BLACK BOX NETWORK SERVICES

TEMPEST

Common Criteria

ServSwitch Secure KVM Switches with USB, EAL4+ Certified/TEMPEST Level I

Combat a range of potential data leakage threats with these ultra-secure switches.

- Prevent data from leaking between ports.
- Prevent sensitive data from being stored in the device.
- Prevent electronic snooping.

Combating potential threats

Threat: Microprocessor malfunction or unanticipated software bugs causing data to flow between ports.

Solution: Unidirectional data flow is enforced by hardware "data diodes" so data isolation doesn't rely on software integrity.

Threat: Malicious modification of microprocessor software causing data to leak between ports.

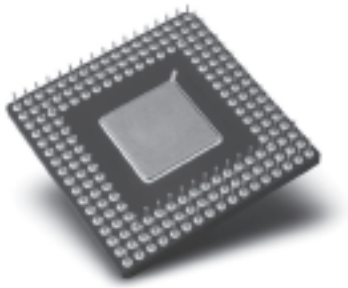
Solution: Microprocessors are one-time programmable and soldered on the board. Data isolation does not rely on software; it is ensured by hardware.

Threat: Subversive snooping by detecting electromagnetic radiation emitted from the equipment.

Solution: Carefully shielded metal case with dual shielding in critical areas. The TEMPEST versions, with their low-emissions profile, meet the appropriate requirements for conducted/radiated electromagnetic emissions.

Threat: Detection of signals on one computer by monitoring for crosstalk (leakage) signals on another computer.

Solution: No connections to sensitive analogue inputs (such as computer microphone ports). Minimum crosstalk separation (80-dB on the VGA models/ 60-dB on the DVI versions) provided between signals from one computer and input or I/O signals to another.



Threat: Timing analysis attacks (looking at what happens on one port to determine data flow patterns on another).

Solution: Only one computer is connected at a time to any shared circuitry. Links are unidirectional, preventing timing analysis.

Threat: Signaling by shorting the power supply or loading the power.

Solution: Each port is independently powered by its USB port. Shorting the power supply on one port will not cause the power on the other ports to be switched off.

Threat: Data transfer by using common storage or common RAM.

Solution: Shared circuitry and the keyboard and mouse are powered down at each switchover to clear all volatile memory of any previous connections.

Threat: Physically tampering with your switches.

Solution: The switches are fitted with holographic, tamper-evident seals to protect against physical tampering.

Highly secure in their overall design and manufacture, as well

KVM switches for VGA video that are Level I (Level A) qualified for low radiated emissions!

The ServSwitch™ Secure KVM Switch with USB, VGA, EAL4+ Certified/TEMPEST Level I (Level A) Qualified models are all TEMPEST USA NSTISSAM Level I and NATO SDIP-27 Level A qualified.

What this means is the low radiated emissions profile of these switches meets the appropriate requirements for conducted/radiated electromagnetic emissions.

The TEMPEST designation is required by military organisations. As a security standard, it pertains to technical security countermeasures, standards, and instrumentation that prevent or minimise the exploitation of vulnerable data communications equipment by technical surveillance or eavesdropping.

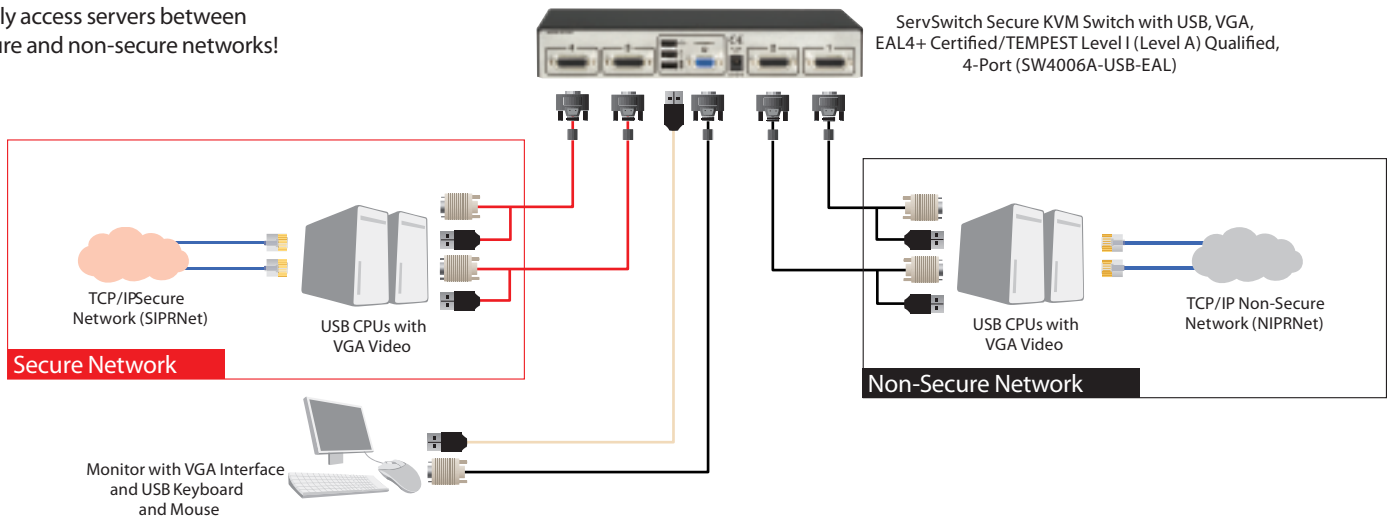
Even better, two of the VGA models support keyboards with integrated Common Access Card (CAC) readers, meeting Homeland Security Presidential Directive 12 (HSPD-12) requirements. The units automatically disable themselves if there's a breach of the physical case.

In addition, the card reader models also support standalone USB (CAC) card readers.

Features

- High port-to-port electrical isolation, which facilitates data separation (RED/BLACK).
- Permanently hard wired, preventing access from one CPU to the others or access from one network to others.
- External tamper-evident seals. Easy to spot attempted tampering!
- 80-dB channel-to-channel crosstalk isolation protects against signal snooping, so software tools and applications cannot be used to access any connected computer from another connected computer.
- Users can safely switch among as many as four computers operating at different classification levels.
- A non-Flash-upgradable ROM for security.
- Offer true DDC video support, which can be disabled for installations requiring the highest security.
- Built with a solid metal case and dual shielding in critical areas.
- Provide robust isolation between networks, so they're ideal for government applications that access classified networks in addition to public networks such as the Internet.
- Hardware-based data isolation ensures unidirectional data flow with hardware data diodes to provide robust security against port-to-port data leakage.

Safely access servers between secure and non-secure networks!



as in their shipment to you!

Access both secure and non-secure networks from a single keyboard, monitor, and mouse station.

These switches provide control and separation of up to four PCs connected to secure and non-secure networks through just one keyboard, monitor, and mouse. Along with the security features already mentioned on the previous page, the switches offer:

Unidirectional flow of keyboard and mouse data

This way, it's not possible for the computer to send data along the keyboard and mouse signaling channels. This advanced design ensures data isolation through hardware and prevents the keyboard and mouse interfaces from becoming covert computer-to-computer signaling channels from software holes or unanticipated bugs.

Enumeration at the keyboard and mouse ports only

Keyboard and mouse devices can only be enumerated at the keyboard and mouse ports. Any other USB peripherals connected to these ports will be inhibited from operating, preventing, for example, a USB thumb drive from uploading or downloading unauthorised data.

USB host controller that erases entire RAM

At each channel switchover, the USB host controller circuit, which controls shared peripherals, erases its entire RAM. This prevents residual data from remaining in the channel after a channel change and being transferred to another computer.

Additional protections against residual data

Every time the channel is changed, shared USB peripherals are powered down, reset, and re-enumerated. This also minimises the possibility of residual data transfer. What's more, every time the channel is changed, the USB host controller is powered down and reset, further ensuring no transfer of residual data.

Dedicated DDC bus and EDID memory emulation at each port

This prevents the shared monitor link from being used as a covert attack channel. EDID data is collected once from the monitor when the switch is turned on and transferred unidirectionally once to each of the ports. Because each of the ports has its own copy of the EDID, one computer can't transfer information to another via the DDC bus and EDID.

Clear, unmistakable channel selection

With only one selection button per channel, the switches enable direct and unambiguous channel selection. Colour-coded visual feedback confirms the channel selection.

No common power supply

Ports are powered through the computer's USB ports, while the shared keyboard, mouse, and monitor are powered by the switch's power supply. The lack of a common power supply minimises electronic signaling.

No microphone connection

Microphone circuitry within a computer enables sensitive recording of small analog signals. Even very low crosstalk levels could be "recorded" and act as a means by which a non-selected computer could read data being sent to another computer.

EAL4+: secure from design to distribution.

All the ServSwitch Secure KVM Switches with USB featured in this document have been certified for Common Criteria Evaluation Assurance to Level 4+ (EAL4+), augmented by ALC_FLR.2 and ATE_DPT.2.

What exactly does "Common Criteria" mean? It's an international standardised process for information technology security evaluation, validation, and certification. The Common Criteria scheme is supported by the National Security Agency through the National Information Assurance Program (P).

EAL4+ itself defines a common set of tests to evaluate the security of an IT product relating to its supply chain, from design and engineering to manufacturing to distribution.

This evaluation tests the process of the design, testing, verification, and shipping of new security products. Customers, in turn, can have a level of trust in how a product has been designed, tested, built, and shipped.

No possible remote switching control

Hotkey and mouse switching are excluded, preventing remote control of the switch.

Availability of authentication certificate

For added security, users can request an authentication certificate; when requested, it is sent separately from the switch. With it, users verify the firmware status of the KVM switch to ensure it has not been compromised.

In addition, the VGA card reader versions include active authentication verification to enable the user to check the status of internal tamper detection circuits and to verify the authentication of the switch. Also, active tamper detection permanently inhibits normal switch operation. If tampering is detected, subsequent authentication attempts will fail.

Item	Code
ServSwitch Secure KVM Switches with USB, VGA, EAL4+ Certified/TEMPEST Level I (Level A) Qualified	
2-Port	SW2006A-USB-EAL
4-Port	SW4006A-USB-EAL
2-Port with Card Reader	SW2009A-USB-EAL
4-Port with Card Reader	SW4009A-USB-EAL
ServSwitch Secure KVM Switch Cables for VGA	
VGA and PS/2 * to HD26, 6-ft. (1.8-m)	EHNSECURE1-0006
VGA and USB to HD26, 6-ft. (1.8-m)	EHNSECURE2-0006
VGA, USB, and CAC USB to HD26, 6-ft. (1.8-m)	EHNSECURE3-0006
VGA Monitor, 6-ft. (1.8-m)	EHNSECURE4-0006
NOTE: VGA cables also available in 12-ft. (3.7-m) lengths.	
Or order an EAL4+ certified version for DVI video…	
ServSwitch Secure KVM Switches with USB, DVI, EAL4+ Certified	
2-Port	SW2008A-USB-EAL
4-Port	SW4008A-USB-EAL
ServSwitch Secure KVM Switch Cables for DVI	
DVI and USB to DVI and USB, 6-ft. (1.8-m)	EHN900024U-0006
10-ft. (3.0-m)	EHN900024U-0010