BELKIN®

Implementing KVM Switching in Secure, Mission-Critical Environments

GSA

Common Criteria

BELKIN

Addressing the Government's Secure KVM Switching Challenge

Throughout the military, intelligence, and other government industries, multiple computer environments, often spread across various levels of classifications, are commonplace.

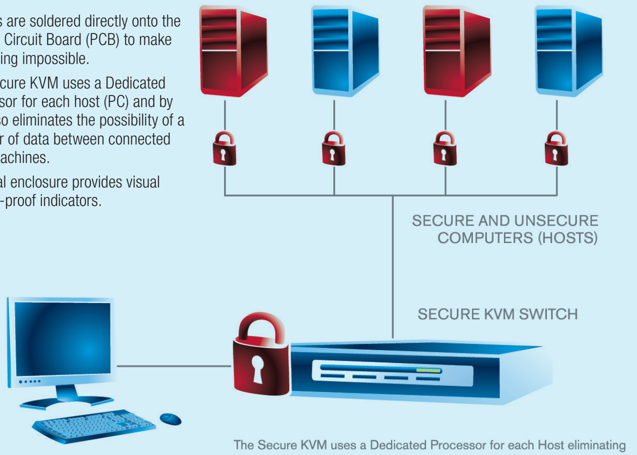
Security requirements throughout secure military and intelligence organizations have prompted the development of multiple classifications of data, generally separated into distinct silos of information. In these environments, many end users are forced to operate multiple computers and associated peripherals at their workspace.

Maintaining separate networks and computing hardware effectively ensures that data from distinct networks cannot be combined or transferred amongst multiple pieces of hardware. To reduce costs and clutter at the workspace, this situation creates a need for efficient keyboard, video, and mouse (KVM) switching. KVM switches provide an immediate hardware cost savings by eliminating the need for separate keyboards, video monitors, and mice. These devices also free up valuable desk space and reduce an organization's power and cooling expense.

Traditional KVM switching products are not designed to operate amongst multiple levels of security classification and do not effectively isolate data across these distinct networks. In the absence of secure KVM products, designed and certified to address this issue, users previously were forced to use a separate keyboard, monitor, and mouse to access data from separated computer systems, crowding desktops with excess computer equipment. Using a secure KVM switch, users can utilize a single keyboard, monitor, and mouse, saving valuable "real estate" and hardware costs. Additionally, shifting between multiple computers at different security levels was previously considered an unprotected vulnerability that was also considered operationally inefficient.

Secure KVM Switching

- Circuits are soldered directly onto the Printed Circuit Board (PCB) to make tampering impossible.
- The Secure KVM uses a Dedicated Processor for each host (PC) and by doing so eliminates the possibility of a transfer of data between connected Host Machines.
- External enclosure provides visual tamper-proof indicators.



The Secure KVM uses a Dedicated Processor for each Host eliminating the possibility of data transfer between connected Host Machines.

Secure KVM switches combine computer monitor, keyboard, and mouse signals so government users can share peripherals while efficiently switching securely between separate systems and networks. Secure KVM solutions allow users to switch safely between computers operating at different security levels from a single switch, providing continuous access to critical data. Customers in military and intelligence agencies want to be assured that any secure KVM solution has the features in place to ensure that data from public, unsecured networks is isolated from networks that are used exclusively for secure networks, and vice versa.

Common Criteria EAL 4 NIAP Certification

National Information Assurance Partnership (NIAP) is a collaboration of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) that oversees the government's information technology security standards, often referred to as Common Criteria, and tests products to certify them for use in highly secured government environments.

The Common Criteria Evaluation and Validation Scheme (CCEVS) has become widely accepted by IT suppliers and agency consumers as the flagship program used to meet security testing, evaluation, and assessment requirements for IT products.

TAA Compliance

The federal government's Trade Agreements Act (TAA, 19 U.S.C. 2501, et seq.) is designed to protect U.S. companies from unfair foreign competition in federal purchasing.

General Services Administration (GSA) maintains that the purpose of the TAA is:

- to implement the trade agreements of the Trade Act of 1974;
- to foster growth and maintenance of an open world trading system;
- to expand commerce of the United States in international trade; and
- to improve the rules of international trade and enforce those rules.

TAA compliance is a significant consideration for manufacturers working with the federal government. GSA works to keep noncompliant IT products off the GSA Schedule, and the Justice Department has repeatedly demonstrated that it will enforce the regulation, imposing hefty fines on TAA violators.

Common Criteria

BELKIN®

Belkin OmniView® Secure KVM Switch Common Criteria EAL 4 NIAP Certified

Los Angeles-based Belkin International, Inc. designed and developed the OmniView Secure KVM Switch specifically for military and government installations, enabling government users to control multiple computers from a single console. This solution is National Information Assurance Partnership (NIAP) Common Criteria validated to Evaluation Assurance Level (EAL) 4, and ensures data integrity by safely switching among secure and unsecured computers.

The CCEVS assessed the results of a security evaluation conducted by Certified Laboratories to issue its Common Criteria certification for the Belkin OmniView Secure KVM Switch.

Because the OmniView Secure KVM Switch keeps secure and unsecured computers separate and secure at all times, and prevents data transfer among them, this allows government users to control multiple USB computers from a single USB console, while ensuring the integrity of their data.

Dedicated manual switches with LED “switched state” indicators for each channel assure that the channel selection is unambiguously indicated. In addition, an on-board keyboard/mouse emulator was tested to assure that connected computers boot uninterrupted regardless of switched status. The OmniView Secure KVM Switch provides plug-and-play compatibility to assure that the host computer can quickly access needed configuration data.

Through its dedicated switching mechanism, the connection between the peripherals and the selected computer is activated. The design of these switches and associated circuitry assure that only a single computer can be engaged by the keyboard, mouse, and video monitor resources. By design, through isolated hardware, the OmniView Secure KVM Switch precludes the sharing or transfer of data between computers.

Available in 2-, 4-, and 8-port models, the OmniView Secure KVM Switch features both a dedicated processor per computer port and a dedicated path per channel to ensure each computer’s information and applications maintain separation and security at all times, and to prevent data transfer between systems. The device has no memory buffer or data-storage capability, making it impossible for entered keystrokes and other data to unintentionally transfer as users switch between computers.

While security is a primary feature of the OmniView Secure KVM Switch, in civilian government environments, KVM switching is also used to share expensive resources, such as high-resolution monitors, among multiple systems.

Belkin’s KVM Security Features

Belkin’s OmniView Secure KVM Switch provides full support for USB keyboards and mice and addresses an array of critical security requirements. Users can safely switch between as many as eight computers operating at different classification levels, all from a single keyboard, monitor, and mouse. Key security features include:

EAL compliance – assures that Belkin’s secure KVM solutions isolate information from separate computers (see section on EAL compliance).

No memory buffer – to avoid unintentional transfer of keystrokes or other data when switching between computers.

Non-reprogrammable firmware – to ward off tampering with KVM logic.

Circuits soldered directly to circuit board – to inhibit tampering with components.

Tamper-evident tape on enclosure – to indicate whether a KVM switch has been physically compromised and to visually confirm security when intact.

Dedicated processor per computer port – to keep computers running on different security levels separated, protecting classified data and preventing data transfer among computers.

Dedicated path per channel – to ensure data cannot be transferred across multiple classifications.

Built in the U.S.A. – Trade America Act (TAA) compliant (see section on TAA).

Additional Features and Benefits

In addition to advanced security features, OmniView Secure KVM Switches offer a host of additional features, providing superior value for the end user:

Compact metal enclosure – provides physical integrity and allows the KVM Switch to be placed beneath a monitor or other desktop item.

USB support – for USB-compatible keyboards, mice, and peripherals including Common Access Card (CAC) readers.

Substantial cost savings – reduces the number of peripherals required to manage multiple computers at each desktop.

Reduced clutter – the number of devices and wiring needed for each user is reduced, saving valuable desktop real estate and reducing clutter both on the desktop and in server-room environments.

Reduced energy costs – fewer peripheral devices require less energy for daily operations.

Dedicated port selector – allows users to switch easily from one computer to the next.

LED indicators – enable users to easily identify which computer is being accessed.

Compact design – provides flexible desktop or rack-mountable installation.

Heterogeneous system support – with no dependence on the hardware, database, or operating system of specific manufacturers, these KVM Switches support virtually all operating systems and applications.

High-res video support – video resolution up to 1920x1440@75Hz.

Global power adapter – for both domestic and international installations.

3-year warranty – includes free technical support, both online and by phone.

Belkin Advantage

Belkin provides SMB solutions that include structured cabling, KVM switches, LCD rack consoles, and racks and enclosures, in addition to a broad USB and cable product mix. A privately held company founded in California in 1983, Belkin has developed industry-leading innovations, prized by channel partners and end users alike for their dependability, customer service, and comprehensive warranties. Belkin has achieved over 20 consecutive years of dramatic growth and remains committed to making significant strides in the areas of research and design.

In addition to corporate headquarters in Los Angeles, Belkin now has offices throughout Europe—in the United Kingdom, the Netherlands, and Germany, among others—and in the Asia Pacific region, including Australia, Shanghai, and its regional headquarters in Hong Kong.

For more information, please visit www.belkin.com/kvm/secure or call (866) 623-3248.
GSA Schedule No. GS-35F-0085U.

F1DN102U

F1DN104U

BELKIN®

www.belkin.com

Belkin International, Inc.
501 West Walnut Street
Los Angeles, CA 90220, USA
310-898-1100
310-898-1111 fax

Belkin Ltd.
Express Business Park, Shipton Way
Rushden, NN10 6GL, United Kingdom
+44 (0) 1933 35 2000
+44 (0) 1933 31 2000 fax

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk, The Netherlands
+31 (0) 20 654 7300
+31 (0) 20 654 7349 fax

Belkin Ltd.
4 Pioneer Avenue
Tuggerah Business Park
Tuggerah, NSW 2259, Australia
+61 (0) 2 4350 4600
+61 (0) 2 4350 4700 fax