BLACK B⬧X®

Secure KVM Switches
Solutions Brochure

Combat the Variety of Security Threats that Arise when Sharing Peripherals between Computer Networks with Different Security Levels

Why Secure KVM

Cyberthreats are constantly evolving, becoming more frequent and sophisticated every day. Our reliance on technology, sharing of global resources, and need for real-time collaboration have led to a growing web of data. While interconnectivity helps us work together more efficiently and effectively, it also leaves us increasingly vulnerable to devastating cyberattacks.

Major defense agencies and other organizations alike use advanced security measures to isolate networks and safeguard information from outside threats. However, there is one place where isolated networks and sensitive information come together: the user desktop.

Unsecure KVM switches are susceptible to cyberattacks and can allow cybercriminals to access classified data. If a cybercriminal wants to steal information from a classified server, they can attach a USB drive with malware of a virus on it into an unsecure KVM switch to access multiple servers instead of just one. Unsecure KVM switches are also susceptible to malicious use of LCD monitors (via EDID signal), microphones, or or CAC devices.

Through these methods, a wealth of classified information can get into the wrong hands and be used to harm the organization.

Traditional KVM Switches

KVM switches allow access and management of multiple computers from a single workstation with a keyboard, mouse, and video monitor. Users can easily access information and applications on completely separate systems by pushing a button or using keystrokes.

KVM technology provides monitoring solutions for automation, processes, and workflow. It gives users improved operability and a quick return on investment due to better workplace ergonomics and productivity. KVM switches enable users to save space by reducing interface devices, save costs by eliminating redundant peripherals, and react faster in critical situations.

LEARN MORE BLACKBOX.COM/SECUREKVM
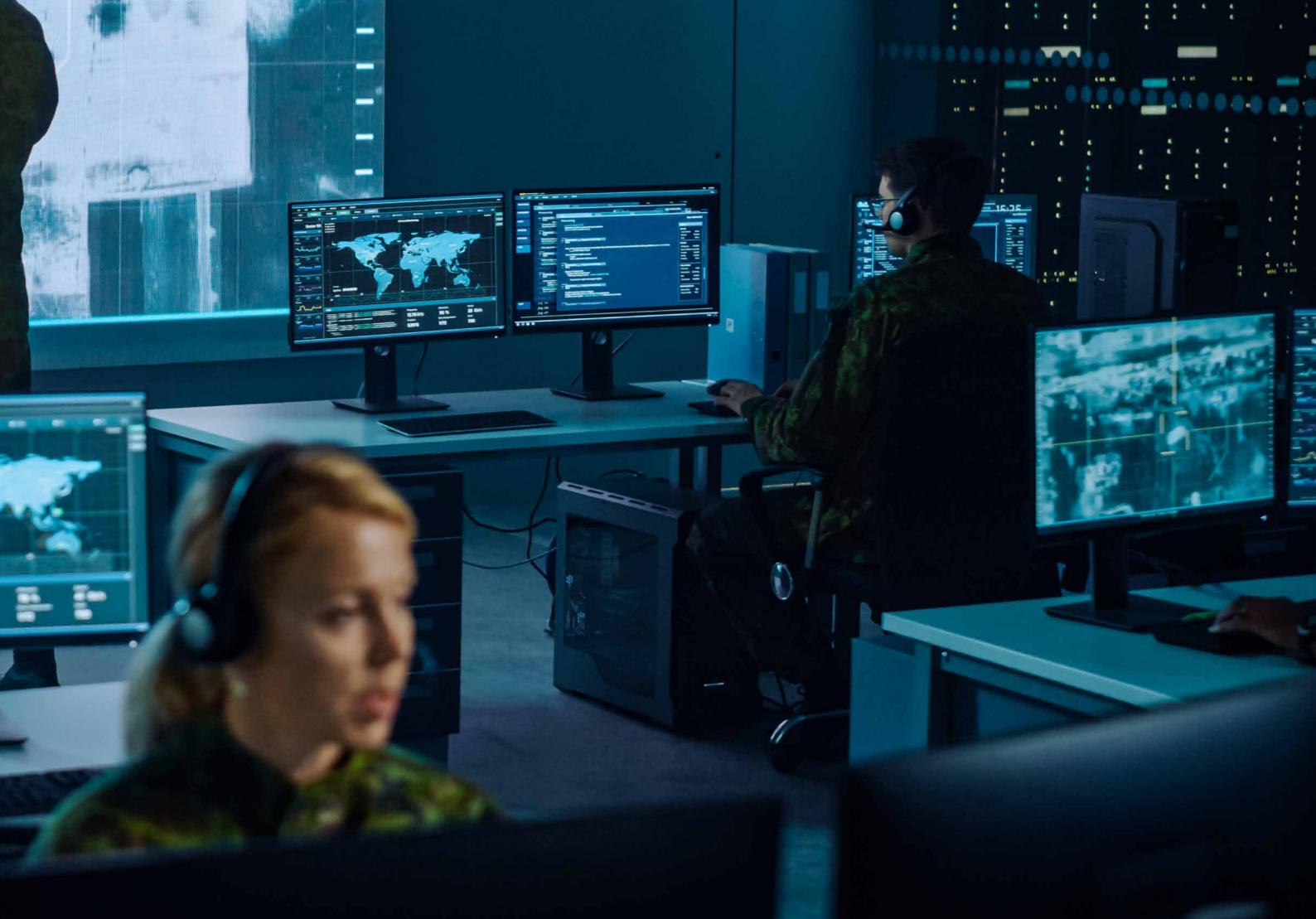
Secure KVM Switches keep sensitive data classified

A secure KVM switch is a 2-, 4-, or 8-port desktop switch that provides control and separation of PCs connected to networks of differing security classifications. Unlike traditional KVM switches, secure KVM switches can only be controlled using push button control. Hotkey commands are disabled, which ensures only the right users have access.

Secure KVM switches won't allow a USB drive that isn't recognized to access any information. It allows administrators to choose which USB devices are authorized or recognized. Secure KVM switches do much, much more to protect Government agencies from today's most terrifying cyberthreats.

NIAP Protection Profile for Secure KVM

Until recently, the National Information Assurance Partnership (NIAP) used Common Criteria Evaluation & Validation Scheme (CCEVS) to evaluate and approve KVM switches for security.

NIAP has implemented the Common Criteria Recognition Arrangement (CCRA) Management Committee Vision Statement for the application of the Common Criteria and no longer evaluates against Evaluation Assurance Levels (EAL). This strengthens evaluations by focusing on technology-specific security requirements.

As a result, they upgraded the Protection Profile (PP) for peripheral sharing switches to PP 4.0 NIAP Protection Profile for Peripheral Sharing Switch Version 4.0, which are tests regarding the process of the design, testing, verification, and shipping of security products. This protection profile is an international, standardized process for information technology security evaluation, validation, and certification.

How Secure KVM Switches Combat Cyberattacks

Rigid Security Features inside Black Box Secure KVM Switches

- Mechanical, electrical and optical signal isolation prevent hacking and data leakage –> absolute isolation / no data leakage between secure ports and the outside world

- Protected firmware keeps intruders from reprogramming or reading firmware (non-reprogrammable ROM)

- Opto-Isolated USB ports and keyboard/internal cache wiping keep USB data paths electrically isolated from each other to prevent USB data leakage between ports

- Secure EDID/video & aux emulation restricts discovery of newly-connected displays during switching operations which prevents unwanted and unsecured data from getting transmitted between the computers and the display

- Chassis intrusion protection: equipped with active anti-tamper switches and external hologram tamper-evident seals

- Optional configurable Common Access Card (CAC) support for smart cards, biometric readers, and registration of external USB devices

- Unidirectional data flow to special peripherals like a projector, printer, or audio system

- Certified to NIAP PP 4.0, the highest Common Criteria level (Protection Profile for Peripheral Sharing Switch Version 4.0)

- TAA compliant and made in USA

- Audio in is permitted but only if no other peripheral types are supported by the switch (microphone cannot coexist with speakers)

Tested and certified to the latest NIAP PP 4.0 security profile

Secure KVM switches from Black Box are designed for use in secure defense and intelligence applications where sensitive data must be protected. The secure KVM switches from Black Box are NIAP PP 4.0 certified and equipped with the highest security features that meet today's information assurance safe control standards. The switches contain unique hardware configurations that prevent data leakage between PCs and connected peripherals that eliminate any potential cyberthreat. NIAP PP 4.0 applies a base-protection profile with individual modules for peripheral types.

Multi-level security for strict information assurance

An absolute isolation of the mechanical, electrical, and optical signals through air gapping prevents hacking and data leakage between the ports and the outside world. Each port of the secure KVM switch uses its own isolated data channels. By upfront switching on another target computer, the KVM switch erases the internal cache and keyboard data to ensure that no residual data remains in the channel. The fixed, secure firmware and ROM are non-reprogrammable and keep intruders from reading, reprogramming via unwanted firmware upgrades, or physically removing sensitive data.

Chassis intrusion protection

The secure KVM switches feature active, anti-tamper switches; external hologram, tamper-evident seals; and a long-life, internal, anti-tampering battery. If the cover is removed from the chassis, the KVM switch shuts down connection with all attached PCs and peripherals and disables any functionality to protect against any attempt of physical intrusion. Tamper response is optional in V4.0 (it is mandatory in V3.0), because some devices may have swappable cards for different peripheral types (in which case tamper seals are sufficient). V3.0 prohibits audio in (microphone) capability, while V4.0 permits audio in (but only if the device does not support any other peripheral types, for example, a microphone cannot coexist with speakers).

Keyboard & Mouse emulation

The secure KVM switch emulates the presence of a keyboard and mouse for every attached computer through a USB cable. Both selected and non-selected computers maintain a constant connection with the switch's keyboard mouse emulation controllers, allowing for ultra-fast switching and restricting discovery of newly connected peripherals during switching operations. Emulation of keyboard and mouse also prevents direct connection between the peripherals and the connected computers, shielding systems from potential vulnerabilities. PS/2 ports are allowed in V3.0 and are banned in V4.0.

Fully configurable Common Access Card (CAC) port for external USB peripherals

Many secure KVM switches support CAC (Common Access Card) devices, such as smart-card and biometric readers, bolstering security when using the device. However, Black Box takes CAC security even further, allowing authenticated administrators to register and assign specific peripheral devices to the CAC port (optional). Users can then switch the connection between the assigned device along with the KVM switching of the connected computers.

Restricts new monitor connections during switching

The secure KVM switches simulate a generic EDID as default, allowing them to operate most of the connected monitors. Selected and non-selected computers maintain constant connection with the switch's video and AUX emulation controllers, allowing for ultra-fast switching and restricting discovery of newly connected monitors during switching operations. This shields systems from potential vulnerabilities through unwanted and unsecure data transmittance through DDC lines. V.4.0 allows the use of multiviewers (however, they must use OSD to identify the active video channel[s]).

Use Cases

Ideal for Multiple Industries

Government

Defense & Military

Control Rooms for Traffic Management

Banking and Finance
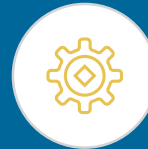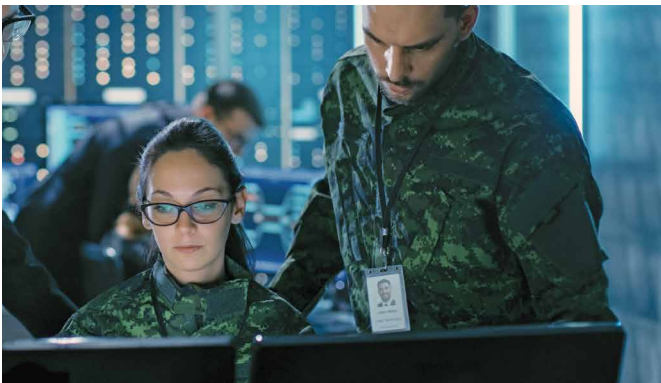
Education

Healthcare

R&D Departments

Utilities

Use Cases

Defense Communications Center

A defense customer came to Black Box with two pressing issues: inefficient network access and a cluttered workspace.

Their operators needed to access multiple computer networks in secure communications centers. It was a time-consuming process because each computer network required a separate keyboard, monitor, and mouse, which meant the operator had to move between the different systems to access sensitive data and intelligence networks. This also required a table for all six different monitors, six different keyboards, and six different mice, which made for a cluttered and cramped workspace.

To overcome these challenges, they purchased an 8-Port Secure KVM Switch from Black Box that reduced their configuration to one monitor, one keyboard, and one mouse, saving valuable time for operators having to switch between multiple networks and opening up a wealth of desk and office space. Now they operate more efficiently in a clean workspace while ensuring their vital data has no way of being compromised.

Police

A company contacted Black Box when they required a highly secure solution for a police project. Project engineers needed to switch between on open (green) and a secure (red) network. Black Box suggested the 4-port DVI USB Secure KVM Switch, which perfectly suits all their requirements. More than 1.000 secure KVM switches have already been installed.
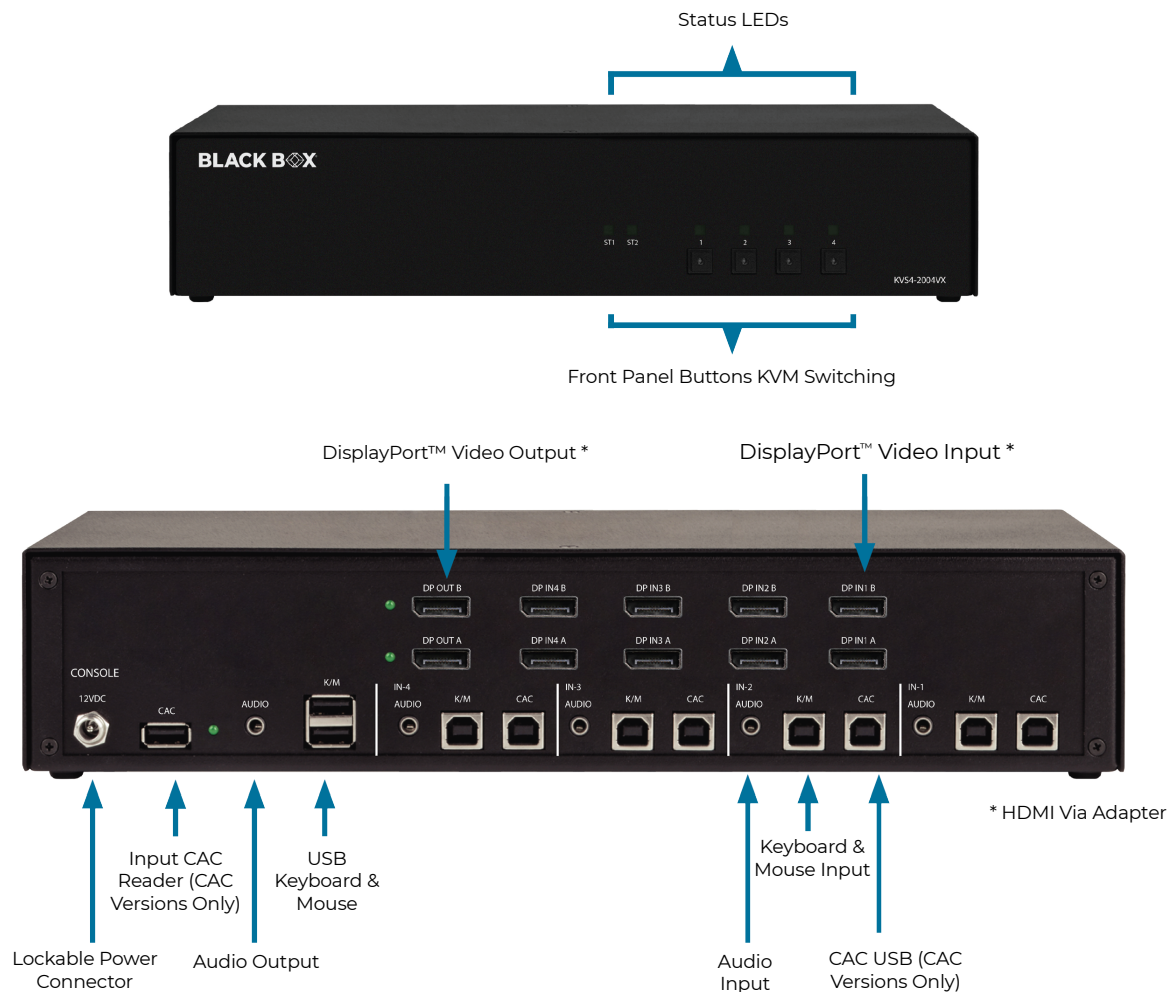
Enterprise

Sharing of global resources, and need for real-time collaboration have led to a growing web of data. While interconnectivity helps organizations work together more efficiently and effectively, it also leaves them increasingly vulnerable to devastating cyberattacks. Ultimately systems that access the Internet need to be kept away from other systems which are used for sensitive corporate or personal data. To maintain their information assurance, many organizations are replacing standard KVM switches with secure KVM switches.

# Secure KVM Product Overview

Secure KVM Switch Design

Example 4-Port Secure KVM Switch, single user, DisplayPort, USB, and CAC KVS4-2004VX

Status LEDs

Front Panel Buttons KVM Switching

DisplayPort™ Video Output *

DisplayPort™ Video Input *

* HDMI Via Adapter

Input CAC Reader (CAC Versions Only)

USB Keyboard & Mouse

Keyboard & Mouse Input

Lockable Power Connector

Audio Output

Audio Input

CAC USB (CAC Versions Only)

Secure NIAP 4.0 Certified Desktop KVM Switch Types

Secure Desktop KVM Switches, Single User

- Share a single user console between two, four, or eight computers

- Available with DVI-I, DisplayPort, or HDMI/DisplayPort video

- High-quality DisplayPort 1.2/HDMI video with resolutions up to 4K@60Hz and best DVI-I dual-link resolution up to 2560x1600 @ 60Hz

- Choose from models with single-, dual-, or quad-monitor connections to the console

- USB keyboard/mouse plus stereo audio

- Available with or without CAC support

- Made, Tested, and Certified in the USA

Find the Right Product in the Selector on Pages 10 & 11.

LEARN MORE **BLACKBOX.COM/SECUREKVM**
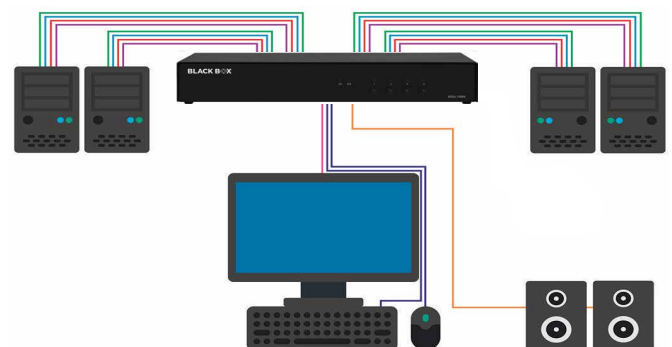
Secure KVM Controllers

Secure KVM Pushbutton Controller

- Switch between classified, top secret, and open networks, keeping the NIAP4-certified KVM switch off the desk

- Controls 2 and 4 port Secure KVM Switches using only a single USB cable

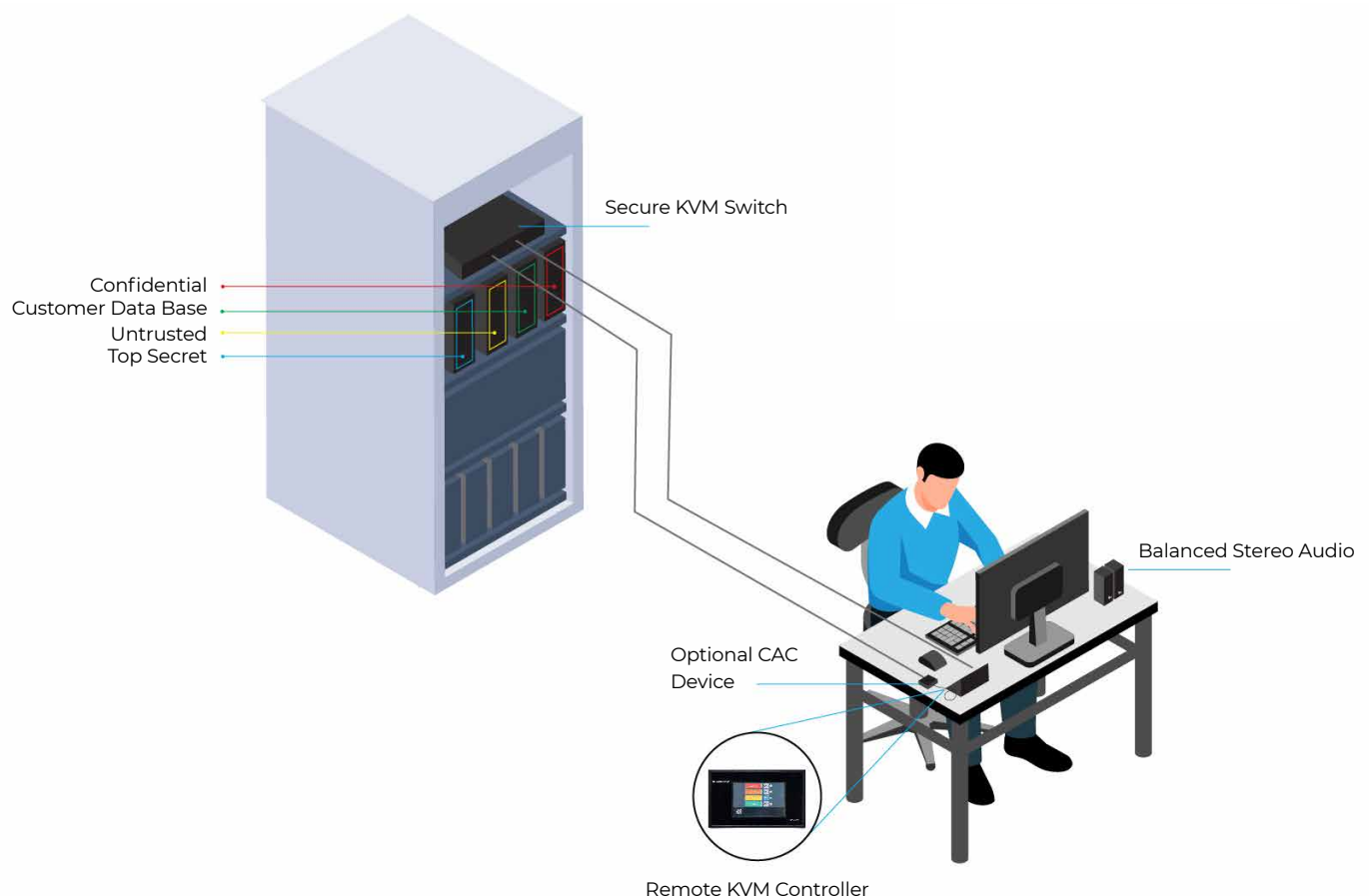- Supports switching of CAC up to 9m away from the switch

Secure KVM Pushbutton Conroller KVSC-4

Secure KVM Touchscreen Controller

- Automatically detects up to 16 ports

- Color LCD Touchscreen display with backlight ensures a crystal-clear view of your connections

- Supports switching of keyboard and mouse up to 15 meters (50 ft) away from switch

- Futureproof: This single-USB cable solution supports your system now, and later when it grows

Secure KVM Touchscreen Conroller KVSC-16

Secure KVM Switch

Confidential
Customer Data Base
Untrusted
Top Secret

Balanced Stereo Audio

Optional CAC Device

Remote KVM Controller

Secure NIAP 4.0 Certified KM Switches

- Switch by moving your mouse from monitor to monitor (Glide & Switch)

- View multiple sources concurrently through dedicated computer/monitor connections

- Stereo audio support

- Share a single user console with USB keyboard and mouse between four or eight computers

- Stereo audio support

- Available with or without CAC support

- Made, Tested, and Certified in the USA

LEARN MORE **BLACKBOX.COM/SECUREKVM**
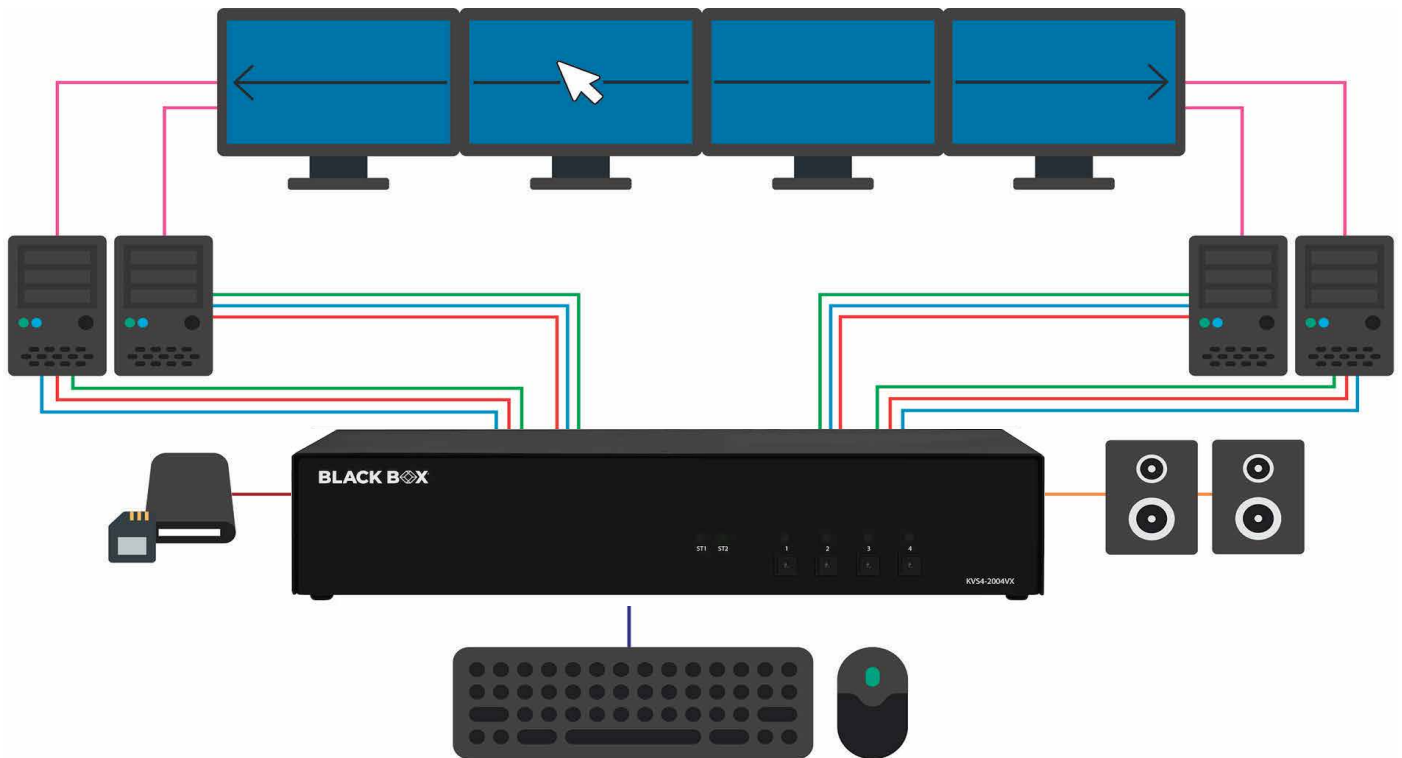
Secure NIAP 4.0 Certified KVM Switch - FlexPort HDMI/DisplayPort

- Secure Keyboard, Video, and Mouse operation on up to two or four computers with one or two HDMI/DisplayPort monitors using FlexPort technology

- Certified for NIAP Protection Profile for Peripheral Sharing Device Version 4.0

- Supports resolutions up to 4K@60Hz

- Made, tested, and certified in the USA

- External power supply
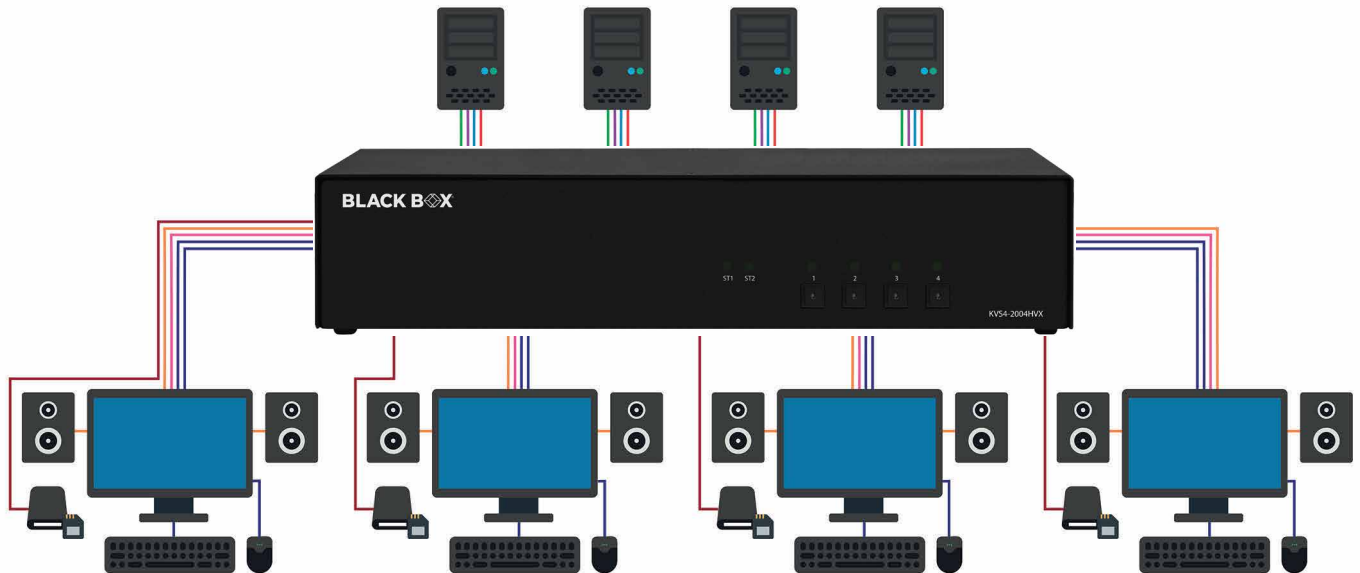
Find the right product in the selector on Pages 10 & 11. 10

Secure KVM Peripheral Defender, NIAP 4.0 Certified - CAC

- Isolates one computer from the DVI-I, HDMI, or DisplayPort monitor, keyboard, mouse, and CAC to ensure safety and security.

- Certified for NIAP Protection Profile for Peripheral Sharing Device Version 4.0

- Single-Monitor video interface

- Keeps unsecured peripherals protected

- Tested and certified under the USA scheme

- External power supply

- Ensures unidirectional data flow of video, USB, and audio from the computer to the peripheral

- Supports most monitors through Secure EDID Learning/ Emulation

- Ideal for conference room to protect laptops from intrusions through the shared display connection
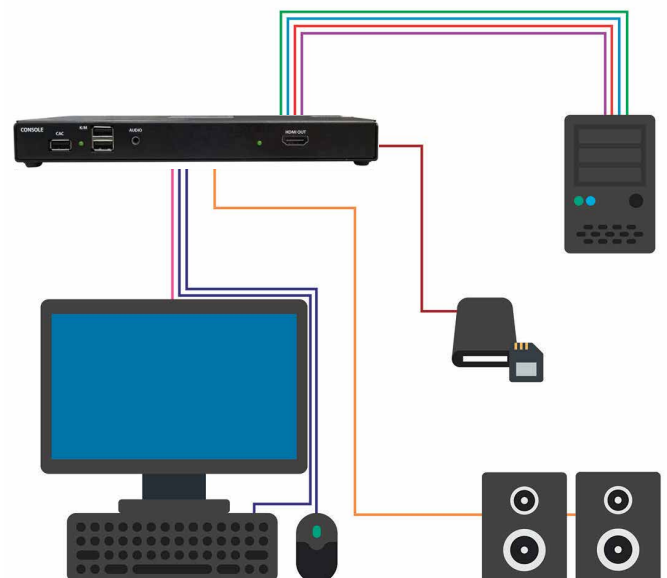
Find the right product in the selector on Pages 10 & 11.

NIAP 4.0 PRODUCT SOLUTIONS

SECURE KVM SWITCH, NIAP 4.0 CERTIFIED, DISPLAYPORT

ITEM #	KVS4-1004V	KVS4-2002V	KVS4-2004V	KVS4-2004VX	KVS4-2008VX
Description	2-Port, Single-Monitor, DisplayPort	2-Port, Dual-Monitor, DisplayPort	4-Port, Dual-Monitor, DisplayPort	4-Port, Dual-Monitor, DisplayPort, CAC	8-Port, Dual-Monitor, DisplayPort, CAC
No. of Sources	2	2	4	4	8
Computer Compatibility	Windows®, Mac®, and Linux® OS				
Max. Resolution	Up to 4K@60Hz				
Monitor Compatibility	Most Monitors through Secure EDID Learning and Emulation				
PORTS TO USER CONSOLE					
Monitor Connection(s)	(1) DisplayPort	(2) DisplayPort	(2) DisplayPort	(2) DisplayPort	(2) DisplayPort
Keyboard/Mouse Connections	(2) USB 2.0 Type A, Keyboard and Mouse Only				
Audio Output	(1) 3.5-mm Audio Jack with Balanced Speaker Outputs and Switching				
CAC Support	No	No	No	(1) USB Type A, Fully Configurable	(1) USB Type A, Fully Configurable
PORTS TO COMPUTERS					
Monitor Connection(s)	(1) DisplayPort per Source	(2) DisplayPort per Source	(2) DisplayPort per Source	(2) DisplayPort per Source	(2) DisplayPort per Source
Keyboard/Mouse Connections	(1) USB 2.0 Type B with USB Emulation per Source				
Audio Output	(1) 3.5-mm Audio Jack per Source				
CAC Support	No	No	No	(1) USB Type B per Source	(1) USB Type B per Source

SECURE KVM SWITCH, NIAP 4.0 CERTIFIED, DVI-D

ITEM #	KVS4-1002D	KVS4-1004D	KVS4-2002D	KVS4-2004D	KVS4-2008D
Description	4-Port, Single-Monitor, DVI-D	4-Port, Single-Monitor, DVI-D	2-Port, Dual-Monitor, DVI-D	4-Port, Dual-Monitor, DVI-D	8-Port, Dual-Monitor, DVI-D
No. of Sources	4	4	2	4	8
Computer Compatibility	Windows®, Mac®, and Linux® OS				
Max. Resolution	2560 x 1600 at 60 Hz				
Monitor Compatibility	Most Monitors through Secure EDID Learning and Emulation				
PORTS TO USER CONSOLE					
Monitor Connection(s)	(1) DVI-D	(1) DVI-D	(2) DVI-D	(2) DVI-D	(2) DVI-D
Keyboard/Mouse Connections	(2) USB 2.0 Type A, Keyboard and Mouse Only				
Audio Output	(1) 3.5-mm Audio Jack with Balanced Speaker Outputs and Switching				
CAC Support	No	No	No	No	No
PORTS TO COMPUTERS					
Video Input(s)	(1) DVI-D per Source	(1) DVI-D per Source	(2) DVI-D per Source	(2) DVI-D per Source	(2) DVI-D per Source
Keyboard/Mouse Inputs	(1) USB 2.0 Type B with USB Emulation per Source				
Audio Output	(1) 3.5-mm Audio Jack per Source				
CAC Support	No	No	No	No	No

SECURE KVM SWITCH, NIAP 4.0 CERTIFIED, FLEXPORT HDMI/DISPLAYPORT

Item #	KVS4-1004HV	KVS4-2002HV	KVS4-2004HV	KVS4-2004HVX
Description	4-Port, Single-Monitor, FlexPort HDMI/DisplayPort	2-Port, Dual-Monitor, FlexPort HDMI/DisplayPort	4-Port, Dual-Monitor, FlexPort HDMI/DisplayPort	4-Port, Dual-Monitor, FlexPort HDMI/DisplayPort, CAC
No. of Sources	4	2	4	4
Computer Compatibility	Windows®, Mac®, and Linux® OS			
Max. Resolution	Up to 4K@60Hz			
Monitor Compatibility	Most Monitors through Secure EDID Learning and Emulation			
PORTS TO USER CONSOLE				
Monitor Connection(s)	(1) HDMI/DisplayPort FlexPorts	(2) HDMI/DisplayPort FlexPorts	(2) HDMI/DisplayPort FlexPorts	(2) HDMI/DisplayPort FlexPorts
Keyboard/Mouse Connections	(2) USB 2.0 Type A, Keyboard and Mouse Only			
Audio Output	(1) 3.5-mm Audio Jack with Balanced Speaker Outputs and Switching			
CAC Support	No	No	No	(1) USB Type A, Fully Configurable
PORTS TO COMPUTERS				
Video Input(s)	(1) HDMI/DisplayPort FlexPorts per Source	(2) HDMI/DisplayPort FlexPorts per Source	(2) HDMI/DisplayPort FlexPorts per Source	(2) HDMI/DisplayPort FlexPorts per Source
Keyboard/Mouse Inputs	(1) USB 2.0 Type B with USB Emulation per Source			
Audio Output	(1) 3.5-mm Audio Jack per Source			
CAC Support	No	No	No	(1) USB Type B per Source

SECURE KVM PERIPHERAL DEFENDER, NIAP 4.0 CERTIFIED - CAC

Item #	KVS4-8001DX	KVS4-8001HX	KVS4-8001VX
Description	DVI-D, CAC	HDMI, CAC	DisplayPort, CAC
Computer Compatibility	Windows®, Mac®, and Linux® OS		
Max. Resolution	2560 x 1600 @ 60Hz (DVI-D) Up to 4K@60Hz (HDMI and DisplayPort models)		
Monitor Compatibility	Most Monitors through Secure EDID Learning and Emulation		
PORTS TO USER CONSOLE			
Monitor Connection(s)	(1) DVI-D 23-pin (female)	(1) HDMI 1.4	(1) DisplayPort
Keyboard/Mouse Connections	(2) USB Type-A for keyboard and mouse connection only (1) USB Type-A for CAC connection	(2) USB Type-A for keyboard and mouse connection only (1) USB Type-A for CAC connection	(2) USB Type-A for keyboard and mouse connection only (1) USB Type-A for CAC connection
Audio Output	(1) Connector Stereo 3.5-mm Female	(1) Connector Stereo 3.5-mm Female	(1) Connector Stereo 3.5-mm Female
CAC Support	(1) USB Type A, Fully Configurable	(1) USB Type A, Fully Configurable	(1) USB Type A, Fully Configurable
PORTS TO COMPUTERS			
Video Input	(1) DVI-D 23-pin (female)	(1) HDMI 1.4	(1) DisplayPort
Keyboard/Mouse Inputs	(1) USB Type-B	(1) USB Type-B	(1) USB Type-B
Audio Output	(1) Connector Stereo 3.5-mm Female	(1) Connector Stereo 3.5-mm Female	(1) Connector Stereo 3.5-mm Female
CAC Support	(1) USB Type B	(1) USB Type B	(1) USB Type B

BLACK BOX®

Why Black Box?

Expertise

Black Box project engineers can assist with system assessment, design, deployment, and training.

Breadth

Black Box offers the most comprehensive suite of engineered KVM solutions in the industry.

Support

Reflecting our commitment to complete satisfaction, our dedicated team of highly trained support technicians is available by phone free of charge, every day of the year.

Warranties

Secure KVM Switches come with a 3-Year warranty and extension options are available.

Experience

Providing leading technology solutions since 1976, Black Box helps more than 175,000 customers in 150 countries build, manage, optimize, and secure IT infrastructures.

Center of Excellence

Black Box offers a Center of Excellence featuring professional services and support agreements that help optimize customers' systems and maximize uptime.

Service Level Agreements

Our Service Level Agreements give customers access to technical support, product training, dedicated application engineers, and more.

EN_KVM_Brochure_Secure KVM NIAP 4_2412

LEARN MORE   BLACKBOX.COM/SECUREKVM