belkin Cybersecurity

Stay in step with new Q2 Secure KVM solutions.

Your network is worth protecting against security breaches.

Welcome to the second installment of this year's Cybersecurity Dispatch quarterly newsletter. In Q2, the federal government, financial services and oil and gas industries are all going through various changes and challenges. Hiring freezes in the cybersecurity sector and proposed cybersecurity and technology bills are contributing to the volatility. In times like these, resellers and distributors can rely on Belkin as a leader in innovative Secure KVM solutions designed to serve their customers' evolving needs. Our DisplayPort DuoClave and MultiClave SKVMs and desktop remote controls are the latest to join our SKVM portfolio. These switches are designed to monitor up to 8 networks simultaneously from up to two displays. Have a look at our new secure solutions that keep networks secure and workforces productive.

View up to 4 networks simultaneously on up to 2 displays!

With multiple predefined working modes, MultiClaves offer flexible layouts for any task. Choose from single monitor modes like Side-by-Side, Quad and Quad-T, or dual monitor modes such as Duo/Matrix, Quad, and Scale. Switching modes is as simple as pressing a button, giving you seamless control over your workspace. For added flexibility, access additional modes, like Picture-in-Picture, with the press of a button. The always-on, battery-backed, active anti-tamper circuit protects the unit from a breach while in transit and after deployment.

DisplayPort MultiClave Secure KVM with CAC
F1DN104MVKVMDC4

Why choose this SKVM:

- Designed for use on government and military networks and developed for NIAP Protection Profile PSD 4.0, Common Criteria, and TAA compliance
- Situational awareness:
- Convenient preconfigured port coloring ensures front panel facilitates channel identification, reducing operator errors (channel 1 = green, channel 2 = white, channel 3 = red, channel 4 = white)
- Innovations for optimal user experience:
- Compatible with the optional Belkin SKVM Remote Control series including our 4- and 8-port variants, TAA docks, mounting solutions and extender portfolio
- True data path isolation:
- Optical data diodes prevent peripherals from being used to breach systems
- Additionally available in an 8-port option (F1DN108MVKVMDC4)

MultiClave Remote Control, 4-Port
F1DN-KVM-REM4MC

Belkin Secure KVM Remote Control provides operators access to the SKVM at the desktop. A 4-port remote control is integrated with a backlit USB keyboard for Belkin's Universal 2nd Generation, Universal DisplayPort and Modular SKVM/SKMs (Modulars require available adapter). Its cascade (or daisy-chain) feature allows operators to pair DuoClave or MultiClave Remote Control with standard SKVM remote control to enable host selection on each display.

Why choose this remote:

- Available in 4-ports (to integrate with Belkin Universal 2nd Generation, DuoClave and MultiClave SKVM/SKMs and Modular KVM – with adapter)
- Situational awareness:
- LED colorization gives clear indication of the active channel, reducing operator errors
- Declutter the desktop with relocated SKVM off-desk and stable fit on the desktop optimizes ergonomic use
- Gives clear visual parallel:
- Mimics the front panel of the SKVM to show operators the enclave they're working in

DisplayPort DuoClave Secure KVM with CAC
F1DN108MKVMDC-4

Belkin DuoClave SKVM Series enables simultaneous secure management of two networks from two independent displays. Featuring ten predefined monitor layouts, DuoClave offers a setup for most use cases with just a keyboard shortcut. Whether you're working with two, three, or four connected monitors, our presets make it easy to navigate and customize your workspace for maximum productivity.

Why choose this SKVM:

- Designed for use on government and military networks and configured to meet NIAP Protection Profile PSD 4.0, Common Criteria, and TAA compliance
- Convenient preconfigured port coloring ensures front panel facilitates channel identification, reducing operator errors (channel 1 = green, channel 2 = white, channel 3 = red, channel 4-8 = white)
- Compatible with the optional Belkin SKVM Remote Control series including our 4- and 8-port variants, TAA docks, mounting solutions, and extender portfolio
- Additionally available in a 4-port option (F1DN104MKVMDC-4)

Universal 2nd Gen Secure KVM Switch, 8-Port Single Head w/ CAC
F1DN108KVM-UN-4

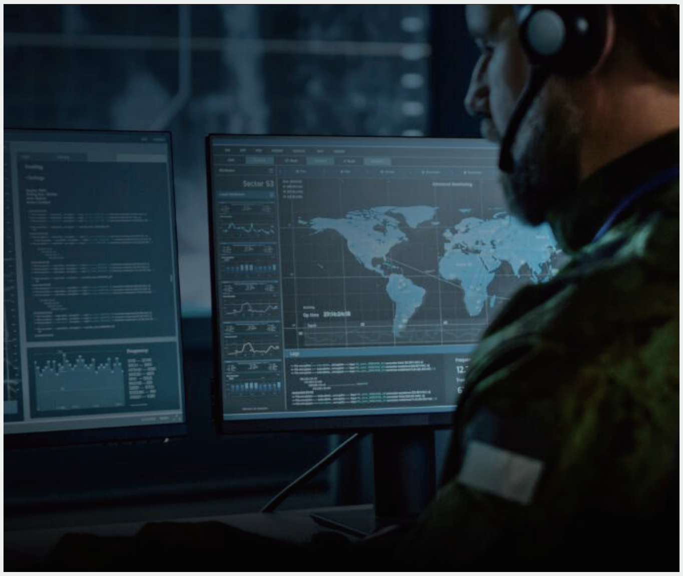
Designed to deliver a streamlined user experience when working across multiple security enclaves, Belkin's Universal 2nd Gen Secure KVM Switch, 8-Port Single Head w/CAC meets the latest in Common Criteria and NIAP Protection Profile for Peripheral Switching Devices version 4.0 requirements. Compatible with the Remote Control with Integrated Keyboard and the new Universal Remote Control. This switch elevates the user experience and improves both user and bystander enclave awareness, minimizing operator error by synchronizing backlit LED enclave color designation.

Why choose this switch:

- Designed for NIAP Protection Profile PSD 4.0, Common Criteria, TAA compliance
- Combo connector video support for up to 4K (3840x2160), @60Hz refresh
- Universal Video (DisplayPort and HDMI inputs and outputs)
- Customizable port coloring on the front panel: Facilitates port identification and reduces user switching errors. Color coding mimicked by Belkin Secure KVM Remote Control with Integrated Keyboard (F1DN008KBD)

Industry News

Content condensed from articles that originally appeared on MeriTalk at www.meritalk.com/articles/



DOGE Suspected of Cutting Cybersecurity and Privacy Corners

A former senior Social Security Administration (SSA) official has claimed that the Department of Government Efficiency (DOGE) bypassed cybersecurity and privacy protocols when accessing sensitive SSA data. A group of labor unions filed a motion to halt DOGE's access to this data, based on concerns over privacy and security breaches.

In her declaration, former SSA employee Tiffany Flick detailed how DOGE pressured SSA officials for immediate access to sensitive systems without proper justification. Flick also expressed concern over the loss of expertise at SSA, which she believed could jeopardize its operations.

In response to concerns over DOGE's secrecy, a federal judge ruled that the agency must release its internal documents to the public, shedding light on its operations and influence, including Elon Musk's role in the department.

Cybersecurity and Tech Bills Advanced by House E&C

The House Committee on Energy and Commerce advanced several cybersecurity and technology bills, sending them to the full House for consideration. Key bills include the NTIA Policy and Cybersecurity Coordination Act, which aims to strengthen the National Telecommunications and Information Administration's (NTIA) cybersecurity role, and the Understanding Cybersecurity of Mobile Networks Act, which examines mobile network vulnerabilities. Additionally, the Promoting United States Wireless Leadership Act seeks to ensure U.S. leadership in global wireless technology, while the Consumer Safety Technology Act focuses on AI and blockchain technology for consumer protection. These bipartisan bills, which were approved by the House last Congress, but not enacted, address critical cybersecurity and technological challenges.

Hiring Freeze on Cyber Workforce Causing Concern

Rep. Bennie Thompson expressed concerns during a Homeland Security Committee hearing that President Trump's hiring freeze could worsen the cybersecurity workforce gap in the federal government, delaying recruitment and onboarding of top cyber talent. Republican lawmakers dismissed these concerns, citing exceptions in the freeze order that supposedly protect the federal cyber workforce. Max Stier, CEO of the Partnership for Public Service, echoed Thompson's worries, noting that job offers and opportunities for cybersecurity students have been rescinded or paused due to the freeze. Thompson plans to introduce two resolutions and send a letter to OPM to seek clarification on how the freeze impacts the cyber workforce.

For questions and 24/7 U.S.-based Secure KVM Support, contact us at **800-282-2355** or **federalbusinessdivision@belkin.com.**

For resources including white papers, compliance information, datasheets, installation and administration guides, user manuals, warranty information, and software downloads, and to learn more about our products, visit:

www.belkin.com/products/product-resources/cybersecurity/resources/