



## White Paper

# KVM over IP and Enterprise Security: Safeguarding Access to Your Critical IT Infrastructure

### WHAT'S INSIDE

**Hub and spoke failover architecture, exit macros and other security elements you should insist on in a KVM over IP switching system**

### EXECUTIVE SUMMARY

Information security is a primary concern for every IT organization and every business. No company can afford to have its critical systems disrupted for any length of time. No company can afford to have proprietary data or valuable customer information fall into the wrong hands. And no company can afford to be in non-compliance with today's increasingly stringent regulations governing data protection and retention.

Because security threats come in so many forms – and because it's never wise to rely on a single point-of-protection when guarding against these threats – effective information security requires a multi-layered approach. Physical, logical and operational security are therefore all essential ingredients for a successful enterprise security strategy.

KVM switching solutions provide secure remote data center management, but they also should integrate with the existing security infrastructure. KVM over IP switching systems uniquely enable security managers to control physical access to critical data center resources – as well as power systems, environmental controls, security devices, branch office servers and other distributed IT assets. KVM switching ensures that only authorized personnel can perform critical management operations on servers or network devices.

The KVM platform that any enterprise chooses to implement must itself be extremely secure. It must offer appropriate protection from exploits launched from outside the enterprise. It must have effective controls to prevent unauthorized access by internal users. And it must safeguard critical systems from the dangers that can result from human error.

The Avocent KVM platform is especially well suited for supporting enterprise security objectives. The DS Series KVM over IP switching systems provide field-proven security features and benefits to ensure that KVM functions themselves are not maliciously or inadvertently used to compromise critical enterprise assets. These benefits include standards-based authentication, multiple encryption modes for remote sessions, exit macros, and the comprehensive event-reporting capabilities that security managers need to properly audit the end-to-end IT environment.

When considering the benefits a KVM over IP system offers, a company needs to consider the KVM security architecture to ensure integrity of its critical IT resources. Avocent is the only KVM provider with hub and spoke failover architecture and delivers powerful technology for achieving security, while simultaneously generating significant ROI as a result of performance and productivity gains. This unique combination of optimized security and streamlined IT access and control makes Avocent KVM over IP switching a must-have for today's security-conscious IT-centric organization.

### **The critical role of multi-layered KVM switching in enterprise security**

IT organizations face a growing number of cyber-security threats. These threats continue to evolve in their virulence and sophistication. They also represent a greater business risk than ever before, since productivity, revenue and customer relationships depend more than ever on the health and availability of critical IT services.

Fortunately, enterprise defenses are also evolving. New technologies and best practices are helping IT better protect critical services. By implementing the right combination of technologies and practices, IT organizations can effectively minimize risk without putting undue strain on their finite financial and human resources.

One particularly important component of any enterprise defense strategy is the implementation of a "layered" security model. Under a layered model, security tools and techniques are applied across multiple tiers of the enterprise architecture. While the specific structure of these models may vary, they generally segment the enterprise architecture into some combination of perimeter, network, host, data and/or application tiers. Perimeter defenses, for example, typically include firewalls and anti-virus email gateways. Network defenses may include network-based intrusion detection systems and access/authentication controls. Data-layer defenses may include encryption and another set of access/authentication controls.

There are several reasons that a layered security model is compelling. First, it prevents critical business assets from being put at risk because of the failure of any single security measure. Second, it creates additional work for potential intruders – thereby increasing the likelihood that they will move on in search of easier targets. Third, it often creates synergies between layers that can effectively thwart exploits that might otherwise be successful. This is the case when an application-level access control tool blacklists the IP address of someone who makes too many password guesses and then forwards that banned IP address to a network-level defense to prevent additional attempts on other systems.

Layered models may also segment security measures into physical, logical and operational components. Again, these multiple layers create redundancies and synergies that help to more effectively protect the enterprise from both the malicious and accidental threats that can originate internally and externally.

KVM technology is a critical component of any such layered security strategy. At the logical/network layer, KVM acts as an internal “firewall” to prevent unauthorized users who have penetrated perimeter defenses from gaining access to data center resources. At the same time, KVM provides host-layer security from both a physical and logical standpoint. Physically, the technology allows host resources to be placed in a secure environment so that their use can be restricted to those users who are authorized via the KVM system’s remote access mechanisms. Logically, it protects host resources by providing the means by which users are given access to specific systems for specific tasks.

The control of physical access to critical servers is particularly important in light of current compliance requirements. For example, a corporate data center may have its database servers in the same physical location as its email servers. Allowing email server administrators into the same room as database servers without supervision is likely to compromise Sarbanes-Oxley policies. With KVM over IP switching, on the other hand, email server administrators can be granted the console-level access they need without compromising those policies.

Combined with associated best practices – such as ensuring that the rights of technicians who leave the company are rescinded in a timely manner – KVM switching provides a uniquely powerful and effective way of ensuring that critical computing resources are not compromised by unauthorized access. As such, it is the ideal complement to the other classic components of a layered security model such as firewalls and admin-level passwords.

### **Leveraging industry-standard security**

Of course, in order to provide such valuable security capabilities to the enterprise, a KVM over IP system must itself be highly secure. Not all IP-based switching systems are created the same. A significant differentiator is the layered security model. Choosing the wrong KVM system that allows appliance-based access could lead to a security breach. Data could be corrupted or stolen. Critical business services could be compromised. And, theoretically, a malicious intruder could use a hijacked KVM system to continue “eavesdropping” on sensitive IT activities over an extended period of time.

Effective security is therefore an essential consideration in assessing, implementing and managing KVM over IP technology.

Just as enterprise security as a whole requires a multi-faceted approach, so too does KVM security. The following are the key “facets” to consider when evaluating KVM over IP system security models.

***Authentication*** - KVM authentication mechanisms are critical for restricting access to authorized users. Ideally, an industry-accepted authentication method (such as Active Directory, Lightweight Directory Access Protocol (LDAP) or NT) should be used in conjunction with the KVM system’s own access control to ensure that the specific user is entitled to access each specific device. You should be able to assign device-level rights based on a user’s name so that administrators have access to more devices than an entry-level technician.

Additional security can be achieved through a key exchange between the KVM appliance and the client access software. Best practice security also requires that a time limit be put on this exchange.

To streamline administration, a centralized engine should be used to manage access rights across all enterprise locations. This eases security-related workloads and ensures that common security policies are implemented for all devices. Many organizations will want to leverage their existing LDAP infrastructure so that the administration of their KVM security is fully integrated with their overall enterprise security processes.

**Encryption** - Encryption of data transmissions eliminates the possibility of critical systems being compromised by the interception of legitimate KVM sessions. The level of encryption that can be used is contingent on the ability of the OS, device and/or browser involved. Best KVM security practices should include 128bit SSL encryption and 3DES encryption – which encrypts, decrypts and re-encrypts data with three separate keys. Ideally, the KVM system will automatically implement the highest level of encryption that the environment can support in order to optimize security.

**Failover** - In addition to providing protection against internal and external security threats, a secure KVM system must also be capable of preventing critical business processes from being interrupted because of power failures, fire, severe weather and other cataclysmic events. If a KVM system can be disrupted by a single point-of-failure, it may expose the business to unacceptable risk. To eliminate this risk, a KVM system should offer mirrored, redundant authentication capabilities with fully automatic failover functionality. In the event that a primary server goes off-line for any reason, the secondary server should fully support KVM access to all target resources with exactly the same sets of rights and privileges in place.

**Auditing** - Auditing mechanisms are also critical to the maintenance of KVM security. Security managers should have access to highly granular logs of all KVM activity. These logs should provide appropriate native reporting and/or be exportable into popular reporting applications so that anomalies and trends can quickly be detected. In particular, security managers should continually monitor events such as failed authentications and attempts to gain access beyond authorized permissions. Comprehensive audits should also be performed regularly in conjunction with other security best practices.

### **The Avocent advantage**

Avocent KVM over IP solutions offer a field-proven security architecture used by thousands of customers worldwide in complex IT environments. Avocent continues to enhance its security mechanisms in response to evolving threats and changing approaches to enterprise security management.

Avocent DS Series KVM over IP solutions, including DSView<sup>®</sup> 3 management software, provide several key advantages for IT organizations seeking to ensure the absolute integrity of critical computing resources while gaining the security and productivity advantages offered by KVM technology.

**Reliable failover capability** - Avocent introduced the hub and spoke model for IT data center device management. The hub and spoke engine provides a solid failover system.

DSView servers are synchronized in real time; if the “hub” server suffers a problem or shuts down for routine maintenance, a “spoke” server becomes the primary without loss of data or transactions. A customer can prepare for disaster recovery or any outage with up to 15 separate, remote spokes. All components are kept in sync ensuring the integrity of the entire system.

**Secure credentials and authentication** - Upon opening DSView 3 software, users are only presented with a view of the resources for which they have been granted access. When a user clicks on a resource to establish a KVM session, the DSView server first authenticates the user. The DSView server then retrieves the information necessary to establish the KVM session from the targeted resource and forwards that information to the DSView client. Only then can the DSView client connect via the KVM switch to the resource.

This “moderated connection” model is widely accepted for securing communications (as, for example, with H.232 for VoIP). Also, it is important to note that the moderated connection simply establishes communication between the DSView client and the targeted resource. The user must still use secure credentials to actually log on to the resource. Thus, in addition to enabling layered security, Avocent DS Series solutions employ a layered security model.

The Avocent DSI5100 IPMI proxy appliance, also managed by DSView 3 software, provides a browser-based, out-of-band interface to securely monitor and control power and system health on IPMI-enabled servers. DSView 3 software allows access to these servers only after user authentication and uses the same interface used for KVM, serial and external-managed power connections.

**Secure communication process** - The DSView client communicates with the DSView server using a standard Web browser. The communication protocol used between the client browser and the DSView server is the HTTPS protocol. The TCP port used is configurable on the DSView server and must be specified in the browser URL. HTML documents are transmitted over this HTTPS link.

When the DSView client first connects, it must authenticate with the DSView server using either a login or client certificate. If the DSView server is configured for external authentication, the login request is re-directed to the External Authentication Server (LDAP). The protocol used depends upon the type of External Authentication Server.

The security of authentication using DSView 3 software is strengthened by:

- The use of message timestamps to automatically terminate sessions that are not established in a timely manner
- DES, 3DES or 128bit SSL encryption of session establishment messages
- Use of X.509 certificate-based SSL for all communication between DSView client, DSView server and Avocent appliances

Security and ease-of-administration are enhanced through the use of Single Sign-On (SSO), which allows users and permissions to be added, modified and deleted in a common manner across multiple devices. This eliminates the potential security lapses and additional administrative work created when multiple redundant user databases must be managed separately.

Customers may also leverage their LDAP implementations to support KVM permissions management. This can further streamline security administration and enable KVM access rights to be managed in a common manner with other enterprise systems. This authentication environment ensures that only authorized users gain access to KVM-enabled resources and that those users only access devices for which they have been given specific permissions. It also enables security managers to enforce security policies with minimal manual intervention.

**Powerful encryption** - The Avocent KVM solution automatically applies the highest practical level encryption -- including DES, 3DES and 128bit SSL technology -- to all authentication and operational sessions communications. Authorized security administrators can also set encryption levels manually. Encryption of the video stream is configurable.

It is also important to note that in the case of remote KVM sessions taking place across VPNs, the traffic between the user and the resource is already being encrypted. This provides another level of protection for KVM traffic and may affect decisions about whether or not to additionally encrypt that traffic using the encryption functionality of the Avocent platform.

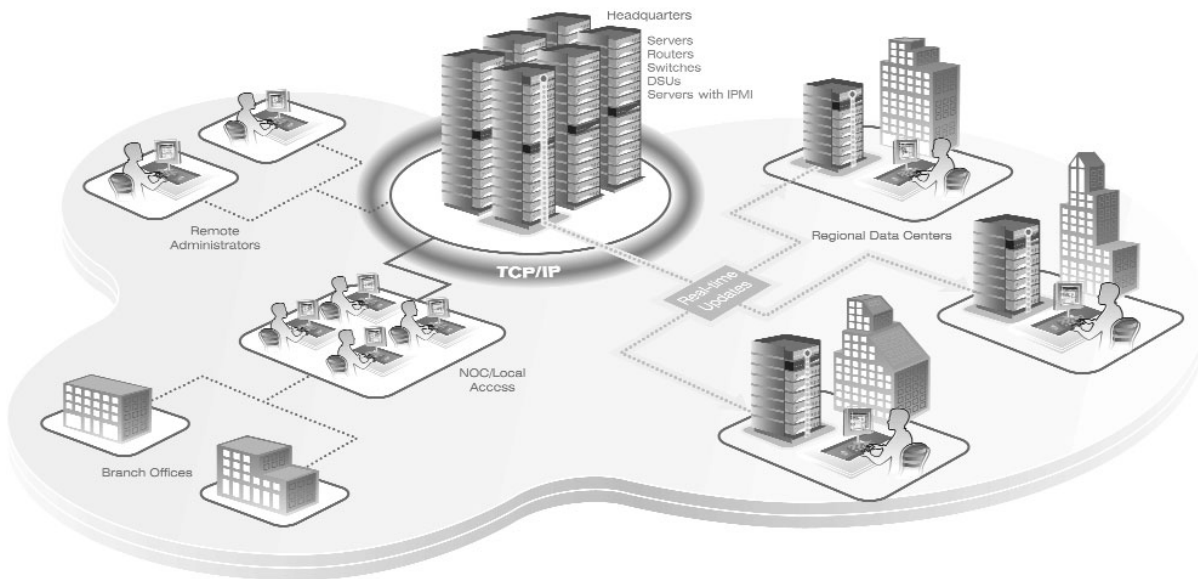
**Non-stop operations** - Avocent KVM protects customers from service interruptions by providing full failover capabilities using multiple mirrored authentication servers. Each location may be equipped with its own hub DSView server with remote locations operating spoke servers. DSView clients may access any number of DSView servers anywhere across the enterprise for full failover capabilities -- eliminating the operational disruption and business risk associated with a single point-of-failure.

**Auditing capabilities** - Avocent DS solutions capture all relevant data about sessions, users and operations across the environment. This data can be used to generate native reports for granular security auditing – or exported in CSV format for use in popular applications such as Microsoft Excel and Crystal Reports. Such reports can be examined to see if anyone using one identity to gain access to the KVM system is using a different identity to log on to specific servers. This would be clear evidence of a potential internal security breach.

In addition to offering IT organizations the most secure architecture for KVM implementation, the Avocent solution also provides a variety of features that make it especially effective for supporting layered enterprise IT security. For example, with DSView 3 software, KVM views can be automatically populated by retrieving the requisite data from remote devices. This supports the implementation of highly secure server rooms that strictly control physical access to servers, while eliminating the labor and potential for error that arise when views are manually populated.

Another advantage Avocent offers is the unique breadth of its switching solutions line, which ranges from 1x16 (i.e. single concurrent user and 16 device ports) to 8x16 (i.e. eight concurrent users and 16 device ports) models. With such a wide choice of models, IT organizations can select the solution most appropriate for each application. For example, an organization may choose to use a 1x16 model to manage a large bank of redundant front-end Web servers – since problems with any individual server is not likely to be critical, especially if a load balancer is being used. On the other hand, an 8x16 model might be more appropriate for a set of special-purpose database servers – since multiple systems administrators may be called upon to work on all of those machines simultaneously.

*DSView 3 management software and the DS Series appliances give administrators secure browser-based remote access to any server or network device all from a single interface without leaving their desk.*



*The power of DSView 3 software is its hub and spoke architecture – a fully redundant, replicating database system that includes both SNMP and IPMI support. Users securely authenticate to a central management hub server or up to 15 mirror spoke servers if the primary server is unavailable. This allows for real-time updates and load balancing across multiple sites.*

**Exit macros** - One of the perils of suffering a network failure, client machine lockup or inactivity disconnection is exposure to outside manipulation or attacks. Your servers are still basically “open,” logged in, and highly vulnerable. Most KVM providers are helpless to provide a solution. Avocent is the exception. To further enhance security, Avocent DSView 3 software provides exit macros that send the keystrokes required to log out each user when a session is terminated for any reason. This protects against one user accessing a server under the assumed identity of the person previously on the same server.

Avocent thus delivers a KVM solution that is uniquely secure and uniquely powerful for enhancing enterprise security and operational efficiency.

### **An action plan for KVM acquisition**

Because KVM technology is such a valuable component of any enterprise security strategy, IT security managers are typically leading business drivers for acquiring a KVM switching system. The three key issues managers face as they pursue acquisition of KVM technology are scope, cost justification and competitive evaluation.

**Scope** - Before being able to calculate the exact cost of a KVM solution – or which vendor’s solution is most appropriate – it is first necessary to determine the scope of the KVM implementation. Factors affecting scope include the number of devices being managed, the number of distinct locations where those devices are situated, the number of staff members being given KVM access privileges and the diversity of those privileges.

**Cost justification** - KVM acquisition is usually not cost-justified based on security benefits alone. Instead, it is the operational benefits of KVM that are primarily used in ROI analyses. These operational benefits include reduced labor, reduced travel, and increased uptime. They are almost always sufficient for cost-justifying acquisition of the technology, which means that the additional security benefits provided by KVM are essentially all “gravy.”

For example, one of America’s mostly highly regarded regional banks has a projected ROI of more than \$768,000 in three years with an initial investment of \$236,000 in an Avocent KVM over IP solution. Their investment would produce a projected savings of close to a million dollars alone in reduced travel and labor for the IT staff.

This unique combination of operational and security benefits make KVM one of the most compelling investments available to today’s IT buyer.

**Competitive evaluation** - Once the decision has been made to acquire KVM over IP technology, the next question is which KVM over IP vendor offers the best solution to buy. Key considerations in any evaluation of competing KVM solutions are likely to include operational features, ease of implementation, ease of use, scalability and overall value. However, as outlined in this paper, security concerns are also important to consider when selecting an enterprise KVM platform. In particular, decision-makers should carefully assess and compare the following security-related characteristics of competitive KVM over IP solutions:

- Failover functionality
- Strength of authentication and encryption mechanisms
- Ease and granularity of administration of KVM privileges
- The ability to administer security policies for KVM in a common manner with other IT management systems
- Auditing capabilities
- Exit macros

It's also important to choose a KVM vendor with a proven track record of technical advancement and innovation. As the overall IT landscape evolves, KVM over IP solutions must also evolve accordingly. And, with these systems playing an increasingly critical role in IT operations and IT security, the ability of KVM over IP solutions to keep pace with changing requirements should be a primary consideration.

## **ABOUT AVOCENT CORPORATION**

Avocent (NASDAQ:AVCT) is the leading worldwide supplier of KVM (keyboard, video and mouse) switching, remote access and serial connectivity solutions that provide IT managers with access and control of multiple servers and network data center devices. Branded products include switching, extension, intelligent platform management interface (IPMI), remote access, video display solutions and mobile devices. Avocent KVM solutions are distributed by the world's largest server manufacturers and installed in Fortune 100 companies around the world. Visit [www.avocent.com](http://www.avocent.com) for more details.