

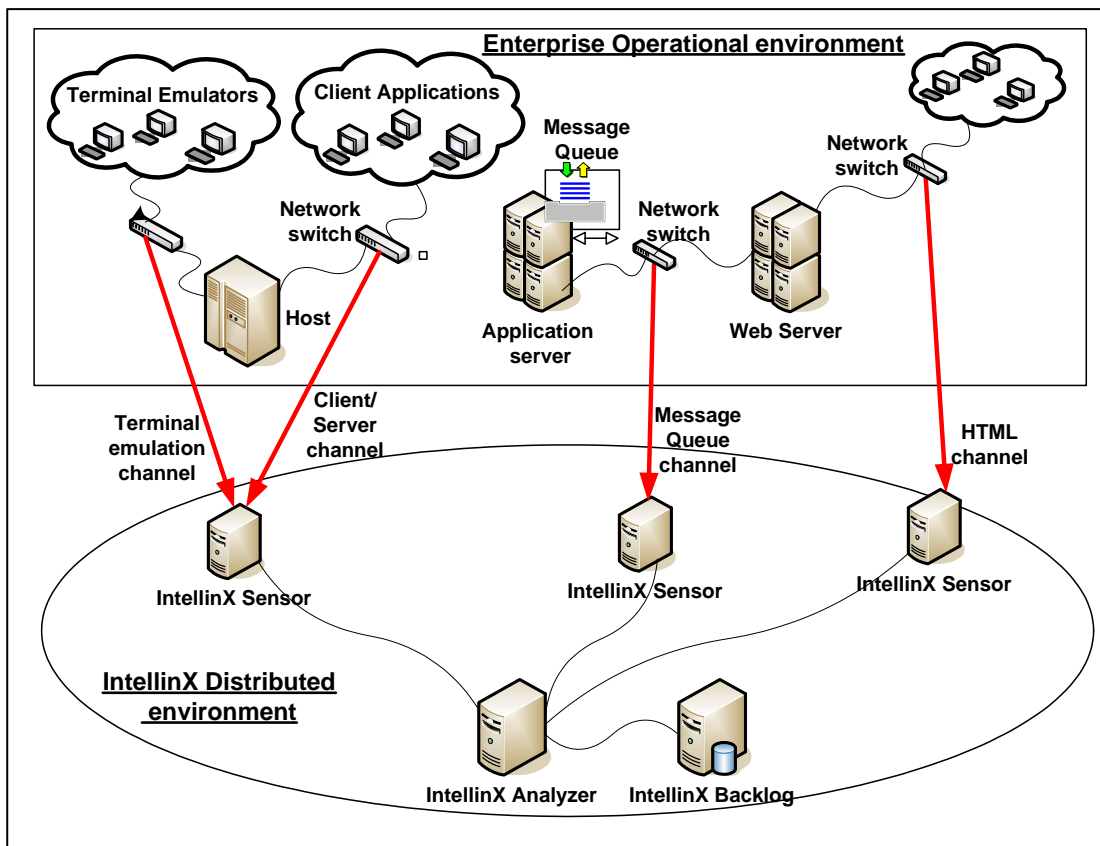
## Intellinx V2.1 - Technical Data Sheet

### The Architecture

The Intellinx system architecture is modular and scalable designed to track activity of unlimited number of users in a distributed environment. The system is comprised of the following components (services):

- Repository
- Sensor
- Data Channel
- Backlog Writer
- Action Service
- Backlog Viewer

Each component may have one or more instances. For example, you may run several sensors. Each sensor may listen to several network switches. You may run several data channels each monitors a different protocol of a different server. The services communicate using queues that can be implemented in various ways.



### The Operating environment

#### 1. Operating Systems on which Intellinx runs

- Microsoft Windows 2000, XP, 2003
- Linux Redhat Enterprise 4 or similar
- Unix

## 2. DBMS in which the Intellinx database can reside

- DB/2
- MS SQL/Server
- Oracle
- MySQL
- Any JDBC compliant DBMS

## 3. Monitored protocols

- 3270 – SNA, TN3270, Enterprise Extender, SSL support
- 5250 – SNA, TN5250, MPTN, SSL support
- Client/Server messages – TCP/IP, MQ Series, MSMQ, mainframe SNA LU0 and LU6.2, SMB
- HTTP, HTML, SSL Support

## 4. Amount of disk space required

In general, the disk space required is relatively not large since the system stores raw network traffic, not screen images. The screens are reconstructed from the network data when needed.

- 3270/5250 screen activity – recorded activity of one user in one workday requires on average 50KB - 60KB. Based on that, recording of 10,000 users for 6 months requires about 80GB – 90GB.
- HTTP screen activity - The space required is somewhat higher than 3270 screens depending on the nature of the application, but still only the raw data is stored, not the screen images.
- Client/server messages – the required disk space depends on the amount of messages stored by the system. The stored data is condensed with typical ratio of 1:10.

## 5. Intellinx health alerts

The Intellinx Analyzer sends SNMP alerts when it detects that:

- The Sensor does not capture data from the switch for a period of predefined time
- The Analyzer detects that the queues are empty for a period of predefined time, which means that the Sensor is not operating
- The Backlog queue files exceed some threshold size
- The disk space available for the Recordings is smaller than a particular threshold

# The Business Rule Engine

## 1. Investigation capabilities

- Search over raw data
- Extract specific fields that are stored as index
- New rules may be applied to old recorded data for after-the-fact analysis

## 2. Business Rules

- Analyze flow of Screens/Messages/HTTP requests, Fields, Business Events
- Inner session, cross session, cross platform analysis
- Logic for identifying user activity flow and processes is defined using a point-and-click wizard
- Complementary logic can be specified by JavaScript

## 3. Alerts and Actions

The result of a business rule may include:

- Sending Email or SMS
- Issuing SQL statements for writing to databases
- Sending a message over MQ
- Executing a Web Service