RICHEY MAY

MOVING HOLLYWOOD TO THE CLOUD: A PACKING LIST

Alvin Tugume

Cyber Security Engineer

RICHEY MAY

THERE'S NO CLOUD. IT IS JUST SOMEBODY ELSE'S COMPUTER

- The term "Cloud" is used to describe a global network of servers
- These servers serve a different purpose to deliver computing services over the internet (the "Cloud")

TYPES OF CLOUD

- Private Cloud: a server, distributed network that is dedicated to one organization. For example: Microsoft HyperV
- Public Cloud: this type of cloud is ran as a service by an external vendor that may include servers in one or multiple data centers. For example: AWS and Microsoft Azure

RICHEY MAY

Cloud Service Models

- SaaS – Software as a Service. These are applications that run completely in the cloud. For example, cloud-based Microsoft Office 365
- PaaS – Platform as a Service – this is a cloud service that provides you a set of tools and services designed to make coding and deploying those applications quick and efficient.
- IaaS – Infrastructure as a Service – This cloud model offers virtualized computer services over the internet. For example, Amazon AWS

RICHEY MAY

The Benefits of Utilizing the Cloud in Hollywood

- Accelerates digital transforming efforts with unlimited compute power and storage
- Availability, Scalability and Flexibility
- Robust Production
- Reduces Cost

Out of Sight doesn’t mean Out of Mind

- Cloud Security Monitoring
- Access Controls and Security Control
- Enforced Antivirus, Antimalware scans
- Enforced Multifactor Authentication

RICHEY MAY

Cloud Security Monitoring

- Determine the inventory of resources used in your environment
- Map out all the data attributes, which you desire to collect and monitor
- Make a mutual decision regarding software that suits your needs

Cloud Security Monitoring (cont'd)

- Automate the Monitoring Process – since operations carried away on the cloud are virtual, it simplifies the configuration of automated monitoring efforts

Access Controls

- Access Control in cloud security is a process in which access and permissions to content is regulated and monitored
- Formulate policies to restrict access through specific IP addresses, browsers, devices, and or during specified time shifts

RICHEY MAY

Enforced Antivirus and Antimalware Scans

- Adopting a cloud service in an organization doesn’t mean that you are free from the stress of that comes with content protection. Alike on-premises security, enterprises must take care of information stored on the cloud
- Utilize AV and AM solutions to continue full periodic scans of endpoints

Enforced Multifactor Authentication

- Enable and enforce per-user MFA
- Enforce a uniformed approach to MFA to studio-owned resources

RICHEY MAY

Remember, Out of Sight does not mean Out of Mind

Q/A Session

Thank you, everyone!