Brought to you by: CIO FROM IDG

ENTERPRISE PUBLIC CLOUD FEARS ABATE

ENTERPRISE IT IS WARMING UP TO PUBLIC CLOUD – EVEN FOR CORE BUSINESS APPLICATIONS.

Many organizations now have years of experience gained through the adoption of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS). Scalability of cloud services was always a given, and now it seems that IT has turned a corner with confidence in the security frameworks of public cloud providers.

"Enterprises have spent two years putting the pieces in place to move applications to PaaS and IaaS; they're now ready to go full speed ahead," declares an InfoWorld column by cloud expert David Linthicum. He says that SaaS is most often used for new, often off-the-shelf software and that the true measure of enterprise cloud progress is the migration of on-premises applications.

Linthicum estimates that going into 2017 Global 2000 companies had migrated just 5% to 7% of applications. But by the end of this year it will be 18% to 20%, followed by a similar jump in 2018.

MANAGING CLOUD RISK

"Those who trust public clouds now outnumber those who distrust public clouds by more than 2-to-1," Intel declared earlier this year when it released results of a global survey of 2,000 IT professionals.

Intel reported that private cloud use declined from 51% to 24% over the previous year, while those using a hybrid private/public cloud infrastructure increased from 19% to 57% over the same time.

To help enterprise IT manage hybrid cloud security issues, ONUG's Open Hybrid Cloud working group last year published a providing guidance on some key steps. These include:

- Categorizing applications and data in tiers of low, medium, medium+, and high risk, and managing them accordingly
- Using a cloud broker to mitigate exploits before they hit the enterprise
- Encrypting traffic on an end-to-end basis, with IT taking complete control and management of encryption keys
- Ensuring IT executives control key functions such as access controls and auditability

GETTING COMFORTABLE

That's not to say everyone is completely comfortable with wholesale public cloud adoption. As they say in the movies, it's complicated. The Intel survey found 49% of respondents slowed cloud adoption due to the lack of cybersecurity skills. And, with almost 40% of cloud services being commissioned without the involvement of IT, almost two-thirds of those surveyed believe the Shadow IT phenomenon compromises their ability to keep the cloud safe and secure.

The reality for many companies is that while they may be creating a formal hybrid cloud infrastructure, it's likely there are other, perhaps many, clouds in use throughout the enterprise. This multi-cloud environment can result in greater innovation and speed to market, but it "complicates the job of properly architecting the security posture," writes Jason Wolford, product manager for Rackspace's Managed Security Practice.

"Efficiently and effectively securing all operational environments, no matter where the infrastructure is located, is pivotal to successfully meeting the demands of the current landscape," Wolford asserts.

"Whether those skills and expertise come from within an organization via well built security teams or via partnerships with those whose sole function is to provide these services, understanding this need is finally permeating the organization from the IT administrator up to the board," Wolford says.

That understanding is key to further adoption of public cloud within the enterprise IT environment.