

Cloud Security: An Independent Assessment

A Quantix White Paper

Dec 2010



Call us on: 0115 983 6200
Visit us on-line at: www.quantix-uk.com
E-mail us at : enquiries@quantix-uk.com

WHY ARE PEOPLE CONCERNED WITH CLOUD SECURITY?

Many aspects of cloud security are based on established enterprise architecture principles. Indeed, many cloud architectures will offer as standard a level of security which many midsized businesses will struggle to achieve within their own resources.

There are however, some specific aspects of the cloud model, which raise particular challenges for information security:

- Multiple customers will be sharing the cloud infrastructure to store data. How do you ensure absolute segregation of such data?
- Each customer will have their own security policies to control how their user can access applications and data on their own network. How do you maintain such individual access controls rather than all customers having to comply with a standard service?
- Scalability is a key benefit of cloud. How is data integrity assured as the underlying virtual servers and storage expand and replicate to meet the needs of multiple customers?
- Out of date application and operating system versions and patches are a key security vulnerability in any system. How do I know my data won't be compromised by another cloud user with an out of date security configuration?
- Customers can (usually) quickly detect attempts to compromise security on their own networks. How will a Cloud Service provider deal with a real or suspected security breach?

Many of these issues are highlighted in the Cloud Security Alliance statements on cloud security best practice and we comment on these specifically later in this report. Not all clouds are the same, and how a Cloud architecture deals with these issues goes to the heart of the effectiveness of its security model.?

The Top 7 Security Threats to Cloud Computing Services

In March 2010, The Cloud Security Alliance published its "Top 7" security threats to cloud computing services. These are based on its more detailed best practice guidance issued in 2009:

1. Abuse and Nefarious Use
Customers with malicious intent able to apply for and use cloud services
2. Insecure Interfaces and APIs
Gateways (internal and external) to services leave open routes by which information can be compromised
3. Malicious Insiders
Cloud provider staff able to compromise security from the inside
4. Shared Infrastructure Issues
Poor design and use of enterprise infrastructure components allow "leakage" between customer data sets
5. Data Loss or Leakage
Customer data can be lost or compromised by system failure or breach of security between domains
6. Data Loss or Leakage
Customer data can be lost or compromised by system failure or breach of security between domains
7. Unknown Risk Profile
Insufficient information available to allow the true level of security risk to be assessed by an individual customer



HOW DOES QUANTIX ADDRESS THESE THREATS?

Many cloud architectures are based on traditional enterprise architecture designs, with cloud-specific security features ‘bolted on’ as a reaction to changing market perceptions or to meet specific customer demands. Quantix has taken the time to build a cloud-specific, multilayered security architecture which has been designed from first principles with the specific needs of customers choosing to use the cloud in mind.

This independent review highlights the following key features of the Quantix Cloud Service Architecture which ensure that it addresses the above issues:

- **ISP class firewalls** : in common with all services this type, customers connect to the Quantix Cloud using standard internet protocols, either over the web (home and remote users) or over dedicated telecoms connections (office users) . As with any internet service, the first point of access (“perimeter security”) is an internet firewall. Quantix has chosen to base its firewall services on Juniper SRX650 devices. These provide the highest possible level of IDP (intrusion detection & protection), spyware and other malware defence protocols. Each firewall can be configured to meet the access control needs of individual customers based on the concept of separately configurable “zones”. These are “ISP Class” firewalls, comparable to those used by public internet service providers and provide some of the highest levels of perimeter security available today.
- **Customer specific access security:** remote access for users to the Quantix Cloud is provided by the Quantix SecureConnect service, based on an industry standard SSL VPN architecture. An SSL VPN provides a highly secure method to connect and authenticate user over the web and without any requirement to install software on the user client.
- **VLAN segregation and multi-layer security policies:** once connected, users access cloud resources on their own private virtual (VLAN) operating as an extension to their own network. The standard logical separation of such VLANs is strengthened by a physical implementation at the network switch level (based on enterprise class Juniper EX series switches) which implements a customer-dedicated switch and firewall “stack”. This provides two key security benefits:
 - **VLAN “hopping”** (the weakness in some cloud networks which allows switching between VLANS) is completely disabled by turning off VLAN-level switch management and auto-trunking
 - **Customer specific security policies** can be configured and enforced at each level (firewall, SL VPN, Switch and VLAN) of the stack, exploiting the capabilities of the integrated use of top-end Juniper devices
- **Independent hypervisor layer:** Quantix utilises industry standard VMware technology to operate the virtual machines at the heart of its cloud infrastructure. By design, however, these resources are not shared, but are dedicated environments for each customer, providing customer-specific server clustering, resource scheduling and local data replication. Not only does this effectively ringfence resources at the database and application level, but allows customer specific patching and configuration management policies to be applied.



Physical server assets within the data centre are not shared but are managed within Quantix dedicated racks and secure areas - provisioned to a minimum of Tier 3 standards - preventing any risk of compromise from other data centre users

- **Replication and resilience:** the cloud infrastructure incorporates a redundant component design at all levels; firewalls, SSL VPN, switch and server/storage. Virtual machine technology (based on VMware and an enterprise-class Netapp storage network) builds in resilience at the data storage and application level, with high-availability underpinned by site to site replication incorporating automatic failover at multiple levels. Secure, off site data backups can also be provided if required.
- **Auditing and monitoring:** logs and environment monitors are provided by many of the individual components within the architecture, with much of this status data available through secure customer portal. This capability is further enhanced by the bespoke Quantix reporting system GEM, which also provides comprehensive management of change control (what, when and by who changes have been made to system configuration). Quantix is currently investigating the deployment of state of the art industry tools to further strength this area of capability.
- **Support processes:** customer setup and support processes are designed and managed to ISO 20000 standards. This includes the use of standard security templates which can be customised to meet individual customer requirements. A comprehensive event logging and monitoring system is backed up by regular security penetration tests carried out both in house and by accredited external agencies. The results of such tests are available for customer inspection.

Taken together, these features combine to ensure that the Quantix Cloud Architecture provides a very high level of information security, consistent with the best practice proposed by the Cloud Security Alliance.



WHO ARE QUANTIX?

Quantix is one of the UK's premier providers of Managed Cloud Services, Application Managed Services and Hosted Infrastructure Solutions for Enterprises and Independent Software Vendors – a true managed Cloud Services Provider.

Our secure, dependable platform and proven application expertise allows us to provision a wide portfolio of both hosted and on-premise application management services that can deliver considerable IT cost savings and de-risk technology investments. Through production-ready services such as Managed Application Hosting, Cloud-based Disaster Recovery, SaaS Enablement and Managed Messaging we are already delivering demonstrable competitive advantage to our clients.

Capitalising on experience gained through supporting over 250 managed services clients, as well as our top-tier relationships with best of breed vendors such as Oracle, Microsoft, Juniper and VMware, Quantix has created an enterprise grade Virtual Private Cloud platform that offers compelling SLAs and flexibility.

WHAT WE SUPPORT:

- Oracle Database 8i, 9i, 10g and 11g
- Oracle RAC
- Oracle Application Server
- Oracle E-Business Suite 10x, 11x, Oracle R12
- Microsoft SQL Server 6.5, 2000, 2005, 2008
- MySQL

CONTACT QUANTIX:

Call us on: 0115 983 6200

Visit us on-line at: www.quantix-uk.com

E-mail us at: enquiries@quantix-uk.com

Nottingham Office:

Quantix House
Chetwynd Business Park
Nottingham
NG9 6RZ

London Office:

23 Austin Friars
London
EC2N 2QP

