# The evolution of PaaS

When Platform-as-a-Service first came on the scene, it took a while before people began to understand its benefits. That makes sense; not only is it cloud-based, but PaaS is a different way of managing platforms. It includes several components, including application development tools, database management systems and integration of middleware. All of this results in automated, simplified application lifecycle management in ways that can meet service level requirements and user needs.

PaaS continues to mature, further separating itself from Infrastructure-as-a-Service (IAAS). In fact, many now confuse the two, but there are significant differences. While IaaS addresses the hardware and software powering the infrastructure, PaaS provides the tools and services that make developing and deploying the applications more efficient.

Slowly but steadily, organizations are relying more on the PaaS model, generally to improve operations and application uptime. As PaaS offerings have matured — they now provide the ability to incorporate new services and provide more control over scale — organizations are learning to expect more from PaaS. According to a 2013 study by Engine Yard, organizations today are more focused on strategic benefits, such as faster delivery of applications, supplementing an IT team's experience and leaving more time for application innovation.

The study also found that mobile applications are particularly well-suited to run on PaaS, as are social applications. Both are increasingly important to government agencies. Government agencies at all levels are embracing worker mobility, and as a result, have implemented mobile device management (MDM) infrastructure for security and manageability. Many have found that the best way to do that is by using a private PaaS set-up, which provides an environment for developing and managing the devices themselves, along with a common set of web services accessible by any approved mobile device and full application lifecycle management.

## THE FLAVORS OF PAAS

Choosing to make PaaS part of your environment is only the first of several decisions you must make. In addition to choosing the right vendor, it's important to understand the differences between public, private and hybrid PaaS. In many ways, they are similar to the descriptions of public, private and hybrid cloud in general, but there are differences. Here are the pros and cons of each approach.

### Public PaaS

**PROS**

- **Infrastructure is not managed on site. This is especially useful for organizations that don't have the IT resources or that want to spend more time on mission-related activities.**
- **Organizations can share hardware and software among many users or divisions, and can be set up so different divisions or user groups pay for only what they use.**
- **It is a cost-effective option.**

CONS

- An organization's application and data often reside on resources shared by other enterprises, possibly raising security concerns, especially for agencies responsible for financial, intelligence or security data. According to a recent IDC survey, security has been the top concern about public cloud for the past three years.
- Compliance regulations sometimes require that data be kept inside an organization's firewall.

### Private PaaS

**PROS**

- **Allows organizations to run legacy and mission-critical applications that can't be entrusted to others.**
- **Provides the highest level of control, security and oversight.**
- **Allows full control over development operations and deployment tools.**

CONS

- Organizations are responsible for installing and maintaining physical servers as well as the application stack.
- Often more expensive than other forms of PaaS.

### Hybrid PaaS: A combination of private and public cloud resources

**PROS**

- **Organizations can pick and choose whether private or public PaaS is best for specific applications, managing cost issues effectively and ensuring that security-sensitive applications remain on private PaaS.**
- **Mitigates cost and security concerns.**
- **Because a workload can switch back and forth between public and private PaaS, it's best for dealing with scalability spikes. For example, a tax agency probably has spikes throughout the year, and a defense-based agency may have spikes related to world events.**

CONS

- There is some learning curve in managing workloads between two types of environments.

# PaaS in government

The federal government is crystal clear in its expectations for the cloud. In addition to the "Cloud First" mandate, which requires agencies to consider the cloud when possible, the federal government's PortfolioStat program and the Federal Data Center Consolidation Initiative (FDCCI) have spurred agencies to turn to the cloud. And it's working: A recent IDC Government Insights report found that federal agencies expect to move toward cloud services in increasing numbers over the next few years.

And it's not just federal agencies making the move. According to the National Association of State Chief Information Officers (NASCIO), adoption of cloud services is a top state CIO priority for 2014, just under security and consolidation/optimization.

While Software-as-a-Service (SaaS) continues to be the leading type of cloud deployment governmentwide, both Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) are expected to grow significantly through fiscal 2017, according to IDC.

Virtually every agency is either deploying PaaS or considering it. The FCC, for example, expects to migrate some of its legacy systems to PaaS to improve data sharing. NASA's Jet Propulsion Laboratory uses PaaS to handle development efforts that require fast scaling of hardware and software. The USDA's National Finance Center provides cloud services, including PaaS, for 170 agencies.

Other agencies with big plans for PaaS include the Army, Department of Interior and the Defense Information Systems Agency. On the state and local side, states from Texas and Colorado to Idaho and Hawaii are on the road to PaaS.

## PAAS BY THE NUMBERS

- **While SaaS is currently the most widely used form of cloud computing, with IaaS second, PaaS will grow the fastest over the next five years, to 72% of organizations.**
- **Across government, the market for PaaS will grow to $1.1 BILLION by 2017.**
- **30% of organizations have already implemented a PaaS solution, and 13% more plan to do so within the next year.**
- **Federal private cloud spending will rise to more than $1.7 BILLION in FY2014.**
- **68% of state governments already have some applications in the cloud, and more are considering it.**

## EXPERTS PREDICT: PAAS CONTINUES TO GROW AND CHANGE

Platform-as-a-Service continues to mature and grow as vendors add capabilities like better integration to existing applications and support for development in more languages. At the same time, users are becoming more comfortable with the PaaS concept and are branching out in how they use it. Here are three advances that experts predict will take off in the next few years:

- **PaaS capabilities will expand.** PaaS vendors will add more integration, third-party services, database clusters and runtimes, with the result being a complete custom stack for customers. PaaS offerings also will start incorporating configuration management and orchestration tools.
- **IaaS and PaaS will merge.** To some extent, PaaS and Infrastructure-as-a-Service (pay-as-you-go computing infrastructure) have similarities. In the future, IaaS vendors are likely to add PaaS-like capabilities. In other cases, IaaS and PaaS vendors could merge their operations. This will make it easier for organizations buying IaaS and PaaS services.
- **More will use PaaS to manage mobile environments.** PaaS and mobility are a good match: It's an effective way for IT organizations to manage mobile applications and an organization-wide BYOD framework. It's also a good way to develop, test and deploy mobile-enabled applications.

**PAAS AND MOBILITY ARE A GOOD MATCH: IT'S AN EFFECTIVE WAY FOR IT ORGANIZATIONS TO MANAGE MOBILE APPLICATIONS AND AN ORGANIZATION-WIDE BYOD FRAMEWORK.**

# A New Approach to PaaS for Government

Platform-as-a-Service (PaaS) offers big benefits for agencies that have taken advantage of it so far, especially the ability for application developers to access resources on demand, on a predefined, standardized platform. PaaS also provides the type of agility, scalability and flexibility that agencies' application developers need.

But for the many agencies and departments that have security concerns about PaaS in a public cloud environment, the choices have been few and far between. While there have been a few private PaaS options for government, they have typically required agencies to invest in their own infrastructure, from servers to middleware and databases. In a world where capital expenditures are under increased scrutiny, that's a tough sell. What agencies really need is a secure rapid application development, testing and hosting environment built entirely in the cloud.

DLT Solutions (DLT), a leading IT solutions provider for the public sector, decided that the time was right to address all of these issues for its government customers. DLT partnered with Red Hat, leveraging its OpenShift Enterprise PaaS offering, along with Amazon Web Services, to create a rapid private PaaS offering that would enable agencies to reap the benefits of PaaS without worrying about security or physical infrastructure.

## PRIVATE PAAS FOR GOVERNMENT

The resulting product, DLT's elastic private platform-as-a-service solution, makes OpenShift Enterprise, Red Hat's successful PaaS offering that provides development resources on demand, available on the Amazon Web Services (AWS) platform. This allows agencies to build their own OpenShift PaaS on AWS' fully- configured, scalable, secure infrastructure.

"In essence, this approach creates a walled garden within Amazon that only the agency and their agents can access," explains David Blankenhorn, DLT's Chief Cloud Technologist. "The agency holds all of the keys."

OpenShift Enterprise provides developers with the programming languages and tools they are most familiar with in a format that provides auto-scaling and extreme density. And because all of the infrastructure is provided by AWS, agencies don't have to worry about providing their own hardware, databases, middleware and other infrastructure.

Scalability is particularly important in environments where demand can change quickly. For example, an unexpected troop deployment can require quick access to resources, as can legislative changes and any number of other unexpected events. With DLT's elastic private PaaS solution, developers can quickly access the resources they need during demand peaks and remove those resources when the demand decreases.

With DLT's elastic private PaaS solution, agencies can now start to gain the benefits that PaaS can offer without worry — rapid deployment, capacity on demand, fast speed and agility, and extremely rapid scalability. •

## SECURITY AND PAAS: A WINNING COMBINATION

When it comes to government data, security is top priority. All of the components of DLT's elastic private PaaS solution were developed with this in mind.

Red Hat's OpenShift Enterprise PaaS platform is hardened with technologies like Security Enhanced Linux (SELinux), a Linux kernel security module that supports U.S. Defense Department-style mandatory access controls (MAC). The technology also employs a stateful and stateless inspection firewall, full intrusion detection and port monitoring, remote logging and encrypted communications.

In addition, Red Hat's technology has been certified for the Common Criteria for Information Technology Security Evaluation, an international security standard used by the U.S. government that evaluates a system's entire security profile. Red Hat Linux, on which OpenShift is based, has been certified at an Evaluation Assurance Level (EAL) of 4, which is a high level of assurance.

The Amazon Web Services (AWS) cloud infrastructure also meets stringent government security requirements, including PCI DSS Level 1, ISO 27001 (for information security management), the Defense Department's Information Assurance Certification and Accreditation Process (DIACAP), HIPAA, FISMA and FIPS 140-2.

AWS also is fully compliant with FedRAMP, a U.S. government-wide program that fosters a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.