

September
2010

Beyond. Security

How security and the cloud can
work together to deliver **results**



1

Organisations across the world are seeking the best ways to do the same or more with less.

To work smarter, more efficiently and more productively – while reducing costs.

Squaring this circle has demanded that computing infrastructure be optimised, and that services be quick and dynamic. This is why cloud computing has been touted so enthusiastically as a revolutionary game changer.

Despite the universal hype, adoption has been slow. Our customer research shows that the most common concern among organisations contemplating moving to a cloud is security.

Partly, this stems from a very human psychological suspicion of something that can't be seen and touched. Many CIOs don't like the idea of a shared, non-physical resource. They fear the lack of control that something in 'the cloud' suggests, as opposed to the reassuring visibility of something they can touch.

But the trepidation about moving to the cloud is more than that.

Our research shows that 44 per cent of CIOs believe they deal with information that is too sensitive for the cloud. With cyber crime currently number three on the FBI's priority list, these concerns are less easily dismissed. There are other real and justifiable problems, such as concern about geographic location. The storage of information on a remote, hosted server can be anathema to some enterprises. To others, such as those in heavily regulated financial services, it is a regulatory impossibility.

So, not all these fears are unfounded. But some are misplaced. It's time to move beyond the scare stories and examine where the risks really lie.

Firstly, no organisation should simply assume that a service provider's security is up to scratch. Data storage is simply too mission-critical today to leave hostage to presumption. It is the single most valuable commodity to most organisations, and nobody wants to be responsible for losing any of it.

“During the last five years, not a single security incident has occurred. During that period, BT has consistently enhanced the resilience of our business and has enabled our banks and their clients to meet and exceed regulatory obligations. At Isabel, we have come to appreciate BT as much more than a mere provider of network infrastructure services.”

Philippe Dermine
Chief Technology Officer
Isabel

2

No matter how good a lock you place on your front door, most people choose to outsource this protection and keep their savings in a bank. But banks, like anything, are not 100 per cent risk-proof, as events of recent years have shown.

The truth is that organisations have every right to want more than assurances over the security and geographic location of their data. So we need a pragmatic solution.

Let's tackle the security threat first. 'Public' clouds carry a degree – however small – of risk. 'Private' clouds are more secure, but don't offer the same benefits of flexibility and cost efficiencies. The pragmatic solution is simple: take the best of both worlds.

A hybrid system combines internal resources, which stay under the control of the organisation, with external resources delivered by a cloud provider. You get the productivity and efficiency benefits of cloud services but you can keep sound control over those parts of your network or data that are very sensitive. It's a way to solve some of the trust issues of the public cloud without sacrificing the benefits.

“The new network not only delivers increased bandwidth and improved network availability but is also a platform for future expansion.”

Roberto Parra
CIO, Director de Sistemas
de Información

Second, let's tackle the more intractable problem of geographic location, so often a regulatory and compliance stumbling block for organisations that would like to use the cloud but need to ensure their customer data is stored within their national borders.

Looking beyond the hype, the solution is again startlingly simple: organisations are outsourcing critical elements of their business and need to look at it in that light. They achieve the right level of compliance via the development and enforcement of outsourcing contracts with their cloud provider. This implies the need to ensure that their provider understands, and adheres to, all relevant legal and regulatory requirements relevant to the storage and movement of their data. As with so many cloud-based services, discussed elsewhere in this series, such as Unified Communications and hosted contact centres, the time is finally here when it is possible. Which means organisations should feel positive about going beyond the scare stories and towards a bright, cloud-based future.

3

How can BT Global Services help keep your cloud secure?

“Last year BT invested £2bn in network and products. Now is the time for our customers to leverage that investment.”

Most importantly, our suite of managed security services keep organisations secure, whether their head is in the cloud or not.

Managed Firewalls, Security Event Monitoring, Message Application Security, Distributed Denial of Service Mitigation, Web Access Security and Intrusion Prevention Service comprise the main components of that suite of services. Together, this integrated network security offers a cost effective, dynamic protection of global networks and IT infrastructure, be it premises-based or cloud-based.

When it does come to security in the cloud, however, which we recognise worries many CIOs, BTGS offers a comprehensive assessment Cloud Security Readiness Assessment. This reviews an organisation’s current security programme and creates a roadmap for maintaining its current level of security during the migration to cloud computing.

In addition to improving organisational understanding of the risks inherent in changing IT infrastructure, the information BT provides enables organisations to:

- Draft cloud-based service level agreements, contracts, RFPs, and security requirements
- Manage corporate policies regarding legal, HR, compliance, and risk management to address security implications of adopting the cloud
- Determine which existing security capabilities and practices that can be applied to the cloud environment and optimise them to manage new security challenges
- Evaluate recommended additions and changes to the security program to ensure it aligns current security expectations to the realities of cloud computing

“Nationwide is seeking to introduce standard security services across its business, to reduce costs and to improve business agility. BT was chosen because it demonstrated a complete understanding of the security architecture needed to ensure delivery of these objectives”.

Peter Stafford
IT Director, Nationwide

4

“When it comes to internet security we felt most confident in the offer made by BT. The fully managed BT proposal would support a wide range of client devices.”

Wilson Ferguson
Head of Online Channels, Direct Banking
NAG Europe

Geographic location

This year, BTGS is the first major networked IT services provider to respond to organisations' cloud-based concerns by implementing its Virtual Data Centre (VDC) solution on a country-by-country basis. The sole driver of this is its customers' need to meet regulatory requirements regarding location of data storage.

Granular control

BTGS is also releasing VDC Dedicated, a solution that makes the most of the scale and automation of cloud computing yet retaining the customers' absolute requirements for performance, complexity and security. VDC Dedicated gives organisations all the benefits of a cloud-based service but allows them to regain some of the granular control over their data and applications.

Security at the heart of everything

Security is woven into every service BTGS provides, regardless of whether that service is cloud-based or not:

- We have one of the largest dedicated security practice communities in the world – a security community of 1400+ full time client-facing consultants, architects and designers.
- Our security practice manages and monitors more than 300,000 devices globally
- We manage secure data networks for 90 per cent of the UK's major financial institutions.
- More than 10,600 financial sites are connected by BT around the world
- The world's largest four banks rely on our networks to keep their data secure
- We have vast expertise acquired via acquisitions, including Frontline, Counterpane, Radianz, Infonet, iNet, INS and Net2S (Cybernetworks)
- We have achieved BS 27001/ISO17799, SAS70-II and FIPS 140-2 accreditation
- This year (2010), our Security Services Group received the highest rating overall among 65 of the world's leading IT security services vendors in Datamonitor's Black Book of Outsourcing report
- BT Global Services is one of two providers noted as having “comprehensive” ranking for breadth of managed security services in Forrester's Market Overview: Managed Security Services.

BTGS is helping organisations move beyond fears of security, location and loss of control.

Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

Janette Bennett
Clinical Director – Asia Pac
Global Health Practice
BT Global Services
Tel: +612 9269 1000
Email: janette.bennett@bt.com
www.btglobalservices.com
Designed by Tag