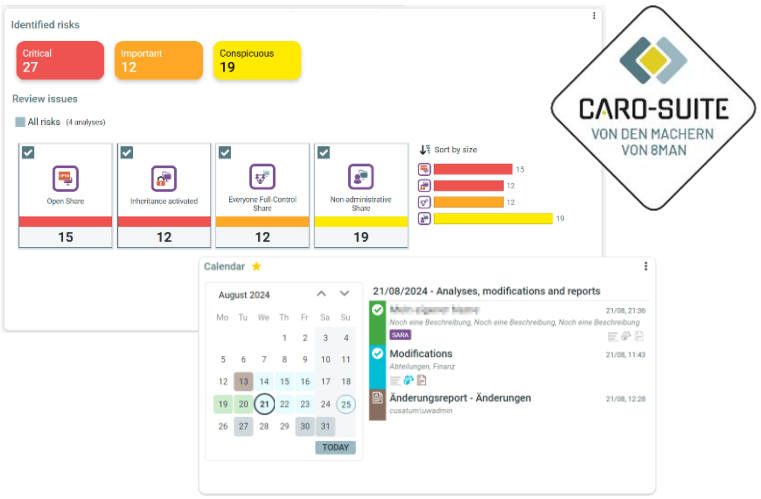
CARO-Suite

CARO is now conquering the cloud!

CARO-Suite 2024.8 Available for the CLOUD

CARO-Suite Version 2024.8

- Cleans up your cloud too
- Combines file server, Active Directory and Entra ID information
- Performs analyses for hybrid scenarios
- Easily displays Entra ID information and role access authorisations easily
- Makes access right management and IDM systems work more efficiently



CARO-SUITE VON DEN MACHERN VON 8MAN

CUSATUM

CUSATUM Service GmbH

Head office
Wiesenweg 16
16548 Glienicke / Nordbahn

E-mail: info@cusatum.de
www.cusatum.de

Support

Phone: +49 30 94 86 3401
Mobile: +49 175 221 11 04

E-mail: support@cusatum.de

August 2025

SECURITY MADE IN GERMANY

Entra ID technology

Microsoft Entra ID connection

To connect CARO to an Entra ID system, we offer you an integrated workflow for app registration of your client secret.

The CARO resource view displays important information, such as members of Entra roles, licences and applications used or guest users.

Analyses for Entra ID

Access checks in the cloud

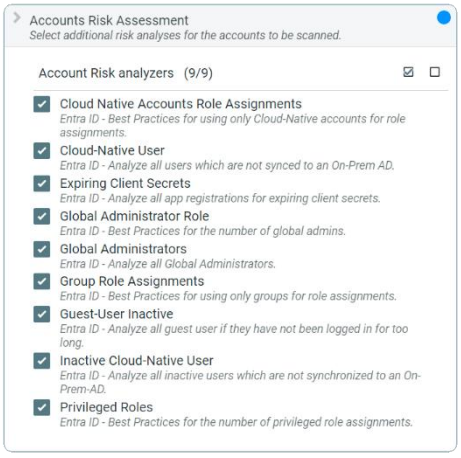
With CARO, you can now check and clean up your access for cloud-based and hybrid resources on Entra ID. CARO integrates best practices for Microsoft Entra roles.

Best practices according to Microsoft*

- Check and clean up your **global administrators** for **permitted numbers** and role assignments.
- Verification that only **cloud-native accounts** are used for role assignments.
- Exclusive use of **groups** in role assignments.
- Check the number of **privileged role assignments** for the permitted number,

Further risk assessments

- Finds all **expiring client keys** in the app registrations that have already expired or will expire in x days.
- Find your **inactive guest users** who have not logged in for a period of time X.
- Analyse all global administrators.
- Find all **cloud-native users** who are not synchronised with an on-prem AD.
- Finding all **inactive cloud-native users** who are not synchronised with an on-prem AD and have not logged in for a period of time X.



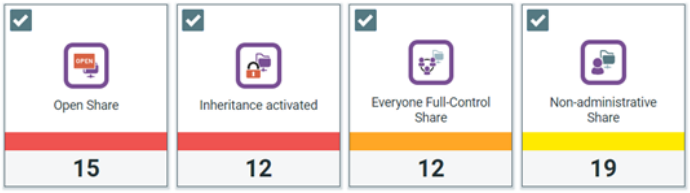
*A detailed description of Microsoft Best Practices can be found here: https://learn.microsoft.com/de-de/entra/identity/role-based-access-control/best-practices

CARO-Suite

Analyses - New share checker SARA

CARO checks risky access rights to file server shares and finds your *open shares*. This means that data can no longer be accessed unnoticed.

By enabling you to check your systems daily, CARO supports you where Access Rights Management and IDM systems reach their limits.

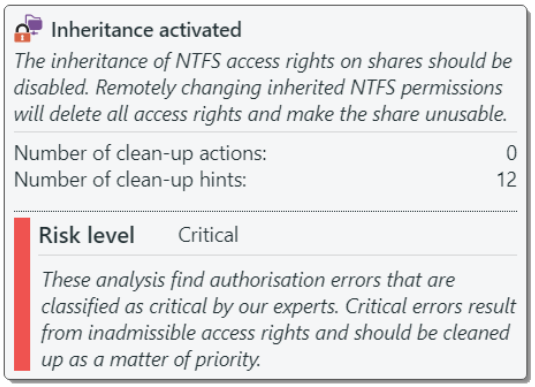


Activated inheritance

- Checks for inherited NTFS access rights in the shares
- The inheritance of NTFS access rights to shares should be deactivated
- Changing inherited NTFS permissions remotely deletes all access rights and renders the share unusable
- Risk classification: *critical*

Open shares

- Identify *open shares*, i.e. all authenticated accounts (Active Directory and local) have at least read access rights to the information in the file system share
- This can lead to an uncontrolled outflow of data
- Risk classification: *critical*



Everyone full access shares

- The Everyone account should have maximum change access rights to the share.
- With full access, there is a risk that users can unknowingly cause damage with extended NTFS permissions.
- Risk classification: *important*

Non-administrative shares

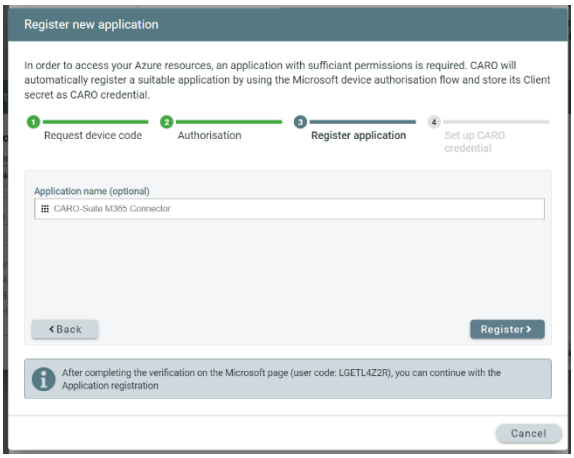
- Check server for the existence of non-administrative shares
- Administrative authorisations (C$, etc.) are ignored
- Approvals can allow uncontrolled access to critical information
- Risk classification: *conspicuous*

Technology

Microsoft Entra ID connection

To connect CARO to an Entra ID system, we offer you an integrated *4-click workflow* for app registration of your client secret.

Where other manufacturers often only offer help via a website, with CARO you only need to enter the tenant name of the Entra ID system and the registration process is then carried out automatically.



Data Owner Report

Simple authorisation overview

In this data owner report, permission errors can be identified at a glance, even by data owners with small technical background knowledge.

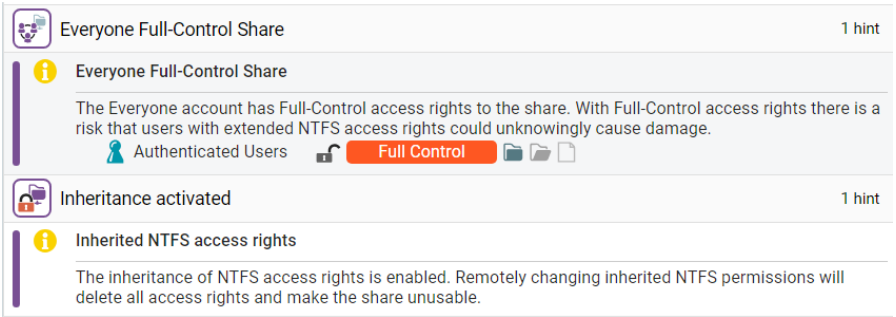
Presented compactly on just a few pages, important information can be directly interpreted by users.

CUSATUM\I__Daten_IT_md	Full Control	Modify	Read & Execute	Restricted List
IT *\\fileserver\Abteilungen\IT*		✔		
30_TestDaten *\\fileserver\Abteilungen\IT\30_TestDaten*		✔		
Berichte *\\fileserver\Abteilungen\IT\30_TestDaten\Berichte*		✔		

Usability

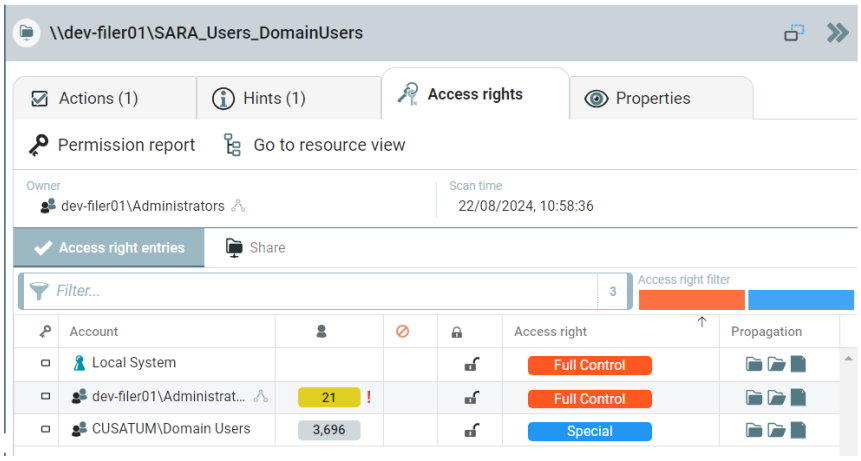
Transparency

Experience more transparency with CARO recommendations for clean-up actions.



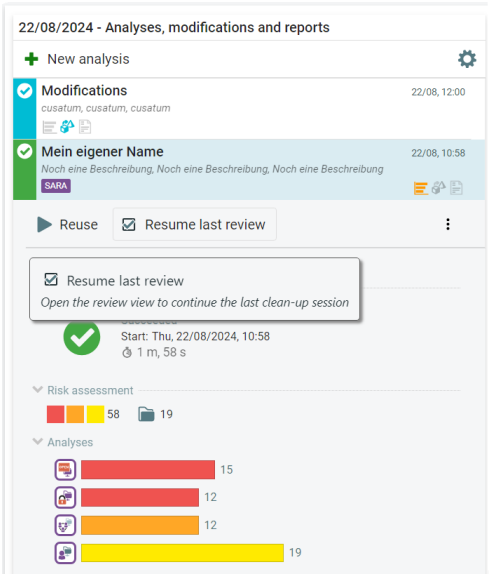
Traceability

Look at the directory access rights for each action or note in the comparison to evaluate the CARO clean-up actions more quickly.



Improved navigation

The CARO-Suite offers simplified navigation in many places, so you can go directly to your last assessment, for example, to continue your clean-up process. Or to the account detail view to check the group memberships of a conspicuous account.



Security, stability and performance

The use of a modern web framework for the user interface of the CARO-Suite takes into account the necessary security requirements of web interfaces. More effective database storage by reducing the amount of data stored has also been implemented in this version of CARO-Suite.

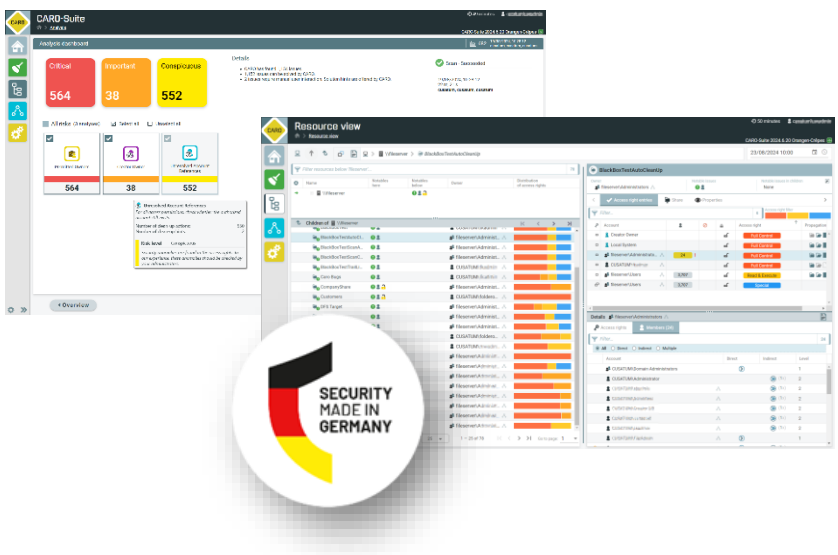
CARO-Suite

CARO-Suite - Access rights securely under control!

Historically grown permission structures are a thing of the past with CARO. Problems with access rights are eliminated and automatically reduced. CARO brings order to your IT structures!

The CARO-Suite in detail

- Risk assessment with expert knowledge
- Detailed analyses for access rights errors
- Comprehensive recommendations for cleaning up
- User-configurable dashboards with clean-up history and task planning
- Global resource view of access rights with group memberships
- Account view with direct and indirect group memberships
- High-performance scans and comprehensive analyses to change your problematic access rights
- Scans and changes can be scheduled for any point in time
- For file system, Active Directory and Microsoft Entra ID
- Integration into other systems via Rest API
- Automation of employee processes with C-MAN add-on module
- Reports in PDF format, easily customizable to your own corporate identity using Word Office report templates
- Audit-proof logging of all changes made
- Multilingual web client with multi user support
- Data storage in MS SQL database
- Simple license model



CARO-Suite

CUSATUM - Together for more safety!

CUSATUM Service GmbH in Berlin/Brandenburg is a software and consulting company with a focus on access rights management and the automation of employee workflow processes. Since 2017, we have been supporting our customers in implementing effective access rights management solutions.

We have accompanied Protected Networks' 8MAN from its inception. With our CARO Suite, the CUSATUM Access Rights Optimizer, we are offering our customers a software product for the first time that enables them to easily and automatically resolve access rights issues.

Mike Wiedemann, CEO
His passion is customer satisfaction. He also goes the "extra mile" for satisfied customers!

Ute Wagner, CDO
A user interface must not only be easy to use, but it must also be a pleasure to use!

Christian Schönfeld, CEO
Converting my experience directly into CARO - that is my claim! There is a solution for everything. Let's do it!

Publisher

CUSATUM Service GmbH

Head office
Wiesenweg 16
16548 Glienicke / Nordbahn

E-mail: info@cusatum.de
www.cusatum.de

Support

Phone: +49 30 94 86 3401
Mobile: +49 175 221 11 04

E-mail: support@cusatum.de

August 2025