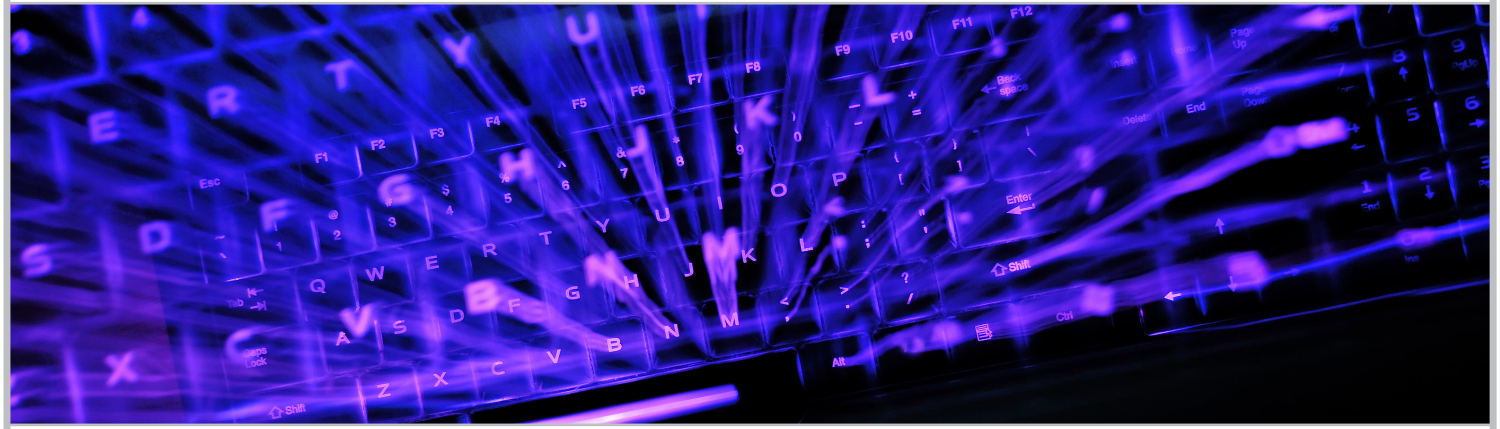
WHITE PAPER

Raytheon | websense®

When Secure KVM Isn't Enough

Increase Security and Flexibility with Advanced Simultaneous Multilevel Access



How an improved thin client infrastructure, that uses the cloud and Advanced Simultaneous Multilevel Access technology, can replace secure KVM while doing more with less expense.

Contents

Introduction

Government agencies are grappling with an increased need for secure systems on one end and tight budgets on the other. This is nothing new as agencies have continually been challenged to do more with less. But today, technology seems to be working in their favor. New technologies are not only helping to secure data and prevent its theft or loss, but are also contributing to the bottom line with lower overall cost of ownership and the flexibility to deliver value far into the future. In this paper, we will take a look at widely used secure KVM switching technology and how an improved thin client infrastructure, that uses the cloud and Advanced Simultaneous Multilevel Access technology, can replace secure KVM while doing more with less expense.

Secure KVM Yesterday and Today

A secure KVM switch is a hardware device that provides access to individual PCs at multiple sensitivity levels, one at a time, from a single keyboard, monitor and mouse (KVM). The switch allows personnel to manually choose which network level to connect to, and to change back and forth between them, although it only allows the user to view one system at a time. Depending on the type of KVM product, the switch may present native connectors on the device where standard keyboard, monitor and mouse cables are attached. Another method is a single connector that aggregates connections at the switch with three independent keyboard, monitor and mouse cables. This method has been recently phased out and replaced with a newer KVM cable that combines the keyboard, video and mouse cables in a single wrapped extension cable. This technology advancement has reduced the number of cables needed between the secure KVM switch and the connected computers. These cables are costly, however, and many organizations opt to continue with the tangle of wires at each desk.

The method of switching from one computer to another depends on the switch. The original switches developed in the late 1980's used a rotary switch, which then evolved into push button switches developed circa 1990. In both cases the KVM aligns operations between different computers and the user's keyboard, monitor and mouse (user console).

KVM switches differ in the number of computers that can be connected. Traditional switching configurations range from 2 to 16 possible computers attached to a single KVM device, but the standard KVM switch has four ports and allows four computers to connect from one user console consisting of a keyboard, monitor, and mouse.

A New Option for the Desktop: Secure Thin Client with Advanced Simultaneous Multilevel Access

With the advent of Virtual Desktop Infrastructure (VDI), the access point or endpoint device can be separated from the physical machine. The virtual desktops reside securely in the data center or cloud and they are redisplayed to the user through his or her endpoint device. The information accessed is entirely stored in a secure data center. Because the virtual desktops are separate instances attached to separate sensitivity levels or networks, they are able to be displayed to the user simultaneously. Each desktop instance is a separate entity and no actions can be performed between them, such as cut-and-paste. Because data is stored in the cloud, security and access control is easier to maintain and audit. Cost savings are achieved with less hardware and operational support.

The VDI computing model has opened the doors to next generation infrastructure models such as Advanced Simultaneous Multilevel Access, which allows a user to securely view more than one desktop environment and more than one sensitivity level, at a time (with KVM, the user may only view one environment at a time). This has significant impact for users throughout governments, intelligence communities, law enforcement and other organizations looking to ensure security, trusted collaboration, mission and enterprise agility, and scalability while reducing costs.

Within an Advanced Simultaneous Multilevel Access solution environment client endpoints are built on a read-only trusted operating system that enables users to access private, community and classified clouds securely from a single device through their familiar user interface. Solutions such as Raytheon|Websense's Trusted Thin Client® provide secure simultaneous access to all authorized networks from a single endpoint with streamlined administration needs. The solution is comprised of two components: client software and a Distribution Console. The Distribution Console is the go-between from the individual networks to the endpoint device, can accept an unlimited number of network connections, and acts as a centralized audit repository to track use and activity.

Cost savings are achieved with less hardware and operational support.

Software-based Multilevel Access versus KVM: A Clear Choice

There are a number of key elements well worth considering when evaluating a secure KVM system versus a multilevel access solution.

Data Monitoring

Data accessed through KVMs essentially cannot be monitored which in today's active blackhat environment is a serious drawback. A secure KVM system is assumed to be used in a secure environment and the devices themselves are reliable. However, if a new method of attack is developed through a KVM there is no way for the organization to know that they have been compromised. If an authorized user was stealing or tampering with data in an environment with only a secure KVM switch, there would be no way to audit or discover this illegal activity.

Software-based multilevel access solutions, such as Raytheon|Websense's Trusted Thin Client solution, offer data and performance monitoring through a centralized server acting as an administration and monitoring hub. The Distribution Console is used to establish and maintain users, is a central audit repository for user activity including session security levels accessed, and it monitors system performance. So when it comes to data monitoring, whether for security or system performance, a thin client solution is the safest and most secure option.

Desktop Real Estate

Compared to a thin client installation, secure KVMs require significantly more real estate both on top of the desk and underneath. The KVM must be connected to each computer and user console (keyboard, monitor, mouse) at each desktop location. All of this hardware and cabling must be managed and supported by administrative personnel on site. For example, if a user accessed networks at six different classification levels, they would require two 4-port KVM switches, six separate CPUs under the desk, and all the corresponding wiring, heating and cooling.

There are a few important scenarios where this has significant impact. The first is during deployment. Especially for large deployments, a lot of manpower is necessary: every system must be taken out of the box, connected to computers and networks, and hooked up to monitors and other peripherals. It is labor intensive and largely prone to error. Post deployment, the issue continues with cleaning crews and employees pulling out cables and plugging them back in incorrectly. Trouble shooting these systems is a methodical and tedious process consuming resources, and impacting productivity.

Another scenario is the compromise of a secure location. Dismantling and then securing sensitive data on a KVM system takes time and a serious frenzy of hard work. With a thin client infrastructure, communications and connections to sensitive data can be cut within seconds because nothing actually resides on the hardware onsite. The data center is in a safe location and there is one cord to unplug from the endpoint.

The Trusted Thin Client is able to handle 300 users (clients) on average per one Distribution Console. So when it comes to saving time and money, a multilevel simultaneous access solution is helping the government do more with less. With KVM there is a keyboard, monitor and mouse on the desk, connected by cables to multiple computers that reside near or underneath the desk. With the Trusted Thin Client model, there is simply one endpoint client, typically a thin client device or a virtual machine client resident in the host PC or laptop, on the desk. A multilevel access solution is much more adaptable to any office or tactical setting. The small footprint becomes very apparent in tactical environments with recognizable space constraints, such as ships, airframes, Humvees, and submarines. Users in these environments can more securely and efficiently access all the required networks to execute their mission while also reclaiming much needed space.

Scalability

Trusted Thin Client provides the ability to support access to a large number of security levels (15+) from a single endpoint. In addition to direct security level access, Trusted Thin Client provides seamless access to remote networks in other Trusted Thin Client environments (based on specific permission granted). This remote network access capability provides a cost-effective means to access needed networks and data without requiring the addition of extra wiring and networks to administer.

Dynamic Response

Trusted Thin Client provides the ability to quickly and dynamically add security levels and access permissions. Access permissions electronically limit access to levels based on user access and/or endpoint.

Compatibility

When it comes to connecting a secure KVM system to an already existing environment of peripherals, there are often compatibility issues. Although they can connect through the ports, their systems cannot always talk to each other which can cause additional costs to the user. Peripherals such as mice, keyboards, and monitors do not adhere to any sort of standards so there is a wide variety on the market. KVM vendors have to generalize for peripherals they support and this often leaves out many types and/or brands.

The compatibility issue complicates the purchasing process when having to consider the different flavors of KVM (PS2, USB, VGA, DVI, Display port, dual head, quad head, CAC) and its compatibility with an organization's already existing set of peripherals. In one example, during a large KVM deployment, thousands of keyboards had to be replaced across an organization because the KVM system purchased turned out not to be compatible with the keyboards the company already owned. This caused a major delay in the customer's deployment.

A thin client model, by virtue of its simple infrastructure, reduces the compatibility variables. It will work with most standard peripherals. This impacts ease and cost of deployment and allows individuals to use the peripherals of their choice.

Portability

Imagine trying to relocate 100 secure KVM users with all the cabling, systems and hardware. Then the effort required to keep it all organized and redeployed in a new location. This is a cumbersome process and we see the cycle start again with complications in an error prone set up process, time spent trouble shooting, etc. Moving a KVM system also presents a security risk and if a system was compromised, there would be no way to know that it happened or by whom.

With a thin client solution, the smaller footprint allows for more flexible and streamlined portability. Most endpoint security issues are addressed with the data resident in the cloud rather than on the endpoint. Because there is only one wire for each endpoint location, moving a system simply requires authenticating clients, wherever they may be within the environment, to the Distribution Console.

Power Consumption

With KVM, each desktop needs power to support the workstation, monitors and other peripherals, plus the KVM switch and local network. Each individual KVM switch pulls approximately 2 kilowatts, which is not significant when you are considering just a switch or two. But in a large enterprise there may be 20,000 switches and power consumption rapidly adds up. With the Trusted Thin Client system there is one thin client and one wire from the desktop per user. This saves money on a day to day basis but is also particularly impactful in the case of an attack or natural disaster such as an earthquake or storm that knocks out the central power source. The thin client system would require significantly less back-up generated power versus the traditional KVM setup with all the power required to run multiple PCs.

Asset Tracking/Age Monitoring

Using secure KVMs requires the organization to maintain and keep track of more assets and take constant measures to keep them secure. Each KVM battery lasts four years from the date of its initial activation. After four years, the switch deactivates, so the dates of each switch's deactivation must be tracked. There is also an anti-tamper mechanism on each KVM, but, if the unit is opened, it stops functioning. This adds a layer of management and asset tracking that is not necessary with a thin client solution outside of the standard refresh cycle.

Network Infrastructure

The network infrastructure required to support the Trusted Thin Client environment is heavily streamlined versus a KVM environment. Trusted Thin Client deploys one network wire to each desktop, regardless of the number of sensitivity levels, versus multiple wires – one for each network – in a KVM setup.

The Impact of Trusted Thin Client

In addition to increased security Trusted Thin Client is proven to deliver additional savings throughout the enterprise. One Intelligence Community customer experienced the following results:

- Value of Trusted Thin Client savings and other net benefits amounted to more than $7.7 million over three years, for overall 54% ROI.
- Computer requirements were streamlined from three machines per user to just one.
- Infrastructure savings came from a reduction in network needs (using one instead of four to six networking connections for each workspace). Including the elimination of some area networks and redundant network access switches.

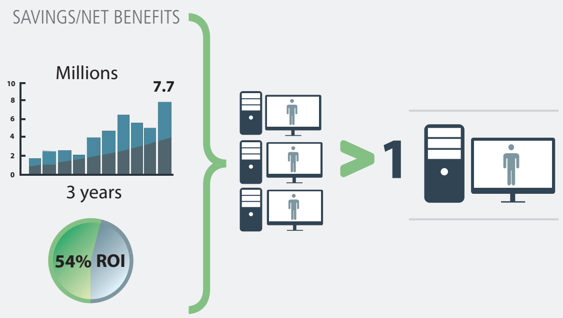


Figure 1 - The Impact of Trusted Thin Client

Security: The Main Driver

When it comes to comparing KVM and thin client in terms of security, there are so many benefits to Trusted Thin Client security that it warrants its own section in this paper. The advantages of a thin client model versus a secure KVM switch are the main driving factors for solutions like the Trusted Thin Client. Simply put, providing secure simultaneous access to all required networks from a single endpoint achieves the highest levels of security available today in a desktop system. There is no longer a need to work around the security architecture, which, by virtue of its simple thin client model, keeps data safe and works for the users making them more productive and efficient.

There are a few important areas where it is clear that a thin client solution such as Raytheon|Websense’s Trusted Thin Client offers a more secure environment than KVM.

- **Desktop Security.** It is easier to keep a data center secure where the thin client system lives (the Distribution Console in Trusted Thin Client), than at each individuals’ desk where a KVM lives. Desktop environments are notoriously insecure and so the less equipment present on or around the desktop, the better. The thin client model has only one thin client and one connection per desktop which is a much easier configuration to manage and secure.
- **Monitoring.** There is no monitoring with a KVM system. If there is a breach there will be no alarms or indications or ways to track it. A thin client system is monitored at the centralized server console and audits user activity and security levels accessed.
- **Peripheral Authentication.** On a KVM system, any peripheral may be plugged in and operated (if it is compatible), and there is no authentication system in place or customization of peripherals. With a thin client solution, peripherals can be specified, white listed and black listed. A user can specify which peripheral to use, down to the serial number, or only use peripherals that are shielded so data is protected.
- **Network.** Only authorized clients can communicate on the Trusted Thin Client network and authenticate to the Distribution Consoles. With KVM a standard network connection is available to any system.
- **Points of failure.** KVM increases the quality and quantity of points of failure. All connections to a KVM are potential points of failure. These are only as secure as the connection to them. Key strokes can be stolen and connections compromised at each connection. This is not the case with a thin client that uses only one connection that is maintained and monitored for high levels of security.
- **Accreditation.** Trusted Thin Client is accredited at many locations for both Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) – and is included in the US Unified Cross Domain Services Management Office (UCDSMO) baseline list. The SELinux operating system on which Trusted Thin Client runs is certified under National Information Assurance Partnership (NIAP) for Common Criteria requirements. Secure KVM is certified under the NIAP for Common Criteria requirements.

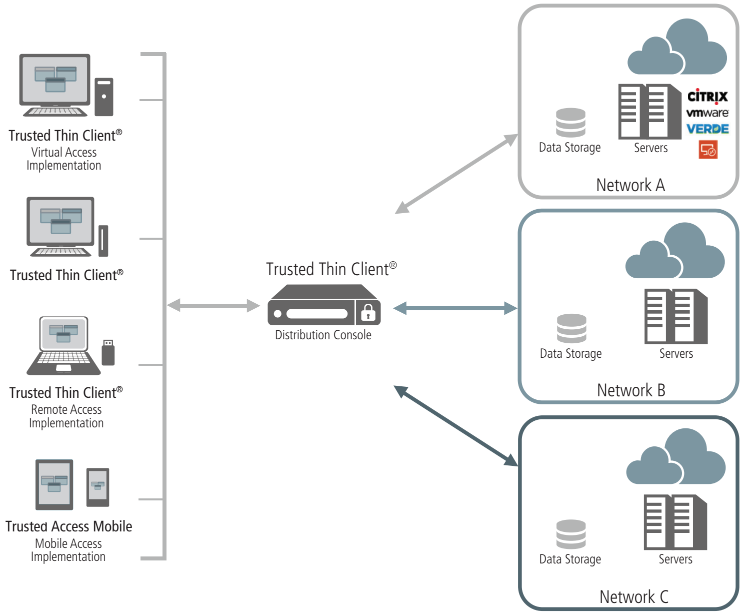


Figure 2 - Trusted Thin Client Architecture

Conclusion

Government agencies need the ability to provide users the flexibility to securely access agency data—at any sensitivity level, on any device, from any location—and ensure that the agencies deliver the right information to the right people at the right time. They need to do this within a cost structure that fits agency budgets and the highest degree of security. The thin client model, exemplified by Raytheon|Websense’s Trusted Thin Client solution with its Advanced Simultaneous Multilevel Access technology, satisfies these requirements along with high levels of agility. Where KVMs require a separate investment and individual management of an external piece of hardware plus cabling per user, Trusted Thin Client consists of software for a thin client and a Distribution Console. The cost advantages lie in its simplicity with less hardware to manage, less resources to deploy, and less power needed for use. The newer technology speaks for itself in this case with lower cost of ownership and superior security against both internal and external threats. These advantages make Raytheon|Websense’s Trusted Thin Client the obvious choice when considering a multilevel desktop infrastructure investment.

For further information contact:

Raytheon|Websense
12950 Worldgate Drive, Suite 600
Herndon, Virginia
20170 USA
866.230.1307

www.raytheoncyber.com