Unified Digital Application Management Platform:

A key component in Digital Transformation

Author: Jothi Rengarajan, Principle Architect

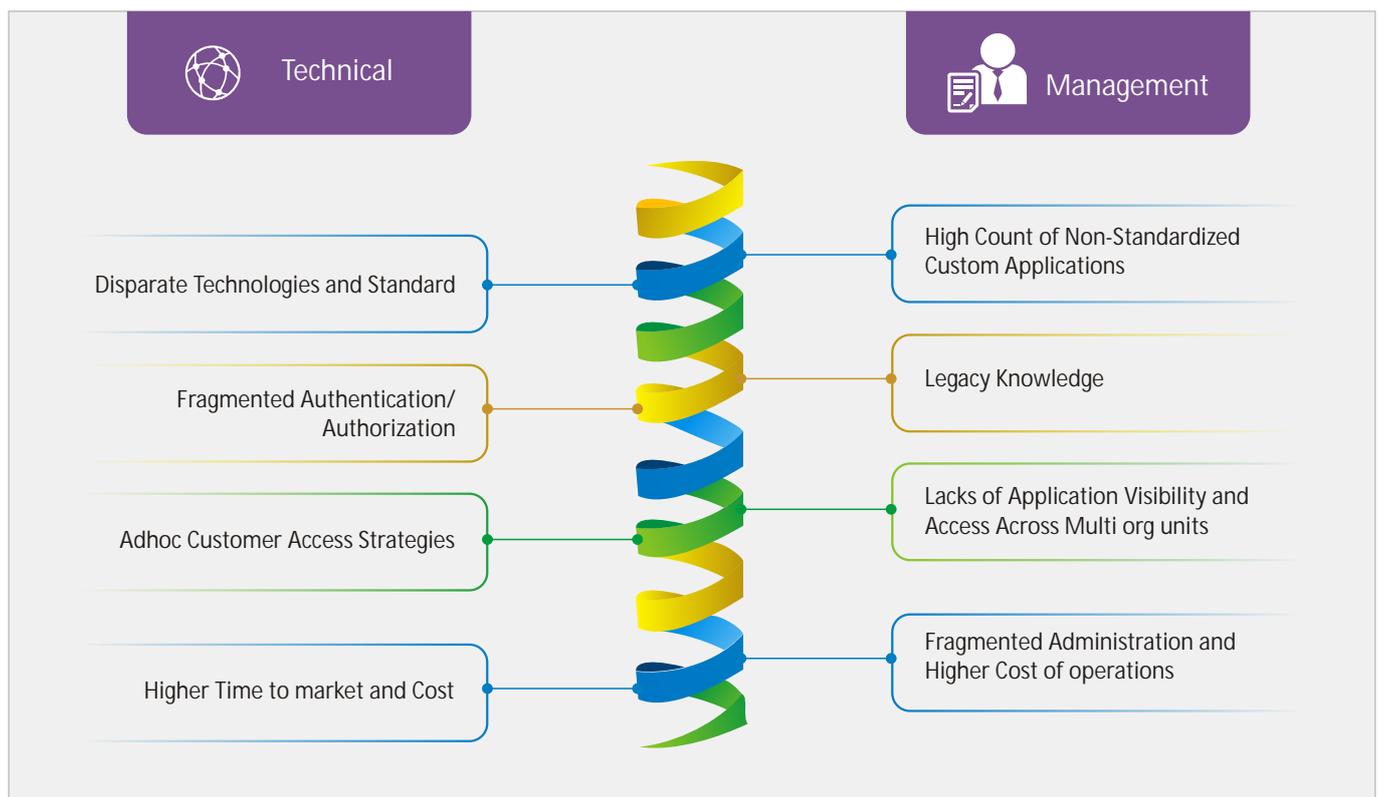Development Practice Head: Aju Mathew, aju.mathew@aspiresys.com

C O N T E N T S

Unified Digital Application Management Platform:
A key component in Digital Transformation

There is no further need to stress the way that enterprises need to experience a digital change to remain significant to their business. Many are in the process of this journey and many have already moved pretty much ahead. In the rush of doing so enterprises have failed to anticipate the gush of heterogeneous and disparate technologies in their IT. These applications have grown without appropriate models and hidden standards prompting the bad dream of IT operations and maintenance. . It is even more a bigger challenge for bigger organizations with multiple branches and geographies as there is no single point of control.

Challenges with Lack of Standardization

A model like this effectively prompts the blast of general cost of operations and support.. The other measurement of hazard to this is client disappointment.. If an enterprise exposes multiple applications to a customer and if they all have different standards and approaches the customer is going to struggle with the overall experience. Factors such as user sign on experience, branding, notification models are going to vary from application to application and are not uniform. This does not represent a single face of the enterprise to the customers. These issues are going to be multi-fold when the enterprises have disparate and fragmented custom developed applications as opposed to COTS. Following diagram represents the key challenges of a non-standardized approach for building/managing applications.

Technical		Management
Disparate Technologies and Standard		High Count of Non-Standardized Custom Applications
Fragmented Authentication/ Authorization		Legacy Knowledge
Adhoc Customer Access Strategies		Lacks of Application Visibility and Access Across Multi org units
Higher Time to market and Cost		Fragmented Administration and Higher Cost of operations

When should you definitely consider an unified platform

- Your organization has multiple branches and there is no visibility of applications and micro-services between each branch.

- You have the need or have built more than 5 customer facing applications and they all have their own administrations and access controls.

⮞ Your customers use more than one of your custom applications

⮞ You are thinking of taking your knowledge base as a subscription based software

⮞ You are thinking of building a trusted component so that it would be cost effective , pre - tested and ready to go.

Platform Centric Standardization

As we need the right foundation on top of which you build a multi storied building, an enterprise needs a strong platform on top of which you can build and deliver applications and solutions. People often mistake that the only platform that is required is a hosting platform or an application life cycle management platform leaving out the application platform. At an application level there needs to be a strategy to deliver quality of services uniformly and enable reuse across the organization. In order to achieve this there needs to be a single application platform for the entire organization which is used to build, provision, manage and govern applications.


Development Accelerator

The need for enterprises to build custom applications is increasing today. Below are the top reasons why enterprises build custom applications:

⮞ Unique requirement

⮞ Better control on customer experience

⮞ Integrate and consolidate multiple data sources

⮞ Application is the backbone of the enterprise offering/service

⮞ Application is opened to customer, partners and suppliers
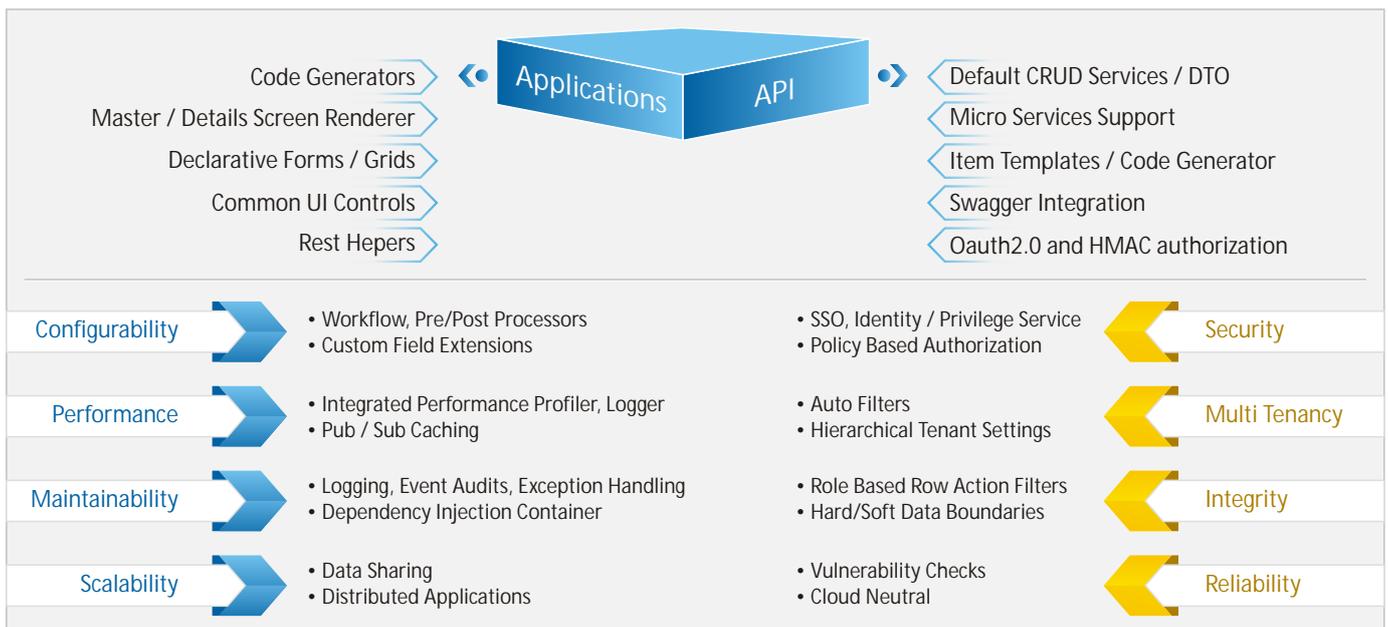
As you could see, the accelerator needs to address both architecture level and productivity components that are critical for the maintenance of the application. It is also very critical to ensure that the accelerator can be modified to the trends of architecture tomorrow and you have that control to do so. Some enterprises go in the path of visual development tool as accelerators. Before they do that, they need to examine the pitfalls it has such as rigidness and loss of control. An accelerator should be focussed on developers. It should enable developers to think and develop faster by taking away the mundane tasks they do. One another important attribute that the applications should be designed for is to enable the administrators to perform small variations driven by business change by just configurations without coming back to the development team. For example, being able to add another additional field to a form, changing the display name of a field etc..

Access Control

Employee access control vs Application identity and access control

It is very important for an organization to have a centralized identity and access control mechanism for all their applications. If not it is a pain for administrators to secure, manage and control access of applications in umpteen different places. Enterprises sometimes mix up application identities with employee identity management solutions such as active directory. Employee identity management solutions are best to provide access to internal hardware resources such as machines, servers, software policy within that machine etc. Application access is different and abstracted from internal employee attributes. It is fine if the applications are internal and are employee centric. When the enterprises deal with customer facing applications or applications dealing with multiple parties, they have to isolate the customer based identity and access management solution from their employee identity management.

Let's take a look at the various factors that brings in the demarcation within the access control requirement of an internal application vs customer facing application
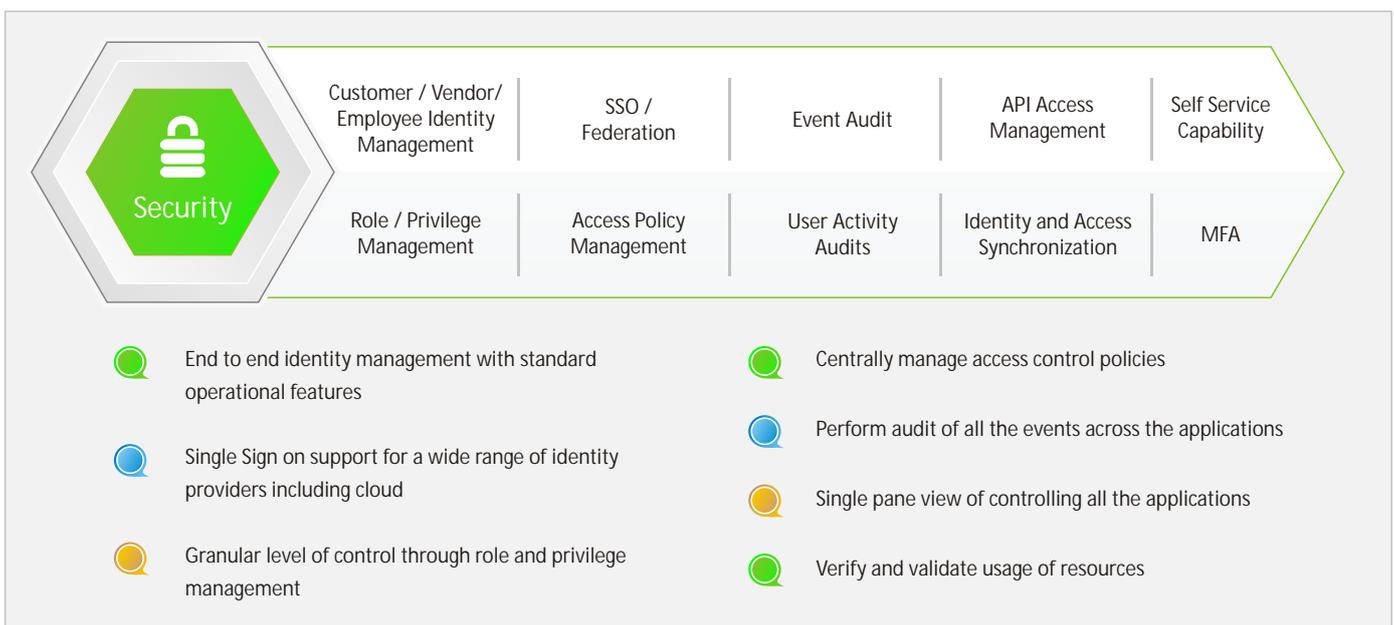
Parameters	Customer Facing Applications (CFA)	Internal Enterprise Applications (IEA)
Authentication	• Identity of the customers and consumers need to be different from the internal employee identity as the provisioning process, lifetime and de-provisioning for the customer/consumer user is very different from employee provisioning	• Employee identity management is typically used for application identity management as well

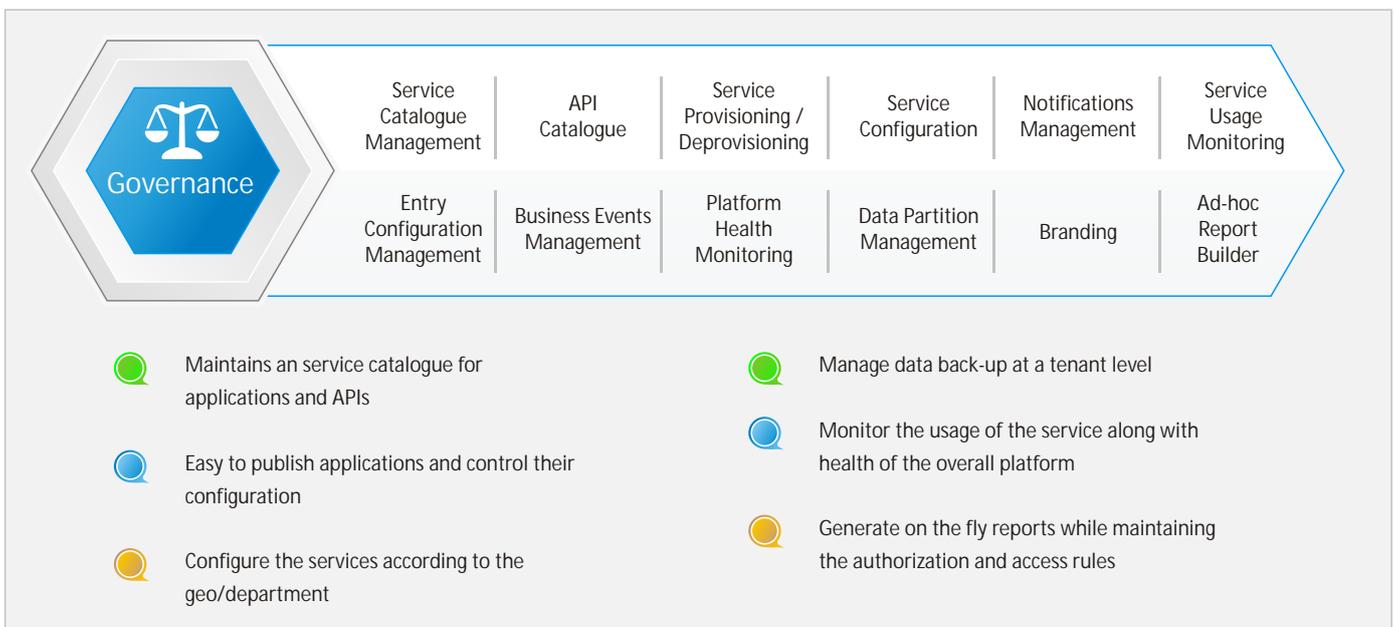|		
	• Customers prefer to have a single sign-on (SSO) with their existing identity systems or through an established social networking application • Self-service is important where customers get control of features like password reset • Multi-factor authentication becomes important • Brand management for the authentication experience is important	• Self-service for identity management of the employee may not be required
Access Management	• Comprehensive access framework will be required to ensure data boundaries are maintained properly and users see only the data that they are supposed to see especially when the customers are B2B customers. • Access policies should be defined by the business application, business rules and business attributes. Policies cannot be defined by internal organization directory groups. • Customer facing applications require a configurable access policy which could vary from one customer to another customer. • The entire access management should have to be managed seamlessly without involving an external IT person and be end user-friendly to configure. • IP zone based restriction is important. • The entire access management should have to be managed seamlessly without involving an external IT person and be end user-friendly to configure.	

Enterprise Access Control Components

To provide a complete access control solution the platform should support the following components:

Security	Customer / Vendor/ Employee Identity Management	SSO / Federation	Event Audit	API Access Management	Self Service Capability
	Role / Privilege Management	Access Policy Management	User Activity Audits	Identity and Access Synchronization	MFA

- End to end identity management with standard operational features
- Single Sign on support for a wide range of identity providers including cloud
- Granular level of control through role and privilege management

- Centrally manage access control policies
- Perform audit of all the events across the applications
- Single pane view of controlling all the applications
- Verify and validate usage of resources

Governance

The platform should provide necessary flexibility and control to the administrators to configure small variations happening in the business needs. A simple example could be that an administrator should be able to control and change the templates for notification that are sent from the applications without having to go back to the development team. Another need is that the administrators go and control and tweak the workflows in the systems. Platform should also have the capability to provide a single panel view of the KPIs and application health of the system. While hardware monitoring can provide reports at a hardware level, application monitoring provides details at an application level. A single pane view of all the user activities and business events happening in the system along with the next level information of the details of users and action involved in the action is necessary for the admins to perform the real status check of the applications. Platform should also provide necessary reports and dashboards to the management to view the business KPIs of the applications in the system without having to go to multiple places. The platform should also provide visibility for and reuse of application cross geographies and branches. Following are the key components of the platform to enable Governance.

Service Catalogue Management	API Catalogue	Service Provisioning / Deprovisioning	Service Configuration	Notifications Management	Service Usage Monitoring
Entry Configuration Management	Business Events Management	Platform Health Monitoring	Data Partition Management	Branding	Ad-hoc Report Builder

- Maintains an service catalogue for applications and APIs
- Easy to publish applications and control their configuration
- Configure the services according to the geo/department
- Manage data back-up at a tenant level
- Monitor the usage of the service along with health of the overall platform
- Generate on the fly reports while maintaining the authorization and access rules
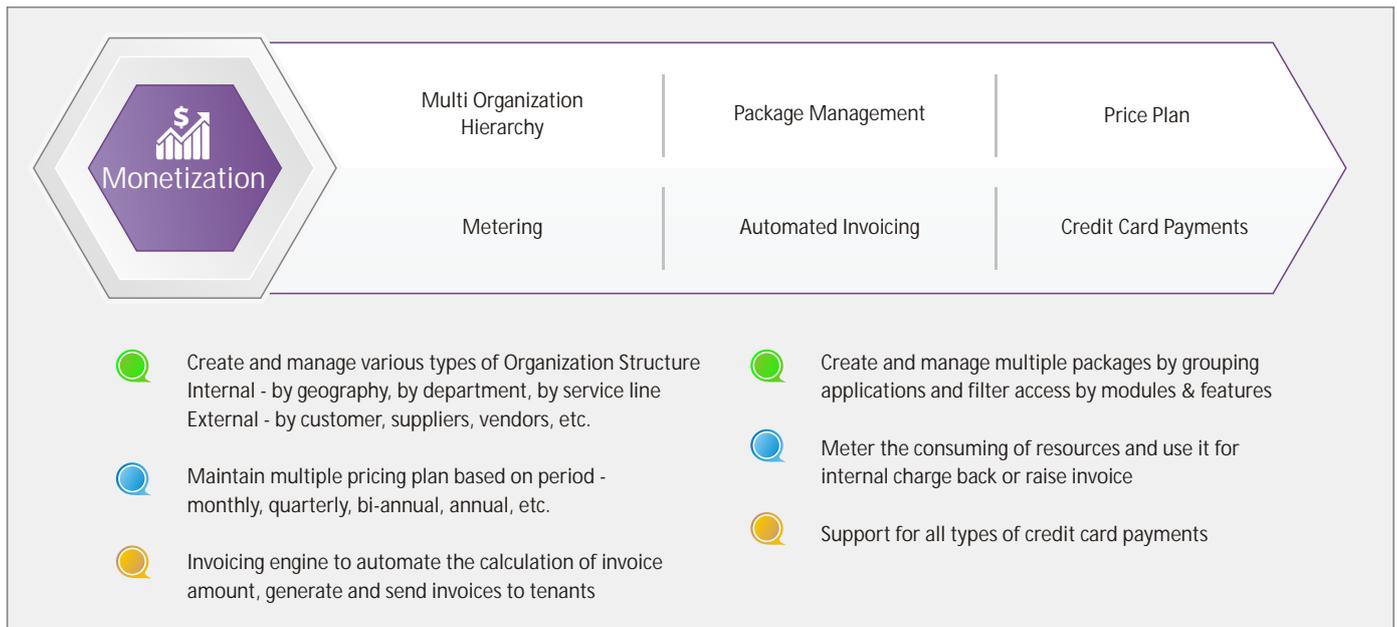
Monetization

It is surprising to see how many enterprises are moving to the next level by monetizing their applications. Following are the use cases where enterprises adopt this model

➡ One solid use case we are seeing is the place the Enterprises are taking their insight and information and converting that as a product and selling it to other enterprises. The product could be a value-add to their existing service or could be a completely independent steamline as well. In this case they almost act like an ISV. Many enterprises IT is taking this route. Keeping this in mind, to accomplish it a strong subscription system is required..

➡ Internal chargebacks: IT departments of the enterprises have dependably been in the back burner if it must be seen as profitable, it needs to have a cost.. Utilization based chargeback is the most ideal approach to construct a cost to-esteem relationship for IT Servoces, and it is one of the cornerstones for running IT as a business within a business. As long as IT has a solid understanding of its costs, it can use pricing as a strategic tool for improving alignment with the business by giving executives better

understanding and control over applications. Diverse models, with various classes of service, can be utilized to drive more cost-proficient utilization of IT and to accomplish more powerful matching of service to business need.

In order to achieve the above uses cases a strong subscription system is required. Following exhibit describes the components required for such a subscription model

Monetization	Multi Organization Hierarchy	Package Management	Price Plan
	Metering	Automated Invoicing	Credit Card Payments

- Create and manage various types of Organization Structure Internal - by geography, by department, by service line External - by customer, suppliers, vendors, etc.

- Maintain multiple pricing plan based on period - monthly, quarterly, bi-annual, annual, etc.

- Invoicing engine to automate the calculation of invoice amount, generate and send invoices to tenants

- Create and manage multiple packages by grouping applications and filter access by modules & features

- Meter the consuming of resources and use it for internal charge back or raise invoice

- Support for all types of credit card payments

Conclusion

Enterprises in the digital age need a unified platform that can manage digital applications with a standardized approach to architecture, administration, monetization, governance and security. This can be achieved with a development accelerator that provides a robust foundation to build such highly scalable and customizable digital services. The accelerator would have to be technology agnostic and should be able to leverage cloud for unlimited scalability. In this way, enterprises can gain enhanced visibility and control of multiple customer-facing and enterprise applications.