

ZignX Product Matrix

Features	ZignX Medical Advanced	ZignX Medical Basic	ZignX
Access Control Authentication to PC using Token (SmartCard) and PIN code. This is operated through the ZignX front panel. The Access Controls is validated only in the ZignX box hence works independently of the operating system.	X	X	X
Log-off function (system lock) This function allows the user to securely leave the PC. When the user pulls out his SmartCard, the mouse and keyboard automatically locks and can only be unlocked by the original user, the Superuser, or a preset "Group" member".	X	X	
PIN-code Policies PIN-code min-max. length, expiration interval, and renewal can be set. This will force the user to comply with a predefined PIN-code policy.	X	X	X
Internal memory All recordings done by ZignX are stored in non-volatile memory located inside the unit. The data can be extracted (in Superuser mode) through an external serial port. ZignX will notify user on low storage capacity.	X	X	
Recording of Keystrokes The keyboard recorder will record keystrokes made on the PC keyboard and save it with time stamp in the internal memory.	X		
Recording of Log events Log-events (log-in, log-out, log-attempts and failures) as well as setup changes made in the ZignX unit are recorded with time stamp and stored in the ZignX internal storage.	X	X	
Recording of RS-232 port The RS-232 recorder will record a copy of data passed through RS-232 com port and save it with time stamp in the internal memory.	X		
Data Integrity Log files kept in ZignX can only be accessed by extracting the file from the unit. When extracted the file are given an "end time stamp" and secured with a MD5 hash checksum. ZignX automatically generates a new log file which is given a "start time stamp" identical to the preceding "end time stamp" to verify log-file succession.	X	X	
Intrusion detection system The ZignX intrusion detection system will detect, log, and notify if anybody opens the PC or interrupts the ZignX control of peripheral devices such as keyboard and mouse.	X	X	(X) only case intruder switch
Drive Control ZignX controls the power to each drive, e.g. HDD and CD-ROM drive, inside the PC. Each drive are controlled individually and linked to a ZignX boot-profile which is used to create different boot scenarios. Using two HDDs will enable two completely separated boot-up configurations.	X	X	X

Network Separation As with the Drive Control, optional ZignX Network Interface Cards (NIC) can be used to separate networks. Pairing two HDD with two ZignX NIC in two different <i>boot profiles</i> will completely isolate one network from the other.	X	X	X
Operating System independent ZignX runs 100% autonomous. It only needs power to operate using the 20-pin ATX power cable from the power supply.	X	X	X
No impact on existing system ZignX relies only on hardware controls and will not interfere with the Operating System or programs on the host system.	X	X	X
Internal NIC The ZXM Advanced is equipped with internal Ethernet card which is for optional usage.	X		
Internal Time The ZignX unit has an integrated clock which is used for timestamp. The ZXM clock can only be set by the Superuser.	X	X	X
Time Frame Time frames can be set in which the user has access to the PC.	X	X	X
Unique ID Each ZXM can be identified by a unique (<i>not changeable</i>) ID number.	X	X	X
Backup Battery The battery backup secures system settings and alarms status in case the power is disconnected.	X	X	X