# Advanced Hybrid KVM
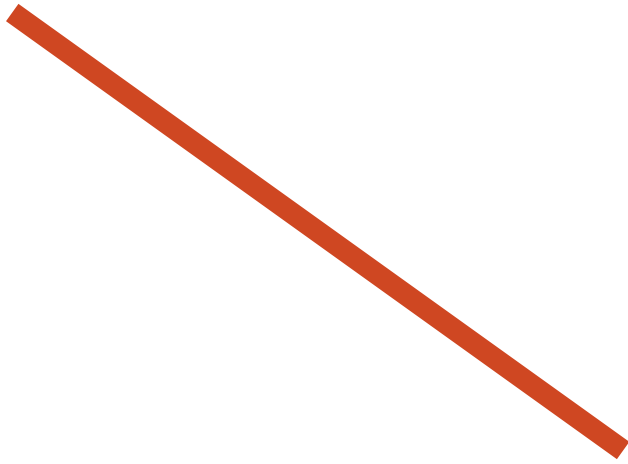
# Essential Guide

**EG**

# Introduction

By Tony Orme, Editor at The Broadcast Bridge

**As users return to the studio and office the need to work remotely is more powerful now than ever. Hybrid is the new way of working and computing innovation is rising to the challenge to provide broadcast users with easy to use, and secure operations from their local PC/Workstation.**

Security is at the foremost thoughts of every broadcast professional. With high-value media prevalent in every broadcast facility and cyber criminals desperate to get their hands on the digital media, the need to keep data secure cannot be underestimated. Although the need to be secure whilst maintaining ease of use may seem like diametrically opposed concepts, a new form of KVM (Keyboard, Video, Mouse) is making its mark in computing which is extending to broadcast television.

As broadcasters progress on their IP journey, more and more processes are moving to COTS servers. From video encoding to editing and quality assurance, COTS infrastructures are dominating broadcast production workflows. The massive amount of research and development investment from non-broadcast industries such as finance and medical, are driving data throughput and processing power through the roof. Although we've been able to process real-time audio through servers for many years, the progress made in COTS technology, with the associated progress in networks, means real-time video processing is now a reality.

Software processing creates workflows that are much more flexible and scalable, with resource-on-demand being easily achievable. COTS servers facilitate software processing and are proving to be an integral component in broadcast workflow.

Traditionally, COTS servers operated from private datacenters, and this made operations relative straightforward as many of the devices were in the same physical area so were relatively easy to operate. Hardware KVM was often used for convenience allowing multiple servers to be operated from the same local computer.

Due to the complexity of how KVMs operated, they were often restricted to IT professionals, especially as secure VPNs (Virtual Private Network) were often used to maintain high levels of secure access. As hardware KVMs developed, it was possible to operate multiple servers from a workstation for non-IT specialists for applications such as editing, and library ingest. However, they were restricted to working within the same private network as hardware KVM encoders were required at the both the servers and local computer.

Public cloud computing is the next advance from private data centers. Although cloud computing delivers unprecedented flexibility and scalability, the locality of the physical server is often left unknown to the users. Generally, this isn't an issue but when considering KVM, life becomes a little more challenging as hardware KVMs require encoders to be placed within the vicinity of the servers in the datacenter as well as the user's computer. Adding a hardware encoder to a public datacenter is virtually impossible.

Software-KVM remote computing solves a very unique challenge, that is, multiple servers can be accessed from a single local PC/workstation. Furthermore, the remote servers do not need to be in the same datacenter, location, or even continent.

Tony Orme.

Security is further improved as VPNs, and video and audio encryption can be easily achieved using a flexible software solution. From the user's perspective, each remote server appears as a separate window on their local PC/workstation which is fully encrypted during transit enabling the highest of secure methodologies to be adopted.

Hybrid computing using software-KVM remote desktop is further empowering non-technical users to operate complex broadcast operations. No longer do users need a deep understanding of VPNs and video encryption as all this is taken care of by the software-KVM to provide ease of use from the users local PC/workstation.

Tony Orme
Editor, The Broadcast Bridge

# Advanced Hybrid KVM

**EG**

**ESSENTIAL GUIDES**

By Tony Orme, Editor at The Broadcast Bridge

**The need to seamlessly work remotely and from the studio is becoming evident as broadcasters emerge from lockdown. Advanced software KVMs delivering low latency and high-quality audio are showing that the perfect work-home environment may well be in our grasp.**

With the benefit of hindsight, hybrid workflows seem like an obvious solution for many television professionals. Even after lockdown, many are realizing it's not always necessary to work directly in the studios or control rooms, and the flexibility hybrid working is providing is unprecedented.

Workflows are improving in efficiency as processes are no longer stalled waiting for key people to provide their input and make the necessary decisions to continue the production. Having a hybrid solution allows directors, for example, to review edits from their home, or on the move, as opposed to travelling to the facilities premises to review the latest composition.  Traditionally, an editor would have had to wait until the director could be in the same room as them to review a selection of edits, meaning they couldn't progress with the production until they had the ok.

The transition to remote desktop operation for many of our working practices has enabled hybrid working. Editing, reviewing, and even grading is now possible due to the power of COTS servers and their associated networks as the contributions from other non-broadcast industries has seen massive research and development investment that has improved the data throughput and processing power.

Broadcasters have traditionally relied on custom hardware designs to process video and audio due to the signal bandwidths involved. However, the wave on innovation that has delivered low latency and high data throughput servers is benefiting broadcasters. Other industries, such as telecoms, finance, and medical have ploughed massive amounts of resource into their research and development to deliver readily available flexible hardware that is capable of processing video and audio in real-time, even for 4K.

The combination of COTS, software video and audio processing, and the internet has enabled a new generation of software KVM. Although KVM has been available for many years, software-KVM excels as it does not require custom hardware to convert the keyboard, video, and audio signals to IP for delivery over the internet. Instead, software running on the client device and host environment replaces traditional local PCs and workstations.

### Improved Availability

A major benefit of software-KVM remote desktops is that it provides much greater flexibility, especially for cloud and datacenter operations where the provision of additional hardware may not be viable.

The users' terminal computer, whether Mac, Windows PC, or Linux PC, tablet, zero client or thin client, connects to the internet and then directly to the remote desktop/workstation or virtual desktop if virtualized, in the office, data center or cloud. This means that wherever an internet connection is available, then the user's computer can connect to the remote computer.

As the software-KVM operates directly on the terminal computer and remote servers, it's not limited by any custom hardware. Therefore, proprietary video and audio compression can be more easily provisioned to meet the specific needs of the internet link it is connected to. Furthermore, systems can be updated as new software versions are made available.

Pixel video compression facilitates the transfer of high-quality images across the internet allowing for quality assurance monitoring as well as image grading.

### Improved Security

When working with high-value content, security is in the foremost thoughts of most broadcasters and falls into two areas: media security and access.

VPNs do provide good security for remote access to IT systems, but the major challenge is that they need to be manually established before each session. Although this is relatively easy to achieve, it is another process to go through and has an impact on the quality of the user experience.
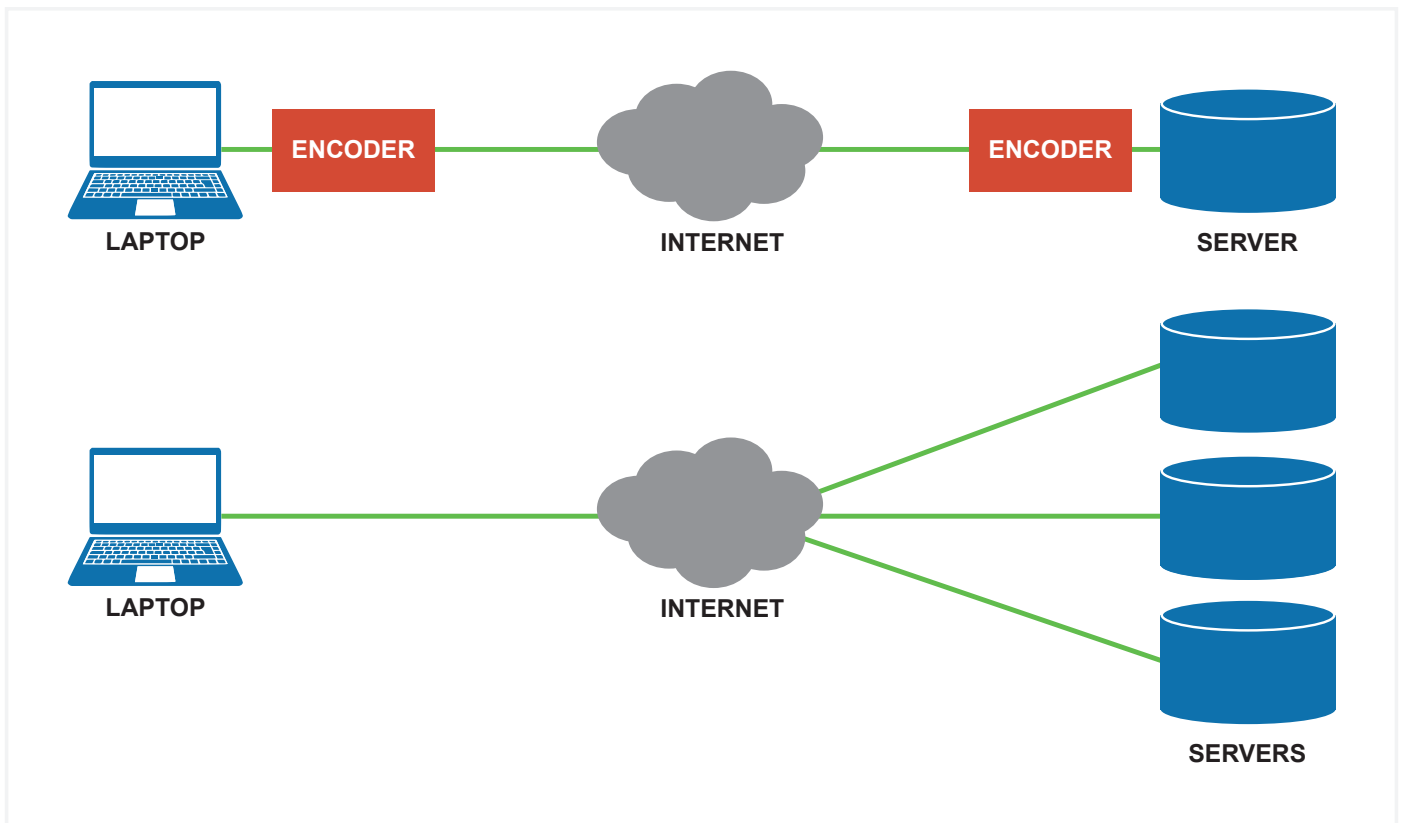


Figure 1 – the upper part of the diagram shows a typical configuration using a hardware system. As the video connections need to be close to the hardware Tx and Rx KVM encoders, they must reside within close proximity of the user and server within the datacenter, this makes hardware KVM impossible to use with public cloud providers as users do not have access to the physical datacenter. The lower part of the diagram shows a software-KVM remote desktop solution where multiple servers can be accessed from the same or different datacenters throughout the world, even when they are situated in the public cloud.

It is possible to provide a generic VPN server within a broadcast facility. This provides users an entry point to the network where they can then access the rest of the network. But this does have some security shortcomings as anybody accessing the VPN servers also potentially has access to the rest of the network.

A software-KVM system can directly access each of the servers it is connected to without a specific VPN being established. It may well use an SSH or its own VPN type connection at the transport level, but it will establish the connection as part of session start sequence and will be out of view of the user. Also, multiple sessions can be established so that a user's terminal can connect to many different servers, none of which need to be in the same datacenter and can be geographically dispersed.

Although security is incredibly important, it shouldn't be the concern of the user. Broadcast teams vary greatly in their technical ability and the less they are involved with low-level security then the more secure a system is likely to be. Even though editors and QA engineers are usually highly technically skilled, they still want to just get on with the job in hand and not be concerned with establishing secure links into networks.

From a management point of view, system administrators can still see who is accessing servers from their management console. Not only does this give visibility of user access, but also allows them to see who is accessing which part of the systems.

Integration with Active Directory further empowers security as no special configurations are needed for the software-KVM remote desktop access. The login credentials provide the same level of access to the remote user as they would have if they were in the building sat by the side of the server.

As the video compression is very high quality when in transit between the data center and the user's remote computer, broadcasters are increasingly concerned about cyber criminals stealing video and audio streams as they traverse the internet. This concern is further exasperated if a high-value content is streamed over a WiFi link in a user's home as anybody with the WiFi access credentials can intercept the stream.

End to end video and audio encryption prevents anybody from illegally viewing the material. It's entirely possible for them to access and even record the stream, but it's almost impossible for them to view the encrypted content.

### End to End Solution

Ease of use is paramount for any user and the software-KVM remote desktop not only provides secure access but makes the whole user experience much more enjoyable. The end user can use the remote desktop from their client device as if it is local and switch between each of the remote desktops.

It is certainly possible to bring together various software solutions such as VPN, SSH, and windows managers, but the whole experience is clunky and difficult to operate.

Without a complete end-to-end solution, the user would have to establish a VPN connection, then SSH into a server and finally establish a remote windows environment.

Although this is all possible, it proves far from optimal and does not create a harmonious user experience.

Furthermore, if multiple servers are needed to be accessed then it's entirely possible that multiple VPN circuits will need to be established, especially if the datacenter servers are in physically different locations. If a user was accessing servers in three different datacenter locations, which may not even be on the same continent, then they would have to establish and keep track of three different VPN and SSH sessions. This is certainly difficult to achieve for seasoned IT professionals and would prove almost impossible for users who do not specialize in IT to achieve and maintain.

Using a non-integrated method also creates incredible challenges for security. VPN and SSH sessions rely on dual key authentication leading to users and administrators having to maintain multiple SSH keys (potentially hundreds), and for most operational applications this will turn out to be an unrealistic proposition.

Adding the video feed into the mix further creates a complicated solution for anybody looking to manually encrypt the video feed. It is possible to do this but it's not for the faint of heart and can lead to more problems than it solves.

Although an integrated solution may well use video encryption and VPNs with SSH sessions, abstracting away the underlying complexity leads to an efficient and secure method of access, especially if video encryption is also used. This is even more apparent when multiple servers are accessed from one user computer.

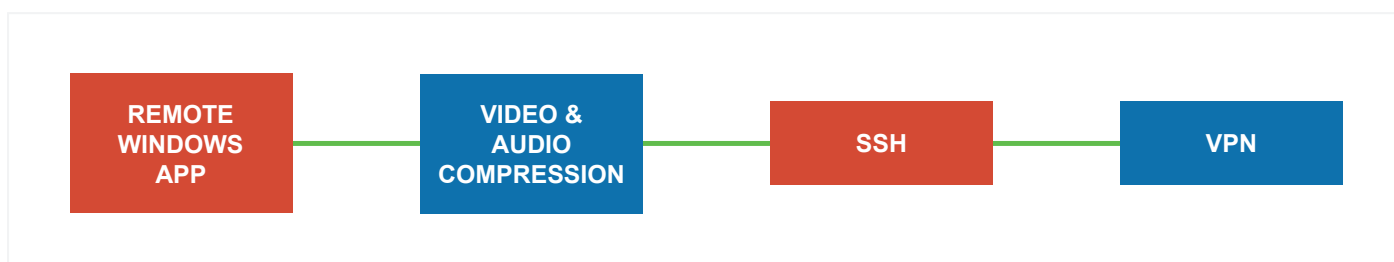| REMOTE WINDOWS APP | — | VIDEO & AUDIO COMPRESSION | — | SSH | — | VPN |

Figure 2 – multiple processes are used within the user's computer and remote server to achieve full software-KVM remote desktop operation. Although these can be built manually, the resulting solution is almost unusable. The fully automated end-to-end software-KVM remote desktop makes the operation seamless and significantly improves the user experience.

## Adaptive Streaming

Internet connections vary enormously in their quality, that is, their bandwidth and latency. Even for low bandwidth requirements such as keyboard entries and mouse clicks, latency can have a detrimental impact on the user experience as the response time of these events becomes noticeable. Therefore, a greater awareness of the underlying transport stream must be achieved.

As we add video into the mix, the needs to understand how the internet is performing between servers and the user's computer is paramount. Not only does the software-KVM remote desktop need to measure the bandwidth, but also the latency too. Adaptive video streaming is one of the tools that are available to deal with varying internet quality.

It's also worth remembering that the internet quality isn't static, it varies enormously from hour to hour, and sometimes from minute to minute. Having a system in place that dynamically adapts to the underlying changes in bandwidth and latency improves the user experience beyond all recognition.

Combining the video rate adaption with the bandwidth and latency analysis, allows the video data rate to be able to scale to the quality and availability of the network and internet. This is especially important if a user is switching between different servers. Furthermore, using a proprietary codec allows micro tuning of its parameters to deliver a very high user experience.

With high quality internet connections and by using proprietary codecs adapted to the network ability, it's possible to achieve such incredibly high-quality video that QA and color grading could be achieved.

Software-KVM remote desktop delivers incredibly high levels of flexibility as the required code is installed directly on the server and user's computer. This is especially important when working with public cloud installations as there is often no opportunity to install custom hardware into the datacenter. Security and video compression are often considered at the very beginning of the design leading to a rounded solution that is easy to use and provides an outstanding secure and flexible user experience.

**teradici**®

## The Sponsors Perspective

## The Future Of Broadcasting Is Hybrid

By Ian Main, Distinguished Technologist, HP.

For broadcasters to be profitable and stay ahead of the curve in this competitive market, they need to develop hybrid strategies with secure technology to accommodate remote workers without losing productivity. This was a direction the industry had been heading towards for some time, but the pandemic forced the industry's hand at a more accelerated rate.
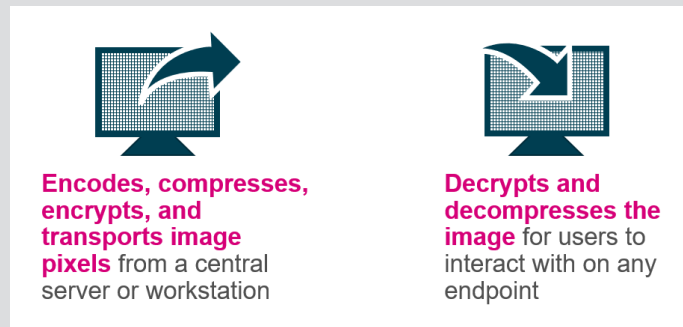


### Lessons Learned From The Pandemic

Not all industries had the luxury of closing up shop for a few weeks to figure out their remote working policies and technology. Broadcasters, especially live broadcasting, were not afforded that luxury. Thankfully, many were already working on what remote working would look like, so the transition was much faster than in other industries.

Many broadcasters were working over a KVM (Keyboard-Video-Mouse) infrastructure to access their digital work resources, but that infrastructure was not designed to work over a wide area network (WAN). It was not scalable to support high volumes of remote workers, like was the case in March 2020 at the start of the pandemic. Many had to switch their infrastructure over to PCoIP® technology during the pandemic to handle remote workflows better.

Supported by

**teradici**®

For the creative team members in broadcasting and production, moving to a remote work situation during the pandemic was scary. Many had old-school views of what "remoting" into their work desktop looked like, and they feared that would significantly hinder latency and graphics quality. However, once they saw how far PCoIP technology had come, the transition period was quick.



**Encodes, compresses, encrypts, and transports image pixels** from a central server or workstation

**Decrypts and decompresses the image** for users to interact with on any endpoint

## User Experience Requirements And Struggles

Attention to detail and graphics quality are essential in broadcasting. Creatives are very discerning, and they often work best when they can focus on their creativity and not on technical hiccups or latency slowing down their creative process.

The future of broadcasting may see some hesitancy from creative personnel in the transition to remote working. But, the transition period will be relatively short with the right technology solutions supporting them. As they see their colleagues around the world adopting successful, easy-to-use remote workflows, the hesitancy will dwindle.

## The Future Of Employee Workflows

Teradici did a remote work survey of nearly 700 IT decision makers about the future of remote working in their industries. The survey found that 67% of respondents would change the way they shift employees if another event similar to COVID-19 were to happen again. Also, 56% of IT and technology workers will continue to work from home once the pandemic is over.

This tells us that the future of nearly every industry, including broadcasting, will take a more hybrid approach, with employees splitting their time between on-premises and remote working for a variety of reasons (including necessity and preference). This also means we're going to see a continued evolution of the traditional workplace cubical environment.

## The Future Of The Workplace Cubical

In broadcasting, there will always be roles that are better suited to be on-premises, like television anchors, for example. However, most post-production and creative teams can work from anywhere, given the right access to digital resources and real-time collaboration tools.

We anticipate a future where post-production and creative teams can work from the office or home seamlessly because they won't be tied to a physical desktop computer machine under their office desk.

These individual computer towers will become centralized in an on-premises location. This will allow any team member with a company-issued end client to access these resources via PCoIP whether they're on-premises, working from home, or travelling. As long as they have an internet connection, they can do their work from anywhere, just as if their computer tower was sitting under their desk.

Since working from an on-premises cubical will no longer be required, HR teams are no longer restricted to hiring locally. They can find the right team members to join from anywhere in the world.

"With our technology, there's an initial expectation, and then there's a value increase," says Ian Main, Distinguished Technologist, HP. "From the decision makers' point of view, I think now it's about refining their architectures to meet that hybrid work model that everybody agrees is the future forever, really. And I think we know that employees are going to be more picky about working for broadcasters that can offer that flexibility."

## Technology Trends In Remote Working For Broadcasting

As technology advances and merges, we see several technologies and feature trends emerging as it relates to remote working in this industry:

- **Collaboration:** teams need technology that facilitates ease of collaboration.

- **PCoIP Ultra AV lock:** to get audio and video seamlessly synchronized.

- **Sustained high frame rates at 4K/UHD resolutions and beyond:** this needs to be sustained in a high-performance client windowed mode.

- **Multi-channel audio:** critical for creating broadcast-quality content, especially immersive content intended for cable or OTT distribution.

- **HDR color:** for high dynamic range content.

- **Peripheral integrations:** so creatives can seamlessly use Wacom tablets and other tools with their computing systems.

We also expect to see more centralization of digital assets and computing across many industries, especially broadcasting. This will help streamline workflows and IT Team management and support of computing systems and devices.

Supported by

**teradici** ®

# teradici®
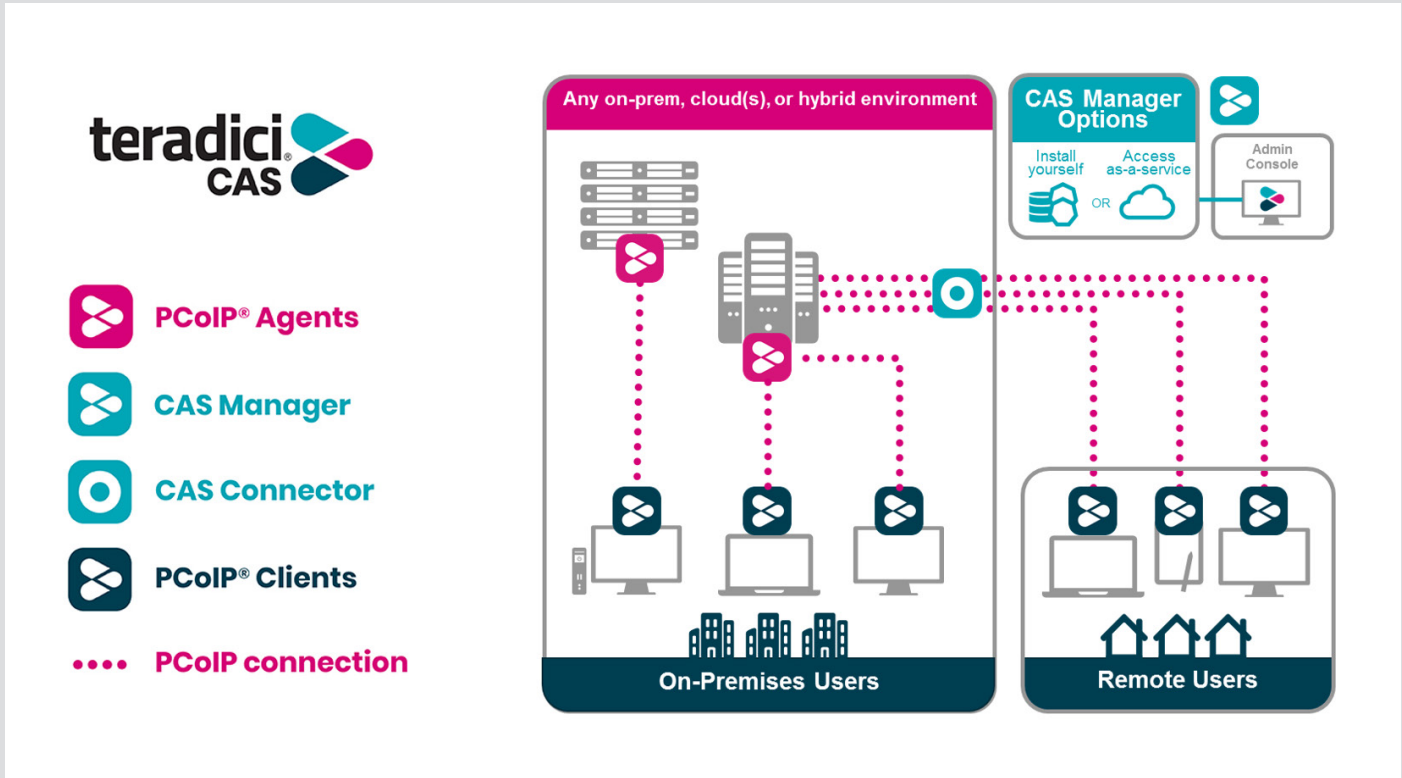


## Requirements For The Future Of Broadcasting And Post-production

Forward-thinking broadcasters will also be looking for a solution that meets three essential requirements:

1.  **Remote worker ease and satisfaction:** All contract and employee team members need to be comfortable using the remote working technology so that their creative processes are not hindered.

2.  **Security protocols:** With the recent increase in corporate and media company data breaches, broadcasters need to ensure that their intellectual property is protected when team members access digital content and apps over the cloud.

3.  **Ease for IT Team:** Centrally based IT teams need the ability to onboard new users quickly without needing to visit everyone's remote workplace (their home or remote site) and manage access and security from a centralized location.

Technology and processes that meet these critical needs are going to be more common within the industry.

## What Teradici Is Excited About For The Future Of Broadcasting

"Many broadcasters have only just dipped their toe in the water [when it comes to using PCoIP technology for remote working]," says Rodney Tafuro, Teradici Account Executive, HP. Rodney and his colleagues at Teradici are excited to be working with prominent public broadcasters to help create this future.

The team is excited to discover how technology companies and broadcasters can innovate and find new ways to merge existing technologies to meet the needs of broadcasters better. Building on the strengths of each technology and platform, this will support broadcasters to work more efficiently than before, on more secure systems that are easy to use and manage.

**Ian Main, Distinguished Technologist, HP.**

# BROADCAST
# THE ——— BRIDGE
## Connecting IT to Broadcast

teradici ®

| | |
|---|---|
| **CI** CORE INSIGHTS | **EG** ESSENTIAL GUIDES |
| ▶ MEDIA | ARTICLES |

For hundreds more high quality original articles and
Essential Guides like this please visit:

thebroadcastbridge.com

11/2021

Supported by

teradici ®