CARO-Suite

Zugriffsrechte sicher im Griff!

CARO findet Ihre Berechtigungsprobleme, räumt diese automatisiert auf und hält die Berechtigungen auf Ihre Daten sauber.

- Risikobewertung von Experten
- Automatisierter Bereinigungsprozess
- Individuelle Dashboards
- Analysen für hybride Szenarien
- Rollen-Zugriffsberechtigungen einfach dargestellt
- Einfach integrierbar und leicht zu bedienen

RISK ASSESS ©

Für Ihren Durchblick

Übersicht durch Experten-Risikobewertung und umfangreiche Berechtigungsanalysen.

AUTOMATE ©

Für Ihre Entlastung

Effizienz durch detaillierte Handlungsempfehlungen und automatisiertes Bereinigen.

SECURE ©

Für Ihre Kontrolle

Mit compliance-konformen Reporten und revisionssicherer Protokollierung.

CUSATUM

CUSATUM Service GmbH

Hauptsitz
Wiesenweg 16
16548 Glienicke / Nordbahn

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

SECURITY MADE IN GERMANY

CARO-Suite

3 Module für Ihre IT-Sicherheit

Mit der CARO-Suite können Sie Berechtigungsfehler und Risiken von Zugriffsrechten analysieren und automatisiert bereinigen. Sparen Sie Zeit und Geld durch saubere Berechtigungsstrukturen mit optimierten Zugriffsrechten.

Die CARO-SUITE bietet für Ihre IT-Sicherheit:

CARO - RISK ASSESS ©

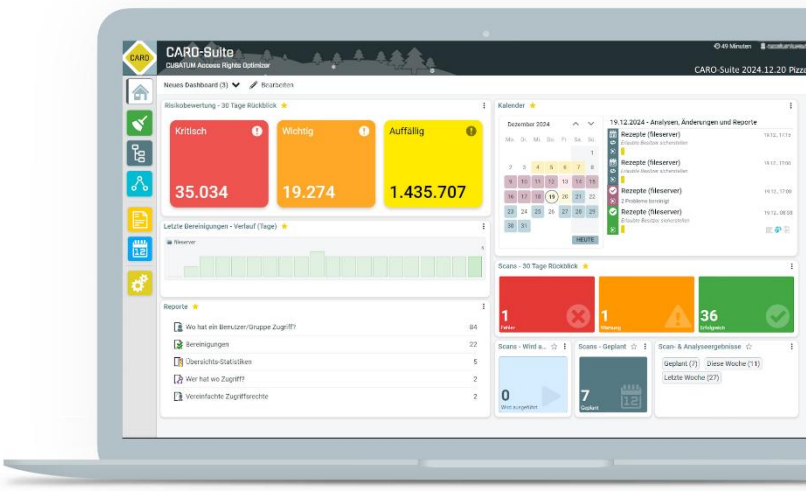
- Risikobewertung von Experten
- Berechtigungsanalysen
- Accounts- und Ressourcenansicht

CARO - AUTOMATE ©

- Automatisiertes Bereinigen
- Handlungsempfehlungen
- Schnelle Aufgabenplanung

CARO - SECURE ©

- Revisionssichere Reporte
- Zugriffsreporte für Data Owner
- Compliance-konform
- Konfigurierbare Dashboards



SECURITY MADE IN GERMANY

CARO-Suite

Risikobewertung von Experten

Mit dem **Risiko-Dashboard** erkennen Sie auf einen Blick, wo bei Ihnen die größten Risiken zu finden sind und wie Sie die Probleme mit wenigen Klicks automatisiert bereinigen.

Risiko-bewertung	Bereinigungsbausteine	Erklärung	Analysen
Kritisch	VASS, ARCA, RAPA, DUKE, DARS, BAKS, SARA	Diese Analysen finden Berechtigungsfehler, die von unseren Experten als kritisch eingestuft werden. Kritische Fehler entstehen durch unzulässige Zugriffsrechte und sollten vorrangig bereinigt werden.	✓ Erlaubte Besitzer-Analyse ✓ Direkte Benutzerberechtigung ✓ Redundante Zugriffsrechte ✓ Unterbrochene Vererbung ✓ Inaktive Computer ✓ Kennwort läuft nie ab ✓ Aktivierte Vererbung in Shares ✓ Offene Freigaben ✓ Privilegierte Rollen ✓ Globale Administrator-Rolle ✓ Anzahl Globale Admins ✓ Ablaufende Clientschlüssel
Wichtig	ERBE, MARS, VASS, ARCA, LARS, SARA	Diese Analysen finden weitere als wichtig eingestuften Probleme in Ihrem System. Solche relevanten Probleme sollten zeitnah behoben werden.	✓ Ersteller-Besitzer ✓ Mindest-Berechtigungen ✓ Verschobene Verzeichnisse ✓ Ungewollte Konten ✓ Inaktive Benutzer ✓ Listgruppenanalyse ✓ Jeder-Vollzugriff Freigaben ✓ Gruppen-Rollenzuweisungen ✓ Cloud-Native Konten Rollenzuweisungen ✓ Inaktive Gastbenutzer ✓ Inaktive Anwendungen
Auffällig	TEUS, ARCA, SARA	Es werden Sicherheits-auffälligkeiten in den Zugriffsrechten gefunden. Diese Auffälligkeiten sollten nach unserer Erfahrung durch Ihre Administratoren überprüft werden.	✓ Verwaiste Kontoreferenzen ✓ Veraltetes Kennwort ✓ Deaktivierter Benutzer ✓ Nie angemeldete Benutzer ✓ Leere Gruppen ✓ Gruppen ohne Beschreibung ✓ Nicht-administrative Freigaben ✓ Inaktive Cloud-Native Benutzer ✓ Cloud-Native Benutzer

CARO-Suite

Analyse- und Bereinigungsbausteine

Standardmäßig werden 13 Bereinigungs- und Analysebausteine mit der CARO-Suite ausgeliefert.

BAKS

Besitzer-**A**nalyse- und **K**orrektur-**S**oftware

- Stellt zulässige Besitzer sicher, damit administrative Konten Ihre Berechtigung behalten, z.B. damit Backup-Tools funktionieren
- Analysiert Sicherheitsrisiken durch das Entfernen von unerlaubten und unkontrollierbaren Zugriffs-Berechtigungen

Besitzer korrigieren

Kritisch

LARS

Listgruppen **A**nalyse- und **R**estrukturierungs-**S**oftware

- Analyse der Berechtigungen in Ordner-Hierarchien
- Verwalten von List-Berechtigungen in übergeordneten Ordnern

Fehler in Listgruppen Analysieren

Wichtig

TEUS

Tool zur **E**ntfernung **u**nbekannter **S**IDs

- Entfernt tote SIDs und macht die Dokumentation Ihrer Berechtigungen wieder leichter lesbar und verständlich
- Reduziert die Nachfragen Ihrer Revision und dokumentiert, dass Sie die volle Kontrolle haben
- Bietet mehr Sicherheit, da weniger Angriffsfläche für SID History Injection

Verwaiste SIDs entfernen

Auffällig

DARS

Direktzugriff **A**nalyse- und **R**estrukturierungs-**S**oftware

- Identifiziert Direktberechtigungen von Usern
- Korrigiert effizient diese Einträge

Direkte Berechtigungen prüfen

Kritisch

RAPA

Redundant **A**ccount **P**ermission **A**nalysis

- Identifiziert redundante Berechtigungen
- Überprüfen von Gruppenmitgliedschaften mit gleichzeitiger Direktberechtigung

Redundante Berechtigungen Beseitigen

Kritisch

SARA

Share **A**ccess **R**ights **A**nalysis

- Analyse von Freigabe-Zugriffsrechten
- Prüfen auf vererbte NTFS-Zugriffsrechte
- Sucht „offenen Shares" für authentifizierte Konten
- Suchen von Jeder-Vollzugriff Freigaben
- Prüfen auf die Existenz von nicht-administrativen Freigaben

Freigabe-Berechtigungen überprüfen

Analyse- und Bereinigungsbausteine

Standardmäßig werden 13 Bereinigungs- und Analysebausteine mit der CARO-Suite ausgeliefert.

DUKE

Direktzugriffsrechte **U**ngewollter **K**onten **E**ntfernen

- Identifiziert alle Zugriffsrechte der konfigurierten ungewollten Konten und entfernt diese
- Reduziert Sicherheitsrisiken durch das Entfernen von unbekannten und unkontrollierbaren Zugriffsberechtigungen

Direkte ungewollte Berechtigungen entfernen

Kritisch

VASS

Vererbung-**A**nalyse- und **S**anierungs-**S**oftware

- Identifiziert veränderte Berechtigungen in Ordner-Hierarchien
- Angleichung der Berechtigungen durch Vererbung oder andere systemspezifische Werkzeuge

Aufgebrochene Vererbungen wieder-herstellen,

Kritisch

Verschobene Verzeichnisse finden

Wichtig

ARCA

Account **R**isk- und **C**ompliance-**A**ssessment

- Analysiert Konto-basierend auf Best Practice-Kriterien
- Für Active Directory und Entra ID
- **AD**: Inaktive Benutzer- oder Computerkonten, deaktivierte Benutzerkonten, nie angemeldete Benutzer, leere Gruppen und Gruppen ohne Beschreibung, Konten mit nie ablaufenden Kennwörtern,
- **Entra ID**: Globale Administratoren Anzahl an Gruppen und deren Mitglieder, Privilegierte Rollenzuweisungen, Gruppen in Rollenzuweisungen, Nutzung von Cloud-native-Konten, Ablaufende Clientschlüssel, Finden von inaktiven Gastbenutzern und inaktiven Cloud-native Benutzern, inaktive Anwendungen,

Risk- und Compliance Dashboard für Active Directory und Entra ID

ERBE

ERsteller-**B**esitzer auf Dateisystemen **E**ntfernen

- Entfernt den Ersteller-Besitzer und verhindert das Entstehen von neuen toten SIDs
- Erlaubt damit eine saubere Migration, z.B. in die Cloud

Ersteller-Besitzer entfernen

Wichtig

MARS

Mindestberechtigungen **A**nalyse und **R**estrukturierungs-**S**oftware

- Prüft alle Dokumente und Ordner auf erforderliche Zugriffsrechte für Konten und berücksichtigt dabei sowohl direkte als auch indirekte Zugriffsrechte
- Setzt fehlende Berechtigungen

Mindest-Berechtigungen Überprüfen

Wichtig

Berechtigungen anzeigen und dokumentieren

Mit dem Module EBIS zeigt CARO eine globalen Ressourcenansicht mit der IST-Berechtigungssituation an. Sie können Berechtigungs- und Use-Case-Reporte erstellen, einfach an Ihre Corporate Identity anpassbar durch Microsoft-Word-Office-Vorlagen.

EBIS

Erfassung der **B**erechtigungs-**I**st-**S**ituation

- Zeichnet die Berechtigungslage auf Fileservern auf
- Analysiert u.a. auf unterbrochenen Vererbungshierarchien, verschobene Verzeichnisse oder Null-DACL in den ACEs
- Anzeige von fehlenden Besitzereinträgen
- Zeigt im Detail geänderte Berechtigungen unterhalb an, wie hinzugekommene oder entfernte Zugriffsrechte
- Zeigt Gruppenmitgliedschaften mit direkten und indirekten Mitgliedschaftsbeziehungen
- Reporte für die IST-Berechtigungssituation „Wer hat wo Zugriff?"
- Reporte über geänderte Berechtigungen unterhalb
- Differenz-Reporte für eine Verzeichnisstruktur
- Report „Wo hat ein Benutzer Zugriff?"

IST-Situation erfassen und Berechtigungen reporten

Best Practices

Für das Bereinigen ist es sinnvoll, bestimmte Analysen gemeinsam zu nutzen. In unserem Flyer *Best Practices und Anwendungsfälle zum Bereinigen* erfahren Sie mehr über eine empfohlene Reihenfolge und sinnvolle Kombinationen von CARO-Analysen für ein effizientes Bereinigen.

Ebenfalls werden zu jedem Bereinigungsbaustein Anwendungsfälle beschrieben.

	Reihenfolge	Analyse-Bausteine	Technologie	Sinnvolle Einstellung in der CARO-Suite
1	Domänen-Scan als Grundvoraussetzung	ARCA	AD, Entra ID	Täglich scannen, Mindestens inaktive Benutzer suchen
2	Freigabe-Berechtigungen überprüfen	SARA	FS	Mindestens 1x pro Woche
3	Tote SIDs finden und entfernen	TEUS	FS, AD	Mindestens 1x pro Woche
4	Besitzer korrigieren	BAKS	AD, FS	*Damit ggf. die durch CREATOR_OWNER erzeugten Direktberechtigungen durch spätere ERBE-Bereinigungen bestehen bleiben.
5	Direkte Berechtigungen aufräumen	DARS	FS	
6	Problematische Ersteller-Besitzer korrigieren	BAKS DARS ERBE	FS	*Darf laufen, wenn DARS gelaufen ist **ODER** auf dem System ein Gruppenkonzept eingesetzt wird **UND** DARS keine Hinweise liefert, d.h. es fehlen keine Berechtigungsgruppen.
7	Direkte ungewollte Berechtigungen entfernen	DUKE	FS, AD	
8	Redundante Berechtigungen beseitigen	RAPA	FS	

Herr L., System-Administrator*
„Ich will gar nicht so euphorisch sein, dass wir so viele Fehler gefunden haben.
Aber nun bin ich wirklich froh, dass hier die CARO-Suite so schnell aufgeräumt hat!

*Namen und Firmeninformation sind aus Datenschutzgründen gekürzt. Gerne geben wir Ihnen in einem persönlichen Gespräch diese Referenzen weiter.

CARO-Suite

CARO-Suite - Zugriffsrechte sicher im Griff!

Historisch gewachsene Berechtigungsstrukturen gehören mit CARO der Vergangenheit an. Sicherheitslücken werden beseitigt und automatisch reduziert. CARO sorgt in Ihren IT-Strukturen für Ordnung!

DIE CARO-SUITE IM DETAIL

- Risikobewertung mit Expertenwissen
- Benutzerkonfigurierbare Dashboards für den Bereinigungsfortschritt
- Umfangreiche Handlungsempfehlungen zum Bereinigen
- Detaillierte Analysen für Berechtigungsfehler
- Übersichtliche Aufgabenplanung mit Kalenderansicht
- Globale Ressourcen-Ansicht der Zugriffsrechte mit Gruppenmitgliedschaften
- Accounts-View mit Gruppen-Übersicht, Suche und Anzeige von Auffälligkeiten
- Hoch performante Scans und umfangreiche Analysen zur Änderung Ihrer problematischen Zugriffsrechte
- Planbarkeit von Scans und Änderungen für einen beliebigen Zeitpunkt
- Für Filesystem, Active Directory und Entra ID
- Integration in andere Systeme über Rest-API
- Automatisierung von Mitarbeiterprozessen mit dem Zusatzmodul C-MAN
- Basis-Reporte im PDF-Format, durch Word-Office-Report-Vorlagen einfach an eigene Corporate-Identity anpassbar
- Revisionssichere Protokollierung aller durchgeführten Änderungen
- Mehrsprachiger Web-Client mit Multi-User-Support
- Datenspeicherung in MS-SQL-Datenbank
- Einfaches Lizenzmodell

CARO-Suite

CUSATUM – Gemeinsam für mehr Sicherheit!

Die CUSATUM Service GmbH am Standort Berlin/Brandenburg ist ein Software- und Beratungsunternehmen mit dem Fokus auf Berechtigungsmanagement und Automatisierung von Mitarbeiterprozessen.
Als „Macher der ersten Stunde" haben wir den 8MAN von Protected Networks entwickelt. Dieser heißt jetzt SolarWinds-ARM und ist bis heute ein großer Erfolg im deutschsprachigen Raum.

Unsere Erfahrungen aus eineinhalb Jahrzehnten im Berechtigungsmanagement haben wir heute in unserer CARO-Suite vereinigt. Sie ist die notwendige Ergänzung zum ARM, die bisher gefehlt hat! Die CARO-Suite unterstützt Unternehmen im Berechtigungsmanagement zur Erfüllung gängiger Sicherheits- und Compliance-Richtlinien.

Mike Wiedemann, CEO
Seine Leidenschaft ist Kundenzufriedenheit. Für zufriedene Kunden geht er auch die „extra Meile"!

Ute Wagner, CDO
Ein User Interface muss nicht nur einfach zu bedienen sein, es muss auch Freude machen, es zu nutzen!

Christian Schönfeld, CEO
Meine Erfahrungen direkt umwandeln in CARO - das ist mein Anspruch! Für alles gibt es eine Lösung. Packen wir es an!

CUSATUM

Herausgeber

CUSATUM Service GmbH

Hauptsitz
Wiesenweg 16
16548 Glienicke / Nordbahn

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

Support

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

E-Mail: support@cusatum.de

Stand: Januar 2025

SECURITY MADE IN GERMANY