

Overview

The integrity and security of your data is vital to you. We know that, and therefore continue to invest heavily in secure, robust and reliable systems architecture. Information and documents residing within the Viewpoint For Projects solution are available securely 24 hours a day, 365 days a year and we confidently offer Service Level Guarantees far in excess of the industry norm.

By deploying the Viewpoint For Projects application, you can eliminate the risk of information loss through network failures, email, virus or server hardware faults. Our system allows you the peace of mind that all information is fully available, fully secure and fully backed-up for the duration of the project – and into the future.

Viewpoint are ISO 27001:2005 certified; the highest international standard for Information Security Management available. As such, you can be assured that the highest standards possible are applied to everything that we do, including the overall security and processing of your data.

Rackspace hosting provider

Viewpoint partners with Rackspace for hosting services. All services are located within the UK in three of Rackspace's data centers in the London area. The three data centers are used to provide primary, secondary and archive computer facilities. A further hosting facility is located in our EMEA Head Quarters and data is streamed here as a backup of the primary and secondary facilities. This provides for a disaster recovery mechanism should it be required, data is streamed asynchronously ensuring even the most recent data is available should a disaster occur.

Network

Rackspace guarantee 100% uptime on network services, this is powered by their Cisco infrastructure. The network runs at approximately 20% utilization at peak times and when utilization reaches 30% new infrastructure is automatically added. One of the strengths of Rackspace is their peering (the agreements with other Internet Backbones to exchange traffic). Peering enables Internet Backbones to exchange traffic between each other efficiently and quickly. Peering is provided both privately and at neutral exchange points. BGP (Border Gateway Protocol) routing ensures automated failover to alternate providers in event of connectivity issues. The Rackspace network also includes a patented Denial of Service mitigation service to protect against external threats.

Physical Security

No public access - Public access to Rackspace data halls is strictly forbidden. This removes the need for anyone other than highly trained Rackspace Engineers to be allowed into the data halls.

Video surveillance - Live video surveillance of each data center facility is monitored 24 x 7. All entrances to the building and data center are monitored to ensure only authorized personnel enter sensitive areas.

Onsite security personnel - The security team monitor each data center building 24 x 7. Rackspace security personnel provide the first layer of security for access to the data center.

Biometric security - Biometric scanners are used to restrict access to each data center. The biometric security systems represent the second layer of security for access to the data center. Within the organization, only Rackspace Engineers are authorized to access restricted areas.

Pass cards - In conjunction with the biometric scanners, access to each facility is restricted to those who hold a Rackspace pass card. The pass cards are also required for moving from room to room within the data center. Our security pass card system is the third layer of security in the data center.

Environmental Systems

Power systems - Each data center gets its power from commercial utility underground conduits. There is a 10minute battery backup to provide continuous power if a short failure of the mains utility supply occurs. We also have multiple diesel generators with full load capability, on standby to provide long term power in an emergency.

UPS systems - The power systems are designed to run uninterrupted even in the unlikely event of a total power outage. All staging and production systems are fed with conditioned UPS power which will run if utility power fails. The UPS power subsystem is N+1 redundant with instantaneous failover in case the primary UPS fails.

Diesel generator systems - Onsite diesel generators will automatically start in the event of a power surge or power system failure. The power subsystems are designed to cut over immediately with no interruption in the event of a power failure. Both are regularly tested to ensure they will function properly in the event of a power system failure.

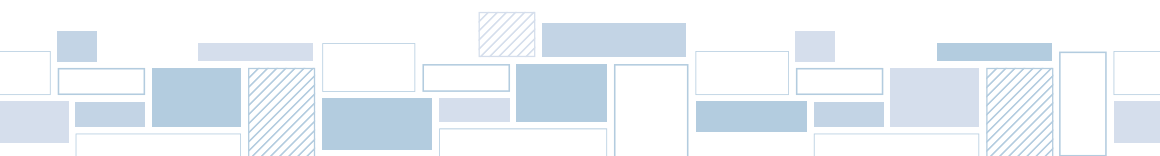
Cooling - The data center facility has a closed loop chilled water system. It is cooled by 5 x 1.5MW chillers in an N+1 arrangement (8 at maximum capacity). Each data hall is configured in a hot and cold aisle arrangement. An 800mm pressurized plenum is fed by computer room air handling units in an N+25% arrangement connected by a flow and return chilled water loop.

Smoke detection & fire suppression - Early warning of any fire hazards at the facility is provided by Protec Stratus high sensitivity smoke detection systems. These are backed up by Protec fire alarms. In the unlikely event that the worst should happen, fire suppression is provided by dry pipe double knock sprinklers. This requires two smoke detectors in a single zone to trigger an alarm. The sprinkler head bulb will then only burst when the temperature exceeds 60 °C in that immediate area.

Policies, Procedures and Controls

ISAE 3402 is an international auditing standard intended to provide customers and prospects with third party validated visibility of a service provider's controls. Rackspace is subject to an ISAE 3402 Type II (SOC1) audit annually covering all data center facilities globally.

Information Security - ISO/IEC 27001 is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS). All hosting operations performed in the Rackspace data center have been certified compliant to ISO27001:2005. The certificate can be viewed on the Certification Europe website by following this link: <http://client.certificationeurope.com/print/5053>



Application Architecture

The Viewpoint For Projects hosting facilities are physically secure, authentication of users is highly sophisticated, and the software solution itself provides a high degree of flexibility, providing either full open collaboration, tightly controlled security, or a balance between the two. Strict measures are in place to detect and counter hacking attempts, denial of service and virus attacks. As you would rightly expect, external penetration tests are conducted annually.

Tiered Security Architecture

To protect clients' data, an absolute minimum of the application infrastructure is exposed to the Internet. Those parts of the system that are by necessity available are extremely secure. The presentation, application and database tiers are on separate secure networks with firewalls securing a minimum level of access between each tier. This ensures that all data is protected behind several layers of security.

Access Control

Access control is done on several levels. Security is driven on an individual basis determined by the specific role of the user. The access control security is enforced via Viewpoint For Projects' own business objects, which operate on a hierarchical basis so that the system can be as open or restricted as required. Individual Logins provide a full audit trail and track of who has accessed specific documents. In addition there is optional module and folder level security to restrict access to advanced or sensitive areas such as secure documents.

Infrastructure

Viewpoint are dedicated to providing the highest uptime possible to our customers. We utilize infrastructure from Dell, Cisco, BIGIP, NetApp, VMware and of course Microsoft to deliver the application. The hosting environment has been designed to have no "single point of failure". All major server, storage and network components are configured in an N+1 configuration; Servers are clustered to provide failover and load-balancing capabilities, this includes a highly available SQL Server database cluster to secure the heart of the Viewpoint For Projects application.

Complementing the hardware infrastructure is a 24x7x365 pre-emptive monitoring service coupled with fanatical support from Rackspace. Hardware replacement guarantees are of one hour or four hours dependent on the device.

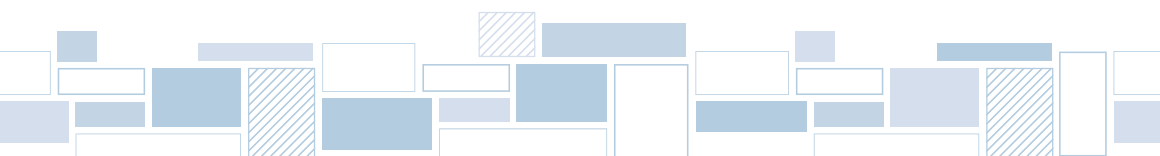
A gigabit network is used for presentation, application and database devices with a 10 gigabit network powering file storage, block storage and the hyper-visor tier.

SSL Security

Viewpoint utilize SSL technology to ensure that all data passing between the web browser and the server is transferred securely. All Viewpoint For Projects Web Servers have been specifically hardened to remove the weaker ciphers and enforces a minimum of 128-bit encryption across the board.

Anti-Virus

Every file uploaded to the system is automatically checked by anti-virus software in a secure area before it is moved to the file storage system.



24/7 Pre-emptive Monitoring / Alerting

Viewpoint has an extensive internal monitoring system in place, which provides round the clock monitoring of all elements of the systems and applications, providing pre-emptive alerts of any faults or alerts conditions.

This is backed by external monitoring to get a customer perspective, our external monitoring service 'Pings' the site every minute from over 10 global locations. Exceptions are triggered through our alerting system on a 24 x 7 x 365 basis.

Server Security

Management access to all servers is strictly controlled and audited - only a set list of qualified Viewpoint staff have access rights. Remote access is made via a secure network connection from our EMEA headquarters. Servers are built to a standard and then 'hardened' to remove all unnecessary services.

- Only authorized users get access to the system
- Authorized users can only perform actions they are allowed
- All actions are audited

No user data is stored on web servers - All data are stored in the database or secure file store. 128-bit SSL encryption is available to all users, giving the best level of security available for data transmission over the internet. All users' passwords are stored using a one-way encoding algorithm so not even Viewpoint staff can read them.

Backup and Archival

The database and all servers are backed up to the primary location and this is replicated to a secondary Rackspace data center. Full backups are taken weekly, Incremental backups nightly, Transaction log backups every 5 minutes. All backups are kept for 3 weeks. Subject to pricing archival copies of your data can be sent to you on an external hard drive. This data can be read with our Offline Archive product. Archives contain a read-only full replica of your data at a set point in time, preserving access rights and including audit trails.

Still have some questions?

Please feel free to contact Viewpoint if you require a more complete explanation of any aspect of our security or hosting infrastructure.

Visit us at www.viewpoint.com to learn more or see an informative demo.

