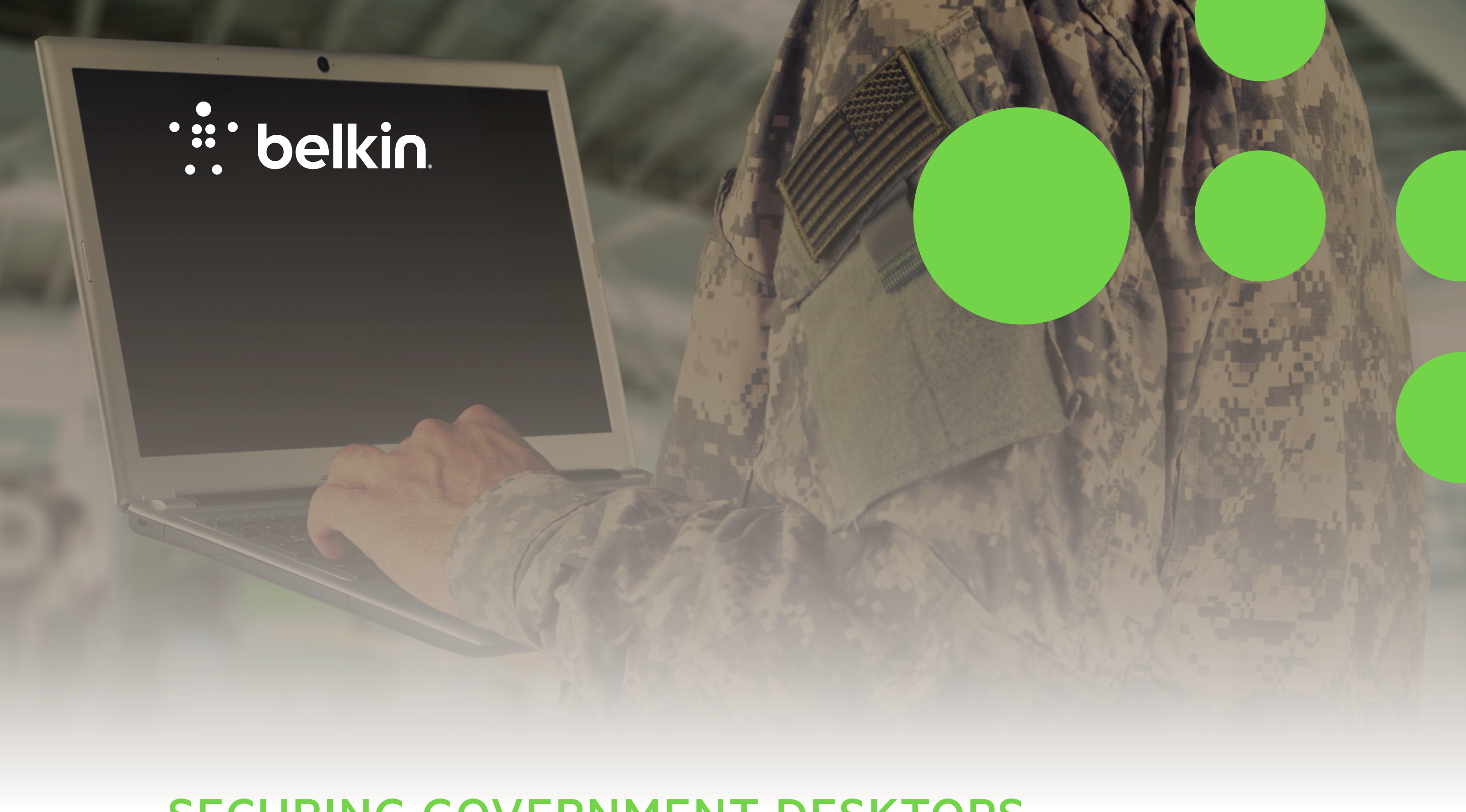


SECURING GOVERNMENT DESKTOPS
from Cyber Threats with the Latest KVM Technology

Foreign nations, terrorists, and cyber criminals see state and local government IT infrastructure as an extremely attractive target for data theft, attacks, and disruption. The stakes are high. Attacks have taken down entire systems, destroyed valuable equipment, and left many government agencies repeatedly vulnerable in countries throughout the world. The cost of remediation and repair after these attacks is significant and, even more importantly, the cost in terms of possible loss of life and confidence in key government systems and services, is unimaginable.

Secure keyboard-video-mouse (KVM) switches allow access to multiple computing systems at different security classifications, from a single desktop. This segregates secure and non-secure computing use and ensures a vulnerable element in the network cannot be used to breach more sensitive assets. It's an approach long used by the federal government. Now, it's becoming appealing for state and local government as well.

Cyber-based threats to state and local systems and critical infrastructure are evolving and growing. These threats can come from a variety of sources, including criminals and foreign nations, as well as hackers and disgruntled employees. And as long as they prove vulnerable to attack, the threats will continue to escalate. According to the Security Scorecard 2016 US Government Cybersecurity Report, "[w]hen compared to the cybersecurity performance of 17 other major industries, government organizations ranked at the bottom of all major performers, coming in below information services, financial services, transportation and healthcare."

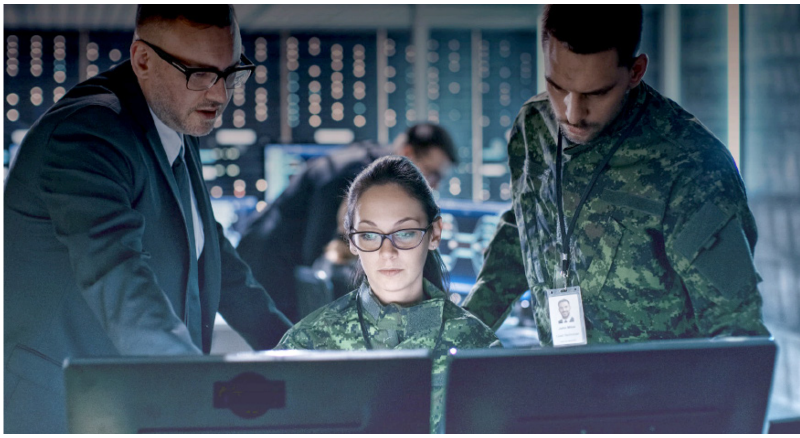
As part of a broader cybersecurity defense strategy, Federal intelligence and military agencies such as the CIA, NSA, FBI, and Defense Department physically isolate their networks and network assets, ensuring that the most mission-critical data is never exposed to the public internet and only accessible to those with tightly controlled permission. The air-gap network ensures that advanced signaling attacks that may compromise a desktop have no way of propagating to more sensitive systems as there simply is no route from one network to the other. Further, to protect against internal theft or maleficence, these agencies also filter or block exposed USB ports on servers and desktop computers to ensure the data integrity is never compromised.

It's time for state and local governments to follow the lead of these federal agencies and add air-gap network isolation to their cybersecurity strategy.

Secure KVM for State and Local Government

Many federal government agencies mandate the use of NIAP certified secure keyboard-video-mouse (KVM) switches at operator stations that need access to network assets at different security classifications. Using these switches, operators have access to multiple computing systems from one desktop console, easily switching between various systems as their jobs require. This system helps segregate secure and non-secure computing use. For example, a government 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 while ensuring operators are not encumbered with having to use multiple keyboards, mice, or monitors to conduct their jobs. Not all KVM switching systems are secure, however. 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 typically probes networks for vulnerabilities, sneaks in and finds a way to hide from detection, all while 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 secure KVM as these are designed to block any path for signals to travel from one system to the other and create guaranteed air-gap isolation.

Is your KVM Solution Secure Enough?

Many unsecure KVMs lack the comprehensive security features that state and local government systems 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 that the PC is attached. 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 of servers. Only secure KVMs force USB ports to be uni-directional (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 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. Secure KVMs 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. Secure KVMs isolate the audio and ensure uni-directional flow for audio output.

Memory Buffer Leaks

KVM switches use on-board 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. Secure KVMs 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. Secure KVMs 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 Secure KVM 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.

STATE AND LOCAL GOVERNMENT:

Choosing the Right KVM Solution

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 nor after deployment.

In an effort to continually improve the security and reduce vulnerabilities in computing systems used by the government, 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. These directorates are used as the basis for testing and certifying commercial components and serves 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 latest directorate, NIAP Protection Profile version 3.0 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 in making certain that any potential KVM device they purchase conforms to the NIAP recommendations.

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

Cyber threats are on the rise, with state and local government data and computer systems becoming a prime target for hostile foreign governments, terrorists, and cyber criminals. The internal threat posed by improperly secured desktops in government agencies should be addressed with as much due diligence and vigorous security measures as firewalls, intrusion detection, and other external threat mitigations. Government purchasers of KVM equipment need to carefully weigh all the security and functional features of these devices to make certain the units provide the safest, most secure and user-friendly functionality to prevent any possible compromise of government assets.

The Belkin Solution

Based in California, Belkin is one of the most respected and successful computer component designers and manufacturers in the world. Its secure KVM switch solution is NIAP-listed and approved to the latest KVM testing standard (NIAP Protection Profile 3.0). One of its exclusive innovations is the use of true data path isolation.

Optical Data Diodes

Isolated processors are an integral part of the Belkin solution, but its next-generation engineering takes a unique step forward by introducing optical data diodes to provide unidirectional data paths to completely eliminate 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

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

Tamper-Proof Design, Packaging, and Shipping

Belkin KVM products are designed, built, and shipped in the U.S. under the strictest security. Every Belkin KVM switch includes tamper-proof sensors and seals on external and internal components as well as 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 KVM 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 agencies to connect their Belkin KVM switch simultaneously to legacy VGA and newer high resolution computers and monitors. In addition, the Belkin Secure KVM switches allow for CAC-reader connectivity on dedicated ports that are separated from the keyboard and mouse ports.

Other Advanced Features

The Belkin KVM switch incorporates many other advanced features:

- 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
- No keyboard or mouse delays when switching ports
- Integrated mounting track to allow under-desk or side-wall mounting to improve desk space
- Customizable port-coloring to facilitate network identification
- High-resolution support for graphic-intense applications used on larger displays
- Dual-monitor support to increase user productivity
- Remote desktop controllers allow KVMs to be deployed away from operators without sacrificing usability nor introducing security vulnerabilities