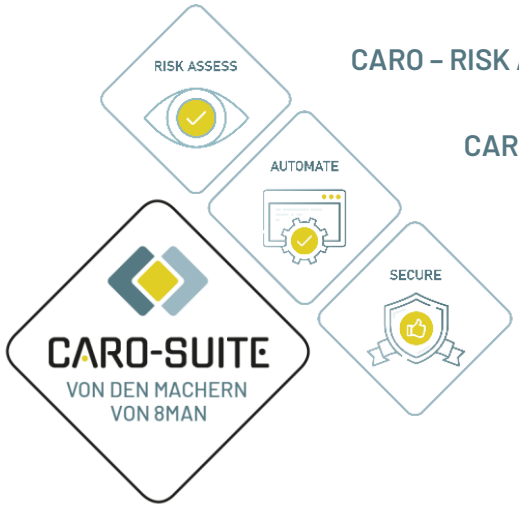
CARO-Suite Cloud

Mit der CARO-Suite an Ihrer Seite schließen Sie gezielt Sicherheitslücken in Ihren Zugriffsrechten und schützen Ihre wertvollen Daten.

- Kombiniert Fileserver, Active Directory und Microsoft Entra ID Informationen.
- Räumt auch Ihre Cloud auf.
- Führt Analysen für hybride Szenarien aus.
- Stellt Microsoft Entra ID-Informationen und Rollen-Zugriffsberechtigungen einfach dar.
- Lässt Access Right Management- und IDM-Systeme effizienter arbeiten.

CARO-Suite
Microsoft Entra ID
Verfügbar für die CLOUD



CARO – RISK ASSESS © - *Für Ihren Durchblick*

CARO - AUTOMATE © - *Für Ihre Entlastung*

CARO - SECURE © - *Für Ihre Kontrolle*

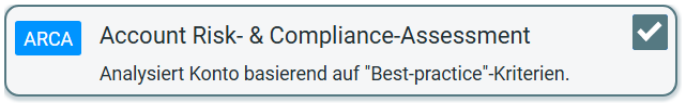
SECURITY MADE IN GERMANY

Microsoft Entra ID

(ehemals Microsoft Azure Active Directory oder Azure AD)

Analysen und Bereinigungen mit der CARO-Suite

Mit dem Analyse- und Bereinigungs-Baustein ARCA können Sie cloudbasierte Analysen durchführen. CARO ordnet die gefundenen Probleme und Auffälligkeiten automatisch in Risikostufen ein. Der Baustein ARCA ist standardmäßig in der CARO-Suite-Lizenz enthalten.



Analysen für Entra ID

Zugriffsüberprüfungen in der Cloud

Mit CARO können Sie jetzt Ihre Zugriffe für cloudbasierte und hybride Ressourcen auf Entra ID überprüfen und bereinigen. CARO integriert dabei Best Practices für Microsoft Entra-Rollen.

Eine ausführliche Beschreibung der Microsoft Best Practices (*) finden Sie hier: https://learn.microsoft.com/de-de/entra/identity/role-based-access-control/best-practices

ARCA

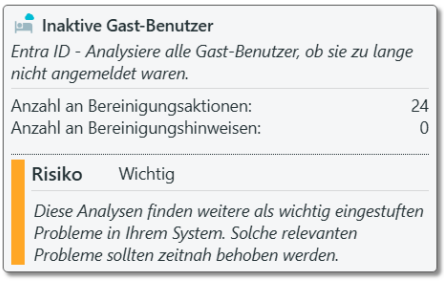
Best Practices nach Microsoft*

- Überprüfen und Bereinigen Ihrer Globalen Administratoren auf zulässige Anzahl und Rollenzuweisungen mit Mitgliedern.
- Überprüfung, dass nur Cloud-native-Konten für Rollenzuweisungen genutzt werden.
- Ausschließliche Nutzung von Gruppen in Rollenzuweisungen.
- Überprüfung der Anzahl von privilegierte Rollenzuweisungen auf die zulässige Anzahl.

Weitere Risiko-Analysen

- Findet in den App-Registrierungen alle ablaufenden Clientschlüssel, die schon abgelaufen sind oder in X Tagen ablaufen. Die Anzahl der Tage ist konfigurierbar.
- Finden Ihrer Inaktiven Gast-Benutzer, die sich für einen längeren Zeitraum nicht angemeldet haben.
  Der Zeitraum ist bei der Analyse konfigurierbar.
- Analysiere alle Globalen Administratoren.

- Finden aller Cloud-native Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind.
- Auffinden aller Inaktiven Cloud-native Benutzer, die nicht mit einem On-Prem-AD synchronisiert sind und sich für einen längeren Zeitraum nicht angemeldet haben. Der Zeitraum ist konfigurierbar.
- Ablaufende Clientschlüssel in den App-Registrierungen finden.
- Ablaufende Abonnements finden.
- Finden von inaktiven On-Prem-Benutzern, die nicht mit einem On-Prem-AD synchronisiert sind.

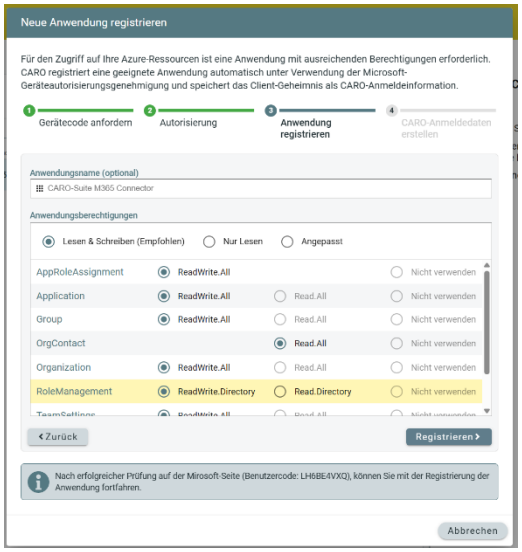


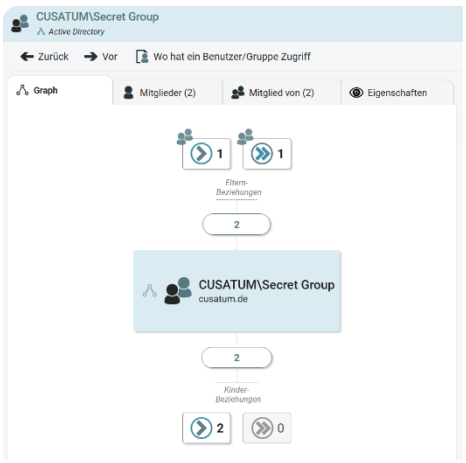
Anbindung an Microsoft Entra ID

Automatische App-Registrierung

Für die Anbindung von CARO an ein Entra ID-System bieten wir Ihnen einen integrierten *4-Klick-Workflow* zur App-Registrierung ihres Client Secrets an.

Wo andere Hersteller oft nur eine Hilfestellung per Webseite anbieten, brauchen Sie bei CARO nur den Tenant-Namen des Entra ID-Systems einzugeben, der Registrierungsprozess wird anschließend automatisch durchgeführt.





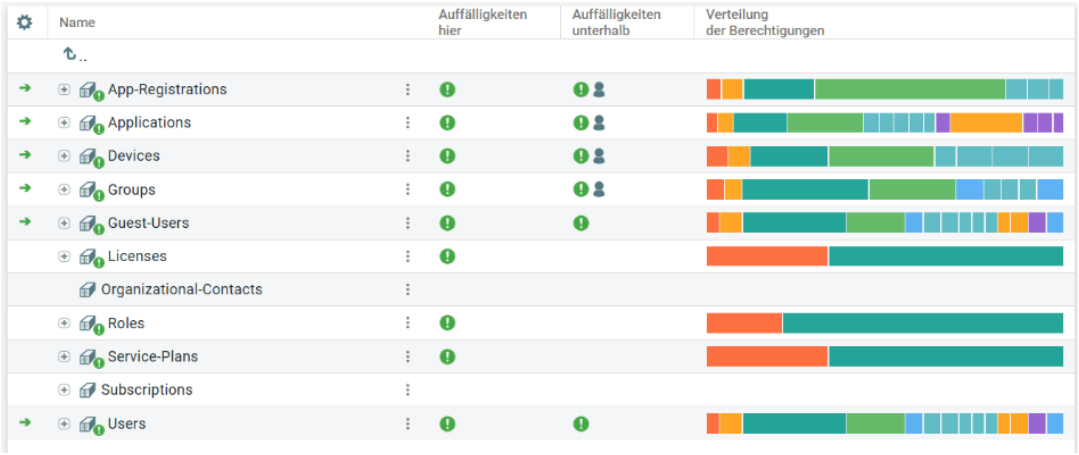
Gruppenmitgliedschaften

Direkte und indirekte Gruppenmitgliedschaften

In der CARO-Kontenansicht werden auch für Entra-ID-Konten die Gruppenmitglieder und deren Gruppenmitgliedschaften angezeigt. Ebenfalls werden spezifische Eigenschaften der Konten aufgeführt.

Berechtigungen im Detail

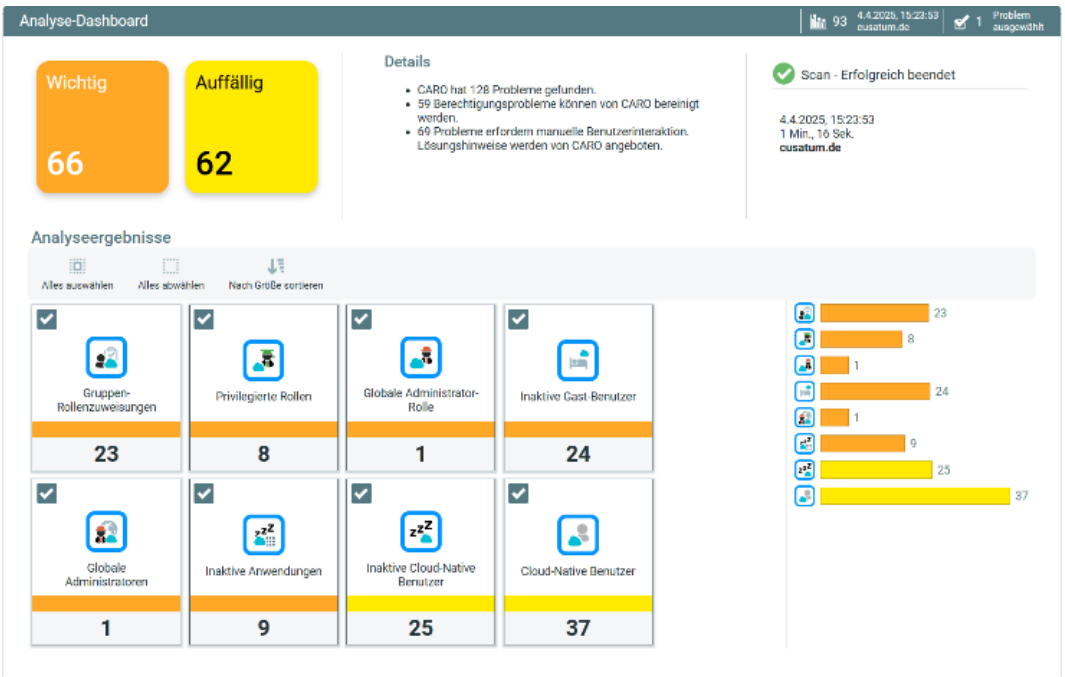
In der CARO-Ressourcenansicht sind wichtige Informationen zu den rollenbasierten Zugriffsrechten im Entra ID dargestellt, ebenso Mitglieder von Entra-Rollen, verwendete Lizenzen und Anwendungen oder auch Gast-Benutzer.



Risikobewertung von Experten

Die erkannten Probleme aus den Analysen der CARO-Suite werden in 3 Kategorien eingestuft: kritische, wichtige und auffällige Probleme von Zugriffsrechten, analog zur Risikobewertung zur BSI-Risikomatrix.

(Quelle: Matrix zur Einstufung von Risiken, BSI-Standard 200-3, www.bsi.bund.de/grundschutz, v 1.0).



CARO-Suite

BSI-Risikomatrix*

Alle gefundenen Probleme aus den Analysen der CARO-Suite werden in 3 Kategorien eingestuft: kritische, wichtige und auffällige Probleme von Zugriffsrechten, analog zur Risikobewertung zur BSI-Risikomatrix.

(*Quelle: Matrix zur Einstufung von Risiken, BSI-Standard 200-3, **www.bsi.bund.de/grundschutz**, v 1.0).

Risiko-bewertung	Erklärung	Analysen mit ARCA
Kritisch	Diese Analysen finden Berechtigungsfehler, die von unseren Experten als kritisch eingestuft werden. Kritische Fehler entstehen durch unzulässige Zugriffsrechte und sollten vorrangig bereinigt werden.	**Entra ID Analysen** ✓ Privilegierte Rollen ✓ Globale Administrator-Rolle ✓ Anzahl Globale Admins ✓ Ablaufende Clientschlüssel Weitere Analysen im Active Directory ✓ Erlaubte Besitzer-Analyse ✓ Direkte Benutzerberechtigungen ✓ Redundante Zugriffsrechte ✓ Unterbrochene Vererbung, Aktivierte Vererbung in Shares, Offene Freigaben ✓ Inaktive Computer ✓ Kennwort läuft nie ab
Wichtig	Diese Analysen finden weitere als wichtig eingestuften Probleme in Ihrem System. Solche relevanten Probleme sollten zeitnah behoben werden.	**Entra ID Analysen** ✓ Gruppen-Rollenzuweisungen ✓ Cloud-Nat. Konten Rollenzuweisungen ✓ Inaktive Gastbenutzer ✓ Inaktive Anwendungen ✓ Ablaufende Abonnements Weitere Analysen im Active Directory ✓ Mindest-Berechtigungen ✓ Verschobene Verzeichnisse ✓ Inaktive Benutzer ✓ Listgruppenanalyse ✓ Jeder-Vollzugriff-Freigaben

Risikobewertung von Experten

Risiko-bewertung	Erklärung	Analysen mit ARCA
Auffällig	Es werden Sicherheits-auffälligkeiten in den Zugriffsrechten gefunden. Diese Auffälligkeiten sollten nach unserer Erfahrung durch Ihre Administratoren überprüft werden.	**Entra ID Analysen** ✓ Inaktive Cloud-Native Benutzer ✓ Inaktive On-Prem-Benutzer ✓ Cloud-Native Benutzer Weitere Analysen im Active Directory ✓ Verwaiste Kontoreferenzen ✓ Veraltetes Kennwort ✓ Deaktivierter Benutzer ✓ Nie angemeldete Benutzer ✓ Leere Gruppen, ohne Beschreibung ✓ Nicht-administrative Freigaben

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.

Den Flyer *CARO-Suite Best Practices.pdf* finden Sie **hier**.

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 BAKS 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.

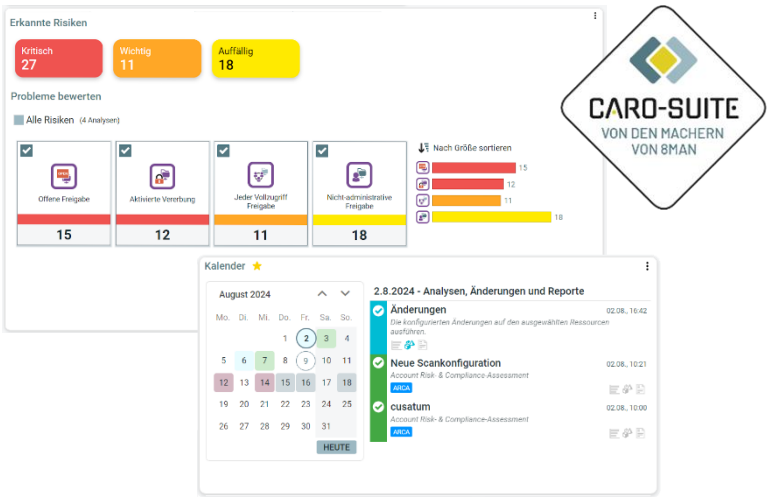
CARO-Suite

CARO-Suite - Zugriffsrechte sicher im Griff!

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

Die Caro-Suite Im Detail

- Risikobewertung im Analyse-Dashboard mit Expertenwissen
- Detaillierte Analysen für Berechtigungsfehler enthalten
- Umfangreiche Handlungsempfehlungen zum Bereinigen
- Benutzerdefinierte Dashboards mit Bereinigungsverlauf und Aufgabenplanung
- Globale Ressourcen-Ansicht der Zugriffsrechte mit Gruppenmitgliedschaften
- Konten-Ansicht mit direkten und indirekten Gruppenmitgliedschaften
- 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 Microsoft 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 WebClient 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, COO
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: April 2025

SECURITY MADE IN GERMANY