MicroStrategy Cloud for Government

SECURITY WHITE PAPER

Table of Contents

Introduction

The MicroStrategy Cloud for Government service is a software-as-a-service (SaaS) offering that MicroStrategy manages on its customers' behalf in Amazon Web Services that includes access to, collectively, (a) the Cloud Platform version of MicroStrategy software products (an optimized version of the MicroStrategy software platform built specifically for deployment in Amazon Web Services) licensed by the customer; (b) Cloud Support, as described below; and (c) Cloud Architecture, as described below. MicroStrategy's SaaS delivery model is designed to allow businesses to consume the MicroStrategy Enterprise Analytics platform in an isolated single-tenant architecture without the need to deploy and manage the underlying infrastructure.

MicroStrategy Cloud for Government offers a distributed compute architecture using cloud-native services provided by Amazon Web Services. As this technology evolves, MicroStrategy continually incorporates new services that allow for increased availability, security, or performance to ensure the latest architecture is available to our customers. At the core of the solution is MicroStrategy—a secure, scalable, and resilient BI and enterprise analytics platform.

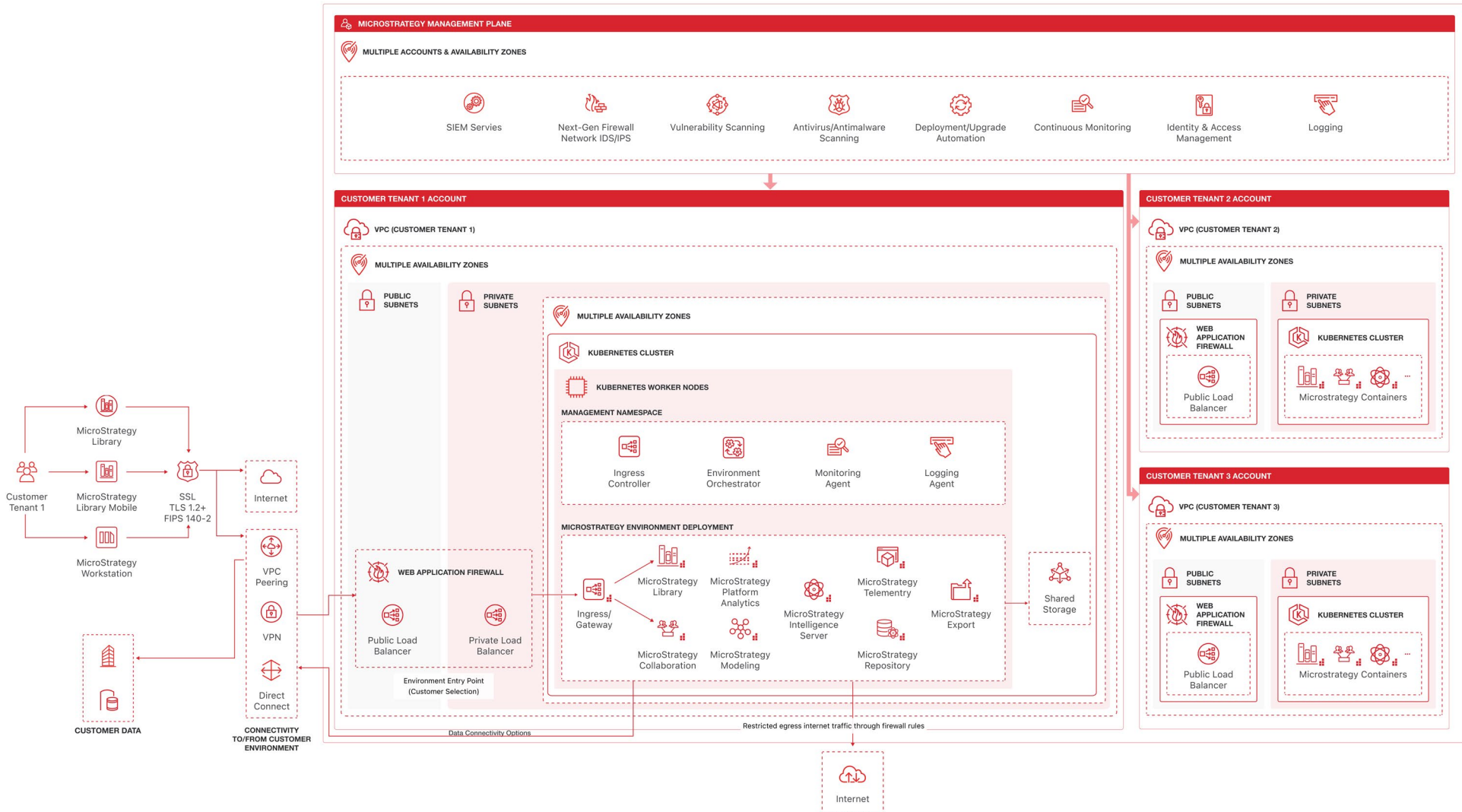
MicroStrategy Cloud for Government also includes the elements needed to operate, access, and manage the intelligence architecture. Users are provisioned with their own dedicated intelligence architecture based on a reference architecture. Once provisioned, users can develop, tailor, and manage the application components to meet their respective needs.

Based on this operating model, customers administer and control their analytics solution while MicroStrategy maintains the supporting cloud-based infrastructure and application upgrades.

Microstrategy Cloud for Government

Cloud Architecture

MICROSTRATEGY CLOUD FOR GOVERNMENT ARCHITECTURE DIAGRAM



Defense-In-Depth and Investment

Whenever possible, multiple controls and technologies are applied to limit the possibility of any single point of failure.

To manage, analyze, and improve security effectiveness, MicroStrategy invests in personnel, tools, and technologies.

Principles of Trust

MicroStrategy's vision is to be the government's trusted cloud analytics SaaS provider, based on the values of maintaining the confidentiality, integrity, and availability of Customer Data. MicroStrategy's methods to fulfill this vision are built upon an executive commitment to maintain and continuously improve the security of the MicroStrategy Cloud for Government.

Microstrategy Compliance Maturity

Federal Risk and Authorization Management Program (Fedramp)

MicroStrategy's information security program for MicroStrategy Cloud for Government is aligned with the FedRAMP requirements at the Moderate impact level. To obtain compliance with FedRAMP, MicroStrategy has conducted a security assessment and authorization activities in accordance with FedRAMP guidance and NIST SP 800-37 Rev. 2. MicroStrategy has documented a System Security Plan (SSP) in accordance with NIST SP 800-18 Rev. 1 for MicroStrategy Cloud for Government service offering. The SSP identifies control implementations for MicroStrategy Cloud for Government and in-scope customer-facing products according to the FedRAMP Moderate baseline. In accordance with NIST SP 800-53A Rev. 5 and FedRAMP Moderate requirements, a third-party assessment organization (3PAO) conducted a security assessment of MicroStrategy Cloud for Government. The security assessment testing determined the adequacy of the security controls used to protect the confidentiality, integrity, and availability of MicroStrategy Cloud for Government and the Customer Data it stores, transmits, and processes. To maintain compliance with FedRAMP, MicroStrategy conducts continuous monitoring, which includes ongoing technical vulnerability detection and remediation, remediation of open compliance-related findings, and annual independent assessments of all security controls.

Security And Compliance

Information Security Governance

Information security governance is a term that encompasses all the tools, people, and business processes an organization uses to ensure the security and privacy of the data that its systems maintain. MicroStrategy's approach to information security governance is structured around the ISO 27001/27002 framework and consistent with the requirements identified in NIST SP 800-53 Rev. 5, and includes many components:

- **Employees** – Employees receive annual information security training. Employees in positions with logical access receive additional role-based training specific to their roles [AT-2, AT-3].
- **Security Staff** – MicroStrategy has dedicated security staff and teams supporting the system [PM-2].
- **Counsel** – MicroStrategy has a team of Privacy Counsel, Compliance, and Government Contracts Attorneys who are responsible for ensuring compliance with global privacy laws, international regulatory regimes, and federal procurement regulations.

- **Assessments** – MicroStrategy regularly conducts both internal vulnerability assessments (for example, architecture reviews by security professionals, vulnerability scans) as well as external third-party audits and external vulnerability assessments [RA-5, SI-2]. Beyond what FedRAMP requires, MicroStrategy conducts full-scope audits every year, which gives us better assurance that the controls are implemented and operating effectively.
- **Policies and Procedures** – Detailed internal MicroStrategy Security Standards dictate how MicroStrategy handles various aspects of the security and compliance governance. Examples include Security Incident Response Plan, MicroStrategy: Access Management Standard, Configuration Management Plan, etc. [IR-1, AC-1, CM-1]

MicroStrategy incorporates security into its development processes at all stages through the MicroStrategy Secure Development Lifecycle. Further, MicroStrategy has integrated a Product Security team in all stages of the secure development lifecycle. From initial architecture considerations to post-release, all aspects of software development incorporate security. The following describes some of the standard practices MicroStrategy employs, which help make it the trusted provider that it is today.

- **Design phase** – Guiding security principles and security training help ensure MicroStrategy engineers make the best security decisions possible. Security representatives are present during sprint reviews and help define security requirements. Threat assessments on high-risk features help to identify potential security issues early in the development lifecycle [SA-3, SA-8].
- **Development phase** – Defined security requirements for high-risk features are incorporated in feature development. MicroStrategy addresses standard vulnerability types using secure coding patterns and anti-patterns and uses static code analysis tools to identify security flaws [SA-10]. Secure code development during design, development, and release is controlled through a secure code repository.
- **Testing phase** – Internal MicroStrategy staff and independent security consultants use scanners and proprietary tools along with manual security testing to identify potential security issues. Further, releases and changes are analyzed in a dedicated test environment [SA-11].
- **Prior to release** – MicroStrategy Security leadership provides sign-off for each release once all security bugs are either closed or have an approved exception. New functionality is verified to ensure security requirements have been met. Code is tested and approved prior to release.

Shared Security and Compliance Model

With MicroStrategy SaaS, data security and compliance are a shared responsibility with customers. While MicroStrategy provides secure and compliant services to protect Customer Data and applications, customers are ultimately responsible for properly configuring and operating those services as required by their organization.

With MicroStrategy Cloud for Government, customers inherit the majority of security controls from MicroStrategy and AWS GovCloud. While customers do bear some responsibility for ensuring security and compliance, MicroStrategy provides numerous enablement resources, including training and implementation guides. Specifically, for customers seeking compliance with FedRAMP Moderate, MicroStrategy provides a Customer Configuration Guide tailored to those requirements. This shared responsibility model greatly reduces both risk and burden for customers, allowing them to place more focus on their business and mission.

Platform Security

MicroStrategy strictly manages access to MicroStrategy Cloud for Government. Before being granted access, employees must pass a thorough MicroStrategy background check [PS-3]. After a person is authorized for logical access, they can access the production environment using secure methods, such as private networks, stringent segregation of duties, and least privilege [AC-2, AC-5, AC-6, IA-2]. With respect to physical security, MicroStrategy uses an infrastructure provided by Amazon Web Services, Inc. (AWS), to host Customer Data submitted to MicroStrategy Cloud for Government customers.

Qualified Personnel

MicroStrategy enforces usage conditions for all personnel with access to MicroStrategy Cloud for Government. Specifically, all personnel must successfully undergo a MicroStrategy background investigation, be U.S. citizens, and are required to access MicroStrategy Cloud for Government from U.S. soil. Further, to obtain production access to the MicroStrategy Cloud for Government, all personnel must go through an enrollment and identity proofing process in accordance with NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing Requirements.

Controls and Database Security

Physical and Environmental Controls

MicroStrategy uses infrastructure provided by a third party, Amazon Web Services, Inc., to host Customer Data submitted to the MicroStrategy Cloud for Government. Each customer's instance is hosted in a dedicated customer account.

MicroStrategy inherits all physical and environmental controls from the pre-existing AWS GovCloud FedRAMP JAB ATO. AWS GovCloud (US) has been granted a JAB ATO for the High impact level. The services within the scope of the AWS GovCloud (US) JAB ATO boundary at High baseline security categorization can be found within AWS Services in Scope by Compliance Program (https://marketplace.fedramp.gov/#/product/aws-govcloud?sort=productName&productNameSearch=AWS).

Data centers are monitored using AWS global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

To detect the presence of water leaks, AWS equips data centers with the functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water to prevent any additional water damage. For further information, visit: https://aws.amazon.com/compliance/data-center/controls/.

Network Protection

MicroStrategy secures its network on many different fronts, for example:

- Transport Layer Security (TLS) cryptographic protocols encrypt network data transmissions between the customer to MicroStrategy, with a preference for TLS 1.2. HTTP Strict Transport Security (HSTS) is enabled by default on all MicroStrategy pages [SC-8(1)].
- Network gateways and firewalls at the external network boundary are configured by default to deny all traffic and allow by exception, filtering unwanted network traffic. If necessary, they apply traffic rate limits. Filter events are logged and monitored for anomalies. [CM-7, SC-7, SC-7(3)].
- AWS Security Groups act as virtual firewalls that restrict and control communication boundaries and prevent unauthorized traffic between services. [SC-7].
- Stateful packet inspection (SPI) firewalls inspect all network packets and prevent unauthorized connections [SC-7].
- Secure routing and traffic flow policies ensure that customer traffic is encrypted entering MicroStrategy until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the MicroStrategy Cloud for Government authorization boundary. Network devices enforce traffic flow policies in the MicroStrategy Cloud for Government [SC-4, SC-5, SC-7, SC-7(3), SC-7(4), SC-8, SC-8(1)].
- Denial-of-Service (DoS) protections are provided by AWS. At the network hardware level, AWS provides industry-leading network DoS and DDoS protections on a 24/7 basis to detect and react to any perceived attacks. Further, MicroStrategy also monitors for DoS at the SaaS layer to guard against resource exhaustion and capacity attacks [SC-5].

Data Connection Security
Logical Access Controls

MicroStrategy secures its network on many different fronts, for example:

- Authorized users are granted production access after manager approval and based on business justification. All personnel with logical access must go through an enrollment and identity proofing process in accordance with NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing Requirements. Terminated users are removed in a timely manner [AC-2] [IA-5].
- Two-factor authentication processes verify the authentication of access requests. Further, authentication is NIST SP 800-63B AAL3 compliant utilizing FIPS 140-2 compliant authenticators [IA-2(1)].
- Segregation of duties and least privilege is enforced to ensure that employees are granted only the necessary level of access to the production network to perform their assigned job functions based on their role [AC-5, AC-6].
- Infrastructure and AWS logging are enabled to capture system activity and logs are forwarded to a central logging system that is located within the authorization boundary [AU-2].

Configuration and Change Management

MicroStrategy implements industry-accepted best practices to harden underlying systems that support the various software layers of the service [CM-2, CM-6]. For instance, hosts are configured with non-default software configurations and minimal processes, user accounts, and network protocols. Hosts log their activity in a remote, central location for safekeeping. MicroStrategy has performed a review of device configurations against industry best practices and required standards for government markets [e.g., Center for Internet Security (CIS) Benchmarks (where available) to ensure devices are configured securely [CM-6, CM-6(1)].

Change Management processes dictate that system changes and maintenance are documented in MicroStrategy's internal ticketing system. Changes require approval, testing, and security impact analysis prior to deployment [CM-3, CM-4]. In addition, any changes that constitute a significant change, per FedRAMP's Significant Change policies and procedures, require analysis and a thorough impact assessment to determine the impact to the MicroStrategy Cloud for Government environment [CA-6].

Operational Monitoring

The MicroStrategy application and website are monitored on a 24x7 basis for reliability and performance. This includes:

- The Cloud Operations team monitors the service and has Subject Matter Experts (SMEs) in various disciplines.
- Overall system monitoring is provided by a variety of tools and alerts are aggregated.
- Monitoring tools are automated and route issues, warnings, and problems to the Information Security team.
- Alerts of significant events are routed to on-call personnel as well as to the Cloud Operation team.

MicroStrategy has built extensive monitoring and instrumentation into the application itself so that the application can accurately report its health and performance to on-call support staff and engineers [IR-2, PM-6].

Security Monitoring

A variety of tools, third-party resources, and a dedicated Information Security Incident Response Team (ISIRT) provide comprehensive monitoring of the MicroStrategy production environment. These include:

- Intrusion Detection Systems (IDS) – IDS monitors the production network for potentially malicious network traffic [AC-4, SC-7, SI-4].
- Logging and Alerting System – Activity logs from production devices and servers are sent to a logging and alerting system within the authorization boundary that reports and alerts on events [AC-2(4), AU-2, AU-6, SI-4].
- Threat Monitoring – The MicroStrategy security team receives and reviews threat alerts from a variety of sources including SANS, United States Computer Emergency Readiness Team (US-CERT), and Open Web Application Security Project (OWASP). Threats that are deemed critical are escalated to the appropriate resource to respond [SI-5].
- Vulnerability and Configuration Scanning – Vulnerability scans are performed at least monthly to check all operating systems, databases, and applications for known vulnerabilities. MicroStrategy also performs operating system and database configuration baseline compliance scanning. Vulnerabilities and misconfigurations are remediated in accordance with established remediation timeframes [RA-5].
- Security Incident Monitoring – The ISIRT monitors for security incidents. Identified security incidents are handled in accordance with the Incident Response Plan [IR-4].

Incident Response

MicroStrategy maintains an Incident Response Plan and has an established Security Incident Response process. MicroStrategy will notify customers promptly in the event that MicroStrategy becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may be made by any of the following methods: phone contact by MicroStrategy support, email to customer's administrator, and Security Contact (if submitted by customer). [IR-4, IR-6, IR-8].

MicroStrategy Cloud for Government customers can report security incidents related to their MicroStrategy products and offerings via **security@microstrategy.com**. MicroStrategy will respond in accordance with the incident response process.

Disaster Recovery and Backup

Standard Disaster Recovery (DR) routines allow for backups and system state data with storage spanning AZs. MicroStrategy develops, documents, and disseminates a comprehensive set of procedures for implementing DR and contingency planning activities for the MicroStrategy Cloud. Each MicroStrategy Cloud for Government deployment includes an intra-region DR zone such as within the AZs in the AWS region in use. Paid Professional Services are available for customers in which specific automation and routines are configured so all Customer Data is collected and copied to an alternate region.

The procedures have been developed for a Moderate impact system and are designed to recover the MCGs essential missions/business functions within the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) as mentioned below when the primary processing capabilities are unavailable.

- Recovery Time Objective (RTO) of 48 hours: RTO is the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and supported mission/business processes.
- Recovery Point Objective (RPO) of 24 hours: RPO is the maximum tolerable period in which data might be lost from an IT service due to a major incident.

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

Platform and Application Security

MicroStrategy Cloud for Government provides extensive features and tools that provide security for the data generated by customers. Customers can use many of these features to implement security policies governing exactly who, what, from where, when, and how users can access specific IT applications and data and meet related auditing requirements.

The default user authentication mechanism for MicroStrategy Cloud for Government requires MFA single sign-on mechanisms to simplify and standardize user authentication across a portfolio of applications [IA-2(1), IA-5, IA-5(1)]. MicroStrategy Cloud for Government supports two single sign-on (SSO) options:

- Federated authentication using Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) allows a session to send authentication and authorization data between affiliated but unrelated Web services.

Customers can implement multi-factor authentication by integrating with one of MicroStrategy's SSO capabilities [IA-2(1)]. Specifically, customers who require user authentication via Government-issued smart cards, such as a Common Access Card (CAC) or Personal Identity Verification (PIV) card, can implement federated authentication to authenticate users via a SAML assertion or OIDC token generated by their identity provider (IdP).

User authentication and identity confirmation determine who can log in, and network-based security features limit the time and location from where users can log in. When an organization imposes IP address restrictions and a connection request originates from an unknown address, the connection is denied, helping protect data from unauthorized access and phishing attacks [SC-7(3), SC-7(4)].

To protect established sessions, MicroStrategy Cloud for Government monitors and terminates idle sessions after a configurable period of time. Session security limits help defend system access when a user leaves his/her computer unattended without first disconnecting [AC- 11].

MicroStrategy Platform has a robust security model that enables you to create users and groups, determine how they are authenticated, control what data they can see, and what functional privileges they can have. Security filters further enable you to control what warehouse data users can see and access.

Logical Security

MicroStrategy Cloud for Government's innovative single-tenant architecture delivers operational and cost efficiencies for cloud-based applications with further strengthening the security of each organization's information.

Data Ownership and Retention

Protecting PII and Privacy

MicroStrategy has conducted a Privacy Impact Assessment (PIA) for the delivery of the MicroStrategy service. The MicroStrategy service is rated as a Moderate impact system. As such, MicroStrategy has implemented security controls aligned with the FedRAMP Moderate security baselines and which are assessed against both by an independent third-party assessor at least annually [PL-5].

Customers are responsible for conducting their own PIA for Customer Data stored in MicroStrategy. NIST SP 800-60 provides guidance to organizations on categorizing an information system, and states that for PII, the confidentiality impact level should generally fall into the Moderate range. MicroStrategy recommends that federal agencies relying on our FedRAMP P-ATO determine the Security Categorization of their data to ensure the data stored in MicroStrategy does not exceed the Moderate impact level [PL-5].

As outlined in the previous sections, MicroStrategy Cloud for Government has numerous configurable security features that allow customers to customize security based on the sensitivity of the data customers store in the application, consistent with the FedRAMP requirements for Moderate impact systems.

Return or Deletion of Customer Data

Due to the nature of the MicroStrategy Cloud for Government Service, MicroStrategy's External Service Provider provisions Customer with controls that Customer may use to retrieve or delete Customer Data. Up to the termination of the master agreement between Customer and MicroStrategy (Governing Agreement), Customer will continue to have the ability to retrieve or delete Customer Data in accordance with this section. For 30 days following that date, Customer may retrieve or delete any remaining Customer Data from the MicroStrategy Cloud for Government environment, subject to the terms and conditions set out in the Governing Agreement. MicroStrategy will delete Customer Data when requested by Customer through the MicroStrategy Cloud for Government Service controls provided for this purpose.