SPEED AND SAFETY FOR THE HYBRID CLOUD

This white paper presents the benefits for operators and large enterprises of adopting a policy-driven approach to platform as a service (PaaS), which enables both speed and safety in a hybrid cloud world across diverse workloads and multiple global clouds.
INTRODUCTION

In today’s Networked Society, software is emerging as the primary way for global enterprises to engage with their customers. Software, cloud, mobile and connected devices are converging to disrupt industries and enable innovation. The ability to capitalize on these new opportunities as they arise is rapidly becoming a competitive differentiator for new business growth.

Speed in software innovation is critical in order for enterprises to remain competitive. This need for speed is accelerating the adoption of cloud amongst enterprises, providing the ability to deliver the greater immediacy that customers now demand, while also realizing the new economies of cloud.

Hybrid cloud – a combination of public cloud and private cloud – is being positioned as the way for enterprises to balance the desire to go ‘all in with cloud’ while managing complexity and risk and meeting the needs of a diverse mix of applications (workloads). Industry analysts are unanimous that we are entering an era where hybrid cloud will mature and become the dominant cloud strategy for large enterprises.

But as the move to hybrid cloud accelerates and the underlying technologies change, the shortcomings of traditional infrastructure as a service (IaaS) and platform as a service (PaaS) solutions are beginning to cause numerous problems for large global enterprises. These shortcomings are negatively affecting their ability to innovate at the speed needed to be competitive.

Multiple technology approaches, multiple vendors, multiple generations of software and infrastructure add to the complexity for a typical large enterprise. A recent survey revealed that 66 percent of enterprises are either “concerned” or “very concerned” about the need to manage and govern a hybrid cloud [1].

A new approach is required to deliver the benefits of hybrid cloud to enterprises – a new type of platform that provides a dynamic approach to solving the problem of enabling speed and safety, in the context of a complex enterprise environment.

- **Speed**: empowering the business to act faster – faster time to market; faster software development; faster access to global IT resources.
- **Safety**: ensuring IT governance and compliance; seamless, built-in, and policy-driven.
- **Freedom**: the ability to deploy diverse workloads, across multiple cloud infrastructures (while avoiding lock in), and to expand, grow and adapt the cloud to business needs.

This new type of platform should implement a policy-driven approach to deploying, orchestrating and governing diverse workloads across multiple cloud infrastructures, building on an enterprise-wide digital industrialization strategy to modernize, transform and automate IT for growth and competitive differentiation.
As the adoption of cloud accelerates, business executives are being forced to choose between speed and safety. They must decide whether to:

- leverage cloud to deliver software innovation at breakneck speed, but expose the company to higher levels of risk, or;
- mitigate risk and burden IT efforts with policy, which holds back development speed.

The need for the business, represented by the chief marketing officer (CMO) and developers, to deploy new software and applications quickly is continually growing. Empowered with readily available public cloud resources, the CMO is able to access and deploy cloud resources as and when needed. While some chief information officers (CIO) are able to provide a process for this, it is often aligned with the rise of “shadow IT,” inadvertently bypassing organizational IT requirements for control and governance, to enable the business to innovate and deliver new software services faster.

It is therefore not surprising to see a continual shift of organizational IT budgets toward the CMO and away from the CIO, with IT spending by the CMO predicted to account for 38 percent of total IT spending in 2015 to over 50 percent in 2017 [2].

While this helps achieve the goal of speed and innovation, how does the business ensure that these new applications deployed through shadow IT are being managed within the context of strong IT governance and policy?

A bimodal approach for IT has been proposed to help business move quickly for innovation while maintaining safety for core systems. The bimodal approach suggests splitting the enterprise IT organization into the following two IT organizations:

- One that focuses on ‘systems of innovation’ (applications that are built on an ad hoc basis to address new business requirements or opportunities) and ‘systems of differentiation’ (applications that enable unique company processes or industry-specific capabilities).
- Another that focuses on ‘systems of record’ (established packaged applications or legacy home-grown systems that support core transaction processing and manage the organization’s critical master data).

The challenge with this approach is in attempting to make the distinction between systems of record and systems of innovation ongoing. Accessibility of enterprise data in new and innovative ways is at the heart of the digital enterprise, blurring the lines between the risk profiles of different systems. And the traditional approach of locked-down IT security and multiple risk profiles for applications becomes difficult. The bimodal approach also brings the added complexity of running two different IT organizations with two different IT investment profiles.

The following diagram illustrates the dilemma:

**Figure 2: The organizational IT dilemma.**

---

**THE CHALLENGE: SPEED AND SAFETY**

---

A NEW ERA OF PAAS • THE CHALLENGE: SPEED AND SAFETY
The dilemma: speed and safety (governance) are being treated as trade-offs that can be accommodated with an appropriate risk assessment, or division of labor or multiple IT infrastructures. While a risk assessment is useful for identifying risks and ensuring mitigation strategies are in place, the assessment is limited in its ability to actually reduce the level of risk or cater for new levels of enterprise data accessibility.

The challenge confronting enterprises is how to create a modern and automated IT platform optimized for trust, delivering on faster IT development speed with a high level of IT governance.
SPEED, GOVERNANCE AND NEW IT ECONOMICS

Speed and safety are not opposites, like up and down, or light and heavy. Instead, speed and safety are currently trade-offs within the current era of cloud and IT.

To overcome this trade-off and unlock new IT economics, a new era of PaaS is required. A platform approach must be designed to take the best elements of PaaS for empowering developer speed, in combination with the best elements of dynamic enterprise policy control for IT operational governance. It must then be applied across multiple distributed cloud infrastructures to cater for the complexities and business needs of enterprise IT – including diverse workloads (modern and legacy), deployment preferences, and multiple private, public and industry specific cloud infrastructures – as well as ensuring global compliance.

This new approach would create an industrialized hybrid cloud, modern and automated, where all products driven by the business are possible on a common underlying infrastructure rather than having the infrastructure dictate what and how.

**THE BEST OF PaaS FOR HYBRID CLOUD**

**It’s about deployment**

Speed of deployment is fundamental, along with competitive options for cost, performance and availability. As mentioned earlier, IT spending by the CMO is predicted to account for 38 percent of total IT spending in 2015 and over 50 percent in 2017 [3]. This is primarily driven by the need to deliver new software services in a manner that the traditional IT organization is currently unable to do.

Imagine a scenario where the CMO or developers could instantly acquire the appropriate cloud resources (public or private) directly from the enterprise hybrid cloud, with IT governance baked in. This would eliminate any inadvertent sourcing of external ungoverned cloud. In essence, the enterprise hybrid cloud becomes the wanted solution, directly competing against shadow IT, catering to both the CMO and the developer as its target customers and fulfilling the needs of new applications.

In response, this new era of PaaS needs to be built on a platform that supports speed of deployment for developers across complex enterprise environments, where diverse workloads, workload portability and composable microservices are critical to success.

- Diverse workloads: enterprises need to provide developers with the ability to deploy diverse workloads in a standard and fast way across the hybrid cloud. This includes new applications written in multiple languages as well as composable legacy applications, and containers such as Docker.
Workload portability: once an application is deployed in a hybrid cloud, the workload needs to be portable (within the constraints of the policy set for it). This includes the ability to move the application across infrastructures/clouds, scale the application, and restart the application – without the need for application-specific code.

Composable microservices: it should be possible to turn workloads into scalable and modular ‘services’ to support scale-out architectures and the new world of open application programming interfaces (APIs).

**It’s about orchestration**

In addition to deploying workloads, orchestrating workloads throughout the life cycle is just as important to aspects of speed, automation and achieving the new economies of IT.

A new era of PaaS should be built on a platform that puts the workload at the center. The purpose of the underlying cloud infrastructure – which could be a virtual machine, a run-time environment, a container or a service, on one or multiple clouds – is to service the needs of the workload. By understanding the workload requirements, the platform is able to use the hybrid cloud infrastructure to become much more efficient, powerful and secure. IDC predicts that more than 50 percent of enterprises building hybrid clouds will acquire ‘workload-aware’ cloud management products by 2016 [4].

Orchestration is about workload management, and all the things needed to ensure ongoing uptime and efficiency. These factors include:

- Life cycle management: orchestrating workload updates and versions is important to ensure agility for software development and faster time to market for the business. Deployment is one aspect, ongoing software management is another.
- Service bindings: workloads do not live in a vacuum, nor do they live in a trusted world by default. With this in mind, an approach is needed to both connect and secure workloads to optimize for trust. Workloads should be secured and locked down by default, with the ability to orchestrate service bindings between workloads and other external services. An example of a service could be connectivity to the internet or a database, where a workload is bound to the service, with specific environment variables for additional layers of automation and trust.
- Resource management: workloads run on compute, storage and network infrastructure resources. The ability to orchestrate the allocation of these cloud resources to workloads, and optimize them within and across clouds, is important. This should include the ability for scaling up and down, high availability and migrating workloads.
- Semantic awareness: to speed up deployment and maximize automation and efficiency, the platform should be able to understand certain characteristics of the workload and act accordingly. Orchestration should include built-in semantic awareness: the ability to assign certain characteristics to a workload based on the underlying runtime or staged environment adds huge value.

**POLICY IS ESSENTIAL TO PaaS FOR HYBRID CLOUD**

**It’s about governance**

There is no doubt that governance across deployment and orchestration is the key to success. A hybrid cloud should not have to choose between speed and safety – it needs to solve both problems. Governance is the ability to apply policy to enforce consistency from which safety can be derived and maintained. Without policies, efficient automation is not possible.

Unfortunately, governance today is implemented as a patchwork of bolt-on policies and custom-written tools, which do not scale and bring speed of deployment to a grinding halt.

A new era of PaaS demands a policy-driven approach where policy is foundational, built into the platform and pervasive to every aspect of the way a workload is deployed, orchestrated and governed. Policy should not be a static manual effort that increases work effort. It should support rapid deployment, be dynamic, scripted and at the core of every action.

In this context, policy is more than simply having role-based access control mechanisms in place or traditional perimeter security models. A policy-driven PaaS for hybrid cloud needs to provide the ability to govern all aspects of distributed workloads, including both security aspects and effective use of the IT resources. Policy should include:

- Access controls: for example, what users can and cannot do.
- Credentials: for example, server-server authentication, including ephemeral enhancements.
- Efficiencies: for example, how to best allocate hybrid cloud and IT resources to workloads.

A NEW ERA OF PAAS  •  SPEED, GOVERNANCE AND NEW IT ECONOMICS 6
Performance: for example, how to ensure workloads get the right IT resources.
Resilience: for example, availability of workloads across hybrid cloud resources.
Life cycle: for example, management of workload deployments.
Compliance: for example, workload affinity, workload connectivity, data integrity.

The platform should provide the ability for operations to configure policy based on workload, resource, cloud, region, namespaces and user/group, allowing developers to get on with the job of deploying and orchestrating applications fully managed and bound by the policy that governs all aspects of the hybrid cloud. Behavior outside the policy is simply denied or automatically adjusted.

For example, a policy could exist for lowest cost cloud infrastructure. Workloads deployed with this tag would be deployed onto the lowest cost cloud infrastructure within the hybrid cloud. Likewise, a policy could exist for high performance or geo-compliance, and workloads tagged with these policies would be deployed accordingly. This creates a whole new opportunity for hybrid cloud governance across cost, performance and security.

The key to the success of this is the ability to programmatically define policy dimensions and attributes, alongside a mechanism to apply and enforce at scale across complex hybrid cloud architectures.

In terms of solving the trade-off between speed and safety (risk), speed is enabled through the outcome of dynamic flexible applied policy to all workload events, while safety (risk) is addressed through the enforcement and governance of the policy.

At a high level, three aspects of policy should be addressed by the platform:

- Policy and audit dimensions: the ability to set policy based on multiple dimensions such as users, namespaces, workloads, clouds, resources, services and more, is critical to ensuring flexibility, automation and compliance. The ability to use a dynamic policy scripting language would enable an enterprise to programmatically define and execute custom policy dimensions that suit the compliance and economic needs of the enterprise.

- Workload isolation: each workload should be isolated by default, with policy defining all possible interactions between workloads, should these interactions be invoked. Workload isolation is important to ensure factors such as performance and security compliance, and is particularly critical in multi-tenant environments, which demand isolation.

- Fine-grained user and application privileges: enterprise environments are complex. They include many applications, many development groups, many infrastructure resources, and possibly even many organization structures and countries. The ability to set fine-grained policy to govern such a large scale enterprise hybrid cloud is critical.
A simple example to illustrate the concept of this new era of PaaS for hybrid cloud, achieving both speed and safety, might look something like the following.

A typical enterprise needs to be able to deploy multiple types of workloads developed by multiple teams of developers, governing compliance and resource allocation according to IT policy.

In this example, operations would be able to implement an overarching policy to govern:

- developer access to specific cloud infrastructure resources, based on user, workload or namespace
- developer ability to deploy and orchestrate different workloads
- deployment of development and staging workloads to lowest cost cloud infrastructure
- deployment of production workloads to resilient, high-performance cloud infrastructure.

Developers would be able to use standard command line interface (CLI) tools to seamlessly deploy workloads, create new services, orchestrate service bindings and manage resources in real time, within the confines of the policy. The policy set by operations governs all developer capability to ensure IT policy is enforced across every event.

Other example policies:

- Development sandbox environments deployed to the lowest cost cloud infrastructure.
- Production workloads deployed across multiple resources for resilience and scale.
- Geo-sensitive workloads deployed to geo-specific cloud infrastructure to meet global compliance requirements.
- A ‘no delete’ rule to ensure data records from databases cannot be deleted by any workload (including database admin connectivity) to comply with data retention requirements.
- Service bindings between workloads and database services to abstract database access credentials.
- Namespaces created per workload, or per business unit, to enforce developer access and privileges.

Figure 4: Policy examples.
THE BENEFITS

Having the right platform for hybrid cloud is an important step for enterprises in modernizing and automating software. The key benefits attained in solving the core conflict between speed and safety are very much aligned to the needs of large enterprises, in particular the need to drive agility and efficiency.

Increasing agility can be realized through faster application deployment, faster development, simplified life cycle management and simplified hybrid cloud resource management. The benefits include:

- more time spent on software development versus software deployment
- faster software deployment and go to market
- increased levels of innovation and growth opportunities
- increased ability of operations to respond to unexpected infrastructure resource requirements to meet business needs
- aligned DevOps ways of working across the business
- rich APIs and higher levels of programmability add further levels of agility and flexibility.

Efficiencies and cost savings can be realized through reduced opex, and capex, as the deployment and life cycle management of business-critical applications is made more efficient, and the alignment of applications (workloads) to specific cloud infrastructures is realized. The benefits include:

- all clouds (public and private) become possible infrastructure resources – true cloud brokering
- leverage based on performance, jurisdiction, cost, network, location, or scale
- increased levels of automation within operations
- lower cost to trial new services – lower cost to fail
- next-generation architecture for all workloads, including industry workloads such as network functions and the Internet of Things.

Governance and compliance can be realized through the ability to define and audit policy across all workloads and cloud infrastructures – leveraging the same capability used to increase agility and efficiencies to reduce the actual risk to the business. The benefits include:

- compliance across global cloud infrastructures
- governance of workloads, users, resources and clouds according to business policy
- logging and auditing of all events and state changes.

Figure 5: Hybrid cloud benefits.
Every enterprise is now in the software business. The opportunity for unprecedented levels of industry disruption and growth, spurred on by the Networked Society, is creating the need for enterprises to move faster.

Modernizing and automating IT infrastructure is the key to moving faster and creating a strategic competitive differentiator for enterprises. As a result, hybrid cloud adoption is accelerating, and is being positioned as the way for enterprises to further embrace the cloud by managing the need for speed while mitigating risk across differing workload needs.

However, today’s approach to cloud still falls short, requiring a trade-off between speed and safety. This is impacting the ability of large enterprises to fully embrace the cloud for business-critical workloads.

A new era of PaaS is required to eliminate this trade-off and combine the best aspects of PaaS for deployment and orchestration with a new policy-driven approach to ensure IT governance and control.

Policy in this context is more than just access control. Policy is applied to all workload events across the hybrid cloud to maximize agility, scale, efficiencies performance and enterprise compliance.

Hybrid cloud should be about getting access to the most appropriate private and public cloud infrastructures, accelerating innovation and time to market. In short, developers and marketing get what they want, and operations get what they need. Getting this right is critical to unlocking the new economies of cloud and creating true strategic competitive differentiation through software innovation.
REFERENCES


GLOSSARY

API  application program interface
CIO  chief information officer
CLI  command line interface
CMO  chief marketing officer
IaaS infrastructure as a service
PaaS platform as a service

© 2015 Ericsson AB – All rights reserved