# Make security awareness top of mind.

Welcome to the Belkin Cybersecurity Dispatch quarterly newsletter with Secure KVM news and solutions for government and military professionals. This issue highlights our new SKVM landing page, a rich resource with tools to research SKVM purchasing options.

As the year winds down, we're excited to be a part of the giant steps taken by the SKVM/Cybersecurity industry. We look forward to finishing the year strong and not only keeping pace with new trends, but setting the pace for further network security advancements.

Your purchasing journey simplified with new SKVM resources.
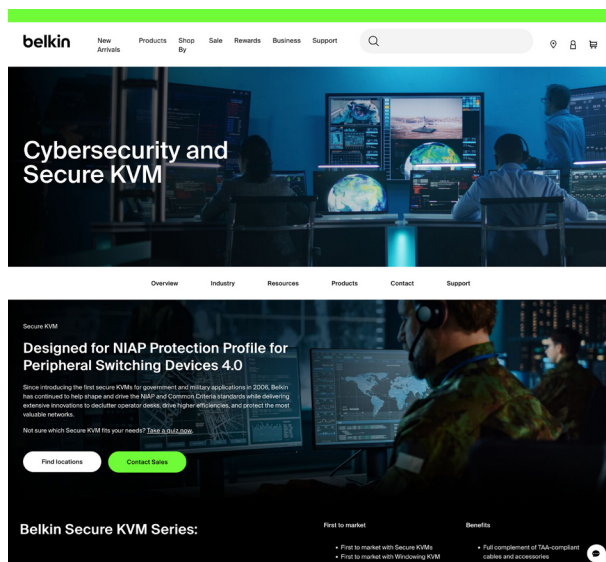
Our revamped landing page offers an improved user experience with more tools to assist with the SKVM purchasing journey, including:

- **Contact us:** We're making it easier for customers to get in touch with our sales team for quotes and information about our products.

- **Refined product categories:** Customers can easily find specific products thanks to our organized categories, which group items appropriately to streamline the user experience.

- **Monthly tradeshow schedule:** Our tradeshow schedule is now posted by month — with show dates and booth numbers featured.

- **Interactive banners:** Experience the Belkin difference through interactive features that showcase our SKVM colorization options.

- **Cybersecurity Dispatch Newsletter:** All quarterly newsletters are posted, including this edition.

- **Support:** We strive to provide the best support possible, and we've made it easier for all our customers to receive the help they are looking for.

For more information, visit us at www.belkin.com/cybersecurity

Color-Coded Protection

KVM Remote Control with Integrated Keyboard

F1DN008KBD

Security awareness is the cornerstone of keeping classified information from unauthorized access and preventing cyber incidents. Without visibility, companies and agencies are vulnerable to outside and inside threats.

This product allows organizations to utilize color as an indication of the security enclave, and the programmable front panel LED lights used in conjunction with this keyboard provide visibility and security awareness to operators of multiple levels of classified information.

User benefits:

- Compatible with the Modular Secure KVM 2-,4-,8-port
- Pairing it with the Belkin Universal and Modular Secure KVM provides channel selection options for the 1-8 port Secure KVMs
- Minimizes operator error by synchronizing backlit LED with enclave color designation
- Automatically syncs the enclave colors configured into the Universal 2nd Gen SKVM or the Modular Secure KVM

F1DN008KBD

Featured Products

Why choose this switch:

- Designed for NIAP PP PSD 4.0 compliance and 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

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

F1DN108KVM-UN-4

Use Cases

Always on, active anti-tamper and some of the most advanced protections against ultrasonic audio attacks make this switch perfect for use in government and military IT environments.

4-Port Single Head Modular SKVM Switch Base Unit PP4.0 W/ Remote

F1DN104MOD-BA-4

Why choose this switch:

- 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 4 host computers

Use Cases

The Belkin Secure KVM series is ideal for use in IT environments that demand rigorous cybersecurity provisions — including government, military, and healthcare applications. Ideal for highly sensitive applications that demand isolation between different network security enclaves, the Belkin Modular Secure KVM switches utilize optical data diodes and peripheral emulation on each channel.

Extender Transmitter Fiber SFP, Universal Video (4K 60Hz 4:2:0)

F1DN-KVM-EXTFI

Why choose this transmitter:

- Control your computer, secure enclave or SKVM switch with signal boost up to 984 feet (300m)
- Ensure reliable network connections
- TAA-compliant
- Compatible with Belkin multi-mode, single-mode cables
- Matching receiver: Extender Receiver Fiber SFP, Universal Video (4K 60Hz 4:2:0), F1DN-KVM-EXRFI

Use Cases

A ready-made solution for government and military fiber-optic networks requiring extending signals over distances while maintaining stringent security.

Extender Receiver Fiber SFP, Universal Video (4K 60Hz 4:2:0)

F1DN-KVM-EXRFI

Why choose this receiver:

- Receive transmissions to control your computer, secure enclave or SKVM switch with signal boost up to 984 feet (300m)
- Ensure reliable network connections
- TAA-compliant
- Compatible with Belkin multi-mode, single-mode cables
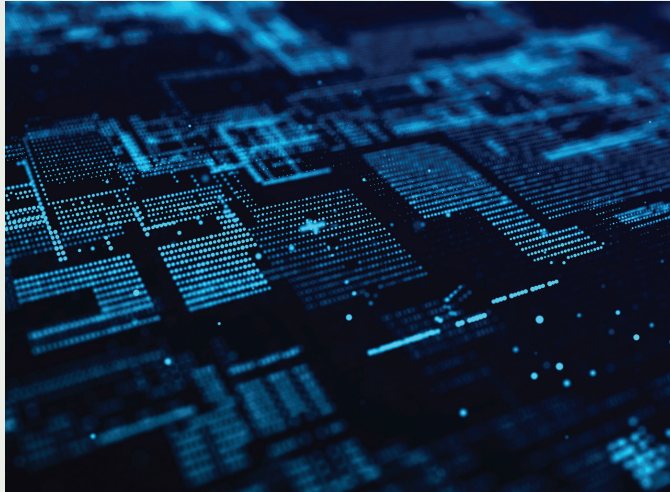- Matching transmitter: Extender Transmitter Fiber SFP, Universal Video (4K 60Hz 4:2:0), F1DN-KVM-EXTFI

Use Cases

An ideal solution for government and military fiber-optic networks requiring extending signals over distances while maintaining stringent security.

Industry News

CISA steps up cybersecurity measures with awareness campaign and reporting portal

The Cybersecurity and Infrastructure Security Agency (CISA) has launched Secure Our World, a campaign to create awareness about the importance of cybersecurity and encourage engaging in best practices. The program includes PSAs, digital content, toolkits and other cybersecurity resources to ensure the safety of both personal and business accounts. Additionally, CISA established a new cyber incident reporting portal and released a voluntary reporting resource, seeking to improve incident reporting and address the increasing digitization of work and life.

Georgia Tech sued by DoD over alleged cybersecurity failures in contracts

The Department of Defense has filed a lawsuit against the Georgia Institute of Technology (Georgia Tech) and Georgia Tech Research Corp. for failing to develop and implement a system security plan as required by their contracts with the DoD. The lawsuit claims that the institution's Astrolavos Lab plan implemented in February 2020 failed to provide security across all laptops, desktops and servers. Georgia Tech challenges the allegations and maintains the lawsuit misrepresents the institute's "culture of innovation and integrity."

HHS bolstering cybersecurity to combat rising healthcare attacks

The Department of Health and Human Services (HHS) is implementing cybersecurity goals and a gateway to mitigate escalating cyber threats in the healthcare sector. Last year, ransomware attacks on the U.S. healthcare industry increased by 128%, impacting patient care and data security. HHS is working to enhance cybersecurity measures for electronic health records (EHR), notoriously vulnerable to cyberattacks. The agency's strategies include new CPGs, a gateway website and partnerships with government agencies to strengthen incident response.

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