Metomic

Is Google Drive Secure for Organisations?

Everything you Need to Know to Fully Secure your Google Drive

Despite built-in security features, Google Drive carries cybersecurity risks. After scanning approximately 6.5 million Google Drive files, Metomic's 2023 Report found 40.2% contained sensitive data that could put an organisation at risk of a data breach or cybersecurity attack.

- Organisations such as financial institutions face escalating cyber threats, including ransomware attacks and generative AI sophistication, emphasising the imperative for heightened security measures to safeguard valuable data stored in platforms like Google Drive.

- To address these risks, organisations are advised to adopt best practices such as strengthening access controls, implementing Multi-Factor Authentication (MFA), educating employees on data security and utilising **Data Loss Prevention (DLP) tools**

- See how secure your Google Drive account is in seconds with **Metomic's FREE Google Drive Scanner.** Discover who still has access to your files and who they were created by. Find risky files exposed publicly to anyone on the internet.

Metomic

Is Google Drive Data Secure?

Using Google Drive can bring valuable productivity benefits to companies, but many aren't aware that storing data on the platform carries significant cybersecurity risks.

Our 'Google Drive Risk Report' highlights over 350,000 of the files analysed were left publicly accessible, meaning a lot of businesses aren't doing enough to protect their data from breaches and potentially exposing vast amounts of sensitive company data.

These gaps in Google Drive security are particularly pressing for organisations who must comply with industry regulations. As they are responsible for more sensitive data than most, failing to take the necessary protective measures can lead to serious financial, reputational and legal consequences.

Staying compliant with industry regulations

Those that don't properly protect themselves against breaches like these risk falling foul of **data security regulations** across North America and Europe. Compliance regulations such as the **Payment Card Industry Data Security Standard (PCI DSS)** and the **General Data Protection Regulation (GDPR)** mandate strict measures for securing sensitive data, with non-compliance penalties ranging from strict fines to costly forensic audits.

Beyond cyberattacks, organisations also need to guard against other Google Drive data loss scenarios, like:

- accidental deletion
- data corruption
- hardware malfunctions

Such incidents can lead to damaging operational disruptions and financial losses.

Metomic

What are the Security Risks in Google Drive?

As we have mentioned, Google Drive is not completely secure from cyber threats. Here are some of the security risks that could spell trouble for an organisation:

1

Phishing and social engineering

Google Drive is a secure platform and does contain plenty of security features to help protect your data, such as encryption, two factor authentication (2FA), and phishing and malware detection tools.

However, even with these tools, the weak security link in all of these is the human element. Phishing and malware databases need to be constantly updated, making it likely that an attack may slip through the net. After that, all that's needed for a data breach is for someone to click on a suspect link.

2

Connection to multiple devices

If one of your devices that is connected and signed in to Google Drive is misplaced or stolen, the thief potentially has access to everything in your Google Drive, including any sensitive financial data you're storing in there.
Considering that just over half the UK population has lost at least one phone, it's easy to see how this can be a pretty big problem.

3

Connection to multiple accounts

Now, multiply the problem in the previous point by how many people are using that Google Drive. Any Google Drive used for work will have multiple accounts connected to it, which increases the potential attack surface exponentially.

4

Data encryption stays with Google

Google Drive's encryption sits on the server side, and not the client. This poses risks for storing data, as users entrust all security to Google. This reliance on one company heightens vulnerability to breaches.

5

It's not specifically designed for financial data

While Google Drive does offer secure storage options, it isn't specifically designed for financial data storage, leading to concerns about the platform's suitability for the storage of sensitive information.

6

Typical hacking risk

Brute-force hacking attempts to crack passwords occur every 39 seconds, putting your organisation at increased risk of a data breach or leak.

7

Lack of control over third-party API's

Data stored on Google Drive could be compromised if vulnerabilities in third-party APIs are exploited by hackers. Furthermore, users have limited oversight and control over the security practices of third-party developers.

Metomic

8 Steps on How to Secure your Google Drive Data

For institutions to fill the gaps left in Google Drive's basic security features, they should follow the following best practices:

1

Strengthening access controls

Institutions should limit access to their most sensitive documents. Exposed data increases the risk of unauthorised access or public exposure, especially through settings like 'Anyone on the internet with the link can view'.

2

Enabling Multi-Factor Authentication (MFA)

Without MFA, an organisation's defences are inadequate. **MFA adds an extra security layer** by requiring a second form of verification (like a text message), making unauthorised access much harder. It's also important to use MFA that follows a **zero-trust model**.

3

Monitoring account activity

Organisations should use automated tools to monitor employee and contractor activities within your Google Drive. This allows unexpected changes in sharing settings, downloads of sensitive data, or third-party app access to be flagged and rapidly addressed.

4

Backing up data

Regular backups are essential, particularly for emergency situations where data recovery might be challenging. Also, it's important to have a contingency plan in case Google Drive ever has service interruptions.

5

Educating employees

Companies should train their employees to be vigilant about data security. Knowledgeable employees can better manage sensitive data and make smart sharing decisions, acting as a shield against breaches. We call this the **Human Firewall.**

6

Implementing a Data Loss Prevention (DLP) tool

A **modern DLP tool** can automate security tasks and scan Google Drive for sensitive data, showing who has access. This saves time and offers added oversight over how secure the company's data is.

7

Adding extra encryption

For the most sensitive data, financial institutions may need to use zero-knowledge encryption, which Google Drive doesn't provide. Adding this extra layer of encryption helps to ensure that these most important records are as secure as possible.

8

Comprehensive auditing processes

It's important to set up thorough auditing processes to track who accesses and modifies data within Google Drive. Regular audits help identify potential security gaps and ensure that data handling practices meet the stringent standards required in the financial sector.