EVANS&CHAMBERS
TECHNOLOGY

LAUNCHING SPACE DATA WORKLOADS INTO THE CLOUD

Produced by Evans & Chambers Technology

EVANS & CHAMBERS TECHNOLOGY

Table of Contents

EVANS&CHAMBERS
TECHNOLOGY

Chapter 1

Introduction

Chapter 1

Introduction

In the realm of space intelligence and defense, the collection, analysis, and interpretation of data are vital for safeguarding national security and advancing our understanding of space-based threats and opportunities. The ability to migrate and harness the power of the cloud for handling and analyzing space data has emerged as a game-changer in this dynamic landscape. Evans & Chambers Technology is at the forefront of this transformative journey, providing comprehensive solutions tailored to the unique needs of space intelligence and defense agencies.

With an unwavering commitment to security, reliability, and innovation, Evans & Chambers Technology is dedicated to empowering space intelligence and defense organizations to elevate their capabilities through the migration and analysis of critical data in the cloud. By combining our deep expertise in cloud technologies, data management, and intelligence methodologies, we help our clients unlock new insights, drive informed decision-making, and stay ahead of evolving threats in the space domain.

The cloud provides numerous advantages over legacy platforms, including increased agility, scalability,

performance, and security.

However, it also presents challenges and considerations that must be carefully addressed to ensure a successful and secure migration.

In this ebook, we will explore Evans & Chambers Technology's proven approach to migrating space intelligence data and workloads from on-premises infrastructure to the cloud, with a focus on the unique needs and requirements of federal government agencies. We will discuss key considerations, best practices, and important factors that federal agencies should keep in mind when planning and executing a cloud migration initiative.

This ebook will cover various aspects of cloud migration, including assessing current costs and benefits, selecting the right cloud provider, securing sensitive data, complying with federal regulations and standards, implementing appropriate security measures, optimizing costs, and ensuring smooth operations in the cloud environment. We will also highlight the importance of a security-first approach to cloud migration, with a particular emphasis on data encryption, multi-factor authentication, and compliance with the Risk Management Framework (RMF).

Throughout this ebook, we will provide practical insights, examples, and guidance to help federal agencies make informed decisions and successfully migrate their workloads to the cloud. Whether you are considering a migration from bare metal or virtualized infrastructure like VMWare, this ebook will provide you with valuable

information and strategies to elevate your workloads to the cloud in a secure and efficient manner.

Join us as we embark on this mission to advance space intelligence through cloud migration and analysis. Together, we will strengthen national security, enhance operational readiness, and unlock the untapped potential of space data. Let Evans & Chambers Technology be your trusted partner on this transformative journey, propelling your space intelligence and defense capabilities to new horizons of excellence.

EVANS&CHAMBERS
TECHNOLOGY

Chapter 2

Assessing Your Workloads for Cloud Migration

Chapter 2

Assessing Your Workloads for Cloud Migration

The availability and accessibility of accurate and timely data are critical for informed decision-making, threat detection, and mission success. As organizations in the space intelligence domain consider migrating their data to the cloud, a comprehensive assessment of the current landscape including on-prem infrastructure becomes essential to lay the foundation for a successful migration strategy. This chapter will explore the key considerations and steps involved in assessing the landscape before embarking on the migration journey.

Understanding the Space Intelligence Data Ecosystem:

The first step in assessing the landscape is gaining a holistic understanding of the space intelligence data ecosystem. This involves identifying the various sources of data, such as satellite imagery, telemetry, radar data, and intelligence reports. Additionally, it is crucial to evaluate the volume,

velocity, and variety of data to determine the scalability and performance requirements for cloud migration.

Evaluating Data Quality and Completeness:

Space intelligence relies on accurate, reliable, and comprehensive data. During the assessment phase, it is imperative to evaluate the quality and completeness of existing data. This includes assessing data integrity, metadata availability, and any data gaps that need to be addressed before migration.

Analyzing Data Security and Compliance:

Space intelligence data often contains sensitive and classified information that requires robust security measures and adherence to strict compliance regulations. It is vital to conduct a thorough analysis of the security requirements and compliance standards, such as NIST SP 800-171, ITAR, or FISMA, that apply to space intelligence data. This assessment ensures that the cloud environment and associated services meet the stringent security and compliance needs.

Evaluating Storage and Processing Requirements:

Space intelligence data sets can be vast and continuously growing. Assessing storage and processing requirements is crucial to determine the cloud infrastructure needed to handle the data effectively. Factors such as data access patterns, processing workflows, and real-time analysis requirements should be considered when evaluating the scalability and performance aspects of the cloud environment.

Considering Integration and Interoperability:

Space intelligence agencies often rely on a diverse range of tools, applications, and systems for analysis and mission operations. Assessing the compatibility, integration capabilities, and interoperability of these tools with cloud services is essential to ensure seamless migration and continuity of operations.

Estimating As-Is Costs and Identifying Potential Savings:

An important aspect of assessing the landscape is conducting a comprehensive cost analysis of the existing on-premises infrastructure and operations. This estimation helps organizations understand the financial implications of migrating to the cloud and identify potential cost savings, such as reduced hardware maintenance, enhanced resource utilization, and scalability benefits. Federal agencies should conduct a thorough analysis of their current costs, taking into consideration both direct and indirect costs. Direct costs are the expenses that are directly associated with the infrastructure, such as hardware and software purchases, licensing fees, and maintenance costs. Indirect costs are the expenses that are not directly tied to the infrastructure but still impact the overall cost of running the environment, such as labor costs, energy costs, and facility costs.

By conducting a thorough assessment of the landscape, space intelligence organizations can gain valuable insights into their data ecosystem, security requirements, infrastructure needs, and potential cost savings. This

foundational knowledge serves as a blueprint for developing a robust migration strategy that aligns with the unique characteristics and objectives of space intelligence operations.

In the next chapter, we will explore the intricacies of designing a secure and scalable architecture for space intelligence data migration in the cloud.

EVANS&CHAMBERS
TECHNOLOGY

Chapter 3

Designing a Secure and Scalable Architecture

Chapter 3

Designing a Secure and Scalable Architecture

As federal agencies consider migrating their workloads to the cloud, security must be at the forefront of their decision-making process. Protecting sensitive data and ensuring compliance with federal regulations and standards is paramount. One critical aspect of security for federal agencies is the support for Common Access Card (CAC)/Personal Identity Verification (PIV) cards, which play a vital role in the authentication and authorization of users.

CAC/PIV cards are smart cards issued by the Department of Defense (DoD) and other federal agencies to provide secure access to systems, networks, and facilities. These cards contain digital certificates that enable secure identification and authentication of users, ensuring that only authorized personnel can access sensitive information and perform actions based on their privileges.

When migrating workloads to the cloud, it is crucial to

choose a cloud provider that supports CAC/PIV card authentication. This ensures that federal agencies can maintain the same level of security and compliance in the cloud as they do in their on-premises environment. By leveraging CAC/PIV cards for authentication, federal agencies can prevent unauthorized access to their cloud resources, protect against data breaches, and ensure compliance with security requirements.

Additionally, a security-first approach to cloud migration should also include robust access controls, least privilege, and encryption of data at rest and in transit. Implementing a zero trust security model, where access is granted based on the principle of "never trust, always verify," can provide an additional layer of security. This approach involves verifying the identity of users and devices, assessing the security posture of devices, and dynamically granting access based on real-time context.

Furthermore, compliance with federal regulations and standards, such as the Risk Management Framework (RMF), is crucial for federal agencies. RMF provides a structured and systematic approach to managing risks associated with information security in federal systems. Ensuring that the cloud provider follows RMF guidelines and has relevant certifications, such as FedRAMP (Federal Risk and Authorization Management Program), can help federal agencies meet their compliance requirements and maintain the security of their workloads in the cloud.

In summary, a security-first approach to cloud migration for federal agencies should include support for CAC/PIV card authentication, robust access controls, least privilege, data encryption, and compliance with federal regulations and

standards such as RMF and FedRAMP. By prioritizing security in the cloud migration process, federal agencies can ensure the protection of sensitive data, maintain compliance with federal requirements, and safeguard their workloads in the cloud.

EVANS&CHAMBERS
TECHNOLOGY

Chapter 4

Choosing the Cloud Provider for Your Workload

Chapter 4

Choosing the Cloud Provider for Your Workload

As federal agencies operate in accordance with today's cloud contracting environment, choosing the right cloud provider becomes a critical decision. With initiatives like the Cloud Computing Environment (C2E) driving cloud adoption across federal agencies, it is essential to conduct thorough due diligence when selecting a cloud provider to ensure that it meets the unique needs and requirements of your workload.

Understanding C2E and Its Implications:

The federal government's C2E initiative aims to provide a standardized and secure cloud computing environment for federal agencies to host their applications and services. C2E offers a framework for federal agencies to select, procure, and manage cloud services in a consistent and compliant manner. It includes guidelines, policies, and best practices for cloud adoption, security requirements, and procurement considerations.

With C2E in place, it becomes even more important to carefully evaluate cloud providers based on their ability to meet the C2E requirements and comply with federal regulations and standards. This includes considerations such as data security, privacy, compliance with Federal Risk and Authorization Management Program (FedRAMP), Federal Information Processing Standards (FIPS), and other relevant regulations. Choosing a cloud provider that aligns with C2E can help ensure that your workload is hosted in a secure and compliant environment.

Due Diligence in Cloud Provider Selection:

When selecting a cloud provider for your workload, it is crucial to conduct thorough due diligence to assess their capabilities, features, and security measures. Some key factors to consider include:

- **Security:** Data security is of paramount importance for federal agencies. Ensure that the cloud provider has robust security measures in place, such as encryption at rest and in transit, multi-factor authentication, and robust access controls. Additionally, assess the cloud provider's compliance with relevant security standards, such as FedRAMP, FIPS, and other relevant regulations.
- **Compliance:** Compliance with federal regulations and standards is critical for federal agencies. Verify that the cloud provider has appropriate certifications and compliance measures in place, such as FedRAMP authorization, FIPS compliance, and adherence to other relevant regulations.

- **Reliability and Performance:** Evaluate the cloud provider's track record in terms of uptime, availability, and performance. Consider their service level agreements (SLAs) and performance guarantees to ensure that they can meet your workload's performance and availability requirements.
- **Cost and Pricing:** Assess the cloud provider's pricing models, including factors such as data storage, data transfer, compute resources, and other costs associated with your workload. Consider options like reserved instances, which can help optimize costs for federal agencies that follow government procurement methods.
- **Support and Service Level Agreements:** Evaluate the cloud provider's support options, including their responsiveness, availability, and expertise in handling federal agency workloads. Review their service level agreements (SLAs) to ensure they align with your agency's requirements.
- **Scalability and Flexibility:** Consider the cloud provider's ability to scale resources up or down based on your workload's requirements. Auto-scaling and right-sizing of resources can help optimize costs and performance.
- **Importance of Cloud Provider Selection for C2E Compliance:** With C2E driving cloud adoption in federal agencies, selecting the right cloud provider becomes even more critical.

Conclusion

Choosing the right cloud provider for your workload is a crucial decision for federal agencies, especially in the

context of the Cloud Computing Environment (C2E) initiative. With C2E driving cloud adoption and standardization across federal agencies, it is imperative to conduct thorough due diligence when selecting a cloud provider to ensure compliance with C2E requirements and federal regulations.

Considering factors such as security, compliance, reliability, cost, support, scalability, and flexibility, federal agencies must carefully evaluate cloud providers to determine their suitability for hosting sensitive workloads. This includes assessing the cloud provider's adherence to relevant security standards, such as FedRAMP and FIPS, and their ability to meet the unique needs and requirements of federal agencies.

By selecting a cloud provider that aligns with C2E and complies with federal regulations and standards, federal agencies can ensure that their workloads are hosted in a secure, compliant, and reliable cloud environment. Proper due diligence in cloud provider selection is essential to mitigate risks and ensure that the sensitive data and applications of federal agencies are protected in the cloud.

EVANS&CHAMBERS
TECHNOLOGY

Chapter 5

Cost Reduction Strategies

Chapter 5

Cost Reduction Strategies

Optimizing cloud resources is a critical aspect of cloud migration for DoD agencies to ensure cost efficiency without compromising performance or security. By leveraging features such as auto-scaling, reserved instances, and right-sizing of resources, DoD agencies can optimize their cloud resources to achieve cost savings while meeting their operational requirements.

Auto-Scaling: Auto-scaling is a cloud feature that automatically adjusts the resources allocated to an application based on its workload. It allows DoD agencies to automatically increase or decrease the number of instances, containers, or virtual machines based on demand. By leveraging auto-scaling, DoD agencies can optimize their resources by only using what is needed, which can result in cost savings during periods of low demand.

Reserved Instances: Reserved instances are a purchasing option offered by cloud providers that allow DoD agencies to reserve cloud resources for a specific period at a discounted rate compared to on-demand instances.

Reserved instances are especially relevant for federal government procurement methods, as they align with longer-term planning and budgeting cycles. By utilizing reserved instances, DoD agencies can achieve significant cost savings and cost predictability for workloads that require consistent resources over an extended period.

Right-Sizing of Resources: Right-sizing of resources involves analyzing the utilization of cloud resources and adjusting them to match the actual requirements of the workload. This process involves identifying over-provisioned or under-utilized resources and optimizing them to align with the actual workload demands. By right-sizing resources, DoD agencies can avoid unnecessary costs associated with over-provisioning or under-utilization of resources. Monitoring and Optimization: Continuous monitoring of cloud resources is crucial to identify opportunities for optimization. By leveraging monitoring tools and services provided by cloud providers, DoD agencies can gain insights into the utilization, performance, and cost of their cloud resources. This information can be used to identify areas where further optimization is needed and take appropriate actions to achieve cost efficiency.

Regular Review and Optimization: Cloud optimization is an ongoing process that requires regular review and adjustment of resources. DoD agencies should establish a process to periodically review their cloud resources, including auto-scaling policies, reserved instances, and resource utilization, and make necessary adjustments to optimize cost efficiency continually. By optimizing cloud resources through features such as auto-scaling, reserved instances, and right-sizing of resources, DoD agencies can achieve significant cost savings while ensuring that their

operational requirements are met in the cloud environment. It's important to work closely with cloud providers, utilize monitoring tools, and establish a regular review and optimization process to continually optimize cloud resources for cost efficiency, with a particular emphasis on leveraging reserved instances that align with federal government procurement methods.

Chapter 6

Data Encryption in the Cloud

Chapter 6

Data Encryption in the Cloud

Securing sensitive data is a top priority for DoD agencies during cloud migration. One critical aspect of data security is encryption. Encryption is the process of converting data into a form that is unreadable without the appropriate decryption key, making it secure from unauthorized access.

In the cloud, data encryption can be achieved through various methods, including at rest, in transit, and in use. When selecting a cloud provider, it is essential to ensure that the encryption features meet the security requirements of DoD agencies and comply with Federal Information Processing Standards (FIPS), a set of security standards established by the National Institute of Standards and Technology (NIST).

Here are some key considerations for data encryption in the cloud:

Encryption at Rest: Data stored in the cloud can be encrypted at rest, which means it is protected while it is stored in the cloud provider's data centers. Look for cloud

providers that offer FIPS-compliant encryption algorithms, such as AES-256, for data at rest.

Encryption in Transit: Data transmitted between the cloud provider and the user's environment should also be encrypted to protect it from interception and tampering. Look for cloud providers that use secure communication protocols, such as SSL/TLS, for data in transit.

Key Management: Proper management of encryption keys is crucial to ensure the confidentiality and integrity of encrypted data. Look for cloud providers that offer robust key management options, such as key rotation, key versioning, and separation of duties to meet DoD agency's security requirements.

Compliance with FIPS: Compliance with FIPS is critical for DoD agencies to ensure that data encryption in the cloud meets the required security standards. Look for cloud providers that have undergone FIPS validation and provide documentation of their compliance.

Access Control: Access to encrypted data should be strictly controlled, with only authorized personnel having the appropriate decryption keys and permissions. Look for cloud providers that offer robust access control mechanisms, such as role-based access control (RBAC) and granular permissions, to prevent unauthorized access to encrypted data.

Monitoring and Auditing: Monitoring and auditing of encrypted data in the cloud is essential to detect and respond to any security incidents. Look for cloud providers that offer comprehensive logging, monitoring, and auditing

features to help with security incident detection and response. By ensuring that data is encrypted in the cloud and compliant with FIPS, DoD agencies can add an additional layer of security to protect sensitive information during cloud migration.

Note: It's important to consult with legal, security, and compliance experts when implementing data encryption in the cloud to ensure compliance with relevant regulations and policies, including FIPS and other security requirements specific to DoD agencies.

Chapter 7

Conclusion

Chapter 7

Conclusion

Migrating space intelligence data to the cloud presents a transformative opportunity for organizations to enhance their capabilities, improve operational efficiency, and leverage advanced analytics for critical decision-making. By following a systematic and well-planned approach, organizations can successfully navigate the complexities of cloud migration while addressing the unique requirements and challenges of space intelligence operations.

In this ebook, we have explored the crucial considerations for migrating space data to the cloud, emphasizing the importance of a security-first approach, compliance with regulations, and the need for a scalable and resilient architecture. We discussed the significance of assessing the landscape, understanding data characteristics, evaluating security requirements, and estimating costs to lay the foundation for a successful migration strategy.

Furthermore, we delved into the intricacies of designing a secure and scalable architecture tailored to space intelligence needs. By embracing cloud-native security services, ensuring data privacy and compliance, establishing resilience and high availability, implementing data governance, and optimizing performance and scalability,

organizations can create a robust architecture that meets their unique operational requirements.

As space intelligence agencies embark on their cloud migration journey, it is essential to collaborate with experienced and knowledgeable partners who understand the intricacies of space data and possess deep expertise in cloud technologies. Together, we can leverage the power of the cloud to unlock the full potential of space intelligence, enabling faster insights, better decision-making, and increased operational effectiveness.

At Evans & Chambers Technology, we are committed to guiding organizations through their cloud migration journey, leveraging our expertise in space intelligence, cloud technologies, and data management. Contact us today to learn more about how our proven approach can help you elevate your space intelligence capabilities in the cloud.

Remember, the future of space intelligence is in the cloud, and by embracing this transformation, organizations can stay ahead of the curve, drive innovation, and achieve new heights in their missions and objectives.

Ready To Get Started?

Ready to embark on your cloud migration journey? Let our team guide you through a proven methodology tailored to your agency.

Contact Us today