

Google Cloud Next '20: OnAir Explore curated content on demand, every Tuesday starting July 14. [Register now](https://cloud.withgoogle.com/next/sf/) (https://cloud.withgoogle.com/next/sf/).

JUMP TO (#) 

Cloud Data Loss Prevention

Fully managed service designed to help you discover, classify, and protect your most sensitive data.

Try Cloud DLP free (<https://console.cloud.google.com/freetrial>)

- ✓ Take charge of your data on or off cloud
- ✓ Inspect your data to gain valuable insights and make informed decisions to secure your data
- ✓ Effectively reduce data risk with de-identification methods like masking and tokenization
- ✓ Seamlessly inspect and transform structured and unstructured data

BLOG [\(/blog/products/identity-security/taking-charge-of-your-data-using-cloud-dlp-to-de-identify-and-obfuscate-sensitive-information\)](https://cloud.google.com/blog/products/identity-security/taking-charge-of-your-data-using-cloud-dlp-to-de-identify-and-obfuscate-sensitive-information)
Use Cloud DLP to mask sensitive information

Gain visibility into the data you store and process

Create dashboards and audit reports. Automate tagging, remediation, or policy based on findings. Connect DLP results into Security Command Center, Data Catalog, or export to your own SIEM or governance tool.

Configure data inspection and monitoring with ease

Schedule inspection jobs directly in the console UI or stream data into our API to inspect or protect workloads on Google Cloud, on-premises, mobile applications, or other cloud service providers.

Reduce risk to unlock more data for your business

Protection of sensitive data, like personally identifiable information (PII), is critical to your business. Deploy de-identification in migrations, data workloads, and real-time data collection and processing.

Key features

Data discovery and classification

With over [120 built-in infoTypes](/dlp/docs/infotypes-reference) (/dlp/docs/infotypes-reference), Cloud DLP gives you the power to scan, discover, classify, and report on data from virtually anywhere. Cloud DLP has native support for scanning and classifying sensitive data in Cloud Storage, BigQuery, and Datastore

and a streaming content API to enable support for additional data sources, custom workloads, and applications.

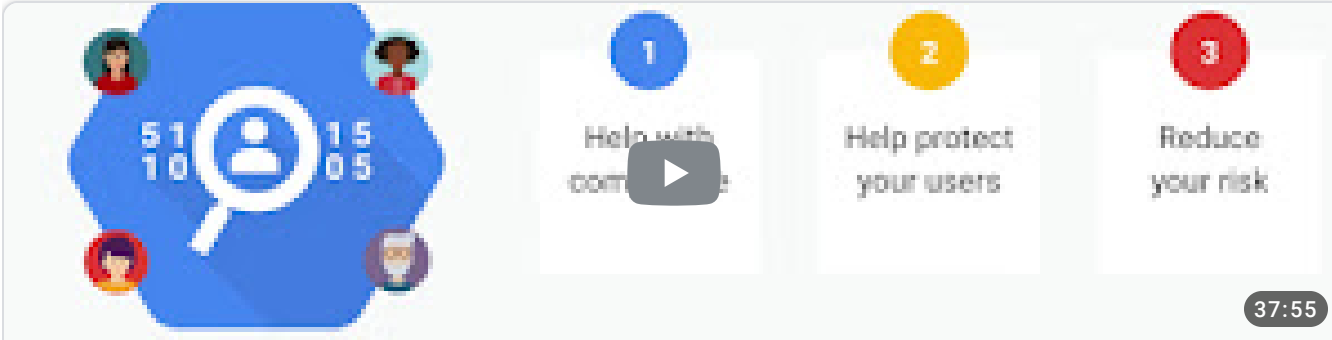
Automatically mask your data to safely unlock more of the cloud

Cloud DLP provides tools to classify, mask, tokenize, and transform sensitive elements to help you better manage the data that you collect, store, or use for business or analytics. With support for structured (/dlp/docs/examples-deid-tables) and unstructured (/dlp/docs/deidentify-sensitive-data) data, Cloud DLP can help you preserve the utility of your data for joining, analytics, and AI while protecting the raw sensitive identifiers.

Measure re-identification risk in structured data

Enhance your understanding of data privacy risk. Quasi-identifiers are partially-identifying elements or combinations of data that may link to a single person or a very small group. Cloud DLP allows you to measure statistical properties such as k-anonymity and l-diversity, expanding your ability to understand and protect data privacy.

[View all features \(#\)](#)



(<https://youtube.com/watch?v=7RqG-pjgZeQ&autoplay=1?t=1>)

VIDEO

[Learn how Cloud DLP helps enterprises discover and manage sensitive data assets.](#)

(<https://youtube.com/watch?v=7RqG-pjgZeQ&autoplay=1?t=1>)

Customers

Sittercity



Maintaining better security and performance

Read the story (</customers/sittercity>)

Story highlights

- Detects and redacts personal data to keep its service secure
- Uses Google Cloud to build a trusted child care marketplace
- Giving parents and sitters a better, more efficient process

Industry

Technology

What's new

[Sign up](https://cloud.google.com/newsletter) (https://cloud.google.com/newsletter) for Google Cloud newsletters to receive product updates, event information, special offers, and more.

BLOG POST

[Scan for sensitive data in just a few clicks](#)

[\(/blog/products/identity-security/take-charge-of-your-data-scan-for-sensitive-data-in-just-a-few-clicks\)](/blog/products/identity-security/take-charge-of-your-data-scan-for-sensitive-data-in-just-a-few-clicks)



[Read the blog.](#)

Documentation

TUTORIAL

De-identification of PII in large-scale data using Cloud DLP

This solution shows how to use Cloud DLP to create an automated transformation pipeline to de-identify sensitive data like personally identifiable information (PII).

[Learn more \(/solutions/de-identification-re-identification-pii-using-cloud-dlp\)](/solutions/de-identification-re-identification-pii-using-cloud-dlp)

TUTORIAL

Automating the classification of data in Cloud Storage

This tutorial shows how to implement an automated data quarantine and classification system using Cloud Storage and other Google Cloud products.

[Learn more \(/solutions/automating-classification-of-data-uploaded-to-cloud-storage\)](/solutions/automating-classification-of-data-uploaded-to-cloud-storage)

PATTERN

Relational database import to BigQuery with Dataflow

This proof-of-concept uses Dataflow and Cloud DLP to securely tokenize and import data from a relational database to BigQuery.

[Learn more \(https://github.com/GoogleCloudPlatform/dlp-rdb-bq-import\)](https://github.com/GoogleCloudPlatform/dlp-rdb-bq-import)

PATTERN

Using a Cloud DLP proxy to query a database

This concept architecture uses a proxy that parses, inspects, and then either logs the findings or de-identifies the results by using Cloud DLP.

[Learn more \(/solutions/example-architecture-dlp-proxy-query-database-sensitive-data\)](/solutions/example-architecture-dlp-proxy-query-database-sensitive-data)

TUTORIAL

Inspecting storage and databases for sensitive data

Instructions for setting up an inspection scan using Cloud DLP in the Cloud Console, and (optionally) for scheduling periodic repeating inspection scans.

[Learn more \(/dlp/docs/inspecting-storage\)](/dlp/docs/inspecting-storage)

QUICKSTART**Scheduling a Cloud DLP inspection scan**

You can schedule inspection scans of storage repositories like Cloud Storage, BigQuery, and Datastore using Cloud DLP's job trigger feature.

[Learn more \(/dlp/docs/quickstart-create-job-trigger\)](/dlp/docs/quickstart-create-job-trigger)

APIS & LIBRARIES**Cloud DLP Client Libraries**

This page shows how to get started with the Cloud Client Libraries for the Cloud Data Loss Prevention API.

[Learn more \(/dlp/docs/libraries\)](/dlp/docs/libraries)

Not seeing what you're looking for?

[View all product documentation \(/dlp/docs\)](/dlp/docs)

Explore more docs

Quickstarts

[Get a quick intro to using this product.](#)

[\(/dlp/docs/quickstarts\)](/dlp/docs/quickstarts)

How-to guides

[Learn to complete specific tasks with this product.](#)

(/dlp/docs/how-to)

Tutorials

[Browse walkthroughs of common uses and scenarios for this product.](#)

(/dlp/docs/solutions)

APIs & references

[View APIs, references, and other resources for this product.](#)

(/dlp/docs/apis)

(/dlp/docs/release-notes)

RELEASE NOTES

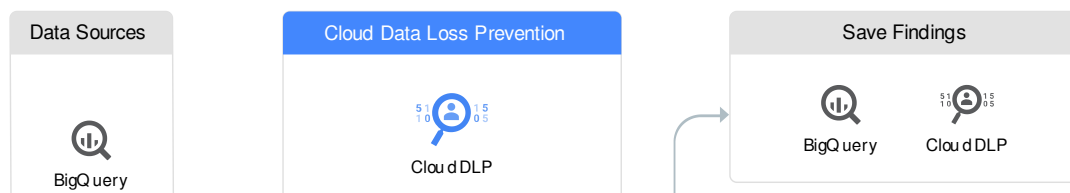
Read about the latest releases for Cloud DLP

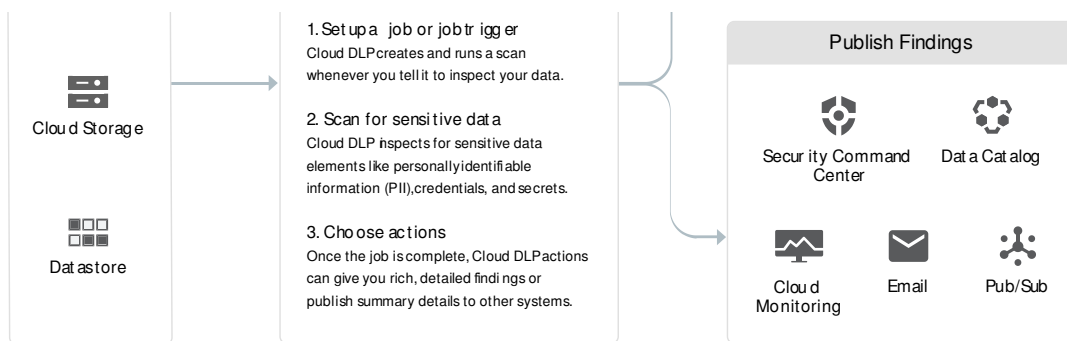
Use cases

USE CASE

Classify data across your enterprise

Cloud DLP can help classify your data on or off cloud giving you the insights you need to ensure proper governance, control, and compliance. Save detailed findings to BigQuery for analysis or publish summary findings to other services like Data Catalog, Security Command Center, Cloud Monitoring, and Pub/Sub. Audit and monitor your data in Cloud Console or build custom reports and dashboards using Google Data Studio or your tool of choice.



**WHITEPAPER****Scan for sensitive data in just a few clicks**

A deeper look at the Google Cloud Console user interface for Cloud DLP to show how you can start to inspect your enterprise data with just a few clicks.

Learn more (</blog/products/identity-security/take-charge-of-your-data-scan-for-sensitive-data-in-just-a-few-clicks>)

TUTORIAL**Automating the classification of data in Cloud Storage**

This tutorial shows how to implement an automated data quarantine and classification system using Cloud Storage and other Google Cloud products.

Learn more (</solutions/automating-classification-of-data-uploaded-to-cloud-storage>)

QUICKSTART**Quickstart: Scheduling a Cloud DLP inspection scan**

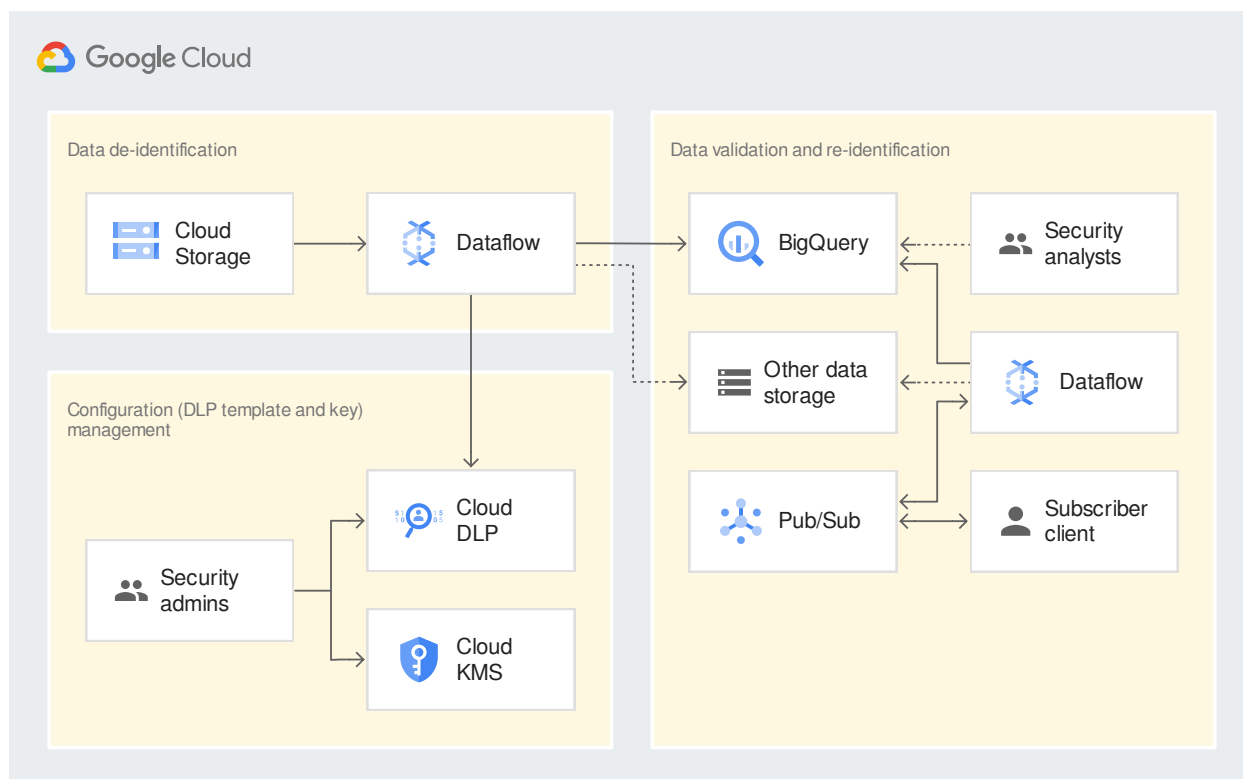
Get started with Cloud DLP to inspect and monitor your data using jobs and job triggers.

[Learn more \(/dlp/docs/quickstart-create-job-trigger\)](/dlp/docs/quickstart-create-job-trigger)

USE CASE

Protect sensitive data as you migrate to the cloud

Unblock more workloads as you migrate to the cloud. Cloud DLP enables you to inspect and classify your sensitive data in structured and unstructured workloads. De-identification techniques like tokenization (pseudonymization) let you preserve the utility of your data for joining or analytics while reducing the risk of handling the data by obfuscating the raw sensitive identifiers.



TUTORIAL

De-identification of PII in large-scale datasets

Reference on how to use Cloud DLP to create an automated data transformation pipeline to de-identify sensitive data like personally identifiable information (PII).

[Learn more \(/solutions/de-identification-re-identification-pii-using-cloud-dlp\)](/solutions/de-identification-re-identification-pii-using-cloud-dlp)

PATTERN

Relational database import to BigQuery with Dataflow

This concept architecture uses Dataflow and Cloud DLP to securely tokenize and import data from a relational database to BigQuery.

[Learn more \(https://github.com/GoogleCloudPlatform/dlp-rdb-bq-import\)](https://github.com/GoogleCloudPlatform/dlp-rdb-bq-import)

[View all technical guides \(/dlp/docs/how-to\)](/dlp/docs/how-to)

All features

Flexible classification

120+ pre-defined detectors

(</dlp/docs/infotypes-reference>) with a focus on quality, speed, and scale. Detectors are improving and expanding all the time.

Simple and powerful redaction

De-identify your data: redact, mask, tokenize, and transform text and images to help ensure data privacy.

Serverless

Cloud DLP is ready to go, no need to manage hardware, VMs, or scale. Just send a little or a lot of data and Cloud DLP scales for you.

Detailed findings

Classification results can be sent directly into BigQuery for detailed analysis or export into other systems. Custom reports can easily be generated in Data Studio.

Secure data handling

Cloud DLP handles your [data securely](#) (</dlp/docs/support/data-security>) and undergoes several independent third-party audits to test for data safety, privacy, and security.

Pay-as-you-go pricing

Cloud DLP is charged based on the amount of data processed, not based on a subscription service or device. This customer-friendly pricing allows you to pay as you go and not in advance of demand.

Easy workload integration

Efficiently deploy Cloud DLP with reusable templates, monitor your data with periodic scans, and integrate into serverless architecture with Pub/Sub notifications.

Custom rules

Add your own custom types, adjust detection thresholds, and create detection rules to fit your needs and reduce noise.

Pricing

Pricing for Cloud DLP is based on total bytes processed with rate schedules based on total volume. You can try DLP for free using the monthly free tier.

[View pricing details \(/dlp/pricing\)](/dlp/pricing)

Take the next step

Start building on Google Cloud with \$300 in free credits and 20+ always free products.

[Try Cloud DLP free \(https://console.cloud.google.com/freetrial\)](https://console.cloud.google.com/freetrial)

Need help getting started?

[Contact sales \(https://cloud.google.com/contact/\)](https://cloud.google.com/contact/)

Work with a trusted partner

[Find a partner \(https://cloud.withgoogle.com/partners/\)](https://cloud.withgoogle.com/partners/)

Continue browsing

See all products (<https://cloud.google.com/products/>)