can be dedicated to a customer or can be set up as part of a shared instance. This solution also requires that connectivity be established directly from the customer site to the MicroStrategy Cloud environment.

CLOUD AND ON-PREMISES

If it is not possible to establish a secure connection between your network and MicroStrategy, it may be possible to move data to files and then load data from those files into the MicroStrategy Data Warehouse. In this case, the data integration agent is installed at your site. The agent can be used to pull data from your data sources and push the results via secure FTP to a secure data store in the MicroStrategy Cloud. From that location, your chosen data integration tool can be used to load data into your data warehouse instances.
MICROSTRATEGY CLOUD DATA WAREHOUSE SERVICES

SERVICE OPTIONS

MicroStrategy Cloud Data Warehouse Services provides a tiered set of relational database capabilities designed for data warehousing and configured to support customer data analysis requirements. The MicroStrategy Cloud team offers the tiers of service required by a customer based on a number of factors. These factors include database size, database growth projections, performance requirements, disaster recovery and SLA, security, encryption, and other dynamics. Analysis to determine the appropriate tier of service is typically performed during the analysis phase of the customer engagement. MicroStrategy will work with the customer to determine the optimal tier and database solution. The following tiers of service are available:

- **Basic Edition.** The basic edition is the most cost effective option, designed for small scale data warehouse solutions. This solution is designed to support a maximum data volume of 1 TB. This option features a low compute-to-storage ratio, a low memory-to-storage ratio, and standard disks.

- **Performance Edition.** Based on a standard data warehouse appliance offering from a leading analytical database vendor, this option delivers strong performance and scalability. This option features a medium compute-to-storage ratio, a medium memory-to-storage ratio, and fast disks.

- **Enterprise Edition.** Based on a high end appliance from a leading analytical database vendor, this option is designed to support use cases with large amounts of data, high levels of concurrency and demanding analytical challenges. This option features a high compute-to-storage ratio, a high memory-to-storage ratio, and very high performance disks.

In some instances, customers may require a customized model to support their specific needs. Please consult with your MicroStrategy Account Executive to determine the best edition to fit your needs.
Data Warehouse installations include a single node by default with the total amount of allocated storage specified in your Cloud contract. This node can be partitioned to support development, test, and production per customer requirements. Additionally, customers can purchase separate instances to support multiple cloud database environments.

MicroStrategy partners with several vendors to provide performance and platform editions of the MCDWS. These vendors provide level-3 support for MicroStrategy Cloud. Should a customer’s data warehouse need to move to another performance tier, MicroStrategy Cloud operations managers and MicroStrategy Professional Services work with the customer to plan and execute the operation.

WAREHOUSE CONNECTIVITY

MicroStrategy Cloud Business Intelligence Services can connect to databases or warehouses operating either on premises, in a third party cloud or hosted in the MicroStrategy Cloud. MicroStrategy offers high performance hosted data warehouse services. MicroStrategy also supports access to heterogeneous data sources via its MultiSource Option capability, which is included with the MicroStrategy Cloud Platform.

If you choose to maintain your database on-premises, a typical implementation involves establishing a VPN connection between the MicroStrategy Cloud and your database or data warehouse (See the section on MicroStrategy Cloud Secure Connectivity MCSC). The performance of this architecture can vary based on a variety of factors, including the physical distance between the MicroStrategy Cloud data center and the customer data source, the latency of the data connection, the bandwidth of the connection, the amount of usage and its query intensiveness, the query-response latency of the customer data source, and other variables.

MicroStrategy Cloud leverages framework capabilities that enhance performance including Intelligent Cubes, caching, and pushdown analytics. These capabilities reduce the query traffic between the MicroStrategy Cloud and data sources.
MICROSTRATEGY CLOUD AND CUSTOMER RESPONSIBILITY

MicroStrategy provides management and basic database administration functions. The administration offerings include environment setup, configuration, monitoring, as well as additional services designed to maintain the high availability of the environment. MicroStrategy is responsible for managing the physical implementation of the data warehouse environment and restricts access to the server instances running the data warehouse. As part of the warehouse services, MicroStrategy manages patching the environments at the server and database level.

MicroStrategy customers are responsible for logical administration of the data warehouse including data modeling, creation of the data structures, and application development related tasks. Application performance tuning and optimizations are the responsibility of the customer. With customers responsible for designing and developing database objects, they are also responsible for change control and change management of database objects, and handling migrations between development, test, and production environments.

As customers are responsible for the data in the MicroStrategy Data Warehouse Services, they are responsible for implementing security best practices on the data warehouse. MicroStrategy personnel will have limited access to customer data with only critical administrators and support personnel specifically granted access by the customer. As a result, customers are responsible for all data they place in the MicroStrategy Cloud Data Warehouse service.
PERFORMANCE AND CONFIGURATION

The MicroStrategy Cloud operations managers have optimized the environment to enhance the performance of the configurations provided via the MicroStrategy Cloud Platform. The MicroStrategy Performance Lab runs extensive tests on the MicroStrategy Cloud environment providing optimization recommendations. These recommendations are used to tune the overall environment and establish the recommended default setting for new environments being set up in the cloud. Because each set of customer requirements and applications is different, MicroStrategy Cloud Engagement Managers meet with customers to review their requirements prior to implementation and configuration of an environment. Based on this analysis additional optimization settings may be applied.

SERVICES

By default, customers are responsible for the design, development, change control and logical administration of the data warehouse, including data modeling, creation of data structures, and the tasks related to developing projects, reports, and documents. In addition, application performance tuning and optimizations are the responsibility of the customer. If desired, MicroStrategy Professional Services can be contracted to provide or assist with system tuning. Data loading, quality, and cleansing are responsibilities of the customer. MicroStrategy offers various Data Integration service options to load and validate data in the customer environment. Please contact your MicroStrategy Account Executive for more details.

DATA WAREHOUSE MANAGEMENT AND ACCESS

The environment is managed with a utility server provided as part of the MicroStrategy configuration infrastructure. The utility server’s tools provide access to build and manage the customer’s database instance. Access to the utility server is provided via Web VPN. Once environment configuration has been completed, details for connecting to the utility server are provided by MicroStrategy as part of your Connectivity Information sheet.

Example reference link to a Cloud Utility Box:

https://webvpn.cloud.microstrategy.com/CustomerName
DATA MANAGEMENT AND LOADING

Data can be loaded into MicroStrategy Cloud Data Warehouse Services in multiple ways. MicroStrategy provides a full suite of Data Integration Tools to load your data. For more information, see Data Integration Services, above. If you already have internal data integration tools, they can be connected to MicroStrategy Cloud Data Warehouse Services to manage data in the warehouse environment. Please speak with your Cloud Engagement manager for full details.

MICROSTRATEGY CLOUD INFRASTRUCTURE AS A SERVICE

The MicroStrategy Cloud Infrastructure as a Service (IaaS) offering is an optional support service that provides customers with infrastructure resources to support their business intelligence environment. MicroStrategy Cloud can provide storage, network, and compute infrastructure. These resources require that the MicroStrategy Cloud Business Intelligence server be purchased in conjunction.
Storage: By default, the MicroStrategy Cloud Business Intelligence Service comes with a 35 Gig block of storage that is available for customers to use. Typically this storage is utilized for images, files, video, plug-in development and other files needed to support the MicroStrategy Business Intelligence environment. Often times this dedicated storage space does not provide adequate space for files needed for data integration, data warehouse, and business intelligence development. MicroStrategy Cloud provides the option to purchase additional storage.

Compute: MicroStrategy Cloud Services offer a wide array of tools to build out enterprise scale business intelligence applications. Even with the tools available, the MicroStrategy Platform cannot offer all of the applications and services that a company may require. To enable customers to implement their own software or third party software not supported by the MicroStrategy Cloud, a Compute IaaS offering is available. With the Compute IaaS offering, customers are able to select from a pre-defined list of virtualized compute instances sized (RAM, CPU, Disk Space) to meet their application needs. In addition, they have a choice between a specified list of Windows and Linux operating systems.

Customer Access and Responsibilities: With the Compute IaaS, customers are provided admin level access to the compute nodes. This enables the installation and development of applications that can be integrated into the Business Intelligence applications. In the Compute IaaS model, MicroStrategy will provide monitoring of the compute environment and provide operating system and infrastructure level patching. MicroStrategy will automatically install patches unless the customer notifies us otherwise. In order to assist customers with maintaining their own 3rd-party software tools, MicroStrategy will send regular vulnerability reports. Customers are responsible for the maintenance and support of any software application they install on the Compute IaaS nodes as well as licensing for software they install in the MicroStrategy Cloud environment. It is the customers’ responsibility to ensure the software is secure and properly patched and licensed. MicroStrategy can at will request to review that the Compute IaaS system is in compliance. The MicroStrategy Compute IaaS offering is designed to support business intelligence applications and is not set to be a standalone service. MicroStrategy reserves the right to review applications and licensing of software running in the environment and if abuses are identified terminate customers’ use of the service.

**MICROSTRATEGY CLOUD INITIAL ENVIRONMENT SETUP**

An initial environment setup includes building a virtualized environment according to this User Guide with an initial RAM allocation as specified in the customer’s Cloud contract. The Business Intelligence environment includes a Development node and a Production node cluster, installation of selected MicroStrategy Technology and creation of metadata database. Initial setup services shall be deemed complete when MicroStrategy sends you the IP address or URL permitting access to the environment.

If applicable, initial setup also includes a hosted Data Warehouse, Data Integration Service, or Infrastructure-as-a-Service machine with configurations as specified in the customer’s Cloud contract. All necessary connections will be made upon environment delivery.

Additional input from the customer may be required after the initial environment setup is complete. Examples include establishing a Virtual Private Network, restoring existing MicroStrategy metadatas or data warehouse backups to the cloud, and establishing a customer-hosted LDAP server.
CLOUD PLATFORM SECURITY OVERVIEW

Security is a key concern. In a cloud environment, security responsibilities must be shared by the service provider and by the customer. Security topics covered in this document include:

- Information Security Management
- Control Environment
- MicroStrategy Certifications and Accreditations
- Security Policies
- Security Procedures
- Shared Security Responsibility
- Certain User Obligations
- Configuration Management
- Network Security
- Physical Security
- Data Retention & Destruction Policy
- MicroStrategy Employment Practices
- Data Breach Policy

For additional questions related to MicroStrategy Security practices in the cloud, send an email to Cloud@MicroStrategy.com.

INFORMATION SECURITY MANAGEMENT

MicroStrategy has a dedicated Compliance and Security Team consisting of the Director of Compliance and Security information security and compliance management specialists. Members of the Compliance and Security Team protect and monitor the security posture of the MicroStrategy Cloud Platform and work in concert with the Senior Executive Vice President and Chief Technology Officer (CTO) who serves as the Chief Security Officer for Cloud Operations, Vice President of Worldwide Information Systems, COM Team, Engagement Management Team, and Quality Assurance Team to ensure security controls are in place, operating effectively, and monitor compliance activities.

MICROSTRATEGY CONTROL ENVIRONMENT

MicroStrategy Cloud leverages and shares various aspects of MicroStrategy’s overall control environment in the delivery of our Cloud services. The MicroStrategy Cloud controls are based on the Cloud Security Alliance control matrix and the SOC2 security and availability trust criteria. As such, MicroStrategy is able to map its controls to the most common industry control frameworks, including COBIT, NIST, ISO27001/2, PCI, HIPAA, etc.

MICROSTRATEGY CERTIFICATIONS AND ACCREDITATIONS

MicroStrategy's US data center locations are fully SOC 1 Type II compliant and leverage state-of-the-art biometric controls, stringent controlled entry processes, and video surveillance to provide security. The international data centers are ISO certified including ISO 27001:2005. Customers may request to review relevant SOC and/or ISO Reports for our data centers.
SECURITY POLICIES

MicroStrategy maintains Cloud Platform Security and Availability Policies and related processes that govern the MicroStrategy Cloud Platform engineering and operations activities. These policies and procedures are in place and reviewed and updated as needed annually. The policies address:

- Access control
- Awareness and training
- Audit and accountability
- Configuration management
- Contingency planning
- Incident response
- Maintenance
- Media protection
- Physical and environmental protection
- Personnel security
- Risk assessment
- System and communication protection
- System and information integrity
- Availability

Access Management

Access to any and all MicroStrategy Cloud Platform resources is tightly controlled and users are only granted access to facilities, hardware, and software based on the minimum level of access required to perform their role. Access to the Cloud Platform is controlled through role-based access management in a centralized authentication directory. All access is based on documented approvals by appropriate Cloud Platform team management. The ability to create, modify, or delete accounts within the Cloud Platform is limited to authorized personnel, and all access is periodically reviewed by the Compliance and Security Team to verify whether individuals' access is still required and to identify any unnecessary user accounts. Human Resources (HR) notifies the Cloud Team of any terminations and transfers and the associated MicroStrategy Cloud Platform accounts are disabled within one business day. In the event of involuntary terminations, accounts are deactivated immediately upon notification. Access to the datacenters, privileged user accounts, and remote access privileges are reviewed quarterly and any accounts that are inactive for 90 days are automatically identified and access is disabled.

Network Segmentation and Access Management

Network access is controlled based on an implicit “deny all” network access control strategy. Network access controls have been implemented at all layers of the MicroStrategy Cloud Platform to only allow required network traffic and deny all other network traffic. Perimeter firewall appliances control all ingress and egress network traffic to/from the Internet at each datacenter, VPN appliances control access to the Cloud Platform systems and internal resources, hypervisor-based network security enforces VLAN-based access controls between all client and management VLANS, and centrally managed host-based firewalls control network traffic on each server. MicroStrategy clients are only permitted to access their assigned Cloud Platform environment and all other access is denied.
Change Management

MicroStrategy’s change management program controls all changes to the Cloud Platform. Change management policies and procedures require changes to be requested via a documented Change Request (CR) ticket, which must be reviewed by subject matter experts, approved by appropriate management, and tested prior to implementation. Proposed changes that may have a significant security, performance, or availability impact must be reviewed and approved by the Change Control Board (CCB) prior to implementation, which consists of members of the COM, engineering, database, network, quality assurance, technical support, and engagement management teams.

System Auditing and Logging

The MicroStrategy Cloud Platform technical configuration and supporting security and platform operational capabilities and procedures provide the required tools and processes to capture and monitor system activity throughout the entire Cloud Platform. Key platform components have had auditing and logging facilities enabled and configured to capture system events, generate log files, and send log files to the centralized SIEM software for correlation, analysis, and alerting. The Security Team uses a variety of security tools to identify and detect potential security threats and incidents, including but not limited to, firewall logs, VPN appliance logs, IDS alerts, malware and host-based firewall alerts, vulnerability assessments, and operating system event log files. These alerts and notifications are analyzed by the SIEM, and security engineers monitor the alerts and respond as necessary 24 hours a day 7 days a week.

Problem Detection and Incident Management

MicroStrategy has formal problem detection and response capabilities and procedures in place to monitor the Cloud Platform infrastructure and applications, identify potential issues, and respond appropriately. A suite of centralized monitoring tools are in place to proactively monitor the health and performance for the Cloud Platform, both internally and externally using Simple Network Management Protocol (SNMP), customized system and application checks, and vendor provided monitoring tools. Alerts from monitoring tools automatically send emails to the respective Cloud Platform team mailboxes, which are monitored by operations teams 24x7. Procedures are also in place to allow customers to report problems themselves, by opening a technical support case, or by calling the MicroStrategy Technical Support Team. Problems detected by internal monitoring tools or by MicroStrategy staff are analyzed to determine if further analysis and/or action is required. When required, Help Desk Tickets are opened for further analysis and remediation. Customer reported problems that cannot be resolved by Technical Support are escalated to the COM Team. The COM Team will analyze problems, take appropriate action, and close all corresponding tickets in the HelpDesk ticketing system when the problem has been resolved.

Potential security incidents detected within or affecting the MicroStrategy Cloud Platform are reported to the MicroStrategy Security Incident Response Team (SIRT), who will activate and follow the MicroStrategy Incident Response Plan which includes detailed security incident handling procedures for analysis, containment, eradication, and recovery.

System Backup and Recovery
MicroStrategy uses disk to disk data replication and backup techniques to backup both systems and data on a daily basis. Access to the data backup systems and management software is limited to authorized users. MicroStrategy performs backup restoration testing on a quarterly basis.

**Information and Communication**

The Information and Communication activities of an organization provide a method of the foundations of the Control Environment to be captured and administered to employees. With effective information and communication channels an organization enables its people to understand and exchange methods for internal control.

MicroStrategy Cloud Platform employees and contractors are required to complete Cloud Platform security awareness training upon hire, and complete a refresher annually thereafter. Security Awareness training addresses relevant security threats and risks and notifies employees of their responsibility to communicate security concerns. Ethics and security hotlines are also in place for employees to notify management of inappropriate behavior and suspected incidents.

The MicroStrategy Cloud Platform Security and Availability Policies and associated procedures have been published and communicated to all employees and contractors that support the Cloud Platform. Mandatory Cloud Platform training is also required of all Cloud Platform team members, which provides detailed training on the security and availability processes as well as the key processes and procedures required to maintain a secure and resilient environment.

Employees with elevated security responsibilities for the Cloud Platform are required to complete specialized security training pertaining to their roles. Additionally, the Compliance and Security Team distributes a monthly newsletter to all MicroStrategy employees and contractors with information on maintaining and continually improving the security of MicroStrategy technology assets. Cloud Platform Policies and procedures are maintained, updated, and communicated to employees on a periodic basis. Current versions of policies and procedures are available to employees on the MicroStrategy intranet.

**Risk Assessment**

MicroStrategy regularly reviews risks that may impact the MicroStrategy Cloud Platform and threaten the achievement of the criteria for the security and availability Trust Services Principles. MicroStrategy has a formal IT Risk Management Program for assessing and identifying risk, risk analysis and tracking, and monitoring risks and remediation activities for the Cloud Platform. Risks are identified through annual IT Risk assessments, recurring vulnerability assessments, annual penetration testing, compliance assessments, and monthly IT risk management meetings Cloud Platform senior management. As risks are identified, the impact, likelihood, and mitigating controls are analyzed to determine the residual risk and documented in a risk register. Risk remediation activities, technical, operational, and strategic are documented and status is monitored by the Compliance and Security Team. Tactical risk remediation issues are tracked through resolution using the MicroStrategy Cloud Platform Plan of Action and Milestones (POA&M) system.

**Monitoring**

MicroStrategy’s COM and Compliance and Security Teams perform monitoring across the Cloud Platform to ensure controls are implemented within the Cloud Platform and remain effective. This monitoring allows MicroStrategy to react to changing conditions and assess if controls continue to operate as designed and appropriately.
addition to the Risk Management Program and risk assessment and monitoring activities described in the previous section MicroStrategy conducts weekly vulnerability scanning, bi-annual technical baseline configuration validation testing, quarterly user access reviews, real-time SIEM and SourceFire IDS alert monitoring, and security patch implementation verification.

The Compliance Team, in concert with the Cloud Platform senior management, have implemented a suite of monitoring activities, such as spot checks and periodic reviews, to ensure control activities are performed effectively over time. Policy and procedure compliance failures identified through monitoring activities are captured in the POA&M process and individuals are assigned responsibility for remediation. The Compliance Team monitors remediation status.

**System and Data Back-up**

MicroStrategy Cloud backup policies and procedures are designed to reduce downtime to the customer should an unforeseen incident occur that impacts the quality or availability of the customer’s data. These backup procedures are designed as part of an overall effort to provide high levels of availability to MicroStrategy Cloud customers.

The MicroStrategy Cloud team will back up the following customer components on a nightly basis:

- MicroStrategy environment including metadata
- Customer access control lists
- Virtual environment parameters and settings
- Applicable audit logs

Backup copies will be maintained in multiple secure sites to provide business continuity should a major incident occur. The MicroStrategy backups should not be construed as a substitute for customer backups of critical data. Metadata backup copies will be maintained for a period of 30 days.

**Physical Access Management**

The MicroStrategy Cloud Platform is physically located in two co-location facilities owned and operated by Equinix Inc. (Equinix) in Ashburn, VA and Seattle, WA. Access to MicroStrategy cages containing MicroStrategy Cloud Platform equipment within each Equinix data center is managed by MicroStrategy. To meet the security and availability principles, MicroStrategy validates Equinix has implemented effective physical security and environmental protection controls via annual SOC 1 Type II report reviews.

**Logical Access Management**

Logical access to the MicroStrategy Cloud Platform is controlled using a combination of a centralized identity and access management system and multiple layers of network access controls. All external network access to the Cloud Platform is controlled through stateful inspection firewalls and VPN appliances that are configured with default deny all access control policy.

Within the Cloud Platform the network has been segmented into VLANs based on the purpose and access requirements. SDN network routing, NAT, and access controls working in concert with host-based firewalls on all virtual servers control all network access between VLANs based on a default deny all policy.
A centralized directory-based identity and access management platform is in place to control user access across the entire platform. Upon request, customers may also use their own LDAP server to authenticate their respective users on their assigned BI systems.

All remote administrative access to the Cloud Platform requires two-factor authentication using RSA SecurID tokens coupled with role-based access management. User accounts and assigned privileges are required on a quarterly basis to ensure only the minimum number of individuals have access to the Cloud Platform and user are only assigned the necessary privileges required to complete their assigned responsibilities.

Customer user accounts are only granted access to their assigned customer environments and customers are responsible for managing their own customer accounts through the Self-Service Portal.

SECURITY PROCEDURES

MicroStrategy has implemented detailed operational procedures to enforce MicroStrategy Cloud Platform Security and Availability Policies. Procedures are reviewed at least annually by senior management and updated as required. Procedures address the following topics:

Access Control

MicroStrategy’s access control policies are enforced through procedures that define how access is requested, approved, and managed for the MicroStrategy Cloud Platform. User account management procedures govern creating new user accounts (new hires, privileged accounts, vendor accounts, and customer accounts), managing changes in access, managing employee transfers, and termination of all user accounts. Access management and enforcement procedures govern ongoing management of Cloud Platform access, including: establishing roles, reviewing account access, account termination and changes, administrative and privileged account management, and disabling accounts.

Segregation of duties policies and procedures prevent the assignment of conflicting roles and privileges within the Cloud Platform. Access control procedures require unsuccessful login attempt requirements to automatically lock user accounts after five (5) unsuccessful consecutive logon attempts and remain locked for at least 30 minutes. Session locks and termination procedures for terminating inactive sessions and enabling locking screensavers when systems are idle. Remote access procedures are in place for users, customers, and privileged users to securely connect to the MicroStrategy Cloud Platform using encrypted Virtual Private Networks (VPN).

Physical Access Control procedures include detailed procedures for managing physical access to the Equinix datacenter facilities and cages containing Cloud Platform equipment. These procedures include managing permanent access, temporary access, and associated procedures for requesting and authorizing physical access, changes to user access, inactive accounts and termination, and physical access reviews.

Change Management

MicroStrategy maintains separate testing and production Cloud Platform environments. All changes to the production Cloud Platform infrastructure must be initiated through a Change Request (CR) ticket in the Change Request ticketing system. All CRs require detailed justification, potential impact analysis, deployment procedures, and back-out procedures which require review and approval prior to testing. Only after following successful testing, CRs will be approved for implementation in production. Proposed changes that have a significant security,
performance, or availability impact must be reviewed and approved by the Change Control Board (CCB) prior to implementation in production environments. All changes are required to pass Quality Engineering (QE) testing and certification once applied in the production environment. In the event an emergency change must be implemented that can’t wait for CCB approval, verbal approval is required by Cloud Platform Management, and immediately following the change a retroactive CR ticket must be submitted, reviewed, and approved by the CCB.

Incident Response

MicroStrategy Cloud Platform Incident Response procedures establish the responsibilities and processes for security incident detection, notification, analysis, containment, eradication and recovery, and post incident analysis. The procedures also included how the Incident Response Plan is tested and MicroStrategy Cloud Platform security incident intake, tracking, and custody forms.

Patch Management

Patch Management procedures establish the responsibilities and process for maintaining patch levels across the MicroStrategy Cloud Platform infrastructure. High risk patches released by vendors will be implemented or mitigated within thirty days of identification. Patches are tested prior to implementation in production per the change management procedures. Patch deployment will take place during scheduled maintenance windows.

Configuration Management

Configuration Management procedures establish the standard configuration baselines for key MicroStrategy Cloud Platform infrastructure components and the mechanisms used to maintain the configurations. Policy-based configuration management tools push standard configurations to systems and enforce configurations. In addition, the configuration of malware and host-based firewalls on all servers is centrally managed.

Problem Detection and Response

Problem Detection and Response procedures establish the responsibilities and processes for identifying potential issues within the MicroStrategy Cloud Platform infrastructure and applications, appropriate response, internal and external client communications, and problem resolution and follow-up procedures. This includes what software tools are used to monitor systems, where alerts will be sent, what MicroStrategy teams are responsible for analysis, and how to respond to customer reported problems.

Remote Access

Remote Access procedures establish the responsibilities and processes for requesting and approving secure remote access for to the Cloud Platform, setting up WebVPN sessions, obtaining two-factor tokens for privileges access, and remote access monitoring and logging. All remote administration requires two-factor token-based access and session timeouts are in place to automatically disconnect idle VPN sessions.

Exception Management

Exception Management procedures establish the responsibilities and processes for documenting, approving, and monitoring any exceptions to the MicroStrategy Cloud Platform Security and Availability policies. Any exceptions or waivers must be formally submitted to the Director or Compliance and Security for review and approval.
Approved exceptions are only valid for a maximum of one year and monitored by the Compliance and Security Team.

Security Information & Event Management (SIEM) Monitoring

SIEM Monitoring and Escalation procedures establish the responsibilities and processes for monitoring the SIEM software, managing log file data, log file retention, alerting, notification and escalation. The Compliance and Security Team monitors the SIEM alerts 24 hours a day and retains Cloud Platform log data for 90 days online and offline for at least one year.

Vulnerability Management

Vulnerability Management Program procedures establish the responsibilities and processes for vulnerability detection, tracking, and remediation. The Compliance and Security Team subscribe to a wide range of vulnerability advisory services, conduct weekly internal vulnerability scanning within the MicroStrategy Cloud Platform, and have third-parties perform quarterly external vulnerability assessments and annual penetration testing. As potential vulnerabilities are identified the Compliance and Security Team works with the COM Team to validate potential risks and develop risk mitigation solutions.

Contingency Planning

Contingency Planning procedures establish the responsibilities and processes for maintaining service during and following incidents that impact the MicroStrategy Cloud Platform. The Contingency Planning procedures establish the recovery objectives and provide detailed processes for assessing the impact of an incident at the datacenter facilities, conduct damage assessments, activating the plan, transfer operations to a backup facility, reconstitution, and deactivation of the plan. The Contingency Plans are tested annually and are updated based on the results of the tests and as the technical environment and operational procedures change over time.

Backup and Recovery

Backup and Recovery procedures establish the responsibilities and processes for backing up virtual servers, client cache and image data, and metadata databases on a daily basis, replicating this data between the datacenters, and conducting quarterly restoration testing to verify data can be successfully restored.

Risk Management

Risk Management Program and associated procedures establish the procedures for proactively identifying and managing risk within the MicroStrategy Cloud Platform. The MicroStrategy Cloud Platform management team meets on a monthly basis to review new risks that are identified, Risk Register containing risks that have been previously identified, risk remediation activities, and any prior risk acceptance. Risk assessments are conducted for the Cloud Platform and identified risks are added to the Risk Register for management review and mitigation planning and monitoring.

Plan of Action and Milestones (POA&M)

POA&M procedures establish the responsibilities and processes for tracking and monitoring tactical risk mitigation activities for the Cloud Platform. The Compliance and Security Team maintains the POA&M and monitors the
status of each POA&M item and works with the respective system manager to track mitigation progress through completion.

Security Awareness

Security Awareness and Training Program and associated procedures ensure all MicroStrategy staff that manage the Cloud Platform complete annual security awareness training on relevant risk management and IT security threats, countermeasures, and trends. The entire MicroStrategy Cloud Platform team has attended mandatory training on all key Cloud Platform policies, procedures, and operational controls. All MicroStrategy staff who manage the Cloud Platform are also required to complete privileged user training and acceptable use acknowledgement. The Compliance and Security Team also publishes monthly IT security newsletters company-wide.

Inventory & Asset Management

Inventory and Asset management procedures establish the responsibilities and procedure for tracking all physical assets used in the MicroStrategy Cloud Platform as well as software and IP address assignments for cloud customers and management systems. Physical assets are tracked within MicroStrategy’s Asset Tracking System (ATS) and hardware teams perform annual audits of all assets.

Media Handling

Media Handling procedures provide detailed procedures for handling media containing data from the MicroStrategy Cloud Platform. All media will be stored in a locked environment where access is tightly controlled, protected while in transit, and if no longer required the media will be sent to MicroStrategy headquarters for disposal. Any media used in the MicroStrategy Cloud Platform will not be reused in any environment.

The procedures outlined above address how MicroStrategy captures significant events, such as provisioning or de-provisioning users, performing changes, detecting and responding to incidents, recovering systems in the event of a disaster, and detecting and responding to problems. The procedures also dictate when information regarding changes or events need to be communicated to customers. Control Activities performed when following the defined procedures are presented in Section 4, “Trust Services Security Principles, Criteria, Related Controls, and Tests of Controls.”

SHARED SECURITY RESPONSIBILITY

MicroStrategy provides a secure infrastructure, controls, standards, and processes for our customers. The establishment of a customer instance in the MicroStrategy Cloud represents a partnership between MicroStrategy and the customer to provide a secure business intelligence environment.

In establishing the MicroStrategy Cloud environment, MicroStrategy assumes responsibility for the management and security of the network, hardware infrastructure, and software. When connecting to our service via the internet, our responsibility for the network includes the connections from the internet to our infrastructure; however, when utilizing VPN tunnels between the Customer and our Cloud Platform, the responsibility is shared. Our security practices include installing appropriate security patches, virus protections, upgraded hardware infrastructure, high availability, disaster recovery, and monitoring.

Our customers play a critical role in protecting their own environments. As part of the MicroStrategy Cloud environment, customers are provided access to build projects, reports, and documents, manage user access,
define password policies, and perform various development, maintenance, and administrative tasks. Customers must take responsibility internally to protect the accounts that access their systems to prevent unauthorized access. MicroStrategy provides the ability to track and audit changes in the environment, but the customer must ensure that accounts are protected, password policies are followed, and application access is controlled.

Customers are also responsible for the management of user access. MicroStrategy will provide a set of tools that allow customers to add, modify, and delete user access. The tools permit management of users and groups. As part of user management, customers will provide password management policies which can be integrated into the MicroStrategy platform. MicroStrategy recommends that companies implement strong password policies.

CERTAIN USER OBLIGATIONS

MicroStrategy’s services were designed with the assumption certain controls would be implemented by user entities. These controls should be in operations at user entities to complement MicroStrategy’s controls. The user entity controls subsequently presented should not be regarded as comprehensive list of all controls that should be deployed by user entities.

With regard to the security and availability of MicroStrategy Cloud Platform services, customers are responsible for:

Access Management – Customer Support Liaisons and Access Portal Admins

- Selecting personnel appropriate for fulfilling the Customer Support Liaison and/or Access Portal Admin role and requesting MicroStrategy provide these users access.
- Providing security awareness training and communicating other security obligations, such as rules of behavior, to their Customer Support Liaisons and Access Portal Administrators.
- Confirming their Customer Technical Support Liaisons have read and understand the Technical Support Policies and Procedures provided by MicroStrategy.
- Confirming their Access Portal Admins have read and understand the Portal Administration Policies and Procedures provided by MicroStrategy.
- Reviewing users who have Customer Support Liaison and/or Access Portal Admin role on a periodic basis and notifying MicroStrategy to a change in authorized users, including removal of access upon termination.
- Requesting a termination for a Customer Support Liaison and/or Access Portal Admin role in the event of a termination, and identifying the request as urgent if the user access needs to be removed within one day.

Access Management – Access Administration Portal

- Administering access to their Cloud Platform environment only to authorized personnel who are properly trained.
- Providing security awareness training and communicating other security obligations, such as rules of behavior, to their user groups.
- Adjusting the password policy enforced for users in their environment according to security requirements.
- Determining the groups necessary to support business processes and establishing those groups.
- Administering unique accounts to their users groups and prohibiting the use of shared accounts.
- Reviewing the user groups and authorized users for their environment on a periodic basis and updating access rights as needed.
- Disabling access of terminated users from user groups within their Cloud environment on a timely basis.
Access Management – Customer Managed Identification & Authentication

- Managing all aspects of Access Management if the customer uses identification and authentication mechanisms (e.g. LDAP controller) to authorize access to their Cloud Platform environment.

Maintenance Windows

- Planning operational use of the Cloud Platform in accordance with designated standard maintenance windows.
- Communicating conflicts to their MicroStrategy Engagement Manager in the event a system change or maintenance has been planned by MicroStrategy outside of, or extending past, a standard maintenance window.

Incident Reporting and Support

- Contacting customer support via the Technical Support hotline or Technical Support Ticketing System in the event of a known or suspected security incident, availability issue (outage), or other operational issues.
- Cooperating with the MicroStrategy response teams in the event an availability issue or if security event is identified, in order to identify the root cause and resolve the availability issue and/or security event.

Cloud Environment Build

- Confirming the initial setup of their Cloud Platform environment reflects an appropriate level of security (such as VPN encryption).
- Providing complete and accurate information for set-up of a new environment, such as: IP addresses, user defined firewall rules within VPN tunnels, email addresses for Customer Support Liaisons, etc.
- Requesting deviations from MicroStrategy’s Cloud Platform standard build only when absolutely required, and accepting responsibility for the resulting risk.
- Requesting patches, fixes, or updates be applied on the additional middleware or utility software specially requested to be installed on their servers.

Backups

- Requesting a copy of the virtual environment backup within in 30 days of termination of the subscription for hosted services (if a copy if desired).

File Transmission and Connectivity

- Verifying the content and health of files uploaded to their Cloud Platform environment.
- Ensuring the security and health of customer-owned systems connecting to the Cloud Platform environment over VPN.
- Reviewing error messages that result from uploading files to their utility box and responding to the error timely.

Personally Identifiable Information and Customer Data Protection

You are solely responsible for the development, content, operation, maintenance, and use of Your Content. You are solely responsible for the compliance of your Content with the MicroStrategy’s Cloud Platform Policies and all laws that may apply to your data including those in your location as well as the data center location. You are responsible the handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Content violate such person’s rights, including notices pursuant to the Digital Millennium Copyright Act. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain
appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving of Your Content. MicroStrategy Cloud Platform log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

CONFIGURATION MANAGEMENT

To validate network and infrastructure integrity, appropriate patch management protocols of integrated third-party products will be observed. MicroStrategy Cloud operations managers subscribe to automatic notifications for patches that are released by major vendors such as Microsoft, RedHat, Cisco, etc. In addition, MicroStrategy Cloud operations managers will check periodically for patches and releases that may be unannounced. MicroStrategy will assess whether a released patch is a service pack, feature upgrade, or security patch to establish the priority of deployment and appropriate procedure for release.

Each potentially applicable patch will be evaluated to determine whether it is applicable to the environment and how, when, and whether it should be deployed. Any patches proposed for implementation will be subject to appropriate isolated testing and verification prior to deployment. Enterprise systems will be patched after approval from MicroStrategy. The MicroStrategy Cloud Systems Engineering Team will follow standard procedures for migrating patches into production, including notifying field or remote users when a patch may be unknown to, but of importance to, a MicroStrategy customer.

The MicroStrategy Cloud team will notify end users and rely upon their compliance when a security patch should be installed to end user machines. Where possible, MicroStrategy will work with customers to minimize the impact of patches and maintenance and work around customers schedules. In some cases, due to system wide maintenance and after providing you reasonable notice, MicroStrategy will solely decide when maintenance will be applied to the Cloud customer environments. Patches will be managed by patch management software. The MicroStrategy Cloud team will use automated software deployment, whenever possible, to implement those patches designed to repair security vulnerabilities.

NETWORK SECURITY

MicroStrategy has architected the MicroStrategy Cloud Secure Connectivity (MCSC) infrastructure to establish secure connectivity between the MicroStrategy Cloud infrastructure, the customer’s data center, and devices. The MCSC provides a secure connection between MicroStrategy and the customer’s network for the MicroStrategy Cloud environment to access data from the customer environment. The MCSC is built on a secure computing infrastructure inside an isolated segment of the MicroStrategy Cloud network and is managed by MicroStrategy Information Systems professionals. The MCSC uses equipment that is self-contained and MCSC security practices are designed to protect electronic information and validate system integrity.

As part of a customer environment, each customer will be provided 3 connections between customer’s data centers and the MicroStrategy Cloud environment as part of the initial service. Additional connections can be purchased by contacting your MicroStrategy Account Executive.

The MCSC is a virtual network environment. The physical MCSC is located in MicroStrategy’s core data center and access is restricted to authorized personnel. Computing equipment in the MCSC is specifically and exclusively designated to be used by MicroStrategy Cloud customers. Access to configurations is limited to the authorized network professionals at MicroStrategy. Secure Shell (SSH) is used to access the network devices.

A secure firewall is used to protect and control network traffic. The firewall is configured to hide internal IP addresses using Static Network Address Translation (SNAT) and Static Port Translations (SPAT). External customer
networks access the MCSC through a secured Virtual Private Network (VPN) tunnel. VPN connections can be configured to the specifications of external parties that are recognized by the security community standards, and alternative access methods can be granted based on customer requirements.

Virtual Local Area Networks (VLANs) are used to grant or deny access of specific MCSC machines to specific external networks. Each customer is designated an individual VLAN to provide a network separate from other customer networks. These networks cannot communicate with each other and users within the network cannot access one VLAN from another. Each customer environment can be configured for customer specifications. MicroStrategy Technical Support Engineers connect to the MCSC via Web VPN to work so that the engineer’s machine does not directly access the customer’s corporate network. This secure connectivity helps to prevent the spread of malicious traffic between networks.

By default MCSC computers do not have external access to the public Internet, unless specifically requested by the customer. Network monitoring and connection tracking systems are used in the MCSC and network connections are logged. Wireless computer network technology is not used inside MCSC.

IPSec VPN tunnels may also be configured to add layer of security for data transmissions between the MicroStrategy Cloud Platform and customer networks. Our network engineers work closely with your network team to establish either IKE Phase 1 (ISAKAMP) or Phase 2 (IPSec) tunnels per your requirements. During the configuration, we have your network team fill out the requirements and our network engineers apply these parameters to your Cloud environment.

**MCSC SYSTEMS ENVIRONMENT**

Restrictive permissions to files, services, and system settings are applied to MCSC computers. Access Control Lists (ACLs) are used to limit access. Unnecessary operating system services are removed or disabled before system deployment in MCSC. Users are required to authenticate using a unique username and password to access any MCSC computer. An up-to-date antivirus scanner is installed on MCSC computers and vulnerability scans are conducted on MCSC computing equipment regularly. Security and other important patches provided by MCSC equipment vendors are routinely reviewed and applied by MicroStrategy Information Systems professionals. A Cloud support VLAN contains Windows Server Update Services (WSUS) and antivirus (AV) servers which provide appropriate updates to each network.

Virtual machines are deployed in the MCSC to support each customer configuration and they are governed by the same system security practices of physical machines.

US data centers supporting the Cloud Platform are SOC 1 Type II compliant and EMEA Data Centers supporting the Cloud Platform are ISO 27001 compliant. MicroStrategy reviews data center compliance on an annual basis to ensure that our providers continue to meet the standards.

**PHYSICAL SECURITY**

The MicroStrategy Cloud Platform infrastructure is operated in co-located data centers. The data center provides an array of controls, monitoring tools, and physical intrusion detection systems to provide controlled access to systems.

The data centers are operated by a third party operator and designed to provide physical security of IT assets. The data centers are staffed 24 hours a day, 365 days a year. The data centers are built in low profile buildings with no signage and high grade security features. The centers are designed to prevent unauthorized access and track authorized access to the center.
The MicroStrategy data center partner uses a patented multi-level security tracking system using a five-layer approach to control physical access. Access to the data centers is by appointment only. Once inside, biometric hand-readers, sign-in procedures, and visual confirmation are required prior to granting access. The center uses hundreds of security cameras and hand geometry readers to continuously monitor critical areas of the data centers as well as customer cages.

Within the data center, the MicroStrategy Cloud infrastructure has been installed in an isolated environment, configured in its own set of cages, isolated from other customers and other MicroStrategy environments within the data center. The cages are physically secured and locked to prohibit unauthorized access. The MicroStrategy Security team keeps a list of MicroStrategy employees that have been granted access to the environment.

**Customers may request to conduct their own scans of the MicroStrategy Cloud environment as long as these scans are focused only on the customer’s instances and do not violate MicroStrategy Cloud’s Acceptable Use Policy. The customer must request advanced approval for scans. A customer may request permission by emailing Cloud@microstrategy.com. Please provide at least 30 days prior notice for any scanning activity.**

**DATA RETENTION & DESTRUCTION POLICY**

MicroStrategy has a commitment to protect the assets provided by customers and partners. One of the most critical assets is the data that is entrusted to MicroStrategy as part of the MicroStrategy Cloud Service. MicroStrategy is committed to the protection of this data while under contract with customers and its destruction when MicroStrategy and customers determine it is necessary to terminate the relationship.

**DATA RETENTION**

MicroStrategy has implemented a data and record retention policy designed such that documents are retained in a uniform format for a specified period of time based on a defined retention schedule. MicroStrategy employees, contractors, and its directors are responsible for following the policies outlined in the Data Record Retention Policy. Policies covered under this policy include:

1. Retains records as necessary for business purposes, including maintaining the continuity and availability of records in the event of a disaster or hardware failure.
2. Retains records in accordance with applicable federal and state laws.
3. Retains records relevant to pending or reasonably anticipated legal proceedings, consistent with the company’s legal obligations.
4. Retains records as necessary for tax purposes.

The Data Record Retention Policy also specifies policies related to the destruction of documents that are no longer required for business, legal, tax, or other reasons. As part of the data destruction policy, the method for proper document destruction and disposal is defined.

Customer data created by MicroStrategy as part of conducting business falls under the MicroStrategy Data Record Retention Policy and will be managed as such.

**CUSTOMER-PROVIDED DATA**

Data that a customer provides to MicroStrategy includes, but is not limited to, business intelligence metadata values and descriptions, database schemas, ETL workflows and routines, data content (in database and text files), database backups, virtual machine images, user access information, and custom data manipulation code.
Data provided by the customer to MicroStrategy will be removed from the MicroStrategy environment and deleted within 30 days of termination of an agreement.

The customer may request, in writing, copies of the data to be provided. Such requests must be made prior to the termination of the agreement. Such copies will be subject to a fee based on the time required to fulfill the request.

MICROSTRATEGY EMPLOYMENT PRACTICES

MicroStrategy is dedicated to creating and maintaining a work environment that develops and values employees, providing opportunities for them to contribute to the company’s business success. MicroStrategy protects the personal welfare of employees with a work environment that does not tolerate unlawful discrimination, harassment, retaliation or violence, and requires adherence to the Federal Drug-Free Workplace Act and applicable environmental health and occupational safety laws and regulations.

EQUAL EMPLOYMENT OPPORTUNITY

MicroStrategy maintains policies for equal opportunity and advancement for qualified individuals without distinction or discrimination based on age, race, color, religion, creed, sex (including pregnancy, childbirth, or related medical conditions), marital or family status, national origin, ancestry, physical or mental disability, medical condition, veteran status, sexual orientation, or any other consideration prohibited under applicable law.

BACKGROUND SCREENING

MicroStrategy conducts pre-employment background screening on all applicants for employment. As permitted by law, MicroStrategy also conducts background screening on current employees who hold certain designated positions as circumstances warrant. Such background screening is done in accordance with applicable federal, state, and local laws.

ETHICAL STANDARDS

MicroStrategy is committed to upholding the integrity of the company through ethical business practices. Ethical conduct on the job is simply a matter of dealing fairly and honestly with MicroStrategy, fellow employees, customers, suppliers, competitors, investors, and the public. MicroStrategy employees are expected to avoid any action that results in or gives the appearance that they are using their employment at MicroStrategy for personal gain.

Every MicroStrategy employee is expected to adhere to the following company standards for activity in business-related locations or functions at all times:

- Engage in honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships
- Provide full, fair, accurate, timely and understandable disclosure in reports and documents that the Company files with, or submits to, the Securities and Exchange Commission and in other public communications made by the Company
- Provide prompt internal reporting of violations of the Code of Conduct to the appropriate person or persons indicated in this Code of Conduct and fully cooperate with Company investigations
- Treat customers and suppliers in a fair and honest manner
- Conduct the company’s business with integrity
- Comply with applicable governmental laws, rules and regulations
- Maintain accountability for adherence to the Code of Conduct
• Maintain efficient, proper standards of work performance
• Maintain professional conduct during all company business and events
• Adhere to all work-related written and verbal company policies and instructions
• Maintain MicroStrategy business offices as clean and safe work environments

MicroStrategy employees are expected to always judge a proposed course of action based on ethical standards outlined in the MicroStrategy Employee Handbook.

EMPLOYEE CODE OF CONDUCT

All MicroStrategy employees are required to sign, indicating that they:

• Received a copy of, or have convenient access to, the Code of Conduct
• Read and understood the Code of Conduct
• Will act in accordance with the Code of Conduct to the extent permissible under applicable law
• Understand that the provisions contained in the Code of Conduct: (i) represent policies of MicroStrategy Incorporated and its subsidiaries and (ii) are applicable to all employees, officers and directors of MicroStrategy Incorporated and its subsidiaries
• Are obligated to bring to the attention of the appropriate personnel (as described in the Code of Conduct) any suspected violations of law or of the Code of Conduct
• Comply with, and will continue to comply with, the Code of Conduct

CONTRACTING

MicroStrategy performs background screening of contractors performing work on behalf of the company.

DATA BREACH POLICY

The MicroStrategy Cloud environment is developed to block any attempted hack of its systems or data. Port scanning or network scanning tools are strictly forbidden within the environment. MicroStrategy does not allow customers to install third-party monitoring or direct access to our core monitoring systems without agreement from the Cloud Operations team.

In the case that the MicroStrategy Cloud Team determines an anomalous event including, but not limited to, Denial of Service, Malicious Code, Unauthorized Access, Inappropriate Use, Physical Breach, and Data Breach, to be deemed a security incident; the team will immediately activate its Computer Security Incident Response Plan (CSIRT). The plan includes provisions for prompt response including Security Incident Detection, Notification, Analysis, Containment, Eradication, Recovery, and Post Incident Analysis.
MICROSTRATEGY CLOUD PLATFORM SERVICE LEVELS

During the term of your subscription, MicroStrategy shall use reasonable commercial efforts to provide an Online Service that is available to you 99.9% of the time in any calendar month. Subject to the following provisions and in the event you experience availability in any given month falls below the benchmarks listed below, you will be eligible to 1) receive Credits, as described below or 2) an extension of the license term for such licensed software equal to such credit.

To receive a service credit, you must be operating an approved version of the MicroStrategy Technology when the outage event(s) occur and you must submit a request to MicroStrategy within fifteen (15) days following the month in which the outage event(s) occurred. The service credits set forth in the table below are customer’s sole and exclusive remedy when the availability in any given month falls below the stated benchmark. You understand and acknowledge that you may also engage in conduct that may cause your cloud based business intelligence environment to be unavailable and that MicroStrategy is not responsible for downtime experienced by an user as a result of customer activity.

MicroStrategy’s Service Level commitment is applicable to a single customer environment at a time. In the event a customer has two available environments during the course of an upgrade, the MicroStrategy SLA is applicable to only the environment that was established first. After the customer cuts over to the upgraded environment, the SLA is then applicable to only the upgraded environment.

MicroStrategy’s Service Level commitment covers availability of the following (“SLA Components”):

- Cloud Infrastructure Hardware (firewalls, network behind Online Services firewalls, servers and storage devices);
- Virtual Machines; and
- Clustered Instances of the MicroStrategy Technology including attached metadata databases.

This SLA is not applicable to outages or decreased response times resulting from issues related to applications built on the MicroStrategy Technology including: project, report, and document issues; migration problems related to customer design; ETL application problems; Internet outages; improper database logical design and code issues; factors outside of our reasonable control; downtime related to scheduled maintenance; general internet unavailability and other application issues out of the reasonable control of MicroStrategy.

### Availability Benchmark Table

<table>
<thead>
<tr>
<th>Period</th>
<th>Monthly Availability Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting January 1st 2013</td>
<td>99.9%</td>
</tr>
</tbody>
</table>

### Service Credit Table

<table>
<thead>
<tr>
<th>Period</th>
<th>Availability</th>
<th>Service Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting January 1st 2013</td>
<td>99.9%</td>
<td>1.00%</td>
</tr>
<tr>
<td></td>
<td>99.83% to 99.74%</td>
<td>3.00%</td>
</tr>
<tr>
<td></td>
<td>99.73% to 95.03%</td>
<td>5.00%</td>
</tr>
<tr>
<td></td>
<td>95.02% or less</td>
<td>7.00%</td>
</tr>
</tbody>
</table>
“Applicable Monthly Service Fees” means the total fees actually paid by you for the Online Services that are applied to the month in which a Service Credit has accrued.

“Unavailability” means the total minutes in a month during which you report that one or more of the SLA Components are unavailable.

“Service Credit” is the percentage of the Applicable Monthly Service Fees credited to you following claim approval.

“Monthly Availability Percentage” for the SLA Components is calculated by the following formula:

\[(\text{Total number of minutes in a month} - \text{Unavailability}) / \text{Total number of minutes in a month} * 100.\]

Note: Services credits are listed as hours.

If we fail to meet the minimum Monthly Availability Percentage described above for the Online Services, you may submit a claim for a Service Credit.

You must submit a claim to technical support at MicroStrategy that includes: (i) a detailed description of the event that resulted in Unavailability; (ii) information regarding the duration of the Unavailability; and (iii) descriptions of your attempts to resolve the incident at the time of occurrence.

We must receive the claim and all required information by the 15th day of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 10, we must receive the claim and all required information by March 15. We will then evaluate all information reasonably available to us and make a good faith judgment on whether a Service Credit is owed. You may not unilaterally offset any invoice for claimed Service Credits.

If you purchased the Online Service from a reseller, you will receive a service credit directly from your reseller and the reseller will receive a Service Credit directly from us.

**MICROSTRATEGY UPGRADE POLICY AND PROCESS**

As new versions of the underlying MicroStrategy business intelligence platform are released, MicroStrategy Cloud Platform is updated with the enhancements contained in those releases. For customers subscribing to the Cloud with a clustered environment, the update process proceeds in the following ways depending on the type of platform update.

A. Minor patches and infrastructure and operating system upgrades

   1. MicroStrategy maintains a scheduled three hour maintenance window on Wednesday and Saturday night of each week with an optional third maintenance window on Tuesday during business hours.

   2. MicroStrategy applies patches during the window of scheduled downtime. Scheduled maintenance downtimes do not count against MicroStrategy’s uptime SLA.

B. Major MicroStrategy software releases and upgrades

   1. MicroStrategy performs rigorous testing of major release versions prior to upgrading customer environments to maintain stability.
2. MicroStrategy provides a timeframe within which customers are able to schedule a time, allowing customers to minimize the impact of the transition.

3. For customers subscribing to MicroStrategy environments with clustering services, MicroStrategy creates an instance of your system based on the upgraded software platform to maintain your service during the upgrade. This instance runs in parallel with your production environment for a period of two weeks, during which time you may test the system using MicroStrategy Integrity Manager or other means. MicroStrategy also conducts its own tests during this time period.

4. At the end of the two week period, users of the old system are redirected to the new instance, and the old instance becomes unavailable.

All costs associated with these processes are included in your MicroStrategy Cloud Platform contract. MicroStrategy can accommodate additional, non-standard services or a customized upgrade process, for example, to accommodate more extensive user acceptance testing, subject to additional fees. New functionality is available to customers as soon as an upgrade has been completed. To the extent that the use of any new functionality is dependent on business intelligence solution design, the customer maintains control over the new functionality in its projects, reports, and documents. During the upgrade process, the SLA applies to only the primary environment being used by the customer.

**MAINTENANCE PLANNING**

MicroStrategy Cloud uses maintenance windows in support of planned maintenance activities. If the customer wishes to reschedule planned maintenance, the customer must submit a request to do so. Our maintenance windows may be scheduled from 2:00 AM – 5:00 AM on any Wednesday or Saturday during the year. MicroStrategy maintains an optional maintenance window on Tuesday between 9am – 12pm EST*. Times are relative to the location of the primary Data Center which hosts the customer’s Cloud environments for Wednesday and Saturday windows. Certain types of cross environment maintenance may not be possible during the Tuesday window and will be required during the Wednesday and/or Saturday windows. We will provide our customers at least 48 hours advanced notice when a maintenance window is activated. Support Liaisons, Technical Contacts, and Maintenance Contacts are notified for each activated maintenance window. During these scheduled interruptions, MicroStrategy Cloud systems may be unable to transmit and receive data through the provided services. Customer systems should include a process to pause and restart the applications around planned maintenance activities.

When it is necessary to execute emergency maintenance procedures within less than 48 hours until the beginning of the maintenance window, MicroStrategy notifies the customer by email and addresses pertinent concerns in an expedited manner.

*Tuesday maintenance windows are opt-in only and are not mandatory. Customers wishing to have maintenance conducted during this window must notify the MicroStrategy Cloud team in writing of the desire to do so. Please note that there may be instances in which cross system maintenance is required, which may require that the customer participate in a Wednesday and/or Saturday maintenance window.
CLOUD SUPPORT


MicroStrategy Cloud Support provides MicroStrategy Cloud Platform users with support 24 hours a day, 365 days a year. Many of the features from MicroStrategy support are available to MicroStrategy Cloud customers including:

- Access to the MicroStrategy Knowledge Base for technical and troubleshooting documentation
- Access to the MicroStrategy Discussion Forums, in which customers participate in open discussions and share best practices
- Access to on-line case logging through the MicroStrategy support site

For priority-level 1 and 2 emergencies related to MicroStrategy Cloud infrastructure issues, the MicroStrategy Cloud 24x7 emergency number is 1-855-CB1-MSTR (1-855-221-6787).

**NOTE: 24x7 support is provided in English only.**

BUSINESS AND SUPPORT OPERATIONS

MicroStrategy is headquartered in Tysons Corner, Virginia with the Cloud Services run out of multiple geographically dispersed locations including:

- Ashburn, VA – Data Center
- Seattle, WA – Data Center
- Slough, England – Data Center
- Tysons Corner, VA – Operational Support
- Chiswick, England – Operational Support
- Warsaw, Poland – Operational Support
- Hangzhou, China – Operational Support

<table>
<thead>
<tr>
<th>Data Center</th>
<th>Wednesday Maintenance</th>
<th>Saturday Maintenance</th>
<th>Tuesday Maintenance (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ashburn, VA, USA</td>
<td>2am - 5am EST</td>
<td>2am - 5am EST</td>
<td>9am - 12pm EST</td>
</tr>
<tr>
<td>Seattle, WA, USA</td>
<td>2am - 5am PST</td>
<td>2am - 5am PST</td>
<td>9am - 12pm EST</td>
</tr>
<tr>
<td>London, UK</td>
<td>2am - 5am GMT</td>
<td>2am - 5am GMT</td>
<td>9am - 12pm EST</td>
</tr>
</tbody>
</table>
SUPPORT LIAISONS

Support liaisons are individuals designated by the customer in their license or maintenance agreement as a point-of-contact with MicroStrategy’s support personnel. Cloud Support services may only be obtained by support liaisons. The support liaisons maintain ownership of issues escalated into MicroStrategy Cloud Support and as such, case-related communication is conducted with these named individuals. Your support agreement with MicroStrategy provides for a set number of support liaisons that are authorized to contact MicroStrategy Cloud Support. Additional support liaisons can be acquired through the customer’s account management team if needed. Customers may request to change their support liaisons six times per year. It is the customer’s responsibility to advise MicroStrategy Cloud Support if there are any existing support cases that should be transferred when a support liaison is changed.

CONTACT SUPPORT

Problems or questions related to MicroStrategy Cloud Platform must be reported to MicroStrategy Cloud Support using the standard communication channels.

To contact MicroStrategy Cloud Support, access the MicroStrategy Global Support website: https://resource.microstrategy.com/support/

LOGGING A CLOUD SUPPORT CASE

To log a MicroStrategy Cloud support case, the designated support liaisons may contact MicroStrategy Cloud Support via email, telephone, or by using the Online Case Tracking Interface, located on the MicroStrategy Support Site: https://resource.microstrategy.com/support. Only the designated support liaisons can log cases with MicroStrategy Cloud Support. Upon logging a case, the support liaison receives a case identification that should be used for communications regarding this case.

When logging a case, be prepared to provide the following information:

- Personal Information
- Name
- Company and customer site (if different from own company)
- Contact information (phone and fax numbers, e-mail address)
- Case Details
- Configuration information, including MicroStrategy software product(s), version(s), and DSI in which the products are installed
- Full description of the case containing symptoms, error message(s), steps taken to troubleshoot the case thus far
- Log files or other supporting data
- Customer system impact

TYPES OF CLOUD SUPPORT CASES

MicroStrategy Cloud support cases are segmented in two different categories:

b) Cloud infrastructure issues: issues are referred to the MicroStrategy Cloud operations managers by Cloud Support and follow the priority and response guidelines outlined below.
### PRIORITIES AND RESPONSE GUIDELINES

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Escalation Level</th>
<th>Definition</th>
<th>Priority Level Examples</th>
<th>Initial Response Time</th>
<th>Status Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical</td>
<td>Critical component(s) are degraded or offline and the production systems are impacted.</td>
<td>Virtual application is unavailable.</td>
<td>&lt; 2 Hours</td>
<td>Daily / As status changes</td>
</tr>
<tr>
<td></td>
<td>(Immediate Action)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Major</td>
<td>Non-critical component(s) are degraded or offline and the production systems are impacted.</td>
<td>Reports are not delivered by Distribution Services</td>
<td>&lt; 2 Hours</td>
<td>Daily / As status changes</td>
</tr>
<tr>
<td></td>
<td>Within 8 Hours (Same Business Day)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Medium</td>
<td>Component(s) are degraded or offline but the production systems are NOT impacted. (e.g. Development, Test &amp; Support Systems)</td>
<td>I-Cubes are not automatically refreshed in the development system.</td>
<td>&lt; 4 Hours</td>
<td>As status changes</td>
</tr>
<tr>
<td></td>
<td>Within 48 Hours (2 Business Days)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>Little or no business impact.</td>
<td>How frequently snapshots of the VAPPs are taken?</td>
<td>&lt; 6 Hours</td>
<td>As status changes</td>
</tr>
<tr>
<td></td>
<td>(As Time &amp; Priorities Permit)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### PROVIDING DATA TO MICROSTRATEGY CLOUD SUPPORT

During the course of troubleshooting and researching issues, it may be necessary to provide MicroStrategy Cloud Support personnel with data from your systems (diagnostics, metadata copies, result sets, etc.). For the convenience of our customers, MicroStrategy provides several methods to transmit this data including, but not limited to, Email, the MicroStrategy Support Site, the MicroStrategy Download Site and MicroStrategy Health Center.

It is your responsibility to ensure that you do not provide us with data that could be considered Protected Health Information (PHI) or any Personally Identifiable Information (PII) in the data set sent to assist in troubleshooting your case. In no event will MicroStrategy, or any of its affiliates, be liable for any indirect, special, incidental, consequential, or exemplary damages, whether in contract or tort, or otherwise, if such data is sent to MicroStrategy. Customers should work with the Cloud Support Engineer assigned to their case to coordinate all data transfers.
**DOMAIN URL DEFINITION**

Each MicroStrategy Cloud customer is given a separate URL to access the service. MicroStrategy provides a default domain for companies defined as yourdomain.cloud.microstrategy.com. You can request additional domains for your company at additional charge to cover the cost of security certificates required to support the domain. Contact a MicroStrategy Cloud expert for questions regarding custom domain mapping to a custom URL such as cloudBI.yourdomain.com.

**ACCESSING THE MICROSTRATEGY CLOUD**

Upon handoff of the MicroStrategy Cloud environment, designated customer representatives are provided a specification document outlining items related to their service. This document includes the configuration and connectivity details required to access their system.

MicroStrategy offers two options to access the Cloud Environment. The first method establishes a VPN connection between a customer network and the MicroStrategy Cloud. With this method, the MicroStrategy Cloud servers are not exposed directly to the Internet and appear as a set of machines on your private intranet. The second method allows the MicroStrategy Cloud servers direct access to the public Internet. This method is implemented upon customer request. By default web connectivity is set up using SSL/HTTPs.

The basic connection to MicroStrategy Cloud supports single factor authentication. Two-factor authentication is offered for an additional setup charge.

**DEVELOPER ACCESS**

Developers access MicroStrategy Cloud Platform using a Web VPN connection. Customer development teams are provided individual user accounts to access the development environment to build projects, reports, and