THE BELKIN UNIVERSAL SECURE KVM

Simplify the Secure Desktop

Evolving Video Standards Create Complexity

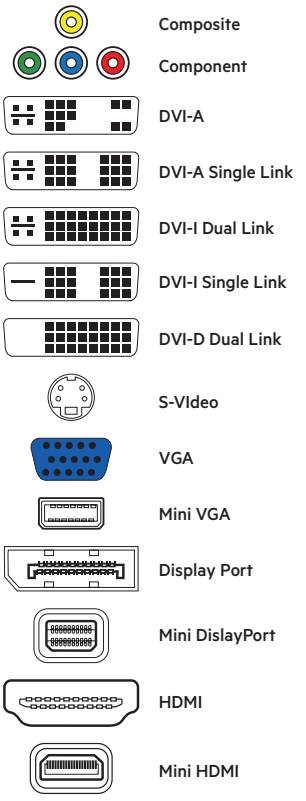
Look in any large workplace with computers and you're bound to come across a storage closet filled with old computer equipment. Broken keyboards, old monitors, out of date speakers. Inevitably you'll come across a tangle of old cables. VGA video cables that ruled in the age of analog video. Composite component cables. DVI cables. Even newer HDMI and DisplayPort cables.

As video standards evolve to allow for advanced functionality, such as 4K and higher video resolution, IT managers are left with a complex task: matching video hardware with the right cable type, across large scale updates and deployments.

This is an especially difficult problem for administrators at agencies that build "air gap" systems to isolate different platforms and networks as a security precaution against cyber breaches. Agencies often deploy secure KVM (Keyboard, Video, Mouse) switches to allow one set of peripherals to be used across different networks with differing levels of security. Not only does this maintain air gap separation, but it also reduces desktop clutter, increases efficiency, and helps save budget without needing to buy multiple sets of desktop hardware.

However, most secure KVMs are built to support a particular video standard while a large agency may have three or more different computing platforms with various video interfaces. This makes it extremely hard to properly manage secure KVM devices throughout their lifecycle, creating unnecessary burdens on IT departments and ultimately wasting time and budget. Deployment costs go up, IT managers lose the uniformity across their domain that they seek, and long-term maintenance costs become an unknown liability.

Proliferation of Video Display Technologies



The Belkin Universal Secure KVM: Solving Complexity, Maximizing Security

The Belkin Universal Secure KVMs have been engineered to solve the problem of incompatible video standards, simplifying the desktop experience for administrators and users.

The Universal Secure KVM features a combo-connector that can easily accept both an HDMI cable and a DisplayPort cable. As HDMI uses the same signal characteristics as DVI, the universal KVMs can support any input or output that takes DisplayPort, HDMI, or DVI on any channel.

The Universal Secure KVM combo connector works in tandem with another Belkin innovation, an auto-sense mechanism with two data paths for video to traverse. If the input is a DisplayPort source, the universal secure KVM will convert the video signal to an HDMI 2.0 compatible signal to meet NIAP requirements for disabling the DisplayPort Aux channel and physically eliminating any potential for bi-directional data transfer. If the input is HDMI or DVI, the signal is passed to the output circuitry unchanged. The same connector and auto-sense capability is also on the output side of the universal secure KVM.

If the monitor's EDID information indicates that the monitor is a DisplayPort monitor, the HDMI video signal is converted back to a DisplayPort format to drive the monitor. If the EDID signal comes back as HDMI then the Conversion to Displayport doesn't need to happen and the signal simply passes through.

With DisplayPort output, the Universal Secure KVM is capable of up to 4K resolution, 30Hz refresh rate video, making it more than suitable for high resolution video applications.

If the monitor's EDID signature indicates that it is an HDMI 2.0 compliant display, the HDMI signal is used to drive the monitor at up to 4K resolution/60Hz refresh rate, making the Universal Secure KVM the ideal solution for those looking for both high resolution and high-speed video. Finally, if the monitor indicates that it has a DVI input, the universal secure KVM uses the HDMI signal path and a passive HDMI to DVI cable to drive the monitor.

The ability of the Universal Secure KVM to accept DVI, HDMI, or DisplayPort video inputs eliminates the problem of having different computing platforms at a given site. As long as the computers can output a DisplayPort, HDMI, or DVI compliant video signal, the Universal Secure KVM can accept and process the traffic.

Cyber-based threats to government 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.

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 at the desktop cannot be used to breach more sensitive assets.

The universal plug-and-play capability on the output of the KVM also eliminates compatibility problems with monitors. If the monitor happens to still have a DVI connector, a simple HDMI to DVI cable can be used to passively drive video from the HDMI output of the KVM to the DVI input of the monitor. If the monitor accepts HDMI inputs, the universal KVM simply uses a HDMI to HDMI monitor cable to transmit the HDMI signal directly to the monitor. If the monitor has a DisplayPort input, the universal KVM uses a simple DP to DP monitor cable to drive the display.

> With the Universal Secure KVM, all of the complexity and cost of finding, qualifying, and managing external dongles and powered video converters is completely eliminated.

Future Proof Technology

The Universal Secure KVM fully supports new technologies, such as USB-C and mini-DisplayPort which are emerging as preferred standards on many new devices. Using a passive combo cable, the universal KVM can connect to sources or monitors with mini-DisplayPort inputs/outputs.

Since USB-C is used for video as well as USB traffic, Ethernet traffic, and even charging, it can be more susceptible to security breaches if not handled carefully. For security reasons, when a USB-C source is used, an active cable is needed to separate the video traffic and USB traffic before interfacing with the KVM. A USB-C to DisplayPort active cable creates the ideal solution to interface with sources that use USB-C to drive external monitors.

Simplify Complexity and Lower Total Cost of Ownership

Today, the lines between consumer, enterprise, multimedia, portable, and high-performance computing platforms are quickly fading. As these platforms evolve, so too do the cables that connect and power them. That evolution is usually a good thing. It allows advanced functionality and new features. But for agency IT administrators handling highly secure computing desktops, systems, and networks, trying to sift through and match differing hardware with the right cables across large deployments can introduce unwanted complexity, unnecessarily sapping resources and efficiency.

The Belkin Universal Secure KVM is engineered to make secure desktop computing simpler. It ends the problem of incompatible video and connector cables with plug and play capability that makes it easy for administrators to securely offer the most advanced computing hardware with complete flexibility and confidence throughout the entire technology lifecycle.

For more details on the Belkin Universal Secure KVM lineup, visit http://www.belkin.com/cybersecurity