Strategy₿

WHITEPAPER

Cloud Security

Deliver best-in-class security with the Strategy Managed Cloud Enterprise

Table of Content

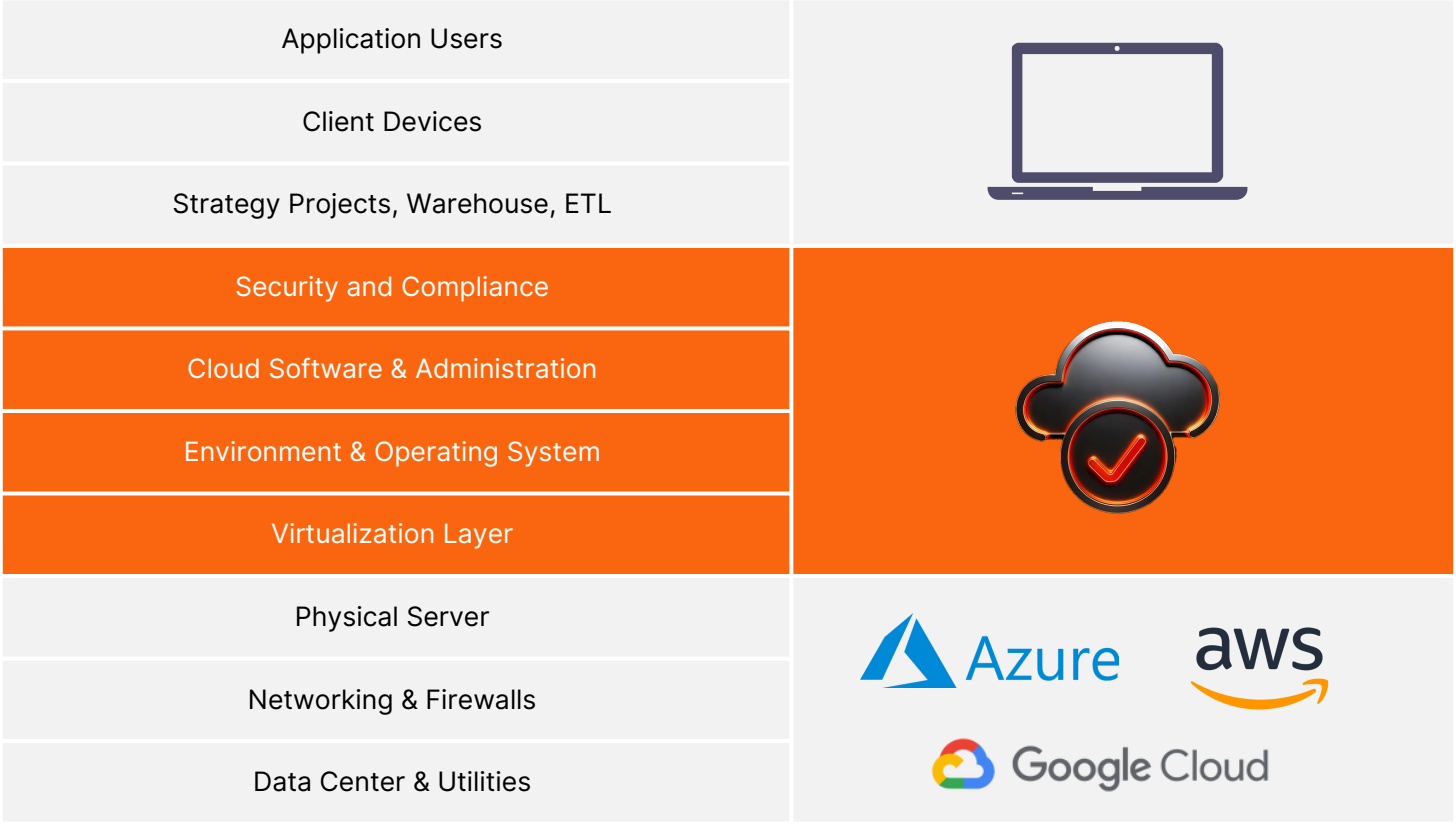
Introduction

The Strategy Managed Cloud Enterprise (MCE or Strategy Cloud) is a software-as-a-service (SaaS)| offering that Strategy manages on its customers' behalf as a unique Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP) implementation. MCE features a fully optimized version of the Strategy Intelligence Platform built specifically for deployment in a customer-licensed AWS, Azure or GCP environment. Further, Strategy's SaaS delivery model is designed to allow businesses to consume the Strategy Enterprise Analytics platform in a single-tenant architecture without the need to deploy and manage the underlying infrastructure.

MCE is built on an architecture using either AWS, Azure or GCP cloud-native services to provide customers with a secure operating environment for their analytics deployment. As this technology evolves, Strategy 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 MCE - a secure, scalable, and resilient BI enterprise analytics platform integrated with the latest artificial intelligence (AI) capabilities.

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

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



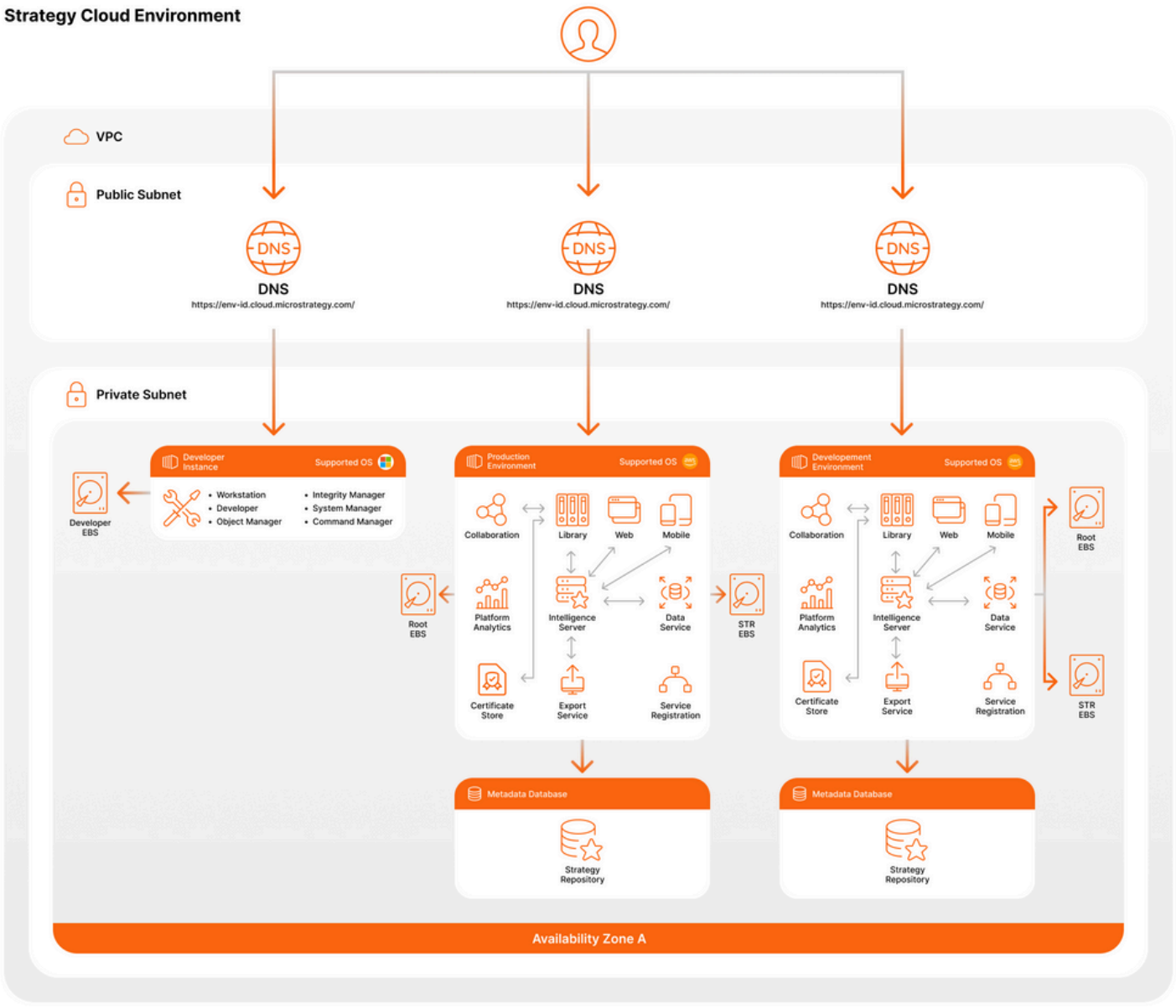
MCE Architecture

With the release of Strategy One in early 2023, Strategy's platform has been completely refactored leveraging a modern cloud-native containerized microservices architecture. Strategy is available on-prem and within AWS, Azure and GCP providing customers with agility and freedom of choice to support their evolving business needs. As previously described, MCE features a fully optimized version of the Strategy platform in a single-tenant architecture built specifically for each unique MCE deployment within a customer-licensed AWS, Azure or GCP environment.

MCE utilizes public cloud service providers (CSPs) to deliver the physical infrastructure-as-a-service (IaaS) components of its solution architecture. When leveraging the AWS, Azure and GCP IaaS models, Strategy platform nodes can be 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 ensures logical isolation from other MCE customers.

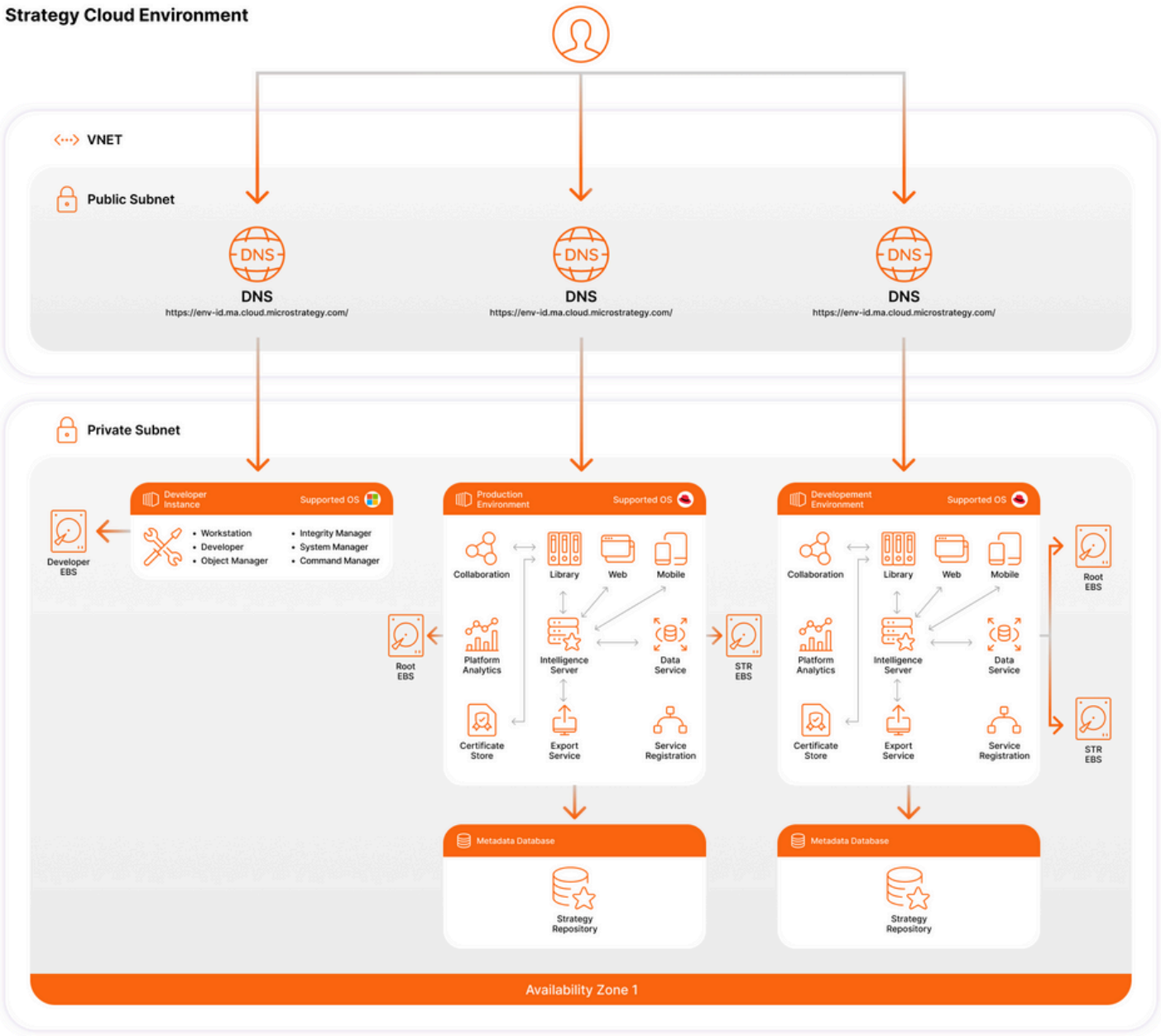
AWS Deployment Overview

For customers utilizing the AWS public cloud for their MCE deployment, a dedicated cluster of Strategy Server components is established within a unique AWS Virtual Private Cloud (VPC).



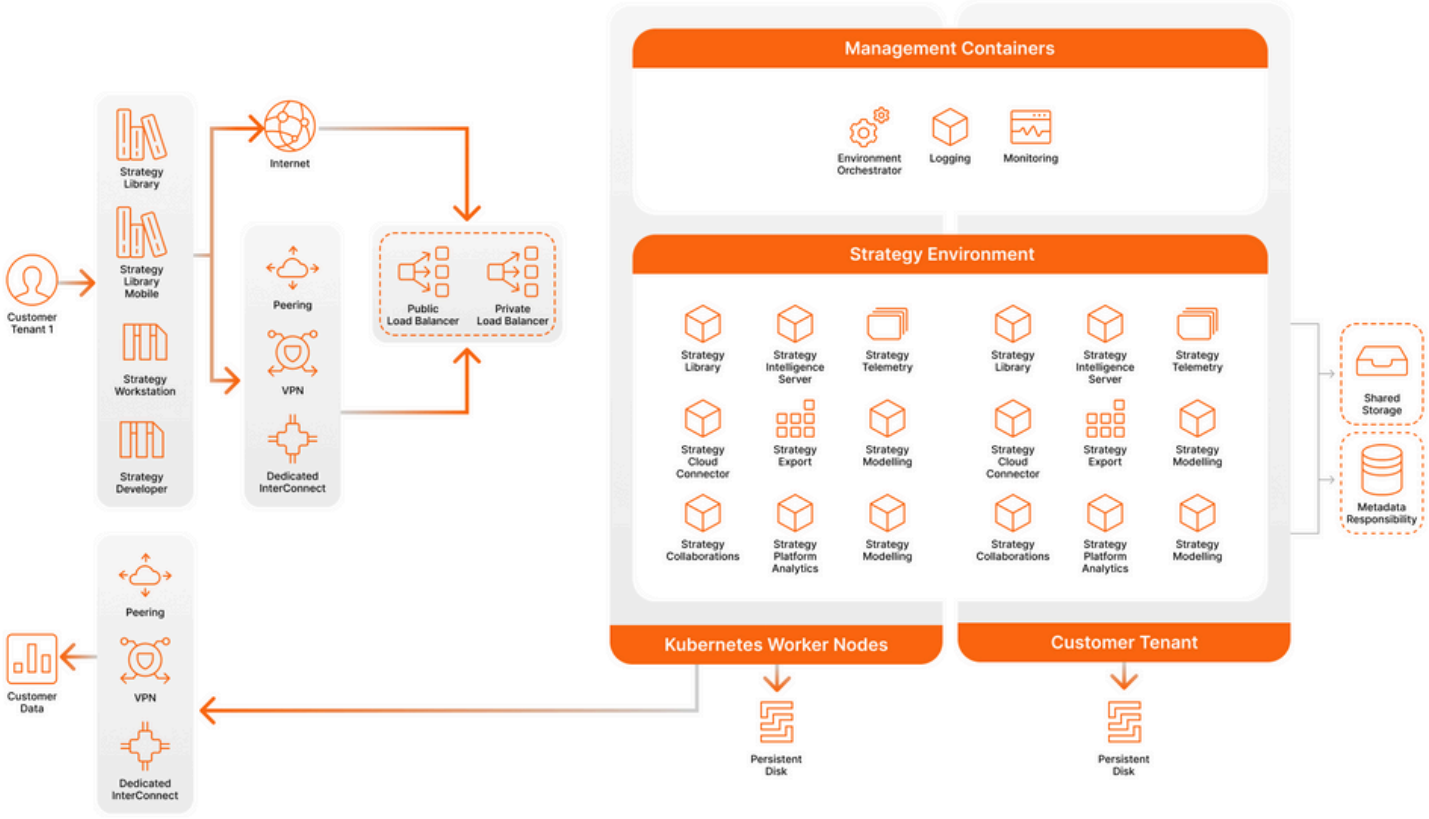
Azure Deployment Overview

Customers leveraging the Azure public cloud for their MCE deployment can benefit from a dedicated cluster of Strategy Server components. This cluster is deployed within a distinct Azure VNET.



GCP Deployment Overview

Customers leveraging the GCP public cloud for their MCE deployment benefit from container-based solution. The worker node is deployed in GCP distinct VPC.



Asset Management

Strategy 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, Azure and GCP virtual machine image instances.

Instance Segregation

Strategy implements and wholly manages a unique virtual private cloud instance for each Strategy 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. Strategy 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. Since cloud computing involves multiple layers of providers and users, an effective security posture requires commitment to governance at all levels of the organization. Strategy 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.

Organizational Alignment

Strategy 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.

Information Security Policies

Strategy 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 industry best practice governance standards for information security noted above. Strategy 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.

Segregation of Duties

Strategy 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. Strategy employs 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

Strategy 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 Strategy code of conduct, security, and confidentiality policies. Current copies of policies are available to all employees on the company intranet.

Strategy requires that newly hired personnel, including employees, interns, and contractors, who support the Strategy Cloud team receive and acknowledge security awareness training related to organizational privacy and security requirements. This training and acknowledgement are facilitated by Strategy's learning management system and requires recertification at least annually thereafter.
In addition, Strategy's information security team reinforces security culture by organizing various awareness activities and trainings throughout the year.

Strategy prioritizes security by enforcing rigorous requirements foar all personnel.

- Pre-offer technical assessment
- Pre-hire background check
- Onboarding InfoSec training
- Global Data Protection Training
- Code of Conduct acknowledgment
- Annual renewal of security training

Best-in-Class Security

Strategy has built a dedicated internal information security and compliance team to ensure that industry best practice processes are continuously maintained, enhanced, and verified. The team has established extensive data protection and privacy policies and procedures in compliance with General Data Protection Regulation (GDPR) requirements. The information security and compliance team also work closely with Strategy's legal department to ensure complete compliance with regulatory requirements across local and federal laws in every jurisdiction in which the Strategy Cloud is offered.

Compliance Certifications

MCE for AWS, Azure and GCP 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 Strategy Managed Cloud Enterprise 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

ISO/IEC 27001:2022 Certificate Number: ISMS-MI-13123

Data Privacy Framework EU, UK, Swiss and US

Payment Card Industry Data Security Standard (PCI DSS), Self-Assessment Questionnaire, Type D (SAQ-D), for Service Providers, Version 4.0

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

Data Security

Strategy 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 Strategy Managed Cloud Enterprises on our customers' behalf.

Data Privacy

Personnel responsible for operating the Strategy Cloud as a fully managed SaaS 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 Strategy 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. MCE customers will have a seven (7) day backup retention period, a thirty (30) day extended backup cycle encompassing metadata, and a monthly backup archive for the preceding eleven (11) months. Strategy does not store any customer data at the platform level, but the application can create caches and cube files locally.

Data In-Transit

Strategy uses the best methods in the industry to secure any data that is sent or received from the Strategy Cloud. Data in transit is encrypted by using IPsec and/or SSL VPN gateways, with TLS 1.2+ for encryption. Strategy handles SSL certificates for customers as part of the managed service and can also use certificates that customers provide if needed.

Data At-Rest

Strategy uses common encryption methods (AES-256) to safeguard and encrypt data at rest anywhere within Strategy Cloud limits. To meet the needs of MCE customers who handle sensitive types of personally identifiable information (PII), electronic protected health information (ePHI), or are subject to regulation, Strategy thoroughly assesses the platform to ensure that PII and ePHI is not kept in permanent state within the MCE platform.

Due to the architecture of the Strategy platform, if a customer chooses to utilize caching and intelligence cube capabilities, then application data files that are at-rest are backed up on Strategy-managed Intelligence Servers. Due to data privacy considerations, Strategy does not have visibility into the data stored in MCE by the customer

Bring Your Own Key/Host Your Own Key (BYOK/HYOK)

MCE allows BYOK/HYOK. Bring Your Own Key (BYOK) is a security approach that lets organizations keep ownership and control over the encryption keys that protect their data in cloud environments. Instead of depending on the key management of the cloud service provider (CSP), organizations create and manage their own encryption keys, which are sent securely to the CSP for data encryption.

Host/Hold Your Own Key (HYOK) is a security approach where organizations have full control and ownership of the encryption keys, storing them within their own infrastructure. This approach is usually used in hybrid cloud environments or when organizations have strict regulatory requirements or high-security needs.

Data Handling

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

Data Control Requirements

MCE customers and administrators from the Strategy 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. Strategy 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, Strategy Cloud team members utilize a restricted role within MCE, enforced by access control lists (ACLs) that the customer can view. ACLs allow the appropriate personnel to fully manage the deployment while prohibiting access to customer data.

Data Storage

Strategy 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

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

After the customer confirms, Strategy fully erases all customer data and any potential copies. Or, if the customer wants, Strategy can give instructions for customer administrators to erase all relevant data themselves. In both situations, customers can ask for electronic discovery features to show that all data has been erased.

System Acquisition, Development, and Maintenance

The Strategy Cloud incorporates security principles into every phase of the system development lifecycle (SDLC). These security principles are applied both through the design of the MCE systems, and through specific activities needed for key lifecycle stages. The Strategy Cloud depends on strong security standards, protocols, and procedures that are embedded in all steps of the SDLC for effective development, deployment, maintenance, and optimization.

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 CWE/SANS Top 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 Strategy 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 Strategy Change Control Board (CCB).

Change Management

Strategy 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

Strategy 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. Strategy Cloud personnel implement these procedures at least once monthly within a scheduled maintenance window. If critical or zero-day vulnerabilities are identified, Strategy works with individual customers to establish an emergency maintenance window to update or patch the vulnerability within each unique MCE instance.

Vendor Management

Strategy 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, Strategy 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 Strategy Cloud architecture, AWS, Azure and GCP 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.

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

GCP Data and Security AWS Data Center Controls Azure Physical Security

Attestations of Compliance

Strategy 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 Strategy and the service providers that are implemented and maintained to protect and ensure the highest security standards for the MCE offering.

Communication Security

Strategy 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

Strategy 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. Strategy also implements web application firewalls (WAFs) within each customer's unique account to provide additional application layer protection.

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

GCP Cloud Armor AWS Shield Azure DDoS Protection

System Firewalls

The Strategy 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. All firewall changes 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. Strategy requires private subnet egress on TCP port 443 to *.cloud.Strategy.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

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

Dedicated connections establish a direct line of communication between the on-premises data center and an MCE AWS VPC or Azure VNet deployment.

GCP InterConnect AWS Direct Connect Azure ExpressRoute

Peering connections establish a direct line of communication between different MCE AWS VPCs or Azure Vnet deployments.

AWS VPC peering Azure Vnet peering

Intrusion Detection and Prevention

Strategy 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 trigger 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 Strategy 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.

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

- Unique ID assignments forall privileged users
- Multi-factor authentication (MFA) requirements for access to all remote and privileged systems
- Use of a centrally managed organizational security information and 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 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

Access Control

The Strategy 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 with the ability to strictly control access to each environment.

Multi-Factor Authentication

Strategy 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

Strategy centralizes auditing and logging for all systems monitoring and user activity using a third-party SIEM tool that aggregates, reviews, stores, and secures all log information. The service associated with this tool provides 24/7 monitoring and alerting services and immediately notifies Strategy 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 Strategy Cloud and its associated systems. Strategy utilizes a centrally hosted and managed solution that provides continuous monitoring and endpoint detection and response (EDR) capabilities.

Security Monitoring

Strategy uses an array of public cloud and third-party security monitoring tools and dashboards to provide comprehensive monitoring of the Strategy 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 preventing and remediating risks of future issues.

Vulnerability Scanning

The Strategy Cloud employs extensive vulnerability scanning and analysis across all levels of its technology stack. Strategy 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.

Strategy 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

Strategy 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 validation scans within 30 days until all requirements are met.

AI Solution

The effective deployment of artificial intelligence (AI) in business intelligence (BI) significantly depends on the integrity of the underlying data. The foundational understanding is clear – the accuracy of AI models and their subsequent results directly correlate with the quality of the input data. For AI systems driving business decisions, accuracy isn't merely beneficial, it's imperative. These systems need to be trustworthy to be of genuine utility.

Our AI solution is engineered to accurately interpret business questions presented in natural language, employ logical reasoning, and produce relevant results autonomously. This synthesis of BI's structured analysis and AI's adaptability ensures that Auto, Strategy suite of AI capabilities, meets the dual needs of data integrity and flexible user engagement.

AI capabilities augment the Strategy Cloud offering through AI-assisted data exploration, automated dashboard design processes, SQL generation tools, and ML-based visualization methods, through Auto and Python-driven Advanced ML analytics exclusively housed within the MCE. By anchoring it within the MCE framework, we ensure that AI capabilities consistently benefit from and uphold the robust environment isolation standards intrinsic to MCE.

In essence, Strategy's AI capabilities are not merely an intelligent data processing tool, but rather, an integral part of the MCE service deeply integrated into a cloud environment where every architectural decision prioritizes user security. The stringent environment isolation properties of the MCE further highlight our unwavering commitment to safeguarding our customers' data integrity.

Business Continuity

Strategy 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 Strategy Cloud team to ensure the highest levels of business resiliency on their behalf.

Incident Response

Strategy implements a coordinated incident response process to effectively identify and resolve any security incidents involving MCE information systems and associated data for these environments. Strategy 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 qualified security personnel.

Incident Notification

If a confirmed security incident impacts an MCE customer, the Strategy 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 Strategy Cloud team perform preventive measures that may proactively decrease occurrence of specific incidents.

Disaster Recovery

Strategy develops, documents, and disseminates a comprehensive set of procedures for implementing DR and contingency planning activities for the Strategy Cloud. Each MCE deployment includes and intra-region DR zone such as within the Availability Zones in the AWS, Azure and GCP region in use. The operating model for the Strategy 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 Strategy Managed Cloud Enterprise 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 Strategy website.

Strategy Incorporated, 1850 Towers Crescent Plaza, Tysons Corner, VA 22182.

strategysoftware.com