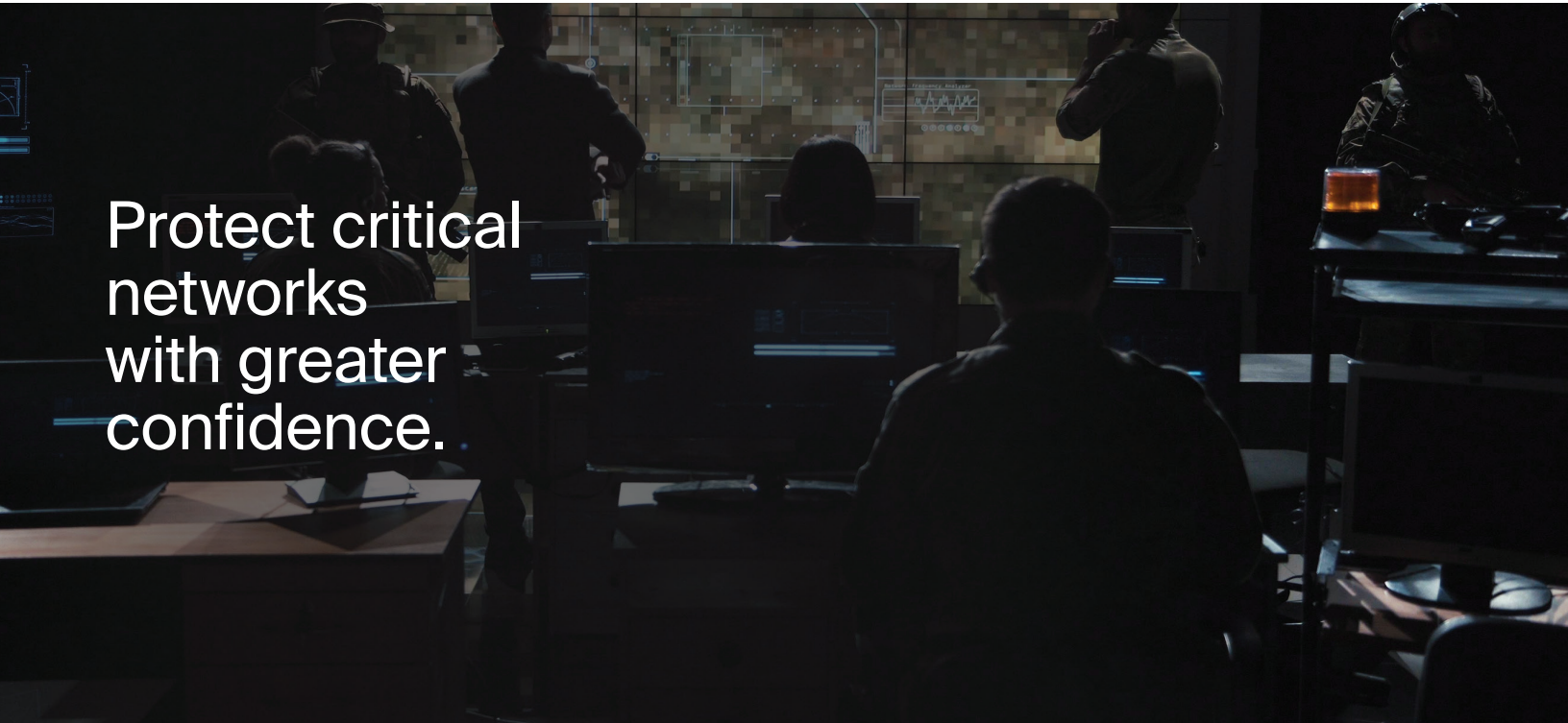




Protect critical networks with greater confidence.

Cybersecurity requirements continue to evolve as AI, Zero Trust and hybrid infrastructures reshape secure computing environments. This quarter, we're re-introducing our standard 5-year warranty on select Secure KVMs, which provide longer lifecycle support while maintaining the security, reliability and compliance trusted by government and defense organizations.

Experience the Belkin difference.

All our Secure KVMs are:



NIAP-compliant



TAA-compliant



Built for government application



Featured Products

Best for environments requiring mixed legacy and modern video connectivity.

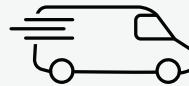
Universal 2nd Gen Secure KVM Switch, 4-Port Single Head w/ CAC

F1DN104KVM-UN-4



Features:

- Supports video for any combination of DP, HDMI, and DVI-D I/O with only passive cables.
- Resolutions from 800x600 up to 4K (3840x2160) @60Hz.
- Always-on, battery-backed, active anti-tamper circuit that protects the unit while in transit and after deployment.
- Port color coding is mirrored on the optional Remote Control with Integrated Keyboard (F1DN008KBD) for enhanced situational awareness.



**In stock now and
ready to ship.**

Built for secure workflows that don't require CAC.

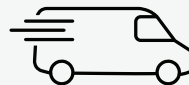
Universal 2nd Gen Secure KVM Switch, 4-Port Single Head No CAC

F1DN104KVM-UNN4



Features:

- Available in 2-, 4-, 8-channel models with customizable, preconfigured U.S. industry-standard color schemes.
- Combo connector video support for up to 4K (3840x2160) @60Hz.
- Preconfigured port coloring and naming facilitates channel identification and helps reduce operator switching errors.
- Port color coding is mirrored on the optional Remote Control with Integrated Keyboard (F1DN008KBD) for enhanced situational awareness.



**In stock now and
ready to ship.**

Purpose-built for environments requiring the highest level of signal isolation.

IsoClave RED/BLACK Secure KVM Switch, 4-Port Dual Head

F1DN204KVM-UN4C



Features:

- Meets stringent RED/BLACK requirements of CNSSAM-CTTA, calling for 60 dB isolation for digital signaling.*
- Blocked audio, HDMI and remote control ports enhance isolation, while allowing existing electronics to remain in place.
- Preinstalled isolating host cables enable efficient deployment.
- Preconfigured, customizable port coloring simplifies channel identification and helps reduce operator switching errors. (channel 1 = green; channel 2 = red)

* Detailed in the committee's TEMPEST/01-13, Tables 2 and 6.
Electrical isolation does not imply TEMPEST certification.

Reduce operator error while improving workspace efficiency.

Remote Control with Integrated Keyboard

F1DN008KBD



Features:

- Compatible with our Universal DisplayPort, Universal 2nd Gen and Modular SKVM/SKMs in 2-, 4- and 8-port models.
- Integrates an 8-port remote control with a backlit USB keyboard to reduce desktop clutter.
- High-reliability mechanical keys deliver quiet, dependable operation.
- Single USB connectivity and adjustable backlighting enable simplified deployments and improved operator comfort.
- Channel color-matched backlighting provides a clear visual indication of the active security enclave.

Industry News

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



Up to 80% of Routine Defense Work Could be Handled by AI

DISA officials say artificial intelligence could eventually automate 75% to 80% of routine defensive cyber tasks, allowing cyber operators to focus on more advanced threats while AI tackles everyday detection and response. Before AI can make autonomous cyber defense decisions at scale, however, the Defense Department must address challenges involving trust, accreditation, security and data integrity. DISA is currently building a unified cybersecurity data environment to provide the foundation for future AI-powered cyber operations.

Warnings Issued of CISA Election Security Cuts Before Midterms

Sen. Mark Warner is warning that CISA has scaled back election security support for state and local officials ahead of the 2026 midterm elections, raising concerns. Although CISA maintains that it still provides voluntary threat intelligence, information sharing and cybersecurity services to states upon request, staffing cuts and proposed budget reductions could leave election systems more vulnerable to cyber threats and foreign interference.

Is AI Forcing Zero Trust Rethink on Risk, Control?

Federal cybersecurity leaders say AI is forcing agencies to rethink zero trust security as machine-speed decision-making outpaces traditional human approval processes. Officials emphasized the need for predefined security rules, stronger identity controls and continuous validation to manage AI-driven activity, while cautioning that AI systems remain vulnerable to manipulation and require human oversight.

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