M+E JOURNAL

The Future is Automated

The landscape ahead for M+E looks uncertain. Automation can ease the journey.

WORKFLOWS AND THE CLOUD
From cloud-based productions to unprecedented storage demands, the supply chain has never been more challenging

SMART CONTENT
The questions around AI, metadata, and analytics are endless. But we do have many of the answers already

SECURITY SOLUTIONS:
Cybersecurity and content protection in M&E is always on defense. Can automation can change that?

23.01

THE CLOUD IS ONLY AS SECURE AS YOU MAKE IT

Moving to a cloud-first production workflow? Take precautions

ABSTRACT: High-profile data and security breaches are a hot topic in the news as more companies transition their teams from on-premises environments to cloud computing solutions. Risk, compliance, and technology managers have a looming list of concerns when determining if adopting a cloud solution will open their organization to cybersecurity attacks. In this article, LucidLink discusses the precautions, controls and assurances content owners need to keep in mind when moving to a cloud-first production workflow.

By Randy Magiera, Director, Information Security, Privacy, LucidLink

High-profile data and security breaches are a hot topic in the news as more companies transition their teams from on-premises environments to cloud computing solutions. Risk, compliance, and technology managers have a looming list of concerns when determining if adopting a cloud solution will open their organization to cybersecurity attacks.

Nevertheless, business leaders understand the importance of the cloud. In a recent poll by Accenture, 80 percent of executives look to the cloud as a means of mitigating business uncertainty and lowering risks. While no security is perfect, many concerns with cloud security stem from a misunderstanding of what causes an organization to be left open to attacks.

Managers and tech executives must understand this to help prevent their company from being targeted.

By 2025, 99 percent of cloud security failures will be due to the cloud service providers' customer's actions, which can be easily prevented.

IT'S NOT THE CLOUD, IT'S ...

Cybersecurity concerns leave IT and risk management executives hesitant to consider adopting and implementing cost-saving, efficient cloud-based technologies. However, contrary to popular belief, the root cause of most cybersecurity breaches is not the cloud itself. It's human error.

Moving to a cloud-based storage solution can be highly secure and beneficial for an organization as such solutions provide cost-effective enterprise storage, which is almost

CONTRARY TO POPULAR BELIEF, THE ROOT CAUSE OF MOST CYBERSECURITY breaches is not the cloud itself. It's human error.

infinitely scalable. Many of the fears executives have surrounding migration to cloud-based solutions stem from misconceptions, resulting in missed opportunities for improving productivity and cutting costs.

According to Gartner, nearly all cybersecurity attacks result from human error, not cloud providers. The security issues behind these attacks frequently result from the customer improperly configuring their cloud environment. There are several reasons for this, but one of the most common reasons for a misconfigured environment is the failure of a company to provide proper training and education to its employees. Gartner's report states that by 2025, 99 percent of cloud security failures will be due to the cloud service providers' customer's actions, which can be easily prevented.

UNDERSTANDING SHARED RESPONSIBILITY

Cloud services are not inherently insecure. Ensuring a secure cloud environment requires shared responsibility of the customer and the cloud storage or service provider being aware of what they're accountable for. Understanding this responsibility and customer expectations can help organizations properly configure and adopt cloud strategies.

The AWS Shared Responsibility Model outlines the aspects of cloud computing for which Amazon Web Services (AWS) is responsible versus the responsibilities of the customers. Understanding this shared responsibility helps customers better understand their roles and obligations when using AWS, and what they can expect AWS to manage on their behalf. In exchange, the customer is responsible for configuring and managing their data properly within the cloud and managing permissions.

For example, when new customers set up an account with a cloud service provider, they are responsible for their own Identity and Access Management (IAM). This means the customer is responsible for creating accounts to log into their environment and ensuring those accounts are secure. The cloud service provides tools to help companies secure their accounts, such as Multi-Factor Authentication (MFA), but it is ultimately up to the customer to configure and enforce MFA. Correctly configuring MFA can keep company data safe and prevent avoidable data breaches.

A SECURE SOLUTION FOR CLOUD STORAGE

As a cloud-native NAS storage provider, our job at LucidLink is to offer high-performance companies a solution that improves scalability, is reliable, and ensures data durability while enhancing team collaboration and productivity. One of the fundamental principles of our product's design is having a strong focus on security to provide a best-in-class solution for highly sensitive workloads. We work with customers to help them better understand their needs and security concerns and ensure that our solutions help them use the cloud cost-effectively and securely.

Our "zero-knowledge" guarantee is one way we approach keeping our customers' data secure. We use a strong end-to-end, full-system encryption to ensure all data is encrypted on the customer's device. The encryption keys remain only in the hands of the customer. In addition, the recent release of single sign-on (SSO) implementation makes LucidLink Filespaces 2.0 even more secure by adding a new security feature, the LucidLink Filespace Key. The Filespace Key enhances our zero-knowledge guarantee and ensures that neither LucidLink, the cloud service provider, nor any third parties can access customers' data.

Security starts with you. A space for your entire team to collaborate securely on the most massive media projects with insanely fast, easy file access starts with LucidLink. ⊞

Randy Magiera *is the director of information security and privacy at LucidLink. He holds about 20 years of expertise in information technology (IT) and information security (IS), supporting leading companies like NetApp, Coopervision, and the University of Rochester. In addition to supporting IT and IS across industries, Randy is an adjunct professor teaching information security and privacy courses at the graduate-level.*
randy.magiera@lucidlink.com @Lucid_Link