Metomic

Lock down your data, not your employees

The Risks of Storing Sensitive Data in Google Drive

Metomic Report 2023

Introduction

With teams collaborating on SaaS apps like Google Workspace day in, day out, sensitive data is constantly being shared and stored in files that your security team may not even be aware of.

Whether it's your customer's PHI, company secrets you need to keep safe, or your employee's bank details you want to protect, SaaS apps can contain hordes of sensitive data that a hacker would love to gain access to.

In 2023, the average cost of a data breach was $4.45m - the highest it's ever been.

While the threat of a data breach never really goes away, the damage it can cause to your business is something firmly within your control. For instance, minimising the amount of data a hacker can access could reduce the potentially catastrophic impact on your business.

At Metomic, we're big advocates of keeping productivity high and allowing employees to do their jobs effectively, while alerting them to the risks of sharing sensitive information.

In Q1 2023, we built our free Google Drive Risk Report to help people understand where their data is stored, who has access to it, what files are publicly accessible, and how they can ensure they can protect their most sensitive data.

The collective findings are outlined in this report, showing the risky nature of storing sensitive data in Google Drive.

Rich Vibert, CEO

$4.45m

Average cost of data breach in 2023

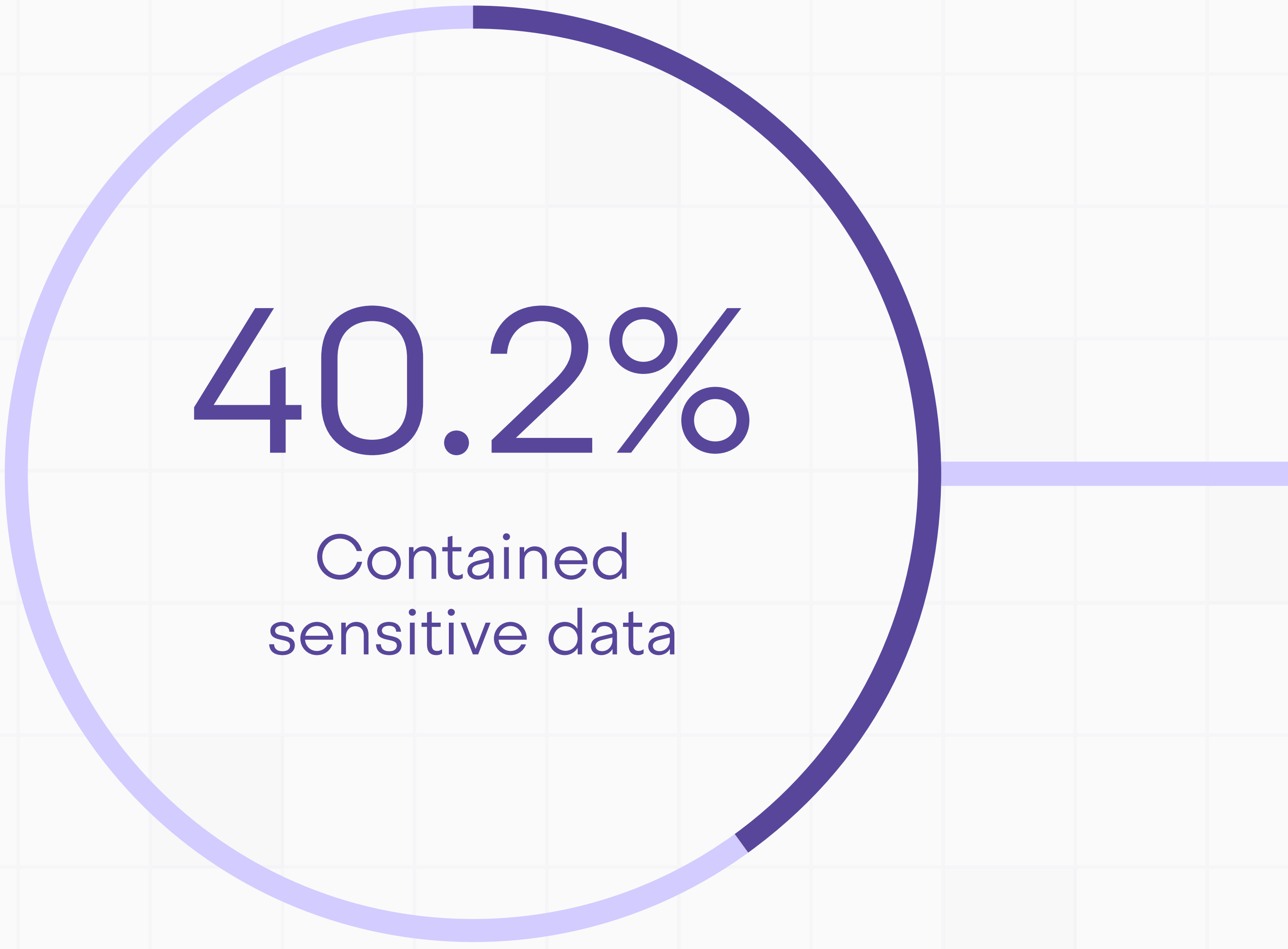
How Risky Is It To Store Sensitive Data in Google Drive?

Sensitive data stored in SaaS apps can make the threat of a data breach seem all the more terrifying.

If that information was leaked, it could lead to massive financial and reputational losses, as well as legal implications.

We found up to 40.2% of scanned files in Google Drive contained sensitive data, suggesting that people are unaware of the huge impact it could have on their business.

Among them, there were confidential employee contracts, spreadsheets full of passwords, and sensitive files that were publicly accessible to anyone on the internet.

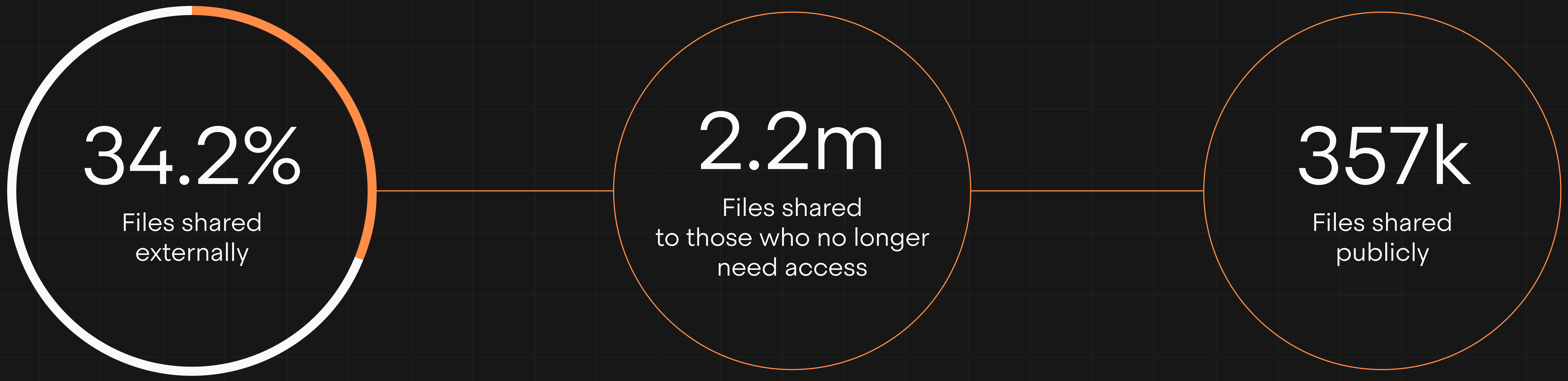


Who's Looking At Your Files?

In an age where data has become a currency all of its own, keeping it away from prying eyes is key.

Despite that, 34.2% of all files scanned were shared externally (with people outside the company domain). That's a total of 2.2m files that may have been shared with those who no longer needed access.

There were also 357k files shared publicly - accessible to anyone on the internet. In making documents easy to share, individuals may not realise just how easy it is for anyone to access their sensitive data.



34.2%
Files shared externally

2.2m
Files shared to those who no longer need access

357k
Files shared publicly

How Risky Are Files in Google Drive?

18k

Files scanned at ‘Critical’ level

Storing files in Google Drive can be hugely risky if they contain sensitive data such as passwords, financial information, or code that needs to be kept private.

Our ranking system found that 18k files scanned were at a ‘Critical’ level, meaning they contained highly sensitive data or permissions weren’t applied securely.

We were glad to see these files were in the minority as they can be particularly dangerous in the wrong hands. Whether hackers want to leak data, sell it on, or hold it to ransom, it could have devastating consequences for a business.

What Can You Do To Secure Your Data?

The consequences of storing sensitive data in SaaS apps like Google Drive are far-reaching, and could be fatal for businesses who may not be able to compete with hefty fines or a significant loss of trade.

There are a few steps you can take to secure your data such as:

With automated rules and policies in place, we help give security teams true peace of mind, knowing their sensitive data is being protected around the clock.

1

Tightening your access controls

Operating a zero-trust strategy or limiting access to documents that contain sensitive data can help to keep your most high-risk files protected.

2

Implement multi-factor authentication

Passwords are not enough to withstand a hacker's determined attempts to get into your workspace. Enabling multi-factor authentication offers an extra layer of security for your business.

3

Build your human firewall

Your people are your best asset and training them to spot unusual behaviour is crucial. To have the biggest impact, this training needs to be ongoing and presented in the context of their role, rather than one-off, annual sessions which are quickly forgotten.

4

Use a DLP tool like Metomic

Using a DLP tool like Metomic can help you protect your sensitive data in SaaS apps while allowing your team to do what they do best. We know how important it is for security teams to feel like they're not restricting their colleagues, while having full visibility over the sensitive data they need to protect.

Metomic

Lock down your data, not your employees

If you’d like to know more, you can reach us on sales@metomic.io
or visit our website: www.metomic.io