



InterVis On-Demand Platform

Security and Availability Datasheet
July 2006

SECURITY

Data Infinity recognizes that data security is crucial to our customers and their business. The InterVis On-Demand platform is built from the ground up using world-class security techniques and principles, encompassing application, server, network and physical security aspects. Coupled with our extensive technical expertise and commitment to continual improvement of our security policies, customers can be assured of unsurpassed protection and privacy of their data.

SECURITY DETAILS

The InterVis On-Demand platform contains a wide variety of security technologies to ensure data protection is maintained at all times. These can be broken into four broad layers – application, server, network, and physical.

Application Security

Data Encryption – Client interaction with the InterVis On-Demand platform is via industry standard 128-bit SSL encryption, with certificates issued from fast-growing certification provider RapidSSL for 99% browser compatibility. This ensures data is fully protected from our production servers to the customers screen.

Data Separation – The InterVis On-Demand platform tags all customer data with identification information inside the database. This information is security checked against the user's logon credentials before any further processing or display occurs. Customers can be assured that their data remains visible only to themselves.

Access Control and Authentication – InterVis On-Demand can only be accessed by users presenting a valid username and password. All communications during the logon process are SSL encrypted, and passwords are hash encrypted before being stored in the database. Idle sessions

have a timeout of 30 minutes, protecting users from unauthorized use of their information.

Furthermore, the application utilizes an access control security model based on the same principles that network firewalls use. Each component in InterVis is protected by an access control list that determines a user's right to use that component. This fine-grained control enables InterVis to support complex security arrangements.

Identity Management – The InterVis On-Demand platform includes a separate application dedicated to managing user accounts and subscriptions. Passwords for normal users can only be reset by their account administrator. However, passwords for the account administrator can only be reset after authentication by Data Infinity support staff.

Server Security

Operating System Security – All production servers use enterprise-grade Linux operating systems. These servers run minimal installation configurations and are maintained at the latest patch levels. In addition, they are enabled with the advanced Security-Enhanced Linux feature - developed by the US National Security Agency - which provides for greater system stability and application security. All access to the servers are protected by strong passwords and encrypted links, and are audited at the operating system level.

Database Security – InterVis is built on Oracle, one of the most secure databases available. Access to the database is controlled at the connection level, and all connection requests and critical operations are audited. In addition, the application itself is limited in the operations it can perform inside the database.

Management Security – Only authorized system administrators from Data Infinity and its managed hosting provider have access to production servers. Server access is strictly audited and access accounts are restricted to select operations for

maintenance, monitoring and data backup purposes.

Network Security

Intrusion Defense – The production network is protected by leading hardware-based firewalls, which are further supplemented by software-based firewalls on the servers themselves. Both are configured to be as restrictive as possible, blocking out known spoofing, denial-of-service and other IP attacks. Data Infinity works closely with its managed hosting provider to proactively identify and manage security threats, including frequent vulnerability assessments of its servers.

Virus Protection – All production servers run on the Linux operating system, making it extremely resistant to virus activity. No components run on the Windows platform, and there are no access points for malware or spyware to exploit.

Server Protection – In addition to the firewalls, a variety of network technologies are used to hide servers from the outside world, including non-routable addressing schemes, port redirection and network address translation. All Data Infinity servers run in its own private network, separate to and protected from other systems in the data center.

Physical Security

Data Center Security – The facilities at Data Infinity’s managed hosting provider is able to offer unparalleled security and reliability for running the InterVis On-Demand platform. The data center is staffed 24x7, with audited cardkey access and regular security patrols. All server and network equipment are monitored continually by a dedicated security department. The center and its equipment are wholly owned by the provider and not shared with others.

Administrative Personnel – Both Data Infinity and its managed hosting provider view security and confidentiality of data with utmost priority. Data Infinity obtains full non-disclosure agreements

with its managed hosting provider protecting the data residing on the InterVis On-Demand production servers. This covers all personnel having access to the equipment.

Additionally, Data Infinity and its managed hosting provider are committed to the continual training of its employees in security technologies and associated interests.

AVAILABILITY

Regardless of how secure a system may be, if it cannot be accessed when needed it is useless. Data Infinity recognizes the importance of reliability and availability in any online application. Careful consideration of this has been made in the development, deployment and ongoing maintenance of InterVis On-Demand.

AVAILABILITY DETAILS

Reliability and availability can be addressed on three factors – Server Uptime, Network Uptime and Application Stability.

Server Uptime

InterVis On-Demand servers have been configured with redundant power supplies, storage and network connectivity to ensure maximum availability. In the event of a catastrophic hardware failure, standby systems can be activated within a moment’s notice. All servers run enterprise-grade Linux, offering enhanced performance and greater reliability than standard versions. Servers are monitored 24x7, with faults paged to both systems engineers and application support teams.

Server backups are taken daily and are transported offsite to a secure data vault via a dedicated fiber optic network. This allows servers to be rebuilt rapidly in the event of complete storage failure.

Network Uptime

Network connectivity within the server data center has been designed with high availability in mind. All carriers are connected via multiple fiber optic rings providing maximum connection uptime to the Internet. Network routing equipment have redundant power supplies, processors and interfaces, with critical failure points configured in clustered formation. Monitoring of the network is carried out 24x7, with faults automatically paged to network engineers.

The data center itself is solidly built, and is located in a region with minimal exposure to natural disasters. It is equipped with redundant power connections and circuits and in the event of a power failure, has an automatic two stage backup system utilizing both batteries and diesel generators. Dual HVAC systems also maintain constant temperature and climate even in the event of a power failure.

Application Stability

The InterVis On-Demand platform is developed using a stringent methodology to ensure the highest level of quality and stability. It uses stable, production-grade open source components that have been rigorously tested and incorporated in other commercial software products. The application undergoes an extensive test cycle, with multiple testing rounds completed before a version is released to production.

InterVis uses an Oracle database to ensure customers data is served efficiently and promptly. Oracle is one of the leading databases on the market, well known for its performance and high availability features.

Data Infinity uses a dedicated support team to monitor the day-to-day running of the InterVis On-Demand platform. In addition, the application generates system alert notifications, enabling proactive action to be taken in the event of an error. Data Infinity is committed to the stability of the

InterVis On-Demand platform and releases patch updates to the application on a regular basis.

Data Infinity may modify its policies from time to time and reserves the right to make changes to this datasheet where appropriate.



InterVis On-Demand Platform
Security and Availability Datasheet
July 2006

CORPORATE HEADQUARTERS
Data Infinity Australia Pty Limited
Level 11, Tower B, Zenith Centre
821 Pacific Highway
Chatswood, NSW 2067
AUSTRALIA

Phone: +61 (2) 9944 3256
Fax: +61 (2) 9944 3260

SALES CENTER
Data Infinity, Inc.
Techmart Center Suite 320
5201 Great America Parkway
Santa Clara, CA 95054
UNITED STATES

Phone: +1 408.850.7208
Fax: +1 408.562.5745

www.datainfinity.com