Technology tools to detect, prevent and mitigate cyber threats.

Welcome to the new quarter and the first edition of the Belkin Cybersecurity Dispatch quarterly newsletter for 2026. Organizations are evaluating their security initiatives in the face of the first AI-driven cyberattack (see Industry News story below) and looking for innovative ways to protect their networks. In this new era of increasingly sophisticated cybersecurity threats, the federal government and military organizations are seeking strategies and tools.

We are proud to be at the forefront of innovation in desktop-level cybersecurity, and resellers and distributors rely on Belkin's Secure KVM solutions as we design our equipment to pinpoint system vulnerabilities to meet customers' evolving needs.

Featured Products

4:2 DisplayPort MultiClave Secure KVM with CAC

F1DN104MVKVMDC4

Developed for compliance with NIAP Protection Profile PSD 4.0, the Belkin DisplayPort MultiClave Secure KVM with CAC is streamlined for DisplayPort setups. New colorization adds more options to view up to 4 networks on up to 2 displays and improves user situational awareness. The always-on, battery-backed, active anti-tamper circuit protects the unit from breach while in transit and after deployment.

Also available in 8-port: F1DN108MVKVMDC4

Why choose this SKVM:

- 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, all others = white).
- **Innovations for optimal user experience:** Compatible with the Belkin MultiClave Secure KVM Remote Control (F1DN-KVM-REM4MC), delivering the ultimate solution for decluttering the desk while enhancing the operator's awareness of the security domain they're working in.
- **True data path isolation:** Optical data diodes assure data can only flow from device to host.

4-Port Single Head DVI Modular Secure KVM Switch PP4.0 W/ Remote

F1DN104MOD-DD-4

The Belkin Modular Secure KVM series packs the latest Common Criteria and NIAP Protection Profile 4.0 security standards in the smallest form factor available. This low-priced switch is future-proof, supporting both legacy and current connectors. An included remote control and innovative mount options allow administrators to craft operator stations that meet security requirements while decluttering the desk.

Also available in dual head: F1DN204MOD-DD-4

Why choose this SKVM:

- Designed for NIAP PP PSD 4.0 compliance and TAA compliance.
- Video support for up to 4K (3840x2160), @30Hz refresh.
- Optional DP, mDP, DPMST, HDMI, DVI, VGA and USB-C cables - host and console.
- Supports up to two host computers.

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

F1DN204KVM-UN4C

The IsoClave RED/BLACK Secure KVM Switch is NIAP PP 4.0, TAA, and Common Criteria compliant for government and military applications. It meets the stringent RED/BLACK requirements of CNSSAM-CTTA, calling for 60 dB isolation for digital signaling detailed in the committee's TEMPEST/01-13, Tables 2 and 6.*
To enhance security, audio, HDMI and remote control ports are blocked, allowing existing electronics to remain in place while improving isolation.

Additionally, IsoClave RED/BLACK Secure KVMs feature integrated cables that meet stringent analog and digital signal isolation requirements.

Also available in a 2-port option: F1DN202KVM-UN4C

Why choose this SKVM:

- Configured for the latest Common Criteria and NIAP PP 4.0 cybersecurity standard.
- **Secure and ready to deploy platform:** Preinstalled isolating host cables enable efficient deployment, while providing the highest level of isolation in any commercial SKVM.
- **Situational awareness:** Convenient preconfigured port coloring with the option to change the color scheme, ensures front panel facilitates channel identification, reducing operator errors (channel 1 = green, 2 = red).
- **Innovations for optimal user experience:** Compatible with the Belkin SKVM Remote with Integrated USB Keyboard (F1DN0008KBD), delivering the ultimate solution for decluttering the desk while enhancing the operator's awareness of the security domain they're working in.

*Note: Electrical isolation does not imply TEMPEST certification.

Secure KVM Remote Control 4-Port

F1DN-KVM-REM4

Belkin Secure KVM Remote Controls are designed to help declutter the desk 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 2- & 8-port models:
F1DN-KVM-REM2/F1DN-KVM-REM8

Why choose this remote control:

- Compatible with Belkin Universal 2nd Generation, Universal DisplayPort, DuoClave and MultiClave SKVM/SKMs and Modular KVM (with adapter).
- **Situational awareness:** LED colorization gives clear indication of the active channel, reducing operator errors.
- Free up desk space by relocating the SKVM off the desktop, while maintaining a stable and ergonomic setup.
- **Gives clear visual parallel:** Mimics the front panel of the SKVM to show operators the enclave they're working in.

Industry News

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

Senators sound alarm after first AI-driven cyberattack targets 30 companies

Bipartisan senators are urging swift federal action after Anthropic confirmed the first known case of an AI system independently carrying out cyberattacks against major tech firms, financial institutions and government agencies. Anthropic reported that a Chinese state-sponsored actor used its Claude Code tool to autonomously execute 80–90% of the operation at speeds unattainable for human hackers. The senators warned that AI-driven, "agentic" attacks represent a new national security threat and asked the National Cyber Director for details on the incident, federal response efforts and coordination with AI companies. They also requested recommendations on how Congress can help counter future autonomous AI cyber threats.

Report finds U.S. cyber progress stalling out for the first time in recent years

A new report from CSC 2.0 warns that U.S. cybersecurity progress has stalled for the first time in years, with the nation "slipping" in its ability to defend itself and its allies. The organization cites rapid technological change, unfilled cyber leadership roles and recent federal workforce and budget cuts — particularly at CISA, State, and Commerce — as key factors eroding momentum, noting that only 35% of the Cyberspace Solarium Commission's recommendations remain fully implemented. To reignite progress, the report urges Congress and the administration to reinforce national cyber leadership, rebuild the cyber workforce, strengthen diplomatic and deterrence tools and restore bipartisan commitment to cybersecurity as a core national security priority.

EPA uncovers large cyber gaps in water sector, urges greater visibility

The EPA's push to identify internet-exposed operational technology in water and wastewater systems is revealing a major cybersecurity gap, as many utilities are unaware their critical devices are accessible online. EPA analyst Cole Dutton explained that small and rural systems often lack in-house technical expertise and rely on third-party vendors, prompting the agency to publish a Cybersecurity Procurement Evaluation Checklist and offer direct assistance to help utilities understand and secure their exposure. Dutton said the EPA aims to improve sector-wide asset awareness, strengthen vendor oversight and proactively identify vulnerabilities — work he sees as a major opportunity to advance cybersecurity heading into FY 2026.

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