M+E JOURNAL

It's Showtime!

Innovation explodes across every workflow as technology emerges from the pandemic.

Where are you in this accelerated evolution?

DIVERSITY & INCLUSION
In the office, behind the camera, and on the screen, diversity is crucial

SECURITY
Remote productions create new security concerns, with assets under siege

SMART CONTENT
Artificial intelligence and machine learning are being applied in new, exciting ways

NEW WORKFLOWS
The cloud is delivering on its promise, powering the future of productions

21.01

THE AGE OF FULLY VIRTUALIZED PRODUCTIONS

It took a pandemic for media and entertainment to adopt the necessary workflows

By Kevin Ottomeyer, Director, Solutions Architects, Teradici

ABSTRACT: Understanding M&E organizations and their requirements has been key to creating that ecosystem of solutions that enabled each unique studio to be successful on their journey to virtualization, either from an on-premises private cloud, a hybrid environment, or public cloud.

Virtualization has been around for quite some time but until the COVID-19 pandemic, the methodology hadn't been widely adopted by media and entertainment companies, mostly due to the workflows that are so unique to the industry.

For one thing, M&E workflows have consisted of high-powered workstations sitting underneath artists' desks that would be used for their heavy graphics workloads. It's tough to tell an artist that you are taking away that machine and replacing it with a device one-tenth the size and convincing them it's going to be an as good or even better experience.

Of course, that challenge was met with other external factors, including requirements for artist pen displays and tablets, color-corrected monitors and multifactor-authentication, among others.

So, from the outside looking in, it seemed like a daunting task to virtualize these workloads and make sure the experience was just like an under-the-desk workstation including all the unique devices artists used for their workflows. To that end, Teradici's ecosystem allows visual effects, animation, broadcast and game development studios to have an amazing remote desktop experience, whether they are in the studio or geographically distributed.

A key part of that experience is making sure there are no negative impacts as artists and content creators are increasingly separating themselves either because of new protocols with COVID-19 or new work from home policies.

Teradici Cloud Access Software (CAS) offers features like Teradici AutoOffload that enables artists to either manually or automatically switch between the image and video fidelity based on their workflows needs. This is key to maintaining the experience between pre- and post-production workflows.

HOW CLOUD TECHNOLOGIES FIT INTO THE EQUATION

Scalability and agility are front and center when we talk about the advantages of using cloud-based architecture. When we talk about the cloud, it can be categorized in three overarching methodologies: private, public and hybrid.

Private cloud is the traditional data center model, with resources, CPU, memory, storage, networking all purchased, managed and maintained by the studio, traditionally a capital expenditure.

In a public cloud, on the other hand, those resources are managed and maintained at the hardware level by the cloud provider and the customer is responsible for everything above that layer.

Teradici plays very well into all these scenarios, including the third, which is the hybrid model.

The hybrid is by far the most popular environment we are seeing in the industry today. We see customers leveraging existing equipment in the data center that still has a lot of life left in it with a combination of some burst resources in the cloud for expansion or short-term projects.

The hybrid model gives the added benefit of flexibility to move existing, and burst new, workloads very easily without the hassle of staging and purchasing new equipment. With CAS, we help link these two data centers by allowing the customer to tap into their on-prem resources and at the same time leverage their cloud resources in one central control plane interface (CAS Manager).

DO YOU NEED THREE REMOTE WORKSTATIONS SPUN UP FOR A NEW PROJECT STARTING TOMORROW?

If so, simply log in to CAS Manager, create three new cloud or on-premises instances from the console, assign them to the correct artists and you are ready to go in a matter of minutes. It's essentially a private Desktop-as-a-Service (DaaS) platform for customers who want both the flexibility of their own applications and images with the ease of use of a managed desktop type of model.

THE HYBRID MODEL gives the added benefit of flexibility to move existing, and burst new, workloads very easily without the hassle of staging and purchasing new equipment.

WHAT THE DATA JOURNEY ALONG THE WAY WILL LOOK LIKE

Where to put the data, how to replicate it and whether it is secure in rest and transit are all key things to think about when architecting an organization's data model.

By utilizing Teradici solutions such as CAS, data is fully encrypted in transit, providing peace of mind so that organizations can focus more on securing that same data at rest. We also have a solution that enables our customers to skip the virtual private network (VPN) and use our built-in Security Gateway included in CAS Manager.

This component of CAS Manager offers a highly encrypted micro-VPN tunnel that allows CAS connections to flow freely between endpoint and remote workstation, essentially displacing the traditional VPN.

All transmissions are then done via pixel transformation and the need to copy files back and forth between a data center and workstations becomes a thing of the past.

This proprietary process allows all the data to stay where it can be secured, cared for and maintained per the organization's strict standards and practices. Allowing for the highest level of data integrity possible, while still maintaining a world-class artist experience.

SECURITY AND CONTENT PROTECTION ARE GUARANTEED AT EVERY STEP OF THE PROCESS

M&E companies can, meanwhile, be confident their content is safe throughout the process if a Zero Trust Architecture is being used, as is the case with Teradici's solutions.

While traditional security is easily exploited with

Kevin Ottomeyer *is the global director of solutions architecture at Teradici. An Emmy award-winning principal solutions architect, he focuses on driving and influencing the roadmap for CAS and CAS Manager, two of Teradici's solutions that are widely adopted throughout the M&E industry.*
kottomeyer@teradici.com @OttoKnowsBest

malicious intent, a zero trust strategy eliminates trust and continuously verifies all applications, devices and users.

Meanwhile, Teradici's PC-over-IP (PCoIP) technology provides an additional level of security. It uses advanced display compression to provide end users with on-premises or cloud-based virtual machines as an alternative to local computers. The virtual workspace architecture compresses, encrypts and transmits only pixels to a broad range of software clients, mobile clients, thin clients and stateless PCoIP Zero Clients, providing a highly secure enterprise environment.

From the user's perspective, there is no difference between working with a local computer filled with software and an endpoint that receives a streamed pixel representation from a centralized virtual computer.

The PCoIP protocol transfers only display information in the form of pixels. Therefore, no business information ever leaves the cloud or data center.

Also, because enterprise data and software are safely secured inside central systems, bad actors can't tamper with the user's data or infiltrate their applications by compromising their local devices.

PCoIP traffic is also secured using AES 256 encryption that meets the highest level of security required by governments.

In the end, collaboration for M&E organizations is crucial but data risk is large. However, PCoIP technology provides a critical additional layer of protection. With it, organizations can work collaboratively from anywhere in the world, confident that sensitive information won't ever leave the data center and work can never be lost or stolen. ⊞