TRICENT
End-user Driven Compliance Tool

Partner Sales Training

Together we can accomplish great things

Microsoft
Partner Network

Google Cloud
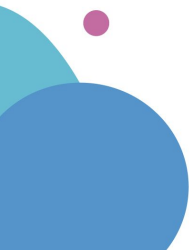Partner
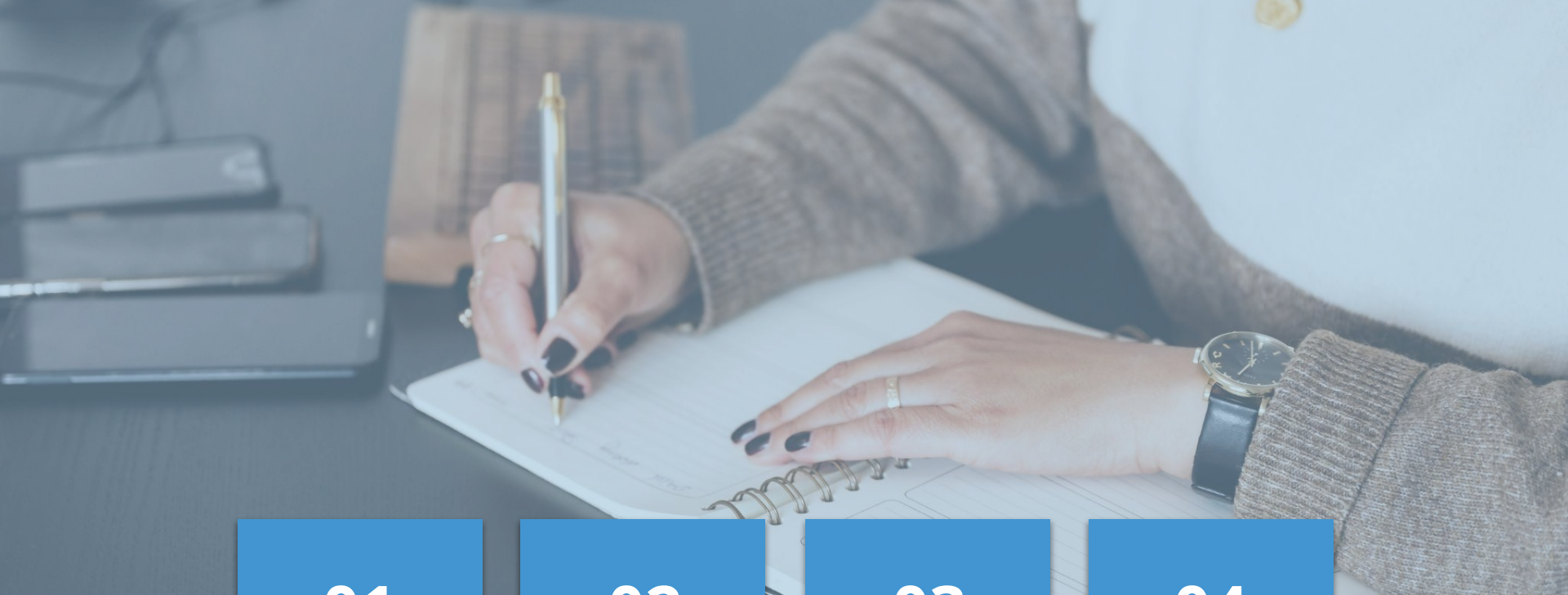
01

What is Tricent?

02

Why organizations need Tricent!

03

How to book the meeting

04

Deal Registration

What is Tricent and what are the advantages

Tricent is an automated compliance tool for both Microsoft M365 & Google Workspace.

Tricent provides:

- Overview
  See the number of company files being shared, and with whom.

- Actionable Insight
  With Tricent, you can easily perform actions directly on the files that need to be unshared.

- Automated Policies
  Set up automated policies to share company data in a controlled and secure way.

- What is Tricent
  (Just to summarize the bullets above)

Discovery Questions

Questions to ask - has the customer ever asked themselves:

- What company data are shared externally?
- How many files/folders are your users sharing?
- Who externally has been given access to company data?
- Why do they have access to company data? Closed projects, not a vendor/customer/partner anymore etc.?
- Do we trust all external domains or users who have access to our company data?

No complete overview of shared files
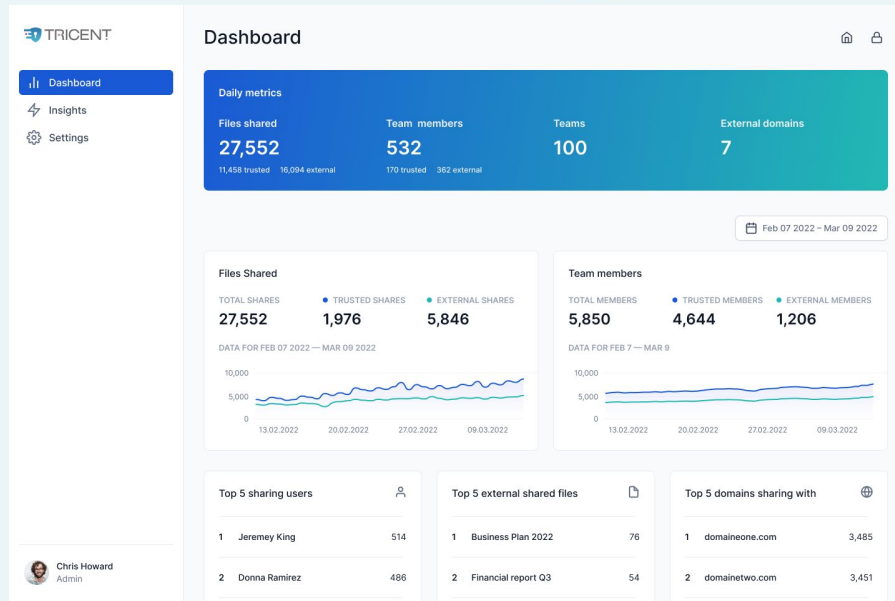
What data are being shared ?

- Business critical data VS Non critical.

Who has access to data ?

- Do we trust external domains/users having access to company data?

Why is the data being shared ?

- Is access to data necessary? eg. projects, partners, vendors, customers etc.

All data - No Actions

Data access control

- Revoke unwanted access to data

External domain control

- Revoke permissions for entire domains or specific user

Legacy sharing cleanup

- Clean up legacy file shares (starting from the first file shared in cloud)

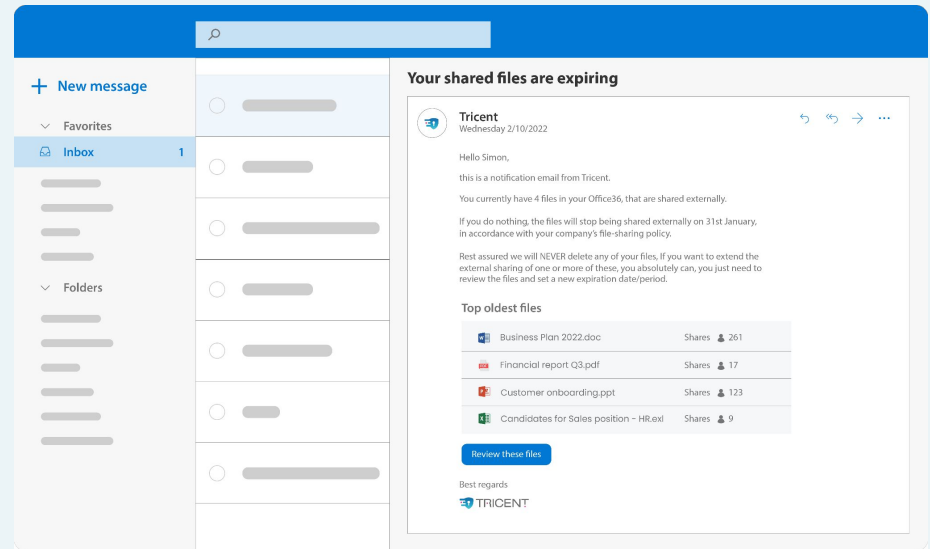# Automated Compliance

User involvement

- Let users decide easily which files should still be shared

Creates awareness

- Make users aware of data they are sharing

Automated policy driven flows

- Automated policy flows will ensure compliance

Objections and how to respond

- *Script it themselves:*
  Tedious and manual task. Demands a lot of resources and are 100% admin driven Will at best give them overview of shared files but no way to involve end users or perform various actions (no dashboard).

- *Just now starting to move to the cloud so not sharing a lot yet:*
  No, but they will. To have control and be able to create awareness for the users is a gift and strengthens their compliance level at an early stage. No mess to clean up (old shares, inactive shares, shares with no owner).

- *We have blocked external sharing:*
  If users need to share files externally they will find a way. Use 3rd party sharing options like Dropbox and Weshare which is outside of MS/Google so no possibility to gain control of these shares. Tricent enables them to keep shares within the MS environment and have complete overview and control.

- *Have E5 and want to see what they can do with it:*
  E5 is great and offers a lot of opportunities that look at content but nothing that looks at permissions. That's why Tricent is a preferred ISV Partner and MS is pushing the solution as a compliment to E3/E5 etc.
  Way easier to implement than DLP and labelling (18-24 months)

- *No resources for new tools:*
  Onboarding in 15 minutes. We spent some weeks crawling data and then we help set everything up within 1 hour. Automation is king!

- *We don't share files:*
  Are you sure? Where do you get the overview?
  What tools do you have in place that can confirm this? Do you trust your end users (Zero Trust)?

- *We already have a solution for this:*
  What does that solution provide? Full overview across services? Actionable insights? Involve the end user?

Support and Guides

Guides & Video for Employees
M365   Google

FAQ for Employees
M365   Google

Guides & Video for Admin
M365   Google

FAQ for Admin
M365   Google

Technical side of Tricent
M365   Google

We'd like you to know…

Trial Terms of Use

Read more >

Subprocessors

Read more >

Service Level Agreement

Read more >

Data Processing Agreement

Read more >

Vulnerability Disclosure

Read more >

Terms of Use

Read more >

tricent.com/legal

Re-selling and Deal registration

- All new deals should go through Partner.

- Registration at:

  - [Microsoft Deal Registration](#)

  - [Google Deal Registration](#)

- All opportunities will be aligned between Tricent & Partner. This will secure full transparency between Tricent & Partner.

- Tricent will help with sales materials and workshops.

- Tricent can be sold as a Stand-alone-product or as a bundle within your current product-portfolio.

Live Demo
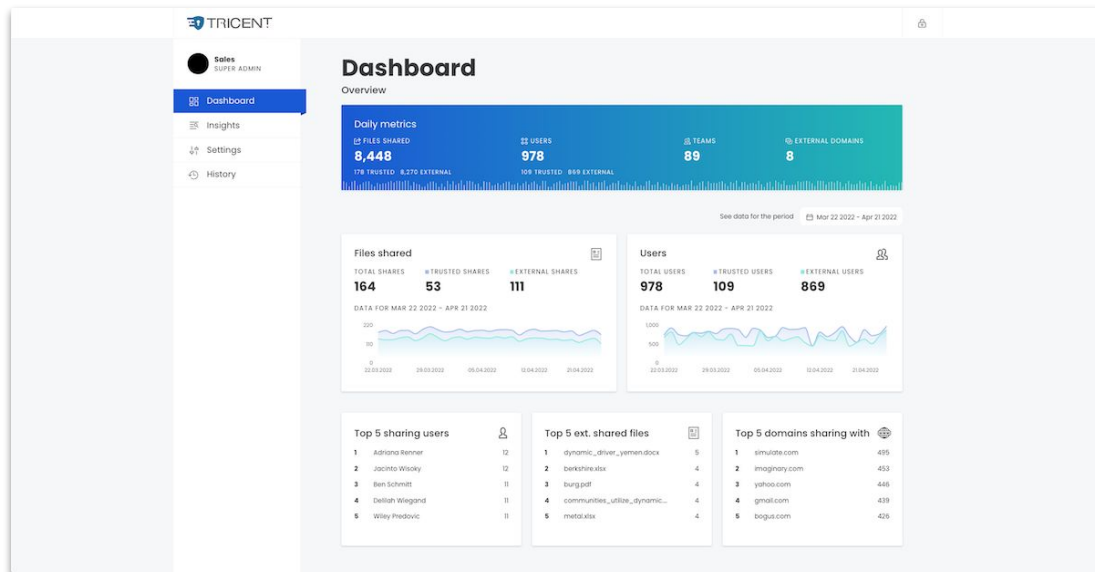
The Ticking Time Bomb of Cybersecurity Breaches

- Every unregulated external collaboration is a potential door for cyber attackers. If you're not using Tricent to control external sharing, you're inviting breaches to your data.

- Tricent's ability to revoke permissions and automate the process ensures your organization is not an easy target.

- Traditional tools that you can find within Microsoft 365 may leave you exposed to threats you don't even know exist.

Who Will Be Held Accountable in Case of a Breach?

- Without Tricent, you could be drowning in a sea of external shares with no clear owner, creating a perfect storm for unidentified security breaches.

- In case of an attack, the fallout can be catastrophic, with hefty fines and a damaged reputation.

The Hidden Risks of Restricting External File Sharing

- While it might seem like a good idea to restrict external file sharing, employees can resort to uncontrolled third-party tools or insecure email attachments.

- This can leave a backdoor for hackers straight into your sensitive data.

- Tricent provides a secure, controlled environment, eliminating this unpleasant possibility.

The Nightmare of Manual Scripting

- Manual scripting is not just complex and resource-intensive, it's also a ticking time bomb. One error, one oversight, and your entire system could be compromised.

- Tricent's automation provides a safety net, reducing the risk of human error.

- By minimizing manual tasks, you're not only saving resources but also preventing scaring off talented recruits due to a heavy workload.

Proposed pitch

IT professionals like yourself come to us as they have no overview and control of what data their users are sharing externally and who have access to this data.

They often believe that this can be solved with one or more of the many features included in their current, and usually quite expensive, GWS license and they get genuinely surprised to find that it is not.

This makes them feel exposed as their current status is based on gut feel i/o actual data. Getting that data with the solutions they currently have available, requires too many resources from their IT department, which causes delay in other projects or they burst their budget using external consultants to solve the challenge - and even then they get a nasty surprise when they find that they only get part of the way.

With Tricent you can remove the guesswork and have a clear overview, actionable insights and automation to keep in control of your shared data.

But maybe you don't see any of this?

Qualifying Questions before setting up the demo with Tricent

Questions to ask to make sure that your customer has priority and budget:

- Discover their primary pains and challenges by using the discovery questions
- What is the **priority** for them to solve this now rather than later? - this is where you as a partner can assist (priority and timing is very important to discover)
- Who else needs to be involved in this? - make sure they can attend the demo meeting
- Do they have the budget? - perhaps they already have a managed service with you that this could be part of (this links to the priority also. If they don't have the budget it is good to know if they are able to find budget anyway - which they can if it is a top priority)

Tricent builds on top of the security and compliance features in Microsoft 365 E5

Tricent for Microsoft 365

→ Focuses on after-the-share risk mitigation - not on stopping the sharing to begin with.

→ Supplies tools for administrators to handle external sharings company-wide.

→ Engages the end-users in cleaning up their externally shared files.

→ Creates data protection awareness by involving end-users.

→ Provides organization-wide insights into external file sharing.

→ Enables automatable cleanup of external file sharing.

Tricent for Microsoft 365 security and compliance value add

Microsoft 365 E5

→ Focus on before-the-share mitigation - not on mitigating risk from already shared data

→ Data Loss Protection for email and files

→ Data classification and basic policies

→ eDiscovery audit

→ Litigation hold

→ Insider Risk Management

→ Data retention rules

Microsoft 365 E5 central security and compliance features