CARO-Suite

Access rights securely under control!

CARO finds your access rights problems,
cleans them up automatically and
keeps the permissions to your data clean.

- Risk assessment by experts
- Automated clean-up process
- Customised dashboards
- Hybrid scenarios analyses
- Easy display of role permissions
- Simple to integrate and easy to use

CARO-Risk Assess©

For your overview

Overview through expert risk assessment and comprehensive access rights analyses.

CARO-Automate©

For your relief

Efficiency through detailed recommendations for action and automated cleaning.

CARO-Secure©

For your control

With compliance-conform reports and audit-proof logging.

SECURITY MADE IN GERMANY

CARO-Suite

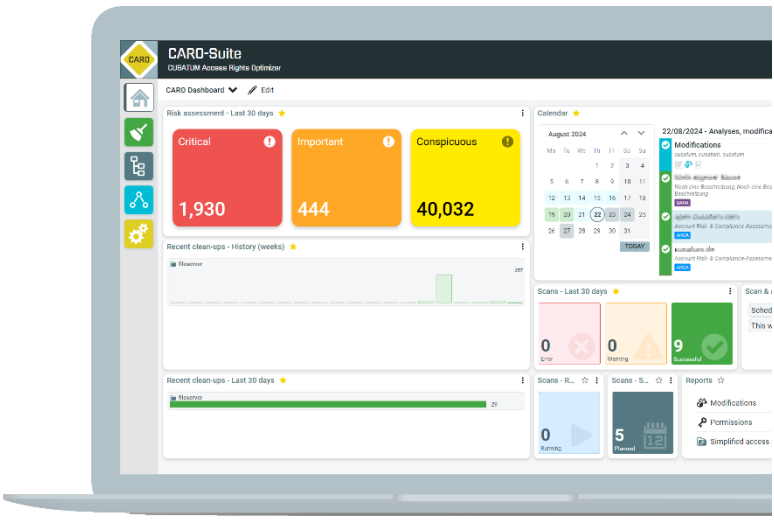
3 modules for your IT security

With the CARO-Suite, you can analyse and automatically eliminate permission errors and access rights risks. Save time and money with clean access rights structures and optimised permissions.

The CARO-SUITE offers for your IT security:

CARO-RISK ASSESS©

- Risk assessment by experts
- Permission analyses
- Accounts and resources view



CARO-AUTOMATE©

- Automated clean-up
- Recommendations for actions
- Task scheduling faster

CARO-SECURE©

- Audit-proof reports
- Simple reports for data owners
- Compliance-conform
- Configurable dashboards

SECURITY MADE IN GERMANY

CARO-Suite

Risk assessment by experts

With the **risk dashboard**, you can see at a glance where your biggest risks are and how you can automatically rectify the problems with just a few clicks.

Risk assessment	Clean-up modules	Explanation	Analyses
Critical	VASS, ARCA, RAPA, DUKE, DARS, BAKS, SARA	These analyses find access rights errors that are classified as critical by our experts. Critical errors are caused by unauthorised access rights and should be rectified as a matter of priority.	Permitted owner analysis Direct user permissions Redundant access rights Interrupted inheritance Inactive computers Password never expires Activated inheritance in shares Open shares Privileged roles Global administrator role Number of global admins Expiring client keys
Important	HERITA, MARS, VASS, ARCA, LARS, SARA	These analyses find other problems in your system that are classified as important. Such relevant problems should be rectified promptly.	Creator-owner Minimum access rights Moved directories Unwanted accounts Inactive users List group analysis Any-full-access permissions Group role assignments Cloud-native accounts Role assignments Inactive guest users
Conspicuous	TEUS, ARCA, SARA	Security anomalies are found in the access rights. In our experience, these anomalies should be checked by your administrators.	Unkown account references Outdated password Deactivated user User never logged in Empty groups Groups without description Non-administrative approvals Inactive cloud-native users Cloud-native users

CARO-Suite

Analysis and clean-up modules

The CARO-Suite includes 12 clean-up and analysis modules as standard.

BAKS

Owner analysis and correction software

Correct owner

- Ensures authorised owners so that administrative accounts retain their permissions, e.g. so that backup tools work
- Analyses security risks by removing unauthorised and uncontrollable access rights

LARS

List groups Analysis and restructuring software

Errors in list groups analyse

- Analysing permissions in folder hierarchies
- Manage list permissions in parent folders

TEUS

Tool for removing unknown SIDs

Remove dead SIDs

- Removes dead SIDs and makes the documentation of your access rights easier to read and understand again
- Reduces the number of queries from your auditors and documents that you have full control
- Provides more security, as less attack surface for SID history injection

DARS

Direct access to analysis and restructuring software

Check direct permissions

- Identifies direct permissions of users
- Corrects these entries efficiently

RAPA

Redundant Account Permission Analysis

Redundant permissions eliminate

- Identifies redundant permissions
- Checking group memberships with simultaneous direct permissions

SARA

Share Access Rights Analysis

Check share permissions

- Analysis of share access rights
- Check for inherited NTFS access rights
- Searches for "open shares" for authenticated accounts
- Searching for any-full-access shares
- Check for the existence of non-administrative permissions

CARO-Suite

Analysis and clean-up modules

As standard, 12 clean-up and analysis modules are supplied with the CARO-Suite.

DUKE

Remove direct access rights for unwanted accounts

- Identifies all access rights of the configured unwanted accounts and removes them
- Reduces security risks by removing unknown and uncontrollable access rights

Remove direct unwanted permisssions

VASS

Inheritance analysis and sanitisation software

- Identifies changed permissions in folder hierarchies
- Alignment of permissions through inheritance or other system-specific tools

Restore broken inheritances, Find moved directories

ARCA

Account risk and compliance assessment

- Analysed account-based on best practice criteria
- For Active Directory and Entra ID
- **AD**: Inactive user or computer accounts, deactivated user accounts, user never logged in, empty groups and groups without description, accounts with passwords that never expire
- **Entra ID**: Global administrators, Privileged role assignments, Groups in role assignments,
- Use of cloud-native accounts,
- Expiring client key,
- Finding inactive guest users and inactive cloud-native users

Risk and compliance dashboard for Active Directory and Entra ID

HERI

Remove creator owner on file system

- Removes the creator owner and prevents the creation of new dead SIDs
- Allows a clean migration, e.g. to the cloud

Remove creator-owner

MARS

Minimum permissions analysis and restructuring software

- Checks all documents and folders for required access rights for accounts, considering both direct and indirect access rights
- Sets missing permissions

Minimum permission check

Display and report permissions

With the EBIS module, CARO displays a global resource view with the *actual permission situation*. You can create permission and use case reports, easily adaptable to your corporate identity using Microsoft Word Office templates.

EBIS

Recording the actual permission situation

- Records the permission situation on file servers
- Analyses for interrupted inheritance hierarchies, shifted directories or null DACL in the ACEs, among other things
- Display of missing owner entries
- Shows changed permissions in detail below, such as added or removed access rights
- Shows group memberships with direct and indirect membership relationships
- Reports for the actual permission situation "Who has access where?"
- Reports on changed permissions below
- Difference reports for a directory structure
- Report "Where does a user have access?"

Recording the actual situation and report permissions

Best Practices

It makes sense to use certain analyses together for cleaning. In our flyer *Best practices and use cases for cleansing*, you can find out more about a recommended sequence and sensible combinations of CARO analyses for efficient cleansing.

Use cases are also described for each clean-up module.

Order	Analysis modules	Technology	Useful settings in the CARO-Suite
1 Domain scan as a basic requirement	ARCA	AD, Entra ID	Scan daily, Search for at least inactive users
2 Check share permissions	SARA	FS	At least once a week
3 Find and remove dead SIDs	TEUS	FS, AD	At least once a week
4 Correct owner	BAKS	AD, FS	*So that the direct permissions created by CREATOR_ONWER are retained by subsequent ERBE clean-ups.
5 Create order for direct permissions	DARS	FS	
6 Correct problematic creator owners	BAKS DARS ERBE	FS	*May run if has been run BAKS OR a group concept is used on the system AND DARS does not provide any information, i.e. no permission groups are missing.
7 Remove direct unwanted permissions	DUKE	FS, AD	
8 Eliminate redundant permissions	RAPA	FS	

Mr. L., System Administrator*
"I don't want to be so euphoric that we have found so many errors. But now I am glad that the CARO-Suite cleaned up so quickly!

*Names and company information have been shortened for data protection reasons. We would be happy to provide you with these references in a personal meeting.

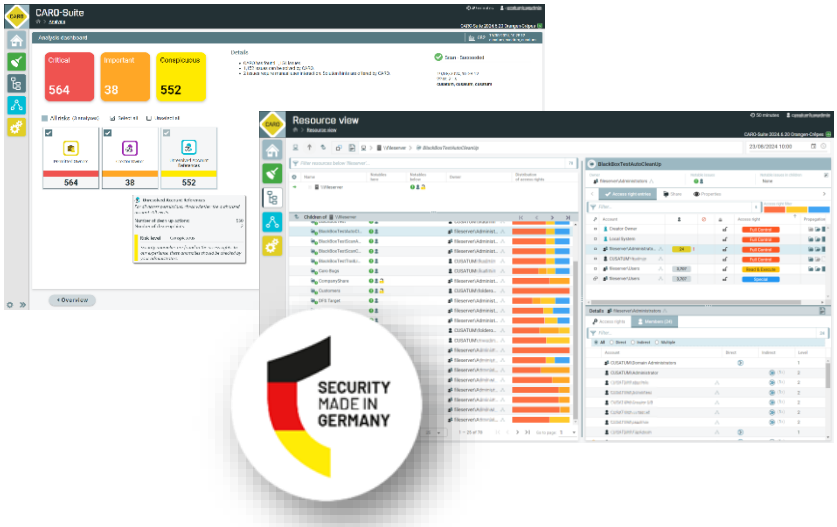
CARO-Suite

CARO-Suite - Access rights securely under control!

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

THE CARO-SUITE IN DETAIL

- Risk assessment with expert knowledge
- User-configurable dashboards for the clean-up progress
- Comprehensive recommendations for cleaning up
- Detailed analyses for access rights errors
- Clear task scheduling with calendar view
- Global resource view of access rights with group memberships
- Accounts view with group overview, search and display of anomalies
- High-performance scans and comprehensive analyses to change your problematic access rights
- Scans and changes scheduled for any point in time
- For file system, Active Directory and 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

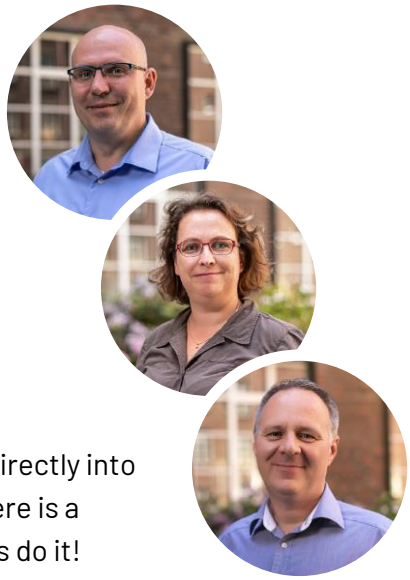


CARO-Suite

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.
As "makers from the very beginning", we developed 8MAN from Protected Networks. This is now called SolarWinds-ARM and is still a great success in German-speaking countries today.

Today, we have combined our experience of one and a half decades in access rights management in our CARO-Suite. It is the necessary addition to ARM that was missing until now! The CARO-Suite supports companies in access rights management to fulfil common security and compliance guidelines.



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!

CUSATUM

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

December 2024

SECURITY MADE IN GERMANY