SKVM for Newbies

Secure. Certified. Connected.

What is a KVM?

There are scenarios when employees must perform a range of tasks that require multiple computers at one workstation to address each specific need. Moving between monitors is an inconvenience, not to mention the crowded space taken up by multiple monitors, keyboards, and mice. Fortunately, there's a device that streamlines desktops, allowing users to conveniently access two, three, or more computers using a single monitor, keyboard, and mouse.

Meet the KVM and Secure KVM switch.

A KVM switch (abbreviation for Keyboard, Video, Mouse) is a hardware device that allows a user to simply click a button to control multiple computers from one keyboard, video monitor, and mouse. KVM switches typically let a user switch audio and USB devices between computers. Benefits of a KVM include convenience, cost reduction, space saving, and decreasing desktop clutter.

Secure KVMs allow users to safely switch between connected computers while protecting sensitive data from accidental transfer or unauthorized access. The Belkin Secure KVM (SKVM) stresses the benefits of security, addressing the rigorous cybersecurity requirements for government, energy, financial services, and healthcare applications. The National Information Assurance Partnership (NIAP) — a government-sponsored program based within the National Security Agency — formulates specific requirements and recommendations to secure nearly every aspect of computing environments. Since 2006, Belkin has helped evolve and drive the NIAP and Common Criteria standards and our Secure KVMs feature the latest in Common Criteria and NIAP Protection Profile version 4.0 design requirements.

Belkin offers SKVMs with 2-, 4-, 8- and 16-port connectivity options for users working on varying numbers of computers. Our TAA-compliant SKVM series is ideal for highly sensitive applications that demand isolation between different network security enclaves. This helps prevent data leakage between computers while maintaining strict air-gap isolation, even when sharing peripherals.

Government

In government work environments, security is top of mind. Breaches give bad actors access to secure documents, leading to unauthorized data transfers that can compromise classified information. The Belkin SKVM series is designed and built for government and military agencies around the world to safeguard critical data and computer systems. Belkin's Universal and Modular SKVMs and SKMs meet all critical security constructs to ensure air-gap isolation and system security. Belkin's Modular form factor is among the smallest on the market, approximately the size of the iPhone. Universal video compatibility, innovative mounting options, and keyboard remote controls allow administrators to declutter the operator's desk without jeopardizing control and access.

The combination of Belkin Secure KVM remote-controls and extenders solves security and distance issues in government scenarios with groundbreaking technology that enables enclave switching control over long distance from the users' desktops. This critical security feature allows the processing side and the SKVMs to be located in a locked, secure data center rather than at the desktop. Although there are no processing components at the desktop, users have the flexibility to switch across a multitude of networks remotely to view data of different sensitivity levels on them. This is ideal for remote desktops, conference rooms, command and control, server farms, and secure video access found in government workspaces.

Energy

Supplying millions of people with daily electricity, heat, and gas is a critical infrastructural task and SKVMs move computers from control rooms into separate technical rooms while providing adaptable IT access to monitor functions. Decentralized facilities can have networks vulnerable to attacks on networked IoT and SCADA (Supervisory Control and Data Acquisition) systems. Energy and utility companies physically isolate networks and network assets to prevent breaches and SKVM switches help meet CIP standards for maintaining guaranteed isolation between multiple classes of network assets.

Belkin SKVM switches grant users access to multiple computing systems from one desktop console, easily switching between various systems as their jobs require. This practice helps segregate secure and non-secure computing use, so an employee accessing internal email systems with a lower level of security can switch and log into a more secure system to perform more sensitive tasks. Switches ensure malware or viruses that may reside on a less-secure system, peripheral, or other IoT device never see a path to jump onto more critical systems. Additionally, it ensures operators are not encumbered by having to use multiple keyboards, mice, or monitors to perform their jobs.

Healthcare

Secure KVMs are critical for healthcare teams on laptops and tablets when inputting patient information and documenting records. Belkin NIAP-certified Secure KVM and KM switches help prevent breaches that can open facilities to costly litigation and penalties. Creating an air-gap network limits access to medical data to users with tightly controlled permission without ever posting it on the public internet or an unsecured LAN.

Security features give added peace of mind for patient privacy and HIPAA confidentiality issues.
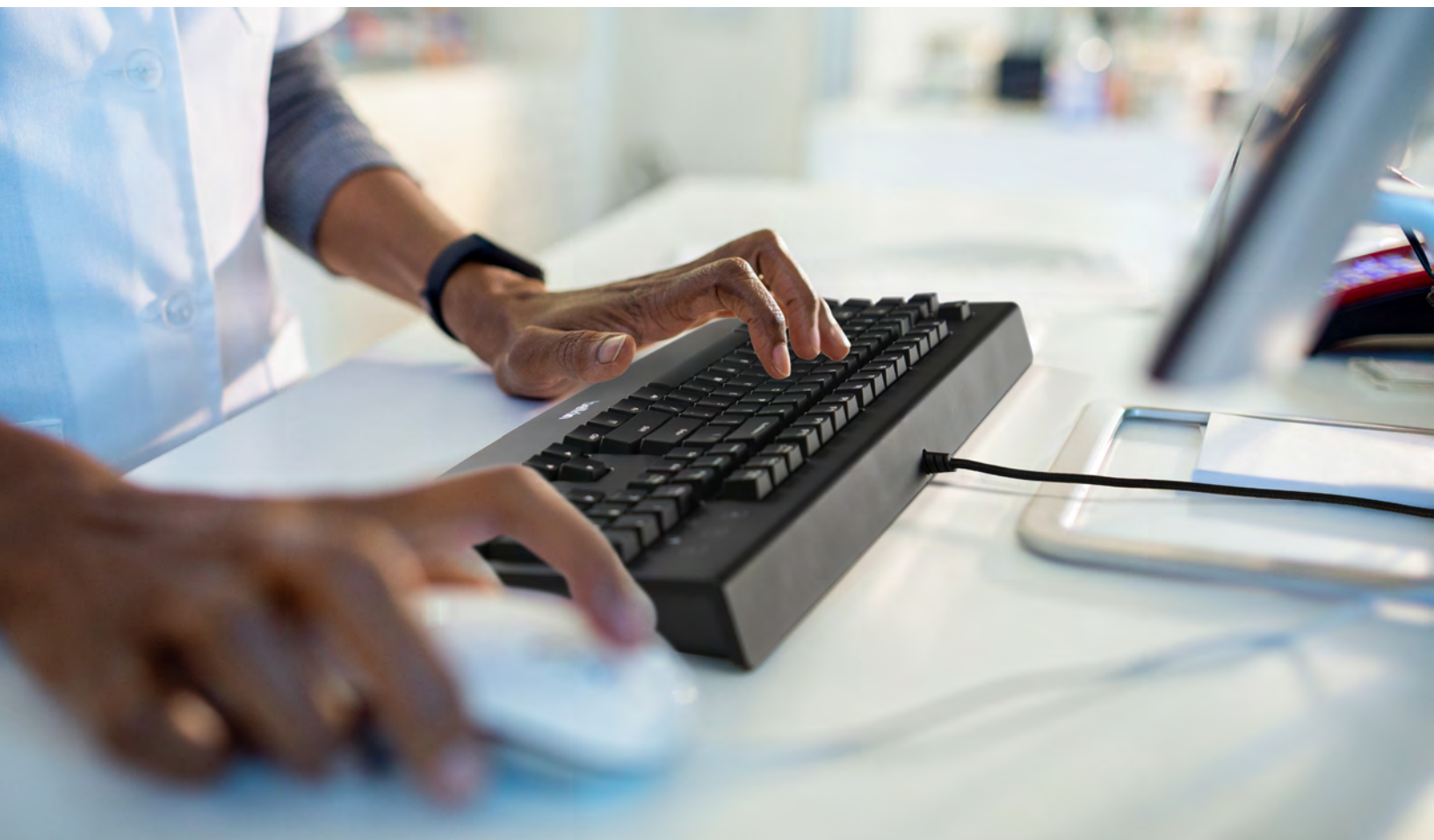
Financial Services

Compounding the challenge to protect potentially valuable network data is the interconnected nature of financial institutions. SKVM switches are vital components to defend against attacks, allowing access to multiple computing systems at different security classifications, from a single desktop. This segregates secure and non-secure computing use and ensures a vulnerable element in the network cannot be used to breach more sensitive assets.

Belkin SKVMs improve security by allowing organizations to rack-mount PCs and servers in one centralized location that can be securely monitored and managed. Switching capabilities are key in places like trading floor environments where a user at one desk needs to switch between multiple machines and is looking at multiple displays simultaneously. Further, SKVMs can enhance operator efficiency by eliminating desktop clutter and allowing one keyboard and mouse to control multiple systems, without the possibility of sharing any data between them.

The ultimate solution

Why choose Belkin Secure KVMs?

- Built to comply with NIAP certifications
- TAA-compliant
- Lowest priced technically acceptable options
- Secure KVMs that meet the highest security standards
- Innovative industry-leading designs and product features, including universal video, 4K at 60Hz

- Innovations to ease selection, procurement, installation, operation, and maintenance
- Customizable port coloring and naming
- An extensive portfolio of remotes, keyboards, and mounts.
- The most compact SKVMs in the market

- Always-on, active anti-tamper, ensuring the unit has not been opened since the final assembly step in the factory
- Supporting military bases worldwide
- Unsurpassed service from ex and active military account managers
- Free, U.S.-based pre- and post-sales technical support
- 3-year warranty with optional 4 and 5 years

Why Belkin

30
years of innovation

460,000,000+
government, TAA-compliant, B2B products sold in over 171 countries

40,000+
businesses and government agencies served

Who we are.

At Belkin International, we create products that help people realize the power of technology and make people's lives better, easier, and more fulfilling. This has been Belkin's mission since our inception in 1983. As a leading provider of SKVM switches for mission-critical applications, we positively impact and improve worker efficiency by delivering innovation and peace of mind to users working across multiple security enclaves. Our offer is certified to the latest Common Criteria NIAP Protection Profile for Peripheral Sharing Devices version 4.0 along with all applicable modules.

Belkin International, Inc.
555 S Aviation Blvd, Suite 180
El Segundo, CA 90245-4852
USA (310) 751-5569
belkin.com/cybersecurity

Support
Secure SKVM/SKM Support
800-282-2355

Sales
FederalBusinessDivision@belkin.com

LinkedIn:

Learn more: