Technical Review

DivvyCloud Cloud and Container Security

Date: July, 2019 **Author:** Tony Palmer, Senior Validation Analyst

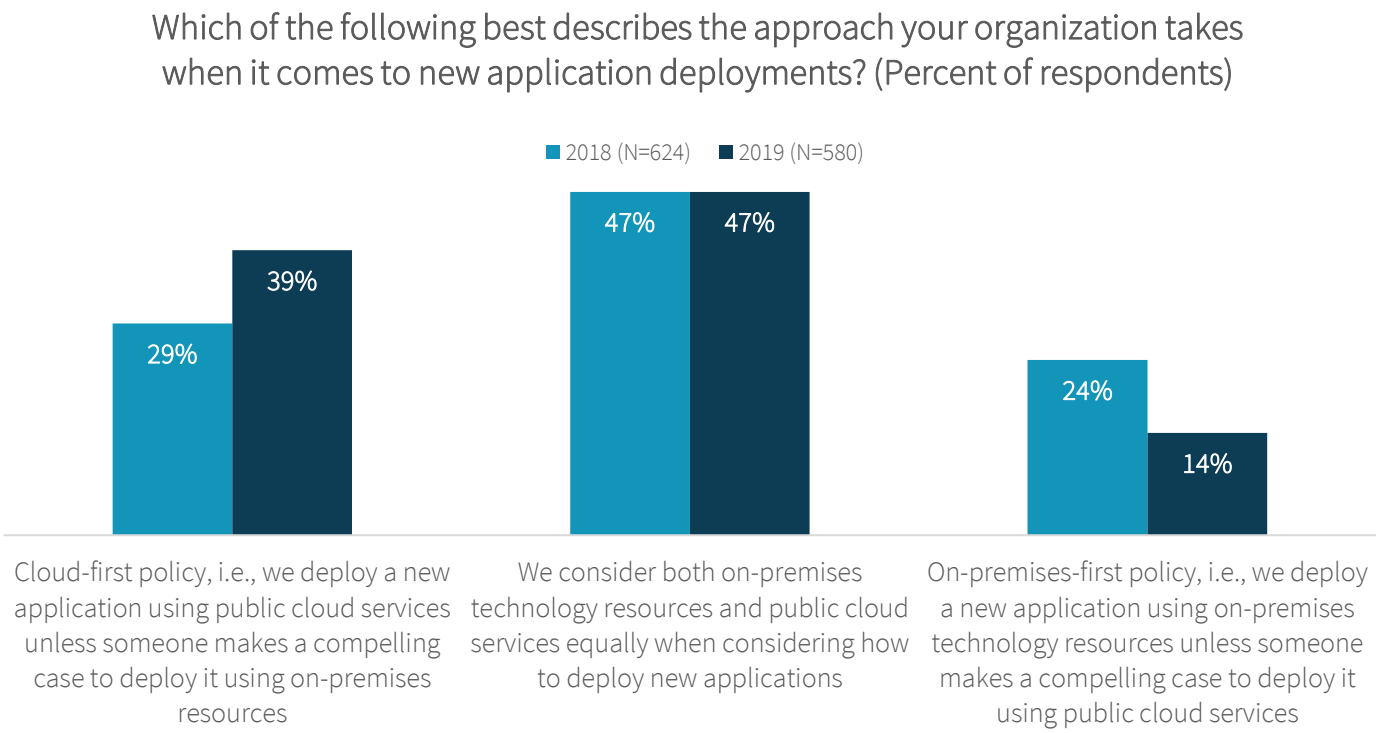
Abstract

This ESG Technical Review of DivvyCloud cloud and container security focuses on how DivvyCloud can enable a friction-free strategy for customers to embrace the cloud in their business operations. ESG explored DivvyCloud's extensible, multi-cloud, software-defined security and governance platform, and how DivvyCloud enables enhanced agility, decreases time to value, and provides automated security for cloud- and container-hosted workloads.

The Challenges

Organizations are increasingly using the agility of the cloud to drive innovation and digital transformation. According to ESG research, not only are more companies using public cloud IaaS (infrastructure-as-a-service)—58% in 2019, up from 42% in 2018—most of those organizations are at least considering cloud for new application deployments, and nearly 40% have a cloud-first policy in place (see Figure 1).[1] In addition, nearly half of those organizations are deploying production applications in the public cloud—49%, up from 46% in 2018. Looking at these trends together, it suggests that cloud is becoming ever more strategic; organizations are increasingly embracing cloud to enhance their ability to innovate and help them bring products and services to market more quickly.[2]

Figure 1. Cloud-first Strategies Becoming More Prevalent



Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.
[2] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

This exposes applications to potential risk that needs to be minimized. Organizations can't let response to risk create friction or slow down innovation, so many of them are compromising by sacrificing security for speed, with predictable results. A common example of this is in data breaches due to cloud misconfiguration. This problem will only continue to grow as storage of organizational data is shifting to public cloud services, including—increasingly—sensitive data. Specifically, almost one-quarter (24%) of respondents said that more than 40% of their corporate data resides on public cloud services today, which is expected to more than double to 58% of organizations within 24 months.[3] Following a similar trajectory, the amount of sensitive data residing in the cloud is expected to increase significantly over the next two years as well. Given the scope of the monetary and brand damage associated with breaches, the increasingly dangerous threat landscape, and the worsening shortage of strong cybersecurity skill sets, it is not surprising that cybersecurity is treated as a business risk rather than merely an IT issue.

The Solution: DivvyCloud

DivvyCloud provides an automated platform to analyze, identify, and remediate cloud infrastructure using customer-definable rules and actions. Once installed, configured, and connected to an organization's clouds, DivvyCloud discovers infrastructure resources across all clouds and distills this information into a normalized database. This database is used to analyze cloud operations, identify risks, and take actions.

DivvyCloud's extensible platform is designed to enable organizations to securely embrace public cloud and containers, giving developers the freedom to innovate without exposing the business to risk. Customers use DivvyCloud's real-time remediation to achieve continuous security and compliance in Amazon Web Services, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, Kubernetes, and other environments. Benefits of DivvyCloud's approach extend beyond IaaS to platform-as-a-service (PaaS), serverless or function-as-a-service (FaaS), and containers-as-a-service (CaaS). DivvyCloud protects cloud and container environments from misconfigurations, policy violations, threats, and IAM challenges. This enables DivvyCloud customers to achieve continuous security, compliance, and governance, and fully realize the benefits of cloud and container technology with freedom *and* control.

Table 1. DivvyCloud Supported Environments

Cloud Categories	Supported Environments
IaaS, PaaS, and Serverless / FaaS	Amazon Web Services—including AWS GovCloud and AWS China, Microsoft Azure—including Azure GovCloud and Azure China, Google Cloud Platform, Alibaba Cloud
CaaS	Amazon Elastic Container Service for Kubernetes (Amazon EKS), Azure Kubernetes Service (AKS), Google Kubernetes Engine (GKE)
Private Cloud	Kubernetes, OpenStack

Source: Enterprise Strategy Group

DivvyCloud Features and Capabilities

Unified Visibility and Monitoring

Unified visibility enables monitoring and understanding of security and compliance posture across all clouds and containers using a standardized asset inventory. DivvyCloud employs a two-tiered monitoring strategy that uses both API polling and an

[3] Ibid.

event-driven approach for faster detection of changes to cloud service configurations to achieve real-time automation and remediation.

DivvyCloud standardizes multi-cloud data to allow security professionals to write policies to resource types, rather than to specific cloud service provider (CSP) services. This is designed to make cloud security more accessible and future-proof policies as new services are released by CSPs. DivvyCloud has developed standard terminology used to describe cloud services across cloud environments. DivvyCloud uses the normalized terminology "Storage Container" for provider-specific resource names like S3 Bucket (AWS), Blob Storage Container (Microsoft Azure), Cloud Storage (Azure), or Swift (OpenStack). Using a standardized asset inventory, organizations can apply unified policies and automated real-time remediation across all environments. Additionally, DivvyCloud's standardized asset inventory is fully accessible via API and this data can be used to orchestrate cloud operations.

Automation & Real-time Remediation

The pace of cloud adoption has left many organizations vulnerable as they struggle to prioritize both innovation and security. DivvyCloud provides a platform to automate the protective and reactive controls necessary for an enterprise to innovate at the speed enabled by cloud environments. Automation is the key to achieving both security and speed at scale. Identifying risk and triggering remediation using API polling and event-driven harvesting, DivvyCloud provides fast detection of changes that enables automated remediation to occur in real time.

DivvyCloud provides a customizable automation engine that allows customers to quickly and easily define workflows—Bots in DivvyCloud terminology—that deliver remediation through orchestration of human-centered processes and third-party systems by programmatically taking lifecycle actions inside cloud environments. A single Bot can be configured to apply a unified approach to remediation across all clouds for a consistent, scalable, and sustainable approach to cloud security. Bots are composed of a scope, filters, and actions:

- Scope—the resources the Bot will evaluate; the Bot will only evaluate resources within the scope of clouds or resource groups chosen by the user.
- Filters—the conditions specifying what a Bot should act upon. DivvyCloud ships with more than 800 predefined filters, and it's easy to define custom filters to act on new signals or data that DivvyCloud should monitor.
- Actions—what a Bot does. DivvyCloud ships with hundreds of pre-defined actions and allows definition of custom actions.

Configuration Protection

DivvyCloud continuously monitors for configuration changes to cloud and container services to provide configuration protection. Each change is evaluated against an organization's policies. When a misconfiguration or policy violation is identified, remediation automatically addresses the risk in real time. All changes are detected by DivvyCloud's two-tiered approach whether via console, provisioning tools, or programmatically—this enables faster detection of changes and automation in real-time.

Organizations can immediately evaluate their cloud environments against hundreds of out-of-the-box policies that map to compliance and industry standards including PCI DSS, HIPAA, GDPR, SOC 2, ISO 27001, CIS Benchmarks for AWS, GCP, Azure, and Kubernetes, NIST CSF, NIST 800-53, FedRAMP CCM, and CSA CCM. Custom policies can be defined based on an organization's own needs and data.

Infrastructure as Code Protection

DivvyCloud integrates with the build process to prevent misconfigurations. This allows developers to move quickly and be more efficient, while providing security and governance. Teams can enforce cloud security and compliance policies at scale.

Infrastructure-as-Code (IaC) templates can be evaluated for security issues, misconfigurations, and policy violations. DivvyCloud's cloud asset inventory enables a simulated run against real cloud data to test policies before deployment. Policy

controls can be integrated into continuous integration and delivery (CI/CD) pipelines and ad-hoc API queries can be run at any point to validate templates. The build process can be immediately evaluated against DivvyCloud's hundreds of out-of-the-box policies that map to compliance and industry standards as described on page three.

Threat Protection

DivvyCloud's unified approach to monitoring and responding to threats to cloud accounts and workloads across multiple clouds is designed to simplify implementation of automation to reduce remediation and recovery time. DivvyCloud leverages CSP services—like Amazon GuardDuty—for threat detection that continuously monitors for malicious activity and unauthorized behavior. These CSP services use machine learning, anomaly detection, and integrated threat intelligence built by the CSPs themselves to identify and prioritize potential threats like crypto-currency mining, credential compromise behavior, communication with known command-and-control servers, and API calls from known malicious IPs.

DivvyCloud can perform automated remediation actions including reconfiguring cloud services, making changes to cloud infrastructure, driving human-centered workflows with integration into systems like ServiceNow and Jira, and orchestrating workflow actions in other security and management systems.

IAM Protection

DivvyCloud helps organizations govern Identity and Access Management (IAM) and adopt a unified zero trust security model across cloud and container environments where everything has an identity: users, applications, services, and systems. This provides enormous flexibility, but also creates the opportunity for substantial risk, as every service is potentially reachable by every other service, regardless of location if an implicit trust is defined. DivvyCloud helps address this perimeter fluidity and the substantial challenges of governing cloud environments at scale.

DivvyCloud helps build a circle of trusted identities and layers of trust to protect the identity perimeter at scale with automated monitoring and remediation around access management, role management, identity authentication, and compliance auditing, including: strong authentication to enforce MFA policies on cloud user accounts; least privilege to provide checks to restrict identities to do no more than they are permitted to; secure management of service accounts and service account keys; auditing to enforce best practices for the use of audit logs and cloud logging roles; and policy management to ensure that policies are implemented and managed appropriately, including identity-based policies, resource-based policies, permission boundaries, service control policies, access control lists, and session policies.

Risk Assessment & Auditing

DivvyCloud helps security, governance, risk, and compliance professionals quickly assess risk and make informed decisions about how to manage and remediate it. To build trust, organizations must be able to prove to executives, auditors, and stakeholders that their cloud environments are well-governed. The Compliance Scorecard delivers a visual representation of risk aligned with regulatory standards, industry standards, or custom corporate standards through an interactive heat map. This heat map provides a unified view across all cloud environments and can be filtered by factors like cloud environment, account, business unit, application, risk profile, compliance standard, etc.

Teams of all types—auditors, operations, security, and compliance—can use the Compliance Scorecard to identify risk and obtain guidance for appropriate action to remediate it. This provides proof to executives and auditors of the current and historical state of security and compliance. Additionally, it can be used to deliver clear and actionable data to inform business units and teams as to how security posture is trending and where improvement is needed. Results can be downloaded on demand, emailed on a scheduled cadence, or exported to cloud storage.

Extensible Platform

DivvyCloud provides levels of adaptability including: configuration through the user interface, customization through its plugin-based architecture, a flexible data model, and exposure of all functionality via RESTful API to facilitate automation in cloud environments. In practice, query filters identify target resources that meet a set of conditions. These can be used

individually or linked together. These filters can answer questions about data in the form of an Insight or instruct a Bot as to what resources to act on. Customers can extend DivvyCloud by using Python to write custom filters to answer new questions about the data.

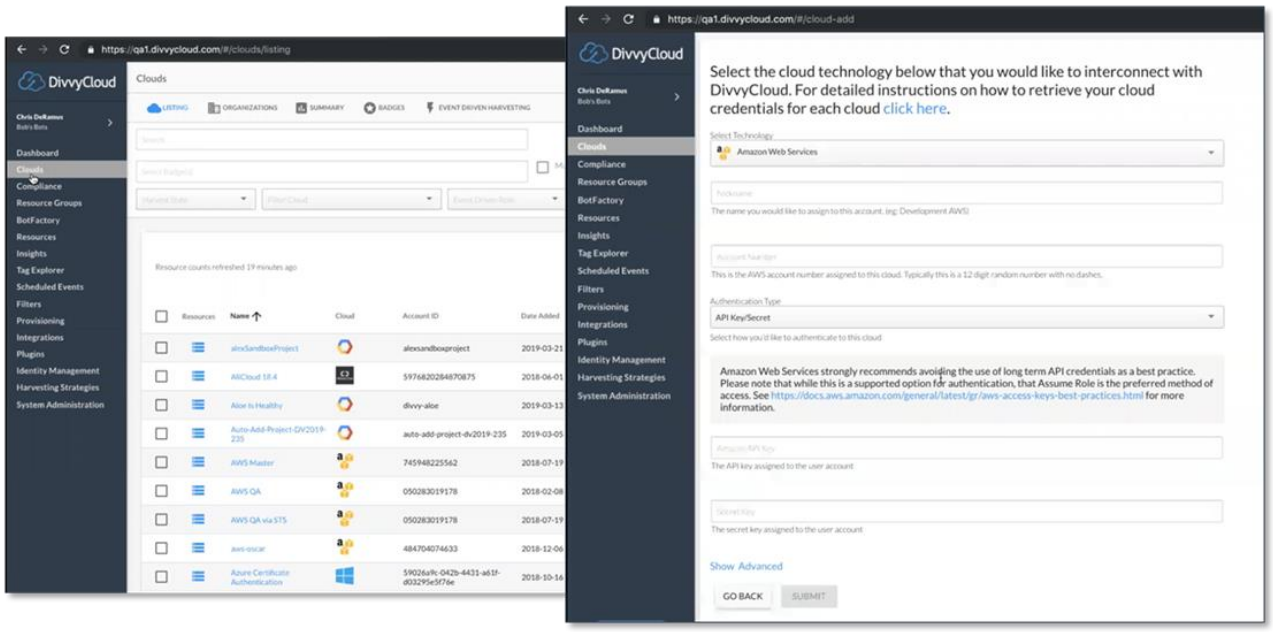
DivvyCloud is designed to integrate with external systems for both inbound—data aggregation, data collection—and outbound—notifications, ticketing—actions. The Integrations interface enables customers to easily configure third-party integrations, such as those for Slack, PagerDuty, ServiceNow, and others.

Combined, these capabilities provide a platform that delivers immediate value out-of-the-box but is also flexible and adaptable to address unique business needs of complex customers.

ESG Tested

First, ESG explored DivvyCloud's ability to provide a friction-free strategy for customers to adopt cloud. Figure 2 shows the ***Clouds*** view of the DivvyCloud dashboard. DivvyCloud connects to multiple clouds programmatically using the cloud providers' developer APIs. We clicked ***Add Cloud*** and entered the required credentials to access our endpoints and DivvyCloud started pulling data from the cloud—AWS, in this case—then modeling and normalizing it.

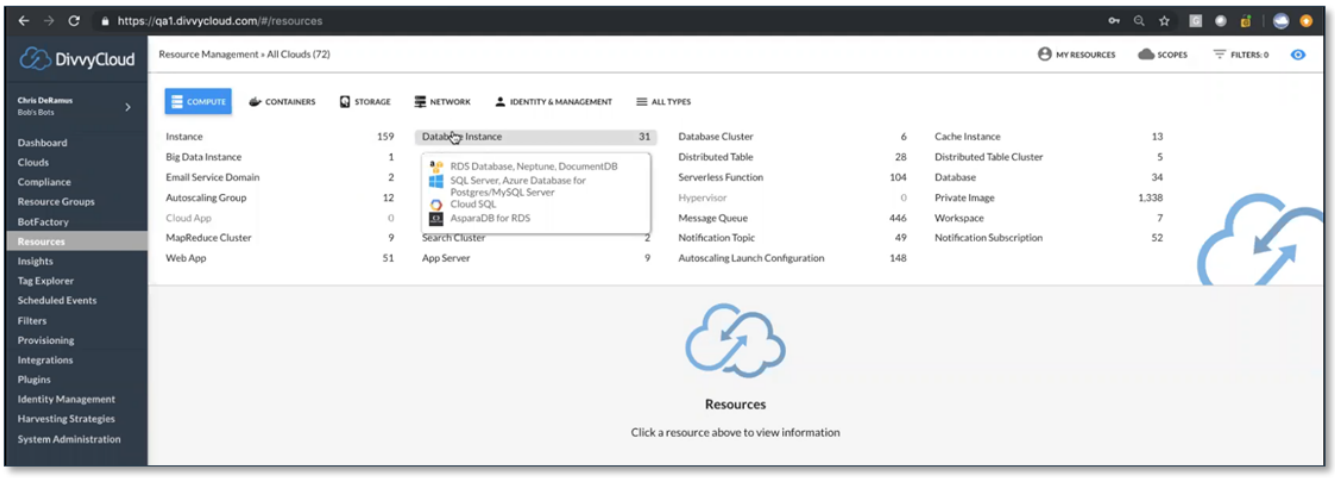
Figure 2. The DivvyCloud Dashboard—Adding a Cloud



Source: Enterprise Strategy Group

Figure 3 shows cloud compute ***Resources***. The most common resource type is a virtual machine or an instance. In this case, we are looking at 159 instances across multiple cloud technologies. Organizations can easily drill down using appropriate upstream vernacular to provide users with useful data about the instances, so it's easy to tell what cloud it's hosted on and what specific type of instance it is—for example, whether it's RDS, Cloud SQL, or SQL Server.

Figure 3. DivvyCloud Resource Management

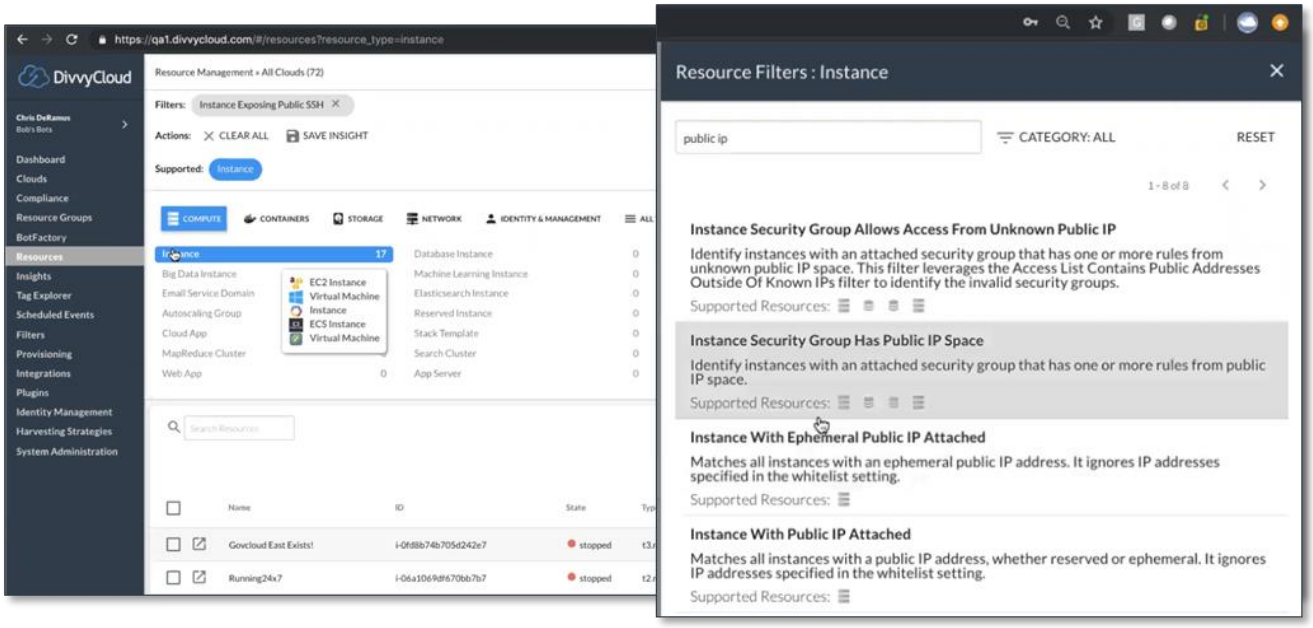


Source: Enterprise Strategy Group

Out of the box, the platform goes beyond getting you that single pane of glass across your cloud footprint. DivvyCloud enables organizations to quickly distill data into useful information. A common question from organizations with production workloads in the cloud is: How many instances do I have that are exposing SSH via TCP firewall or an Azure network security group? To answer this question, ESG ran a quick filter, and DivvyCloud identified 17 of the 159 instances, as seen in Figure 4.

DivvyCloud calls this an Insight. An Insight is a filter or collection of filters; organizations can group as many filters as they like into an Insight to look at factors like the lifecycle state of a resource. We added one filter to only show resources that were running and another to only show instances with a public IP address. With just a few clicks, we narrowed our view down from 159 instances to three that presented a real risk.

Figure 4. DivvyCloud Filters and Insights



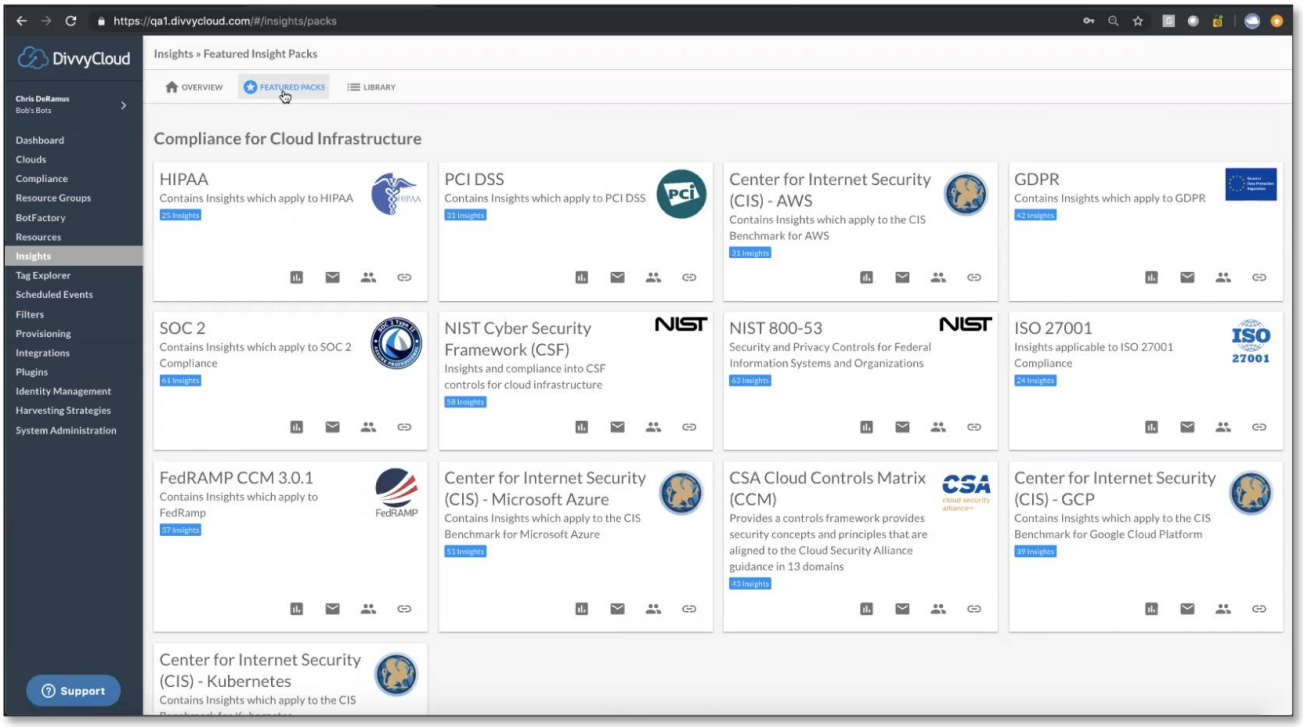
Source: Enterprise Strategy Group

The version of DivvyCloud ESG tested has nearly 800 predefined filters, and DivvyCloud says it is adding 50 to 75 per release. In addition to the hundreds of out-of-the box filters, clients can create their own filters to build custom Insights leveraging their own data. An example used by a large enterprise customer in the real world is managing global compliance strategy.

This customer has tens of thousands of applications in their total environment. Of those, just under 10,000 apps are approved to run in the cloud. Every resource created is tagged with an application ID. They use DivvyCloud to ingest their application database on a regular cadence, which gives them the ability to determine whether a resource's App ID is correct and valid and act upon that information. DivvyCloud custom filters enable organizations to pull in data from other sensors and then apply Insights from that data to their decision making in policy evaluation.

DivvyCloud took the top standards and benchmarks and operationalized them into a set of out-of-the-box Insights. Today, over 300 of them look at everything from elements like S3 buckets open to the world, public snapshots that expose data, cloud root accounts that are not doing multi-factor authentication, etc. Those Insights are aggregated into Compliance Packs to reflect common compliance frameworks today. Some of them focus on specific cloud technologies like CIS benchmarks, and DivvyCloud has Compliance Packs focused on CIS for Amazon, Azure, and Google Cloud Platform.

Figure 5. DivvyCloud Compliance Packs



Source: Enterprise Strategy Group

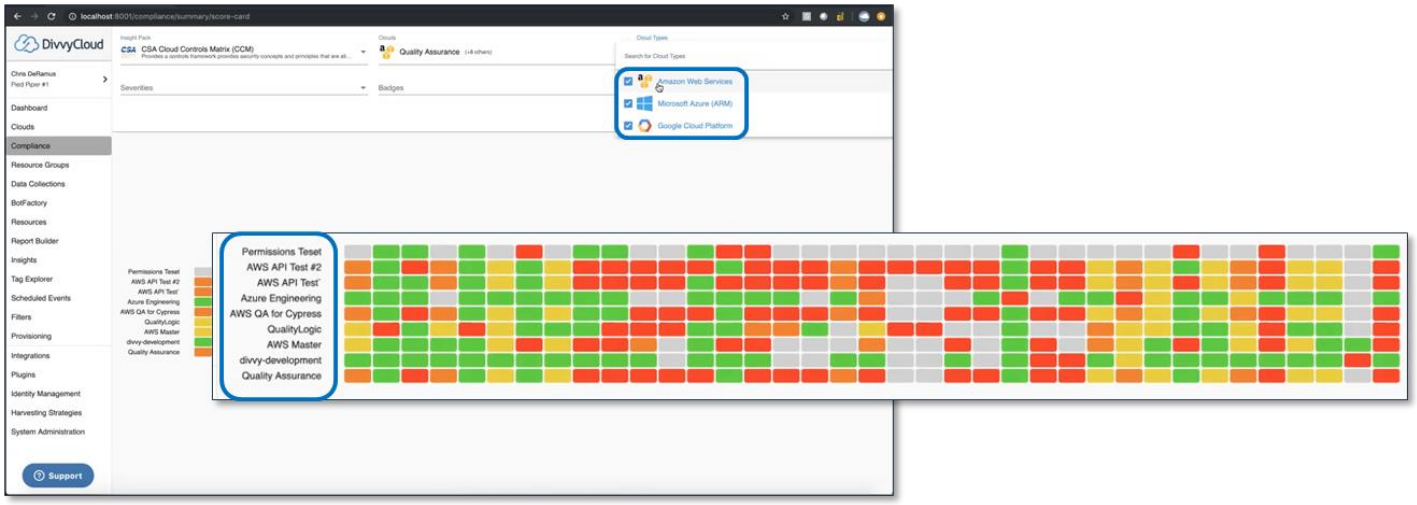
For frameworks that were written before the advent of the cloud like HIPAA and PCI, DivvyCloud does a lot of the abstraction automatically, reading the nomenclature and translating it into useful information. PCI requires that cardholder data be encrypted at rest and in transit, for example. DivvyCloud breaks that down to show IT staff issues that an organization needs to address to be compliant under each standard. With one click, an organization can see and potentially remediate issues with PCI compliance. Rather than manually analyzing 300 individual checks, IT can see the results of the 31 that apply to PCI, including the actual requirements and any impacted resources.

While these prebuilt Compliance Packs can accelerate an organization's path to governance, the real value of the platform comes from the ability to create custom packs tailored to each organization's unique mix of compliance and security requirements.

DivvyCloud Compliance Scorecard provides heat maps across a Compliance Pack or custom pack—shown in Figure 6—that allow analysts to look at the state of clouds, accounts, and resources, then sort them by severity or drill down into specific checks. Resources colored red are less than 85% compliant. Compliance Scorecard can assist teams across an organization—from auditors to operations, security teams to managers—in identifying areas with possible security or

compliance issues in a single view, then provide actionable Insights into both the appropriate actions to take, and the correct resources upon which to apply those actions to mitigate issues.

Figure 6. The DivvyCloud Compliance Scorecard



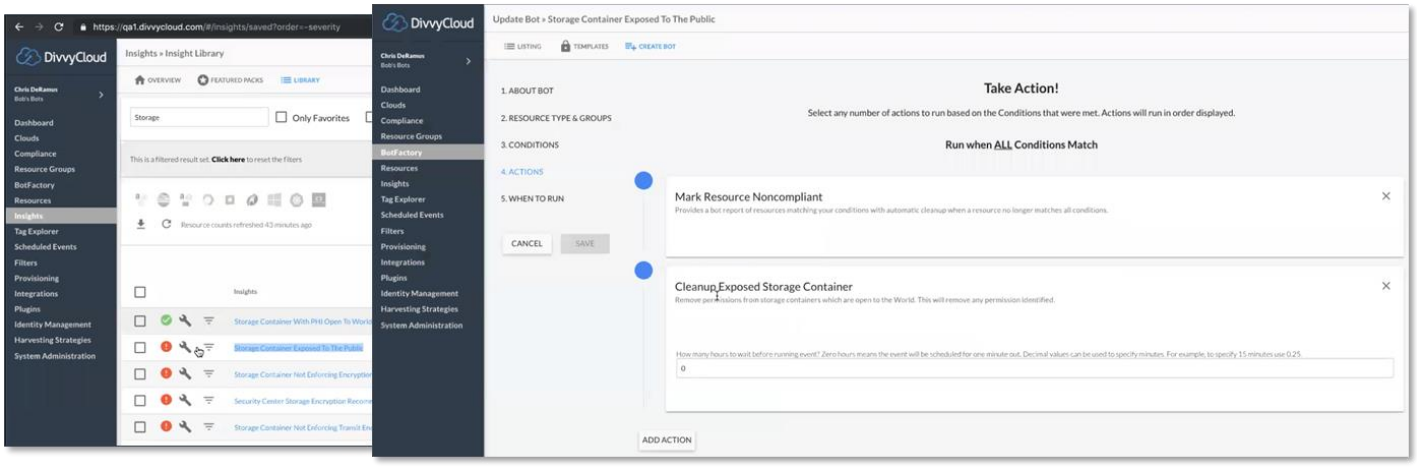
Source: Enterprise Strategy Group

Operators also get detailed Insight information, including an overview of the Insight and why it's important. Remediation processes, including recommended Bot workflows or manual remediation steps and compliance information showing the frameworks to which that specific Insight adheres are also provided.

Remediation is available for almost all DivvyCloud's Insights. The example we used to test this functionality was a common problem: S3 buckets exposed to the world. First, we inspected the situation by clicking on the Insight ***Storage Containers Exposed to the Public*** (as seen in Figure 4) to view a breakdown of which clouds are the biggest offenders for this problem. DivvyCloud does the heavy lifting to normalize this data and make it all look the same across all supported clouds.

DivvyCloud remediation is called Bot Factory. Organizations can build Bots to act on issues. In the example of an S3 storage container exposed to the public, a Bot can be configured to remove all IAM statements in that policy that are exposing it to the public, remove the access control list permissions that make it public, and perform notification and ticketing actions through systems like Jira, pagerduty, ServiceNOW, Slack, or Splunk. Additional integrations are in development and qualification by DivvyCloud.

Figure 7. DivvyCloud Automated Remediation—Bot Factory



Source: Enterprise Strategy Group

Why This Matters

As organizations continue to migrate their on-premises IT infrastructure to the cloud and build next generation applications in the cloud, security, compliance, and governance become more challenging. With 44% of respondents telling ESG that their on-premises data security is much more mature than their data security for public clouds,[4] significant quantities of organizational data that are considered sensitive are not sufficiently secured. Also, as organizations employ a combination of multiple cloud resources provided by both CSPs and SDDC solution providers, traffic can potentially pass between clouds without consistent governance. The ability to secure resources within and between clouds quickly, easily, and consistently, regardless of the underlying platform, would help IT to ensure consistent security policies across an organization. The ability to prove that these activities are happening continuously—and consistently with the appropriate compliance or governance frameworks—is key when seeking the support of executives, auditors, developers, and line of business leaders.

DivvyCloud is addressing these issues by providing a platform for customers to build Insights based on their own data and requirements—integrating with multiple clouds and containers to provide a normalized view of data across all cloud platforms and applications, which creates a frictionless strategy for organizations to adopt cloud without compromising security or compliance.

ESG validated an environment where DivvyCloud provided automated visibility, controls, and remediation across AWS, Google Cloud Platform, Kubernetes, and Azure. We saw how DivvyCloud can monitor risk programmatically using APIs or event-driven harvesting with automatic tagging to provide visibility, management, and enforcement across cloud platforms, reducing the inherent complexity of managing security in multi-cloud environments. Compliance Scorecard can help an organization to improve compliance *and* significantly strengthen its security posture. Automated remediation via Bots makes the entire process continuous.

[4] Source: ESG Master Survey Results, *Trends In Cloud Data Security*, January 2019

The Bigger Truth

When information technology is centrally commanded and controlled by the IT organization, the monolithic approach to delivering IT services creates friction that depresses innovation and makes companies less agile and competitive. This encourages developers to go around IT to directly purchase and access IT services in the cloud. This is the concept of shadow IT, and while it can improve agility and speed, it weakens organizations' ability to consistently adhere to security and compliance standards.

In this modern IT environment, where organizations leverage multiple cloud platforms to provide an agile IT infrastructure, managing security policies consistently, while focusing on workloads and applications, becomes critical. The nature of the cloud introduces security, compliance, and governance risks—traffic that moves between instances within and between clouds and containers, data exposure due to misconfigurations, inconsistent controls, excessive privileges, and lack of visibility into resources are some examples.

ESG validated that DivvyCloud identifies security risks in real time, takes automatic user-defined action to fix issues before bad actors exploit them, and enhances governance by automating tagging of resources. We also looked at how DivvyCloud automates enforcement of policies mapped to a wide variety of compliance frameworks such as NIST Cyber Security Framework, PCI DSS, SOC 2, CSA Cloud Controls Matrix, CIS, and GDPR. We found that DivvyCloud succeeds at doing all of this in a way that is holistic and unified.

If your organization is looking to achieve automated, continuous security, governance, and compliance in hybrid multi-cloud and container environments while improving security and compliance posture as compared with traditional infrastructure, you'll want to take a close look at DivvyCloud.