BLACK BOX NETWORK SERVICES

TEMPEST

Common Criteria

## ServSwitch Secure KVM Switch with USB

# Combat a range of potential data leakage threats with the ServSwitch Secure.

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

# TEMPEST-Secure KVM Switches

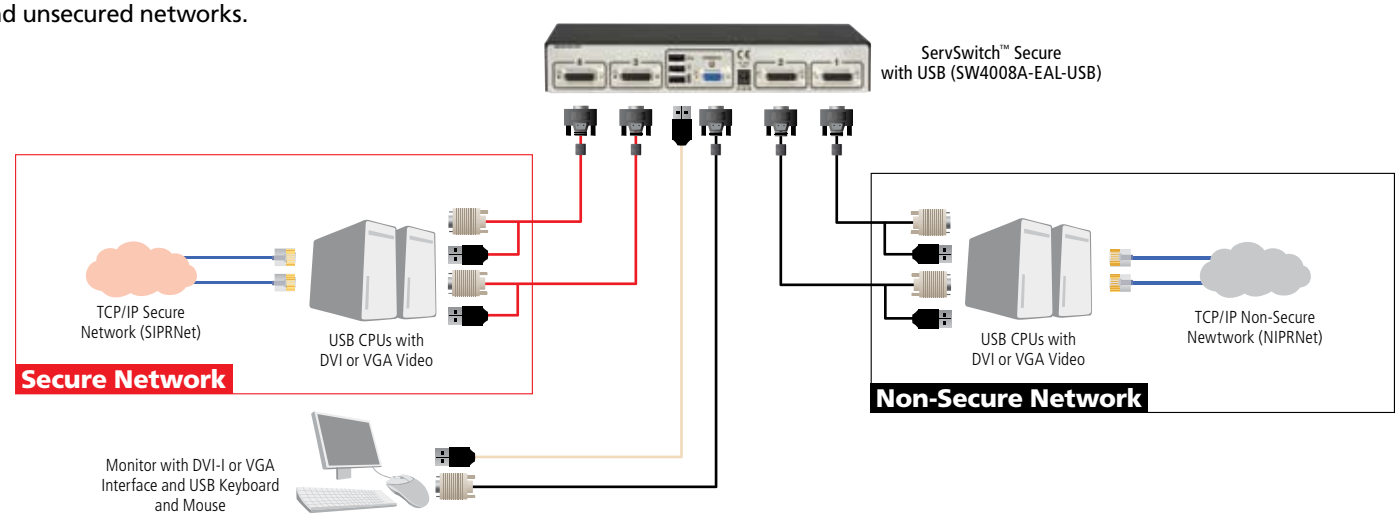
## For 2 or 4 ports, with USB, and DVI-I or VGA

The ServSwitch Secure KVM Switch with USB provides control and separation of up to four PCs connected to secure and unsecure networks through just one keyboard, monitor, and mouse.

## Features

- High port-to-port electrical isolation, which facilitates data separation (RED/BLACK).
- The low radiated emissions profile meets the appropriate national requirements for conducted/radiated electromagnetic emissions.
- Switches are permanently hard wired, preventing access from one CPU to the others or access from one network to others.
- External tamper-evident seals make it easy to spot attempted tampering.
- Channel-to-channel >60-dB 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.
- The switches feature a non-Flash-upgradable ROM for security.
- Support DVI-I video, which is DC balanced and may be encoded for security.
- DVI-I video provides exact video quality and also passes analog VGA signals.
- Offer true DDC video support, which can be disabled for installations requiring the highest security.
- Constructed with a solid metal case and a long-wearing switching mechanism.
- 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.

Safely access servers between secured and unsecured networks.



# Advanced Security Features

A newly developed switch, the ServSwitch Secure with USB and EAL4+, is being evaluated for Common Criteria Evaluation Assurance to Level 4+ (EAL4+). Common Criteria is an international standardized 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 (NIAP).

The ServSwitch Secure with USB surpasses the security profiles of most other KVM switches. Along with the tamper-evident seals and other security features already mentioned, ServSwitch Secure KVM Switch with USB models have:

- Unidirectional flow of keyboard and mouse data, so 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.
- 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 unauthorized data.
- 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.
- Every time the channel is changed, shared USB peripherals are powered down, reset, and re-enumerated. This also minimizes the possibility of residual data transfer.
- 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 prevent 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. Since 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.
- With only one selection button per channel, the ServSwitch Secure models enable direct and unambiguous channel selection. Color-coded visual feedback confirms the channel selection.
- Hotkey and mouse switching are excluded, preventing remote control of the switch.
- 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 minimizes electronic signaling.
- The switch has 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.
- 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.

ServSwitch Secure KVM Switch with USB models have a number of port-isolation and channel power features that prevent residual data transfer.

The switches with card readers have additional features, including:

- Active authentication verification to enable the user to check the status of internal tamper detection circuits and to verify the authentication of the switch.
- Active tamper detection permanently inhibits normal switch operation if tampering is detected; subsequent authentication attempts will fail.

## Applicable Tests

**Common Criteria (EAL4+)**

Common Criteria (EAL4+) defines a common set of tests to evaluate the security of an IT product. The evaluation tests the process of the design, testing, verification, and shipping of new security products. EAL4+ specifies basic functional requirements but not TEMPEST tests. Common Criteria enables customers to assess a level of trust in how a product has been designed, tested, built, and shipped.

**TEMPEST Testing**

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

| Item | Code |
|---|---|
| ServSwitch Secure KVM Switch with USB, in CC Evaluation (EAL4+) | |
| DVI, 2-Port | **SW2008A-USB-EAL** |
| DVI, 4-Port | **SW4008A-USB-EAL** |
| ServSwitch Secure KVM Switch with USB, TEMPEST-approved, in CC Evaluation (EAL4+) | |
| VGA, 2-Port | **SW2006A-USB-EAL** |
| VGA, 4-Port | **SW4006A-USB-EAL** |
| VGA, 2-Port, with Card Reader | **SW2009A-USB-EAL** |
| VGA, 4-Port, with Card Reader | **SW4009A-USB-EAL** |
| ServSwitch Secure KVM Switch with USB, TEMPEST*-approved | |
| DVI and VGA, 2-Port | **SW2007A-USB** |
| DVI and VGA, 4-Port | **SW4007A-USB** |

**NOTE: NSA tested and TEMPEST approved for and by the U.S. Air Force.*

# 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.

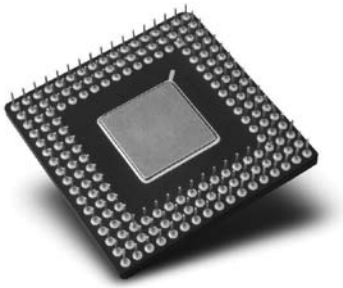
**Solution:** Carefully shielded metal case with dual shielding in critical areas and a low emissions profile.

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

**Solution:** No connections to sensitive analog inputs (such as computer microphone ports). Minimum crosstalk separation of 60 dB 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 the switch.

**Solution:** The switch is designed with tamperproof seals to be fitted over the countersunk screws.

## About Black Box

Black Box is the world's largest technical services company dedicated to designing, building, and maintaining today's complicated data and voice infrastructure systems. Black Box services 175,000 clients in 141 countries with 194 offices throughout the world. In addition, Black Box provides more than 118,000 products via its award-winning catalog and Web site. To learn more, visit the Black Box Web site at http://www.blackbox.com.