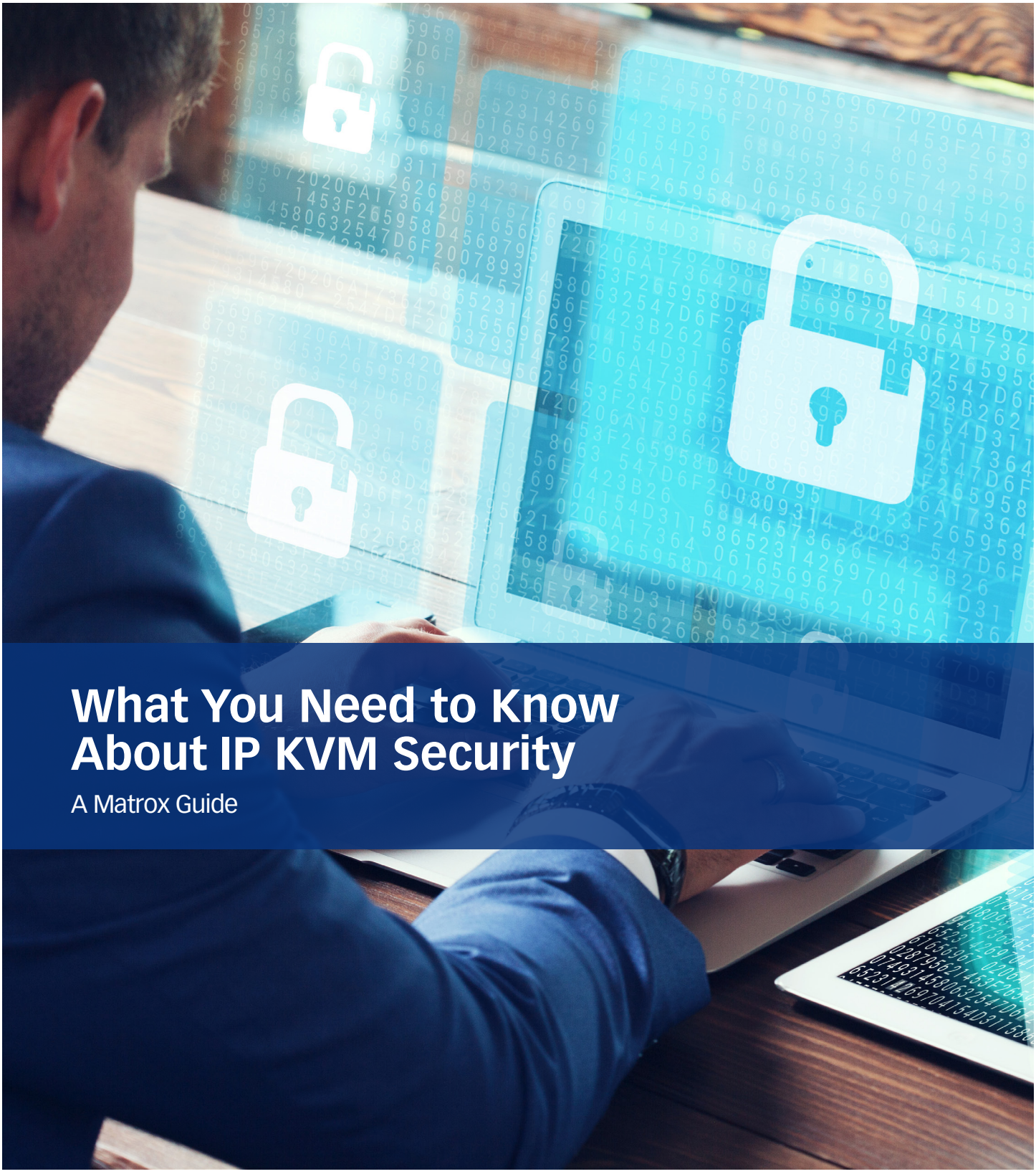


What You Need to Know About IP KVM Security

A Matrox Guide

matrox.com/video

matrox®

What You Need to Know About IP KVM Security

Securing critical environments and distributed workforces is becoming more critical due the rise of cyber-attacks and threats. This guide looks at the essential security elements needed when deploying an IP KVM solution.

Critical Systems

Security is one of the greatest concerns in critical environments, where knowledge workers monitor real-time data, analyze it, and make crucial decisions. Here and in many other environments, IP KVM extenders are deployed to secure computer assets in server rooms and enable users to control them from a distance. This helps prevent hardware tampering and interruptions to day-to-day operations. With the threat of cyber-attacks on the rise, it's more critical than ever to deploy IP KVM extenders that offer key security features in line with an organization's IT security policies and guidelines.

Information Security Principles (CIA Triad)

Information security principles guide organizations in developing policies, procedures, and processes to help maintain the confidentiality, integrity, and availability of business information.

- **Confidentiality** - Protects the privacy of the information, ensuring that only users with the correct privileges can see or use the information.
- **Integrity** - Prevents a third party from modifying the information before it reaches the destination, or destroying it altogether.
- **Availability** - Ensures the information is available when the user needs access to it, and that the overall network is resilient when there's a single point of failure.

Key Security Features

IP security has been around for several decades. Both data and telephone over IP have already gone through multiple generations of constant iterative improvements on security, which directly benefit IP KVM deployments. IP KVM extension and switching solutions transport audio, video, and control signals of the computer system to a remote user station over standard networking infrastructure. It's therefore important to select a solution that offers key security features to help protect the confidentiality, integrity, and availability of the systems that are part of the KVM network.

Encryption technologies

Encryption is a process whereby the IP KVM extender converts the A/V and/or USB signals into a secret code. Encryption thus prevents unauthorized access during transmission and protects the confidentiality of the transmitted signals during transport. The ability to encrypt packetized video, audio, and USB is considered superior to traditional baseband video transmission if there's a concern that someone might try to hack and snoop the feeds. IP KVM extenders that support encryption securely distribute audio, video, and USB signals over the IP network. They also maintain the integrity of the transmitted data by preventing third parties from modifying the content during transport.

IP KVM extenders protect the confidentiality of the signals transmitted by encrypting them during transport.

Advanced Encryption Standard (AES) is one of the most secure data encryption standards accepted worldwide. It was established in 2001 by the National Institute of Standards and Technology (NIST), which is a branch of the US government. Some IP KVM extenders use the AES standard for encrypting the data and passwords.

AES 128-bit and AES 256-bit standards use a symmetric encryption algorithm that uses a single key to encrypt and decrypt the data. In KVM applications, it's important to protect not only the audio and video signals but also the USB signals by encrypting keystrokes for entering passwords safely to safeguard confidential information.

Communication and control channels

IP KVM extender units communicate with each other and exchange commands—for example, when the receiver unit needs to switch and connect to another transmitter unit (source system). The commands between KVM devices need to be transmitted over a secure communication channel, such as Hypertext Transfer Protocol Secure (HTTPS), to prevent tampering with the KVM network by either rerouting signals or interrupting operation.

HTTPS runs over a Transport Layer Security (TLS) connection. TLS is an industry-standard protocol for secure communication over the network. It's a more secure version of Secure Socket Layer (SSL). TLS uses asymmetric encryption (both public and private) to protect the transported information, and relies on digital certificates to validate the identity of the transmitter and receiver devices. A secure communication and control channel within the KVM network is critical for maintaining the confidentiality and integrity of the extended A/V, USB, and control signals. This command-and-control layer can be further protected with permissions and passwords.

Permissions and passwords
Different security levels can be defined by setting up user permissions and passwords. User permissions allow administrators to define which source systems a user can connect to, and from which remote station they can access the systems.

Local users or domain-based users can be created through Microsoft® Active Directory® or other domain servers. Each user needs to log into the receiver unit to view the list of transmitter units or source systems they can connect to. IT professionals also recommend using strong passwords and changing them on a regular basis. Multi-level sign-on adds another layer of security—the user will be forced to sign into the KVM receiver device and source system.

Port-based authentication
A strong form of authentication is provided by the IEEE 802.1x standard—a port-based network access control for wired and wireless devices. IEEE 802.1x standard blocks rogue devices from communicating over a protected network and potentially disrupting operation. The network switch blocks traffic to and from any new device that wants access to the network until it's authenticated by a central server, typically a RADIUS (Remote Authentication Dial-In User Service) server. It verifies the identity of the new device and only then authorizes the device to join the network.

USB device authorization

Viruses and content-based malware can enter systems through infected USB storage devices or thumb drives. According to Honeywell's 2021 Industrial Cybersecurity USB Threat Report, threats propagated over USB rose from 19% in 2019 to just over 37% in 2020. "The increased severity of threat comes from increasingly multi-functional malware, which is capable of directly impacting target systems (20%), downloading stage-2 payloads (9%), or opening backdoors, establishing direct remote access, and command and control (52%)," Honeywell said in its report. The report goes further, suggesting that USB removable media are used to exploit air-gapped environments.

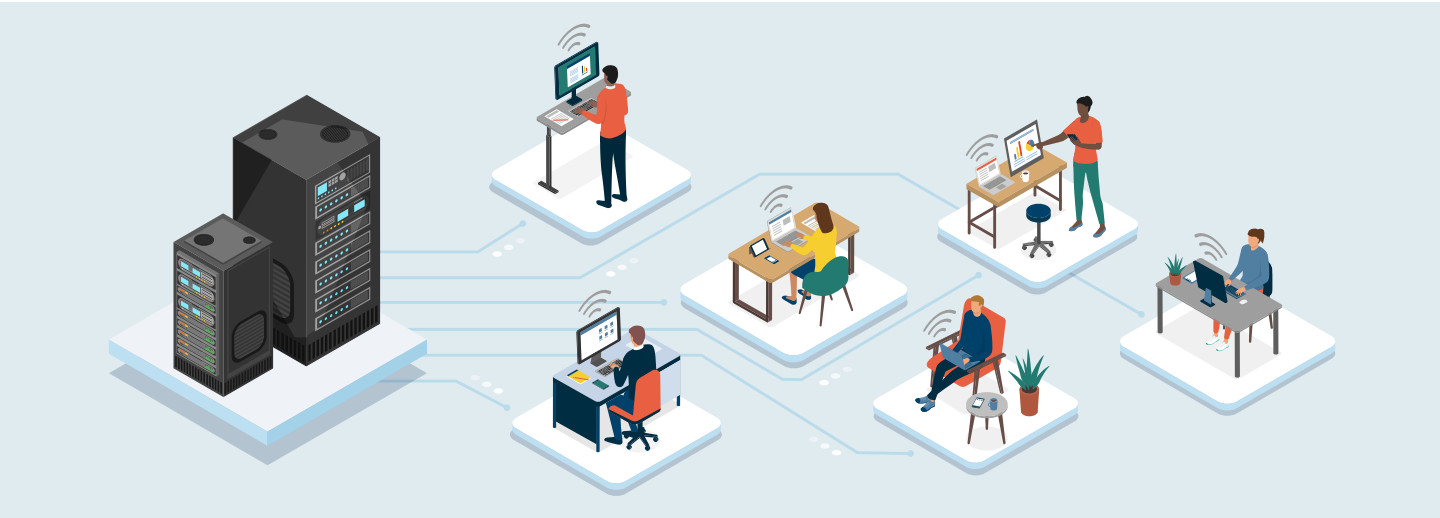
Blocking the operation of USB 2.0 devices on an IP KVM receiver is one way of preventing such intrusions. This is typically done at the product level, where the IP KVM extenders allow connecting to only USB HID devices such as keyboard and mouse, and block all USB 2.0 transactions. For applications that require USB 2.0 support, high-performance IP KVM extenders give administrators the ability to authorize select USB 2.0 devices based on serial number, make and model, and protect systems from attacks.

Network segmentation

A network is composed of various types of devices including computers, servers, IP KVM transmitter and receiver devices, among others. Each device has a different function, and transmits or processes information at different classification levels. The network infrastructure binds all these devices or nodes together—if one node gets infected, the attack can easily spread to the whole network.

Segmentation divides the network by function, with each having a different security requirement. Segmentation by function prevents an attacker from freely moving through the network and further spreading the attack. Networks can be logically segmented by function or traffic type through the creation of virtual LANs (VLAN) and firewalls—for example, the KVM traffic could be on a separate VLAN than the data traffic. Tighter security control is achieved by physically segregating the networks and having a separate infrastructure for each function. This means having a separate set of servers, switches, and routers for the KVM network.

In critical environments—such as military, financial, energy, and utilities markets—air-gapped networks are a common practice. In this scenario, the KVM network isn't connected to the public internet or unsecured LANs. Using fiber optic cables to route the networks also brings in another layer of security. Fiber optic cables are more difficult to snoop than CAT5, and support longer distances, thereby minimizing junctions and potential points of attack.



Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a network technology that creates a protected network connection when using public networks, such as the Internet. VPNs route internet traffic through a VPN tunnel, an encrypted connection between your device and an outside network location. Encryption makes it more difficult for third parties to track or intercept your online activities, even on public networks. A secure encrypted VPN connection is crucial for individuals who remotely access company systems or servers to minimize the risk of data leakage or unauthorized access to data.

Multi-Factor Authentication (MFA)

An additional level of security can be provided through Multi-factor Authentication (MFA). MFA is an authentication method that requires users to provide two or more verification factors to identify a user and gain access to access a resource via VPN. Through its strong identity security, MFA prevents potential attackers from accessing online resources even if the username and password are obtained by other means. As a second layer of authentication, digital certificates are used to identify devices and provide enhanced privacy protection.

Align with IT Security Policies

Although there's no substitute for knowledge and responsible deployment efforts when it comes to securing networks, IP KVM extenders with key security features help to align with an organization's IT security policies and procedures. The right IP KVM extension and switching solution is as secure, or even more secure, than traditional matrix KVM switching solutions. When banking can be done over IP, why not your desktop content?

Matrox Secure IP KVM Extenders

Matrox® offers secure, high-performance IP KVM solutions that integrate seamlessly into your existing IT infrastructure. Matrox Extio™ 3 IP KVM extenders are ideally suited for a wide range of environments, including utilities, transportation, military, defense, broadcast, and post production. Extio 3 delivers pristine 4Kp60 or quad 1080p60 4:4:4 video, keyboard, mouse, USB 2.0, and audio signals at low bitrates, and supports LAN, WAN, or Internet over a standard Gigabit Ethernet network. Engineered in Canada and designed to ease integration and provide operational flexibility for information sharing, fast decision-making, and intuitive collaboration, the Extio 3 IP KVM extender is ideal for a wide range of secure extension and switching applications.

Key Features	Extio 3 IP KVM Extenders
A/V encryption	✓
USB encryption	✓
Secure communication	✓
Password-protected environment	✓
User authentication	✓
Active Directory support	✓
Allow only USB HID devices	✓
USB 2.0 device authorization	✓
Multi-factor authentication	✓
IPsec VPN client	✓
Port-based authentication	—
Digital certificates	✓

About Matrox Video

Matrox Video is a global leader in video technology. Featuring a complete portfolio of best-in-class hardware, software, APIs, and SDKs, Matrox Video enables OEMs, system integrators, value-added channel partners, and end users to push the boundaries of video innovation. Serving the AV/IT, broadcast, and emerging markets for 45 years, Matrox Video is synonymous with quality, performance, interoperability, and support. Matrox Video's legal entity is Matrox Graphics Inc., part of the Matrox Group.

Contact Matrox

Montreal Headquarters: 1-800-361-4903 (North America), 514-822-6364 (Worldwide) | **video@matrox.com**
London Office: +44 (1895) 827300
Serving: United Kingdom, Ireland, Benelux, France, Spain, Portugal, Middle East, Africa
Munich Office: +49 89 62170-444
Serving: Germany, Austria, Switzerland, Denmark, Finland, Norway, Sweden, Central and Eastern Europe, the Baltic States, Greece, Turkey, Italy

For more information, visit **https://www.matrox.com/video**.