<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Introduction</td>
<td>2</td>
</tr>
<tr>
<td>II. Employing Best Practices</td>
<td>4</td>
</tr>
<tr>
<td>Expertise</td>
<td>4</td>
</tr>
<tr>
<td>Certifications &amp; Compliance</td>
<td>4</td>
</tr>
<tr>
<td>III. Application, Platform and Physical Security</td>
<td>4</td>
</tr>
<tr>
<td>Application Security</td>
<td>4</td>
</tr>
<tr>
<td>Platform Security</td>
<td>8</td>
</tr>
<tr>
<td>Physical Security and Protection</td>
<td>9</td>
</tr>
<tr>
<td>IV. Operational Readiness</td>
<td>10</td>
</tr>
<tr>
<td>Vulnerability Assessments</td>
<td>10</td>
</tr>
<tr>
<td>System Surveillance</td>
<td>10</td>
</tr>
<tr>
<td>Incident Management</td>
<td>10</td>
</tr>
<tr>
<td>Communication Plan</td>
<td>10</td>
</tr>
<tr>
<td>V. Redundancy</td>
<td>11</td>
</tr>
<tr>
<td>Disaster Recovery and Business Continuity</td>
<td>12</td>
</tr>
<tr>
<td>VI. Comprehensive Security in the Cloud</td>
<td>13</td>
</tr>
</tbody>
</table>
I. Introduction

MicroStrategy Cloud is revolutionizing business intelligence. In this new BI delivery model, MicroStrategy customers can rely on a fully managed platform for building analytical applications. Within the cloud infrastructure, MicroStrategy takes on the responsibility of building and maintaining the hardware and software infrastructure. This includes all of the BI software and in many cases, data integration, and data hosting software. Consequently a customer’s data may reside inside the MicroStrategy Cloud environment. Many organizations have legitimate concerns about the privacy and security of their data “in the cloud”. MicroStrategy understands this and protecting its customers’ data is of paramount importance.

Threats to data security can come in many forms, including cyber-attacks, on-site tampering, as well as destruction due to acts of nature. These threats exist whether an organization manages its own data or entrusts it to an organization like MicroStrategy. Protecting data against a wide array of highly complex and insidious dangers is not easy. That is why MicroStrategy Cloud has assembled a dedicated services team and charged them with putting in place stringent security measures, based on industry best practices. MicroStrategy’s goal is to ensure its customers’ data is as safe and secure as possible in the MicroStrategy Cloud environment. Moreover, MicroStrategy continues to invest and innovate to stay ahead of the evolving threats to data security.

Data is protected through multiple layers of safeguards.

MicroStrategy employs a multi-pronged strategy to securing systems and data. First, MicroStrategy ensures that the cloud environment meets or exceeds industry best practices by investing in expertise and staying compliant with the many industry standards and frameworks. Second, MicroStrategy has put in place a wide array of counter-measures to ensure application, platform, and physical security. Third, MicroStrategy uses independent, third-party audit services and uses internal monitoring and alerting systems to neutralize any threats. Finally, MicroStrategy ensures high availability through the use of redundancy and reliable backup procedures. Table 1 on the next page provides a summary of MicroStrategy’s multi-pronged strategy as well as specific tactics.
With MicroStrategy Cloud, organizations now have access to MicroStrategy's award-winning business intelligence without the challenges and high costs of standing-up and managing an entire infrastructure. Instead, companies are provided with a dedicated and experienced operations team to build and manage a performance-optimized environment, alleviating the need to budget for and rely on a thinly spread internal IT team. This, coupled with MicroStrategy’s focus on data privacy and security, gives customers the ability to deliver high-performance and secure applications with unparalleled efficiency.

### Table 1. Overview of MicroStrategy Cloud Security Strategies

<table>
<thead>
<tr>
<th>STRATEGY</th>
<th>DETAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Best Practice</strong></td>
<td></td>
</tr>
<tr>
<td>Expertise &amp; Investment</td>
<td>Customers leverage MicroStrategy's significant investment in securing the cloud environment using best practices.</td>
</tr>
<tr>
<td>Certifications &amp; Compliance</td>
<td>Security controls can be mapped to many common industry frameworks including ISO27001/2, PCI, and HIPAA.</td>
</tr>
<tr>
<td><strong>Cyber and Physical Security</strong></td>
<td></td>
</tr>
<tr>
<td>Application Security</td>
<td>User, project and object level authentication</td>
</tr>
<tr>
<td></td>
<td>Support for LDAP and single sign-on</td>
</tr>
<tr>
<td></td>
<td>Enables enforcement of password management policies such as encryption, strength, and duration</td>
</tr>
<tr>
<td></td>
<td>Secure data transmission</td>
</tr>
<tr>
<td>Platform Security</td>
<td>Perimeter firewalls</td>
</tr>
<tr>
<td></td>
<td>Intrusion detection and updated security patches</td>
</tr>
<tr>
<td></td>
<td>Multi-tier architecture</td>
</tr>
<tr>
<td></td>
<td>Support for secure connectivity (SSL, VPN, SSH, and others)</td>
</tr>
<tr>
<td></td>
<td>IP obfuscation and Encrypted communication</td>
</tr>
<tr>
<td></td>
<td>Dedicated and isolated VLAN, VPC, and VMs</td>
</tr>
<tr>
<td>Physical Security</td>
<td>SSAE-16 Type II compliant hosting facility</td>
</tr>
<tr>
<td></td>
<td>24x7 security including video surveillance</td>
</tr>
<tr>
<td></td>
<td>Biometric access to locked cages</td>
</tr>
<tr>
<td></td>
<td>Redundant, fault-tolerant designs</td>
</tr>
<tr>
<td><strong>Operational Readiness</strong></td>
<td></td>
</tr>
<tr>
<td>System Audits</td>
<td>Independent audits of security controls</td>
</tr>
<tr>
<td></td>
<td>Internal reviews to assess conformance to the information security policy</td>
</tr>
<tr>
<td>Monitoring, Alerting, and Reporting</td>
<td>Network Operation Centers (NOC) that operate 24x7 and have global reach</td>
</tr>
<tr>
<td></td>
<td>Continuous monitoring of logs, alerts, and notifications</td>
</tr>
<tr>
<td></td>
<td>Well defined incident management, escalation process, and communication plan</td>
</tr>
<tr>
<td><strong>Redundancy and Business Continuity</strong></td>
<td></td>
</tr>
<tr>
<td>Redundancy</td>
<td>Redundant infrastructure, including servers and network components</td>
</tr>
<tr>
<td></td>
<td>Redundant operating environments (VMs)</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Data and system recovery processes support customers business continuity plans</td>
</tr>
</tbody>
</table>
II. Employing Best Practices

EXPERTISE
Cyber-security is a highly specialized expertise that is evolving continuously. This is driven by the rapid advancements in cyber attacks fueled by well-funded and vigilant hackers. In the 2010 edition of its Annual Threat Review, Symantec noted that attacks were up 93% from the previous year. In order to keep pace with cyber security threats, MicroStrategy employs a highly qualified team of security experts to develop a security program around adaptive defense.

Adaptive defense automates cyber security processes, enabling MicroStrategy to automatically adjust defensive posture in response to incidents and imminent threats. The foundation of adaptive defense is the system of people, processes, and tools that tightly couples security and systems management.

Since inception, MicroStrategy has been built with the philosophy of bringing together the best, brightest and most experienced engineers and computer scientists. The MicroStrategy Cloud Services team is no exception. This group of highly experienced software, BI, ETL, network, storage, and security engineers have put in place industry tried-and-tested security countermeasures and processes to safeguard data throughout the cloud environment.

CERTIFICATIONS AND COMPLIANCE
MicroStrategy has developed a comprehensive compliance management program that is used to manage the health and security posture of every layer in the managed cloud environment. MicroStrategy Cloud controls are based on the Cloud Security Alliance control matrix. As such, controls can be mapped to common industry frameworks including SSAE 16, ISO27001/2, PCI, and HIPAA.

III. Application, Platform, and Physical Security

There are at least three areas of vulnerability that any public facing computing platform must protect. First, at the application layer, the system must be able to thwart any unauthorized attempt to access data. Second, at the platform layer, the underlying architecture and control mechanisms should ensure the integrity and security of the data. Third, at the physical layer, sufficient obstacles must be put in place to make it difficult for any unauthorized persons to access the systems directly. Any security counter-measures that are put in place must, at a minimum, protect these three areas of vulnerability. This section describes the details of how application, platform, and physical security are applied to MicroStrategy Cloud.

APPLICATION SECURITY

Overview
A successful application security implementation uses a multi-layered approach to role-based authentication control (RBAC). This ensures only authorized users are able to access the system and users are only able to view or update data they are authorized to see. MicroStrategy’s multi-tiered approach to application-level security begins with basic user authentication. In addition to its native authentication, MicroStrategy supports single sign on (SSO), direct authentication via LDAP, and database authentication. Once users are authenticated within the MicroStrategy BI application, access to data is governed by the permissions granted to a specific user. As a matter of convenience, users can be organized into groups in order to manage privileges for sets of users. MicroStrategy also provides additional mechanisms, such as security roles and object level security, that allow fine-grained control over projects,
dashboards, reports, and metrics. At the data level, MicroStrategy employs the use of connection maps, security filters, as well as robust cube and caching techniques. For customers using data integration services to support ETL functions there are a number of additional security features built-in to ensure highly secure data transfer.

**Authentication Modes**

The MicroStrategy business intelligence platform supports several authentication modes including LDAP, Single Sign-On, database, as well as MicroStrategy-based authentication. Each mode is differentiated based on the authentication authority. The authentication authority is the system that verifies and accepts the login and password credentials provided by the user. This robust set of authentication mechanisms delivers powerful authentication capabilities across all levels of an application, including at the user, project, and object levels.

**User Level Security**

**USERS**

In order to access a MicroStrategy application, a user must first log in to the system using a login ID and password. Based on individual privileges, a user can then perform tasks such as creating objects or executing reports and documents.

Each MicroStrategy Cloud customer environment is assigned its own metadata and users are created to be metadata-specific. In essence, the customer environment is a private cloud with a unique user base that is managed by the customer.

**GROUPS**

Users can be organized into user groups. Groups provide a convenient way to manage a large number of users. Instead of assigning privileges and security to individual users, customers may assign them to groups and the users will inherit those privileges.

**PRIVILEGES**

Privileges give users access to specific MicroStrategy functionality. Privileges can be assigned to users and user groups directly or through security roles. When privileges are assigned to specific users or groups, those rights are available to users across all projects. On the other hand, when assigned through security roles, privileges are limited to specific projects only. In this way, MicroStrategy enables an additional level of authentication.

**Project Level Security**

**SECURITY ROLES**

A security role is a collection of project-level privileges that are assigned to users and groups. For example, a customer might have two types of users with different functionality needs: the Executive users who need to run, sort, and print reports, and the Business Analysts who need additional capabilities to drill and change subtotal definitions. In this case, two security roles are needed to suit each different type of users.
All three dimensions of user authorization - application functionality privileges, object access permissions, and data access security - may be defined at the user, group, or security role level.

Object Level Security

MICROSTRATEGY OBJECTS

Individual MicroStrategy metadata objects are governed by their own security permissions called Access Control Lists (ACL). Each data abstraction object, business abstraction object, report component, and report definition can be assigned a unique ACL, which grants users or user groups a set of permissions for the object.

Permissions define the degree of control users have over individual objects in the system. For example, in the case of a report, a user may have permission to view the report definition and execute the report but not modify the report definition or delete the report.

Security filters enable customers to control what warehouse data users can see when accessed through MicroStrategy. A security filter can be assigned to a user or group to narrow the result set when they execute reports or browse elements. The security filter applies to all reports and all attribute element requests submitted by a user. Security filters serve a similar function to database-level techniques such as database views and row level security.

DATABASE OBJECTS

In a database, security restrictions for database logins can be placed on tables, rows, and columns. MicroStrategy's BI platform accesses data sources using database connections. Separate database connections can be created to access the same data source with different logins. MicroStrategy users and user groups are linked to database connections using connection maps. All users allocated to a database connection will log in to the database with the same credentials and will be subject to the security settings in the data source.

Furthermore, database views may include restrictions associated with each database login within their definition. This login, obtained from the database connection information, limits the rows that are selected by the view when processing queries. These security views provide row-level security for every query submitted by the user. Since an administrator defines this security view inside the data source, all query tools accessing the data source with a particular login will use the view. The SQL statement used to create the database view can also be used within MicroStrategy to define a logical table in the metadata.
Connection mappings allow customers to assign a user or group in the MicroStrategy system to a specific login ID on the data warehouse RDBMS. The mappings are typically used to take advantage of one of several RDBMS data security techniques (security views, split fact tables by rows, split fact tables by columns) that may be currently implemented.

![Diagram of MicroStrategy's comprehensive application, object access, and data access security](image)

MicroStrategy's comprehensive application, object access, and data access security provides granular control in the MicroStrategy Cloud.

CUBE AND CACHE SECURITY
Caches and cubes are specific to each unique system environment, which runs in a separate virtual environment and is not accessible by any other MicroStrategy customer. Data stored in memory in Intelligent Cubes and caches are secured using a variety of different approaches. Both cubes and caches can be encrypted using MicroStrategy's encryption technology. Cache and cube based data also take full advantage of the physical security environment of the MicroStrategy Cloud infrastructure outlined earlier in this document.

Data Transmission
MicroStrategy Cloud Data Integration Services (MCDIS) is an optional service that supports basic ETL functions and allows customers to move data securely into the MicroStrategy Cloud Data Warehouse environment.

To reduce vulnerability when using MicroStrategy ETL services in the Cloud, data is moved using a secure agent running behind the customer's firewall directly to the MicroStrategy Cloud. No proprietary data passes through or resides on any intermediate or third party servers. The ETL Services are restricted to only storing metadata required to perform tasks in a multi-tenant repository.

The MCDIS service is optimized to work with MicroStrategy Cloud Data Warehouse Service (MSDWS) for customers who chose not to implement their own data integration process. Customers who have their own data integration standards can utilize their in-house tools as long as proper connectivity between the customer network and MicroStrategy can be established.
PLATFOrM SecuriTy

Network Architecture

MicroStrategy Cloud is implemented using a high-performance, multi-tier, scalable web architecture that inherently provides a wide range of security features. The system is comprised of four logical layers, namely the user, web server, application, and data access layers. The network is characterized by secure external connectivity, secure intra-network communication, database isolation, and stringent port controls.

A multi-tier architecture ensures isolation of application and database components.

The MicroStrategy Cloud Secure Connectivity (MCSC) network was architected in such a way as to establish secure connectivity between the MicroStrategy Cloud infrastructure and customer networks. The MCSC provides a secure connection between MicroStrategy and the customer’s network in order 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 ensure system integrity.
Within the MCSC, each customer is provided with a dedicated VLAN to ensure network isolation. In essence, each customer operates in an exclusive virtual private cloud (VPC). By default, all internal IP addresses are obfuscated to reduce the risk of unauthorized network penetration. Remote access to external customer networks is through a secured VPN tunnel. Other alternative access may be granted based on the customer requirements and security risk assessment. In addition, the MCSC supports use of digital certificates. This enables the use of encrypted (SSL) communication with all client web browsers.

Perimeter firewalls are used to create a demilitarized zone (DMZ) and thereby isolate internal sub-systems from Internet traffic. These firewalls are configured to prevent communication on any unnecessary ports. This reduces the network’s susceptibility to “port-scanning,” a tactic often employed by hackers to find active ports and exploit known vulnerabilities. In addition, any remote server calls (e.g. RPC, RMI) are strictly prohibited on any MCSC server. Such remote calls are hazardous because they allow hackers to access and control remote and distributed processes.

System Security
Restrictive permissions to files, services, and system settings are applied to all MCSC servers. Access Control Lists (ACLs) are used to limit access. All unnecessary operating system services are removed or disabled before system deployment in MCSC. All 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 all MCSC computers and vulnerability scans are conducted on all MCSC computing equipment regularly. Security and other important patches provided by MCSC equipment vendors are routinely reviewed and applied by MicroStrategy Information Systems professionals. All virtual machines deployed in the MCSC are governed by the same system security practices of physical machines.

PHYSICAL SECURITY AND PROTECTION
MicroStrategy Cloud servers are housed exclusively in SSAE16 Type II compliant hosting environments. This means that physical access to the servers on which customer data resides is highly restricted. Moreover, the facilities are constructed to prevent damage caused by deliberate acts of vandalism or that caused by acts of nature. Below is a list of security features found at MicroStrategy Cloud’s data centers.

ACCESS CONTROL AT HOSTING FACILITIES
• 24-hour manned security, including foot patrols and perimeter inspections
• Biometric scanning for access
• Dedicated concrete-walled Data Center rooms
• Computing equipment in access-controlled steel cages
• Video surveillance throughout facility and perimeter
• Building engineered for local seismic, storm, and flood risks
• Tracking of asset removal

FACILITY ENVIRONMENTAL CONTROLS
• Humidity and temperature control
• Redundant (N+1) cooling system

POWER
• Underground utility power feed
• Redundant (N+1) CPS/UPS systems
• Redundant power distribution units (PDUs)
• Redundant (N+1) diesel generators with on-site diesel fuel storage
NETWORK
• Concrete vaults for fiber entry
• Redundant internal networks
• Network neutral; connects to all major carriers and located near major Internet hubs
• High bandwidth capacity

FIRE DETECTION AND SUPPRESSION
• VESDA (very early smoke detection apparatus)
• Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

VI. Operational Readiness

VULNERABILITY ASSESSMENTS
MicroStrategy leverages internal risk management and audit functions to provide independent assessments of risk as part of an on-going cycle of audit. Third party auditors are leveraged to provide a final assessment of the control framework and to ensure MicroStrategy is executing controls as documented.

MicroStrategy Cloud Security teams maintain the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy.

SYSTEM SURVEILLANCE
MicroStrategy Cloud operations has established Network Operation Centers (NOC) around the world and offers 24x7 monitoring services. MicroStrategy's Information Security teams monitor logs, alerts and notifications from a variety of systems in order to proactively detect and manage threats. In addition, software agents are deployed across all tiers of the MicroStrategy Cloud framework to monitor hardware, storage, networking, virtualization, operating system, and application, providing real-time visibility into the environment.

INCIDENT MANAGEMENT
In the event of a triggered alert, the alert is triaged and the appropriate issue resolution process is initiated. The objective of this process is to highlight and identify the appropriate level of resources and expertise to isolate and neutralize any threats. The process has a well-defined escalation path and communication plan. It also calls for a “postmortem” of any significant alerts in order to prevent repeat incidents by identifying, and then subsequently rectifying, any gaps in existing controls.

COMMUNICATION PLAN
In compliance with federal, state, or foreign law (as applicable), MicroStrategy has implemented processes to provide notification to customers of lost or compromised data based on the severity of the security threat and the results of any individual attack.
VI. Redundancy

MicroStrategy Cloud’s infrastructure is architected with redundancy in mind. A variety of backup mechanisms and failover processes help contribute to MicroStrategy Cloud’s uptime SLA. This protects against a number of different potential causes of disruption including power outages, loss of Internet connection, as well as hardware failure.

The MicroStrategy cloud has dual, independent 10GB connections to the Internet backbone. Each line is brought in from a different carrier. In the event that there is disruption to one carrier’s service, the additional connection will remain live.

Hardware redundancy is also key to providing uninterrupted service. The cloud infrastructure is designed with redundant load balancers, firewalls as well as physical servers. While typically the mean time-to-failure for such devices is quite long, any of these components are subject to breakdown. Automatic failover mechanisms are also built into the MicroStrategy Cloud infrastructure for these hardware devices. The system would automatically recognize any disabled device and direct traffic to only the remaining functioning hardware.

As noted earlier, all software in the MicroStrategy Cloud runs inside virtual machines. These VMs provide self-contained operating environments that enable a highly effective redundancy strategy. A separate VM is created for each software sub-system, including the MicroStrategy BI application, data warehouse, data integration service, and so on. Redundant VMs are then deployed across different physical servers. Should one of the VMs fail, the system would continue to operate using the backup VM. Similarly, in the event of physical server failure, the system would still continue to operate using the backup VMs on the backup servers.

In any situation involving a component failure, an alert is automatically generated and distributed to the MicroStrategy Cloud Operations team. At that point, the incidence management process would kick in and steps would be taken to remediate the problems.
DISASTER RECOVERY AND BUSINESS CONTINUITY

System Recovery
System reconstruction in the event of a disaster requires MicroStrategy's teams to be able to restore the hardware and software infrastructure to its original state. To support this, MicroStrategy has established and documented processes to re-create the base operating environment. This includes both the hardware and system software components. MicroStrategy’s use of VMs to run customer specific software, then enables its engineers to very easily restore the application software to the last known state.

Data Recovery
MicroStrategy backup policies and procedures are designed to ensure limited downtime to the customer should an unforeseen incident occur that impacts the quality or availability of customer data. MicroStrategy considers the use of additional US as well as international hosting facilities as it is warranted. In a fully operational setting, all customer data will be redundantly stored in separate offsite locations. Initial services are based in Ashburn, VA.

MicroStrategy Cloud Services will perform a scheduled backup on a nightly basis of the following:

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

This backup is persisted in a storage device located in the MicroStrategy Cloud data center and is subject to the same physical security as other MicroStrategy Cloud infrastructure. These backups are retained for a period of 30 days, at which point they are permanently deleted.

These backup procedures are designed as part of an overall effort to support customers’ business continuity plans.
VI. Comprehensive Security in the Cloud

MicroStrategy Cloud delivers a fully managed, high performance platform as a service which customers leverage to build BI applications rapidly with no capital investment. Securing data is a critical requirement in the cloud environment. MicroStrategy Cloud has been architected from the ground up to include a wide range of countermeasures to protect the data it houses. The security controls in place map to many of the common frameworks and standards including SSAE-16 Type II, ISO27001, PCI, HIPAA and others. These controls exist at the application, platform, and physical layers, where every system is highly vulnerable to attacks.

Protecting the large volumes of data is of paramount importance for a BI cloud service. MicroStrategy Cloud’s infrastructure is designed to provide a high degree of data security. Moreover, MicroStrategy continues to invest and innovate to stay ahead of the evolving cyber-security threats. The resulting security framework meets the security needs of any organization deploying business intelligence in the MicroStrategy Cloud. This allows customers to leverage and rely on the MicroStrategy Cloud security infrastructure and focus their efforts, instead, on developing business intelligence tools to solve business problems.