Google Cloud Partner

Microsoft Partner

Tricent mitigates the risks caused by external file sharing

- in bulk or automatically!

Each employee shares 348 files externally every year

Sharing files isn't a problem. However, keeping your shared files "open" to outsiders leaves your organization vulnerable to data theft, leaks, privacy violations, etc.

Tricent gives visibility into who can access your organization's files. Our SaaS tool provides efficient ways of mitigating potential vulnerabilities. Requiring little to no maintenance, resources, or training, it can be set up in less than a day.

Risks

- Data leaks
- Data corruption
- Data theft
- Privacy violations
- (Un)governance
- Search engine indexing
- Security vulnerabilities
- Non-compliance

Read the "5 risks of sharing files externally"

Jeremy, IT Director

"The real killer feature is that the product is nearly 'set and forget.' "

Lars, CIO

"Tricent takes part of the workload off the IT department and puts some responsibility on the users who are sharing the files."

Martin, IT Manager

"I'm not as worried about file-sharing anymore. Now the app is proactive for me."

Tricent helps you

Understand your file sharing footprint

See what's shared externally in a simple overview

Mitigate ongoing file sharing risks

Clear obsolete permissions in bulk or through automation

Future-proof your file sharing governance

Ensure files aren't left accessible to outsiders longer than necessary

Use cases

Overview of externally shared data
Remediate existing data leaks
Cut access for compromised partners
Clean up files shared by ex-employees

Show governance efforts to stakeholders
Reduce risk of data theft and corruption
Clean up orphaned files

Improve awareness in end-users
Embed "security by design"
Secure and compliant file sharing

We keep your data safe

EU or US data center options

All data is fully encrypted at rest and in transit

No data content is ever read or transferred