Connecting Your Enterprise: An API-Centric Approach

By Peter Jarman and Ross Garrett

Peter Jarman, Principal Technology Architect, Digital and Integration Services at Infosys has over 30 years' experience in IT, covering a wide range of business domains. He has significant experience across EAI, BPM, SOA, Digital/Online, Enterprise Architecture and Solution Architecture, and has published a variety of technical papers on these topics.

Ross Garrett, Sr. Director Product Marketing at Axway is responsible for product strategy, marketing and positioning across Axway's API Management & Security portfolio. Ross has helped a range of organizations across multiple industries embrace the value of Web APIs. He is a regular speaker at industry and analyst events.

The Changing World of B2C, B2E, B2B and Cloud Integration

Enterprise IT is facing a sea change — not just in terms of technology, but also in how customers and employees expect products or services to be delivered to them. Perceptions of IT across the board reflect decades of IT saying "no" or limiting flexibility and choice for end-users, typically due to well-intentioned concerns around security and manageability. This perception, and the reality behind it, has driven users to look elsewhere for the tools they need, and as a result organizations now have increasingly less control of their data.

What began with a few employees wanting to access business email on their iPhones has quickly spread to massive adoption of personal devices for business use, including laptops, tablets, smart phones and soon perhaps even wearables. And since users cycle between the latest and greatest technologies extremely quickly, managing security at the device level is no longer a realistic approach, making data security an ever-present worry for system administrators. But the challenge isn't limited to BYOD. Users have also been quick to realize that a range of SaaS applications and cloud-based services can improve their productivity and make their work life easier compared with using corporate-issue products and services. The result is a massive but uncontrolled adoption of products such as Dropbox, Salesforce, Amazon Web Services and Google Apps.

Traditional IT requirements are still valid, yet there is an obvious need for wholesale change in how IT enables corporate users, provides choice, and retains (or regains) control over, and visibility into the flow of corporate data. IT must ask itself a fundamental question: Are the various platforms and solutions underpinning the last ten years of enterprise integration really up to the job of supporting today's demands for agility, connectivity and flexibility? The imperative to support these new demands is impacting IT organizations in four primary ways, spurring:

1. Organizational changes better aligned with providing services to the business
2. A focus on reducing the cost of service delivery, especially through automation
3. A move away from monolithic or large custom development and toward a more lightweight and agile API-oriented approach
4. Re-thinking of IT network topology to enable low-cost integration with cloud-based providers

The Emergence of Hybrid Enterprises

Moving toward greater agility and flexibility, most organizations have now started to embrace the very same cloud applications that previously existed as islands among individuals or teams. But ease of use at the level of one individual or one team is a different order of concern when embraced enterprise-wide. CIOs who endorse and enable corporate use of enterprise cloud services are answering the call for agility and flexibility, but at the same time they may be compounding issues around security, visibility, governance and compliance. Cloud applications don't magically integrate with on-premise applications, and may not be easy to manage out of the gate. Rather, for a true hybrid environment, organizations will need to create an integration layer that acts as the conduit between IT services within the firewall, cloud-based applications that sit outside the firewall, and the processes that underpin fundamental business and operational requirements.

This integration layer is the first step in building a platform for the hybrid enterprise, by resolving conflicts between old and new formats, extending identity and authorization services to the cloud, and enabling a central governance model for data flow and service access. APIs are at the core of this integration layer, transforming existing IT infrastructure into easy-to-consume services and micro-services, and bridging the chasm between on-premise and cloud.

The hybrid enterprise, then, is about full-scale integration to the cloud, providing a seamless bridge to new services while leveraging and extending the utility of existing on-premise applications. The hybrid enterprise does not call for a new architecture; rather, it requires a new layer in your existing architecture, one that enables lightweight integration patterns using Web APIs and other Web standards, and helps your entire organization to navigate safely and securely in the cloud.

Creating a common API layer that includes the ability to traverse between the cloud, on-premise and mobile devices and applications is a necessary IT investment, since a common API layer contains elements that can be reused in subsequent projects. This capability for reuse creates the opportunity to reduce long-term costs, and helps organizations achieve a more compelling ROI story that will in turn build a case for future integration projects.

Is Your Enterprise Ready to Integrate to the World?

In many IT organizations, external service or partner integration is seen as resource intensive, hard to maintain and prone to failure. This perception exists because businesses have traditionally relied on network-based mechanisms for integration, such as dedicated links or VPNs, which are less flexible and not scalable across large numbers of B2B partners, service providers or applications. In addition, in the modern digitally connected world there is an increased need to directly expose functionality externally to customers via digital channels such as mobile apps.

The key need around integration now is the ability to provide digital services to, and consume them from, the outside world, and to do this in a way that protects internal IT systems while securing services and data-in-motion through configuration and policies. This approach allows rapid turnaround on enabling connectivity and access to services and data in a managed and secure fashion that is better able to support an evolving digital business.

To drive business growth there is also an increased incentive to leverage cloud-based IaaS platforms to support the intermittent scalability necessary for project development and testing, which in turn spurs the need for enabling managed external access to internal development and testing environments.

As discussed previously, the impact of this new approach generally goes deeper than simply enabling service use. You must also take into account the considerable impact related to the following questions:

1. If you are no longer in full control of the consumer or the provider, how will you manage the relationship, especially around SLAs or other contractual obligations?
2. Is your organization ready for the potential change in usage profiles? Are your internal systems able to handle usage-change profiles resulting from differing user demands, such as 24x7 operations?
3. How core are your internal IT Systems? Once external access is possible, does it make business sense to move non-core functionality out to a service provider?

The first two questions above can be successfully addressed through API-oriented integration and associated API management functionality (such as throttling, queuing and intelligent routing).

Question number 3, however, results from breaking down the silos of traditional IT services. Looking ahead, the reality is that isolation or protection of core IT services is not the answer; your enterprise should continuously consider how moving "core IT" infrastructure to managed service providers and cloud applications can improve productivity, enable organizational change and drive competitive advantage.

Integrating the Cloud Into the Business

The cloud application and service model has already changed the way business users view IT products and processes. Cloud providers generally shift the focus from systems and applications to a customer-centric service-based model, and this mindset is required within corporate IT as well. For many early adopters of cloud services, the relationship is often directly from the business to the cloud provider, requiring the business to take on more operational responsibility, and this drives a significant organizational change for large organizations: As the business engages directly with the cloud provider (instead of engaging via the internal IT group), challenges and successes are more visible and will thus more directly influence business stakeholders. Also, as the cloud provider is able to develop a better understanding of the business and its pain points, they are often able to identify opportunities for their organisation to upsell their offering based on deliverable business value.

By the very nature of the relationship, cloud providers become more and more able to engage and align around key business objectives within the organization, rather than simply remaining focused on tactical IT problem solving. This in turn puts pressure on internal IT departments to up their game and be able to function and deliver at the same level of agility and flexibility as in a cloud-based model. So, the key question is: What is the most effective way to enable enterprise applications and systems to achieve that goal? One option might be to adopt an ITIL service operational model and act like a cloud provider to a customer. Another option might be to adopt a more lightweight agile or DevOps model with technology teams directly embedded in the business. Regardless of the model adopted, a key driver is the reality that enterprise IT systems are no longer an island and must build their capacity to integrate with the outside world.

To support this goal, the organization needs to adapt its internal infrastructure topology to allow external access to services and functionality, both as a service provider and a service consumer. In addition to solving internal topology issues, businesses must also effectively and flexibly protect the organizational perimeter — both physical and logical — while ensuring strong security around service and data access.

This scenario is where API management solutions can drive significant value. API management technology supports multiple, standards-based integration patterns, and access control and authorization mechanisms based on a flexible, low-cost and policy-based configuration approach. API management can secure and protect internal IT infrastructure and data for external service consumption, ensuring that only the appropriate services and data can be externally accessed. At the same time, API management lets you manage access to external cloud-based services in terms of functionality, services and data.

API, Service and Data Governance

As with effective integration, effective governance must be lightweight and agile. API and data governance should include considerations around security policy, demand capacity planning and data protection, such as:

- Which production and pre-production services can and/or should be exposed to the wider community
- What kind of security policies should be applied
- Whether/how the service can actually meet expected demand

There is also a need to define and document API specification standards to provide for consumer authentication and integration — especially where partners or cloud services may be consuming sensitive data.

One key governance challenge is to ensure the necessary checks and balances without imposing the burden of a fully-fledged SOA governance model on your API layer. Most governance processes tend to be more focused on internal service consumption, and thus are fairly heavyweight and require significant investment at build and run time. API governance, on the other hand, implements a lightweight layer over existing SOA governance models and assumes these aspects have already been validated. Instead of trying to anticipate and define APIs to be set in stone, organizations should assume continuous change and govern to support it, while at the same time re-using existing API services wherever possible.

In summary, key issues for planning API governance are:

- Can the service be exposed?
- Who can access the service and what type of data can be exposed?
- Does the service meet the API service specification standards?
- Do the underlying provider-service SLAs and capacity meet projected API demand?

The overarching goal here is to create a level of governance that is responsive and lightweight, yet fully and easily auditable.

How API Management Simplifies Governance

As we've seen, Web APIs are an incredibly valuable trend for modern IT — they unlock data, increase agility, encourage innovation and reduce time-to-value. As such, the API integration layer is an essential part of modern IT architecture and is key to supporting the strategic vision and business goals of the hybrid enterprise.

The foundation of any robust enterprise API management solution is a fully featured API gateway. One of the main roles of the API gateway in the hybrid architecture described in this paper is to mediate incompatible protocols between cloud providers and the existing IT layer. Existing back-end services come in a variety of protocols — APIs using REST and JSON; web services using SOAP and XML; JMS; straight TCP sockets; a range of FTP-based B2B protocols; and many more. The API gateway you choose should offer a range of bi-directional transformation options, and not be limited to HTTP interfaces. For simple direct transformations such as XML-to-JSON and SOAP-to-REST, the API gateway should provide pre-configured operations; for complex transformations, it should provide configurable policies and pre-built connectors.

An API gateway provides comprehensive API security, including:

- Interface security to protect against attacks
- Access control to prevent unauthorized access
- Data security to prevent leakage of sensitive data

The API gateway should provide message-level firewall protection for APIs. By scanning headers, message content, and attachments, the API gateway can detect and block attacks. This protection is over and above what is provided by a network or even a web application firewall. The API gateway can also restrict use to specifically permitted methods, such as certain HTTP verbs. And the API gateway should be able to perform XML and JSON schema validation to prevent compatibility issues down the line, as well as schema poisoning attacks.

As APIs become an increasingly popular attack vector, unauthorized access is the biggest security and compliance risk for on-premise and cloud-based services. The API gateway is the policy enforcement point for API authentication and authorization. You should expect that your API gateway will support out-of-the-box integrations with leading identity and access management platforms (IAM) such as CA, IBM, Oracle, and RSA. An enterprise grade API gateway will also augment these IAM platforms in the areas of SAML and OAuth federation, fine-grained authorization, and device/application authentication. With these advanced capabilities, the API gateway makes it feasible to use an enterprise IAM platform to control access for both user/browser and API traffic.

APIs can transmit sensitive data such as credit card numbers, health-care records and other Personally Identifiable Information (PII). Thus, APIs are often subject to compliance mandates such as PCI DSS or HIPPA, privacy regulation and data residency. Effective API gateways can detect sensitive data not just in documents, but also in places where data may be embedded as identifiers and attributes, such as HTTP headers, query strings or resource names. Upon detection of sensitive data, an API gateway should be able to block, quarantine, remove, mask, encrypt or tokenize the message based on policies.

Of course, API management extends beyond the wide-ranging integration, transformation and policy enforcement requirements we expect of the API gateway. Organizations are establishing comprehensive API management frameworks to tap the power of today's rapid API adoption. Making it easy and convenient for developers (API consumers) to find, understand, and use enterprise APIs is a key component of a healthy and sustainable API-oriented, hybrid architecture.

An API portal is also a fundamental requirement to support product design, delivery and auditing for your API services. API-oriented architecture requires:

- Centralized management of the API lifecycle
- Governance around developer and cloud integrations
- Usage reporting across enterprise resources.

API lifecycle considers the end-to-end process of API management and models this as a variety of steps or gates that must be passed for an API service or micro-service to be promoted into production. There are typically a number of stakeholders involved in this lifecycle, including design, implementation, security and production operations. An effective API portal must enable and support each of these user responsibilities by offering clear visibility throughout the API delivery process, and bringing together all the enterprise API services into a centralized catalogue.

Whether it is cloud and hybrid integration, or any other integration project, developers are at the front line of service delivery. Your API portal will be expected to provide the tools, artifacts and support these developers need to integrate quickly and successfully. This means providing online and interactive API documentation, in-place testing to see example API calls, and libraries or examples that developers can quickly embed within their projects. Overall, self-service is the key requirement; developers — both internal and external — will expect to interact with your API services with the same ease of use they experience at Amazon or Google.

Enterprise-grade reporting, analytics and audit trails are also necessary requirements when selecting an API portal as part of your API management platform.

Visibility across the entire API management platform is paramount, including being able to leverage end-to-end business and operational intelligence across your organization. Finally, you should also consider how compliance regulations affect the data being transported via your APIs, and select an API management solution that offers detailed and comprehensive reporting.

The New IT Mandate

Change has been forced upon IT — its people, its processes and its technology. All organizations, regardless of scale, must think about how their existing IT services and underlying architecture can adapt to the rapid pace of cloud adoption, user demands and integration requirements. Web APIs provide the agility, and API management provides the scale, for organizations to realize greater utility across legacy infrastructure and to seamlessly bridge to a hybrid model by integrating cloud applications. The need is urgent, and the time is now, for businesses to transform their IT environments into API-centric hybrid platforms.

Another key opportunity offered by an effective API management strategy is the enablement of omni-channel interactions. If the same functional services are available across customers, staff, partners and other 3rd parties then omni-channel becomes a reality as an activity can be commenced in one digital channel and seamlessly continued in any other digital channel using the same set of services. Key to this is not just API enablement, but also ensuring the intent to ensure service functionality is constrained by enforceable security policies and business intent rather than technical and physical constraints.

However organizations should not just look at this as being forced upon them. It also offers significant opportunities for those organizations with some digital vision. Internal IT systems offer a wealth of useful data and functionality and APIs offer a chance to monetize this and provide this to the outside world in a managed fashion. So ensure you are connecting your organisation to the outside world, not just as a consumer of services but also as an effective provider of services to a much broader audience than your current customer base.

For more information, visit www.axway.com

Copyright © Axway 2015. All rights reserved.