



KVM-over-IP Buyer's Guide

Key Factors for Optimizing Benefits and Achieving
Long-term Investment Protection

Table of Contents

Executive Introduction	1
True Anytime, Anywhere Access	2
Enterprise Class Security	3
KVM-over-IP Performance	5
Ease of Use	5
Appliance-based Solution vs. Server-based Solution	7
Total Cost of Ownership	7
Your Digital KVM Partner	8
Making the Right Choice in Digital KVM: A Decision Checklist ...	9

Executive Summary

KVM-over-IP technology is a cornerstone of any effective IT infrastructure management architecture. By providing anytime/anywhere, out-of-band access to system keyboard, video and mouse functions, a KVM-over-IP solution (also somewhat inaccurately referred to as "digital KVM") can significantly improve IT productivity, help ensure reliable delivery of critical business services, accelerate mean-time-to-repair and reduce total technology ownership costs. That's why almost every IT organization of any size needs KVM-over-IP capabilities.

However, it's also very important to select the right KVM-over-IP platform. There are significant differences between vendors' KVM-over-IP offerings. Choosing the wrong platform can limit its usefulness, drive up costs and even compromise security. So, to maximize returns on KVM technology investments, several critical factors need to be carefully considered.

In particular, KVM buyers should strongly consider the advantages of:

- ▶ Importance of true anytime/anywhere resource access
 - Multiplatform support
 - Browser/desktop compatibility
 - IP and dial-up access
 - No-cost, downloadable client
 - Non-blocked access via local ports
 - Full remote power control
 - Virtual media access
- ▶ Level of security and performance
 - Minimized vulnerability
 - External and internal access controls
 - Syslog support
 - Data encryption
- ▶ Appliance-based solutions
 - Ease of implementation
 - Total Cost of Ownership
 - Reliability and uptime
 - Dual Power Supplies
 - Greater Security
- ▶ Other factors that impact ROI – such as ownership costs and ease of use.

This KVM-over-IP Buyer's Guide provides a comprehensive overview of these key selection criteria. It addresses the full range of issues confronting KVM-over-IP buyers today – including access, security, performance and cost. IT organizations can use this guide to make more informed buying decisions and ensure that the companies they serve get maximum value out of every dollar invested in KVM-over-IP technology.

True Anytime/Anywhere Access

One of the primary value propositions offered by KVM-over-IP technology is the ability it gives systems administrators and other skilled staff to access key IT infrastructure assets at any time from anywhere. But here are some issues to consider in evaluating whether or not a given KVM-over-IP platform really fulfills this promise:

Multiplatform support

An enterprise KVM-over-IP solution must be able to support all server platforms and network devices in the environment. In fact, it's probably wise to select a solution that supports a broad range of popular platforms, including those which you may not currently be using. That's because such broad platform support provides IT organizations with the flexibility to implement those platforms should there be a compelling reason in the future to do so – without sacrificing remote manageability or forcing a "rip and replace" of the KVM system.



Browser/desktop compatibility

If your KVM-over-IP platform doesn't readily support a full range of browsers, it won't enable the true anytime/anywhere access your staff requires. It's particularly important to avoid the trap of accepting Internet Explorer (IE) as the de facto "standard" for desktop browsers. Many users and organizations, for example, are implementing Firefox and/or other alternatives to IE because of security considerations. A KVM solution that is primarily IE-based won't give IT the flexibility to adopt these alternative browsers.

It's also not wise to assume the presence of Microsoft® Windows® on every end-user desktop. Linux®, Sun® and Mac® operating systems are also widely used (particularly among the population of systems administrators), both within the enterprise and on the remote PCs and laptops that technicians will at times need to use to diagnose and solve problems while they're away from their desks. No company should spend tens of thousands of dollars on a KVM environment and then not be able to take advantage of it at some particularly critical moment because it's inaccessible to a sys admin running Red Hat on his or her personal notebook PC ... or from PDAs and other mobile devices.

IP and dial-up access

To further ensure immediate access to resources under all conditions, a KVM-over-IP solution should support both IP-based access over the network and dial-up connectivity. Obviously, the same network problem that a technician may be called upon to fix can also potentially prevent him or her from accessing the KVM switch via the network. In these cases, it's essential for the technician to be able to bypass the network and use the public switched telephone network (PSTN) to dial into the switch. This dial-up access protects the enterprise against network failures. Without such access, a vendor's claim of providing "out-of-band" access is invalid, as the shared pathway provides a single point of failure.

No-cost, downloadable client

Two other potential impediments to immediate access are the cost and on-demand availability of client-side software. Some KVM client licensing schemes drive up the cost of the solution based on the number of users, the number of platforms supported or some other parameter. These costly licensing schemes erode the ROI for the solution and may force the buyer to choose between the overall economy of the solution and universality of access. It's also important for the client-side software to be downloadable on demand. This enables technicians to gain access from any machine, even if it has never been used for that purpose. It also makes it easy to update the KVM client software at any time on an as-needed basis – without depending on some centralized desktop software management system or PC administrator.

Non-blocked access via local ports

In addition to being potentially constrained by limited browser and/or platform support, remote access to IT resources can also be "blocked" by technicians accessing resources locally. To prevent this, an effective KVM-over-IP solution should be designed so that a user accessing a local port does not block access by remote users. Therefore, companies should acquire KVM-over-IP technology that allows technical staff to access resources 24 hours a day, regardless of where they happen to be at the time. KVM solutions that don't fully deliver on this promise will not provide this essential capability.

Full remote power control

Sometimes BIOS-level access to a server is not enough. If a server is hung, the best course of action may be to simply do a hard reboot. To do this remotely, technicians have to be able to remotely control the power to managed devices. That's why it's important to select a KVM-over-IP solution that provides power on/off functionality and other remote power management capabilities.

Virtual Media

The benefit of Virtual Media is that it allows the mounting of remote drives/media on the target server to support software installation, remote booting and diagnostics. It's a useful tool for an administrator to access CD/DVD, USB, local and remote drives to install software, run diagnostics, do backups, even boot from remote media.

Enterprise-Class Security

In addition to reducing IT operating costs and increasing service uptime, KVM-over-IP can enhance enterprise security by allowing IT to more tightly control physical access to critical systems and data center facilities. In addition, increasing organizational focus on compliance with SOX, HIPPA and other regulations is providing increasing scrutiny on the security and manageability of the IT infrastructure. It is also important to recognize that any vulnerability in a KVM-over-IP solution's architecture can potentially expose the enterprise to unacceptable risk. That's why the security attributes of KVM-over-IP solutions are extremely critical in any purchasing decision.



Minimized vulnerability

One of the most important aspects of KVM security is elimination/remediation of known vulnerabilities. As mentioned above, this is one reason that many IT organizations are now choosing to use a browser other than Internet Explorer for KVM-based access to critical computing resources. In some cases, it is even causing the IT function to avoid using Microsoft Windows as a server platform.

This doesn't mean that Microsoft's client and server operating systems can't be used as components of a KVM solution at all. However, it typically takes quite a bit of additional administrative time and effort to track the continuing stream of security bulletins relating to Microsoft platforms and to install the appropriate patches. So an alternative approach that uses an embedded, hardened operating system in its KVM-over-IP devices and an intrinsically more secure browser (such as Firefox) may be more cost-effective, in addition to being more secure.

External and internal access controls

Another important component of KVM security is user authentication and authorization. Ideally, a KVM solution should leverage existing enterprise authentication mechanisms, such as Active Directory®, LDAP, TACACS and/or RADIUS. This simplifies administration while protecting the system from unauthorized use.

At the same time, KVM systems should provide their own supplemental mechanisms for authenticating users and authorizing access to specific resources. This is critical in the event that connectivity to an enterprise directory server becomes unavailable. Again, it is critical that the availability of KVM capabilities not be threatened by infrastructure breakdowns – since those are the very times when KVM is the most valuable. Failover capabilities are thus absolutely essential for a KVM system.

Syslog support

To ensure that technicians can easily audit system and user activity, enterprise KVM solutions should fully support syslog functions. Because syslog is so widely used as a standard for system access logs, it is natural to assume that all KVM solutions support it. But this is not the case. Buyers should confirm syslog support before making a final KVM selection.

Strong data encryption

A secure KVM system will encrypt all signals between managed devices and KVM clients (i.e. keyboard, mouse and video) with adequate encryption schemes such as AES or RC4 128-bit encryption. Encryption of the video signal is particularly important, since any view of an administrative screen could be of enormous potential value to an intruder and provide a context for hijacked keyboard and mouse signals. Video encryption should also be highly efficient, since users may be tempted to turn it off if it hogs bandwidth and impedes performance. Security and encryption should not be thought of as "optional."

Other security measures

KVM-over-IP systems should also provide other security features as required – including strong password checking, inactivity timers, etc. These protections are critical for ensuring that the KVM implementation does not add to the overall level of IT-related risk as it provides its essential operational benefits.

KVM-over-IP Performance

The value of a KVM-over-IP solution can be seriously diminished if its performance and responsiveness do not meet users' needs. Performance can be an especially problematic factor if IT staff has to access managed systems via low bandwidth links and/or over connections that are congested with application traffic.

Absolute mouse synchronization

Tight synchronization between movement of the mouse and movement of the screen cursor is critical for technicians to use KVM technology effectively. That's why KVM decision makers should closely assess the absolute mouse synchronization and signal delay characteristics of potential solutions under real world conditions. Synchronization should be tight and consistent across LAN, WAN and dial-up connections.

Bandwidth-adaptive video compression

A seamless KVM experience is obviously contingent upon fast video performance as well. However, to maintain this performance under constrained bandwidth conditions, it may be necessary to compress the video stream appropriately. Ideally, a KVM system will make such adjustments automatically to optimize the end-user experience and ensure that unacceptable lag doesn't adversely impact IT operations. Users can also be given a choice of color depth (i.e. black-and-white, grayscale, 4-bit color and 15-bit color) so that they can exchange video quality for performance as necessary.

Ease of Use

While KVM solutions are primarily used by skilled IT professionals, that doesn't mean ease of use should not be a factor in the purchase decision. Technicians can spend hours every day using KVM to manage critical IT resources. A KVM system that is difficult or clumsy to operate will significantly impede their productivity and prevent the full potential business value of the system from being realized.

Consistent User Interface

KVM solutions should support a consistent, Web-based user interface across local and remote access.

Full-screen display

A good KVM system will automatically sense the video characteristics of each managed resource and adjust the user's desktop display in order to present a full-screen view. This full-screen view eliminates the need to scroll around a screen unnecessarily. Scrolling slows technicians down and undermines their productivity. Productivity is also compromised if technicians have to fiddle around with screen settings every time they switch to a different resource in order to get a full-screen view.



Screen sizing and tiling

Because technicians often have to manage multiple resources and utilize multiple applications simultaneously, an ideal KVM system should enable them to flexibly resize and tile multiple full-screen views on their desktops. This flexibility enables them to work quickly and efficiently without "togglng" between various windows.

Keyboard transparency

Most KVM systems make extensive use of macros in order to differentiate keyboard commands directed at the managed system from being treated as local commands for the user's desktop PC. This can make use of KVM clumsy and extend the learning curve for remote systems administration. Instead, a good KVM system will enable administrators to use their desktop keyboards to manage remote systems just as if they were sitting at those systems – without new and unfamiliar macros.

Other usability factors

Several other characteristics may distinguish the usability of one KVM system over another: the intuitiveness of the GUI, the ease with which multiple technicians can collaborate simultaneously on the troubleshooting and management of a single target system, the speed with which remote sessions can be initiated. All of these are important factors in optimizing and simplifying the day-to-day productivity of IT staff.

Total Cost of Ownership

Cost is obviously a key consideration in the selection of a Digital KVM platform for the enterprise. A variety of factors influence the total cost of ownership for KVM. All of these factors must be taken into account to ensure that KVM implementation is as economical as possible.

Cost per port

Every organization has its own requirements for remote access in terms of both the number technicians requiring access and the number of devices being managed. The key to meeting these requirements cost-effectively is to minimize the cost per port. Larger organizations will want to buy devices with a larger number of ports, so they can buy fewer devices, take up less rack space and lower environmental requirements. Smaller organizations will want to start off with fewer ports and add incrementally as their needs evolve. Ideally, then, the solution should be available in a flexible range of port configurations to precisely meet current needs – as well as to flexibly scale to meet future connectivity requirements.

Cost of entry

Some KVM solutions require the purchase and implementation of a full, enterprise-class KVM management system from the very outset, even if there is only one KVM switch to manage. These server-based solutions obviously drive up the cost and complexity of the KVM implementation. That's why first-time buyers should consider a solution that gives them the flexibility to add management functionality as they see fit – so that they can incrementally build out their KVM environment according to their own evolving needs.

Licensing and price structure

KVM buyers also need to understand how licensing costs affect their overall price structure. Charges for additional users, platforms and features can quickly inflate the cost of a complete KVM solution – especially if some of those incremental needs are not fully anticipated at the time of original purchase. Also, some KVM vendors include a maintenance/renewal fee as part of their price structure. To protect themselves from this type of "price creep," KVM buyers should select solutions that bundle all key features, don't charge extra for incremental client access and don't require maintenance fees.

Ease of installation

In addition to capital costs, KVM buyers need to consider the cost and effort of installation in assessing overall TCO. As noted in the following section, solutions that require setting up a separate authentication server increase initial implementation costs and potentially delay the time-to-benefit. In addition, automated configuration capabilities such as those described above for accommodating different screen parameters and bandwidth constraints will also help lower total implementation costs.

Lifecycle costs

Finally, KVM buyers need to consider ongoing ownership costs when comparing TCO. These costs include systems administration, the addition of incremental capacity, security management and end-user support. The ownership costs are affected by licensing structures, device architecture, ease-of-use, maintenance and other factors. They also include the costs of acquiring and maintaining additional servers that might be required in order to manage the KVM infrastructure.

In other words, KVM buyers should consider a full range of lifetime cost factors when determining which solution will be most economical and effective for their organization over the long term. These cost factors, combined differentiated features and productivity benefits, are critical to understanding the overall KVM-over-IP business case.

Appliance-Based Solutions vs. Server-Based Solutions

One of the biggest decision-points facing any KVM-over-IP buyer today is whether to purchase an appliance-based or server-based solution. Appliance-based solutions are self-contained units that provide a complete package, including specialized server hardware and KVM software running on a hardened operating system. Server-based solutions are installed on general-purpose, commercially available computer systems. The choice between appliance-based and server-based solutions is important for a variety of reasons.

Ease of implementation

Appliance-based solutions can offer out-of-the-box implementation that eases initial deployment and ensures immediate realization of KVM benefits. This is especially true of appliance-based solutions that have strong auto-configuration features. Server-based solutions, on the other hand, require specification, purchase and installation of the appropriate hardware, as well as the time-consuming installation and configuration of the KVM software on that hardware.

Total cost of ownership

When a KVM solution uses a general-purpose server platform, the server and its associated software and operating system require the same "care and feeding" as any other application. This includes server administration, OS upgrades and patches, and optimization of the configuration to support the KVM software. Those costs are often several times that of the server hardware itself. With an appliance-based solution, these overhead costs are eliminated – making the solution less expensive to own and operate over time.

Reliability and uptime

Appliance-based solutions are specifically designed for non-stop KVM operations. Plus, because they require less manual administration, they introduce less opportunity for human error – which is a primary cause of system downtime. Appliance-based solutions are therefore more reliable than those running on commercial servers.

Dual Power Supplies

For increased reliability and redundancy, KVM switches should have dual AC inputs, dual power supplies and automatic failover to support the redundant power distribution used in enterprise data centers. If a power supply fails, users should be notified via front panel LED, SNMP trap or log message.

Greater security

A KVM appliance running a hardened OS kernel is always less vulnerable to attack than a general-purpose server running an OS that is well known to the hacker community. In fact, because it does not use an easily identified OS such as Windows, the internal functions of such an appliance are extremely opaque and inaccessible to any unauthorized user inside or outside the IT organization. Appliance-based KVM solutions are therefore far more secure than their server-based counterparts.

Your Digital KVM Partner

Finally, above and beyond the technical specifications of any specific KVM-over-IP solution, buyers must also take into consideration who they're buying that solution from. Any purchase of KVM technology carries with it a business relationship with a KVM vendor. KVM buyers therefore need to assess the quality of that vendor as an ongoing partner in their long-term IT strategy.

Stability

Because KVM technology directly touches an organization's most critical IT assets, it's important to select a KVM vendor with a proven record of long-term performance and integrity. That performance and integrity should manifest itself in strong relationships with enterprise customers that have lasted a decade or more.

Vision

Because enterprise computing architectures are constantly evolving, it's important to partner with a KVM vendor that has demonstrated an ability to accommodate and respond to that evolution. Otherwise, there is a risk that today's KVM solution may become obsolete before it is fully depreciated.

Completeness of product line

Because KVM requirements change over time as the business changes, it's essential to choose a partner whose offering ensures long-term flexibility. Ideally, the partner will offer a modular, "building block" architecture that includes a centralized management system that can integrate both digital and analog KVM technologies – as well as serial console and power control – into a single logical network with a single sign-on to a single IP address.

Commitment to backward compatibility

Of course, the continued evolution of a vendor's KVM solutions isn't of much value if it requires the scrapping of existing investments. That's why KVM buyers should make sure that their KVM partner has demonstrated a historical commitment to providing backward compatibility across its product lines. When a vendor abandons customers and forces them to "rip and replace" their KVM infrastructure before its economic life has elapsed, this dramatically drives up the TCO.

Service and support

Responsive service and support are essential components of any relationship with a technology vendor. KVM buyers should make sure that their KVM vendor can respond quickly and effectively to technical support needs across all communication channels – including phone, e-mail and the Web.

Making the Right Choice in Digital KVM: A Decision Checklist

Obviously, many factors differentiate one KVM-over-IP solution from another. While none of these factors may individually provide a justification for selecting one solution over another, cumulatively they have a major impact on your business and total ROI.

The following checklist summarizes the key KVM buying decision-points covered in the previous pages:

Access

- Does the solution support all required desktop and server operating systems?
- Does the solution enable access from the leading desktop browsers?
- Does the solution offer true out-of-band support with both IP and dial-up access?
- If dial-up access is provided, is the vendor's compression technology good enough to make it usable?
- Does the solution provide a no-cost, downloadable client?
- Does the solution provide a Java-based client?
- Does the solution provide non-blocked local port access?
- Does the solution provide full remote power control?

Security

- Is the solution secure against common Windows vulnerabilities?
- Does the solution provide both internal and external authentication capabilities?
- Does the solution support syslog access?
- Does the solution provide full encryption of keyboard, mouse and video signals?
- Does the solution provide other key security measures such as password checking and inactivity timers?
- Does the solution leverage your existing authentication and authorization systems such as RADIUS, TACACS, Active Directory and LDAP?

Performance

- Does the solution provide absolute mouse synchronization?
- Can the solution automatically adjust video resolution to avoid a time lag when switching from one system to another?

Ease-of-use

- Does the solution provide full-screen video display, so no scrolling is necessary?
- Does the solution allow user to resize displays in any size, from full screen to thumbnail?
- Does the solution provide keyboard transparency which minimize the use and requirements of keyboard macros?
- Does the solution maximize usability with an intuitive interface, simplified collaboration and other relevant features?

TCO

- Does the solution offer a full range of port densities to cost-effectively meet the specific needs of the business?
- Does the solution force the purchase of more technology than is necessary?
- Do the licensing and price structure protect against "cost creep?"
- Is the solution easy to install?
- Is the solution cost-effective to own and operate over time?
- Does the vendor have a history of providing "backward compatibility" for its solutions as it introduces new technology, or does it require "ripping and replacing" the solution, reducing their economic life-time and driving up the TCO?

Appliance-based vs. server-based

- Will the solution install easily and deliver fast time-to-benefit?
- Will the solution require extensive ongoing systems administration?
- Is the solution sufficiently reliable?
- Does the solution use a hardened, secure OS?

Partner

- Is the solution offered by a stable partner with a solid industry reputation?
- Is the solution offered by a partner with the vision to evolve as information technology evolves?
- Does the partner have a complete, modular solution including serial console, remote power control and analog KVM?
- Has the vendor demonstrated a firm commitment to backward compatibility?
- Can the vendor deliver responsive service and support?

KVM-over-IP technology is extremely valuable in reducing the cost of IT operations and ensuring optimum service levels for critical business applications. By choosing the right KVM-over-IP platform, IT decision makers can fully reap these powerful benefits today – while avoiding unnecessary spending and a variety of management headaches down the road.

About Raritan

Raritan, Inc. is a leading supplier of solutions for managing IT infrastructure equipment and the mission-critical applications and services that run on it. Raritan was founded in 1985, and since then has been making products that are used to manage IT infrastructures at more than 75,000 network data centers, computer test labs and multiworkstation environments around the world. From the small business to the enterprise, Raritan's complete line of compatible and scalable IT management solutions offers IT professionals the most reliable, flexible and secure in-band and out-of-band solutions to simplify the management of data center equipment, applications and services, while improving operational productivity. More information on the company is available at Raritan.com.