MICROSTRATEGY CLOUD SECURITY WHITE PAPER

DELIVER BEST-IN-CLASS SECURITY WITH THE MICROSTRATEGY CLOUD ENVIRONMENT (MCE)

MicroStrategy
Intelligence Everywhere

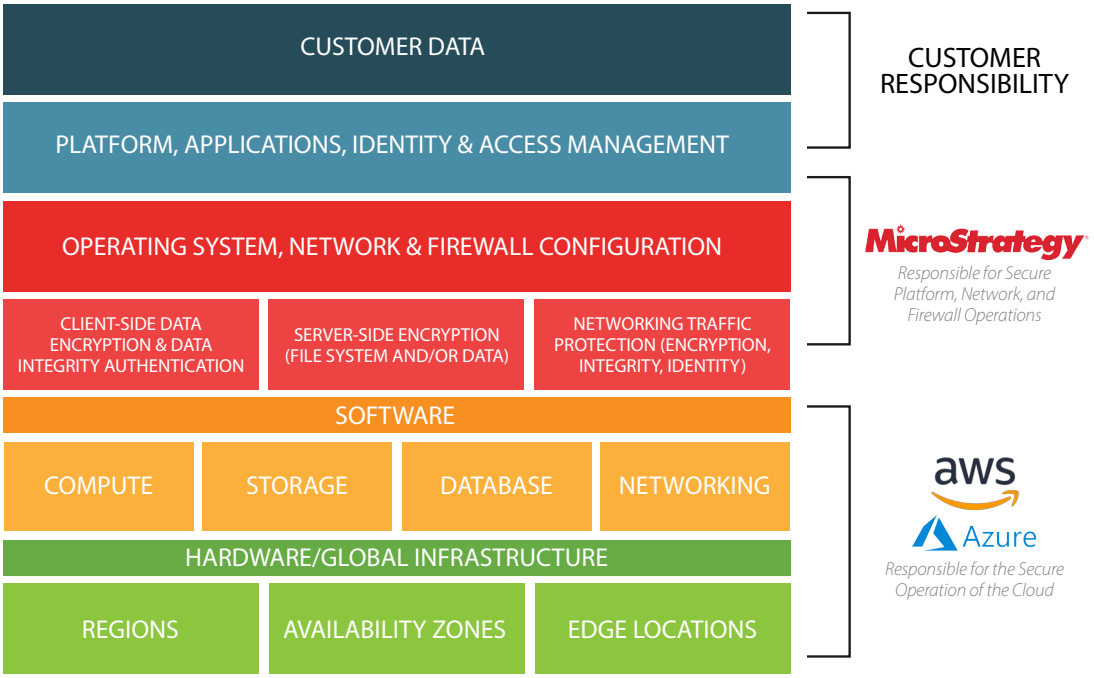
Contents

Introduction

The MicroStrategy Cloud Environment (MCE or MicroStrategy Cloud) is a platform-as-a-service (PaaS) offering that MicroStrategy manages on its customers' behalf as a unique Amazon Web Services (AWS) or Microsoft Azure implementation. MCE features a fully optimized version of the MicroStrategy Intelligence Platform built specifically for deployment in a customer-licensed AWS or Azure environment. Further, MicroStrategy's PaaS delivery model enables businesses to consume the platform in a single tenant architecture without the need to deploy and manage the underlying system infrastructure.

MCE is built on a distributed compute architecture using either AWS or Azure cloud-native services to provide customers with a secure operating environment for their analytics deployment. As this technology evolves, MicroStrategy continually incorporates new services to deliver increased availability, security, and performance within MCE. Through routine upgrades that are also delivered through this PaaS offering, our experts ensure that customers are leveraging the latest version of our fully optimized architecture and its associated enhancements.

MCE also provides customers the ability to operate, access, and manage the intelligence architecture and applications built upon it. Users are provisioned their own dedicated intelligence environment based on our cloud-optimized reference architecture. Once provisioned, users can develop, tailor, and manage the underlying application and data components to meet their respective needs with full functional parity of the features, capabilities, and services available in the MicroStrategy platform.



With this PaaS operating model, MicroStrategy Cloud customers administer and control the platform, the solutions built upon it, and the data those applications present. MicroStrategy maintains the supporting platform and cloud infrastructure on behalf of its customers.

MCE Architecture

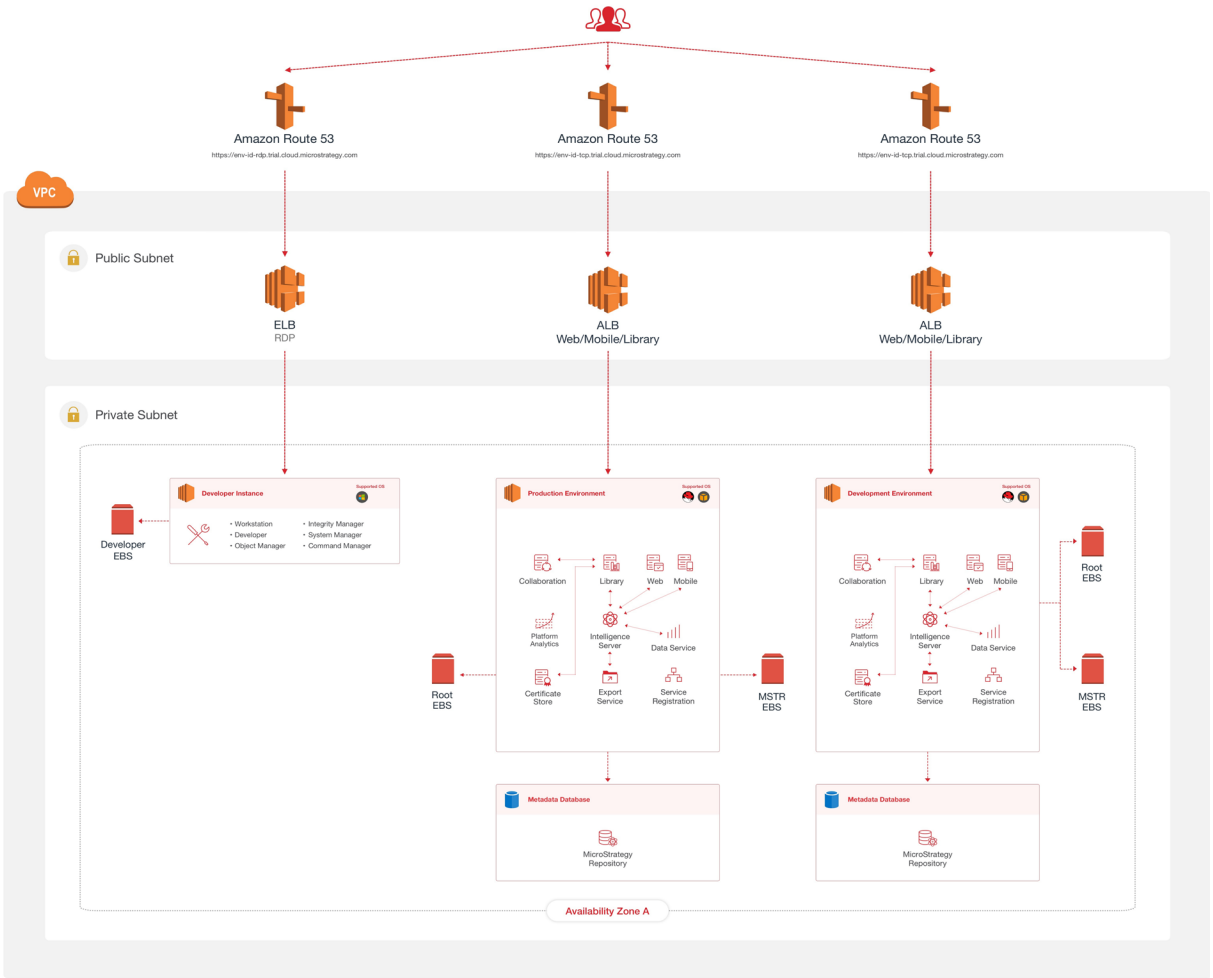
The MicroStrategy Cloud offers an optimized cloud architecture developed over years of partnership with AWS and Azure. As previously described, MCE features a fully optimized version of the MicroStrategy platform in a single-tenet architecture built specifically for each unique MCE deployment within a customer-licensed AWS or Azure environment.

MCE utilizes public cloud service providers to provide the physical infrastructure-as-a-service (IaaS) components of its solution architecture. When leveraging both the AWS and Azure IaaS models, MicroStrategy platform nodes are deployed across a set of availability zones to ensure high uptime and performance. Additionally, a dedicated customer account for every MCE deployment is provided for the exclusive use of the customer which provides logical isolation and separation from other MCE customers.

AWS Deployment Overview

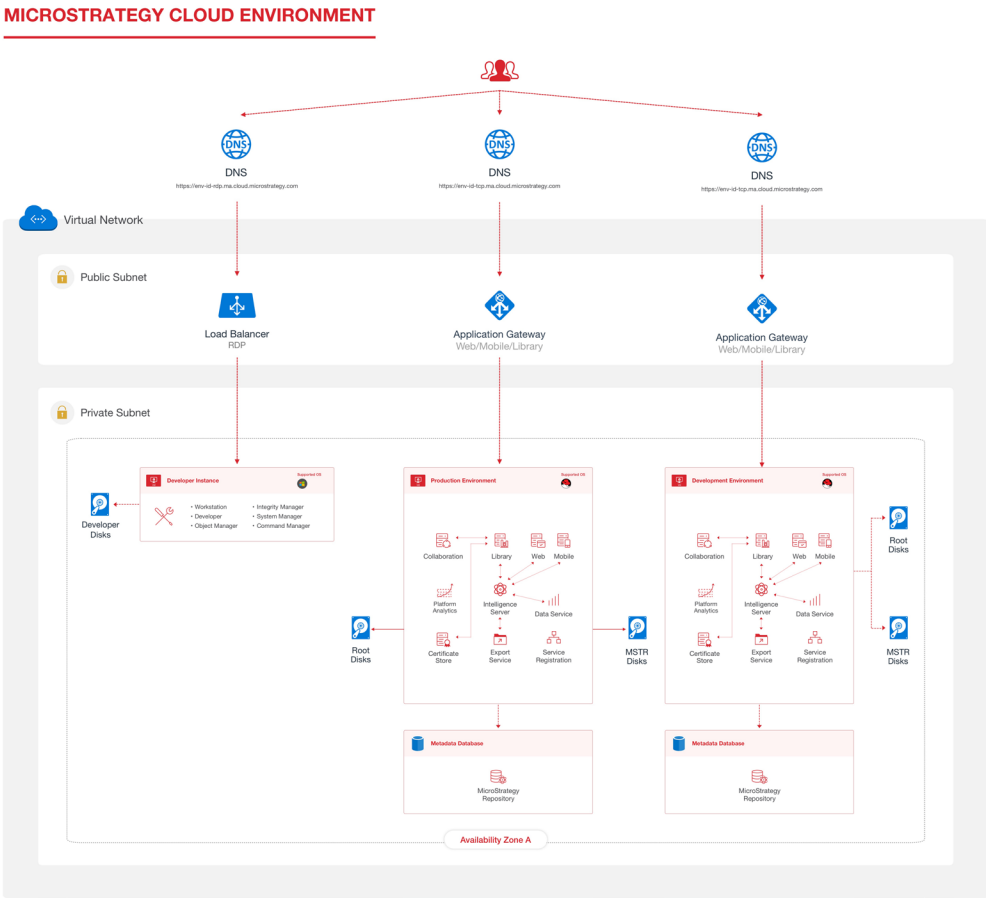
For customers whose MCE deployment is operated on the AWS IaaS public cloud, a cluster of up to eight nodes for the MicroStrategy Server components using Linux is deployed within a unique AWS Virtual Private Cloud (VPC) instance.

MICROSTRATEGY CLOUD ENVIRONMENT



Azure Deployment Overview

Similarly, the MCE offering for Azure deploys a cluster of up to eight nodes of MicroStrategy Server components using Linux into a specific customer-specific subscription account. Further, Azure Net App files are used to accommodate shared storage across the cluster of machines.



Asset Management

MicroStrategy maintains an inventory of all MCE information system components using native public cloud provider management consoles and third-party security tools to catalog all aspects of AWS and Azure virtual machine image instances. Customers may request collaborator access to public cloud consoles to view their virtual assets but are restricted by policy to read-only permissions.

Instance Segregation

MicroStrategy implements and wholly manages a unique virtual private cloud instance for each MicroStrategy Cloud customer. This unique instance serves as a dedicated virtual network and computing environment for each individual account that is logically isolated from the deployments of all other MCE customers. MicroStrategy can launch resources into customer virtual private clouds, as well as create and/or configure internet protocol (IP) address ranges, route tables, network gateways, and security settings as appropriate. Additionally, a customer's unique deployment is established with hypervisor-level firewalls, or security groups, that use cloud and virtualization software to further segregate MCE instances into wholly separated, client processing environments that restrict unauthorized access to all non-public information and/or system components.

Information Security Governance

Information security governance is the management of systems, people, tools, and processes to ensure the optimal security is maintained across the entire ecosystem. Because cloud computing involves multiple layers of providers and users, an effective security posture requires commitment to governance at all levels of the organization.

MicroStrategy is committed to maintaining the highest levels of security on behalf of its customers. Its MCE governance and security controls are structured around the ISO 27002 framework, NIST SP 800-53 requirements, and various management systems and protocols as described below.

Information Security Policies

MicroStrategy develops, documents, and disseminates an organizational information security policy to comprehensively govern its corporate security posture. This policy aligns to the platform's enterprise architecture, is structured on industry recognized frameworks, and is defined by the industry best practice governance standards for information security noted above. MicroStrategy management reviews and updates these policies at least annually, or after any significant changes to the service offerings in the context of the technology landscape.

Organizational Alignment

MicroStrategy maintains a dedicated and independent information security team to provide security insights, manage controls, and identify priority enhancements for MCE. This team reports directly to the Chief Information Security Officer (CISO) and is structured within a clearly defined operating model designed to facilitate direct, cross-functional communication about key areas of authority, responsibility, and lines of reporting to all personnel involved in the design, development, implementation, operation, maintenance, and monitoring of the MCE ecosystem.

Organizational charts to support this operational framework are readily available, regularly communicated to employees, and updated as needed. Individual responsibility and accountability in relation to maintaining the stringent information security posture empowered by this operating model are defined through formal job descriptions, regular performance reviews, and explicit acknowledgment of understanding of individual obligations.

Segregation of Duties

MicroStrategy follows least privileges and needs access principles to separate roles and responsibilities among the different functional teams administering and operating each MCE deployment on behalf of our customers. MicroStrategy employees a full-time information security team that is separated from the Cloud Operations and Support teams. It maintains a segregation of duties policy which outlines each management team's responsibilities for adhering to the principles set forth therein and defines the job descriptions and responsibilities for each role.

Personnel Qualifications

MicroStrategy follows a formalized hiring practice which verifies that all potential new employees or internal transfers are qualified for the responsibilities of their job functions. Human resources conducts and verifies background checks on all new employees and contractors. Upon acceptance of employment, employees are required to acknowledge receipt and understanding of compliance with the MicroStrategy code of conduct, security, and confidentiality policies. Current copies of policies are available to all employees on the company intranet.

MicroStrategy requires that newly hired personnel, including employees, interns, and contractors, who support the MicroStrategy Cloud receive and acknowledge security awareness training related to organizational privacy and security requirements. This training and acknowledgement is facilitated by MicroStrategy's learning management system and requires recertification at least annually thereafter.

MicroStrategy prioritizes security by enforcing rigorous requirements for all personnel.

- ☑ Pre-offer technical assessment
- ☑ Pre-hire background check
- ☑ Onboarding InfoSec training
- ☑ Code of Conduct acknowledgment
- ☑ Annual renewal of security training

Best-in-Class Security

MicroStrategy operates a dedicated internal compliance team to ensure that industry best practice processes are continuously maintained, enhanced, and verified. This compliance team has established extensive data protection and privacy policies and procedures to ensure strict compliance with General Data Protection Regulation (GDPR) requirements. It also works closely with its legal department to ensure complete compliance with regulatory requirements across local and federal laws in every jurisdiction in which the MicroStrategy Cloud is offered.

Compliance Certifications

MCE for both AWS and Azure fully complies with the risk management and information security frameworks listed below. This compliance is verified, and certified where appropriate, by way of comprehensive assessments performed at least annually by qualified third-party and internal resources.

The MicroStrategy Cloud complies with each of the following industry-recognized certifications, accreditations, and regulations.

General Data Protection Regulation

AICPA SSAE-18, System and Organization Controls – SOC 2 Type 2 Report

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 (ISO 27001:2013) – Certificate Number: 1004041-4

Payment Card Industry Data Security Standard (PCI DSS), Self-Assessment Questionnaire, Type D (SAQ-D), for Service Providers, Version 3.2.1

Privacy Shield EU-Swiss and Swiss-US

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Self-Assessment

Data Security

MicroStrategy recognizes the importance of data privacy for our customers and their end users. To maintain the utmost levels of data privacy, protection, and handling, its compliance and legal teams have developed comprehensive privacy controls to restrict the level of personal information visible and accessible to employees who manage MicroStrategy Cloud environments on our customers' behalf.

Data Privacy

Personnel responsible for operating the MicroStrategy Cloud as a fully managed PaaS solution adhere to all regulatory data privacy regulations such as GDPR, California Consumer Privacy Act of 2018 (CCPA), and similar local equivalents in markets where our fully managed cloud service is offered.

Please review our publicly accessible privacy policy for more information.

Data Protection

The MicroStrategy Cloud encrypts data across all virtual instances and backup environments by leveraging native encryption tools and key management systems from public cloud service providers. These encryption protocols are applied by default both in-transit and at-rest for all data located within or surfaced by MCE components.

Data In-Transit

MicroStrategy implements industry best practice cryptography techniques to protect any data transmitted to and from the MicroStrategy Cloud. In-transit data is encrypted by using internet protocol security (IPsec) and/or secure socket layer (SSL) virtual private network (VPN) gateways, which is implemented using industry standard encryption algorithms to meet or exceed minimum bit strengths. MicroStrategy maintains SSL certificates for customers as part of the managed service and can implement customer issued certificates if required.

Data At-Rest

MicroStrategy utilizes industry standard cryptography (AES-256) to protect and secure data at rest anywhere within MicroStrategy Cloud boundaries. To accommodate requirements for MCE customers that process protected forms of personally identified information (PII), electronic protected health information (ePHI), or are considered covered entities, MicroStrategy rigorously evaluates the platform to validate that PII and ePHI is not stored in persistent servers in the data centers.

Due to the architecture of the MicroStrategy platform, if a customer chooses to utilize caching and intelligence cube capabilities, then application data files that are at-rest are backed up on MicroStrategy-managed Intelligence Servers for a minimum period of five days. Due to data privacy considerations, MicroStrategy does not have visibility into the data stored in MCE by the customer. Therefore, MCE customers are responsible for ensuring that these files are encrypted to meet those requirements in accordance with applicable compliance standards and regulations.

Data Handling

Significant measures are taken to ensure that customers retain complete ownership of their data when using the MicroStrategy Cloud.

Data Control Requirements

MCE customers and administrators from the MicroStrategy Cloud team share the responsibility of determining the appropriate controls for the types of data utilized within MCE. These requirements are captured, discussed, and implemented during the MCE onboarding process, and reassessed regularly throughout the lifecycle of each individual MCE instance, to ensure continued alignment.

Data Access Restrictions

MCE customers retain full ownership of their data. MicroStrategy personnel who administer MCE do not have visibility into customer data to perform data identification or classification, and may not access customer data without formal customer authorization through a cloud support case. To maintain data access restrictions, MicroStrategy Cloud team members utilize a restricted role within MCE, enforced by access control lists (ACLs) that the customer can view, that allow the appropriate personnel to fully manage the deployment while prohibiting access to customer data.

Data Storage

MicroStrategy is deeply committed to maintaining customer data privacy. MCE customer data is not stored in any on-premises environment outside of that individual MCE instance. Secure media handling and destruction procedures are inherited from MCE public cloud IaaS providers.

Data Deletion

MicroStrategy regularly assesses the IaaS provider's attestation of compliance for adherence to secure data deletion principles and processes. When a contract termination occurs, MicroStrategy allows a 90-day period during which the customer's MCE administrators can validate that all data migration has been completed.

Once we receive confirmation from the customer, all customer data and any possible copies are completely deleted by MicroStrategy. Alternatively, if the customer prefers, MicroStrategy can provide guidelines to enable customer administrators to personally delete all relevant data. In either case, customers may request use of electronic discovery capabilities to demonstrate that all data has been deleted.

System Acquisition, Development, and Maintenance

Best practice security principles are integrated into all phases of its system development lifecycle (SDLC) for the MicroStrategy Cloud. These security principles are implemented both through the MCE systems design itself, as well as through specific activities required for key lifecycle milestones. Successful development, deployment, maintenance, and optimization of the MicroStrategy Cloud relies on robust security principles, protocols, and procedures integrated throughout all stages of the SDLC.

Steady State Protocols

- Organizational security standards with individual acknowledgment requirements
- Routine training to ensure personnel make security-appropriate decisions throughout the design and architecture phases of the development lifecycle
- Dedicated use and maintenance of unique development, testing, and production environments to ensure production data is never available to unauthorized users or utilized outside of the appropriate environment

Requirement Analysis and Risk Assessment

- Regimented review and approval of all proposed changes through our governed change management process, which is administered by an internal change control board (CCB) that meets weekly
- Regular, proactive MCE risk assessments conducted to continually evaluate potential and confirmed threat considerations and impacts
- Identification of appropriate risk management solutions for any identified vulnerabilities or issues

Testing and Quality Assurance (QA) Procedures

- Use of secure design and coding best practices for all new development and CCB-approved changes
- Robust security testing requirements prior to deployment to ensure a high degree of confidence that the resulting product or board-approved changes do not contain security vulnerabilities
- Application of a suite of security tools throughout the development lifecycle for source code scanning, binary code scanning, internal penetration testing, and third-party independent penetration testing to identify vulnerabilities identified by, but not limited to, the OWASP Top 10 or the Sans-25
- Instance security scanning prior to automated version releases to ensure that each updated deployment is current on all security and operating system updates

Configuration Management

The MicroStrategy Cloud utilizes hardened machine images that align to defined and proprietary baseline configuration documentation to determine the necessary functions, ports, and services used by the platform, and to disallow use of all others by default. MCE also leverages automation tools to deploy consistent hardened instances and prevent any pre-deployment tampering or modification to these images. Baseline configurations are reviewed and reassessed at least annually. Implementation of any additional ports, protocols, and services requested by the customer require formal review and approval by the MicroStrategy CCB.

Change Management

MicroStrategy documents any proposed changes to its cloud offering within a secure, internal ticketing system. Change request tickets must outline detailed descriptions, implementation steps, impact assessments, backout procedures, and requisite approvals for each proposed change.

Every proposed change must be reviewed and approved prior to implementation by the CCB, comprised of senior technical leaders spanning the Information Security, IT Operations, Cloud, and Support teams.

Upon CCB approval, MCE changes are implemented either during standard maintenance windows or during time periods pre-approved by the customer. A post-deployment QA validation is performed for each change to ensure system functionality and integrity are maintained once implemented.

Vulnerability Management

MicroStrategy develops, documents, and disseminates a set of procedures for implementing vendor-provided security patches, quick-fix engineering, and updates for Microsoft Windows- and Unix-based system components that support MCE. MicroStrategy Cloud personnel implement these procedures at least once monthly within a schedule maintenance window. If critical or zero-day vulnerabilities are identified, MicroStrategy works with individual customers to establish an emergency maintenance windows in which to update or patch the vulnerability within each unique MCE deploin a timely manner.

Vendor Management

MicroStrategy performs extensive vetting activities with all vendors before permitting system access or engaging in its offered services. Due diligence activities include risk assessments, attestations of compliance reviews, vendor staff resume screening, and regular reassessments to ensure that the individual personnel at each vendor adhere to and continually comply with the same regulations, requirements, and standards that MCE is required to maintain on behalf of its customers. Additionally, MicroStrategy requires all vendors to read, and acknowledge understanding of, all applicable access control policies and procedures required to perform applicable duties.

Physical Security

As the IaaS providers for the MicroStrategy Cloud architecture, AWS and Azure are responsible for establishing and maintaining physical access control systems (PACS) to restrict data center access to properly authorized individuals within any locations that house the offline storage, backup data, recovery infrastructure, and all media including portable media for hosted systems.

Attestations of Compliance

MicroStrategy reviews the service providers' attestations of compliance to its corporate security requirements at least annually. These attestations of compliance describe in detail the shared responsibilities between MicroStrategy and the service providers that are implemented and maintained to protect and ensure the highest security standards for the MCE offering.

Refer to these vendor links for additional information on physical security measures.

AWS Data Center Controls

Azure Physical Security

Communication Security

MicroStrategy strictly governs and controls all communications across its cloud system components to secure each MCE deployment against unwanted intrusion and enable rapid detection and response should any attempts occur.

Network and Boundary Security

MicroStrategy subscribes to the IaaS public cloud provider's distributed denial of service (DDoS) protection and mitigation services to alert, prevent, and mitigate attacks against the MCE platform. MicroStrategy also implements web application firewalls (WAFs) within each customer's unique account or subscription to provide additional application layer protection.

Refer to these vendor links for additional information about network and boundary security measures.

AWS Shield

Azure DDoS Protection

System Firewalls

The MicroStrategy Cloud leverages native tools from the IaaS provider to implement hypervisor-level web application firewalls (WAFs), security groups, or network devices to protect the virtual private cloud MCE deployment for each unique customer. All such protective components are set by default to deny all firewall changes to ensure that such requests are formally submitted, reviewed, and approved via CCB prior to implementation. Customers may acquire additional next generation firewalls, such those offered by Palo Alto Networks, for implementation within MCE deployments upon request.

Ingress and Egress Workflows

Certain ingress and egress workflows are required to maintain boundary security between the customer and MCE networks. MicroStrategy requires private subnet egress on the TCP port 443*.cloud.MicroStrategy.com. Network traffic restrictions are also recommended for specific customer IP ranges so access is allowed only through a VPN tunnel established directly with the customer.

Data Connection Security

MicroStrategy requires connectivity to customer data sources via a VPN, dedicated, or peering connection. Secure data source connections with the MicroStrategy Cloud may be established in one of three ways.

VPN connections establish a direct site-to-site IPsec tunnel to connect and communicate with on-premises data sources.	Dedicated connections establish a direct line of communication between the on-premises data center and an MCE AWS VPC or Azure VNet deployment.	Peering connections establish a direct line of communication between different MCE AWS VPCs or Azure VNet deployments.
AWS VPN	AWS Direct Connect	AWS VPC Peering
Azure VPN Gateway	Azure Express Route	Azure VNet Peering

Intrusion Detection and Prevention

MicroStrategy deploys a host-based intrusion detection system (IDS) to detect and assess potential intrusion into any managed instance, compare network traffic to known malware signatures and behaviors, and support real-time monitoring and alerting that triggers additional analysis and investigation of specific events as appropriate. The previously mentioned WAFs are configured in IPS mode to proactively block and prevent intrusion activity.

Operational Security

The MicroStrategy Cloud team that administers and maintains each MCE deployment on the customer's behalf conducts all operational activities according to strict protocols to ensure the highest levels of security are always maintained.

Access Control

The MicroStrategy Cloud leverages centralized directory services and automated technical solutions to provision, monitor, modify, or revoke privileged user accounts established for each unique deployment. These MCE components provide systems administrators, database administrators, and other authorized personas the ability to strictly control access to each environment.

Multi-Factor Authentication

MicroStrategy requires that all remote access to corporate systems, and privileged access to MCE deployments, are protected by multi-factor authentication (MFA). Within the application layer, customers may also choose to integrate with their own MFA solutions for their end users.

Access and Audit Logging

MicroStrategy centralizes auditing and logging for all systems monitoring and user activity using a third-party SIEM tool that aggregates, reviews, stores, secures all log information. The service associated with this tool provides 24x7 monitoring and alerting services and immediately notifies MicroStrategy Information Security personnel of any suspicious activity.

Antivirus and Anti-Malware Use

Antivirus and anti-malware software are used to detect, identify, and prevent the introduction of malicious software from the MicroStrategy Cloud and its associated systems. MicroStrategy utilizes a centrally hosted and managed solution that provides continuous monitoring and endpoint detection and response (EDR) capabilities.

The MicroStrategy Cloud implements strict access controls to ensure stringent access governance across all users.

- ☑ Unique ID assignments for all privileged users
- ☑ Multi-factor authentication (MFA) requirements for access to all remote and privileged systems
- ☑ Use of a centrally managed organizational security and information event management (SIEM) tool to monitor privileged user ID activity spanning access attempts and all system interactions
- ☑ Lock out of privileged user IDs for at least 30 minutes occurs after 5 contiguous unsuccessful access attempts or by direct intervention by organizationally approved groups or roles
- ☑ CCB approval requirements for any privileged user ID additions, modifications, or deletions
- ☑ Disabling of inactive privileged user accounts automatically after 90 days
- ☑ Immediate access revocation for all terminated privileged users

Security Monitoring

MicroStrategy uses an array of public cloud and third-party security monitoring tools and dashboards to provide comprehensive monitoring of the MicroStrategy Cloud. A dedicated Information Security team analyzes and responds to all alerts in a timely manner, and regularly reviews received alerts with management to determine appropriate actions to prevent and remediate risks of future issues.

Vulnerability Scanning

The MicroStrategy Cloud employs extensive vulnerability scanning and analysis across all levels of its technology stack. MicroStrategy assigns fully qualified internal resources and leverages automated technical solutions to conduct internal vulnerability scans at least once weekly in accordance with industry-accepted best practices. When applicable, qualified internal resources perform remediation scans until all requirements are met.

MicroStrategy also utilizes a reputable third-party provider to conduct quarterly external vulnerability scans in accordance with industry-accepted guidelines. In addition to quarterly reviews, within 30 days this third-party provider performs remediation scans until all requirements for a passing scan are met.

Penetration Testing

MicroStrategy also enlists the services of a qualified third-party provider to perform penetration testing services for MCE, complete security reviews of the platform application and network boundary, tests ingress and egress controls, and test isolation and segregation controls. When applicable, this third-party provider performs remediation scans within 30 days until all requirements are met.

Business Continuity

MicroStrategy operates a comprehensive business continuity and disaster recovery (DR) program to minimize event-based impact to the people, processes, systems, and technology governed by its information security management protocols, and to ensure rapid and efficient post-event recovery. In conjunction with the other organizational initiatives described in this document, this integrated program constitutes a critical aspect of the comprehensive value MCE offers to customers by enabling the MicroStrategy Cloud team to ensure the highest levels of business continuity on their behalf.

Incident Response

MicroStrategy implements a coordinated incident response process to effectively identify and resolve any security incidents involving MCE information systems and associated data for these environments. MicroStrategy implements detective measures to identify potential security incidents and determine severity and impacts in a coordinated manner, and to ensure all incidents are properly investigated and tracked to resolution by trained security personnel.

Incident Notification

If a confirmed security incident impacts an MCE customer, the MicroStrategy Cloud team will promptly notify the affected customer based on respective contractual obligations and in accordance with established incident response plan policies and procedures, unless otherwise delayed by direction from law enforcement.

Post-Closure Analysis

Closed incidents are routinely reassessed to identify systemic security weaknesses, threats, vulnerabilities, and any trends that can help the MicroStrategy Cloud team perform preventive measures that may proactively decrease occurrence of specific incidents.

Disaster Recovery

MicroStrategy develops, documents, and disseminates a comprehensive set of procedures for implementing DR and contingency planning activities for the MicroStrategy Cloud. Each MCE deployment includes and intra-region DR zone such as within the Availability Zones in the AWS and Azure region in use. The operating model for the MicroStrategy personnel administering the MCE deployment on each customer's behalf is designed to enable meeting a 24-hour Recovery Point Objective (RPO) and 48-hour Recovery Time Objective (RTO) respectively.

Additional Information:

We encourage you to review our publicly accessible MicroStrategy Cloud Environment Service Guide for further information about MCE administration, maintenance, support, SLAs, and terms applicable to processing personal data. The latest version of this document is available on the terms page of the MicroStrategy website.

1850 Towers Crescent Plaza | Tysons, VA 22182

COLL-2241 0521