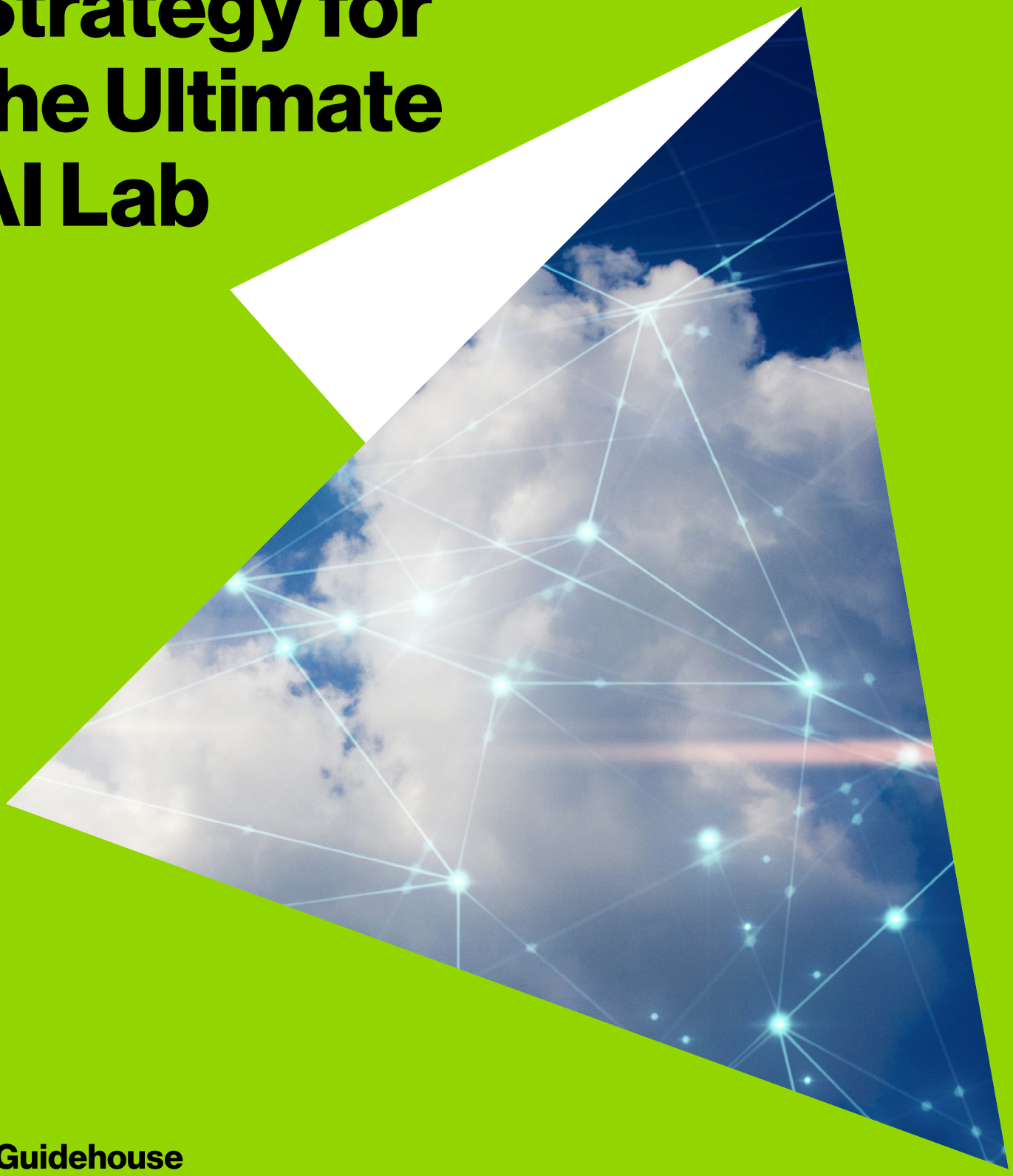
Cloud Strategy for the Ultimate AI Lab



Guidehouse

Overview — Building the Ultimate AI Lab

As public and private sector leaders develop data, cloud, and Artificial Intelligence (AI) / Machine Learning (ML) strategies, the need for a unified framework has never been more apparent. These strategies naturally overlap, presenting challenges spanning strategy development, implementation, continuous delivery, and operations.

Curated, tracked, and governed data served through cloud native infrastructure fuels impactful and high value AI/ML solutions. Organizations and their respective data, cloud, and AI divisions need to coalesce around a unified vision, strategy, and execution plan. Additionally, they must bring to bear rigorous engineering practices, coupled with a scientific approach to continuously deliver solutions that shorten the **time to customer value (TTCV)** and build a sustained competitive advantage.

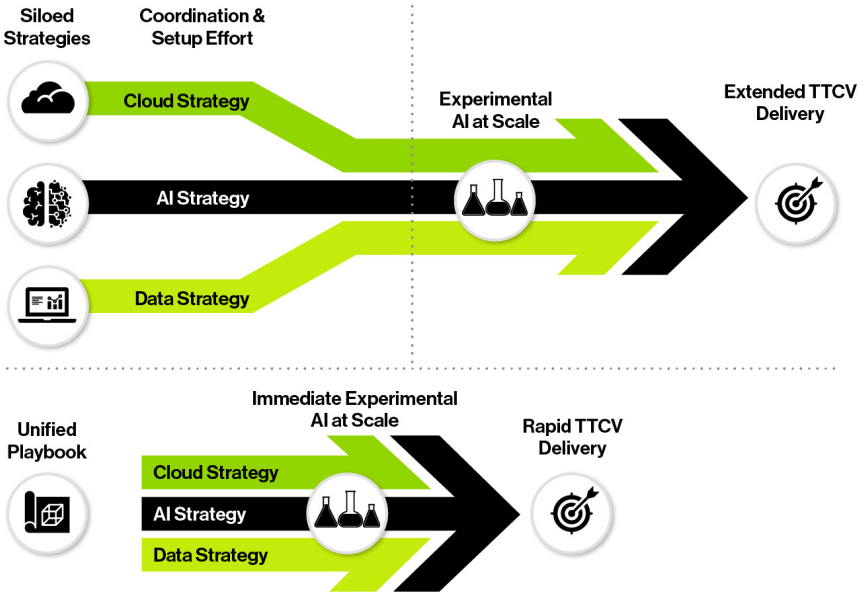


Figure 1: Unified AI, Cloud, and Data Strategies expedites TTCV

This white paper explores some of the challenges and necessary considerations when developing, governing, and releasing AI solutions. While setting an AI strategy is essential to any AI journey, it is also crucial to consider the full-stack AI ecosystem; integrated strategy enables AI teams to develop an Ultimate Lab where data is discoverable and computational resources are scalable and secure. Accordingly, this series also includes the **AI Strategy for the Ultimate AI Lab** and **Data Management and Governance Strategy for the Ultimate AI Lab** white papers, which explore the implementation of each respective strategy, along with a culminating business case for strategy integration: **The Ultimate AI Lab.**

Leveraging its IT strategy, cloud operations, AI, and data governance expertise, Guidehouse provides a unified framework for addressing each of these strategic domains driven by business goals. Our approach harmonizes these interdependencies to develop an organizational strategy focused on delivering and shortening TTCV.

Cloud Strategy

Guidehouse recognizes that cloud service providers have an increasingly robust—and sometimes complicated—catalog of offerings. However, the core set of services remains the same:

- Storage and databases to make data available and actionable;
- Computing resources to run applications and workloads; and
- Networking resources for connectivity, bandwidth, and isolation.

The main advantage of cloud platforms is the ability to scale resources to best match the current workload. This flexibility gives organizations the ability to minimize costs when resources are not needed and efficiently meet challenges and demands when necessary. Additionally, cloud platforms allow organizations to make their resources and products available to employees and customers from nearly anywhere, so strong and clear policies for Authentication, Authorization, and Auditing (AAA) are also offered to secure it all.

The main advantage of cloud platforms is the ability to scale resources to best match the current workload.

Organizations can benefit from implementing cloud strategy across a variety of scenarios:

- To start leveraging cloud resources and defining a clear path to adoption;
- To address compliance, operational, or governance risks associated with cloud resources;
- To gain a competitive advantage over (or achieve parity with) peer organizations; and
- To invest in an alternative to traditional data centers.

Not every team needs a procedure for dealing with the newest, most esoteric service offered in the cloud, but most teams need clear guidance on the standards and practices they should adopt for storage, computing, networking, and AAA.

Choosing and Understanding Cloud Solutions

CLOUD SERVICE PROVIDERS

The choice of cloud service provider can extend beyond comparing specific vendors or providers to also include the decision to adopt a single public cloud, multi-cloud, or hybrid cloud strategy. This strategy decision can have far-reaching impacts across the organization and be necessary in order to fulfill specific requirements. Organizations should approach this decision from a platform-agnostic standpoint to consider the cloud service provider or combination of providers that best aligns with their current and long-term needs.

GOVERNMENT CLOUDS

Several cloud service providers offer purpose-built cloud environments for strictly regulated government workloads. These cloud environments can come at a significant premium, most notably with significantly higher prices for core resources like virtual machines or storage. As a natural consequence, organizations with robust controls, procedures, and governance can leverage this price differential to achieve a decisive competitive advantage. These high performers can minimize their operations on government clouds to control their costs while maintaining the needed level of security. [1]

Single Cloud Solution
Designed so that all cloud services and products associated with the solution are from one cloud service provider.

Multi-Cloud Solution
Utilizing services or products from multiple cloud service providers.

Hybrid Cloud Solution
Solutions that use both local, on-premise resources along with cloud services together.

ENTERPRISE SUPPORT

Major cloud service providers have robust sales engineering programs that can be leveraged to augment the in-house talent of any organization that grows on the cloud. These services offer a broad range of products and support to enterprise customers. In the case of organizations that are pursuing a hybrid or multi-cloud strategy, teams should exercise judgment and proactive communication with sales engineers about their strategic outlook and requirements.

SERVICE LEVELS AND HIGH AVAILABILITY

Service level agreements (SLA), highly available (HA) architectures, and highly reliable services are products of intense, continuous operations and site reliability engineering effort. In particular, the SLA outlines the expected level of uptime and availability when using cloud services, and the compensation given when it is not provided. Yet, for the purposes of operational planning, SLAs are post-hoc remedies, not promises. Organizations cannot plan for every scenario, and SLAs can only ever be part of the answer to: "What happens when things go wrong?" In the same manner, HA architectures must be treated as risk mitigation strategies and can never be replacements for outage planning. Treating SLAs and HA architectures as hedges against operational risk empowers team leaders to accurately determine the services most needed for their cloud investments and to build both additional redundancies and backups for critical pieces of their operations.[2]

COMPLIANCE

Cloud resources are foundational to compliance efforts across the organization; applications cannot operate within compliance if their underlying infrastructure is not compliant as well. Major cloud providers offer a variety of compliance services, and very few of them absolve the user of any responsibility to design for compliance. Consequently, cloud services can only support compliance in operations, and managing compliance remains the responsibility of enterprise architects and operations teams.[3]

Governing Cloud Resources

AUTHENTICATION, AUTHORIZATION, AND AUDITING

The capacities to control how identity is proven, how permissions are granted to identities, and how actions are tracked throughout the system are collectively referred to as Authentication, Authorization, and Auditing (AAA). One advantage of adopting a cloud strategy is the ability to benefit from the robust AAA capabilities that major cloud service providers build into almost every product. As a result, AAA is a fundamental design element of all well-architected cloud, enterprise data, or AI laboratory solutions. Promoting AAA as a priority and ensuring that all domains are aligned ensures that these constraints can be leveraged effectively without undermining confidence or operations.[4]

MANAGED SERVICES

Cloud service products operate based on "shared responsibility" business models, where responsibilities are shared between the organization and the cloud service provider.[5] When the organization does not fulfill or understand their responsibilities, there can be major problems, such as in these well-known examples:

- Misconfigured object storage solutions are frequently in the news for exposing customer data. The cloud service provider is not responsible; in the object storage responsibility model, access configuration is the customer's responsibility.
- The "serverless" movement is not about running applications without servers. Rather, it is when cloud service providers take responsibility for the infrastructure, platform, and/or software, while leaving organizations responsible for managing and providing working applications themselves.

Managed services are not a panacea. Leaders who can accurately distinguish the core of their business from the context can leverage that insight to appropriately select managed services.

PRICE

Cloud services are expensive. Their pricing is difficult to predict, and consumption-based pricing introduces risks that many organizations are not set up to manage. To mitigate these risks, all major cloud providers offer mechanisms that can alert managers about anomalous spending, assign budgets, and enable cost surveillance. In addition to these measures, many cloud service providers offer discounts for organizations that commit to spending or consumption one or more years in advance, enabling groups with a clear long-term strategy the ability to capitalize on their planning.

AUDITING

With some exceptions, cloud service providers are able to produce detailed audit trails of all change requests that they receive. For a variety of reasons, these features do not always have sensible defaults or are not enabled by default. Guidehouse recommends adopting a "set once, consume many times" policy for audit trails, enforcing a strong requirement that audit trails are appropriately enabled and monitored for all cloud environments.

MONITORING

Cloud service providers offer robust monitoring tools and options, presenting a challenge (and cost factor) for operations in terms of storage and management. Setting clear guidelines for monitoring of core resources can reduce operational burden and improve the reliability of services.

Integration with AI and Data Strategy

OBSERVABILITY

Predicated upon a proper data strategy, which collects necessary artifacts and context, "observability" is the practice of building services and architectures that are "transparent" from an operational standpoint.[6] Creating observable systems enables operations teams to infer the status of functional components without intervention or additional tools, reducing the time and effort needed to identify fixes. In complex architectures, designing for observability can consistently improve overall reliability.[6]

DATA GRAVITY

Data gravity is the concept that it is easiest to process data on the cloud where it is stored. For many operations teams, data storage is a highly tactical question, especially as the amount of data gathered grows, but technology leaders should be wary about letting tactics drive strategy. The market for AI platforms-as-a-service (PaaS) has grown considerably in just a few short years, and the selection of cloud service providers has a significant impact on how AI architects can approach the market. Organizations should take the time to find the appropriate solution so that storage and analyses are complementary, and not at odds with each other.

GRANULAR ACCESS CONTROLS

In many cases, cloud services are built to enable organizations to implement granular controls over the data, services, and capabilities any given entity can access. Effective data strategy always leverages roles-based access controls so that the right people have the right resources when they need them.[7] For example, data warehouses of various types may support row-level access controls for users, and effective data strategy informs the use of these features for data architects designing the warehouse. When cloud and data strategy are aligned, the data architect is constrained by the operational requirements of the value stream, not the infrastructure that supports the solution.

Conclusion

Developing AI solutions at scale requires an AI strategy that directly incorporates data management and cloud infrastructure solutions tailored to their organization's needs. Integrating data, cloud, and AI strategies enable organizations to fully realize their investment value in each of these domains while collectively acting as a force multiplier.

Developing secure, agile cloud infrastructure prepares organizations to address a variety of challenges and situations and adapt operations flexibly to meet them. Managed properly, cloud infrastructure by itself brings the ability to scale while controlling costs and to allow access from nearly anywhere. However, this is only the beginning of value creation in the cloud domain; connecting these cloud infrastructure operations to the organization's data strategy enables all lines of business to realize the value of both data and infrastructure. AI operations on cloud infrastructure are only fully empowered when this takes place. Unifying data, cloud, and AI strategies maximize the return on investment while minimizing TTCV, providing organizations a serious competitive edge.

Guidehouse brings unique, combined expertise in applied sciences, life sciences, AI, cloud, data governance, IT strategy, and change management. This diverse but tightly coupled set of capabilities and experience uniquely position us to design and build the Ultimate AI Lab, ensuring fertile grounds for ML algorithmic experiments to discover the most promising models and guaranteeing maximum value for our customers.

1. Challenging Security Requirements for US Government Cloud Computing Adoption (2012) | Fred Whiteside, Michaela Iorga, Lee Badger, Jian Mao, and Shilong Cu
2. Reliability and High Availability in Cloud Computing Environments: A Reference Roadmap (2018) | Mohammad Reza Mesbahi, Amir Masoud Rahmani and Medhi Hosseinzadeh
3. A Survey of Compliance Issues in Cloud Computing (2016) | Dereje Yimam and Eduardo B. Fernandez
4. AAA Protocols: Authentication, Authorization, and Accounting for the Internet (1999) | Christopher Metz
5. Exploring Data Security Issues and Solutions in Cloud Computing (2018) | P. Ravi Kumar, P. Herbert Raj and P. Jelciana
6. Towards a Model of Accountability for Cloud Computing Services (2013) | Daniele Catteddu, Massimo Felici, Giles Hogben, Amy Holcroft, Eleni Kosta, Ronald Leenes, Christopher Millard, Maartje Niezen, David Nunez, Nick Papanikolaou, Siani Pearson, Daniel Pradelles, Chris Reed, Chunming Rong, Jean-Claude Royer, Dimitra Stefanatou and Tomasz Wiktor Wlodarczyk
7. Role-Based Access Control Models (1996) | Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman

Guidehouse

Contact Information

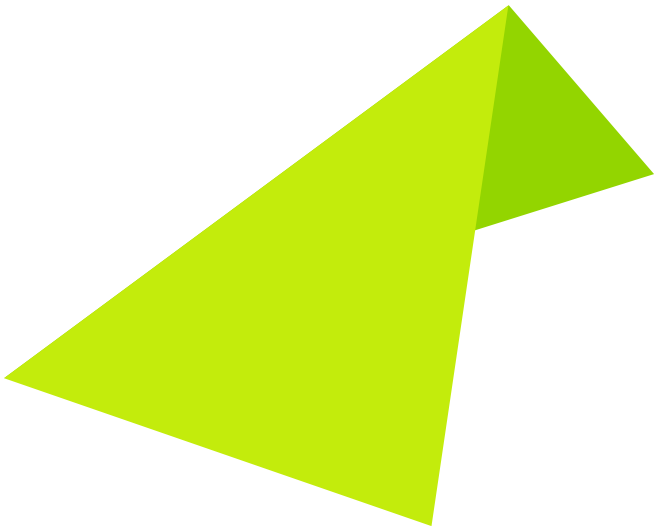
Bassel Haidar
Associate Director, Advanced Analytics and Intelligent Automation
bhaidar@guidehouse.com

Charles Landau
Managing Consultant, Advanced Analytics and Intelligent Automation
clandau@guidehouse.com

Stephanie Ling
Managing Consultant, Advanced Analytics and Intelligent Automation
sling@guidehouse.com

Acknowledgments

The authors would like to acknowledge the following people for their contributions: Alex Gromadzki, Kate Pokrass, Minsoo Kim, Devan Visvalingam, and Stephen Williams



About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges and navigate significant regulatory pressures with a focus on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that prepare our clients for future growth and success. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit: **www.guidehouse.com.**