

TimeLink **OnDemand Edition**

Technical White Paper



Table of Contents

Overview	3
Product Infrastructure	3
N+1 (Redundant) Systems	3
Technical Architecture.....	4
Data Backup	4
Product Security	5
128-bit Secure Socket Layer (SSL) Data Encryption.....	5
Application-Only Access.....	5
User Authentication, Role-Access and Account Lockout	5
Audit Trail	6
Monitoring.....	6
Business Continuity	6
Optional Total Failure Recovery.....	6
TimeLink OnDemand Co-Location Facilities	7
Physical Security	7
Power Supply	7
Internet Connectivity	8
Fire Suppression	8
HVAC Systems.....	9
Appendix A – Failure Modes and Recovery Time	10

Overview

TimeLink's Software as a Service (SaaS) offering, TimeLink OnDemand Edition, delivers the application and infrastructure you need to drive business success. With TimeLink OnDemand, you receive all the benefits of the traditional premise-based TimeLink Enterprise Edition, with the added advantages of a hosted solution. Benefits include a rapid implementation, lowered total cost of ownership, and the ability to focus on your core business. Through TimeLink OnDemand, we operate your entire infrastructure with the appropriate installed and configured TimeLink components over the long term in a high performance Data Center.

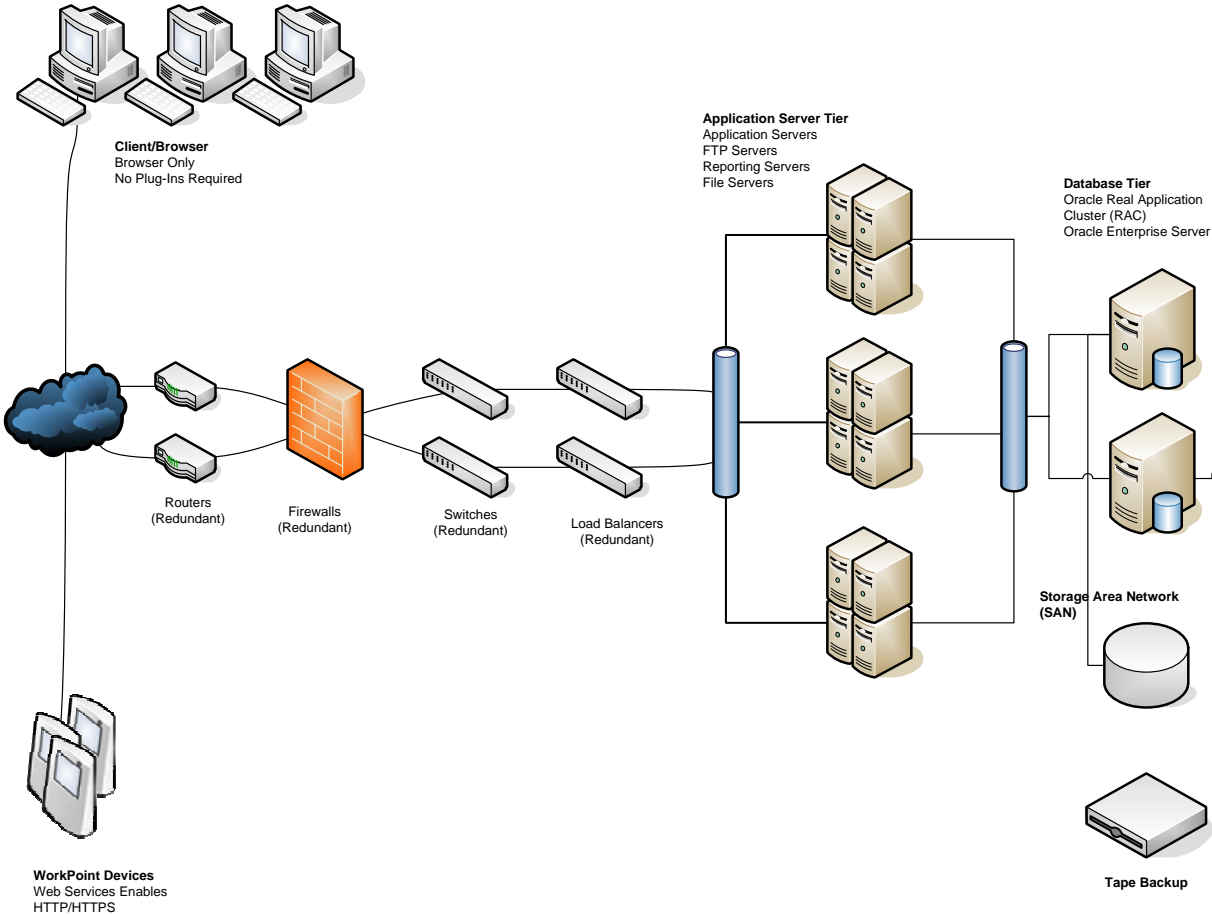
Product Infrastructure

N+1 (Redundant) Systems

The TimeLink OnDemand solution leverages a highly redundant N+1 architecture that has been designed for high availability. The N+1 architecture means that the solution is comprised of multiple redundant elements, and therefore in the event that one of them should fail, the other element can assume its processing load causing little to no interruption in the service.



Technical Architecture



Data Backup

All TimeLink OnDemand data is protected in several ways. All production data is immediately stored on multiple redundant physical disks. This approach protects against a single physical disaster on disk from interrupting service. In addition, there are two daily database backups. The first, a logical backup to disk, would provide a rapid restoration point in the event of a system-level disaster. The second backup is direct to tape media for offsite storage.



Product Security

The TimeLink OnDemand solution has undergone rigorous security and system penetration tests by the industry-leading security provider Symantec.

128-bit Secure Socket Layer (SSL) Data Encryption

The interaction between the client and the TimeLink OnDemand infrastructure is protected using powerful 128-bit SSL encryption technology, the same technology that is used for e-commerce. This approach ensures that information being exchanged between the client browser and the TimeLink OnDemand solution is secure.

Application-Only Access

TimeLink OnDemand has a multi-tier architecture that ensures the separation of the application (business logic) and the data (database server) tiers. Authorized users are only able to access the application via the application servers using their login credentials. There is no access to the data or databases servers directly – providing another level of protection for our client's data.

User Authentication, Role-Access and Account Lockout

TimeLink OnDemand maintains the same comprehensive security components as the premise-based version, TimeLink Enterprise Edition. Users are assigned to roles that allow *access* only to authorized transactions. Additionally, users are limited to edit and/or view only data (such as employees, cost centers) that they are *authorized* to. User accounts can be required to maintain 'strong' passwords with specific configurable composition requirements and



can be automatically locked out if someone has made three (default setting) consecutive unsuccessful login attempts. These security features ensure that users are only able to perform the appropriate actions on the appropriate data in the system.

Audit Trail

The TimeLink application provides for comprehensive auditing, including a trail of all changes to the database.

Monitoring

TimeLink utilizes tools and technologies that address monitoring for the following:

- Network performance
- Network utilization
- Availability (servers, databases and network)
- CPU and disk utilization

Business Continuity

Optional Total Failure Recovery

In extraordinary cases, certain customers may require exceptional safeguards and levels of redundancy outside the standard capabilities provided for by the TimeLink OnDemand solution. In these cases, TimeLink can architect, develop and maintain additional hardware and software infrastructure needed to meet these requirements. This would be outside the scope of the standard TimeLink OnDemand offering and would need to be priced out independently



TimeLink OnDemand Co-Location Facilities

TimeLink maintains a Data Center at a Cervalis Co-Location facility in Wappinger Falls, NY. This facility was a former IBM Data Center and is SAS-70 compliant. To learn more about Cervalis, please visit www.cervalis.com.

Physical Security

The Data Center adheres to an integrated security approach ensuring that our customers' equipment and data are protected at all times with multiple levels of security protection. Dedicated security personnel monitor controlled access at the building perimeter and within the Data Center. Proximity card readers and video surveillance systems monitor and control access within the facility. The Data Center is further protected by biometric readers. Throughout the state-of-the-art facility, 52 video surveillance cameras, motion sensors and biometric identification systems create a fortress-like environment. Each proximity badge is matched to an individual fingerprint. All video surveillance, proximity and biometrical readers' data are monitored from the central security office. There is also security staff for 24x365 physical security management.

Power Supply

The Data Center is designed with full N+1 redundancy so that each component is connected with multiple power and networking connections at all times. Its power design is based on multiple and fully divergent power grids and substations, N+N Uninterruptible Power Supply (UPS), N+1 generator backup, and N+1 generator feeds to the building. It also has a highly available electrical



infrastructure. The electrical system is built on a tiered electrical system:

- 2 In house electrical sub-stations
- 2 Separate Power Grids
- 4 Individual 500KW UPS
- 2 2MW Diesel Generators
- 3000 Gallons of Fuel per Generator

Internet Connectivity

The Data Center has a fault tolerant network which provides divergent routes and multiple connections in networking cable, via multi-homed Synchronous Optical Network Technology ("SONET") rings. This setup establishes a Necessary + 1 ("N+ 1") redundancy. All network devices are, at a minimum, N + 1 redundant. The wide area network is self-healing and fully redundant delivering a high speed local area network infrastructure. The Data Center is currently interconnected and peering with national and international Tier 1 and Tier 2 carriers

Fire Suppression

The facility maintains a comprehensive Fire Protection System. This system monitors all the smoke detectors throughout the building. If a smoke detector is activated, the specific location of the incident is displayed on unit monitors located within the Security Command Center, Network Operations Center, the Data Center, and an offsite Central Station. In addition to standard fire extinguishers mounted throughout the Data Center, there is also 'dry pipe' fire suppression system. Utilizing this municipally mandated system, the fire sprinkler heads and connecting pipe are not filled with water until a fire emergency would require it. Police and fire departments are less than a mile away from the building.



HVAC Systems

The Data Center cooling system is a closed loop, glycol-based system that includes:

- 4-750 ton HVAC cooling towers supported by 5-600KW chiller pumps
- 38 air handlers
- Cold water (approximately 43 degrees Fahrenheit) provided to each unit, circulated through a heat exchange unit that moves cold air under the Data Center floor

Appendix A – Failure Modes and Recovery Time

Component	Failover Action Plan	Estimated Recovery Time
Network Access (Cervalis controlled)	Redundant Internet paths	Immediate
Network/Connectivity (TimeLink controlled)	Redundant Switching	Immediate
	Redundant Load Balancer	Immediate
	Redundant Firewall	Immediate
Database (daily production backup)	Database Node Failure	Immediate
	Database Logical Restore (daily backup)	1 - 4 hours (database size dependant)
	Database Tape Restore (daily backup)	1 - 2 days (database size dependant)
Application Server	Hot Backup	30 mins – 1 hour
File Server	Nightly Hot Backup	30 mins – 1 hour
Report Server	Hot Backup	30 mins – 1 hour
Power	Redundant Power Distribution Units (PDU) – all PDUs have been deployed in an N+1 layout to accommodate a full load in the event of a failure.	Immediate
	Redundant Power Circuits – power circuits have been provisioned and deployed in an N+1 layout to accommodate full load in the event of a failure	Immediate

TimeLink

2975 Westchester Avenue. Purchase, NY 10577

t. 800.474.9300 f. 914.834.9414

e. info@timelink.com

www.timelink.com

TimeLink is a trademark of Time Link International Corp. Other product and company names referenced herein may be trademarks of their respective owners. The information contained herein is subject to change without notice.

Copyright ©2009 Time Link International Corp. All rights reserved.

TIMELINK™

TimeLink OnDemand Edition
Enterprise Workforce Management