

## UPBOUND AIRLINES. CASE STUDY

Lokesh Bollini

Architecture component	Retain, Delete or Add More?	Pros/Cons of Change
Policy and Standards	Delete	<p><b>Pros:</b> Existing policy and standards are specifically designed for current IT infrastructure with around 120 employees in IT department. Hence modifying and delegating policies and standards to the cloud providers like Amazon, Zoho will be appropriate as they are providing tailored services for the company, and they have the right resources to create policies and standards that is appropriate for Upward Airlines and its operations.</p> <p><b>Cons:</b> Scrapping away current policies will limit the control over the potential policies that are introduced by the cloud services as they are mainly sided towards their business operations.</p>
Screening gateway routers	Delete	<p><b>Pros:</b> This is mainly used for basic level of protection by blocking traffic in the servers, however it is not efficient for large attacks. Since Upward Airlines are moving to cloud and the servers are being decommissioned, moving away from this routers is a ideal path and find better alternative in the cloud like Next generation firewalls(NGFWs) for more advanced security features.</p> <p><b>Cons:</b> Upward Airlines must be vigilant and proactive in contract stages to get assurance from cloud services to provide better alternative. This requires extra resources, costs</p>

		and negotiation part to get into contract.
Stateful gateway firewalls	Delete	<p><b>Pros:</b> Stateful gateway is mainly used to track active network connections. However, this process is very complex and costly. Cloud providers will have different personalized versions of this process and it will be included in the overall SLA.</p> <p><b>Cons:</b> The security measures that are followed by the cloud providers plays a vital role as this is a transferrable risk if any security risk arises from cloud vendor side.</p>
Virus walls	Delete	<p><b>Pros:</b> Virus walls are important if a company is using its own servers. Since Upward airlines are moving to cloud, proper cloud protections services are taken by cloud providers</p> <p><b>Cons:</b> This should be properly documented in contract/SLAs as every cloud provider will have their own set of controls for security measures. Hence choosing right provider with right security will be crucial.</p>
Spam filter on mail servers	Retain	<p><b>Pros:</b> Spam filters helps to protect against phishing, spam email. Even in cloud servers this is an important feature to be included.</p> <p><b>Cons:</b> Spam filters should be tailored as per the cloud vendors, and this should be scalable across the organization when implemented. Proper study needs to be done and should be included in SLA.</p>
Antivirus software on mail servers	Retain	<p><b>Pros:</b> Antivirus software on these servers has the logs of all historical data and the scans which is very important to be included in cloud to advance the security further.</p> <p><b>Cons:</b> Antivirus software involves permissions and access for very sensitive information, if not properly regulated there can be a huge attack on cloud platform.</p>
Network-	Delete	Pros: This will be maintained by cloud providers like Google,

based intrusion detection systems (IDSs)		<p>Amazon and Zoho. monitored accordingly. No need to maintain separate IDSs as servers are taken down and moving to cloud now.</p> <p><b>Cons:</b> Cost increase will happen when extra layers of security are added in cloud. These should be added in SLAs before forming contract.</p>
Data Loss Prevention (DLP)	Add	<p><b>Pros:</b> Prevents sensitive data from security attacks in the cloud environment.</p> <p><b>Cons:</b> This can be difficult to integrate and also availability for different vendors can pose an issue for scalability in long run when we want to change the provider in future</p>
Cloud Sandbox	Add	<p><b>Pros:</b> Before releasing into the production, sandbox can be used to test and analyse malicious bugs and rectify. This can be useful for quality purposes.</p> <p><b>Cons:</b> This can be expensive to execute. Also, cloud vendors will take time to provide tailored sandbox version.</p>
Cloud Identity and Access Management (CIAM)	Add	<p><b>Pros:</b> This gives centralized user management facilities and improved visibility over the cloud resources.</p> <p><b>Cons:</b> This can increase complexity and it will be very hard to change the vendor in future.</p>

## Citations:

1. <https://www2.deloitte.com/us/en/pages/consulting/articles/cloud-computing-for-airlines.html>
2. SWISS: Making air travel more sustainable and improving operational quality with Google Cloud: <https://cloud.google.com/customers/swiss>