



High density, small form factor
ultra secure KVM

ADDERView Secure

USB, dual link DVI-I and audio KVM switch for environments where security must be guaranteed

PRODUCT IN BRIEF

The AdderView Secure enables a keyboard, monitor and mouse to be shared between high and low security systems, sometimes known as red and black networks, and is designed carefully to prevent information flowing between computers or to the outside world via emissions snooping. The AdderView Secure design prevents sensitive data from leaking between ports, sensitive data leaking to the outside world and sensitive data from being stored in the device. Furthermore, the switch actively combat a range of potential leakage "threats".

FEATURES

Uni-directional data paths for keyboard and mouse

One-way data paths ensure that data isolation does not rely on trusting microprocessor software, but is instead assured by hardware and prevents a hidden software weaknesses that could potentially cause data leakage. A uni-directional structure also protects against timing analysis or forced malfunction attacks and prevents computers influencing the operation of any common circuitry.

Minimal emissions profile

The AdderView Secure is heavily shielded with double shielding in critical areas to minimise the risk of eavesdropping equipment being able to pick up signals from the equipment.

No shared RAM between ports

The keyboard and mouse processor is powered down and reset at each switchover to thwart shared RAM leakages. Separate memories hold the num, caps and scroll states and are only accessible when the relevant channel is selected. All data buffers are actively cleared once they have been used.

One time programmable microprocessors

Microprocessors are one time programmable and don't contain reprogrammable flash memory. This protects against sensitive data being stored within the device and protects the software against being corrupted.

60dB crosstalk isolation

High crosstalk isolation ensures that less than 1/1000th of any signal from one computer is presented to the input of another computer due to electrical crosstalk.

Restricted USB function

The USB ports will only support keyboards and mice and other devices, such as USB storage drives, are actively prohibited.

No microphone connections

To prevent small levels of crosstalk noise from being "recorded", microphone connections are banned from the design.

Independent power supplies block power line signalling

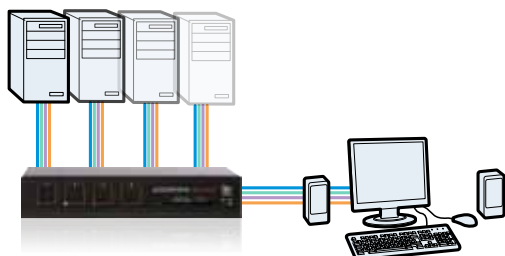
The circuitry for each port is independently powered from the USB lead. Power line signaling is therefore blocked because different port circuits don't share the same power feed.

AdderView Secure checks its own operation

The hardware and software must agree before data flow is enabled. The switch constantly checks its own operation and will stop operating and flash its error light if an unanticipated event occurs.

Maximum compatibility

For maximum compatibility and security USB keyboard/mouse and dual link DVI-I monitor interfaces are used and this...
continued over leaf



ADDERView Secure

USB, dual link DVI-I and audio KVM switch for environments where security must be guaranteed

FEATURES continued...

makes the AdderView Secure truly platform independent.

Superb video performance

Dual link DVI interface operates at full DVI bandwidth to ensure higher end applications that require exact video quality, sometimes at very high video resolutions, are not compromised. DVI interfaces have the added security advantage that randomizing the low order video bit can make snooping much harder.

Additional Features :

- Digital or analogue video
- Simple channel selection
- Tamper evident case seals
- Keyboard and mouse hotkey switching is banned from the design

SUMMARY OF THREATS AND SOLUTIONS

This section provides a list of potential security threats that the AdderView Secure might face during operation and the special steps that have been taken to counteract them.

THREAT	SOLUTION
Microprocessor malfunction or unanticipated software bugs causing data to flow between ports.	Uni-directional data flow is enforced by hardware "data diodes" so data isolation doesn't rely on software integrity.
Subversive snooping by means of detecting electromagnetic radiation emitted from the equipment.	Carefully shielded metal case with dual shielding in critical areas.
Detection of signals on one computer by monitoring for crosstalk (leakage) signals on another computer.	No connections to sensitive analog inputs (such as computer microphone ports) are provided. Minimum crosstalk separation of 60dB provided between signals from one computer and input or I/O signals to another computer.
Malicious modification of microprocessor software causing data to leak between ports.	Data isolation is assured by hardware and so is not compromised by any changes to the microprocessor software. Microprocessors use one time programmable memory so flash upgrades are not possible. Protected by tamper evident seals.

Please refer to the product manual for more information

TECHNICAL SPECIFICATIONS

Hardware compatibility

Supports PC, Sun, Apple, RS/6000, Alpha and SGI-computers with USB keyboard and mouse interfaces and either VGA or DVI video interfaces

Video

Analog: up to 1920 x 1200 x 60Hz
Single link digital: up to 1600 x 1200 x 60Hz
Dual link digital: up to 2560 x 1600 x 60Hz

O/S Compatibility

All known software and operating systems including Windows (all), DOS, Linux, Unix, BSD, Sun OS, Solaris, Mac OS, NetWare etc.

Computer connections

Video: DVI-I, Keyboard/Mouse: USB type B, Audio: 3.5mm stereo jack

KVM console

Video: DVI-I, Keyboard/Mouse: USB type A, Audio: 3.5mm stereo jack

Physical design

234mm / 9.2" (w) x 140mm / 5.5" (d) x 44mm / 1.7" (h) 1.4kgs / 3 lbs.

Power

100 - 240VAC, 50-60Hz, 10W

ORDERING INFORMATION

AV Secure 2 port switch: AVSD1002-XX
AV Secure 4 port switch: AVSD1004-XX

XX = Mains Lead Country Code:
UK = United Kingdom
US = United States
EURO = Europe
AUS = Australia

ADDITIONAL ACCESSORIES

Rack mount kit: RMK3

Operating temperature

0°C to 40°C / 32°F to 104°F

Approvals

CE, FCC

Designed to meet Common Criteria EAL4+ certified (EAL4+ certificate available)

