KEEPING CLOUD SPRAWL IN CHECK

Using the right tools to manage cloud services effectively is **essential for cost control** and optimizing IT assets.

EXECUTIVE SUMMARY

Cloud services simplify the deployment of resources, optimize IT utilization and cut costs. But, while the cloud can do all of these things, it can also create challenges if managed improperly. Too frequently, poor management practices lead to wasted resources, sometimes leaving even IT departments unsure of what software, infrastructure and platforms their organizations have deployed in the cloud.

The culprit: cloud sprawl.

Cloud sprawl occurs when organizations allow cloud resources to proliferate without keeping tabs on their investments. This can lead to issues ranging from overspending and lack of optimization to problems with security and compliance. Fortunately, organizations can take steps to get their cloud environments under control. By establishing clear cloud strategies, conducting audits, building transparency and implementing monitoring and asset management tools, IT departments can rein in cloud sprawl or even prevent it before it starts. As a result, organizations can enjoy the benefits that drew them to the cloud in the first place, while minimizing risk, reducing costs and creating a unified view of their IT assets.

Why Some Organizations Lose Control of the Cloud

No organization deploys cloud resources with the intention of creating a free-for-all environment where different departments purchase their own (often redundant) resources instead of coordinating their investments with the IT department. Rather, a move to the cloud usually is the result of a careful analysis showing that migrating resources off-premises can yield tangible benefits. These include flexibility, scalability, resource management, cost savings, simplified budgeting, ease of deployment and enhanced updating and patching. The cloud can deliver Software, Platform or Infrastructure as a Service, and organizations can turn to the cloud to instantly spin up machines for temporary projects and seasonal workloads, to test and develop new applications, and to provide email without having to manage on-premises equipment.

So how does the cloud result in new management headaches?

The fact is, the same ease of deployment that makes the cloud so attractive can create problems, especially if an organization lacks effective policies and guidelines. Take, for instance, the hypothetical example of an organization that invests in Office 365, Microsoft's popular suite of productivity software. The IT department no longer has to manage on-premises email, and users gain access to cloud tools such as Skype for Business and OneDrive for Business. The move has the potential to be a clear win-win.

But in reality, some users may never utilize — or even know they have access to — the other cloud tools beyond email. When they need to collaborate on documents, they may instead use a company credit card to purchase a consumer license for a stand-alone cloud file-sharing program, rather than utilizing OneDrive. Then, inevitably, some of these users will leave the organization. Without tools and practices to ensure proper management and visibility, the IT shop may never know that corporate data is sitting on a consumer cloud application — placed there by someone who no longer even works for the organization — creating an unnecessary monthly expense and, potentially, compliance and security issues.

Multiply these problems by the hundreds or thousands of users in a large enterprise — and by the myriad cloud tools at their disposal — and it's easy to see why cloud sprawl can be such a large problem for organizations.

Some of the chief risks associated with cloud sprawl include the following:

- **Security:** Until recently, IT teams maintained rigid control over access to computing resources and were able to exercise management and visibility over sensitive data with relative ease. The cloud, along with several other significant developments in IT, has dramatically changed this situation.

  In one recent survey by Forcepoint, 21 percent of cybersecurity professionals said critical data and intellectual property from their organizations were stored with public cloud services. Another 28 percent said the same about their data being on BYOD devices, and 25 percent said that critical data could be found on removable media. Perhaps most worrying, only 7 percent of respondents said they had "extremely good" visibility into how users handle critical data on enterprise and user-owned devices, as well as on applications. Sprawling cloud environments in which IT teams have limited visibility and management capabilities leave organizations vulnerable to attacks and data leaks.

- **Overspending:** When it's easy to purchase new software or services, it's easy for spending to increase, and when this spending isn't managed effectively, it can spin quickly into overspending. Organizations spend more than necessary on their cloud deployments, as a result of both initial over-provisioning and abandoned, unused resources that suck up dollars without providing any value. Too often, operational units purchase cloud resources without taking the time to accurately estimate the amount of computing, data analytics and storage

The Other Side of Compliance

For organizations in highly regulated industries, meeting the terms of software license agreements, while important, is a secondary compliance concern. These enterprises risk massive fines or other penalties if cloud sprawl leads to a failure to protect sensitive data. Just as significant, organizations that lose control of sensitive customer, patient or student data often face serious damage to their reputations.

Finance: Data security regulations and standards, such as the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act, outline strict data management processes, both to protect investors from fraud and to prevent their data from being shared without their knowledge.

Education: The Family Educational Rights and Privacy Act, which protects the privacy of student education records, applies to all schools that receive funds under Department of Education programs.

Healthcare: The Health Insurance Portability and Accountability Act requires healthcare providers to both protect patient data and to ensure that the data is accessible when it is needed to guarantee a high quality of care. Penalties can reach $50,000 or more per violation.

Retail: Any organization that processes credit or debit card transactions must comply with the Payment Card Industry Data Security Standard.

resources they need.

Perhaps just as frequently, these business units spin up resources for temporary projects and then fail to pull back the resources when those projects are complete. Overspending can also happen across an entire organization — with the full backing of the IT shop — when cloud resources aren't matched appropriately with user roles. For example, companies often pay for the "pro" or "plus" versions of software suites without realizing that many users only need basic functionality.

- **Lack of optimization:** When IT staff doesn't have full control of the cloud software and services being purchased throughout an organization, they can't connect users with the IT assets that best meet their needs and, thus, ensure that these resources are being used optimally. Lack of optimization is closely related to overspending, but may also include scenarios in which organizations invest in the appropriate amount of cloud resources but then simply fail to provide access to these resources to the users best positioned to utilize them. An organization with a well-managed cloud environment will often have a library where users can see which resources are available and then request temporary access. In contrast, in an organization with sprawling clouds, users often have no way of knowing which cloud resources are available.
- **Compliance:** It was easy enough for organizations to lose track of software licenses *before* the emergence of the cloud. Now, with users able to subscribe to cloud software and spin up resources in an instant, it's nearly impossible for IT teams to stay in compliance with software licensing agreements unless they appropriately manage their cloud environments. When vendors audit organizations with cloud sprawl problems, the result is often a hefty bill — an outcome that is even tougher to swallow when many of the resources causing noncompliance are "zombie" instances that no one in the organization is using anyway. With software management tools, organizations can ensure constant compliance, taking the sting out of vendor audits.
- **Unmanaged virtual machines:** Virtual machines, for the most part, have essentially the same licensing, security and compliance requirements as physical machines. An IT shop would never connect a physical server to a network and then leave it unattended and unmanaged. But when a user spins up virtual computing resources in the cloud and then leaves them unattended, that action can create the same sorts of problems as an unmanaged physical machine. Only through careful management can IT shops keep tabs on all of the virtual machines that users deploy in the cloud.

Using SAM to Manage Cloud Services Effectively

Organizations don't lose control of their cloud environments because the IT shops are lazy or inherently disorganized. Rather, many IT teams simply don't have the tools, policies and processes in place to effectively manage this newer model. Typically, when an organization first makes investments in the cloud, IT shops manage the new environment via manual processes — for example, setting up spreadsheets that detail all the cloud resources that are being used. This can work for a while, but these manual processes don't scale well as cloud environments inevitably grow, and IT shops can quickly lose track of all the cloud software, infrastructure and platforms various departments are using.

Manual management of routine and tedious tasks is costly and time-consuming. Manual processes tend to be slow, and can also be susceptible to human error, reducing the efficiency of a busy IT workforce. Furthermore, it is simply impossible to efficiently catalog, organize and search all the information associated with cloud investments using a basic spreadsheet. To effectively manage a cloud environment, IT shops need instant access to data about not only the resources a company is paying for, but also which versions of these resources have been purchased, who in the organization is using them, how much the

Going for Broker

As cloud environments grow, they become more difficult to secure. Cloud access security brokers can help. CASBs (pronounced "KAZ-bees") enforce security policies between cloud users and providers. They provide a control point to secure the use of cloud services from multiple providers. Tim Hanrahan, a cloud client executive with the CDW Cloud Team, outlines the pros and cons of three approaches to CASBs.

The API approach: This approach uses an application programming interface that doesn't sit directly between a request and the data. API-based solutions generally display improved performance, and they secure both managed and unmanaged traffic across multiple cloud services.

The reverse proxy approach: This is an "in-line" approach to securing cloud apps, as a proxy is an intermediary that sits directly in the network traffic path, between a requester (client) and one or more data sources (servers).

The forward proxy approach: This is another in-line approach, but forward proxies filter connections going out to the internet from clients sitting behind a firewall. The approach offers the ability to integrate any application, but also may be more difficult to deploy. Further, it may reduce end-user privacy and require the use of digital certificates.

resources cost and detailed information about product licenses and the terms of those licenses.

Software asset management (SAM) tools can play a valuable role in helping organizations manage their Software as a Service (SaaS) applications. The first step of the SAM process is discovery, which itself is made up of two phases: entitlements and deployment. During this initial discovery process, an organization achieves a comprehensive view of what software — including cloud software — it has purchased (and is therefore entitled to), and what software it has actually deployed. This automated approach to IT asset management allows IT departments to ensure that all technologies are considered in total and work in sync. However, these tools often require a significant investment, and therefore need backing from enterprise leaders. Too often, cloud management processes are conducted manually — leading to cloud sprawl — because executives aren't aware of the benefits of automated management.

An effective approach for controlling cloud sprawl should include several important steps:

- **Establish a clear cloud strategy:** A cloud strategy — drafted by an organization's CIO, in partnership with other business and IT leaders — guides cloud processes, policies and standards, and can also give stakeholders a framework with which to periodically re-examine cloud practices. When organizations carefully map out their cloud strategy and then communicate that strategy throughout the enterprise, users understand when and why cloud resources should be deployed and what approval procedures are in place to govern new purchases — preventing scenarios where individual departments make ad hoc, unilateral investments in cloud resources.

While the presence of a strategy cannot guarantee perfect compliance with enterprise guidelines by all employees, the absence of a strategy essentially guarantees noncompliance. Also, the process of creating a cloud strategy gives IT and business leaders a chance to do an in-depth exploration of existing and emerging cloud tools that can help them unlock value and gain a competitive edge, rather than scrambling to find resources when pain points occur.

- **Conduct periodic audits:** Regular health checks and internal audits can help organizations ensure that their cloud services are aligning with operational needs, preventing overspending and promoting compliance with vendor licensing agreements. Audits should cover all aspects of cloud services, including applications, virtualization platforms and underlying infrastructure components. In addition to helping organizations meet their goals, periodic internal audits can also help them prepare for external audits conducted by vendors.

Short of a major data breach, there are few events more anxiety-inducing for IT leaders than an external audit for which an organization is unprepared; when these audits find significant noncompliance, they can result in fines and retroactive licensing expenses ranging into the hundreds of thousands of dollars. Automated SAM tools allow enterprises to instantly generate snapshots of their current environments, thereby ensuring ongoing compliance.

- **Build transparency:** Ultimately, many organizations adopt cloud services to help users do their jobs better and more quickly. And, in fact, that's the same reason users themselves bring shadow IT into the organization. While shadow IT is a real problem, users don't circumvent the IT department and adopt their own cloud tools just for fun; they do it because they need the tools to help them complete specific tasks. Although both users and IT departments share the goal of improving workflows, a disconnect occurs when organizations don't give workers a way to see what cloud tools are already running within the enterprise environment and how to access them.

Faced with the hassle of tracking down resources from within the organization, many users will simply buy a new cloud license with a company credit card, helping them get to work right away. To meet users' needs, it's necessary to maintain a catalog of useful services, fulfill requests efficiently, and manage

Collaborating for Cloud Success

Especially in larger organizations, IT teams can sometimes lose track of who is responsible for what when it comes to the cloud. This presents a potentially dangerous scenario with regard to security. IT teams and IT security personnel should work together to ensure the security of an organization's cloud environment. In particular, teams should make sure everyone understands who "owns" each of the following security processes:

Endpoint security: Typical anti-virus solutions may not be a good fit for cloud-based environments. IT teams should collaborate to identify, implement and manage appropriate endpoint security solutions.

Patch management: Organizations should identify who is responsible for managing systems that regularly check for and download patches, as well as for running those patches in a test environment to evaluate their impact on the environment.

Identity and access management: Well-designed cloud environments will allow users single sign-on access to many of the solutions they need, but IT and security teams should work together to ensure that users are authorized to gain access only to the tools appropriate for their roles.

30% to 40%

The amount of waste in overall enterprise cloud spending[1]

More than 60%

The portion of users who employ public cloud file-sharing services to store and share enterprise data[2]

demand and capacity. By building transparency into their cloud environments, IT shops can set up users for success and limit instances of shadow IT.

- **Use a dashboard to monitor cloud performance:** While some software vendors give organizations access to management dashboards for their own specific products, most IT shops find that they need a comprehensive solution to bring metrics from different vendors together in a centralized location. Enterprise SAM tools, such as those from Snow Software, even give IT departments instant visibility into other factors, including the hardware that programs are running on and information about whether an organization has rights to upgrade or downgrade its software. As a result, IT workers can quickly determine whether a machine will be able to handle the next version of the software.

Another advantage of a SAM dashboard is the ability to compare available resources against actual usage. If a user has been given access to a $600 software suite, for example, but is using only $150 worth of those resources, the organization can redeploy the software in a way that optimizes utilization and prevents overspending.

The Benefits of Effective Cloud Management

There's no shame in an IT shop admitting that an organization's cloud environment is in chaos. In fact, in some ways, cloud sprawl is the inevitable — or, at least, likely — result of an IT model that doesn't require companies to invest in physical infrastructure to scale resources. It's understandable that many organizations adopted cloud services as they became available, rather than as part of a preplanned strategy. And it's also understandable that inefficient manual management processes have persisted as cloud environments have grown, because that's how most organizations have always done things, and many stakeholders weren't aware of a better way.

Now that cloud environments have begun to mature, however, the failure to rein in sprawl and institute effective management practices represents an enormous missed opportunity. While it can be difficult to step away from the day-to-day challenges that inevitably pop up in IT, it is essential for organizations to take the time to map out a comprehensive cloud strategy, explore tools that will ease management burdens and implement effective policies and practices. By investing time — and, perhaps, money — now, enterprises can limit problems and see benefits far into the future.

In particular, effective cloud management can help organizations achieve the following:

- **Unified view of cost and utilization:** When a cloud environment is properly managed, IT and business leaders have a comprehensive view of IT assets, including cloud services and software. This, in turn, helps organizations use these tools more effectively and efficiently. In a well-managed environment, IT staff can accurately track spending and historical trends, and can also attribute resource costs to specific departments, projects or applications, which aids with budgeting and enhances overall utilization. This sort of visibility dramatically improves the position of IT leaders during conversations about resource allocation.

In a sprawling cloud environment, it is difficult for IT leaders to argue with any real credibility that cloud resources are achieving a tangible return on investment, because the organization lacks information about both cost and utilization — two of the main factors needed to demonstrate the true value of the cloud. But in a well-managed environment, IT teams can make a detailed case about how specific cloud tools are helping to eliminate inefficiencies or increase revenue.

- **Minimized risk:** Any action taken to reduce the risk of a data leak or other successful cyberattack has the potential to save an enormous sum of money. In its 2017 "Cost of Data Breach Study," the Ponemon Institute found that the global average cost of a data breach now sits at $3.6 million. The average cost for each lost or stolen record containing sensitive and confidential information, meanwhile, is $141. Effective cloud management practices bolster security and reduce the number

Sources: [1]RightScale, "State of the Cloud Report," 2017; [2]Citrix, "Combating Cloud Sprawl: Why It's Now a Critical Need for Today's Enterprise," April 2017

of vulnerabilities that could be exposed to malicious outsiders. Reining in cloud sprawl also ensures that configurations meet enterprise standards, that data is properly secured and that operational continuity is maintained.

- **Reduced costs:** Various estimates peg the portion of cloud spending wasted through inefficiency at 35 percent or higher. This waste represents a huge opportunity to cut costs without having a negative impact. In an organization that wastes 35 percent of an annual $1 million in cloud spending through inefficiency, merely cutting that waste in half through improved management practices could net nearly $200,000 in savings each year. Effective cloud management helps organizations get rid of unneeded cloud expenses and optimize cloud resources, resulting in better results for less money.

CDW: A SAM Partner That Gets IT

CDW's trained and certified technology experts understand the intricacies of SAM and can help organizations take a comprehensive approach to deploying a solution that fits their unique environments. Our team of experts includes:

- **Software asset management specialists**: Our certified specialists can analyze your licenses in depth and provide reconciliation services to help you understand gaps between entitled and deployed licenses. They can help incorporate software asset management best practices into your regular systems management tasks.
- **Licensing account executives**: By attending onsite meetings and technology briefings, these specialists review your current environment.
- **Presales systems engineers**: The engineers are always available to answer in-depth software, licensing and technical questions.

For software licensing and asset management support services, CDW provides assessment, planning and design; assistance with evaluating software licensing program options; contract planning and management; configuration management; and onsite software installation and lifecycle support. Our step-by- step approach involves:

- An initial discovery session to understand goals, requirements and budget
- An assessment of the existing IT environment and definition of project requirements
- Detailed evaluations, recommendations, environment design and proof of concept
- Procurement, configuration and deployment of the chosen solution
- Telephone support and ongoing product lifecycle support

The CDW Approach

ASSESS

Evaluate business objectives, technology environments, and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

Learn more about how software asset management solutions and services from CDW can help you better manage your IT resources.

CDW offers cloud services for organizations at all levels of cloud maturity. Learn more about how we can help you prepare for growth in the cloud.

Explore Our Featured Partners

ivanti snow vmware®

CDW® PEOPLE WHO GET IT™