Bring **Enterprise Cloud**
Out of the Shadows

*Shine the light on Shadow IT with active policy enforcement and cloud automation*
Executive Summary

Cloud computing has proven revolutionary for organizations hoping to leverage technology, innovation and digital strategies to stay ahead of the competition. Business units can quickly provision up compute, storage and network resources as they need without IT bottlenecks. But easy access to cloud resources has a dark side—one that’s become a growing problem: Shadow IT. Engineers, developers and even business stakeholders are launching resources that IT is unaware of. And what IT doesn’t know can come back to haunt organizations, preventing the IT department from performing critical functions such as controlling security, compliance and costs.

Fortunately, solutions are available to mitigate the risks posed by Shadow IT, especially at production scale. The cloud automation platform developed by DivvyCloud provides comprehensive, real-time visibility of virtual resources and allows enterprises to set and automatically enforce policies regarding cloud provisioning and ongoing operations.

This white paper details the challenges Shadow IT poses for organizations and how DivvyCloud enables those organizations to effectively mitigate security, compliance and cost risks.
The Growing Problem of Shadow IT

IN JULY OF 2015, THE ARMY NATIONAL GUARD EXPERIENCED A TREMENDOUS DATA BREACH. SOCIAL SECURITY NUMBERS, HOME ADDRESSES, AND OTHER PERSONAL INFORMATION FOR APPROXIMATELY 850,000 CURRENT AND FORMER NATIONAL GUARD MEMBERS WERE EXPOSED. BUT THE CAUSE WASN’T WHAT ONE MIGHT THINK. IT WASN’T AN ATTACK FROM MALICIOUS HACKERS; THE BREACH RESULTED FROM AN IMPROPERLY HANDLED DATA TRANSFER TO A NON-ACCREDITED DATA CENTER AS PART OF A BUDGET ANALYSIS CONDUCTED BY A CONTRACT EMPLOYEE.

In other words, the Army National Guard’s data breach was one example of what can happen as a result of “Shadow IT” -- the acquisition of technology by a department or team without the approval, guidance or support of IT.

In the typical scenario, Shadow IT comes about when a business unit or product team becomes frustrated with IT’s inability to deliver what they need when they need it. With business units under increasing pressure to launch new initiatives under tight deadlines in order to win, serve and retain customers, they go off and spin up cloud-based resources on their own, often without informing IT.

Cloud service providers, such as Amazon Web Services (AWS), Google and Microsoft facilitate this behavior by making it simple to access IT infrastructure on demand. No longer must end users go to IT, contend with red tape and wait while IT orders a new server, physically installs it, connects it to a router and so on. Instead, users simply access the software-defined infrastructure, click a button, and voila, they now have new compute resources. These resources are paid for using corporate credit cards or, more often, by accessing an existing AWS or other corporate cloud accounts associated with a master contract and charging back costs.

ENTERPRISE IT IS LEFT HOLDING THE BAG

While cloud consumers are pleased with the rapid access to services, IT departments remain responsible for knowing where data is located and ensuring that it remains...
protected. Yet this type of Shadow IT in the cloud makes it very difficult for an IT department to fulfill its responsibilities because it is often unaware of the resources others in the organization have procured.

These resources are often complex to sort out. Companies find themselves with multiple accounts from numerous cloud service providers (CSPs) for multiple business units. Large numbers of resources can be acquired and distributed across cloud accounts, regions, and environments; it’s not uncommon to see hundreds of instances or thousands of snapshots, along with associated storage volumes, networks, subnets, and security groups. Organizations may even find themselves with growing numbers of new services from a given vendor. For example, AWS continues to introduce new services such as their Relational Database Service (RDS), ElastiCache, and Elastic Container Service (ECS).

Business and technical users that procure new services and haven’t had prior experience managing infrastructure, may not understand what they should and shouldn’t do in terms of configuration. They are probably unaware of how to properly configure security settings or how much capacity/memory to allocate. They may be ignorant of corporate IT rules, choose to ignore them or might just not think about them.

To make matters worse, even if IT were to have a handle on all these resources, the environment continually changes over its lifecycle. Users or the cloud platform itself may open a security rule, back up data to an unapproved region or add excessive compute power, racking up the monthly bill.

- A recent survey of 200 global CIOs by Brocade found that 83 percent of enterprises experienced unauthorized provisioning of cloud services. Nearly 72 percent of executives don’t know how many Shadow IT applications are being used in their organization.¹

- By 2018, Shadow IT will contribute up to 30% of IT activities, up from 15 percent in 2014, according to Gartner.

- A Cisco report found that the number of unauthorized cloud apps used by enterprises was approximately times higher than CIOs predicted. While CIOs reported an average of 51 cloud services running in their organizations, Cisco found that the actual number was closer to 730.³

¹ - "CIOs keep trying to defy cloud gravity" by Matt Asay, TechRepublic http://www.techrepublic.com/article/cios-keep-trying-to-defy-cloud-gravity/
Shadow Cloud Risks

_Lack of visibility and control over shadow cloud resources leads to numerous security, compliance and cost risks for organizations._

SECURITY RISKS

Security risks are the biggest concern for most organizations. Just seven percent of cloud services meet enterprise requirements for security, according to a recent report by Skyhigh Networks.\(^4\) Nearly half of the respondents to a Cloud Security Alliance survey claimed that the security of corporate data was their chief concern with regards to Shadow IT.\(^5\)

Shadow IT can cause security risks in many ways. These include:

- **Opening a back door into enterprise data.** People provisioning instances may not protect them with the appropriate firewall settings. Because some cloud accounts connect directly to the organization's systems, they unknowingly open a back door to those systems. In this case, malicious users can get in and access the organization's sensitive data.

- **Enabling DDoS attacks from the company's domain.** When people provision instances without proper security, an attacker can break into the unprotected instance. They then turn the server into a bot and can use that bot as part of a network performing distributed denial of service (DDoS) attacks. And, since they originate from company's resources, these attacks can harm the company's reputation as well as its wallet (particularly with auto-scaling).

- **Circumventing security policies.** An employee might open an unauthorized network port on a firewall so he or she can work on company projects from a remote location—such as coffee shop, home or airport, and then neglect to close the access point, creating a back-door that malicious intruders can enter.

---


• **Inadequately restricting permissions.** Employees may use cloud services such as AWS S3 Buckets for storing files. Although they can apply permissions, 40 percent of Fortune 500 companies have accounts that are too permissive and consequently leak company data. Shadow IT removes IT's ability to protect and monitor that data.

• **Incorrectly implementing policies.** When an organization creates user accounts that can access cloud services, IT may want to employ two-factor authentication, such as a Smartphone and a pin or fingerprint, to validate that the user is who they say they are. With Shadow IT, this policy may not be enforced.

### COMPLIANCE

Another pressing issue for organizations with regards to Shadow IT is compliance. A CSA survey found that 25 percent of respondents said *compliance is their second biggest concern.*\(^6\) When cloud-based applications are procured without the knowledge or approval of IT, the organization loses its ability to address both regulatory and corporate compliance issues.

**Regulatory compliance.** Regulations often demand that organizations implement specified controls and document their usage. However, a CSP (Cloud Service Provider) may not apply identity management, access control, backup or other practices required by various regulations to protect data, potentially exposing it to unauthorized access and compliance violations.

For example, SOX requires internal controls for ensuring accuracy and integrity of data in financial reports by requiring that information be verifiable and traceable. When data is handled by systems procured via Shadow IT, those systems are not necessarily subject to these security controls or audit capabilities.

Even if the resources implement required controls, they may violate the compliance-related documentation requirements.

**Corporate compliance issues.** Shadow cloud instances rarely adhere to corporate guidelines. For example, one organization had a policy that required users to run cloud resources only in the East Coast region of AWS. Because Amazon doesn’t display all of a company’s resources in one view, if someone spins up resources on the West Coast or in Japan, IT may not realize that resources exist in those unauthorized regions.

---

COST

Uncontrolled costs are another huge issue for companies with Shadow IT. Gartner client inquiries showed that it is not uncommon for public cloud service bills to be 2X to 3X higher than expected.\(^7\) Typical cost risks encountered with shadow IT include:

- **An inability to gauge actual costs.** Cloud providers won’t go out of their way to show what their services really cost. They’ll claim the service only costs 38 cents per hour but won’t state the cost of running the resource 24x7x365. Users selecting services can easily make uninformed decisions with regards to ongoing or extended service costs.

- **Excessive usage fees.** When an unprotected service is compromised and then used to launch a DDoS attack, costs skyrocket. Public clouds charge based on usage when data is transferred off the network. If malware on a compromised service is engaging in a DDoS attack and initiates massive amounts of traffic from an account, the account owner can be on the hook for thousands of dollars. Since IT may not know that the resources exist, this traffic and the associated charges can continue unchecked for long periods of time.

- **Duplicate services.** Costs can spiral as businesses unknowingly purchase duplicate services.

- **Over-Provisioned resources.** Users may over-provision because they want to make sure they have enough horsepower. After all, why would anyone want a Hyundai when they can have a Ferrari at the click of a button? Gartner found that many clients have asset utilization of just 10 percent to 20 percent suggesting there is significant room for optimization in usage and cost.\(^8\)

WHAT'S NEEDED IN A SOLUTION

End users understand that IT needs to sanction cloud resources... after all no one wants the hassle or personal liability of having done something wrong. But, they still demand rapid access to cloud services and compute capacity.

IT is well aware that it can’t prevent end users from chasing flexible solutions to their business needs or leveraging powerful cloud services from a wide variety of service providers. But IT does need visibility into what services end users provision and the ability to ensure that users adhere to high level policies for usage and security.

---


DivvyCloud provides comprehensive, real-time visibility of virtual resources and allows IT to define and enforce corporate policies regarding cloud provisioning and ongoing operations. The system can automatically discover everything running in public and private clouds and identify noncompliant resources as defined by company policy. DivvyCloud also tracks state changes in real time, conducts policy checks against those changes, and can take steps to automatically “heal” cloud resources back to a compliance state with those policies. This is often known as “self-healing infrastructure.”

DivvyCloud is distinguished by the following capabilities:

- **Cloud agnostic.** DivvyCloud can identify and track a broad range of compute, storage, network and advanced resources across leading public and private cloud platforms. It treats all servers the same according to company policy, whether they’re Amazon Web Services, Microsoft Azure, Google Compute Platform, VMware or Openstack deployments.

- **Provisioning agnostic.** Cloud resources can be provisioned via any provisioning method, whether through cloud provider portals, an automated provisioning or DevOps tool, DivvyCloud or a traditional CMP (Cloud Management Platform). DivvyCloud provides post-provisioning visibility, policy compliance and optimization.

- **Automated actions.** Many tools monitor and notify administrators but don’t take any action to address compliance issues. Once DivvyCloud detects an issue, it can take action to automatically apply the appropriate policy on the fly. DivvyCloud enables full resource lifecycle controls across clouds.

- **Extensible platform.** Many software products require administrators to conform to their unique way of doing things. DivvyCloud provides an extensible platform that can be tailored using customer Bots and add-ons. This allows organizations to design automated policies and integrations that meet their unique business requirements, without being limited by DivvyCloud conventions.
• **Community policy bots.** Customers can take advantage of a growing body of prebuilt policy automation bots. Common policy automation bots ship with the core software, including scheduled instances, cloud region control, and instance type control. Additional contributions from DivvyCloud, customers or individual technologists are available on DivvyCloud’s GitHub Repository.

• **Contextual understanding of cloud resources.** Simplistic monitoring solutions that enable IT to set narrowly defined thresholds for notifications are not robust enough for the complex, organic and interdependent nature of cloud computing. DivvyCloud understands the operational interdependencies between compute, storage, network and security services. Policies and automatic remediation can be implemented based on multiple, interdependent actions within the cloud infrastructure.

• **Retroactive policy compliance.** Many tools establish policies when the infrastructure is provisioned. But if policies need to be changed, the organization must tear down the system, change the configuration and relaunch. With DivvyCloud, when a policy is altered, DivvyCloud scans the network, finds resources that have become noncompliant, and automatically brings the environment back into compliance. DivvyCloud also discovers environments not created through a central provisioning tool and can apply policies to those environments.

**BENEFITS**

With DivvyCloud, organizations can address key security, compliance and cost concerns that they’re likely to encounter with Shadow IT.

**Improve security**

DivvyCloud is able to address potential security breaches and prevents DDoS attacks through its enforcement of security policies. DivvyCloud detects security policy violations as they occur and automatically brings the service into compliance. For example, DivvyCloud can detect and enforce policies preventing "users" from provisioning a server without a firewall, opening a port, employing an account without correct access permissions, or accessing a service without two-factor authentication. DivvyCloud can even track SSL certificate expirations and ensure that all SSL certificates are signed and not expired.

Because DivvyCloud allows organizations to set a baseline above which traffic shouldn’t go, it can stop DDoS attacks in their tracks. If a network is compromised and uses the
network to launch a DDoS attack, DivvyCloud will reveal the unusually large amount of outbound traffic, suspend the service and prompt an investigation.

**Enforce compliance**

Both regulatory and corporate compliance are enhanced with DivvyCloud. Organizations can use DivvyCloud to enforce compliance across all cloud environments. Audit trails demonstrate that controls are being followed and provide documentation of remediation steps taken to correct any issues.

**Control Costs**

The visibility and policy enforcement DivvyCloud provides also enables organizations to keep a handle on cloud service costs. The platform provides insight into actual service costs to help users make more intelligent decisions regarding what to provision. Organizations can create policies to set guard rails around what class of resources end users can configure. Because it enables organizations to set baselines on outgoing traffic and sends alerts when those are exceeded, DivvyCloud enables organizations to avoid excessive data usage costs in the event of a DDoS event.

By providing visibility into resource consumption, DivvyCloud also enables organizations to optimally size their cloud resources. For a Fortune 1000 company with thousands of servers, even a 10 percent cost reduction can translate into millions of dollars in savings.
Conclusion

With DivvyCloud, cloud resources provisioned by groups across an organization can now come out from the shadows. Business users retain the flexibility to access the resources they need to compete in a demanding business environment. IT gains the visibility and control necessary to ensure that the IT environment remains secure, compliant and cost effective.

For more information visit www.DivvyCloud.com or contact us at info@divvycloud.com.