The Promise of Multi-Cloud

Visibility and inventory are keys to getting maximum benefit.

Following years of hearing how cloud computing will improve operations, many organizations have begun realizing those promises, yet there is more to gain – greater efficiency, agility and cost savings – especially in the multi-cloud world. Unfortunately, there is no reliable roadmap for getting there.

Simply understanding where digital assets are at any given moment – on premises, in a specific cloud platform, or in some combination – has become increasingly complicated. Lacking full visibility and understanding of the digital environment, agencies are at risk of overpaying for software licenses, degraded system performance and compromised security. Often, the solution is comprehensive and rigorous IT asset management.

"It all comes down to visibility, context and action," said Josh Fraser, vice president of cloud solutions at Flexera, a company that provides integrated solutions to improve insight, spend optimization and agility. "In other words, it's about knowing what you have, how you are using your resources for each specific use case, and then using that information to optimize those resources."

Achieving true optimization requires conquering a host of challenges:

Visibility

A server's power and performance profiles can vary across cloud providers, as does the API call used to access the server and extract information. In such an environment, tracking infrastructure resources and data is difficult.

Ensuring software licensing compliance

Software publishers have created software entitlements for use in the cloud and on premises. This flexibility, while useful, can hinder software licensing compliance. Moreover, some cloud providers offer the option of provisioning resources that include specific software, such as Windows Server, which raises the question of whether to use the cloud provider's instance or your own entitlement?

Security

In the multi-cloud world, the most common model today is one of "shared security," which requires agencies and cloud providers to share responsibility for security. The responsibility model varies by workload and the people who provision and access resources. An agency provisioning a server in the cloud, for example, chooses the way it is set up, who has access to it, and what will reside on it. In making those decisions, the agency must satisfy federal security requirements.

Conquering challenges

These are daunting challenges, yet they can be overcome. It starts with standardizing technology in order to neutralize impediments and grow as an agency moves workloads to the cloud and back again. Key capabilities include the ability to inventory data; repeatable, automated, best practice software asset management (SAM) process; and cybersecurity vulnerability management.

The ability to inventory data is critical. According to a Dec., 2018 GAO assessment, agencies are doing a better job of inventorying software assets, but there is more to be done. The key is finding a

PRODUCED BY: FCW DEFENSE SYSTEMS

SPONSORED BY: Flexera Inform IT. Transform IT.

way to understand current inventories and dependencies, and mapping those dependencies to cloud environments. Fraser advises looking for features such as the ability to collect application dependency data from a data center and map it into a business services view that will show what it would look like and how it would work in a cloud environment. Without that step, agencies are at risk of non-compliance or wasting resources.

It's also important to implement a repeatable, automated, best practice SAM process. That's because infrastructure on demand in the cloud requires a different way of managing software assets. An effective SAM solution will generate service components and processes automatically. This includes defining what gets provisioned, what should happen when something changes in the environment, what to do when entitlements expire, and how to manage the environment as it grows or shrinks. It is also cost-effective. According to one recent report, organizations can save as much as 30 percent in annual software costs by implementing a SAM program.

Even the way cybersecurity vulnerability management is handled must change to consistently detect and remediate risks. Fraser recommends using an automated process to set up policies that constantly scan environments and API data, applying the rules specific to an organization's compliance requirements. And while cloud providers have very good cybersecurity vulnerability management tools, Fraser warns that what works on one type of cloud may not work well on another. As nearly all agencies will ultimately be using more than one cloud provider, it's important to think holistically across the entire portfolio and to have tools and approaches that work in all applicable environments, he said.

Achieving the promise of multi-cloud

With the right tools, processes and mindset, agencies can achieve maximum optimization.

Good visibility leads to better insights. If you understand the resources you are using and where your data is at every point in time, you can make smarter decisions, such as which cloud is the right choice for a particular workload, the right way to configure resources, what resources to use, and whether to use your own software license or buy one from the cloud provider. Visibility makes it easier to predict what an organization needs and provision it as required. If an environment increases in load during peak times of the day or experiences specific types of user behavior when certain applications are running, for example, insights gleaned as a result of visibility allow for decisions that optimize resources.

Cost optimization. According to the Flexera report, optimizing existing cloud use for cost savings is the top initiative for organizations for the third straight year. Appropriate automated tools can promote cost efficiencies by tracking software licensing use and costs and cloud resource costs, including cloud provider discounting options, such as AWS and Azure Reserved Instances.

Increased agility. The ability to access resources where and when you need them is attained by implementing an automated infrastructure that can continually monitor and analyze infrastructure usage, vulnerability information and software and cost – and using that information to make necessary changes. Deploying another server in and of itself doesn't solve a load problem, for example. Rather, solving that challenge requires connecting the new server to others in the environment, loading the appropriate software on the server and setting up appropriate compliance procedures.

Software license optimization. Optimizing software licenses requires querying the internal data center environment to understand license position and whether there are entitlements not currently in use that are eligible for use in the cloud. If the answer is yes, an automated way to enable that entitlement is needed. The ability to resolve that license after using the cloud server will also be necessary. By automating the process, agencies can reduce overspending and optimize licenses.

The way ahead. Lacking a universal roadmap for getting to a multi-cloud solution that maximizes efficiency, agility and return on investment, agencies and their trusted partners are responsible for finding their own way. By taking certain actions – increasing visibility and agility, understanding context, improving security and compliance – agencies position themselves to realize the benefits of a multi-cloud environment, even as the IT landscape continues to shift.