



TECHNICAL BULLETIN A PPENDIX

Date: 01/29/02

Technical Bulletin Appendix TBA013002

Subject: Intellex Lessons Learned Appendix

Intellex Virus Protection
White Paper
December 13, 2001

This white paper addresses protection from computer viruses on the Intellex product.

Intellex is designed to be immune to infection by viruses crafted to attack standard computers and Windows applications. This opinion is formed by knowledge the Intellex design and the known methods of virus attack on computer systems.

Specifically:

1. **Not a standard computer / application.** The Intellex is a specialized computer device running an embedded Windows application. No other applications run on the same host as Intellex. This eliminates one of the common paths for virus introduction, copying foreign data files from an infected host onto Intellex.
2. **No email or web browsing capability.** Most viruses today are introduced into systems via email or email attachments. Since there is no email function in Intellex, this is not possible. And since there is no way to access web sites or download from the Internet, this path for infection is eliminated as well.
3. **No disk drive network sharing.** The disk drives in Intellex are not shared with other hosts on the network. A malevolent virus or worm on another host on the network cannot access the drives on Intellex to damage any system or data files.
4. **Controlled access through Network Client and Intellex API.** The only network communications supported between the Intellex application and any other host on the Network is conducted through the Intellex API. This is a set of software tools that control the communication between a client and the Intellex recorder. Since the only commands and data that are accepted by an Intellex originate within these proprietary tools, any viruses on the client host are prevented from infecting the Intellex.

Information furnished by Sensormatic is believed to be accurate and reliable. However, no responsibility is assumed by Sensormatic for its use; nor for any infringements of other rights of third parties which may result from its use. No license is granted by implications or otherwise under any patent or patent rights of Sensormatic Video Systems Division.

Technical Services Email- vsdtechservices@tycoint.com

Tel (800) 507-6268 (International: 561-912-6259)-Option 2 • Fax (845) 624-7685

Security Considerations:

Continued protection against virus infection requires that the operation of the Intellex is consistent with its design and intended use. Configuration changes or installation of any unapproved application software may provide a means for virus attack as well as result in conflicts with the Intellex application.

Any networked computing device can be hacked, and digital video recorders are no exception. There are other types of attacks possible on network based computer systems that even anti-virus software cannot protect against. It is the responsibility of the corporate IT personnel to provide firewalls and other security measures to block illegal access to their networked computers.

We have thousands of Intellex systems running on customer networks and our own. We have had virus attacks on our email system and network file system, and no Intellex has ever been infected. Also, there is no known occurrence of a customer Intellex being infected by a computer virus.

Video Systems Division Engineering

Information furnished by Sensormatic is believed to be accurate and reliable. However, no responsibility is assumed by Sensormatic for its use; nor for any infringements of other rights of third parties which may result from its use. No license is granted by implications or otherwise under any patent or patent rights of Sensormatic Video Systems Division.

Technical Services Email- ysdtechservices@tycoint.com

Tel (800) 507-6268 (International: 561-912-6259)-Option 2 • Fax (845) 624-7685