



Intellinx

Frequently Asked Questions

Q. Does Intellinx have a minimum or maximum number of users?

The Intellinx architecture is very flexible and scalable, providing a cost effective solution to organisations with 200 employees as well as corporations with over 100,000 employees.

Q. How does Intellinx monitor user activity?

The Intellinx sensors (sniffers) are connected to one or more network switches in an organisation's data centres. Each sensor server may listen to one or more protocols in one or more network switches. Intellinx tracks user activity in internal business applications by sniffing network transmissions between the host servers and the clients.

Q. What protocols can Intellinx monitor?

Intellinx tracks user activity in any application that utilises any of the following protocols:

- IBM Mainframe screen protocol - 3270 on SNA, TCP/IP (TN3270) and Enterprise Extender
- IBM iSeries screen protocol - 5250 on SNA, TCP/IP (TN5250), and MPTN
- Client/Server messages – TCP/IP, MQ Series, MSMQ, IBM mainframe SNA LU0 and LU6.2, SMB
- HTTP, HTTPS
- VT100 and other VT flavours

Q. Can Intellinx monitor legacy systems?

Since the user activity is reconstructed from network transmissions, Intellinx monitors any type of user activity regardless of the host's operating system or TP monitor. This permits monitoring of any type of end user.

Q. Does Intellinx monitor ALL user activity?

Intellinx does not record any activity that runs on the employee's workstation such as web surfing, email or instant messages. It only records interaction between the employee workstation and the business applications running on the corporate servers.

Q. Who can access the Intellinx system?

Only authorised users are allowed to access the Intellinx system. Access to the system is usually limited to internal auditors and fraud investigators.

Q. How configurable is the system?

Intellinx is extremely granular and can be configured to monitor specific applications or users only, whilst other information is filtered out and dropped.

Q. Can sensitive information be hidden from auditors?

Specific fields and screens can be masked or hidden preventing an auditor from seeing sensitive information.

Q. Is access to the system logged?

Every access to the Intellinx system and every action performed within the system is logged giving a detailed audit of which user performed which action.

Q. Can additional protections of employee privacy be deployed?

Fields identifying a user can be hidden by the system when a visual replay is performed. The user ID can be revealed only if a suspicious event is detected or a specific investigation conducted.



Q. How much disk space does Intellinx require?

Intellinx does not store the actual bitmap of the user screens but rather stores the intercepted raw network transmission from which it reconstructs the user screens when needed; hence it is very efficient regarding disk space. The data is condensed at a ratio of 1:10. Based on the experience of Intellinx customers using 3270 based applications the recorded data of one end-user of a whole day typically requires about 50KB – 60KB.

Q. How does Intellinx handle data encryption?

There may be several scenarios:

1. The encryption/decryption are performed on a gateway server and not on the host. In this case, Intellinx can listen to the network transmissions between this gateway and the host, since it is not encrypted.
2. The encryption/decryption are done on the host using SSL. In this case it is required that the private key of the host is supplied to Intellinx; this way Intellinx can decrypt the encrypted traffic. It should be noted that the recorded data is encrypted and digitally signed by Intellinx, so the data is protected once it is decrypted by Intellinx.



e-Solutions & Services UK Ltd

Upper Linbrook Farm, Needwood,
Burton-upon-Trent, Staffordshire
DE13 9PF

Phone: 0870 855 0631

Email: enquiries@e-solutions.uk.com

Web: www.e-solutions.uk.com



Q. Can I record and analyse activity of internal users only or also external users outside our firewall or on the Internet?

Since the sniffing is performed on the switches located close to the host, Intellinx records all user access to these host computers regardless of the user location inside or outside the firewall.

Q. How long does it take to implement Intellinx?

Intellinx is installed on a separate Linux, UNIX or Windows server which is connected to a standard mirror port of the switch. Therefore there is no intervention whatsoever in the host or client software or hardware making it very easy to install and test Intellinx. The installation process is very short, typically just a few hours, and is totally risk-free. Once the system is installed, it can start recording all the screen communication immediately, allowing the internal auditors to perform a search. For example, the auditors can search for all the users who accessed a specific account number in a specific timeframe. Once the system is installed it collects user activity data.

Q. How can I do a proof of concept of Intellinx?

An on site proof of concept typically takes about 3 days, during which time the system is installed and connected to the network and several business events are defined. These business events are configured according to the organisation's specific requirements. User behaviour patterns are tracked in the organisation's business applications and instant alerts are generated on exceptions.

