Boost Your Data Protection with Cloud DLP: Your Solution to Complex Data Challenges

With massive cloud migration happening everywhere in the business world, data has become omnipresent and ubiquitous. From Software as a Service (SaaS) applications to data storage services, collaboration apps, webmail, and video conferencing - cloud data has found its way into every corner of our workspaces. As a result, organizations face the arduous task of managing a colossal amount of confidential data spread across diverse platforms.

Consider this: an organization could potentially have 30 versions of a contract, distributed across 5 different data repositories, and located in 15 different places. This is where the reality of modern data management strikes hard.

Organizations struggle with three primary cloud data challenges:

- Huge migration of data to the Cloud
- Exponential growth in cloud data
- Diverse types of data, including intellectual property, financial, business confidential, and regulated PII/PCI/PHI data, scattered across complex cloud environments

How can an organization overcome these significant hurdles? Enter Cloud Data Loss Prevention (Cloud DLP).

Cloud DLP aims to provide organizations with consistent data security and management tools, protecting their SaaS and IaaS resources — protecting sensitive organizational data from cyber attacks, insider threats, and accidental exposures.

With Cloud DLP, even small security teams can focus on analyzing risk findings and taking timely action rather than getting bogged down with managing and administering complex systems.

We've put together a step-by-step guide on how best-of-breed Cloud DLP solutions go about protecting data in your organization.

1. AUTONOMOUS, SEMANTIC-BASED DATA DISCOVERY

Let Cloud DLP do the work for you. Your first step is allowing the system to automatically identify all your sensitive data without the hassle of creating and managing rules or policies. Cloud DLP can process structured and unstructured data across various data repositories, providing a comprehensive overview of your sensitive data.

Action item: Leverage Cloud DLP for autonomous data discovery across all your cloud and on-premises, structured and unstructured repositories.

2. AUTOMATED DATA RISK IDENTIFICATION AND REMEDIATION

Once your sensitive cloud data is identified, the next step involves understanding the risks associated with different access rights, permissions, activities, or locations. Use Cloud DLP to get a clear picture of potential risks and then take proactive steps to mitigate them.

Action item: Analyze your data, looking beyond its type, and consider the surrounding context, including applications, networks, data classifications, users, identities, and event types.

3. ENFORCE COMPLIANCE AND PREVENT DATA LEAKS

Cloud DLP isn't just about identifying and mitigating risks. It's also instrumental in maintaining regulatory or privacy compliance and preventing data leaks, which is critical to your organization's overall data security framework.

Action item: Utilize Cloud DLP to enforce compliance standards and reduce the risk of data leaks.

4. IMPROVE EFFICIENCY AND COST SAVINGS

The automation-based features of Cloud DLP help improve security team efficiency by reducing the time and resources required to manually review and classify data. This step also increases cost savings due to reduced costs associated with incident response and recovery.

Action item: Leverage the automation features of Cloud DLP to enhance efficiency and achieve significant cost savings.

5. EFFORTLESS IMPLEMENTATION

Finally, take advantage of the ease of implementation that comes with best-of-breed Cloud DLP. With a secure, API-based solution, you can deploy your data loss prevention measures effortlessly across structured and unstructured data repositories,

without the need for agents.
Action item: Implement an API-based Cloud DLP solution that seamlessly integrates with your existing data infrastructure.

Why Concentric for Cloud DLP?

Concentric's Cloud DLP solution can address your complex data security challenges by providing the following benefits:

- Prevent data breaches and block unauthorized access to sensitive data
- Ensure, improve, and maintain regulatory or privacy compliance
- Reduce the risk of data leaks
- Automate the process of identifying and protecting sensitive data, improving efficiency, and reducing the time and resources required for manual data review and classification
- Reduces costs associated with responding to and recovering from incidents, leading to significant cost savingS

With Concentric, you'll be able to:

- Discover, monitor and protect all cloud data types, whether it's structured, unstructured or shared via messaging services
- Gain a risk-based view of cloud data and users
- Leverage automated remediation to instantly fix access and activity violations
- Find risk without rules, formal policies, regex, or end-user involvement
- Secure API-based SaaS solution with no agents required
- Have the peace of mind knowing Concentric has SOC 2 Type 2 company-wide certification

Our solution provides agentless integration with numerous cloud products and services.

It's also so easy to deploy — sign up in 10 minutes and see value in days.