



# Cloud Migration Ebook

## **Migration to Splunk Cloud**

- Migration Workshop
  - Full Migration
  - Hybrid Migration
  - Data Migration
  - Asset Migration
- 

## **On premise migration to your own managed cloud**

- A more dynamic Splunk environment
- 

## **Multicloud Cost Management with Splunk**

- Splunk Multicloud Cost Management App
  - Let Apto help you manage your cloud costs
- 

## **Apto Splunk Services**

- Apto Splunk Support

# Migration to Splunk Cloud

As Splunk's specialist partner in migration from your Splunk environments to the Splunk Cloud we are proud to deliver a streamlined package from an initial migration workshop discovery, to a fully functioning Splunk Cloud environment. Once the migration is complete, we will then train and impart the knowledge you need for your continued success with the new managed environment.

## Too good to be true?

Keep reading for information on the standard packages we can provide to you.



### Migration Workshop

Does your data need to be migrated to the cloud?

How much data would that be?

How will your data be migrated?

What assets do you currently have on your Splunk environment and how can we best package them into apps we deploy to the cloud?

How many forwarders currently exist and how much work will it take to redirect that data to the cloud?

These questions and more are vital for a successful migration to Splunk Cloud. We offer an initial migration workshop, so that you can weigh up the different options you have and together we can determine the best approach going forward.

Typically, we will then provide a full migration to Splunk Cloud (data and assets), hybrid migration to Splunk Cloud (only assets) or a migration to cloud infrastructure you manage such as AWS or Azure.

A standard migration workshop should take days with a writeup, not weeks and we can tailor an education course also. You can expect to receive expert recommendations and a plan of action to get you onto Splunk Cloud.

## Full Migration to Splunk Cloud

The full migration consists of moving both your assets and data into the cloud. The major benefit of this is that it enables you to decommission your old hardware, and start using Splunk Cloud, as soon as the data is migrated.

The main drawback is that you will have to carry out the data migration, which adds another level of complexity to the migration. Your assets will be bundled into apps, following Splunk best practices, and deployed. Once apps are installed in the cloud, the forwarders simply need to have their output switched to the new endpoint, so no data is lost.

Data migration is typically done by either shipping your physical hardware to AWS with their Snowball service, or data transfer over the internet using Smartstore as best practice.

While this can be complex and isn't risk free, it means you will get a fully searchable copy of your data into the cloud.

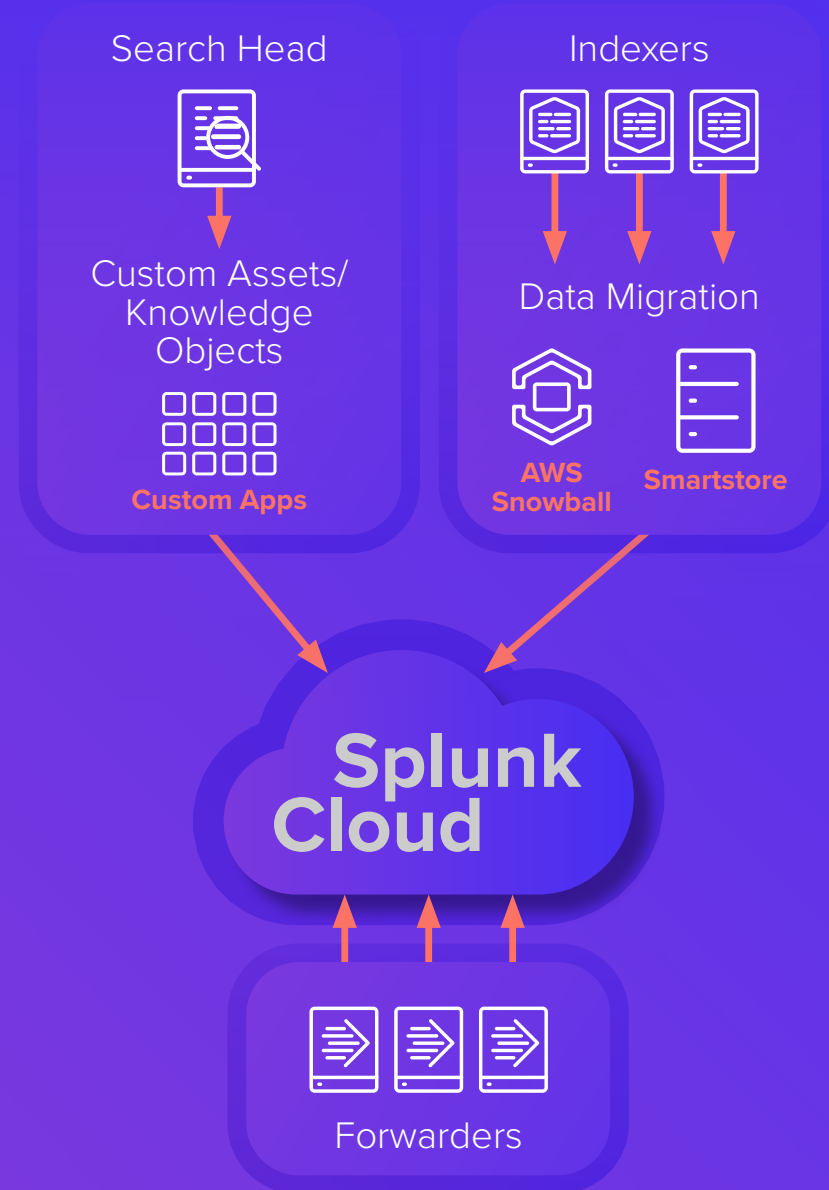
.....  
Migrate retained data to Splunk Cloud in AWS via Smartstore or AWS Snowmobile  
.....

Other assets and knowledge objects deployed to the cloud through Apps  
.....

Must be the same major version of Splunk  
.....

Forwarders Switched to point at the Cloud  
.....

Old Splunk infrastructure switched off  
.....



## Hybrid Migration

The hybrid migration involves migrating your assets and changing your forwarder's endpoint (you keep your data on your current infrastructure until it ages out).

The major reason to do this is to avoid the complexity of the data migration, especially if you have a very large amount of data, or simply to not avoid the cost of moving large amounts of data. The drawback is that you have to keep your current infrastructure.

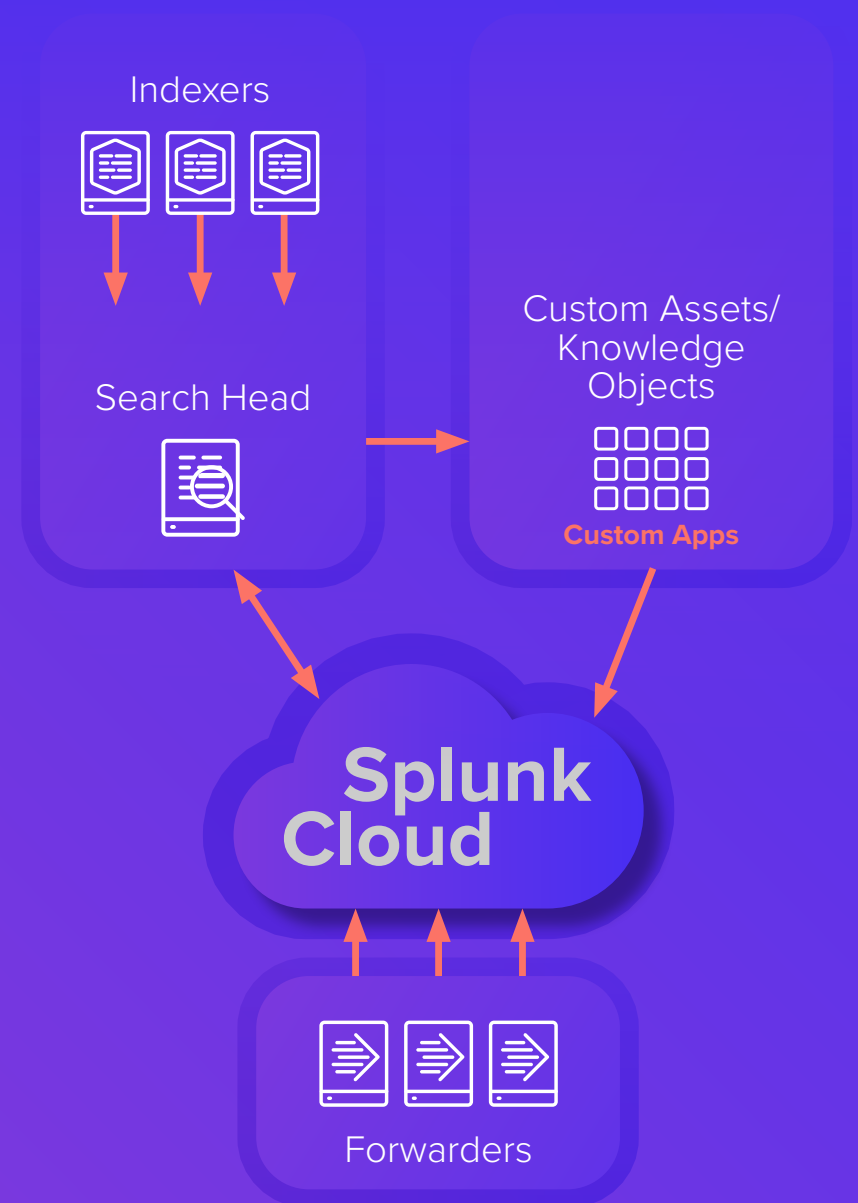
Keep retained data on current infrastructure until it ages off

Other assets and knowledge objects deployed to the cloud through Apps

Forwarders Switched to point at the Cloud

Must search from local search head until data ages off

Old Splunk infrastructure switched off once all data ages off





## Data Migration

When it comes to data migration there are several options for you to consider.

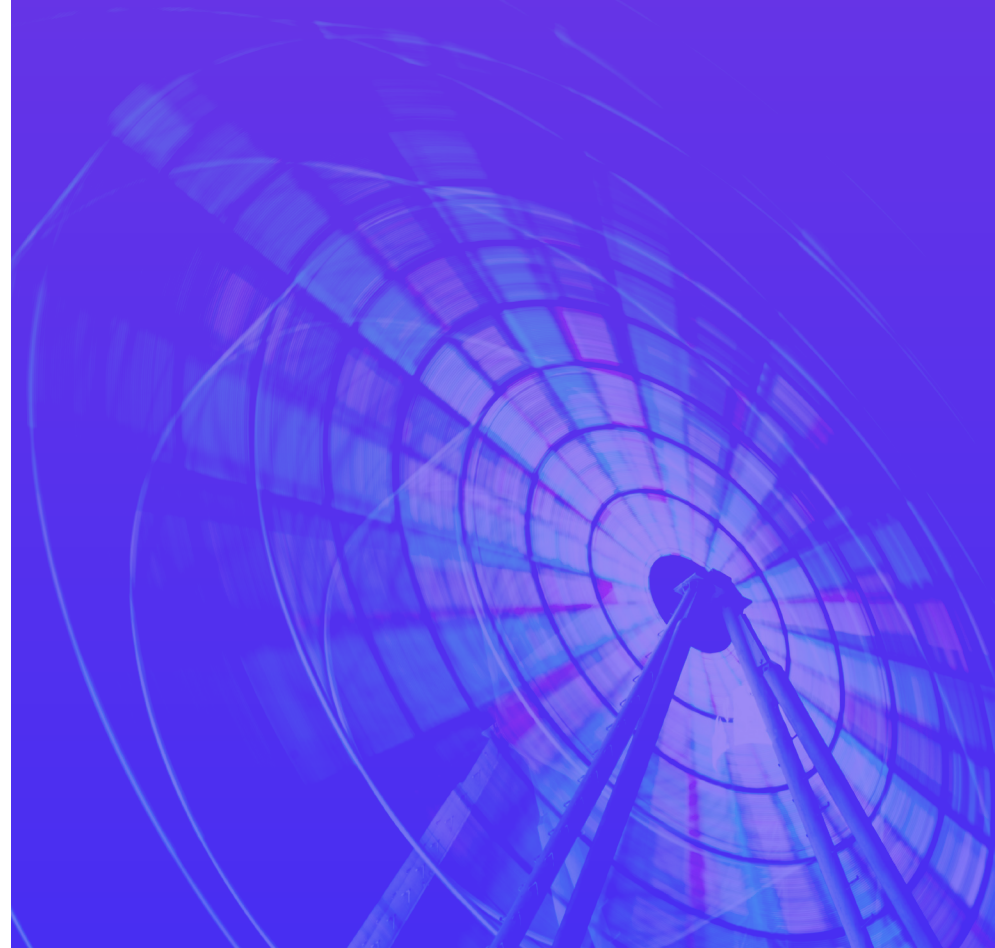
The standard method would be to network transfer your data into an S3 bucket using Splunk's [Smartstore](#). Once in the bucket the data can be very quickly transferred into your Cloud environment. The speed of this data transfer can be greatly increased by using services such as AWS Direct Connect or Azure's Express Route.

Network transfer is not always the best solution. If you have accumulated so much data that transferring it over a network could take days or even weeks then AWS Snowball can be considered. They will directly take a copy of your physical disks and deliver them to their warehouse, potentially saving a lot of time.

If moving from on-premise to your own managed cloud infrastructure, a simpler network transfer method would be to add your new indexers into your old cluster and decommission the old ones, one at a time. Splunk clusters will replicate their buckets over to others indexers in the cluster when one is decommissioned.

## Asset Migration

When we talk about asset migration this includes, but is not limited to: custom dashboards, alerts and other knowledge objects, custom props.conf for your sourcetypes, your index configuration or users and roles. We will assess what custom configuration you need migrated and bundle it into deployable apps.



# On premise migration to your own managed cloud

We do not only help our customers migrate to Splunk Cloud, often we provide customers with the expertise they need to move from on premise Splunk to their own managed cloud, be that AWS, Azure or any other cloud service.

Largely this solution also follows the hybrid or full migration plans, however the migration workshop is extended to assess exactly what architecture your new environment will require. We will plan a bespoke new architecture for your Splunk environment that will meet your current demands and scale into the future.

Furthermore, we can advise you on the exact specifications of cloud infrastructure you need to optimise its costs and performance. See the section below on our Multicloud Cost Management App to get a taste for some of the expertise we have in managing your cloud expenditure.

## A more dynamic Splunk environment

As cloud specialists, we have worked hard on developing unique cloud Splunk solutions, that focus on cloud best practices such as:

High availability

Scalability

Keep configuration as simple as possible

Use cloud managed services where possible

Go serverless

By following these best practices and by utilising technologies such as Terraform, Ansible and Docker we can deliver playbooks that provide many benefits over a classic Splunk deployment:

A cloud managed service with 99.99% availability and 30 second or less up time on new containers

Scalability to almost any load that can cope with even the largest data feeds such as VPC Flow Logs. By configuring an AWS Firehose or Azure Event Hub we can send practically any cloud data we'd like straight to Splunk. The lack of static architecture also means you can reduce your cloud costs when necessary.

A very config light solution that keeps the setup out of the Splunk side and in the cloud

Multiple completely serverless architecture tiers

A system that will keep up to date with the latest Splunk versions automatically



For more information check out our [blog](#).

# Multicloud Cost Management with Splunk

On an individual basis, costs can be negligible, but even in a small – but busy – cloud environment the charges will mount up very quickly. If left unchecked you could end up amassing lots of unused infrastructure that you still pay for such as detached storage and unused virtual machines.

We have had quite a few engagements with clients where, even if not hired to look at cloud, we have noticed cloud infrastructure that isn't being used. In some cases we found tens of thousands of dollars per month spent on infrastructure that is not even used!

However, it is possible to obtain real-time figures and to be alert to any anomalies to expected spend. When monitoring cloud spend, you should:

.....  
have auto actual vs budget analytics and alerts in place  
.....

have a mechanism to verify the spending is justified to multiple audiences  
.....

be able to charge back to your desired level of granularity  
.....

be able to run estimation calculations for different clouds, even before deployment.  
.....

Based on repeating this exercise a few times, we produce a Splunk App described in the next section, to allow our customers and everyone to start taking control back.



For more musings see our blogs

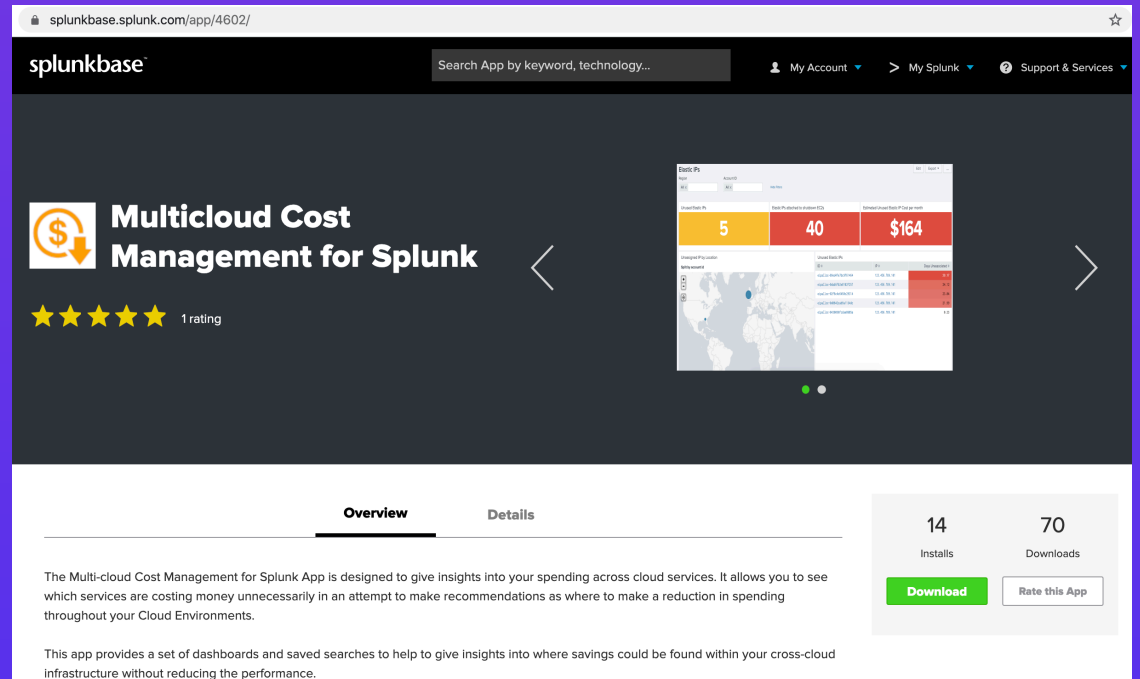
[How to reduce your cloud costs](#)

[Cloud Cost Management 2](#)

# Splunk Multicloud Cost Management App

Many Splunk users already ingest cloud data into their Splunk environment, real time cost management and alerting is only an App away!

We developed the **Multicloud Cost Management App**, that visualises your cloud spending, in one lens for AWS and Azure environments (GCP coming soon), for multiple accounts. This app will give you a taste of how you could start to manage your cloud spending, with data you were likely already ingesting into Splunk. Along side this, with our consulting expertise, we can help set up real time alerting and dashboard for your bespoke cloud needs.




The screenshot shows the Splunkbase app page for 'Multicloud Cost Management for Splunk'. The page features a dark header with the Splunkbase logo, a search bar, and links for 'My Account', 'My Splunk', and 'Support & Services'. The main content area displays the app's title, a 5-star rating, and a preview of the app's dashboard. The dashboard includes a 'Basic FYs' section with three cards showing '5', '40', and '\$164'. Below this is a 'Managed FYs' section with a world map and a table of data. The bottom section of the page has tabs for 'Overview' and 'Details', a description of the app, and statistics for '14 Installs' and '70 Downloads'. A green 'Download' button and a 'Rate this App' button are also visible.

splunkbase.splunk.com/app/4602/

splunkbase

Search App by keyword, technology...

My Account > My Splunk Support & Services

 **Multicloud Cost Management for Splunk**

★★★★★ 1 rating

**Basic FYs**

Category	Value
Managed FYs	5
Unmanaged FYs	40
Total FYs	\$164

**Managed FYs**

Region	Managed FYs	Unmanaged FYs	Total FYs
North America	2	10	12
Europe	1	5	6
Asia	1	3	4
Africa	1	2	3

**Overview** Details

The Multi-cloud Cost Management for Splunk App is designed to give insights into your spending across cloud services. It allows you to see which services are costing money unnecessarily in an attempt to make recommendations as where to make a reduction in spending throughout your Cloud Environments.

This app provides a set of dashboards and saved searches to help to give insights into where savings could be found within your cross-cloud infrastructure without reducing the performance.

14 Installs 70 Downloads

[Download](#) [Rate this App](#)



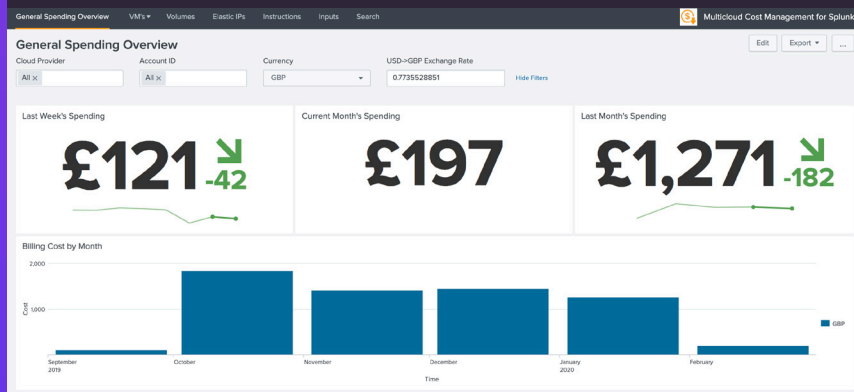
Find our app at

<https://splunkbase.splunk.com/app/4602/>

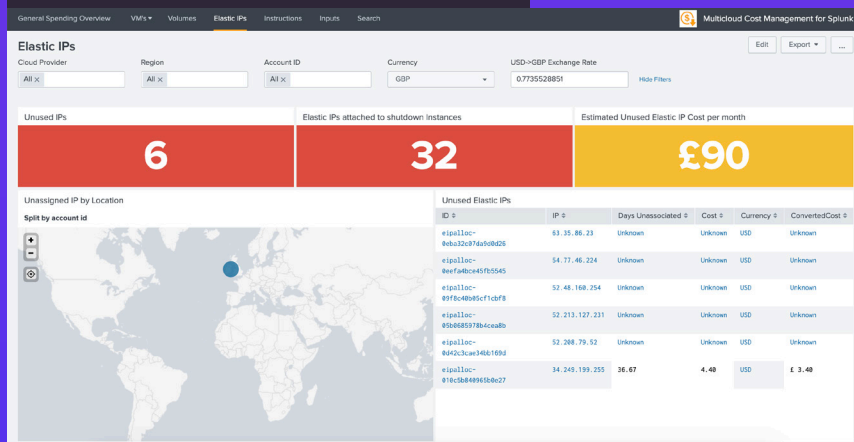


## Current features:

### Track your monthly and weekly spending trends over time



### Highlight unnecessary Elastic IPs



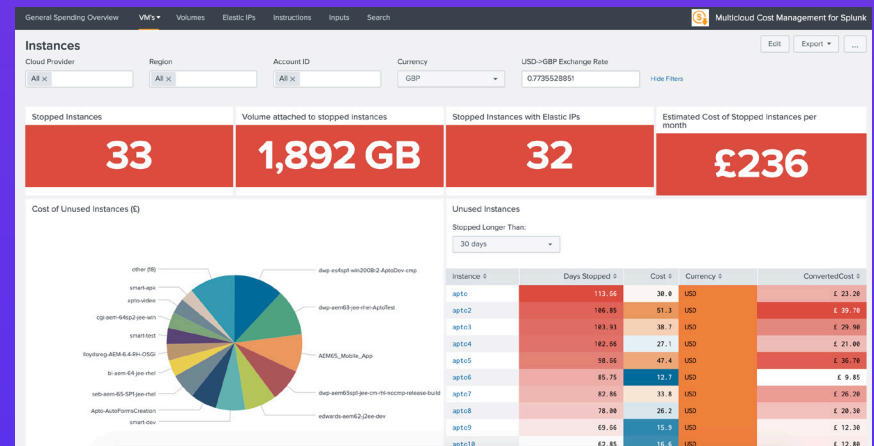
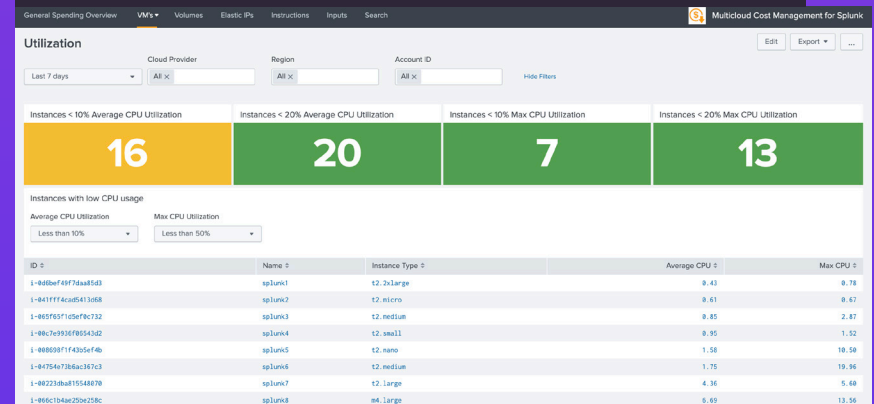
### Drilldown into your itemised spending

Cost by Resource January

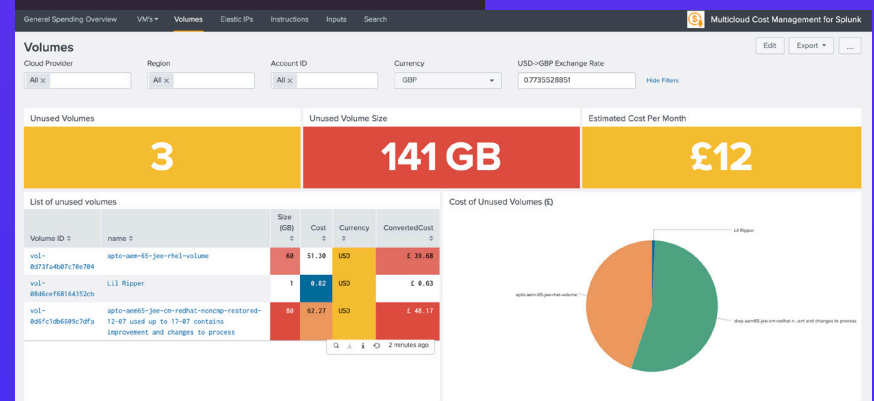
Search: splunk

Name	Cost	CurrencyCode	Converted Cost
apto-splunk-idx1	181.81	USD	£ 79.68
apto-splunk	72.34	USD	£ 56.42
splunk-sandbox	55.47	USD	£ 42.91
apto-splunk-idx1 volume	26.48	USD	£ 20.42
apto-splunk volume	18.56	USD	£ 8.17
snag-splunk-server_beforeAD	7.48	USD	£ 5.79
apto-splunk-indexer	7.43	USD	£ 5.75
splunk_test_for_grafana	3.42	USD	£ 2.65
apto-splunkidx1 to be shrunk	2.87	USD	£ 1.68
seem-63-splunk-ami	1.61	USD	£ 1.25

### Highlight under utilised and unused virtual machines



### Identify unattached volumes



# Let Apto help you manage your cloud costs

Apto can use Splunk and various other tools to analyse and monitor your cloud costs, ultimately reducing your cloud spend. But first we need to identify your particular pain points and specific needs. This pre discovery phase will move you from cloud use to active cloud management.



## A more dynamic Splunk environment

The pre-discovery phase will provide you with a plan to give you:

.....  
an understanding of your current position  
.....

a detailed understanding of the data you'll need to maintain that position  
.....

a review of potential tools to automate the data collection  
.....

an indication of the steps you'll need to take to maintain that automatic process.  
.....

Use the plan to manage cloud costs yourself, or engage us to deliver it and manage your cloud spend for you.

**We'll begin with a workshop of 4-5 hours to:**

.....  
define your problem areas  
.....

identify current constraints and discover what's holding you back  
.....

set clear objectives for the report, including recommended actions in user stories  
.....

identify the resources required, including administrators, techies and budget holders  
.....

commit to a timescale for the sprint and report presentation  
.....

define the sprint end date.  
.....

**Apto will then get to work with our 'technical tool box' to analyse your costs and reduce your cloud spend.**

# Apto Splunk Services

Aside from our specialisations we also provide a wide range of the more standard Splunk services

Design, install and configure Splunk including Cloud - achieving a Splunk Validated Architecture

Security, Cloud Cost Management and Automation Workshops

Design, install and configure Splunk ES, ITSI, UBA, Phantom and Splunkbase Apps

Analyse and review your existing Splunk Architecture and operational environment

Improve the performance of your existing Splunk, reviews include in-depth analysis and reports on an ah-hoc or package basis

Data Onboarding

Design and implement Dashboards and custom apps

Using your licence more its based on data ingestion capacity, use it!! We offer ingestion workshops to listen to what your business would like to see and we can hep with the how

Automation techniques

The list goes on! and we don't make customers fit a list so please [get in touch](#) to discuss your requirements.

## Apto Splunk Support

Apto Splunk Support provides the application support wrapper around Splunk the product. It triages your incidents, makes them replicable if Splunk support is needed, supports both technical and business users. We design the support around your applications and your environment, this is not product support its an entire application platform support, please read more [here](#).



# Contact us

---

## Call

+44(0)845 226 3351

---

## e-mail

[jeremy.hawkey@aptosolutions.co.uk](mailto:jeremy.hawkey@aptosolutions.co.uk)

---

## Web

[www.aptosolutions.co.uk](http://www.aptosolutions.co.uk)

---