illumio

5 Things You Might Not Know About Cloud Security

False assumptions create unnecessary security risks

ASSUMPTION 1

Your Cloud Provider Is Responsible for Your Application Security

Security is a shared responsibility. With any cloud vendor, their security responsibility is limited to protecting just the network fabric. And those agreements are based on "best effort."

Ultimately, protecting your company is your job. As soon as you deploy an application instance on top of a cloud platform, protecting it is your job, not theirs.

ASSUMPTION 2

Cloud Security Is Easy to Manage

The cloud's benefits — speed, agility and elasticity — have also led to a proliferation of cloud services that is creating critical security challenges. Large companies now typically have hundreds of cloud accounts, many with virtual private clouds and their own security groups.

All this makes managing those groups and understanding their security exposure increasingly difficult, especially as hybrid clouds combine public clouds with systems hosted by on-premises data centers.

ASSUMPTION 3

Cloud Services Are Isolated From the Internet

Remember, the cloud is not "least privilege" by default. Instead, it operates on "excess privilege." As a result, any cloud service — PaaS, IaaS, virtual machines, containers and serverless functions — can be open to the Internet.

To ensure cloud security, you need to know exactly what's connected to the Internet and lock down any unnecessary connections.

ASSUMPTION 4

There Are No Limits to Scaling Cloud Services

Public clouds like AWS and Microsoft Azure limit the number of segments that can be created to manage security. This prevents you from achieving fine-grained control of your cloud applications and data.

To scale, you'll need additional help segmenting access. Otherwise, you'll end up with poor visibility, complex policy management, and the need to manually "rewire" network configurations and firewalls.

ASSUMPTION 5

Once You Secure a Workload, Your Work Is Done

When people think about workload security, many assume their workloads stay in one place. But in the cloud, all compute resources, serverless resources and objects are dynamic — moving around in one cloud or moving across multiple clouds.

As a result, cloud workloads must be tracked and protected as diligently as any application running on a server in a traditional data center.

The Cloud Is Here to Stay — and So Are Its Security Risks

As organizations both large and small consider a move to the cloud, they often underestimate security challenges. But to ensure full protection, organizations need to make security planning a fundamental part of their cloud migration plan. True cloud security rests with you.

Learn how Illumio can help you build stronger digital security for your multi-cloud and hybrid cloud environments.

www.illumio.com/cloudsecure

illumio