
Is FinOps SaaS vergeten?

Verbeterde besluitvorming vereist Insight



Howard Daws

Technology Lead, Optimisation and Governance, Insight



Howard is verantwoordelijk voor de ontwikkeling van de oplossingen van Insight om cliënten te helpen bij het optimaliseren en beheren van hun bestaande en toekomstige investeringen in technologie en samenwerkingen in de supply chain.

In de afgelopen 20 jaar heeft Howard een reeks programma's ontworpen en geleverd voor eigenaars van intellectueel eigendom, end-user klantenorganisaties en leveranciers van oplossingen in verschillende sectoren en regio's. Hij heeft geholpen bij het verbeteren van commerciële posities, het realiseren van efficiënte activiteiten en het onderhouden van relaties met derden, met bijzondere aandacht voor softwarelicensing.



Hebt u reeds een 'SaaS-lek' ondervonden? Ik kan u garanderen dat u dat hebt gedaan, zelfs als u het niet als zodanig hebt gelabeld. Misschien heeft u het niet opgemerkt bij het lawaai rondom de cloud, dat de meeste aandacht lijkt te krijgen omdat het spannend is en maar blijft groeien. FinOps – het portmanteau niet voor Financial Operations maar voor Finance DevOps – is er om verantwoording af te leggen voor clouduitgaven. Niet zonder reden, want het is heel eenvoudig om de consumptie van clouddiensten op te drijven en kan enorme hoeveelheden kosten en inefficiëntie genereren.

FinOps heeft rechtstreeks betrekking op cloudfinanciering en niet zozeer op de algemenere boekhoudkundige verantwoordelijkheden waar 'Financial Operations' naar verwijst. Andere namen zijn 'Cloud Financial Management' of 'Cloud Cost Optimisation'.

Volgens de FinOps Foundation is

“FinOps een evoluerende clouddiscipline voor financieel management en culturele practice die organisaties in staat stelt maximale bedrijfswaarde te krijgen door engineering-, financiële, technologische en bedrijfsteams te helpen bij het samenwerken aan datagestuurde uitgavenbeslissingen.”

Het draait dus allemaal om de cloud. Het probleem met al deze focus is dat SaaS-bestedingen en kostenlekken vergeten kunnen worden. Maar als je bedenkt dat de wereldwijde SaaS-markt in 2022 naar verwachting 186.6 miljard dollar zal bereiken, dan komt zelfs een klein percentage lekkage neer op een aanzienlijk bedrag.

Met niet-SaaS-modellen, zowel on-premise als in de cloud, voor perpetual en veel abonnementsmodellen, wordt het bestedingsniveau bepaald en heeft het vaak een vertrouwensbasis voor consumptie. Een bedrijf zou 1000 licenties kunnen kopen en vernieuwen hoe veel het ook nodig heeft voor het komende jaar, en het jaar daarna. Er kunnen incrementele licentieaankopen zijn tegen vastgestelde of marktтарieven, 'true-ups' rond het moment van verlenging of minder gunstige compliance-afrekeningen. Als de vraag afneemt, zal het bedrijf ook een vorm van onderhandelingen hebben om contracten en kosten van de juiste omvang aan te gaan.



SaaS is anders. Het lijkt een beetje op een ouderwetse mobiele telefoonrekening uit de jaren '90, waarbij de leverancier klanten een vast tarief factureerde, inclusief een bepaald aantal telefoontjes en sms'jes. Excessen worden afgerekend op basis van 'as-used' of het gebruiksniveau wordt beperkt. Als gebruiker ziet u misschien een lijst met activiteiten over een maand, maar het valideren ervan is tijdrovend en uitdagend en tamelijk zinloos.

De SaaS-provider factureert het bedrijf op een vergelijkbare manier – wetend wat er verbruikt is omdat het de applicatie heeft doorlopen. De factuur komt binnen op basis van het aantal beschikbare of gebruikte eenheden. Helaas is het niet altijd eenvoudig om extra kosten te valideren of te vermijden. Facturen worden dus

betaald op basis van vertrouwen maar waarde krijgen voor uw geld, loopt een deuk op. In sommige gevallen, in tegenstelling tot clouddiensten, stijgt het minimaal vastgelegde tarief, maar dit kan niet eenvoudig worden verlaagd. Als alternatief kunt u met een 'capped pricing agreement' geconfronteerd worden met een 'you have hit your limit'-boodschap, wat niet goed is voor de klanttevredenheid.

Er zijn reële risico's op ongecontroleerde SaaS-kosten terwijl er tegelijkertijd verspilling is. Daar ligt het gebruik een stuk lager dan wat er gefactureerd wordt. Waarnemers in de sector zeggen vaak dat deze kloof gemiddeld ongeveer 30% bedraagt. Drie vragen doen zich voor: waarom gebeurt dit, waarom laten we het gebeuren en wat kunnen we eraan doen?

1. Hoe komt dat?

Een nieuwe applicatie kan een beetje als glanzend nieuw speelgoed zijn: in het begin allemaal heel spannend. Misschien laat het je veel data zien of biedt het een manier om anders te werken, waardoor het de eerste weken veel gebruikt wordt. Dit kan uit specifieke groepen of uit een hele organisatie bestaan.

En als u eraan gewend bent, kunt u het een keer per week en een keer per maand gebruiken. Een natuurlijke terughoudendheid om te veranderen kan de invoering van nieuwe methoden door een organisatie belemmeren, of misschien lijkt het speelgoed niet zo glanzend als het volgende. Dan wordt het iets waar je toegang toe hebt, maar niet echt gebruik van maakt. Als je het vijf minuten per maand gebruikt, gebruik je een licentie, maar krijg je geen commerciële waarde. Bovendien zorgt de tijd ervoor dat mensen en rollen binnen de organisatie kunnen veranderen. De licentie kan worden toegewezen ondanks dat deze niet wordt gebruikt. Hetzelfde concept bestaat voor datacentersoftware en is een belangrijke drijfveer voor cloudverspilling waarop FinOps zich richt.

2. Waarom laten we dit gebeuren?

Over het algemeen is het een gebrek aan capaciteit om te focussen op SaaS en beperkingen van managementinformatie (MI). Vaak is er geen zicht op hoeveel slapende gebruikers er zijn of hoe hard toegewezen licenties worden gebruikt. Het is gemakkelijk om fysieke assets of licenties terug te roepen die gekoppeld zijn aan een device wanneer een persoon een bedrijf verlaat, maar met SaaS is er geen directe tracerings.

De MI-uitdaging neemt toe met het gebruik van meerdere SaaS-applicaties, wat gebruikelijk is. In 2021 gebruikten organisaties gemiddeld 110 SaaS-applicaties¹ en andere statistieken dat de gemiddelde werknemer minstens acht SaaS-applicaties gebruikt.² Elk heeft zijn eigen logboeken en rapporten die kunnen worden gebruikt om redundantie te identificeren. Vergeleken met traditionele installatie- of personeelsgegevens, waarbij één enkele gegevensbron de meeste bases kan bestrijken, is dit een lastige taak en een

belangrijke governance-overhead voor elk bedrijf.

Hetzelfde geldt voor SaaS-applicaties met niet-gebruikersgebaseerde meetgegevens. Er kunnen initiële schattingen of basislijnen zijn voor vereiste licenties, maar er zijn veel minder gegevens over het gebruik. SaaS-applicaties kunnen enkel alerts geven wanneer er nood is aan capaciteitsuitbreiding en het verwerven van meer rechten.

Hier loop je het risico op SaaS-lekkage. Er loopt geld weg omdat er onvoldoende governance is om de gaten af te dichten.

3. Wat kunnen we eraan doen?

We kunnen gerust zeggen dat er geen wondermiddel is om SaaS-lekken op te lossen. Het is inherent aan het systeem. Niet omdat SaaS-providers oneerlijk zijn, maar het stond gewoon niet op de agenda toen SaaS een ding werd en het niet gemakkelijk is gebleken om dit op te lossen. Innovatie staat centraal in de technologische ontwikkeling en rapportage over de efficiëntie van licenties niet. Het bouwen van MI die het toekomstige verbruik en de toekomstige inkomsten aanzienlijk kan verminderen, zal niet de hoogste ontwikkelingsprioriteit krijgen.

Sommige Software Asset Management (SAM)-tools helpen tot op zekere hoogte en houden bij welke entitlements 30 of 90 dagen niet zijn geopend. Ze worden vaak gekoppeld aan het identificeren van de oorspronkelijke oorzaak van groeiende SaaS- en clouduitgaven – zogeheten schaduw-IT van gedistribueerde inkoop. Anderen richten zich op het volgen van activiteiten, waardoor er behoefte is aan gedetailleerde gegevensanalyse en zorgvuldige omgang met persoonsgegevens. Deze tools kunnen helpen bij IT-governance en kunnen snelle resultaten opleveren rond niet gebruikte licenties. Om de omvang van SaaS-lekkage echt te identificeren en meer besparingen te realiseren, moet u dieper graven. Dat is niet mogelijk of wenselijk voor elke SaaS-applicatie, maar als u kijkt naar uw top vijf of top tien SaaS-providers en 30% van de toekomstige uitgaven terugverdient, levert dat een aanzienlijk rendement op.

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



Organisaties die zoveel mogelijk lekkage willen voorkomen, moeten kijken naar rapporten en logs die beschikbaar zijn vanuit de SaaS-applicatie, maar voor verschillende doeleinden worden gebruikt. Dit is het omgekeerde van hoe de on-premise software audit industrie begin jaren 2000 werd gebouwd. Ze moeten ook kijken naar andere gegevensbronnen die kunnen helpen bij het beoordelen van de consumptie, zoals netwerkverkeer, authenticatiediensten zoals single sign-on records en praten met producteigenaren en samples van de gebruikerspopulatie. Dit kan helpen om het 'voltijds' verbruik te profileren ten opzichte van incidenteel gebruik.

Dit soort diepgaande analyse vergt nog steeds aanzienlijke resources die het FinOps-team mogelijk niet beschikbaar heeft omdat ze zich richten op AWS- en Azure-cloudkosten. Dus misschien is FinOps het SaaS-lek niet echt 'vergeten', maar heeft het gewoon niet de drive of capaciteit om het SaaS-lek te dichten. Dit is waar het inschakelen van externe software asset management-vaardigheden van Insight kansen kunnen bieden om uw SaaS-licenties en verbruik in evenwicht te krijgen, hetgeen een sterk rendement op de investering kan opleveren.



Meer weten

Als u meer wilt weten over hoe wij u kunnen helpen met het optimaliseren en beheren van uw software-assets, waarom vraagt u het niet aan één van onze experts?

[Bekijk Meet the Experts](#)

Verbeterde besluitvorming vereist Insight

Insight 