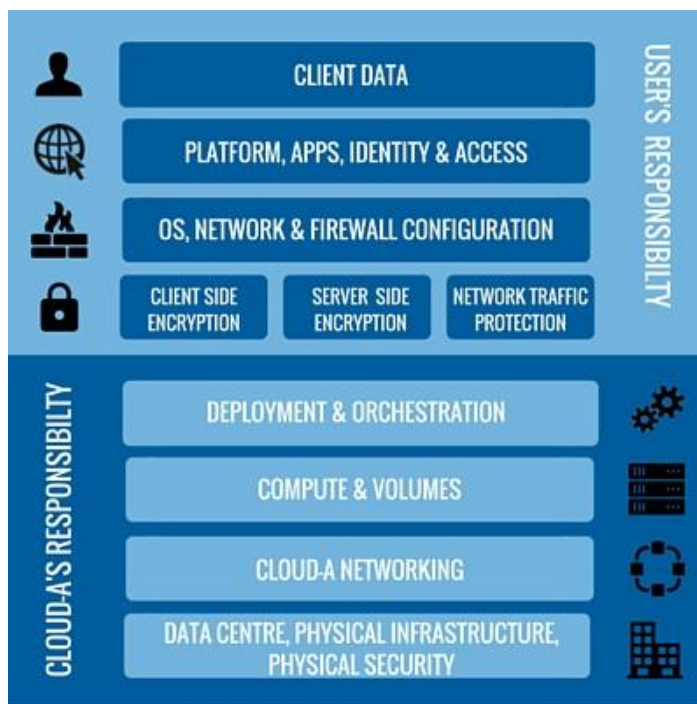




## CLOUD-A SECURITY PARTNERSHIP MODEL

Because you're building systems on top of Cloud-A infrastructure, the security responsibilities is shared: Cloud-A has secured the underlying infrastructure and you must secure anything you put on the infrastructure or connect to the infrastructure. The amount of security configuration work you have to do varies depending on how sensitive your data is and which services you select. This partnership is outlined in our **Cloud-A Security Partnership Model** (below.)



### Cloud-A User's Responsibilities

For IaaS services like Cloud-A compute instances and Swift bulk object storage, you have more control and therefore more configuration work to do. For compute instances, you're responsible for patching the guest OS on the instances as well as any software you install on them, configuring the security group (firewall) that allows outside access to your instances, and setting up any VPC subnets that the instances reside within, etc. For Swift bulk object storage, you must set the access control policies for each of your storage buckets, set up encryption options for the stored data, and specify backup and archiving preferences.

### SECURITY RESOURCES

#### [Cloud-A Managed Security Services](#)

A suite of managed security services designed specifically for Cloud-A's virtual networks.

#### [Cloud-A Security Centre](#)

A deep dive into our security manifesto! All of your Cloud-A security information in one place!

#### [Cloud-A Guide to Cloud Security](#)

Some best practises for securing your virtual networks on Cloud-A

#### [Encrypted Volumes: Linux Edition](#)

A tutorial on how to scale your Cloud-A storage security by encrypting volumes

#### [Configuring a VPN Server Using CLOUD-INIT](#)

A tutorial on how to create and deploy a VPN server on Cloud-A using CLOUD-INIT

#### [Securely Connect to your Cloud-A Windows Server with RDP](#)

A tutorial on how to setup RDP on your Cloud-A Windows Servers

#### [Linux Security Best Practises](#)

Security best practises for managing Linux servers on Cloud-A

### OUR SECURITY PARTNER



Based in Toronto, Canada, [Lyrical Security](#) combines industry expertise with innovative technology to help organizations address their most critical security needs. Lyrical helps organizations attain visibility into security controls, attack surface and posture, using leading edge tools, trusted methods, and proprietary and open-source software. Lyrical helps their clients understand their environment's footprint, secure them, and keep them secure in an ongoing way.