

iQloud

Have everything. Own nothing.

HALOTEQ's iQloud Platform sets the standard for enterprise-class infrastructure and application performance. A robust, virtualized infrastructure deployed as multiple, secure infrastructure clouds in HALOTEQ's data centers, the iQloud Platform serves as the underlying technology for all of our service offerings and is designed to aggregate other cloud services client needs may dictate.

The Platform includes the building blocks of a system infrastructure service, including:

- Virtualized Servers
- Virtualized Desktops
- Virtualized PBX/VoIP
- Windows and Linux operating systems
- Storage
- Networking
- Firewalls
- Load balancers

Enterprise-Class Infrastructure

The iQloud Platform is built on a state-of-the-art infrastructure:

- VMware's vSphere 4 virtualization platform
- Memory configurations specifically optimized for virtualization
- Juniper Virtual Chassis Fabric technology
- IBM XiV tiered storage
- Virtualization firewalls

Highly Secure Cloud Computing Environment

The iQloud Platform employs a multi-prong approach to ensuring and enforcing the security, privacy, and integrity of enterprise applications and data. Our data centers are compliant with SAS 70 Type II requirements for physical and logical security.

We employ an array of physical and data security measures:

- 24/7/365 on-site security personnel and video surveillance
- Two-factor Authentication
- Biometric palm scanners at entrances
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Log aggregation and correlation
- Firewalls & Redundant Anti-Virus Systems
- Role based permissions

These security measures also extend outside of iQloud to **ProTEQ MS**, our network operations, management and monitoring services for "on premise" PCs, servers and network devices.



High-Speed, Scalable Cloud Architecture

High-speed connections to physical servers hosted in data centers ensure that complex applications scale to meet business demands. Load balancing options include low-cost shared solutions to support smaller environments, and multiple virtual load balancers – deployed and managed from within the cloud portal – to support more complex environments.

iQloud Platform Security – A Multi Faceted Approach

Managed Cloud Services—Security

The iQloud Platform provides all of the security measures associated with traditional hosting environments, including two-factor authentication; network intrusion detection and prevention; automated vulnerability scans; and third-party penetration testing.

Advanced firewall technology provides intelligent threat defense with advanced capabilities, including identity-based access control and denial of service (DoS) attack protection. As stated above; role-based access control ensures that users have only the permissions required for their business or support roles. Permissions can also be set on objects or groups managed by HALOTEQ. All activity is logged for auditing purposes.

Compliance is at the heart of the iQloud Platform. Our data center(s) are SAS 70 Type II compliant, and undergo rigorous reviews of policies, practices and security measures by certified independent auditors. iQloud also conforms to the security principles and guidelines established by the Cloud Security Alliance.

iQloud Platform Security Framework

The most effective security is a comprehensive, layered defense based on a framework. iQloud leverages specialized tools to protect the integrity of all virtual machines and Internet communications. iQloud's logical abstraction layers allow for multi-tier security policies in order to provide true defense in depth. Enterprises with limited IT resources may not be able to afford the same security measures, and as a result are at significant risk. Migrating to HALOTEQ's iQloud represents an opportunity for the enterprise to build in security from the ground up.

iQloud Platform Hardening

Hypervisors provide a consolidated, logical view of multiple virtual machines (VMs). VMs running on the same physical machines must be guaranteed to remain isolated from one another, through omission, "mis-configuration", or intentional breach.

The Center for Internet Security and the Defense Information Systems Agency (DISA), as well as hypervisor vendors, publish "hardening" guidelines. Hardening examples include how to correctly protect memory segmentation using container rings, and familiar steps like best-practice configurations, deploying the latest patches, and proper cleaning up of de-provisioned virtual machines and resources.

Hardening helps guarantee virtual machine isolation and challenges penetration from within and without. Properly hardened hypervisor layers prevent end users from inadvertently mapping IP addresses across virtual machines, IP spoofing, intentionally leveraging Network Address Table

(NAT) mapping to hijack communications or installing "eavesdropping programs" to monitor virtual machine memory space. New configurations, patches, or layered security policies are rapidly propagated across the iQloud Platform infrastructure. All of these security concerns are monitored on an ongoing basis in order to continually strengthen security.

Fully Integrated Business Continuity

Designed specifically to meet enterprise IT demands, the iQloud Platform delivers services on best-of-breed technology infrastructure from leading vendors including IBM, Juniper Systems and VMware - all provided with one of the industry's strongest SLAs.

iQloud is configured for high availability – two fabric interconnects are connected as cluster peers, allowing both an active and standby instance of the Juniper Switch manager to run on the fabric interconnects. If the primary instance fails, the standby instance assumes the role of primary instance.

iQloud Disaster Recovery Benefits

Disaster recovery is integral to the iQloud Platform. With a top-tier operations center and a highly-resilient service delivery infrastructure with the ability to span multiple SAS 70 Type II certified data centers, the Platform minimizes the risk of downtime.

Two-Tiered Cloud Computing Storage

The iQloud Platform employs a two-tiered approach to storage. Primary storage is handled by IBM™ XiV storage area networks (SANs) that combines high I/O rates with redundant fiber channel links to the disk arrays. A flexible, elastic, cloud storage capability handles enterprise requirements for secure supplementary file storage, advanced file sharing, and collaboration.

Learn more about our approach and our solutions by contacting a HALOTEQ Sales Representative:

1.877.442.5633

**email: sales@haloteq.com
website: www.haloteq.com**