Making cloud work for business

We are regularly told in survey after survey that corporate concerns about security are the biggest barrier to cloud adoption.

But despite justifiable reservations expressed over the last decade about privacy, control and data residency, cloud adoption continues to grow. This, 'feel the fear and do it anyway' approach was confirmed in a recent study by Gigaom[1]. Of the 500 IT decision-makers interviewed, 71 percent now use Software as a Service (SaaS) solutions, despite some security concerns. Why? The answer was clear: because these products were more economical and agile than in-house alternatives.

Perhaps we have reached a point where commercial pressures and the value of cloud services are just too good to miss? Or is there something more positive at work – a shift in trust and confidence?

Cloud is hardly a bleeding edge technology. The concept of outsourced access to central computing power through a global network has been around since the 1960s. The colossal providers of both hybrid and public cloud services have invested heavily in their security infrastructures to counter trust and security concerns and these investments seem to be paying off.

When the risk averse US intelligence community chooses a commercial cloud vendor to provide a variety of on-demand, pay for what you use, computing and analytic services for the CIA and National Security Agency – you know the tide in cloud acceptance is turning. In a public appearance in 2014, CIA Chief Information Officer Douglas Wolfe called the decision to invest in a $600 million computing cloud developed by Amazon Web Services "one of the most important technology procurements in recent history," with implications far beyond the realm of technology.

So are we witnessing the death of physical data centres within businesses? Unlikely, as even with this very public endorsement of cloud, the service will operate behind the IC firewall. In effect, it will be a public cloud built on private premises.

We predict that using technologies such as VMware or KVM and OpenStack to create private cloud environments through virtualization, will be the way most organizations choose to access the cloud benefits of reduced costs and improved operational efficiency.

Right now, NTT Security is working with organizations across the globe to deliver secure collaborative, convenient, and on-demand network access to a shared pool of computing resources such as servers, storage, applications and services. This paper outlines our approach in terms of strategy, process and technology to turn your data centre from a fixed environment where applications run on dedicated servers to a dynamic, flexible and automated environment – that allows your business users to access the computing and application resources they need anywhere, anytime, and from any device. Whichever cloud model you feel is right for your business – private, hybrid or public – our approach takes you through the steps to create a security architecture that protects, scales and evolves with your changing compliance and business demands.

1. Gigaom, Survey: strategic cloud IT buyers, 2014

1. Using cloud to get closer to your business

When we are asked for specialist advice about cloud security controls, our customers are relieved that our advice is not to treat this element of the infrastructure completely separately. Organizations have invested heavily in relevant policies and governance frameworks – including those for virtualized environments. At a time when further complexity is about as welcome as a fox in a hen house, the good news is that setting out to become a cloud-enabled organization does not mean creating a completely new security architecture.

But cloud security is different and requires a different approach. Here's why.

Mission-critical applications and data have traditionally been kept separate on physical networks, with access controlled by policies underpinned with firewalls and identity and access management. But virtualization and cloud are all about shared resources, so zero trust principles are therefore difficult to enforce using existing technologies. Couple with this demands from business users wanting immediate access to virtual and cloud applications that may previously, in a physical environment, have taken days to conform to carefully designed policies and testing. The pressure is on IT and information security professionals, aware of current and future threats, to balance expectation and risk.

Cloud does not inherently introduce more risk, but the open nature of virtualization means commonly used applications can be used to bypass existing controls. With fewer security barriers to enable performance and efficiency benefits and where data is centralized, attacks are more difficult to see and to stop.

2. Make risk-based acceptance decisions for all applications

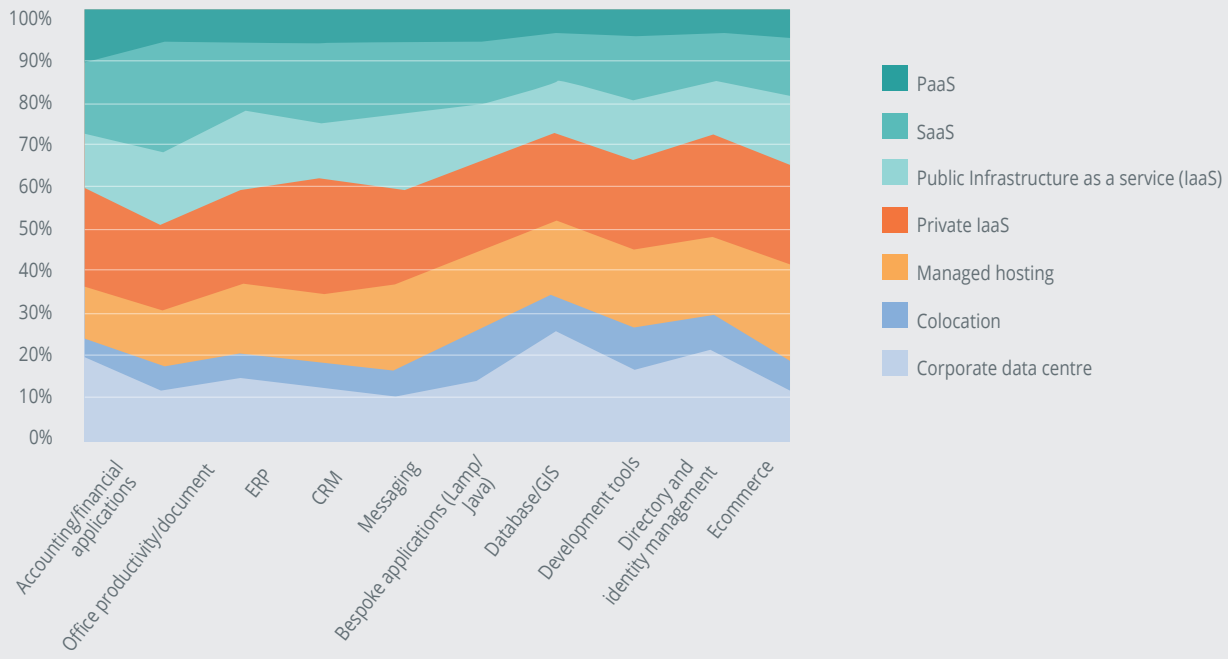
Facing the challenge of cloud security starts with establishing a comprehensive list of services and applications and turning this information into a list of approved suppliers by creating a risk-based acceptance criterion.

The Cloud Reality Check 2015 report from NTT Communications[2], which summarized the findings on a survey of nearly 1,600 ICT decision makers in Benelux, France, Germany, Spain the UK and the USA, found that some 10 percent of apps will never migrate to the cloud, particularly in highly regulated and industrial sectors. Beyond this definite stance, the report illustrated that there is little if any consistency to the delivery model enterprises are choosing for business applications.

Respondents did make it clear, however, that they felt comfortable deploying or migrating core business applications, such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) and e-commerce to a cloud infrastructure with varying forms of control and ownership.

This is often where our conversations with customers begin, as we help them work with the business to explore the right balance of private and public cloud, the flow of data, and most importantly – its value to business collaboration, productivity and performance. We have this conversation at a business level, but also at a deep technology level. We confirm the identity of your data centre applications to ensure that they only use standard ports, stopping rogue applications and applying threat prevention policies to prevent malware entering your organization.

Figure 1 NTT Communications, Cloud Reality Check 2015: Which delivery model do you think is best suited to each of the following applications? (All countries)



2. NTT Communications, Cloud Reality Check 2015

3. Prioritize the application of controls

Once these risk-based criteria are established, IT can work with the business to prioritize the application of controls such as data loss prevention policies, data encryption, identity and access management and change control, consistently across all cloud-based services. This brings them in line with on premise standards and means the same checks and controls are applied.

Talking about cloud with business users does not have to be an adversarial conversation. In fact, in our experience, it can draw IT closer to the business – demonstrating its value by managing cloud adoption in a way that maximizes the productivity and cost benefits of the cloud whilst driving the maturity of its enterprise security. If organizations can increase the automation of controls and the speed of deployment, cloud can actually drive the maturity of information security within organizations.

4. Make cloud work at the speed of business with faster policy deployment

Firewall is a great word, comfortingly implying something solid and impenetrable. But in a virtualized or cloud environment, businesses need something that gives the same level of protection and levels of zero trust control, but can work faster and with greater flexibility.

Over time, many organizations have built firewall estates with hundreds of rules that govern convoluted processes using multiple management tools. Throwing virtualization and cloud into the mix does not have to compound this problem, but too often organizations fail to examine or explore their cloud options. Sadly, the result is a virtualized version of port and protocol security appliance that will only add to an organization's management headache.

A new approach to shared computing resources gives an opportunity to review and refine legacy firewall estates. At NTT Security, we are working together with organizations to develop a new set of simple, consistent next generation firewall controls and advanced threat protection – with native management tools that exploit the speed and cost benefits of virtualized and cloud environments.

5. Establish zero trust in the cloud

Many organizations we talk to are eager to replicate the zero trust principles within virtualized and cloud environments so that they can:

1. Control access based on application, compute workload or user identity
2. Block potentially rogue or misconfigured applications
3. Prevent known and unknown threats from compromising the network and moving laterally
4. Implement application-specific threat prevention policies

Organizations are eager to achieve these goals to safely enable applications by user, application and content without slowing down performance. And because we have done this before, we can help businesses realize these goals.

Conclusion: We make cloud work for your business

Cloud computing is here to stay. The Cloud Reality Check survey shows that organizations anticipate the proportion of ICT budget allocated to cloud will have grown by around 6 percent to 28 percent in 2018.[3] Business wants the benefits that cloud can deliver and our job is to help organizations make cloud work for them, while managing the risk and avoiding additional complexity and cost.

Many organizations have taken the first steps into the cloud, typically through ad hoc virtualization projects or SaaS delivery of specific applications. Without adequate planning however, many of these projects will not realize the full return on investment and economies of scale that can come from a strategic, coordinated approach to cloud deployments.

We are helping our customers take control of cloud initiatives, working with the business to define expectations and outcomes. If IT does not take control of cloud initiatives, change will happen anyway – but it will be fragmented. And in our experience, this not only undermines the business benefits, but potentially introduces more risk from a 'shadow IT' footprint within the organization.

Finally, in planning the journey to the cloud, businesses should be looking for compelling events that justify the next step on the path. Technology triggers such as hardware refresh cycles, major application projects, mergers and acquisitions etc. all provide opportunities to progress the journey, while protecting existing investments and maximizing overall return on investment.

3. NTT Communications, Cloud Reality Check 2015

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.