I. Introduction

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.

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 Express, individuals now have access to MicroStrategy’s award-winning business intelligence directly, without need of a planned data model, or a large infrastructure. Instead, users are given only a subset of functionality that is most relevant to their direct needs. This, coupled with MicroStrategy’s focus on data privacy and security, gives non-technical business users the ability to deliver high-performance and secure applications with ease.

II. Employing Best Practices

EXPERTISE

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.

Further, since inception, MicroStrategy has been built with the philosophy of bringing together the best, brightest, and most experienced engineers and computer scientists. The Express team is no exception. This group of highly experienced software, BI, 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

Express servers are hosted in an SSAE 16 compliant facility.
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 Express

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. Express offers both standard username and password authentication, and integration with Usher, a MicroStrategy application which provides full digital validation of identity. Once a user gains access to Express, their access is restricted only to objects and data leveraged by those objects which they have been granted access to. As Express does not work off of an object based model, connections to the data itself are not reusable.

Authentication Modes
Express offers authentication via both MicroStrategy-Based Authentication, and through the Usher Application Server (part of the Usher Mobile Identity Network) from MicroStrategy (http://ushers.com/). The former follows industry standard authentication authority to process username and password to grant access. The latter uses a digital authentication application, which allows a user to prove their identity with hardware (i.e. an iOS or Android device) rather than a username and password.

Object Security
By default, no dashboard can be seen by any user other than its creator. In order to grant access to a dashboard, a creator must choose to share the dashboard or application, and specifically add users to the access list. At this point, only if the user has a valid Express subscription, will they be allowed to access the dashboard. The permission to access the dashboard can be removed from any user at any time within the same mechanism. The removal of permissions will be instantaneous.

In addition, row level security can be granted through the personalization process. At the level of each individual dashboard access can be restricted to specific data elements, thereby allowing the user access only to the rows that are relevant to him or her. This row level security is applied whether the user accesses the data interactively, via delivery, or any other method.

Data Security
The MicroStrategy In-Memory Cubes underlying each Express dashboard are accessible only to that specific dashboard. This insures that no other user on the system can gain access to the data stored within the In-Memory Cube. The Cubes themselves are secured in a number of other ways, as well, including both the MicroStrategy encryption technology and the MicroStrategy Cloud Infrastructure outlined separately within this document.

Data Transmission
For all flat file data imported into Express, the data is transferred via HTTPS. This is also true, by default for Database data.

Any data replicated into Express In-Memory Cubes is persisted into a proprietary format cache file, which is stored with a RIPEMD-160 encryption. This ensures multiple levels of security for all data.
Express Delivery Dashboards do not utilize the MicroStrategy In-Memory Cube approach, and so in the case of a delivery dashboard, there is no data stored within the Express servers. Data is brought into memory briefly to create the emails, and then discarded immediately after delivery.

Where possible, connections to standard cloud sources such as Salesforce.com utilize industry standard protocols, such as OAuth, to ensure that MicroStrategy does not store credential information for these data providers.

**VPN Option**

In the case that HTTPS level security is insufficient for user security needs, or it is required to connect to a database which is not accessible via the internet, it is also possible to establish a VPN connection between the user environment and the MicroStrategy Cloud servers which host Express.

Our IPsec VPN creates a point to point connection, and allows the user to specify the IP addresses of the Database servers they wish to connect to the servers hosting their Express Teams. It’s also possible to restrict access down to the port level.

This virtual network provides the user with the same functionality, security and management policies of a full local network.

**Session Management**

Express closes all sessions after 30 minutes of inactivity. This ensures that even if the user leaves their computer accessible, data will not be exposed via an orphan session.

**Strong Password Standard**

MicroStrategy strictly enforces strong password standards for all MicroStrategy user accounts. Requiring minimum password length and complexity makes Express user accounts less susceptible to hacking. Passwords must have a minimum of eight characters and contain at least one of the following special characters: !, @, #, $, %, ^, &, +, =.

**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 intranetwork communication, secure data transfer via HTTPS or VPN, and stringent port controls.

Perimeter firewalls are used to 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 MicroStrategy Cloud servers hosting Express.
A multi-tier architecture ensures isolation of application and database components.

SYSTEM SECURITY
Restrictive permissions to files, services, and system settings are applied to all MicroStrategy servers. Access Control Lists (ACLs) are used to limit access. All unnecessary operating system services are removed or disabled before system deployment in the MicroStrategy Cloud Infrastructure. All users are required to authenticate using a unique username and password to access any MicroStrategy Cloud server. An up-to-date antivirus scanner is installed on all MicroStrategy Cloud computers and vulnerability scans are conducted on all computing equipment regularly. Security and other important patches provided by equipment vendors are routinely reviewed and applied by MicroStrategy Information Systems professionals. All virtual machines deployed in the MicroStrategy Cloud Infrastructure 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

IV. Operational Readiness

RISK MANAGEMENT FRAMEWORK
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.

INFORMATION SECURITY PROGRAM
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 SERVEILLANCE
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.

V. 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, Express runs within the MicroStrategy Cloud infrastructure in virtual machines. These VMs provide self-contained operating environments that enable a highly effective redundancy strategy. Redundant VMs are 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.

VI. Contingency Planning
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 will make use of off-site backups to support disaster recovery.

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’ disaster recovery plans.

VII. Conclusion

Express gives control over data to individuals, providing a rapidly deployment process for reporting, at low cost, in the cloud. As the purpose of Express is making life easier for the business user in need of reporting, security has been a critical concern. Express is built on top of the MicroStrategy Cloud which 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 SOC 2 Type I and II, ISO27001, PCI, HIPAA, and others.

Protecting the data of each individual who uses Express is of paramount importance for MicroStrategy. 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. This allows customers to leverage and rely on the MicroStrategy Cloud security infrastructure and focus their efforts, instead, on analyzing data to solve business problems.