**PROBLEM STATEMENT**

Ozmart is a Small-to-Medium Sized retail organisation which is growing at a significant rate. Due to its expansion the current on-premises networking infrastructure is unable to handle increasing demand and network traffic. Due to this the stakeholder and IT team have device to migrate the on-premises infrastructure to cloud to improve the scalability, availability, security of the networking infrastructure and enhance digital communication between different branches. Below are the major technical limitations that are hinderance to Ozmart infrastructure:

**Scalability**: Current on-premises network consists of legacy cisco switches, routers and firewall that are unable to accommodate organisations growth and causing bottleneck. The legacy switch port and firewall port have limited bandwidth (in megabyte) and single point of failure that is the main cause of bottleneck.

**E-LAN connectivity**: Ethernet Local area Network connectivity between different branches (Sydney and Adelaide) using MPLS connection (technique used by telecommunication network that transfer data from one node to another based on short path). Due to MPLS connection the branches are unable to handle increase traffic.

**Resource Constrains**: Internal IT team is facing issues while allocating resources. Due to the legacy system the team have to carefully consider the requirement and compatibility before deploying new hardware. This task is time consuming and can be mitigated after moving to cloud as resources are available on demand in cloud.

**HA and Redundancy in Network:** Current networking infrastructure doesn’t have redundancy and High availability in case a hardware goes down. There are no proper power backups, failover for switches, routers or Firewall. There is not Disaster recover site setup for the server.

**Security**: Currently, Ozmart is only relying on CISCO firewall for all the security. There are no Endpoint protection software’s or log monitoring systems setup. Due to this there is limited visibility to the network traffic and hardware firewalls are hard to scale as the network traffic increases. There is no proper end to end encryption setup.