Welcome to the Content-Related Vulnerabilities: Techniques and Best Practices module.

Module overview

Threat: Ransomware

Ransomware mitigations

Threats: Data misuse, privacy violations, sensitive content

Content-related mitigation

In this module we will cover two main themes: content related threats and some mitigations.

We will start with a review of the ransomware threat, and some of the mitigations you can utilize to help protect your systems from ransomware.

Then we will move to a discussion of threats related to data misuse and privacy violations related to sensitive, restricted, or unacceptable content.

We will also discuss a few mitigation strategies that can be utilized to protect applications and systems from data misuse and privacy violations, then we will end this module with a hands-on lab where you will use the Data Loss Prevention API to redact sensitive data from files.

Content-Related Vulnerabilities

Threat: Ransomware

Ransomware mitigations

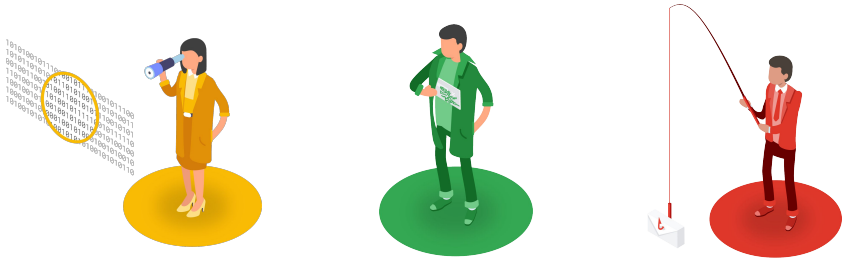
Threats: Data misuse, privacy violations, sensitive content

Content-related mitigation

Let’s begin by examining and defining ransomware threats.

What is ransomware?

- A prominent threat infecting enterprise networks is ransomware.
- Hackers threaten to publish the victim's data or perpetually block access to data unless a ransom is paid.
- Commonly uses cryptoviral extortion to make data inaccessible.

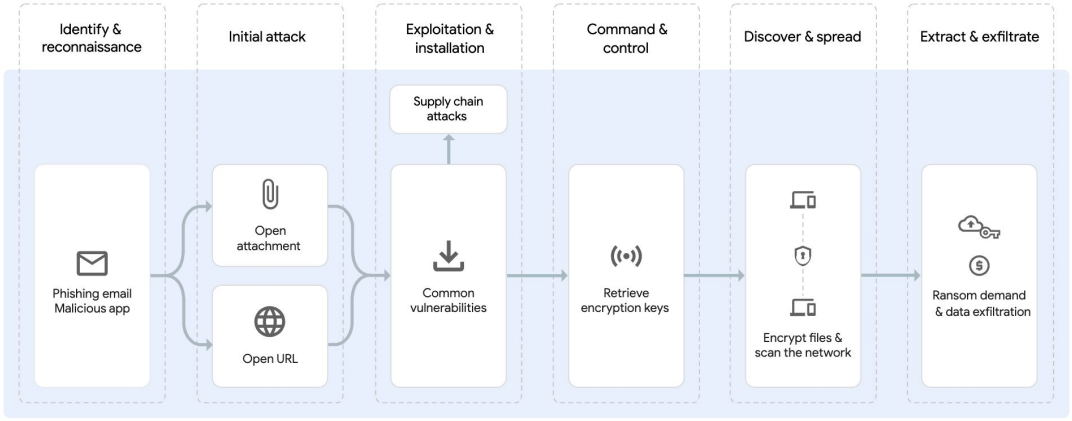


Ransomware is a very prominent content-related threat targeting enterprise networks today.

It's a type of malicious software exploit that threatens to publish the victim's data or perpetually block access to their data unless a ransom is paid. Recent Google research shows cyber thieves have made at least 25 million dollars from ransomware in the last two years and this figure is expected to grow.

Ransomware commonly uses a technique called "cryptoviral extortion" which encrypts the victim's data, making the data inaccessible without the encryption key. The perpetrator will then demand a ransom payment before they will agree to decrypt the files. Digital currencies, such as a cryptocurrency, are used for the ransoms, making tracing and prosecuting the perpetrators very difficult.

How ransomware works



This diagram summarizes the typical ransomware attack sequence.

Ransomware attacks can start as mass campaigns looking for potential vulnerabilities or as directed campaigns. A directed campaign starts with identification and reconnaissance, where an attacker determines which organizations are vulnerable and what attack vector to use.

There are many ransomware attack vectors. The most common are phishing emails with malicious URLs or exploiting an exposed software vulnerability. This software vulnerability can be in the software that your organization uses, or a vulnerability that exists in your software supply chain. Ransomware attackers target organizations, their supply chain, and their customers.

When the initial attack is successful, the ransomware installs itself and contacts the command and control server to retrieve the encryption keys. As ransomware spreads throughout the network, it can infect resources, encrypt data using the keys that it retrieved, and exfiltrate data. Attackers demand a ransom, typically in cryptocoins, from the organization so that they can get the decryption key.

Content-Related Vulnerabilities

Threat: Ransomware

Ransomware mitigations

Threats: Data misuse, privacy violations, sensitive content

Content-related mitigation

Next, let's have a look at some ways you can mitigate the threat of ransomware.

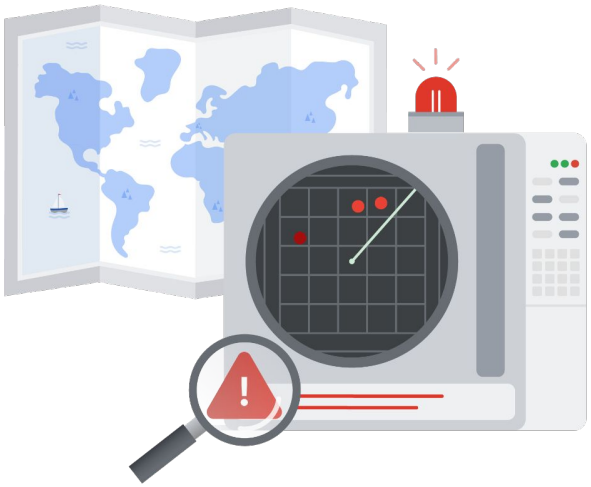
Ransomware mitigations

- Google Cloud provides multiple layers of protection.
- Most protections are automated and available by default.

Google Cloud provides multiple layers of protection against ransomware. Many of these layers of protection are fully automated and available by default, with nothing for you to configure or enable.

Automated mitigations

- Google has global visibility into malicious sites and content.
- This visibility makes the detection of incoming attacks very effective.



For example, Google has global visibility into malicious sites and content. Every minute of the day, Google finds and labels another malware site, and warns incoming users of suspected malware. This makes detecting malware attacks very effective, and there is nothing for you to monitor or configure.

Google also provides many end-user protections to help prevent ransomware from spreading to your resources.

End-user protection

Gmail automatically prevents many malicious attacks from reaching inboxes.

Google Safe Browsing identifies dangerous links.

Google Drive scans files for malware.

If you're a Gmail user, our security and filtering layers will prevent thousands of malicious attachments from ever reaching your organization’s inboxes. If something does reach your Inbox, Google Safe Browsing and our Chrome browser protects users by identifying potentially dangerous links in email and showing warnings if users do click on them.

In Google Drive all files will undergo a malware scan prior to any file download or file sharing attempt.

Data-related mitigations

There are a few things you can do to help reduce vulnerabilities and their ramifications:

- Make regular backups
- Use IAM best practices
- Use the Cloud Data Loss Prevention API

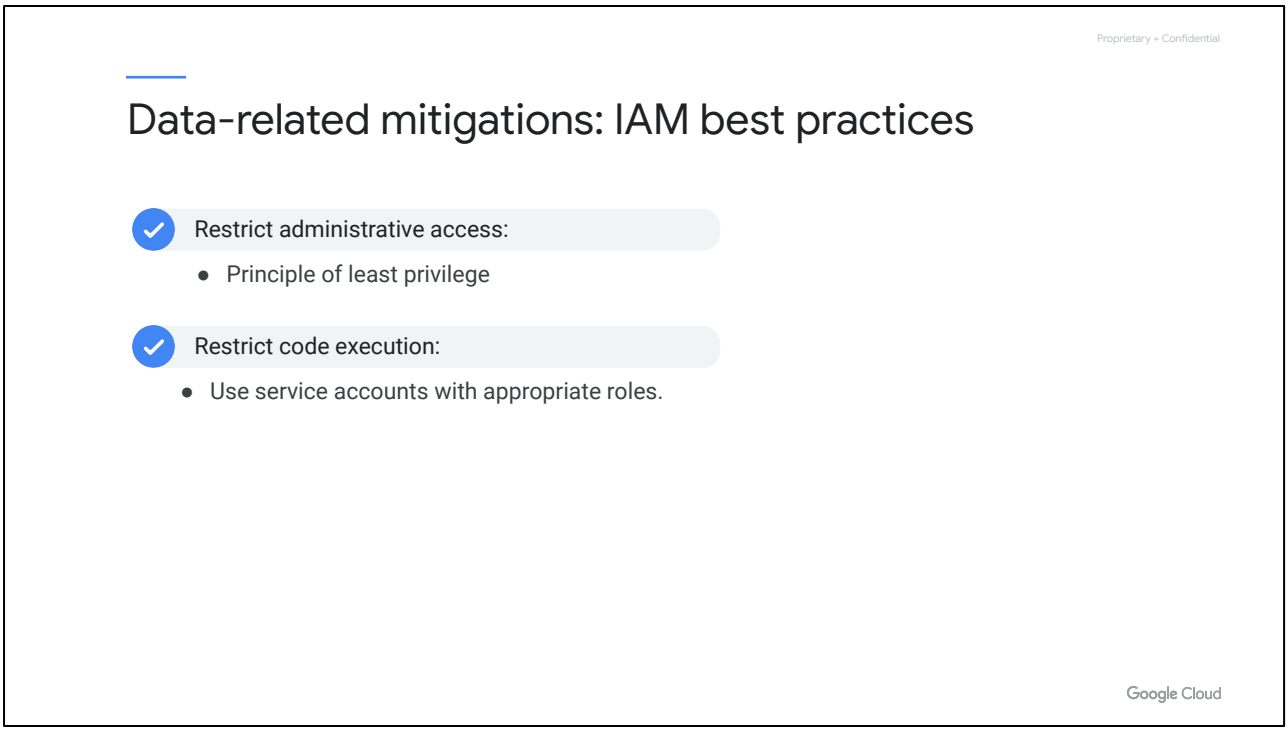
There are also a few things you can do to help mitigate against ransomware and reduce the ramifications of an attack. These steps include making regular backups, using IAM best practices and leveraging the Cloud Data Loss Prevention API.

Data-related mitigations: Backups

- Ransomware often targets backups to prevent data recovery.
- Having durable, secure backups can mitigate effects of ransomware.

How can you use regular backups to lower risk to your data? The bad news is ransomware often targets backups and destroys them as well to prevent data recovery. Therefore, you need to keep your backups safe by conducting regular data backups of your system and then storing the backups securely, in multiple, isolated repositories.

Having durable, secure backups not attached to or accessible by your main systems, which will then not be affected should a ransomware attack occur, will allow you to have a mechanism to recover the data if it is destroyed or held hostage. Think of it as insurance.



Restricting administrative and system access is always a best practice, and is especially helpful for lowering the risk of ransomware attacks. Some strains of ransomware are designed to use a system administrator account to perform their operations. With this type of ransomware, decreasing the number and scope of user accounts and closing all default system administrator accounts can create an extra roadblock.

It is very common for ransomware to be designed to execute from temporary and data folders. If it cannot access these folders due to access control on service accounts, this could constitute a successful roadblock to data encryption.

Data-related mitigations: The Cloud Data Loss Prevention API

- Ensure that sensitive data is not accidentally exposed.
- Leverage the DLP API:
  - Scan all documents for sensitive data before publication.

In the past, sensitive data has been accidentally exposed to the public by organizations via screenshots or other published documents. This data is often used by attackers to help gain the initial access to your systems. Preventing this exposure can help provide a roadblock to a ransomware attack before it ever happens.

The Cloud Data Loss Prevention API (DLP API) can be used to scan all documents for sensitive data before publication, and can even automatically redact any sensitive data found.

Content-Related Vulnerabilities

Threat: Ransomware

Ransomware mitigations

Threats: Data misuse, privacy violations, sensitive content

Content-related mitigation

Let's now consider threats involving the threat of data misuse, privacy violations, and the exposure of sensitive content. These have serious business implications, not least of which is the high monetary cost associated with data recovery and possible litigation, criminal prosecution and fines when user privacy rights have been breached. Reducing the risk of this type of threat is therefore highly important, but difficult to manage and often resource-intensive for many organizations.

Data misuse

Data misuse is the inappropriate use of data:

- Can be a legal/regulatory violation.
- Can also be use of the data in a way that was not intended when collected.

Data misuse is the inappropriate use of any type of data (especially user data). The consequences can be as serious as to cause legal or regulatory violations, or it can result in using the data in a way that was not intended when originally collected.

Types of data misuse

Exposing sensitive content.

Allowing access to restricted content.

Inadvertently including unacceptable content.

Data misuse can happen in many ways. One example is exposing sensitive content when an application accidentally displays an entire credit card number instead of just the last four digits. Another example is when screenshots that contain sensitive data are accidentally created, and then made public, without redaction.

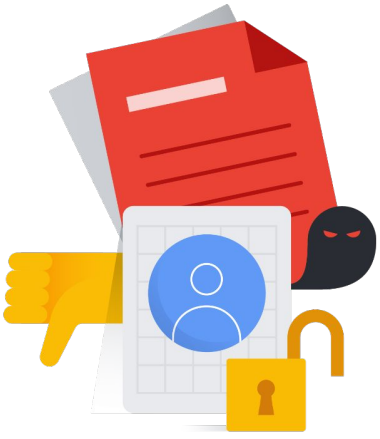
Allowing access to restricted content is another type of data misuse. This occurs when a user is able to access sensitive or restricted data, due to faulty permissions or inadequate server security.

Inadvertently making unacceptable content public is something that may happen when users are allowed to provide public-facing content, such as reviews, images, or videos, without any additional oversight.

Privacy violations

Accidentally exposing sensitive data can have additional ramifications:

- Credibility loss
- Identity theft
- Legal/regulatory risk



Accidentally exposing sensitive data, even when the data loss appears to be restricted to just a small violation, can still have huge additional ramifications.

Because identity thieves are often able to make use of even very innocuous-looking fragments of personal data, the end result may still be a loss of credibility for the organization, identity theft for its users and customers, and legal or regulatory action and fines.

Content-Related Vulnerabilities

Threat: Ransomware

Ransomware mitigations

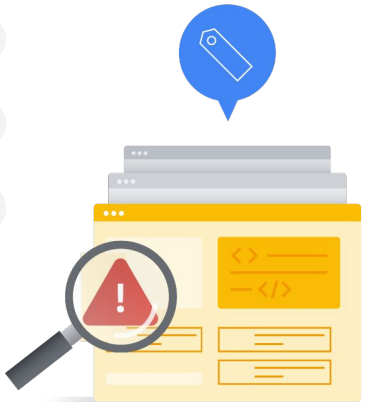
Threats: Data misuse, privacy violations, sensitive content

Content-related mitigation

Now let's talk about some content related threat mitigation strategies.

Mitigation strategies

- Classifying content
- Scanning and redacting content
- Detecting unacceptable content



Mitigating data misuse, privacy violations, and handling sensitive, restricted, or unacceptable content is accomplished by following a three step process. First, classify the content to ensure your security controls align with the value of the data.

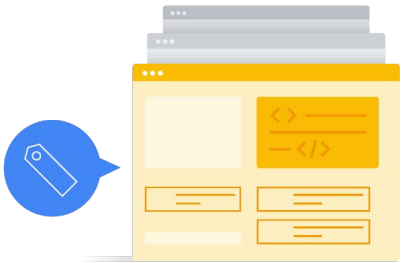
Second, scan content and redact sensitive data.

And third, detect unacceptable content before the item is published.

Mitigation: Classifying content

Classifying content using the Cloud Natural Language API:

- Classifies content into categories along with a confidence score.

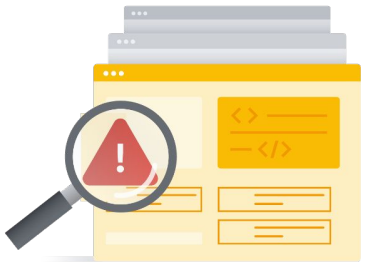


It is important to classify data to ensure your security controls align with required protection protocols for different types of data. Some data is easy to detect, classify and isolate, such as credit card numbers.

Other times it may be more difficult to identify different classifications of data within a large sea of content. The Cloud Natural Language API could be used to help quickly identify different categories of content.

Mitigation: Detecting unacceptable content

- Moderate content and detect inappropriate content.
- Use APIs to automate the moderation process.
  - Vision API
  - Video Intelligence API
  - Cloud Data Loss Prevention API



To prevent the possibility of inadvertently incorporating inappropriate content into your system, you need to monitor and scan files and data that are coming into your applications. There are several APIs that can help automate this process.

The Vision API can easily detect different types of inappropriate content in images, with an ability to flag both “adult” as well as violent content.

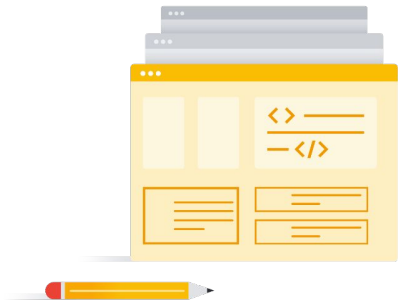
The Video Intelligence API can provide similar monitoring and scanning for videos.

The Cloud Data Loss Prevention API can also be used to detect sensitive data content before it is accidentally exposed to the public.

Mitigation: Scanning and redacting content

Leverage the Cloud Data Loss Prevention API:

- Scan all documents for sensitive data before publication.
- Redact any sensitive data.

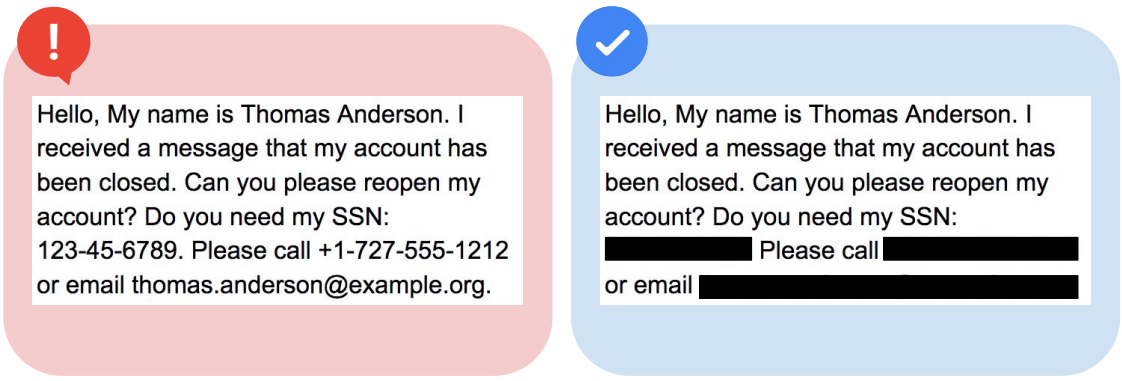


Sensitive data can accidentally be exposed when organizations accidentally publish documents, screenshots or other images that inadvertently were created to contain or show sensitive data.

In addition, sometimes a user may provide unsolicited private/sensitive data for storage within a system that was not designed to protect that data.

The DLP API is a machine learning model that can be used to scan various document formats and images for various types of sensitive data and then redact it, even from images.

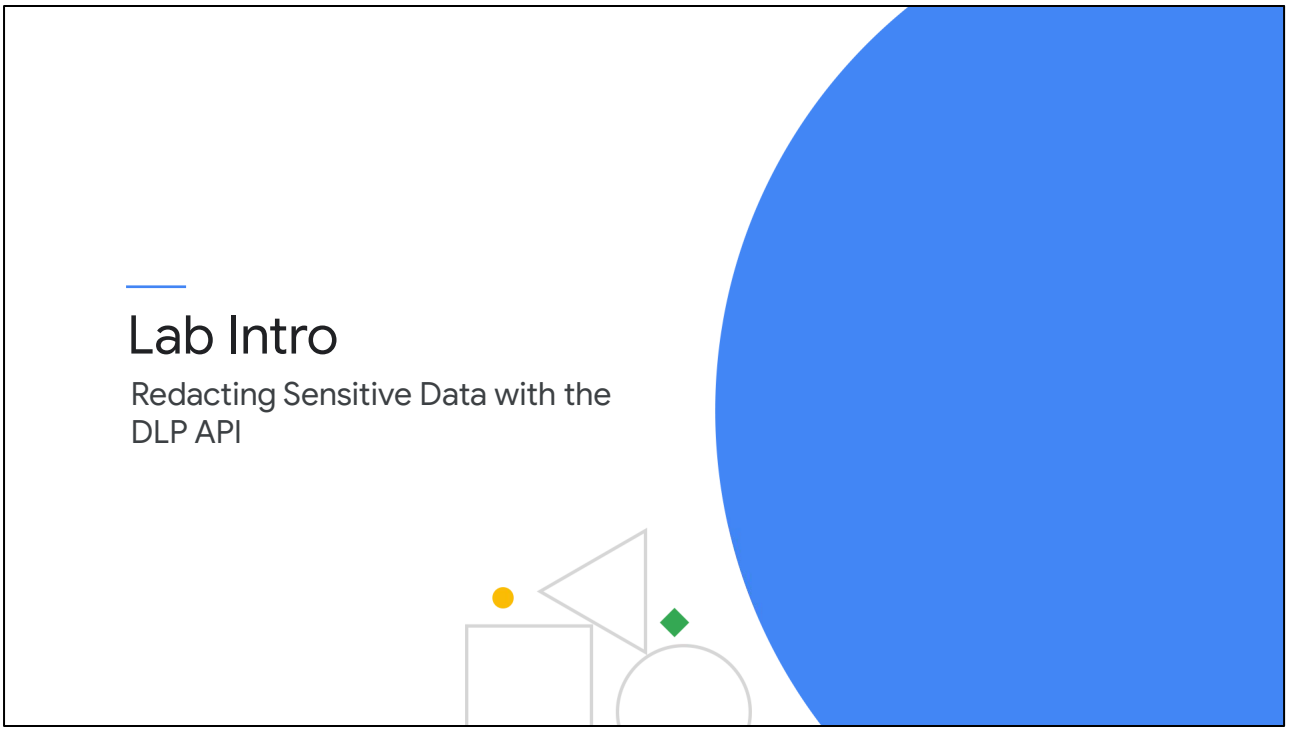
Mitigation: Scanning and redacting content



Look at the screenshot on the left, taken from an application that allows the user to provide unrestricted feedback.

The system was not designed to store this feedback as if it were sensitive data. Therefore, all of the data is stored unencrypted and without other effective security controls.

The screenshot on the right shows this data after leveraging the power of the DLP API. You can see that all of the sensitive data has been detected and then redacted from the image.



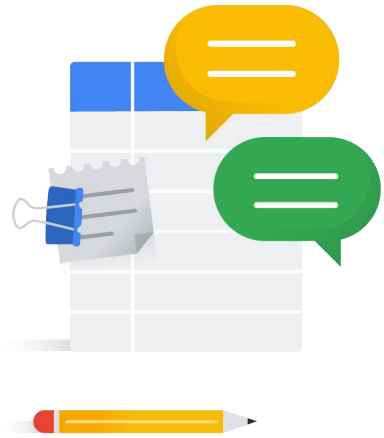
In this lab exercise, you will detect and redact some sensitive data with the DLP API.

You will learn how to perform the following tasks:

- Enable the DLP API
- Install the Node JS DLP API and a sample script
- Inspect string data for sensitive data
- Redact sensitive data from string data and images

Module review

- Ransomware is a type of malicious software exploit that threatens to publish the victim's data or perpetually block access to it.
- Google Cloud provides multiple layers of protection against ransomware by default.
- You should also make regular backups, use IAM best practices and leverage the DLP API.
- Data misuse is the inappropriate use of any type of data (especially user data).



In this module, we covered problems associated with ransomware:

- Ransomware is a type of malicious software exploit that threatens to publish the victim's data or perpetually block access to their data unless a ransom is paid. Digital currencies, such as a cryptocurrency, are used for the ransoms, making tracing and prosecuting the perpetrators very difficult.
- Google Cloud provides multiple layers of protection against ransomware by default, with nothing for you to configure or enable. If you're a Gmail user, our security and filtering layers will prevent thousands of malicious attachments from ever reaching your organization’s inboxes.
- In Google Drive all files will undergo a malware scan prior to any file download or file sharing attempt.
- There are also a few things you can do to help mitigate against ransomware including making regular backups, using IAM best practices and leveraging the Cloud Data Loss Prevention API.
- Data misuse is the inappropriate use of any type of data (especially user data) and the consequences to business can be severe.

Module review

- Google offers several APIs that make mitigation easier and more effective.
  - Cloud Natural Language API
  - Vision API
  - Video Intelligence API
  - DLP API

- Strategies for mitigation include:
  - Classifying content
  - Scanning and redacting content,
  - As well as removing inappropriate content before it is published.
- The Cloud Natural Language API can help quickly identify different categories of textual content so it can be classified.
- Google's Vision API, Video Intelligence API and Cloud Data Loss Prevention API allow you to find sensitive and redact sensitive content, even when it is contained in images.