

Reduce costs and
fortify your network.



Welcome to the second quarter edition of the Belkin Cybersecurity Dispatch newsletter. As federal agencies and critical infrastructure sectors including financial services, energy and education finalize budgets for the year, many organizations are prioritizing technologies that reduce operational risk and escalating costs.

Our new industry-leading standard 5-year warranty on Universal DisplayPort Secure KVMs exemplifies the Belkin commitment to provide long-term reliability and confidence for our customers. At the same time, geopolitical tensions and evolving cyber threats (see news story below) continue to drive increased investments in cybersecurity. Organizations seeking trusted tech to strengthen their network protection rely on Belkin to deliver advanced tools and secure KVM solutions to support evolving federal cybersecurity requirements.

New!

Standard 5-Year Warranty

Belkin is excited to introduce a new industry-leading standard 5-year warranty on Universal DisplayPort Secure KVMs, reinforcing our commitment to deliver long-term reliability and confidence for our customers. This enhanced coverage supports organizations deploying secure KVM technology in government, defense and other secure environments where dependable performance and long product lifecycles are essential. By choosing Belkin, our customers receive greater assurance that their investment is backed by proven support and quality.

Our new standard 5-year warranty delivers:

- A new reliability standard for secure KVM deployments.
- Reduced total cost of ownership across product lifecycle.
- Extended protection for your investments.



Industry-leading 5 year
standard warranty on the
Universal DisplayPort
Secure KVM Series.

With this expanded warranty coverage, customers benefit from greater peace of mind while reducing long-term operational costs. Organizations that standardize on Belkin's secure KVM solutions receive industry-leading protection designed to safeguard their infrastructure and maximize the value of their technology investments over time.

Featured Products



Universal DisplayPort Secure KVM, 4-Port Dual Head with CAC

F1DN204KVM-DC-4



Industry-leading 5 year
standard warranty on the
Universal DisplayPort
Secure KVM Series.



4:2 DisplayPort DuoClave Secure KVM with CAC

F1DN104MKVMDC-4

Designed for maximum user efficiency, this switch includes configurable channel designator lighting. Both the front panel and the remote control provide clear visual indicators of the security enclave in use, helping to prevent operator errors. The 8-port model offers an optional rackmount ears kit for easy installation. Each unit is also equipped with a battery-backed, always-active anti-tamper system that permanently disables the device in the event of any physical breach.

Also available in 8-port: F1DN108KVM-DC-4

Why choose this SKVM:

- **Built for secure environments:** Designed for use on government and military networks and developed for compliance with NIAP Protection Profile PSD 4.0.
- **Situational awareness:** Convenient preconfigured port coloring ensures front panel facilitates channel identification, reducing operator errors. (channel 1 = green, 2 = white, 3 = red, 4 = white).
- **Innovations for optimal user experience:** Compatible with the Belkin MultiClave Secure KVM Remote Control (F1DN-KVM-REM4MC) to declutter the workspace and improve awareness of the active security domain.
- **True data path isolation:** Optical data diodes assure data only flows from device to host.
- **Extended lifecycle protection:** Includes new standard 5-year warranty to help reduce total cost of ownership.

Belkin DuoClave Secure KVMs with CAC allow you to extend the desktop while maintaining consolidated control between computers at different security enclaves. For CAC, optical data diodes on all USB connections ensure unidirectional data flow of HID filtered information. Dedicated Common Access Card input ports consolidate the number of CAC readers and allow a single reader to be shared across all connected systems for user authentication. CAC models feature CAC freeze to allow a user to lock CAC on a given channel while using another channel for keyboard, mouse and video.

Also available in 8-port (F1DN108MKVMDC-4)

Why choose this SKVM?

- **Built for secure environments:** Designed for use on government and military networks and configured to meet NIAP Protection Profile PSD 4.0.
- **Securely multitask:** Efficiently manage and view two active networks simultaneously from two displays.
- **Situational awareness:** Convenient preconfigured port coloring ensures front panel facilitates channel identification, reducing operator errors. (for 4- and 8-port SKVMs, port 1 = green, port = white, port 3 = red, all others = white).
- **Key Press Seamless Cursor Switching (KPSCS):** Keyboard control follows mouse as cursor crosses one physical display to the other with a keyboard key held down.



DuoClave Secure KVM Remote Control 4-Port

F1DN-KVM-REM4DC

Belkin Secure KVM Remote Controls are designed to help declutter desks while increasing situational awareness and effectiveness. This 4-port Secure KVM Remote Control provides operators with access to the SKVM at the desktop. It mimics the front panel of the SKVM, with a clear, visible parallel to show operators the enclave they are working in.

Also available in 8-port (F1DN-KVM-REM8DC)

Why choose this remote control:

- Integrates with Belkin DisplayPort DuoClave Secure KVM series.
- **Situational awareness:** LED colorization gives clear indication of the active channel, reducing operator errors.
- **Workspace efficiency:** Free up desk space by relocating the SKVM off the desktop, while maintaining a stable and ergonomic setup.
- **Clear visual parallel:** Mimics the front panel of the SKVM to show operators the enclave they're working in.



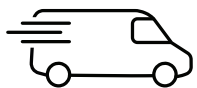
Universal 2nd Gen Secure KVM Switch, 4-Port Single Head w/ CAC

F1DN104KVM-UN-4

The Belkin Universal 2nd Gen Secure KVM Switch, 4-Port Single Head w/ CAC can simultaneously accommodate legacy DVI-D input/output as well as modern, high-resolution HDMI and DisplayPort input/output on the same SKVM. The pioneering connector design and internal video conversion allows the same SKVM to be used for legacy systems and accommodates anticipated technology changes over time. This model supports two different networks, features audio freeze and CAC functionality.

Why choose the Universal 2nd Gen KVM?

- Designed for use on government and military networks.
- Configured to meet NIAP Protection Profile PSD 4.0 and TAA-compliant.
- **Tamper-proof system:** Advanced Universal 2nd Gen SKVMs include an always-on, battery-backed, active anti-tamper circuit that protects the unit while in transit and after deployment.
- **Supports DisplayPort, HDMI, and DVI-D via passive cabling:** Belkin Secure Universal SKVM supports video for any combination of DP, HDMI, and DVI-D I/O with only passive cables at resolutions from 800x600 to 4K (3840x2160) @60Hz.
- In stock now and ready to ship.



In stock now and ready to ship.

Industry News

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



White House Unveils National Cyber Strategy

The White House Office of the National Cyber Director released a national cybersecurity strategy outlining six pillars to strengthen U.S. cyber defenses and guide federal policy and resources. The plan emphasizes deterring adversaries through offensive and defensive cyber operations, streamlining cybersecurity regulations, modernizing federal networks with technologies like zero trust and post-quantum cryptography and protecting critical infrastructure. It also prioritizes maintaining U.S. leadership in emerging technologies and expanding the cybersecurity workforce through stronger talent pipelines across government, industry and academia.

Cybersecurity Leaders Brace for Iran-Related Cyber Threats

Cybersecurity experts are warning that ongoing tensions in the Middle East following U.S. strikes in Iran could trigger increased cyber activity from Iran-linked actors targeting critical infrastructure and vulnerable systems. While large-scale state-sponsored campaigns have not yet been observed, analysts report a surge in opportunistic hacktivist activity and warn that disruptive attacks or intrusions remain possible. Officials urge organizations to strengthen basic cyber defenses as federal authorities continue monitoring threats amid reduced cybersecurity staffing during the Department of Homeland Security shutdown.

FBI Cyber Division's Operation Winter SHIELD takes hold nationwide

The FBI Cyber Division has launched Operation Winter SHIELD, a two-month campaign spotlighting ten high-impact cybersecurity actions designed to help organizations reduce common breach pathways and strengthen critical infrastructure against nation-state and criminal threats. The initiative – now supported by multiple field offices nationwide – translates lessons from real-world investigations into practical steps such as adopting phish-resistant authentication, securing backups and exercising incident response plans. FBI leaders emphasized that the effort goes beyond compliance, urging broad adoption of proven safeguards to build resilience and raise the cost of cyberattacks targeting government, industry and critical infrastructure.

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/cybersecurity/resources