Keeping your Cloud out of the News

An organization that is transitioning to a cloud provider such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP) should immediately consider a shift towards a new model of security, namely continuous control and enforcement of secure configuration of cloud services. Importantly, this cannot be a one-time event, but must be monitored and enforced constantly, as the software-defined nature of cloud leads to frequent changes.

Misconfiguring a cloud database, storage asset, or search engine can have massive consequences, especially if they contain company-proprietary data. Just ask Capital One, whose recent misconfigured firewall led to a former employee of AWS using web application firewall credentials to obtain privilege escalation, which allowed access to one of their S3 buckets, and a subsequent exposure of over 100 million users' data. Facebook, earlier this year, exposed 540 million user records due to a misconfigured AWS S3 bucket from not one, but two different Facebook apps. A publicly accessible MongoDB database with misconfigured settings put Verification.io in the news when they exposed 150 gigabytes of customer data. Elasticsearch misconfigurations, a more recent culprit, left companies including Rubrik, Voipo, Meditab, and Dow Jones with exposed caches of customer information on publicly accessible servers without passwords.

This epidemic has already seen the leakage of more than 14 billion data records in the last five years as reported by Breach Level Index.

Without a holistic approach to security, companies open themselves up to undue risk mostly caused by:

- Inexperienced users
- Failure to shift from outdated security models
- A lack of unified cloud visibility
- Unprecedented rate of change, scale, & scope

Other Notable Recent Company Breaches

Fed Ex (unprotected cloud server)
Verizon (open S3 bucket)
Dow Jones (open cloud storage)
Adidas (undisclosed cause)
National Credit Federation (open S3 bucket)
Australian Broadcasting Corp (open S3 bucket)
Macy's (undisclosed cause)
GoDaddy (open S3 bucket)

> "Through 2022, at least 95% of cloud security failures will be the customer's fault,"
>
> **- Gartner**

Install DivvyCloud today with a free 30-day trial and make cloud misconfigurations a thing of the past.

www.divvycloud.com/get-started
2111 Wilson Blvd, Suite #450
Arlington, VA 22201
+1 (571) 290-5077

Databases, storage containers, and other cloud data repositories are often incorrectly configured. For example, permissions may be too broad, allowing anyone access. These misconfigurations are often the result of human error. A developer may have tweaked a storage container configuration as part of troubleshooting, leaving it open to the public. Once the application began working again, they moved on to another project, forgetting about the exposed data. Organizations are often made vulnerable because they don't have processes in place to prevent, detect, and repair improperly configured cloud data services.

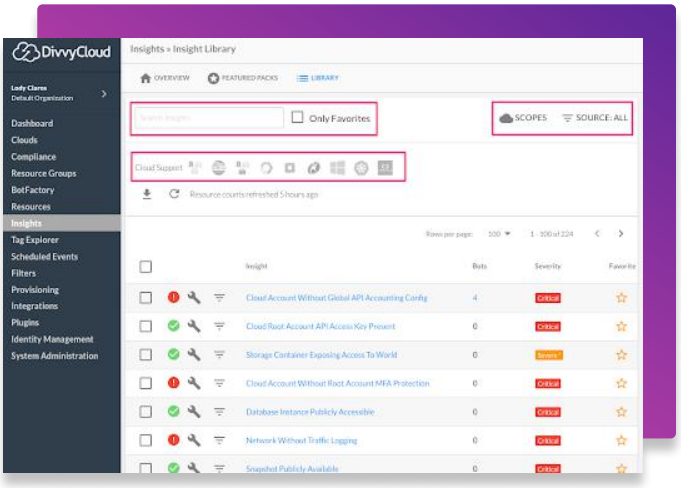

Image 1: Insight Library

How Does DivvyCloud help?

DivvyCloud provides an automated platform, utilized by leading cloud adopters like The Discovery Channel, Twilio, General Electric, Kroger, Fannie Mae, and Autodesk, to analyze, identify, and remediate cloud infrastructure using customer-definable rules and actions. DivvyCloud's 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. 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.

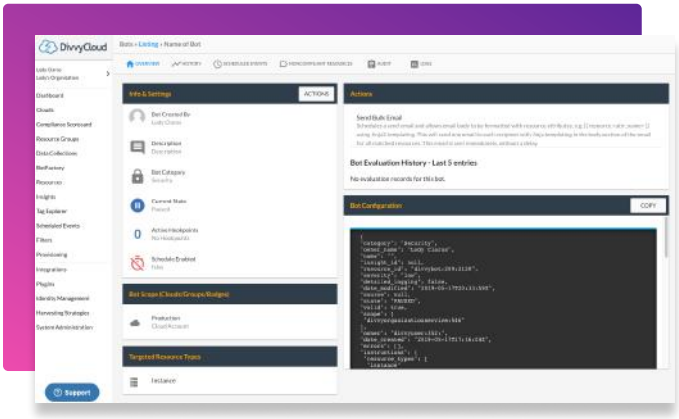

Image 2: Bot Overview

Core to DivvyCloud's platform is an easy-to-use interface from which clients can deploy more than 200 standard security policies, or create their own to manage their cloud environments. At scale, policy enforcement cannot and should not be performed manually. DivvyCloud customers can discover and automatically take action to address security issues. Automation allows for simultaneous offense and defense, resulting in increased innovation and reduction of risk.

DivvyCloud - multi-layer security

Many solutions focus on one layer of security, whether network / firewall-based, IAM policy lockdown or account governance. DivvyCloud knows that true cloud security is at many layers. To that end, DivvyCloud policies address the key weak points not only in CapitalOne's data breach, but in other multi-vector attacks, allowing for real-time detection and elimination of vulnerabilities.

1. Ensuring account-level controls, logging, auditing and monitoring
2. Configuration of storage bucket and compute layers to remediate public access in real-time.
3. Configurable policy-driven approach to find resource-based roles out of standard.
4. Visibility into IAM roles and policies across all accounts, with least privilege control.

