A HURWITZ WHITE PAPER

Understanding IBM's Hybrid and Multicloud Strategy

Judith Hurwitz
President & CEO

Daniel Kirsch
Managing Director

HURWITZ & ASSOCIATES
Insight to Action

Sponsored by IBM

Introduction

Increasingly, business leaders are combining innovation and the flexibility of cloud services with the rigors required to keep the business secure, compliant, and manageable. Pragmatic leaders are converging on an approach that combines the power of the hybrid and multicloud with the flexibility of open source and standards. In this paper, we will provide our point of view on the requirements for the enterprise hybrid multicloud environment in conjunction with IBM's technical strategy.

Defining the Hybrid Cloud

A hybrid cloud is an environment that integrates traditional IT with a combination of public, private, or managed cloud services. In essence, a hybrid cloud becomes a virtual computing environment that matches workloads to the most appropriate computing model. All these services need to be managed as though they were designed to behave as a single unified environment.

… a hybrid cloud becomes a virtual computing environment that matches workloads to the most appropriate computing model.

The Journey to Hybrid Cloud

We recently had the opportunity to speak to a CIO who helped his company make the strategic transformation from an inflexible and chaotic infrastructure to a hybrid computing approach. The business was changing too fast to simply carry on with business as usual. The company had to compete with emerging competitors that did not have to contend with any technical or business legacy. The CIO's mandate was to create an IT environment that was innovative, flexible, scalable, manageable, and safe.

After many years spent focusing on reducing capital expenses through the introduction of public clouds it became clear that this approach was not able to meet the demands of the enterprise. The only viable solution was to embrace open source standards implemented in a hybrid and multicloud environment. At the same time, his organization was able to extract important intellectual property and best practices trapped within existing applications that had to be transformed into modular services. To gain acceptance from management, the new cloud environment had to have security and compliance at its core. Administrators also needed to have consistent ways to manage integration and data services. The predictability and manageability of the hybrid cloud now enables the business to move fast to create new value in light of competitive threats, while at the same time delighting customers with innovation and new products. All of this had to be accomplished while keeping costs under control.

The CIO could not afford to stand by as IT devolved into an unmanageable "Wild West." His goal was to create a modular foundation that could withstand technology and business change. Therefore, he created a plan based on open standards and hybrid and multicloud that would offer business leaders a choice

HURWITZ & ASSOCIATES
Insight to Action

of deployment models that best suited their objectives. He moved forward with platform services that would support a continuous software development and deployment model combined with ubiquitous and security services. At the same time, he began the process of modernizing and refactoring existing applications so that they were modular and flexible. He had to do all of this while maintaining customer satisfaction.

It is clear from the experience of this CIO and many of his peers that business as usual is dead. Instead, enterprise leaders must be on a quest to innovate quickly while maintaining the advantages of their deep intellectual property, their installed base and revenue. It is not a simple transition. Successful enterprise leaders understand the challenge and have selected a hybrid cloud environment. One size does not fit all. Rather, to be successful, businesses are focused on a multicloud, open source strategy that allows them to innovate, scale and protect their assets and their customers.

It isn't enough to have a world-shattering idea if you don't have the technology infrastructure to support change and execute at scale.

Innovation at Scale Matters

It isn't enough to have a world-shattering idea if you don't have the technology infrastructure to support change and execute at scale. We are entering an interesting stage of the digital transformation movement. Established businesses have sounded the alarm as they have watched startups – that have no legacy systems – move fast with great ideas and new business models. These emerging companies have indeed caused revolutions in many industries. Market incumbents have been forced to rethink how they conduct business and how they use technology. Although it might seem like these market stalwarts have no chance against nimble, born-on-the-web competitors, established companies have the benefit of decades of industry and customer data as well as intellectual property and complex business rules. Additionally, these businesses know how to scale to support a global footprint.

How IBM's Cloud Strategy Has Evolved

IBM's cloud strategy has evolved as customer expectations for the cloud have exploded. IBM has poured a significant investment into a hybrid and multicloud foundation based on industry standards and open source. At the core of IBM's cloud strategy is the understanding that customers need a unified and streamlined way to create modular application services, to transform and modernize legacy, and to manage all services, no matter where those workloads reside. All of these services need to be cataloged, secured, managed, and governed based on policy rules.

The only way to accomplish a unified approach to cloud computing is to coalesce a strategy based on open source and standards. Therefore, it is easy to understand why IBM created a platform centered on Kubernetes. The IBM cloud model enables the customer to have the same services available on the

HURWITZ & ASSOCIATES
Insight to Action

IBM private and public clouds as well as on any third-party public cloud and services at the edge. The power and versatility of open source, including Linux, open APIs, and Kubernetes, has helped IBM transform its software so that it has become modular and has unified services that can be more easily managed.

IBM has the benefit of providing computing platforms to support some of the largest and most complex workloads in the world. IBM has many years of experience implementing domain specific applications based on sophisticated business processes. These best practices are based on expertise from Global Business Services and Global Technology Services. These organizations provide business and technical guidance to customers across the globe in vertical markets ranging from financial services to retail and transportation. To plan for dramatic business and technical change, all of these industries depend on a hybrid and multicloud-based environment.

Business leaders understand the inherent risks of relying on a single vendor for all situations. Therefore, smart business leaders are demanding an environment that combines a variety of public and private clouds, hosted services, edge computing, and data center capabilities from a number of different vendors. This hybrid environment must be both secure and manageabie no matter where the services and workloads are deployed.

The IBM customer base is complex and therefore there are different requirements for the transition to the cloud. IBM has defined three entry points or models to support customers.

- **Migrating existing services to the cloud.** Most large enterprises must contend with a large number of outdated legacy applications and infrastructure. These businesses need a path to modernize and refactor their applications so that they gain the flexibility and agility needed for business transformation. These businesses may begin by lifting existing applications so they can be hosted on a cloud through the use of virtualization through VMware services. This entry point is designed to help businesses that want to take expenses out of their infrastructure.
- **Modernizing existing applications and services.** Organizations are transforming their applications with a container platform in order to modernize and migrate existing applications. The computing environment is analyzed to determine which applications can be reconstructed as microservices and which applications will need to be redesigned. Once containerized, it is possible to link those microservices as part of a cloud foundation through the use of open standards. Once these existing applications are refactored, developers can move quickly to create new applications.
- **New Cloud Native Innovative Applications.** Using cloud native services such as Knative and serverless, developers can create next generation applications that can be deployed within an open source Kubernetes environment.

Business leaders understand the inherent risks of relying on a single vendor for all situations. Therefore, smart business leaders are demanding an environment that combines a variety of public and private clouds, hosted services, edge computing, and data center capabilities from a number of different vendors.

HURWITZ & ASSOCIATES
Insight to Action

Hybrid at the Core

In order to maintain a hybrid cloud solution there needs to be a consistent and predictable integration of services and rich connectivity between all applications and services – no matter where they originate. Leveraging existing investments in applications and infrastructure is critical; business cannot just discard core infrastructure investments that are well designed to manage business transactions.

At the center of IBM's cloud strategy is the adoption and support of a hybrid and multicloud environment that allows customers to use the platforms and services they have already invested in, while also providing a large percentage of common open source services for ubiquitous integration, management, security, and data management. This pragmatic approach is critical since up to this point only a minority of workloads have been moved to the cloud. The foundation for hybrid is the principle of a cloud-agnostic strategy that enables businesses to use any existing or new service as part of their computing environment. This needs to be executed in a way that minimizes lock-in and promotes portability of workloads. To build a hybrid, multicloud strategy IBM is able to combine its open source strategy with its depth of product services for integration, connectivity, and management.

The adoption of hybrid computing is moving fast. While many businesses have taken advantage of Infrastructure as a Service, they have resisted moving business critical workloads that require security, low latency, and compliance. With the advent of emerging open source cloud technologies, the shift to the cloud is rapidly evolving. The timing is right for companies across industries to leverage innovation that scales. It is not enough to simply scale with compute services. Enterprises are increasingly demanding Linux as the open operating system, refactoring code as containerized microservices and leveraging containerized middleware services for agile integration while managing complex data and policy. The combination of all of these distributed services needs to be managed in a consistent and secure manner to enable integration across clouds and on premises data and applications.

One size does not fit all. Rather, to be successful, businesses must focus on a hybrid, open source plan that allows them to scale and protect their customers. It is necessary to leverage different computing models for different use cases. There are complex business applications that cannot easily be rewritten without a massive and expensive effort. Many of these services reside in the data center or are hosted in an enterprise cloud. In addition, there is a need for public cloud services to support agile DevOps requirements. Public clouds are ubiquitous and will continue to grow and mature. There is not a single public cloud that all customers demand. Rather, there are a variety of public clouds that are adopted across lines of business. In addition, there are mission-critical workloads containing strategic data that businesses do not want to place in the public cloud. Considerations such as security and compliance and latency are core to why businesses are insisting on a hybrid environment. Given these considerations, IBM has adopted a hybrid and multicloud approach.

One size does not fit all. Rather, to be successful, businesses must focus on a hybrid, open source plan that allows them to scale and protect their customers.

HURWITZ & ASSOCIATES
Insight to Action

To understand IBM's cloud strategy, it is important to understand the IBM cloud offerings. In this next section we will provide context and details of the six technology imperatives.

The core principles of the IBM cloud are:

- Leading with open standards and open source
- Providing a common foundation based on Kubernetes
- Managing containerized integration services
- Supporting a consistent set of security and compliance services including identify, access, encryption, and key management
- Providing management of distributed data and AI
- Providing standards based multicloud management

IBM has long been making significant investments in open source technologies, -- for example contributions to Linux, Hadoop, Spark, Kubernetes, Calico, Helm, Istio and Knative.

The Open Source Requirement

With few exceptions, open source is at the core of the hybrid cloud. For example, multiple studies indicate that open source Linux is by far and away the most popular operating system on the cloud – sometimes referred to as the cloud operating system. The dominance of Linux has opened a broad ecosystem of open source tools platforms that are fueling the hybrid and multicloud market.

IBM has long been making significant investments in open source technologies, -- for example contributions to Linux, Hadoop, Spark, Kubernetes, Calico, Helm, Istio and Knative. This investment in open source has increased dramatically over the past five years as IBM has begun to transform its public and private cloud platforms based on open source standards.

One of the key rationales for IBM's pending acquisition of Red Hat is the reality of Red Hat's business model and customer engagement. (The acquisition is subject to regulatory reviews. Until close, the parties are separate and independent companies.)

Red Hat's product offerings are all based on commercial open source software, ranging from the most popular Linux distribution, Red Hat Enterprise Linux (RHEL), to other offerings like Red Hat Ansible, OpenShift, and CloudForms, which provides a variety of automation and management technologies to improve operational agility.

Both IBM and Red Hat have containerization at the core of their strategies. Both companies focus on managing workloads across the enterprise and assume a hybrid computing environment. Red Hat is well respected by the developer community for its support of open source and its ability to deliver these resources in an enterprise- safe manner. Additionally, Red Hat provides the most important commercial Linux distribution that is the foundation for a majority of enterprise customers. Both companies are focused on creating enterprise scale solutions to support a large variety of solutions and tools all based on an open source framework.

HURWITZ & ASSOCIATES
Insight to Action

Foundation based on Kubernetes

Kubernetes provides an open source container orchestration platform that can automate the tasks of creating modern applications. Applications can either be encapsulated, as they exist today, or rewritten as a series of native microservices. Open source Istio, a service mesh, allows organizations to connect, secure, control, and observe services. Calico allows networking and network policy in Kubernetes clusters across the cloud. Helm, an open source platform, is a packaged manager for Kubernetes that enables developers and operational staff to package, configure, and deploy applications and services onto Kubernetes clusters. Knative is a pure Kubernetes universal resource model that provides a consistent API-based wrapper service for legacy workloads. Knative can work with a variety of models including Cloud Foundry, OpenShift, and serverless (OpenWhisk) frameworks built on top of Kubernetes and Istio in order to support serverless event driven functions.

The benefit of the combination of Kubernetes with services such as Istio, Calico, and Helm permits developers to write services once and deploy them on any cloud. With a Kubernetes and microservices approach, developers can push code out to any deployment model without changing the entire app. This capability allows an increased ability to respond to customer feedback, competition, and potential security issues. With Kubernetes in place, the same infrastructure can exist on any public cloud or private cloud without any change.

Another important benefit of containerization is that with Kubernetes, any service such as data, middleware, and security services can be implemented in these containers with consistent and well-defined APIs. This dramatically transforms the ability to create a consistent and unified hybrid environment.

The benefits of Kubernetes to IBM cannot be overstated. IBM has made the strategic decision to base both its public and private cloud on the same Kubernetes orchestration. Kubernetes is a portable and extensible open source platform for managing containerized workloads and services. One of the values of Kubernetes for IBM is that it is optimized to support all infrastructure platforms --including virtual machines-- to mainframes, and bare metal infrastructure. Another key reason for IBM selecting Kubernetes is the expansive ecosystem of tools and services that IBM leverages. This means that IBM is able to leverage important Kubernetes infrastructure tools including Istio, Calico, and Helm.

Another reason that IBM has adopted Kubernetes is that it provides a standardized way to build, package, deploy and run applications built with any language. Given the breadth of enterprise workloads, it makes sense to provide a platform that reflects the wide variety of IBM's customer deployments.

IBM provides standards-based Kubernetes services. Without exception, all software and platform services have been containerized. In the IBM public cloud, IBM includes the IBM Kubernetes Service. IKS is a container orchestration service standardized workload pattern that enables a workload to run secure workload at the edge or over the network. It can connect through a virtual private network

The benefits of Kubernetes to IBM cannot be overstated. IBM has made the strategic decision to base both its public and private cloud on the same Kubernetes orchestration. Kubernetes is a portable and extensible open source platform for managing containerized workloads and services.

HURWITZ & ASSOCIATES
Insight to Action

connection to use legacy services containerized on the IBM private cloud. For the IBM Cloud Private (ICP), IBM has created a Kubernetes that has containerized both IBM and OpenShift middleware. ICP also containerizes all services that are native to the host environment including IDAP and management services in the host.

One of the most important changes that IBM has containerized is its middleware integration services managed through Kubernetes. The common integration platform includes existing IBM products such as API and APP Connect, MQ, Aspera (secure high speed data transfer) and Event Streams. It has incorporated open source middleware offerings such as Jboss, TomCat, Kafka, and Liberty. All of these offerings are provided in an "as a service" model on both the IBM public and private cloud and on any third-party public cloud.

IBM's approach to hybrid and multicloud security is to create a set of built-in capabilities that are independent of the infrastructure layer.

Security at the Core

One of the most important concerns for businesses is information security. In a highly distributed hybrid and multicloud environment security is a major challenge. Hybrid and multicloud security is complicated because experts cannot simply secure a single location – everything is decentralized. Therefore, a perimeter approach defined by firewalls is no longer adequate. IBM's approach to hybrid and multicloud security is to create a set of built-in capabilities that are independent of the infrastructure layer. These core security services are intended to manage all aspects of security including access management, network security, and data protection services (including protection for data at rest, in motion and in memory). Because of the hybrid nature of the IBM solution, visibility into a variety of log activities and control of access is at the heart of the platform. The IBM cloud platform includes a catalog of certified IBM security services that can be implemented when needed. The catalog services takes on the responsibility of ensuring that all these disparate services can operate within this multicloud environment.

Built-in Cloud Security

IBM has created a set of built-in cloud security capabilities that can be used across a hybrid and multicloud environment. These include the following:

- Ability to gain visibility across clouds
- Access management
- Data protection

Visibility

One of the most difficult security tasks is to have consistent visibility into the security of a hybrid and multicloud environment. IBM has developed what it calls the Security Dashboard. This service provides visibility to the administrator across all platforms. It provides access to logs from all of the services being used through a series of APIs. It also provides a vulnerability advisor that helps set policies for who is allowed to access a service based on compliance and policies. The Security Dashboard (hosted in the IBM Cloud) can bring in data from private as well as public clouds such as AWS and Azure. Third-party vendors

HURWITZ & ASSOCIATES
Insight to Action

can integrate their services into the dashboard. The service keeps track of which employees or contractors are permitted to access services.

Managing Access

One of the greatest security risks in a hybrid/multicloud environment is to be able to control access at both the network level and at the individual level regarding who is allowed to access what service for what purpose. At the network level, it is imperative to be able to identify malicious access and anomalous behavior. Through the access management services, customers can gain insights from activity logs and aggregate those security events and logs in order to understand the risks across a multicloud environment.

Protect Data and Applications

Securing distributed data and applications is not easy. First, data may be at rest, in transit, or in memory. No matter the form, all of the data must be secured. The data may be managed within an object store, a cloud database, a virtual machine, or in the data center. IBM is providing a set of hyper protect data management services that is offered as a cloud service. This brings the highest level of data security and provides ways to control that security. Encryption is a key to any data protection strategy – encrypting all data will ensure that even if there is a breach, the criminals will not be able to read or understand that data. These security services can be implemented in a container, a virtual machine, or on premises in a private cloud. IBM includes key management services, including the ability for the client to be the only holder of the key – meaning that IBM itself has no copy of the encryption key.

Encryption is a key to any data protection strategy – encrypting all data will ensure that even if there is a breach, the criminals will not be able to read or understand that data.

Customers that use LinuxONE or IBM Z as a cloud service are able to take advantage of the platform's pervasive encryption technology. Pervasive encryption can encrypt data both at rest and in flight, and this type of encryption doesn't require application changes. This approach enables companies to encrypt all their data by default with little compute overhead. Because of the overhead of software encryption, businesses in the past have been forced to choose which data to encrypt, leaving the remaining data at risk. In nearly every online interaction, data is left unencrypted at some point in the process. This point, when data is left unencrypted, gives wrongdoers the opportunity to steal data. IBM Z and LinuxONE both have dedicated hardware specifically tuned for encryption. The on-chip encryption co-processor is on every compute chip next to the main processor and can encrypt up to 13 gigabytes (GB) of data per second per core.

Key Protect is a cloud-based security service that provides lifecycle management for encryption keys used in IBM Cloud services. The service enables customers to import their own Roots of Trust (RoT) keys into the cloud service. With the Key Protect API, it is possible to encrypt and decrypt the keys that are associated with a service or data so that the customer controls data security in the cloud. The key protect service complies with the Federal Information Protection Standard (FIPS) 140-2, Level 4, the highest level of protection available.

Managing distributed applications is likewise challenging. IT management

HURWITZ & ASSOCIATES
Insight to Action

must be able to understand the security requirements of the application and be prepared to authenticate the end user. Where is that application allowed to run? Can it run anywhere or are there geographic restrictions? Are there some applications that should only run in the data center or in a private cloud? Can that application migrate from one public cloud to another? The IBM service provides an API-driven industry standard App ID that authenticates users and implements policies regarding who can access data and where it can run. It provides this service across all applications that are part of the hybrid environment.

Additional IBM Cloud Security Offerings

In addition to these core services, IBM offers its broad portfolio of security products including QRadar (both on the cloud and on premises), security connect, cloud Identity, Guardium, and Hybrid Cloud Security and compliance services.

Managing a multicloud hybrid environment

IBM has developed a platform designed to support the need to manage workloads across a hybrid and multicloud environment. This service, called Multicloud Manager (MCM), is a command and control service to manage Kubernetes deployments. The service provides lifecycle for governance, policy management and security in a hybrid environment by managing Kubernetes clusters. The service can manage clusters in either a public or private cloud. To address the needs of virtual machine- (VM) based workloads, MCM can work in conjunction with IBM's Cloud Automation Manager (CAM). CAM can provision the VM, put it into a Kubernetes cluster and then connect back to MCM for management. MCM is designed to provision services across multiple public clouds including AWS, Azure, Google Cloud, and IBM's cloud services.

One of the benefits of MCM is that it can scale out Kubernetes clusters and dynamically add and remove nodes. As applications and services are deployed, MCM provides standards-based Terraform as its load balancer. In fact, all of the services that underlie MCM are based on accepted and emerging open source standards. MCM is available either as a software license or as a managed service.

MCM also provides a consist way to manage integration. To reduce the footprint of integration, the service provides a common user interface, common APIs, and common API management, as well as common logging and management services. The common APIs provide a platform for hybrid cloud data exchange data and business process management services. One of the benefits of the Integration service is that it permits businesses to incorporate existing enterprise services such as billing and transaction management services so that they can be seamlessly integrated with cloud services. MCM also plays an important role in managing security. The only way to secure a distributed environment is to containerize both workloads and data that provide consistent APIs. A containerized approach enables applications, operations, and data services to all

Multicloud Manager (MCM), is a command and control service to manage Kubernetes deployments. The service provides lifecycle for governance, policy management and security in a hybrid environment by managing Kubernetes clusters.

HURWITZ & ASSOCIATES
Insight to Action

be managed in a consistent manner to support security and governance.

The Multicloud Manager is designed with a central point of control so that it incorporates a customer hub to manage the Kubernetes environments. This hub includes a graphic user interface that shows where pods are running, and what the compliance rules are in place across cloud services. Out of the box, MCM includes identity and access management for all services being managed. One of the reasons why MCM is well suited for a hybrid and multicloud environment is that the offering does not have to know in advanced which cloud platform each cluster is running. The system will show the administrator where the cluster is running and indicate the health across clouds. It will notify the administrator if a pod or cluster is failing and indicate the performance of each service, no matter which cloud it is running on. The solution abstracts events and leverages management services such as ServiceNow or IBM's NetCool via APIs to indicate the performance of the overall multicloud environment.

In addition, MCM manages the configuration setting across cloud environments in an abstracted way so that the developer doesn't have to set the right indicators. By enforcing consistent policies and configurations across environments, organizations can avoid the performance, cost and security problems that can occur when developers fail to implement the correct configuration settings.

Managing and Analyzing Distributed Data

As customers begin to migrate to hybrid and multicloud environments, they need to have a consistent and predictable way to manage all of their data sources. This is not an easy proposition since the typical enterprise has a multitude of different databases and data sources that they rely on.

The only practical way of understanding and managing this complex set of data sources in a consistent and predictable way is to leverage advanced machine learning algorithms. To address the challenges of managing, ingesting and analyzing data from a variety of sources, IBM has built machine learning and Artificial Intelligence capabilities throughout the platform. The machine learning technology streamlines and automates time intensive tasks like data cleansing, integration, and cataloging of business ready data.

IBM's Cloud Private for Data (ICP for Data) is composed of a set of pre-configured microservices that run on a multi-node IBM Cloud Private cluster. The microservices enable the organization to connect to a variety of cloud and on premises data sources including relational, NoSQL, IoT, and text data, so they can be consistently catalogued, governed, transformed, and analyzed through a single web application. This pre-integration means that the data layer doesn't require customers to integrate various data management and analytics offerings.

Many companies have tried to break down silos by copying data from different operational systems into central data stores for analysis such as data marts, data

IBM's Cloud Private for Data (ICP for Data) is composed of a set of pre-configured microservices that run on a multi-node IBM Cloud Private cluster.

HURWITZ & ASSOCIATES
Insight to Action

warehouses and data lakes. There are many problems that occur during this data movement. For example, it is expensive, time consuming and cumbersome to manage so many disparate data sources. Data can be inadvertently exposed when data is disconnected from security and governance policies. To avoid the challenges of replicating and moving data for analytics, IBM has developed a data virtualization approach called IBM QueryPlex. Queryplex allows an analytics application to submit a query that is then processed on the system where the data resides. Results of the query are then sent back to the analytics application.

In addition, all of the data services in the IBM Cloud platform are delivered in containers and supported by Kubernetes-based orchestration services. The result of this containerized approach is that IBM hybrid database services can operate on any public or private cloud service including the IBM Cloud, Amazon AWS, and Microsoft Azure. In addition, the platform has standardized APIs to support all services to ease the ability to integrate services.

In addition, all of the data services in the IBM Cloud platform are delivered in containers and supported by Kubernetes-based orchestration services. The result of this containerized approach is that IBM hybrid database services can operate on any public or private cloud service including the IBM Cloud, Amazon AWS, and Microsoft Azure.

The IBM cloud data platform can support a variety of the most widely used relational databases including Db2 and the Db2 Warehouse, Oracle, as well as NoSQL, MongoDB, Postgres, and IBM's Event Store for streaming data from sources like IoT workloads. Within the next year IBM expects to bring on additional data services platforms through its partnerships including Redis, an in-memory datastore.

To be effective in a hybrid cloud environment it is important that there are core foundational services that make it easier to combine data from a variety of sources in a meaningful and accurate manner. Services provided in the IBM Cloud data platform are broken up into two segments: Foundational Platform Services and Premium Services.

Foundational Platform Services

There are three types of foundational services in the IBM cloud data platform:

- Manageability services (dashboard, access to scalable storage services, APIs to link to infrastructure services, business glossary)
- Governance and security
- End to End Data Management integration- data ingestion, data virtualization, ETL, catalog, data curation, meta data management and classification

Premium Services

Once the foundational services are in place, the data platform is designed to enable customers to add premium services – either those offered by IBM or those offered by partners. These premium services are primarily used for reporting, advanced analytics and artificial intelligence (AI). The Watson APIs are available on the multicloud platform to add AI functionality to customer applications. Some of these Watson APIs include Watson Assistant, to help build chatbots; Speech to Text to convert audio and voice into written text; Tone Analyzer to understand emotions and communication style in text; and, Visual Recognition to tag, classify and train visual content. For customers who need

HURWITZ & ASSOCIATES
Insight to Action

basic reporting and business analytics services, there are the Cognos tools and dashboard. For advanced analytics such as predictive analytics and machine learning, IBM offers tools and services including SPSS to build predictive analytics solutions. In addition, IBM offers Watson Studio to leverage open source machine learning libraries to create machine learning-based applications.

The IBM Cloud data platform is designed to help customers break down data silos across their own departments and across all of the various data sources they need to manage their business. The fact that the platform is based on containers, microservices, and APIs enhances the ability to make data services become an equal citizen in creating a scalable hybrid and multicloud environment that is imperative to ensuring that the hybrid and multicloud environment can support the goals of the business.

Leading with Open Standards to Support the Scalable Hybrid Cloud

IBM has been on a journey to create a hybrid, multicloud environment to support the need of its enterprise customers. Open Source and most importantly Linux and Kubernetes play a pivotal role in IBM's transformed cloud strategy. In light of the concentration on open source, it is not surprising that IBM would acquire Red Hat as a natural partner to execute on its strategy. The combination of an adherence to standards and open source and the focus on enterprise scalability should position IBM well for the future.

Open Source and most importantly Linux and Kubernetes play a pivotal role in IBM's transformed cloud strategy. In light of the concentration on open source, it is not surprising that IBM would acquire Red Hat as a natural partner to execute on its strategy.

HURWITZ & ASSOCIATES
Insight to Action

About Hurwitz & Associates

Hurwitz & Associates is a strategy consulting, market research and analyst firm that focuses on how technology solutions solve real world customer problems. Hurwitz research concentrates on disruptive technologies, such as Cloud and Multicloud Management, Big Data and Analytics, Machine Learning and Artificial Intelligence, Information Security, DevOps, and emerging infrastructure platforms that are defining the future of business agility. Their experienced team merges deep technical and business expertise to deliver the actionable, strategic advice clients demand. Additional information on Hurwitz & Associates can be found at www.hurwitz.com.

35 Highland Circle • Needham, MA 02494 • Tel: 617-597-1724
www.hurwitz.com