Cut Cloud Costs with Ghost User Cleanup

Organizations save money by auditing cloud subscriptions and eliminating unused alumni cloud user licenses

"Ghost employee" is a metaphorical term for an individual on the company payroll that doesn't actually work there. In some large organizations, as much as 2% of payroll is paid to former or fictitious employees. Ghost employees could result from errors, hiring manager fraud or payroll fraud. Smaller organizations appear to be more at risk for this type of loss than larger ones.[1]

Like ghost employees, "ghost cloud users" provide no value, also falling into the category of unnecessary and scary expenses. Idle user licenses account for a significant portion of total cloud spending, perhaps taking a bigger slice of the pie than business leaders realize.

25% of Growing Cloud Spending

As cloud usage grows, so will the need to track user counts and licenses. A typical mid-size business might subscribe to ten or more cloud services. Common services include online productivity applications like Office 365, payroll and Salesforce.com, e-commerce platforms, email, marketing and social media tools, accounting and cloud-based security.

Keeping up-to-date records of who has or no longer needs access to what cloud services can be a big challenge. Because tracking and updating licensing and user counts for all cloud services requires planning and effort, some organizations skip the effort and end up paying for more users than they currently have.

Carl Mazzanti, a NYC area cloud expert and managed services provider (MSP), estimates that up to one quarter of total cloud consumption arises from companies paying license fees for former users. With

cloud spending growing six times faster than total IT spending,[2] organizations that pay attention to user license counts will make those dollars go further.

Alumni Cleanup Overlooked

The ghost user problem exists because very few organizations clean up former employees' accounts for cloud subscription licenses or perform regular audits. They also fail to link payroll, phone, insurance and user accounts to discontinue all of them when employees leave.

Sometimes the problem arises from simple misunderstandings. For example, deactivating Salesforce users does not reduce the user license count. That may require the administrator to file a case with support requesting a reduction.

Perform a Cloud User Audit

To address the problem of ghost users, effective organizations establish exit procedures that include deactivating user accounts and reduce the license counts where possible. They regularly perform a cloud user audit that costs relatively little compared to the savings generated.

A cloud user audit might include activities like the following:

- Create a list of inactive accounts on Office 365 with a script to list and check users' last logon dates.

- Perform a Dynamics CRM user access audit. Microsoft Dynamics CRM Online 2016 Update supports this capability.

- Identify the additional procedures required to reduce license counts for deactivated Salesforce or other cloud service users.

- Find and terminate unused apps, including unused desktop app subscriptions. Eliminate apps that are merely distractions.

- Identify and work with line-of-business application owners to inventory, categorize and standardize apps.

- Develop scripts to regularly clean up unused Azure resources.

The audit is not trivial but neither are the savings. Organizations can scare up as much as 25 percent savings on cloud subscription fees by auditing users and reducing unneeded user counts. If done regularly with established procedures, the cost may be only a few hundred dollars per quarter.

[1]According to the Association of Certified Fraud Examiners, payroll fraud occurs nearly twice as often in small organizations as in large ones.

[2]According to International Data Corporation (IDC), worldwide spending on public cloud services will grow at a 19.4% compound annual growth rate (CAGR) -- almost six times the rate of overall IT spending growth –to more than $141 billion in 2019. Software as a Service (SaaS) will remain the dominant cloud computing type, capturing more than two thirds of all public cloud spending.