



# The Instantis Data Center

For Hosted  
EnterpriseTrack™  
Deployments

Version 1.0  
December 2006

# Table of Contents

Introduction

Reliability

Availability

Scalability

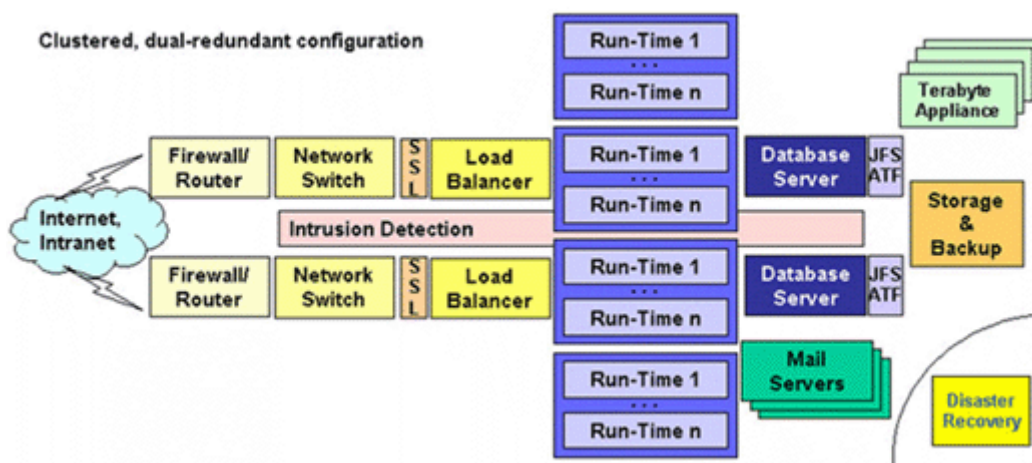
Security

# Introduction

EnterpriseTrack™ is available for deployment on a hosted infrastructure. Through a combination of best-of-breed computing technology, innovative software, proven management practices and skilled personnel, Instantis achieves business-critical levels of system reliability, availability, scalability and security for your application and data.

## Reliability

Instantis has consistently met mission-critical levels of availability since it began offering EnterpriseTrack™ as a hosted application. Historically, planned uptime is virtually 100% and Instantis expects 100% availability from a planned uptime perspective to continue indefinitely. Further, with the exception of major system upgrades -- which have historically occurred approximately once every two years -- planned downtime averages about 12 hours per year. As a result, Instantis achieves a 99.9% availability level even when including planned downtimes. This impressive track record for reliability is the result of significant design efforts, solid engineering and sound technology investments. An important part of EnterpriseTrack™'s uptime achievement is the reliability of the software, hardware and networking components of the system.



# Availability

Critical to EnterpriseTrack™'s high reliability are the redundant systems in place to ensure continued smooth operations in the event of a failure or breakdown of one or more infrastructure components. Redundant hardware devices, disk drives, network connections, power supplies and software components are in place to continue delivering services so that potential service hiccups are transparent to all system users. We also have a backup disaster recovery system that mirrors the production system in terms of configuration and data. These two systems are in different data centers that are geographically separated. If necessary, we are capable of switching between systems on short notice.

**Software Redundancy** — Software redundancy is achieved by having multiple instances of the application server, web server software and other supporting systems running on middle-tier computers. The software components are responsible for maintaining sessions and processing transactions on behalf of authenticated users. In fact, there are multiple instances of software on each middle-tier server, and there are multiple instances of middle-tier computers. Software redundancy is also achieved at the database layer by having two instances of the database software running on two separate computers in active-passive mode such that if one instance of the software fails, then the other automatically and seamlessly takes over.

**Hardware Redundancy** — Hardware redundancy is achieved by having two or more physical instances of each hardware component, thus eliminating single points of failure. The infrastructure includes redundant computers to run application servers and databases as well as specialized devices such as load balancers, firewalls, network switches and mail servers. Each redundant instance of hardware is supported by a separate power supply feed. Devices operate in active-passive mode, with automatic failover. In the event of failure, failover occurs immediately, transparently, and without any interruption of service to the application.

**Storage Redundancy** — Storage redundancy is achieved through disk array technology. The disk array is a highly reliable system that contains multiple battery-backed, redundant storage processors and multiple power supplies. The disk array is a RAID array allowing for any disk to fail with transparent and immediate failover to a spare disk. The connection between the disk array and the database servers is through two redundant fiber connections

to each database server (four in total), each going to separate redundant interface cards in each server.

**Network Redundancy** — Network redundancy is achieved by having multiple, separate high-bandwidth connections to the Internet backbone tied to two separate routers within the data center's network. Thus, if one connection fails, the other is available to transport data traffic.

## Scalability

In addition to EnterpriseTrack™'s high-reliability and availability features, the system is scalable to support extremely large volumes of concurrent usage across multiple dimensions:

- Accounts and/or customers
- Concurrent active users
- Transactions
- Large databases (within a single engine and across multiple engines and accounts)

Further, the intelligent load-balancing capabilities and multi-tiered architecture of the underlying application framework means that this performance is assured with virtually any mix of transactional workload within the system. Scalability is achieved through a combination of intelligent design and "big iron" components. Instantis engineers continually monitor, test and tune performance characteristics of the system, eliminating potential bottlenecks before they arise. Scalability is also the result of major investments in the latest, most sophisticated computer technology. By leveraging its technology investments across multiple customers, Instantis makes its powerful infrastructure available and affordable to organizations of every size.

## Security

Instantis understands how important security is both to you and to your customers. Instantis backs its technology with an experienced team of systems and security experts who follow proven administration procedures to safeguard your applications and data. The multi-faceted security practices include:

**Physical Security** — Production systems are stored in a commercial-grade data center, protected around the clock by security personnel using state-of-the-art monitoring and biometric access technology.

**Firewall Protection** — Multiple layers of firewalls insulate the entire production environment from unauthorized access, providing powerful protection from a broad range of attacks. Network and port address translation and packet filtering obscures internal non-routable IP addresses.

**Security Zoning** — We use multiple layers of firewalls (with redundancy at all layers) to isolate the load balancers, EnterpriseTrack™ servers, mail servers, database servers, etc. into zones and constrain the communication between these zones using firewall rules.

**Intrusion Detection Systems (IDS)** — Network and host-based IDS perform real-time analysis of traffic, protocol, and log messages. They also log packets, significant messages, and search content to detect a variety of attack and probe patterns. These systems raise real-time alerts and produce periodic reports that are examined by deployment personnel.

**Data Encryption** — Instantis uses 128-bit Secure Socket Layer (SSL) encryption, delivering the highest level of transaction encryption available through web browsers today. SSL accelerator hardware speeds processing of encrypted communications.

**User Account and Password Authentication** — To access systems or data, users must provide a valid username/password combination. Users can change their passwords, but cannot eliminate passwords. All valid changes to user accounts and passwords are effective immediately.

**System Hardening** — Only a minimal set of application files and access points required for operation are configured on each computer or device. Passwords are stored in encrypted files separate from application data.

**Database Security** — Separate database segments are used to store objects associated with a single account, eliminating the possibility of authorized users of one engine gaining access to other engines. Access to the database from the Web is exclusively through the application and authentication systems. SQL access via the Internet is not possible.

**Server Management Security** — Automated systems provide around-the-clock monitoring of security events and system malfunctions. Instantis personnel are notified immediately of any issues and take immediate action. All security events are written to a log file for analysis.

**Security Management Practices** — Administrators complete comprehensive screening prior to gaining access to systems. Administrators working on production systems document all actions and changes. Deployment personnel conduct periodic analysis of key server and security metrics.

**Data Backups** — Hot backups of the full database are performed every night and are automatically shipped off-site using secure VPN circuits.

EnterpriseTrack™ is engineered for the highest possible reliability, availability and scalability. While no computing system can assure zero service interruptions, Instantis brings together the technology processes and people to deliver a very high level of service with minimum requirements on the part of your IT or business staff.