radware

5 WAYS APPLICATION DELIVERY CONTROLLERS SIMPLIFY THE TRANSITION OF APPS TO THE CLOUD

Organizations continue to migrate applications to the cloud at an increasingly accelerated rate. According to Radware's C-Suite Perspectives Report, 76% of survey respondents have accelerated their plans for migrating applications and infrastructure to the cloud.

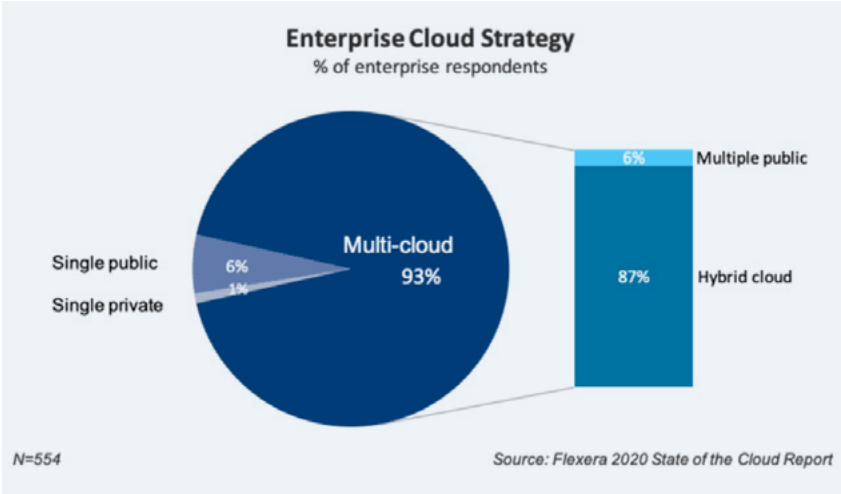
Succeeding in a contactless economy, scalability due to on-demand consumption models, operational instead of capital expenses, and the ability to develop and deploy new applications more quickly are just some of the primary reasons.

Not only are businesses transitioning to the cloud, they're adopting a multi-cloud strategy. According to survey results by Flexera, 93% of organizations have adopted a hybrid cloud strategy.

WITH BENEFITS COME CHALLENGES

But with benefits come challenges. Adopting a heterogenous cloud environment results in lack of continuity for management, security and reporting. Each public cloud environment has its own management tools, monitoring, application delivery and security services.

According to a research by the Enterprise Strategy Group, only 5% of organizations have consolidated cloud management tools (three discrete tools or fewer) for managing the majority of private/virtual clouds and public cloud environments. This fragmented strategy creates a series of challenges:



LICENSING

Budgeting and licensing can become a planning nightmare without cost predictability because scaling an application using a

metered model can result in spikes in operational expenses. Pay-as-you-go models aren't necessarily the answer either, as they can promote shadow IT initiatives that impact both security and cost controls.

VENDOR LOCK IN

This can occur because one cloud provider might provide capabilities/services that another does not. In addition, lack of standardization across clouds may require value-added advisory services, such as technical and consulting.

SELF-SERVICE PROVISIONING BECOMES DIFFICULT ACROSS MULTI-CLOUD ENVIRONMENTS

Provisioning cloud resources typically requires expertise, thereby limiting the ability for end users to self-serve, and complicates the end-to-end automation of processes.

VISIBILITY

Applications that span on-premise and cloud infrastructures inhibits the ability to use a single pane of glass to monitor, manage and identify root cause analysis.

APPLICATION PROTECTION

Moving applications to the cloud complicates cybersecurity. Cloud vendors don't provide comprehensive security controls, nor are they consistent across vendors. Lastly, the attack surface increases once an application leaves the confines of an organization's on-premise data center.

5 CRITICAL CAPABILITIES REQUIRED TO TRANSITION AND MANAGE APPS IN THE CLOUD

SCALABILITY AND AVAILABILITY

The ability to automatically scale is critical for companies looking to automate backend operations. This means having the ability to add and remove services on-demand without manual intervention for licensing and to reclaim capacity when no longer in use. This saves time and money.

COMPREHENSIVE APPLICATION PROTECTION

As hackers probe network and application vulnerabilities to launch DDoS attacks and gain access to sensitive data, application protection becomes critical to protect the business and its brand.

- Prevent denial-of-service attacks that rob applications of performance and undermine the digital experience
- Prevent rogue application ports/applications from running in the enterprise or on their hosted container applications in the cloud
- Prevent bots from targeting applications and systems while being able to differentiate between good bots and bad bots
- Block known vulnerabilities as well as zero-day attack vectors with Web Application Firewalls
- Encrypt data at rest and in motion
- Decrease your applications' attack surface by validating users before they can access an application and grant access based on user privileges

ANALYTICS AND VISIBILITY

As applications are deployed across private and public clouds, monitoring their performance, the user experience, identifying SLA breaches, managing application security events and diagnosing root cause are all critical. A single pane of glass that provides visibility and analysis into all these factors are critical to ensuring an organization's applications are providing a superior digital experience.

AUTOMATION

Cross-domain services that span networking, application and security require collaboration across teams, creating conflicts and delays in testing and provisioning. Automating the deployment of services quickly, or scaling application resources dynamically, becomes critical in a public cloud environment because pricing is structured around usage/resource consumption. Any component in this supply chain requires automation to transform manually-driven processes into automated steps that don't require expertise.

COST PREDICTABILITY

A cloud computing environment only provides as much flexibility as the vendor licensing models your business subscribes to. The ability to control costs when dynamically allocating application delivery and protection services across heterogenous environments when needed is critical. Why? Because many organizations that deploy within public cloud environments often experience unexpected costs once services scale with increased usage.

INVEST IN THE AFOREMENTIONED CAPABILITIES TO ENSURE APPLICATION AVAILABILITY AND SECURITY ADOPTING A HETEROGENOUS CLOUD COMPUTING ENVIRONMENT. ENSURE ANY APPLICATION DELIVERY AND SECURITY SOLUTIONS CHECKMARK THESE CAPABILITIES.

Learn More About What Multi-Cloud Application Delivery Should Encompass

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.