Securing Energy Company Desktops from Cyber Threats

with the Latest Secure KVM Technology

Energy and utility companies are key economic drivers, making their infrastructures tempting targets for a broad range of cyber threats. The energy industry is at risk for cybercrimes related to supply chain partners, OT infrastructure, and IT systems. Decentralized facilities not designed for digital transformation have networks vulnerable to attacks involving ransomware, data theft, billing fraud, and mobile device phishing. Renewable solar and wind is an emerging part of the energy sector that attracts malicious actors looking to exploit weaknesses. Operational disruption in clean energy includes attacks on networked IoT and SCADA (Supervisory Control and Data Acquisition) systems.

Service interruptions can prove costly and potentially damaging to power grids and the reputations of energy industry supermajors. Recent high-profile incidents include the Russian state-sponsored hacking group Sandworm targeting a Ukrainian company with malware in October, 2022, the 2021 attack on the US Colonial Pipeline that prompted a shut down, and the ransomware attack on Volue ASA that occurred prior to it. Nation-states and non-state malicious actors — including foreign terrorist and hacktivist groups, advanced persistent threat (APT) groups, and lone wolf cyber criminals — are among those exploiting vulnerabilities.

According to the 2023 IBM Security X-Force Threat Intelligence Index, “In 2022, 10.7% of observed cyberattacks targeted the energy industry, including electric utilities and oil and gas companies, ranking it as the fourth most affected sector behind the manufacturing industry, the financial sector, and the professional services sector. North American energy organizations accounted for 46% of all energy attacks observed last year, a 25% increase from 2021 levels.”

Parachute Technology’s statistics by industry reveal more granular data on energy industry attacks. Their 2022 statistics disclose that “Cyberattacks cost the energy sector $4.72 million per incident on average, 22% of cyberattacks in oil and gas were related to espionage, and the sector is highly susceptible to social engineering, considering 60% of all data breaches are phishing attacks.”

Introducing AI (Artificial Intelligence) and ML (Machine Learning) into market segments has both negative and positive effects on cybersecurity. Generative technology can be used maliciously to develop smart malware, automate social engineering attacks to evade data security protocols, and create sophisticated phishing emails. Scenarios include proxy cyber criminals attacking public and private companies as part of ransomware campaigns and AI models creating realistic-sounding speech to use in phone-based attacks. On the positive side, AI can bolster cybersecurity by threat hunting, triaging vulnerabilities, automatically generating new security controls and optimizing and monitoring data centers. Its inherent ability for deep learning means it can analyze and mitigate large sets of potentially malicious data and thwart cyberattacks.

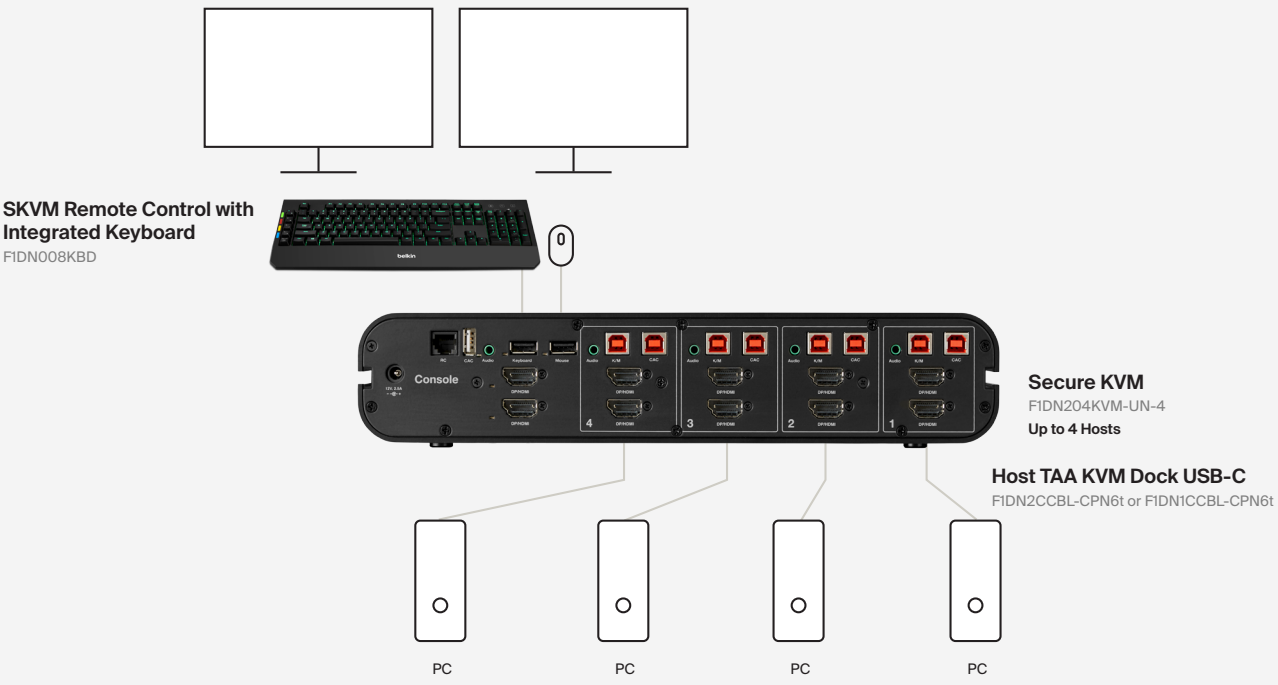
Practicing cyber hygiene means having strong detection measures in place and staying up-to-speed with endpoint protection, firewalls, and multi-factor authentication. Proper firewall and security protocols prevent malicious actors from accessing a remote server and stealing energy from multiple sites. Training energy company personnel on correct email procedures, handling sensitive data, and preparing for cyber incidents is critical for organizations. With substantial energy sector threats escalating, network operators are using a wide spectrum of technology tools to enhance digital resilience.

One preventative security measure adopted by sectors including government and financial services is to physically isolate networks and network assets. Creating an air-gap network limits access to mission-critical data to users with tightly controlled permission without ever posting it on the public internet or an unsecured LAN. This way, advanced signaling attacks that may compromise a desktop have no clear route to restricted systems with sensitive information. Vigilant energy companies are following the lead of other industries by integrating air-gap isolation as part of their cybersecurity strategy.

A critical, powerful piece of the solution is Secure KVM (SKVM) switches. SKVM switches have been utilized effectively to protect high security government and military networks for years and can be equally effective in helping meet CIP standards for maintaining guaranteed isolation between multiple classes of network assets. Further, SKVMs can enhance operator efficiency by eliminating desktop clutter and allowing one keyboard and mouse to control multiple systems, without the possibility of sharing any data between them.

These devices are a win-win solution for energy companies, helping meet CIP requirements while simultaneously delivering greater efficiency and effectiveness for operators.

Use Case Univeral 2nd Gen Secure KVM



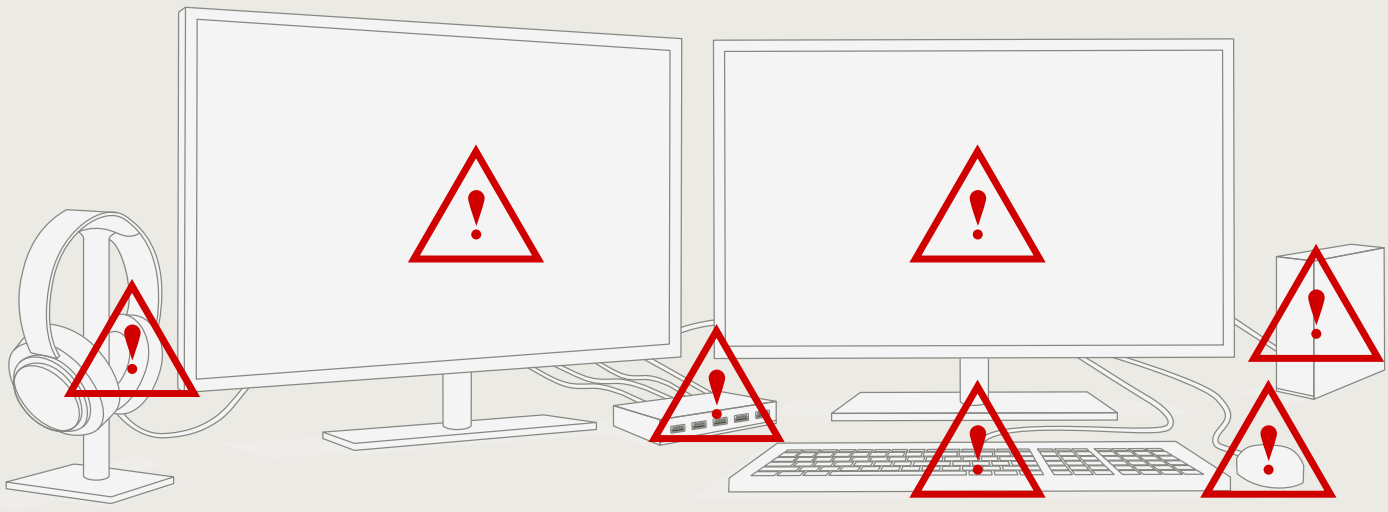
Secure KVM for energy companies

Many organizations in different sectors have mandated the use of NIAP-certified SKVMs and SKMs at operator stations to isolate sensitive systems from those exposed to the public internet and corporate intranets. The energy industry is implementing these solutions as well. With these switches, users have access to multiple computing systems from one desktop console, easily switching between various systems as their jobs require. This practice helps segregate secure and non-secure computing use. For example, an employee accessing internal email systems with a lower level of security can then switch and log into a more secure system to perform more sensitive tasks.

The chief advantage is to make certain that malware or viruses that may reside on a less-secure system, peripheral, or other IoT device never see a path to jump onto more critical systems. Additionally, it ensures operators are not encumbered by having to use multiple keyboards, mice, or monitors to perform their jobs. But not all KVM switching systems are secure. While they eliminate desktop clutter by allowing a single keyboard/mouse/monitor to be used to access multiple systems, unsecured KVM systems are at risk from both intentional and unintentional security vulnerabilities.

A typical cyber attacker generally probes networks for vulnerabilities, sneaks in and finds a way to hide from detection. During this process, the attacker is eavesdropping on user activity and learning as much as possible about network paths to more valuable assets. Anyone looking for a KVM should consider using a NIAP-certified SKVM as these are designed to block any path for signals to travel from one system to the other and create guaranteed air-gap isolation.

Possible threats from unauthorized and untrusted peripheral devices



Is your KVM solution secure enough?

Many unsecure KVMs lack the comprehensive security features that energy companies should require. Is your KVM hiding these vulnerabilities?

USB peripheral vulnerabilities

USB ports facilitate the high speed, bidirectional flow of data to and from the computer, making them a threat that can be used to gain control, intercept, and/or access resources beyond the PC itself and into any computer network attached to the PC. USB thumb drives are a popular way for social engineering threats to get introduced to enterprise systems and to copy and steal confidential information off servers. Only SKVMs force USB ports to be unidirectional (thus preventing copying of data) and filter commands to just HID information (thus blocking malware from being introduced into the system).

Video vulnerabilities

LCD monitors store display parameter data in the form of EDID, which could be exploited. EDID can be used to leak data from a secure network to an unsecured network by using the monitor display memory as a vehicle to transport data when being used with a KVM system. SKVM devices must prevent the reading or writing of display memory with a protected display interface to stop leakages.

Audio vulnerabilities

Integrated speakers on PCs and desktops can easily be hijacked and turned into microphones with no indication. As such, adversaries can easily eavesdrop on private conversations and closed-door meetings. SKVMs isolate the audio and ensure unidirectional flow for audio output.

Memory buffer leaks

KVM switches use onboard buffering to increase performance and have the potential to inadvertently leak data from channel to channel as they use the same switching processor for multiple ports. SKVMs have no buffering and utilize dedicated processors for each channel, thus eliminating the ability to leak data from one system to the other.

Support for smart card authentication

Two-factor authentication can be deployed as an additional layer in controlling who has access to sensitive data. SKVMs have fully isolated and dedicated Common Access Card reader ports that are compatible with the latest smart card technologies and allow an operator to use a single reader with multiple systems. The SKVM fully manages each session, ensuring that session tear down and log-in requirements are never violated.

Poor casing and design

Because so much security enforcement relies on the integrity of the KVM components themselves, it is important that purchasers take a close look at the internal and external components that go into the manufacture and design of the KVM switch. The external housing of the switch must be demonstrably tamper-proof, ensuring that it cannot be opened and modified at any time. The internal components of the switch must also be constructed to prevent tampering of any kind. Purchasers should make certain that they select only trusted vendors such as Belkin with proven security measures in the design, production, and handling of the product throughout their operations.

Choosing the right KVM solution for your energy company desktops

The National Information Assurance Partnership (NIAP), a government-sponsored program based within the National Security Agency, formulates specific requirements and recommendations to secure nearly every aspect of computing environments. The following are a few of the most concerning KVM scenarios that the NIAP testing program examines:

1. Users should not be allowed to connect unauthorized USB devices to the peripheral switch.
2. The KVM must prevent residual data transferred between peripheral port groups with different IDs.
3. Connection shall not be accessible by any other peripheral group with a different group ID.
4. The KVM should prevent a user error when setting shared peripheral connections from one computer system to a different one.
5. A connection, via the KVM, must not allow information transfer between computers.
6. Chassis design and supply chain must guarantee that the KVM switch has not been tampered or altered by any intermediary during transit and after deployment.

To continually improve security and reduce vulnerabilities in computing systems, NIAP directorates are used as the basis for testing and certifying commercial components. They also serve as a trusted security conduit between manufacturers and consumers of computer products used in secure environments.

One aspect of the NIAP program is the evaluation and recommendation for improvements in KVM switches. The agency's 2020 directorate, NIAP Protection Profile (PP) for Peripheral Sharing Devices (PSD) version 4.0 provides certification for products that have been vetted and found to conform to the strictest level of air-gap network isolation. As a part of its program, NIAP tests devices submitted by manufacturers for security compliance. Devices receive evaluation assurance levels that purchasers can use to confirm that any potential KVM device they purchase conforms to the NIAP recommendations.

When deciding on a SKVM product, NIAP is the single best resource to start your research. Additional information on the standard and a list of certified SKVM switches can be found on the NIAP web page at www.niap-ccevs.org/.

With cyberthreats on the rise, the energy sector ranks among prime targets for nation-state and state-sponsored terrorists, ransomware gangs, and lone wolves. The internal threat posed by improperly secured desktops in energy companies should be addressed with as much due diligence and vigorous security measures as firewalls, intrusion detection, and other external threat mitigations. Purchasers of KVM equipment must carefully weigh all the security and functional features of these devices to ensure the units provide the safest, most secure and user-friendly functionality to prevent any possible compromise of company and customer assets.

The Belkin Solution

Based in California, Belkin is among the world's most respected and successful computer component designers and manufacturers. For the past 30 years, Belkin has worked with energy industry leaders and IT specialists in energy work environments. Its SKVM switch solution is NIAP-listed and approved to the latest SKVM testing standard NIAP PP 4.0. Belkin provides the industry leading Secure KVM solution, and one of its exclusive innovations is the use of true data path isolation.

Optical data diodes

Isolated processors are integral to the Belkin solution, but its next-generation engineering takes a unique step forward. Introducing optical data diodes to provide unidirectional data paths eliminates the opportunity for data leaks or data capture on keyboards and mice. The Belkin optical diode connects input and output data paths with a signal that uses light in the following process.

First, it transforms input signals — such as keyboard strokes — into light signals. This light signal is sent along a dielectric channel where the light is captured on the output side of the circuit. Within the isolated diode, this light signal is then transformed back into an electric signal. This innovation goes far beyond isolated processor engineering because data to and from peripherals is never exposed to any form of electrical sniffing or capture. Signals pass, in light form, in one direction, eliminating the typical peripheral vulnerabilities of bidirectional signaling through copper.

Dedicated processors for every port

Belkin's SKVM switch contains dedicated, program-once processors with up to 16 emulators for each KVM, completely isolating the data path between every post and peripheral. Each component is hard-soldered to the electrical board and any removal or tampering renders the entire SKVM inoperable. Audio, USB, video, and peripheral ports support the latest standards and are isolated and secure.

Advanced audio filter

The Belkin SKVM switch secures audio with 40dB isolation up to 60KHz and an 8th-order elliptic filter. Advanced audio filtering requirements add significant technical complexity and cost, but block attacks enacted outside of human audible frequency range.

Tamper-proof design, packaging, and shipping

Belkin SKVM products are designed, built, and shipped in the U.S. under the strictest security. Every Belkin SKVM switch includes tamper-proof sensors and seals on external and internal components and on the outside shipping container. Customers are assured that the product is in its original, securely manufactured state from one end of the process to arrival at their facility. Any attempt to access the internal electronics of the SKVM will immediately render it permanently inoperable.

Advanced USB and cabling technology

USB signals are monitored in real-time and never allow unauthorized traffic or the attachment of unauthorized devices such as flash drives, disk drives, or unapproved peripherals. This is done in hardware out of the box and does not rely on domain profiles managed by system administrators. Belkin provides smart cabling that enables enterprises to connect their Belkin SKVM switch simultaneously to legacy VGA and newer high-resolution computers and monitors. In addition, the Belkin SKVM switches allow for CAC-reader connectivity on dedicated ports that are separated from the keyboard and mouse ports.

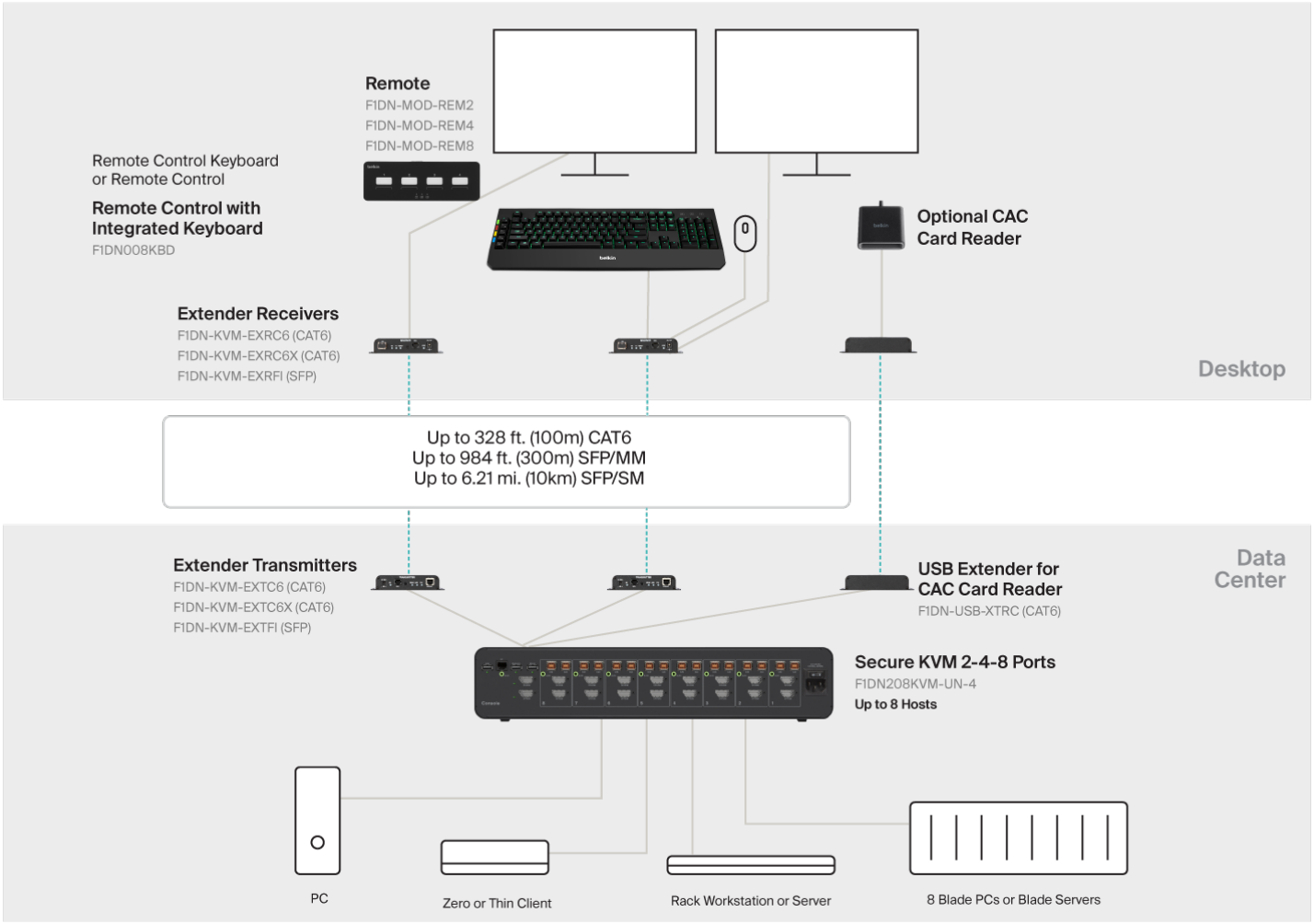
The color of efficiency

Customizable port coloring and naming on the front panel of the Belkin SKVM facilitates channel identification and reduces operator errors. When combined with the industry-first SKVM Remote Control with Integrated Keyboard, the SKVM can be located off the desk for a clean and decluttered workstation. The keyboard's LED backlighting and status indicators mimic the front-panel configuration of the SKVM to enhance operator channel and enclave awareness, minimizing operator error and exposure to uncleared personnel.

Universal video compatibility with combo connector and internal conversion

DisplayPort/HDMI combo connectors on each input and output allow the same SKVM to accommodate systems with DisplayPort, mDP, HDMI, DVI, VGA video outputs and modern and legacy monitors. This eliminates the need, cost, and uncertainties associated with external converters. This flexibility enables IT managers to deploy the same SKVM switch across their network and prolong the useful life of the SKVM simply by matching the appropriate Belkin cable with each connected system and monitor.

Security Use Case



Better than a zero or thin client — it's a no client

The combination of Belkin Secure KVM remote controls and extenders solves security and distance issues with groundbreaking technology that enables enclave switching control over long distances from the users' desktops. This valuable security feature allows the processing side and the SKVMs to be located in a locked, secure data center rather than on the desktop. Users have the flexibility to switch across multiple networks remotely even though there are no processing components at the desktop. This is ideal for remote desktops, conference rooms, command and control, server farms, and secure video access.

Other advanced features

The Belkin SKVM switch incorporates many other advanced features:

- Smallest SKVM/SKM in the market
- No memory buffering of any type
- Ultra-fast protected video display switching through EDID emulators
- Tested and validated multi-platform compatibility and support
- Intelligent Common Access Card switching to prevent unwanted system log-off
- Guard mode for keyboard-mouse (SKM) switching
- No keyboard or mouse delays when switching ports
- Integrated mounting track to allow under-desk or side wall mounting to improve desk space
- High-resolution support for graphic-intense applications used on larger displays
- Dual-monitor support to increase user productivity

The Belkin SKVM combines cutting-edge cybersecurity provisions, video performance and user experience to deliver a no-compromise solution for the most demanding applications.