Has FinOps Forgotten SaaS?

Razor-sharp decision-making takes Insight

Howard Daws

Technology Lead, Optimisation and Governance, Insight

Howard is responsible for the evolution of Insight's solutions to help clients optimise and govern their existing and future investments in technology and supply chain partnerships.

Over the past 20 years, Howard has designed and delivered a range of programmes for intellectual property owners, end-user client organisations and solution providers across many industries and geographies. He has helped to improve commercial positions, achieve efficient operations and maintain third-party relationships with particular focus on software licensing

Have you come across SaaS leakage? I can guarantee that you have, even if you haven't labelled it as such. You may not have noticed it among the noise about cloud, which seems to get most attention because it's exciting and continues to grow at pace. FinOps – the portmanteau not for Financial Operations but for Finance DevOps – exists to bring accountability to cloud spend. Not without good reason as it's very easy to spin up consumption of cloud services and can generate huge amounts of cost and inefficiency.

FinOps relates directly to cloud financing rather than the more generic accounting responsibilities that 'Financial Operations' refers to. Its other names include 'Cloud Financial Management' or Cloud Cost Optimisation'.

According to the FinOps Foundation,

So, it's all about the cloud. The problem with all this focus is that SaaS spending and cost leakage can be forgotten. But when you consider that the global SaaS market is expected to reach USD 186.6 billion in 2022, even a small percentage of leakage adds up to a significant amount.

With non-SaaS models, whether deployed on-premise or in the cloud, for perpetual and many subscription models, the spend level is set and often has a trust basis for consumption. A business might buy 1000 licences and renew however many it needs for the next year, and the year after that. There may be incremental licence purchases at defined or market rates, 'true-ups' around the time of renewal or less favourable compliance settlements. Likewise, if the demand goes down, the business will have some form of bargaining to right size contracts and costs.

> "FinOps is an evolving cloud financial management discipline and cultural practice that enables organisations to get maximum business value by helping engineering, finance, technology and business teams to collaborate on data-driven spending decisions."

SaaS is different. It's a bit like an old-school mobile phone bill from the '90s where the supplier billed customers for a committed tariff, which includes a certain level of calls and texts. Excesses are charged on an 'as-used' basis, or the usage level is restricted. As a user, you might see a listing of activity in a month, but validating it is time consuming and challenging it is rather pointless.

The SaaS provider bills the business in a similar way – knowing what has been consumed because it has gone through the application. The bill arrives based on the number of units available or used. Unfortunately, it is not always easy to validate or avoid additional costs. So, bills get paid on trust and value for money takes a hit.

In some cases, unlike with cloud services, the minimum committed tariff rises but cannot easily be lowered. Alternatively, with a capped pricing agreement you might see a 'you have hit your limit' message which isn't great for consumer satisfaction.

There are real risks of uncontrolled SaaS costs while wastage exists at the same time. That is where usage levels are a lot lower than what is being billed. Industry observers often state this gap to be around 30% on average. Three questions spring to mind; why does this happen, why do we allow it to happen and what can we do about it?

1. Why does it happen?

A new application can be a bit like a shiny new toy: all very exciting at first. Perhaps it shows you lots of data or provides a way to work differently, so it gets lots of use in the first few weeks. This could be from specific groups or across an organisation.

Then, as you acclimatise to it, you maybe use it once a week, once a month. A natural reluctance to change may hinder an organisation's adoption of new methods, or maybe the toy doesn't seem as shiny as the next one. Then it becomes something that you've got access to but don't really use. If you're using it for five minutes a month, you are consuming a licence, but you are not getting commercial value. Plus, the passage of time sees people and roles change. The licence can remain assigned despite it not being used. The same concept exists for data centre software and is a core driver for cloud wastage that FinOps focuses on.

2. Why do we allow this to happen?

Generally, it is a lack of capacity to focus on SaaS and limitations of Management Information (MI). There's often no visibility of how many dormant users there are or how hard allocated licences are being worked. It is easy to recall physical assets or licences that are linked to a device when a person leaves a company, but with SaaS there is no direct trace.

The MI challenge is increased with the use of multiple SaaS applications, which is common. In 2021, organisations used on average 110 SaaS applications[1] and other stats indicate that the average employee uses at least eight SaaS applications[2]. Each has its own logs and reports that might be used to identify redundancy. Compared to traditional installation or headcount-based metrics where a single data source can cover most bases, it is a daunting task and a major governance overhead for any business.

The same applies to SaaS applications with non-user-based metrics. There may be initial estimates or baselines for required licences, but there's much less data on utilisation. SaaS applications may only provide alerts when there is a need to increase capacity and acquire more entitlements.

This is where you run the risk of SaaS leakage. Money is draining away because there is insufficient governance to plug the holes.

3. What can we do about it?

It's safe to say that there is no silver bullet to solving SaaS leakage. It's inherent in the system. Not because SaaS providers are dishonest, but it just wasn't on the agenda when SaaS became a thing, and it hasn't proved easy to solve. Innovation is at the heart of technology development and reporting on licensing efficiency is not. Building MI that can significantly reduce future consumption and revenues it is not going to reach the top development priority.

Some Software Asset Management (SAM) tools will help to a degree, often providing counts of entitlements that have not been accessed in 30 or 90 days. They are often linked to identifying the initial cause of growing SaaS and cloud spend – so called shadow IT of distributed purchasing. Others may focus on tracking activities, prompting a need for detailed data analysis and careful handling of personal information. These tools can help IT governance and can provide quick wins around abandoned licences. To really identify the scale of SaaS leakage and achieve greater savings, you need to dig deeper. That's not possible or desirable for every SaaS application, but if you look at your top five or top ten SaaS providers and recoup 30% of future spend – that's going to deliver a sizeable return.

[1] https://www.statista.com/statistics/1233538/average-number-saas-apps-yearly/ [2] https://elitecontentmarketer.com/saas-stats/

Organisations seeking to right-size should look at reports and logs that are available from within the SaaS application but used for different purposes. This is the reverse of how the on-premise software audit industry was built in the early 2000s. They should also look to other data sources that can help in assessing consumption, such as network traffic, authentication services such as single sign-on records and talk to product owners and samples of the user population. This can help to profile 'full time' consumption versus occasional use.

This type of deep dive analysis still takes up considerable resource that the FinOps team may not have available as they focus on AWS and Azure cloud costs. So, maybe FinOps hasn't exactly 'forgotten' about SaaS, they just may not have the appetite or capacity to plug the SaaS leak. This is where bringing in external software asset management skills from Insight to discover opportunities to right size SaaS licensing can deliver strong returns on investment. When aligned to expertise in using fact-based positions to power commercial discussions, the sums add up.

Find out more

To learn more about how we can help optimise and govern your cloude and software assets, why not ask the experts?

Visit uk.insight.com or speak to our team

Razor-sharp decision-making takes Insight

Insight