Cloud Customer Architecture for Hybrid Integration

Executive Overview

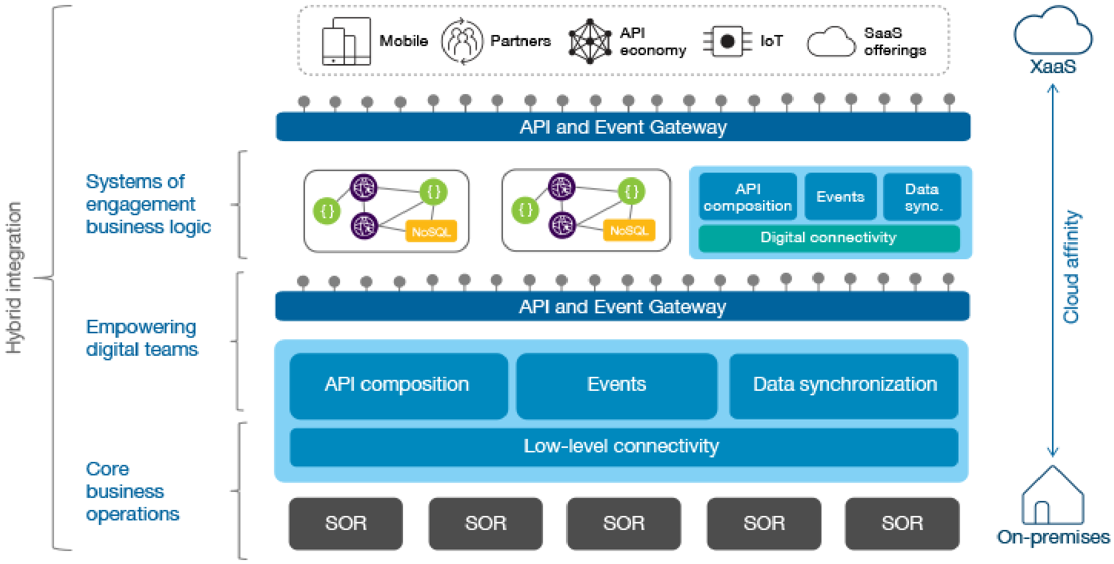
IT environments are now fundamentally hybrid in nature – devices, systems, and people are spread across the globe, and at the same time virtualized. Achieving integration across this ever changing environment, providing it at the pace of modern digital initiatives, and still being able to manage the landscape is a significant challenge.

With the growing need to connect heterogeneous endpoints in various locations, a Hybrid Integration platform is crucial. Leading-edge enterprises are starting to leverage a hybrid integration platform to take advantage of best of breed cloud-based and on-premises integration approaches. Companies that adopt cloud applications view application integration as the critical component to harmonize business processes across their hybrid application landscape. Scenarios of hybrid cloud integration include the following examples:

- Viewing customer information between cloud based customer relationship management (CRM) systems and on-premises enterprise resource planning (ERP) applications.
- Employee data integration between cloud based human capital management systems and back-office applications.

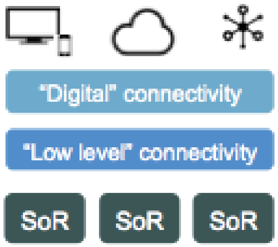
The hybrid integration reference architecture explores common patterns seen in enterprises tackling these issues. This document explains the core reference architecture and concepts for hybrid integration in the enterprise. For a full understanding of the motivations and issues around hybrid integration, refer to the article, *The Evolving Hybrid Integration Reference Architecture*. [1]

Hybrid integration can be looked at from many perspectives including application, data, and infrastructure. This document positions hybrid integration from an application perspective, and presents the reference architecture as a seamless integration from cloud to on-premises for events, APIs, and data.



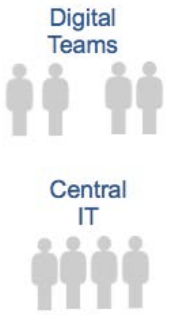
The hybrid integration reference architecture addresses the following considerations:

- **Connectivity**: Integration is about connecting systems and devices with other systems and devices. Integration may involve low level connectivity to systems of record (SoR) and it may require the need to leverage modern interfaces on cloud native systems. In short, any system, anywhere, must be enabled as a first class citizen in the integration landscape.



- **Deployment**: Since modern systems are deployed across a broad landscape of systems, the accompanying integration components must have equally flexible deployment options. The components should be as easy to run on premises in an enterprise as it is to deploy on public cloud platforms. Equally, components should be well equipped to run directly on bare metal, in virtual machines, or in containers. They should be able to integrate within and across network and security boundaries.

- **Roles**: IT in general has become bi-modal, and sometimes multi-modal with independent teams working at different velocities. Integration needs to encompass people from across the entire business. Hybrid integration expands beyond the realm of just integration specialists. Integration standards and tooling have evolved to the point that straightforward integrations can be performed directly by business users and shadow IT departments that are aligned with the line of business. Complex integrations are now often collaborative, where the work of one team in surfacing events or APIs becomes the building blocks for another team.



- **Styles**: In the past, discrete patterns of integration often needed to be blended together to deliver complex solutions. Now, enterprise integration can be combined with APIs, events, and data – tooling and runtimes need to make this as seamless as possible.

Gateway
API
Events
Data

The key to success for hybrid integration architectures is the ability to reduce friction across boundaries, with platform agnostic runtimes that are self-managed or provided as a service along with common frameworks and tooling.

The focus is enabling teams to create valuable assets (APIs, events, and data) for other teams to consume. The ultimate goal is for teams to become self-sufficient in addressing their integration needs to the highest degree possible, while still retaining the ability to manage and refine the more business-critical integrations.

Cloud Customer Architecture for Hybrid Integration Components

The hybrid integration architecture components are illustrated in Figure 1.

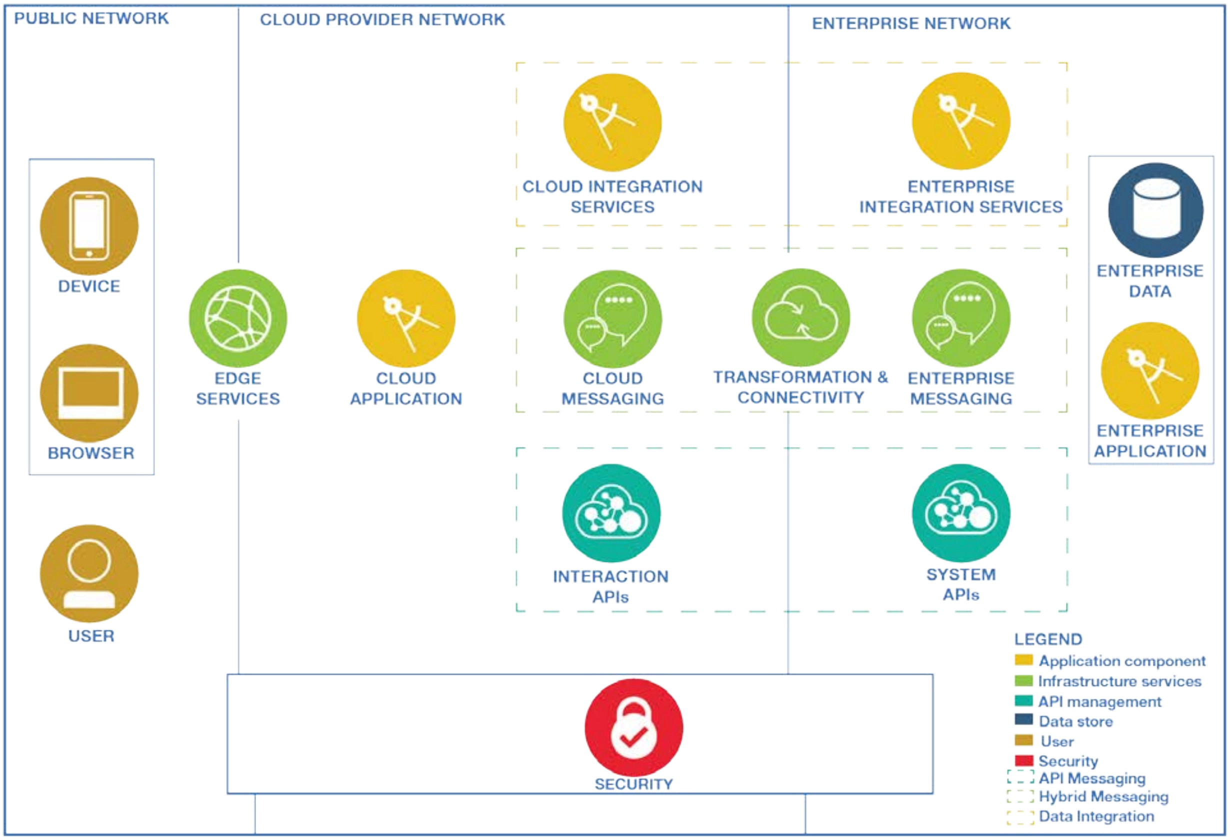


Figure 1 : Cloud Customer Hybrid Integration Architecture

Hybrid Integration provides a seamless platform for applications – both cloud native and on-premises – to interchangeably consume services in their integration patterns in order to implement end-to-end comprehensive mission-critical business capabilities regardless of application platform and deployment model. There are specific tools, technologies, and runtimes that address APIs, events, and data synchronization which are discussed in more detail.

Figure 1 consists of the following three tiers:

- Public Network
- Cloud Provider Network
- Enterprise Network

Security is a cross-cutting theme that is applicable to all three tiers.

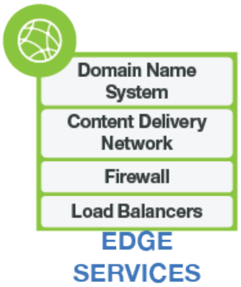
Public Network

User

Users access applications on the cloud provider network using a browser or via a mobile native app. The users could be end consumers or enterprise line of business users of the cloud applications. They could also be enterprise administrative users from the line of business 'Digital IT' team managing the components deployed within the cloud network.

Edge Services

Edge services include service capabilities needed to deliver function and content to the users via the internet. These include:



- **DNS Server** – The Domain Name System (DNS) server maps the text URL (domain name) for a particular web resource to the TCP-IP address of the system or service that can deliver that resource to the client.
- **Content Delivery Network (CDN)** – Content Delivery Networks are geographically distributed systems of servers deployed to minimize the response time for serving resources to geographically distributed users, ensuring that content is highly available and is provided to users with minimum latency. Which servers are engaged will depend on server proximity to the user and where the content is stored or cached.
- **Firewall** – A Firewall is a system designed to control communication access to or from a system, aiming to permit only traffic meeting a set of policies or rules to proceed and blocking any traffic that does not meet these policies. Firewalls can be implemented as separate dedicated hardware, or as a component in other networking hardware such as a load-balancer or router or as integral software to an operating system.
- **Load Balancer** – Load Balancers distribute network or application traffic across many resources (such as computers, processors, storage, or network links) to maximize throughput, minimize response time, increase capacity, and increase reliability of applications. Load balancers can

balance loads locally and globally. Considerations should be made to ensure that this component is highly available and is not a single point of failure.

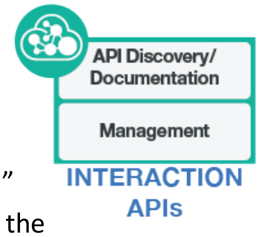
Cloud Provider Network

Cloud Application

The Cloud Application component represents the application designed and developed within the cloud environment. Such applications often use modern techniques such as microservices architecture utilizing, among other things, lightweight runtimes, container technology, and DevOps methods to improve agility, scalability, and resilience. The application's capabilities are often exposed as APIs. Cloud applications that need to access data from other systems can make use of the hybrid integration architecture via API calls, messaging, and data integration services.

Interaction APIs

Interaction APIs provide access to enterprise capabilities. These APIs are maintained by the lines of business 'Digital IT' teams, and are composed typically from lower level fine-grained system APIs. These APIs are business led, looking to cater to market needs rather than being driven by the underlying enterprise systems. They are sometimes also exposed externally, and may even be "monetized" with a funding model based on their usage. This component is the *API gateway* into the enterprise network.

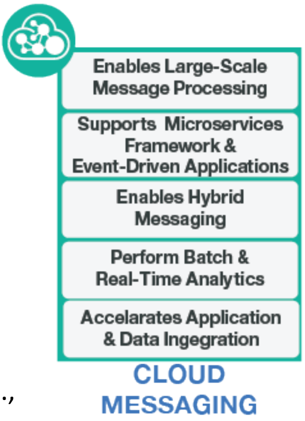


The Interaction APIs component advertises the available services endpoints to which the cloud application has access. This component provides API discovery, catalogs, and connection of offered APIs to service implementations and management capabilities, such as API versioning.

- **API Discovery/Documentation** – Provides the ability for 'Digital IT' developers to find and use APIs securely.
- **API Management** – Provides a management view into API usage by applications and mobile apps using information from gateways, backends, etc.

Cloud Messaging

Cloud Messaging provides fast, scalable, high throughput event delivery to and from the enterprise network. This component needs to support multiple open event protocols in a multitude of programming languages. At the same time, this component abstracts away from its consumers any proprietary non-standard protocols of the enterprise messaging. This component is the *Event gateway* into the enterprise network.



Enables Large-Scale Message Processing
Supports Microservices Framework & Event-Driven Applications
Enables Hybrid Messaging
Perform Batch & Real-Time Analytics
Accelarates Application & Data Ingegration
CLOUD MESSAGING

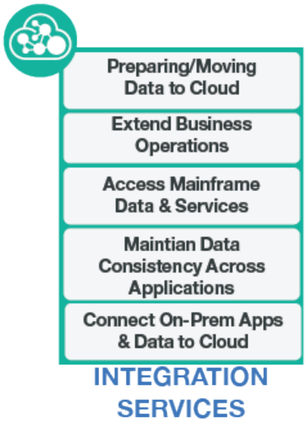
The capabilities of Cloud Messaging include the following:

- **Enables large scale message processing** both in volume and velocity, e.g., real-time streaming events.

- **Supports a microservices framework and event-driven applications** enabling wiring of microservices and other applications together by using open protocols.
- **Enables hybrid messaging** between events on cloud platforms and on-premises enterprise messaging systems.
- **Performs batch and real-time analytics** connecting stream data to analytics engines in order to realize powerful insights.
- **Accelerates applications and data integration** feeding event data to multiple applications to react in real time.

Cloud Integration Services

Cloud Integration Services provide rapid, simple and flexible capabilities for cloud services and third-party applications to integrate with enterprise applications and data. Unlike traditional Enterprise Application Integration (EAI) and ETL solutions that enable complex low-level integration, this component offers simple integration tooling with targeted capabilities where customization can be performed via 'configuration and not code' by people who are not integration specialists. This component is the *gateway* into SoR (System of Records) within the enterprise network.

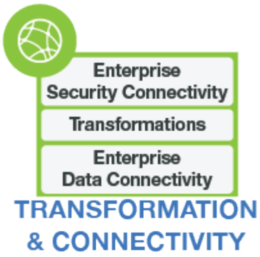

Preparing/Moving Data to Cloud
Extend Business Operations
Access Mainframe Data & Services
Maintian Data Consistency Across Applications
Connect On-Prem Apps & Data to Cloud
INTEGRATION SERVICES

Capabilities include:

- **Preparing/moving data to cloud**, e.g., ability to access SoR data and replicate with cloud data repositories.
- **Extend business operations** by providing a cloud footprint for on-premises enterprise capabilities via services such as enterprise service bus or business process management.
- **Access mainframe data and services** via APIs and connectors.
- **Maintain data consistency across applications** providing the ability to exchange information updates across applications regardless of whether they are on-premises or native.
- **Connect on-premises apps and data to cloud** with synchronization services through connectors and APIs.

Transformation and Connectivity

The Transformation and Connectivity component enables secure connections to the enterprise systems. This component includes the following capabilities:

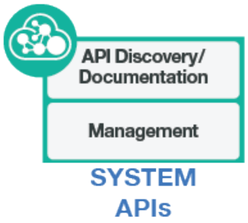

Enterprise Security Connectivity
Transformations
Enterprise Data Connectivity
TRANSFORMATION & CONNECTIVITY

- **Enterprise Secure Connectivity** – Integrates with enterprise data security to authenticate and authorize access to enterprise systems.
- **Transformation** – Transform and enrich data in message headers and payloads as they go through different network domains and heterogeneous platforms.
- **Enterprise Data Connectivity** – Provides the ability for cloud components to connect securely to enterprise data; examples include VPN and gateway tunnels.

Enterprise Network

System APIs

System APIs provide access to enterprise applications and enterprise data. These APIs are maintained by the ‘Central IT’ team, and are typically lower level fine grained APIs. Multiple Interaction API components may consume these APIs to compose higher-level capabilities.

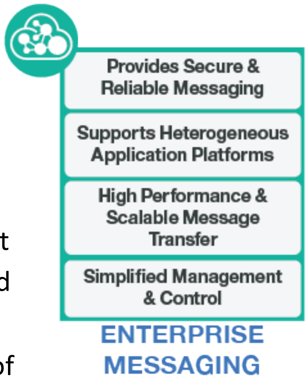


The System APIs component advertises the available services endpoints to which Interaction API components have access. This component provides API discovery, catalogs, and connection of offered APIs to service implementations and management capabilities, such as API versioning.

- **API Discovery/Documentation** – Provides the ability for both ‘Digital IT’ and ‘Central IT’ developers to find and use APIs securely.
- **API Management** – Provides a management view into API usage by applications and mobile apps using information from gateways, backends, etc.

Enterprise Messaging

Enterprise Messaging represents the messaging backbone of the enterprise. This component is the primary messaging interface into the enterprise for the Cloud Messaging component.


Provides Secure & Reliable Messaging
Supports Heterogeneous Application Platforms
High Performance & Scalable Message Transfer
Simplified Management & Control
ENTERPRISE MESSAGING

- **Provides secure and reliable messaging.** Provides reliable delivery, without message loss, duplication or complex recovery. This component preserves message integrity throughout the network, protects data, and helps ensure regulatory compliance with security rich functions.
- **Supports heterogeneous application platforms.** Integrates with a mix of heterogeneous applications with support for multiple platform configurations, including industry-standard JMS messaging, scalable publish-subscribe (pub-sub), and a choice of application programming interfaces (API).
- **Provides high performance and scalable message transfer** that can address evolving workloads and new mobile and cloud deployments. Delivers a highly available solution with fully automated failover, dynamically distributed messaging workloads available through clustering, high throughput, low-latency solution with support for multicast.
- **Provides simplified management and control** allowing visibility and tracking of messages and files for gaining insights through a single dashboard view. A quick audit of the movement of data and completion of transactions is also supported.

Enterprise Integration Services

Preparing/Moving Data to Cloud
Extend Business Operations
Access Mainframe Data & Services
Maintian Data Consistency Across Applications
Connect On-Prem Apps & Data to Cloud
INTEGRATION SERVICES

Enterprise Integration Services represents a broad variety of integrations including Enterprise Application Integration (EAI) components, Data Warehouse (ETL) systems, and Business Process Management systems that exist within the enterprise network. This component is the primary integration interface into the enterprise for the Cloud Integration Services component.

Capabilities include:

- **Preparing/Moving data to cloud** to expose SoR data and prepare for replication with cloud data repositories.
- **Extend business operations** by providing access to on-premises enterprise capabilities such as enterprise service bus or business process management to native cloud applications.
- **Access to mainframe data and services** is enabled with connectors and APIs.
- **Maintain data consistency across applications** by exchanging information updates across applications regardless of whether they are on-premises or native.
- **Connect on-premises apps and data to cloud** with synchronization services through connectors and APIs.

Enterprise Application

Enterprise Application represents applications that run enterprise business processes and logic within existing enterprise systems.

Enterprise Data

Enterprise Data represents the one or more systems of record, for example, transactional data or data warehouses that represent the existing data in the enterprise.

Security

Identity & Access Management
Data & Application Protection
Security Intelligence
SECURITY

Security for hybrid integration addresses the following needs:

- Integrity – Ensures both cloud and enterprise data is not tampered with.
- Threat management – Maintain cloud components up-time despite security threats.
- Compliance – Addresses any industry and regulatory compliance needs.

Capabilities include:

- **Identity & Access Management** – Capabilities to identify and authorize the user providing role-based access to cloud applications. It also enables single sign-on, user lifecycle management, and audit logging. The user types and their levels of access for cloud applications need to be managed. This could include business users (customer, vendor, 3rd party, staff users) or IT users (administrators, privileged users, application users). Identity and access management could leverage the enterprise user directory.

- **Data and Application Protection** – Capabilities that help identify vulnerabilities and prevent attacks targeting sensitive data. It provides protection to cloud components against many malicious threats right from the beginning of the development cycle. In addition, it monitors privileged access to sensitive data. It also protects integrity of sensitive data in transit and at rest and provides network isolation. Firewalls in the public network component tier help protect the network level flows to application and data.
- **Security Intelligence** – Capabilities to monitor the cloud components for security breaches to provide visibility. It provides actionable intelligence to detect and defend against threats using event and log analysis that feeds to a corporate incident management system. Security reports also support regulatory compliance. Security and security management applies across the lifecycle – design, development, deployment and ongoing maintenance. Security governance is an integral part of security management.

Runtime Flow

Use Case 1

Figure 2 illustrates a flow for a user accessing a cloud application that is architected using the hybrid integration style of architecture.

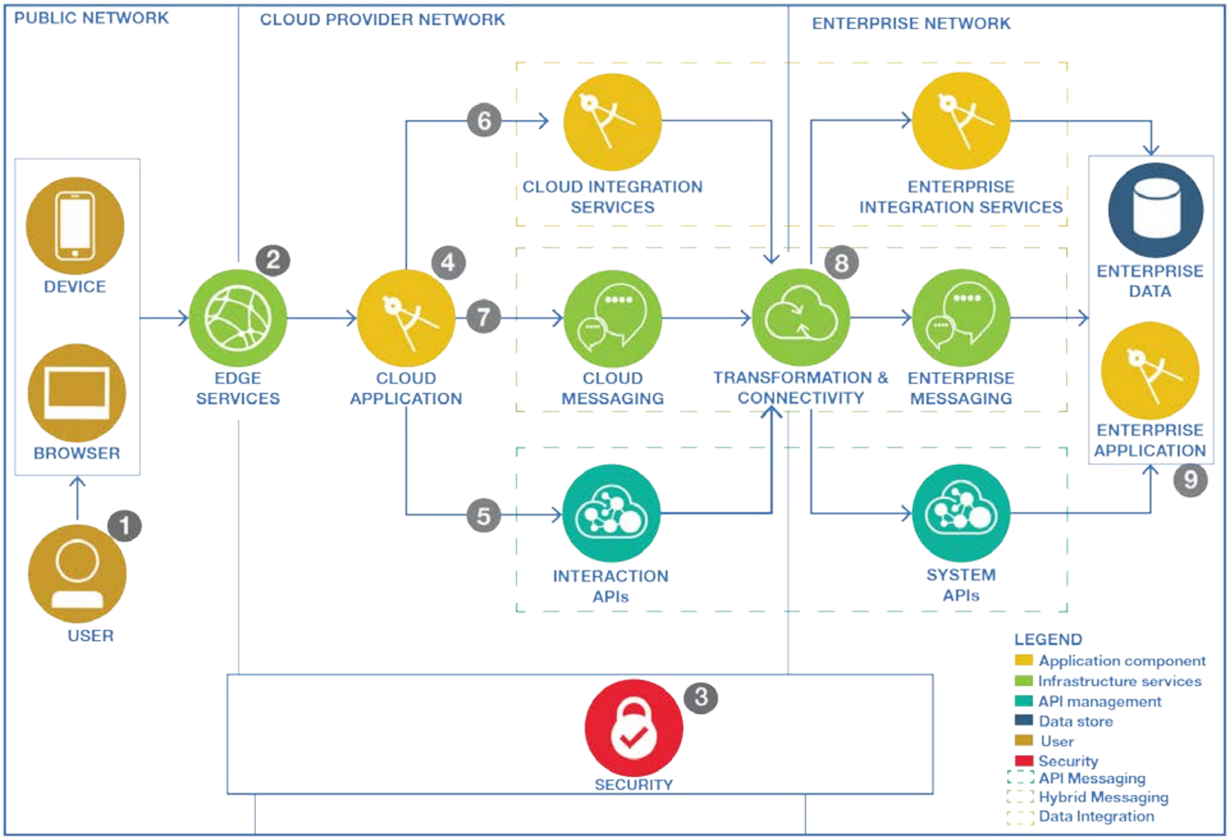


Figure 2: Flow of Interactions

In the scenario depicted above, the CTO of an international bank wants to unlock the value of the bank's business assets by deploying a set of fine-grained system APIs that expose key enterprise capabilities and processes. The CMO wants to expand the bank's market reach by deploying cloud applications and APIs to new interactive channels that would use these enterprise capabilities to accelerate banking transactions and improve the customer experience.

1. Bank customer accesses the cloud application from a web browser.
2. Edge services process the request and route it to the right destination.
3. The user is validated through identity and access management. A key aspect of security is that it is enabled across multiple layers and components. Besides user validation, the cloud and the enterprise components are protected from threats. Individual cloud components are validated prior to accessing the enterprise network using a combination of application IDs, access tokens, and mutual authentication. Sensitive data is protected from end users and privileged users. Continuous monitoring of threats and log analysis in the solution provide visibility and actionable intelligence. Logs are used for audit and compliance reports.
4. The request is received by the cloud application and processing of the request occurs. Making use of asynchronous processing, the cloud application invokes the Interaction APIs and Cloud Integration Services components.
5. The Interaction APIs component receives the request and determines the services that need to be invoked. Additionally, this component validates that the cloud application is authorized and entitled to make the request. In order to process the request, this component makes several successive calls to the System APIs component.
6. The request is received by the Cloud Integration Services component to access enterprise data. After validating the authorization and entitlement, this component interfaces with the Enterprise Integration Services component to retrieve and return enterprise system of record data.
7. Cloud Messaging allows the processing of events and triggers across cloud applications cloud services and on-premises enterprise applications.
8. The Secure Transformation and Connectivity component ensures requests are authorized to access the enterprise components. This component routes the API request to the System APIs component and the data request to the Enterprise Integration Services component.
9. The enterprise application and data components process their requests. The responses are returned back through the enterprise and cloud gateways to the cloud application. The cloud application prepares and returns a response back to the User.

Use Case 2

Figure 3 illustrates a flow for a member accessing a cloud service that is architected using the hybrid integration style of architecture.

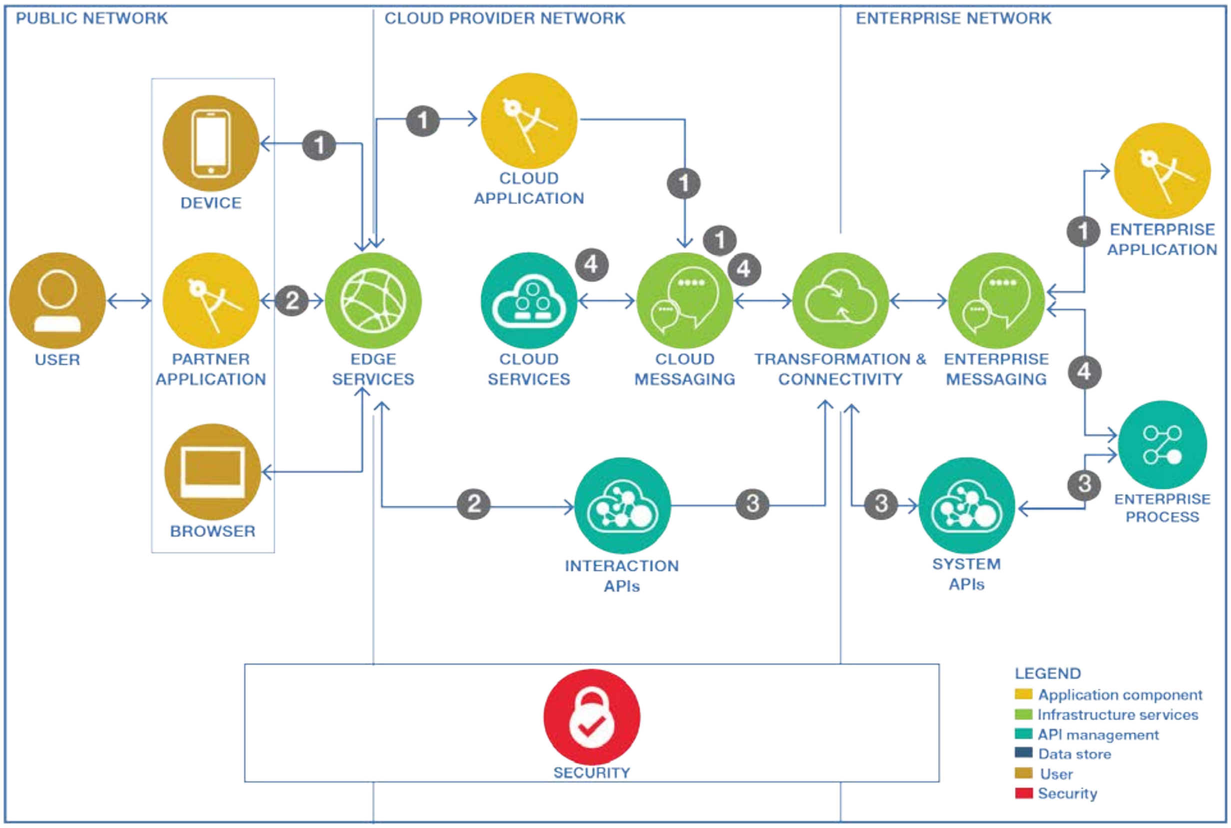


Figure 3: Flow of Interactions

The schematic above illustrates a scenario where an insurance company is rewarding their members with annual premium discounts for participating in fitness activities. However, they do not want high risk members to over exert themselves creating a health crisis. When such a situation is determined, the company sends alert notifications to the member.

1. The member uses a mobile app to log their calories and track their walking steps. These events are sent to the cloud app which in turn places them in the queue for the on-premises application to aggregate and compute the discount percentage on the premium.
2. The member's primary doctor receives the test results. He logs into his hospital's portal to report the test data. As a partner to the insurance company, the hospital's portal invokes an interaction API to report the data.
3. The interaction API invokes an on-premises system API to process the data.
4. The system API triggers an enterprise business process to handle the data. The business process using business rules detects that the member is having a heart arrhythmia condition and is participating in rigorous fitness activity. It then sends an alert to the following cloud services: Mobile Push Notification to send an SMS text or mobile alert to the member.

Cloud Deployment Considerations

Cloud environments offer tremendous flexibility with less concern for how components are physically connected. The need for advanced planning is reduced but still important. This section offers suggestions for better provisioning of data and computing resources.

Initial Criteria

- Elasticity
- CPU/GPU and Computation
- Resilience
- Security

Elasticity

Elasticity is the ability for a cloud solution to provision and de-provision computing resources on demand as workloads change. Public clouds have a distinct advantage since they generally have larger pools of resources available. You also benefit by only paying for what you use. Private clouds and dedicated hardware can make up some of the difference with higher bandwidth data paths.

For hybrid integration use cases, enterprises are placing workloads in environments that are most appropriate based on scaling needs due to business demands. Cloud bursting of on-premises core business capabilities during seasonal surge is an example; replicating selected customer information to a lightweight cloud database for quicker access by mobile apps is another. Hybrid integration needs fluctuate over time and a cloud platform will ensure that application workloads provide the same functionality regardless of their deployment form factor.

CPU/GPU and Computation

The availability of inexpensive commodity processors means the private and hybrid cloud server farms are more viable than in the past. Modern development environments using Hadoop, Spark and Jupyter (iPython) take advantage of these massively parallel systems.

A GPU (Graphics Processor Unit) which started out as a peripheral supplementing the central processing unit (CPU), and previously used to produce sophisticated video and graphics, such as video games, has completely repositioned itself to become the central component in high performance computing, self-driving cars, artificial intelligence, drones, robots, search engines, interactive speech, video recommendations and much more.

A GPU built on massively parallel architecture has thousands of smaller, more efficient cores designed to handle multiple tasks simultaneously, and is capable of accelerating software by 100x. It is used to accelerate deep learning, analytics, and engineering applications. Modern development environments using Hadoop, Spark and Jupyter (iPython) take advantage of these massively parallel systems.

Streams and high speed analytics are an emerging area where cloud applications leverage more powerful processor pools to enable real-time, in-motion data solutions. Dedicated hardware allows for faster development and testing prior to migration towards hybrid and public environments.

A robust hybrid integration platform might require the deployment of multiple environments to support development lifecycle requirements, regional compliance for data location and isolation or simply dedicated runtimes or data repositories. A cloud infrastructure provides this flexibility in provisioning resources.

Resilience

Resilience and fault tolerance is key to a successful Hybrid Integration platform. Hybrid Integration platforms should not depend on one single component at any point and should tolerate the failure of a single component, such as a gateway or a data repository. Components in the provider cloud can be made resilient through clustering and the use of multiple instances of programs and cloud services combined with data replication and redundancy on multiple storage systems.

The networks should also be resilient, for example with multiple paths and multiple providers in the public network. There is no silver bullet to make the entire network available all the time but it should be a highly available and resilient. It is important to ensure that the connectivity capabilities can support resilience.

Security

As more data about people, financial transactions, and operational decisions is collected, refined and stored, the challenges related to information governance and security increase. The data privacy and identity management of devices and individuals is very important from a cloud computing point of view. The simple fact that more people have access to data calls for better monitoring and compliance strategies. The cloud generally allows for faster deployment of new compliance and monitoring tools that encourage agile policy and compliance frameworks. Tools that monitor activity and data access can actually make cloud systems more secure than standalone systems. Hybrid systems offer unique application governance features: software can be centrally maintained in a distributed environment with data stored in-house to meet jurisdictional policies.

Security related to Hybrid Integration revolves around the capability of providing seamless secure data flow between the cloud environment and the on-premises data centers. A Hybrid Integration platform will be able to take advantage of the many standard gateway services and network security capabilities provided by cloud providers such as security gateway services, TLS tunneling, and VPN Services.

Hybrid Cloud and Hybrid Integration

An enterprise routinely needs a combination of public cloud, private cloud, and on-premises components that when linked create a hybrid cloud. Hybrid cloud computing is a deployment model which involves combining the use of multiple cloud services across different deployment models – in particular, combining the use of public cloud services with private cloud services and existing on-premises enterprise systems. See the CSCC's *Practical Guide to Hybrid Cloud Computing* for more information about hybrid cloud. [3]

Businesses implementing hybrid cloud solutions are looking for flexibility and agility in delivering new capabilities. The examples below explain the need for hybrid cloud deployment in support of Hybrid Integration:

- Mobile workforce using mobile applications deployed on the public or private cloud and invoke APIs that access data and transactions located in on-premises data centers.
- Market channel expansion where the enterprise digital platform is hosted on a cloud environment and expose core business capabilities from backend systems residing on-premises via a set of APIs.
- Enterprise B2B integration where inter-enterprise collaboration is enabled through a set of APIs hosted on a cloud platform and brokering B2B capabilities from on-premises back-ends, enterprise private clouds or external cloud services such as commercial SaaS applications.

References

[1] The Evolving Hybrid Integration Reference Architecture
http://ibm.biz/HybridIntRefArch

[2] The Industrial Internet Consortium's Industrial Internet Reference Architecture IIRA paper
http://www.iiconsortium.org/IIRA.htm

[3] Cloud Standards Customer Council 2016, Practical Guide to Hybrid Cloud Computing
http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Hybrid-Cloud-Computing.pdf

Acknowledgements

The major contributors to this whitepaper are: Swami Balasubramanian (IBM), Kim Clark (IBM), Heather Kreger (IBM), John Leung (Intel), Rob Nicholson (IBM), Tien Nguyen (IBM) and Anna Pasupathy (Equinix).