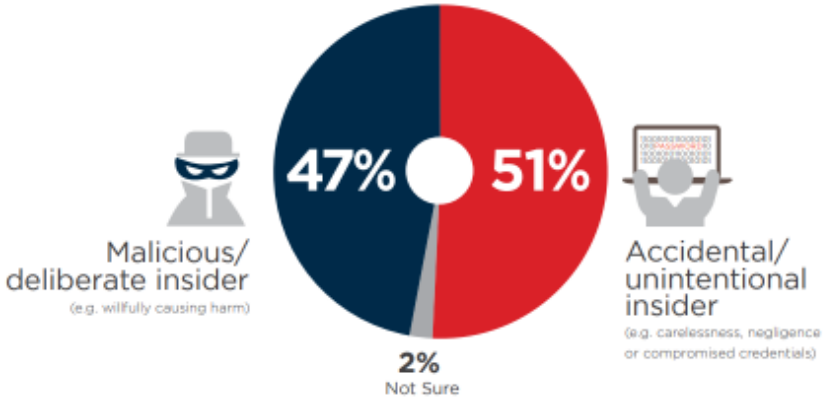
SolarWinds® Access Rights Manager

Interne Risiken so groß wie externe Risiken

Interne Risiken nehmen viele Formen an



KEY SURVEY FINDINGS

1. Ninety percent of organizations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%).

2. A majority of 53% confirmed insider attacks against their organization in the previous 12 months (typically less than five attacks). Twenty-seven percent of organizations say insider attacks have become more frequent.

3. Organizations are shifting their focus on detection of insider threats (64%), followed by deterrence methods (58%) and analysis and post breach forensics (49%). The use of user behavior monitoring is accelerating; 94% of organizations deploy some method of monitoring users and 93% monitor access to sensitive data.

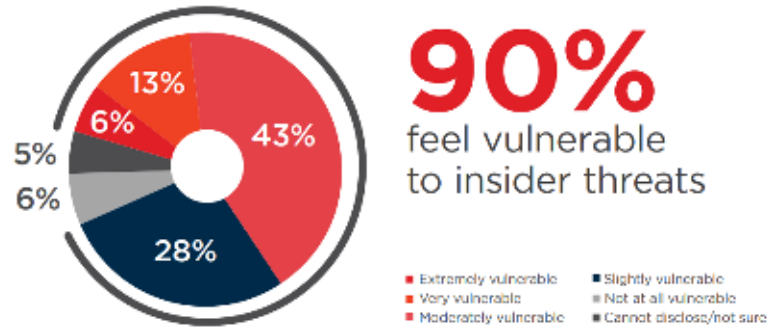
4. The most popular technologies to deter insider threats are Data Loss Prevention (DLP), encryption, and identity and access management solutions. To better detect active insider threats, companies deploy Intrusion Detection and Prevention (IDS), log management and SIEM platforms.

5. The vast majority (86%) of organizations already have or are building an insider threat program. Thirty-six percent have a formal program in place to respond to insider attacks, while 50% are focused on developing their program.

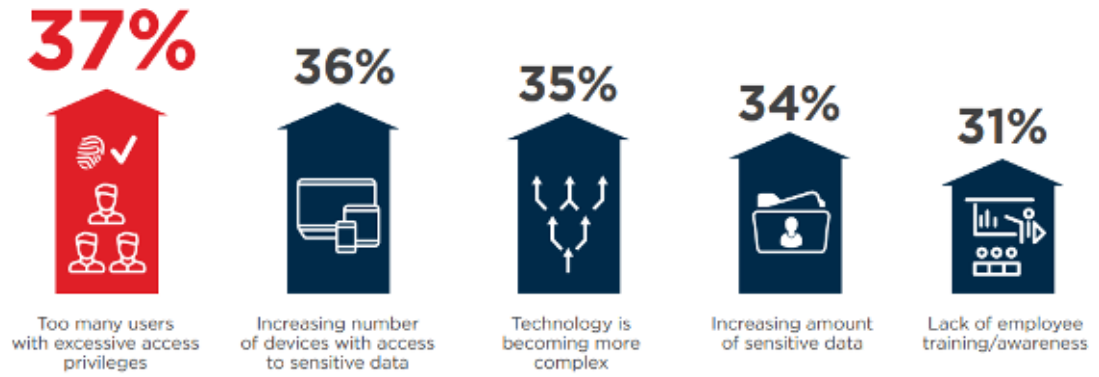
„2018 Insider Threat Report“ Cyber Security Insiders. https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (veröffentlicht 2018, Zugriff März 2019).

Die größten Bedrohungen

How vulnerable is your organization to insider threats?



What do you believe are the main enablers of insider attacks?

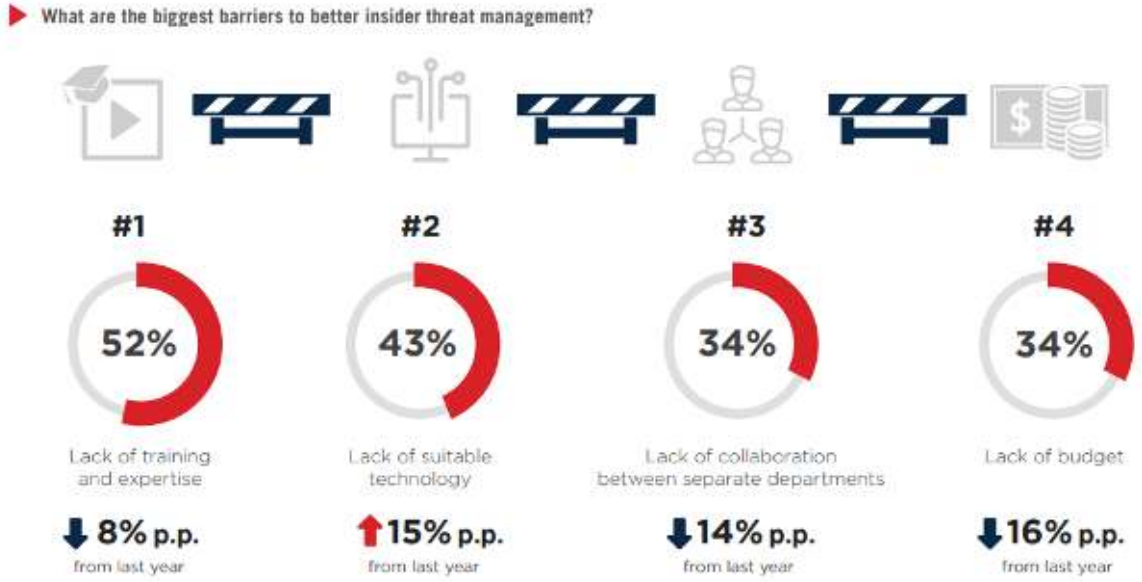


What type(s) of insiders pose the biggest security risk to organizations?*

What type(s) of data are most vulnerable to insider attacks?

„2018 Insider Threat Report“ Cyber Security Insiders. https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (veröffentlicht 2018, Zugriff März 2019).

Wichtigste Hindernisse/Richtlinien/Schulungen



„2018 Insider Threat Report“ Cyber Security Insiders. https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (veröffentlicht 2018, Zugriff März 2019).

Access Rights Manager

Verwalten und Prüfen von Benutzerzugriffsrechten in der gesamten IT-Infrastruktur

Das Sicherheitsniveau und den Schutz vor internen Bedrohungen erhöhen

Automatisieren Sie die Verwaltung, Analyse und Einhaltung von Benutzerzugriffsrechten, indem Sie unsichere Benutzerkonten identifizieren und Prüfprotokolle erstellen.

Compliance nachweisen

Erstellen Sie schnell umfassende Berichte zum Benutzerzugriff für den Nachweis der Einhaltung von gesetzlichen Bestimmungen und Audits.

Benutzerberechtigungen unkompliziert verwalten

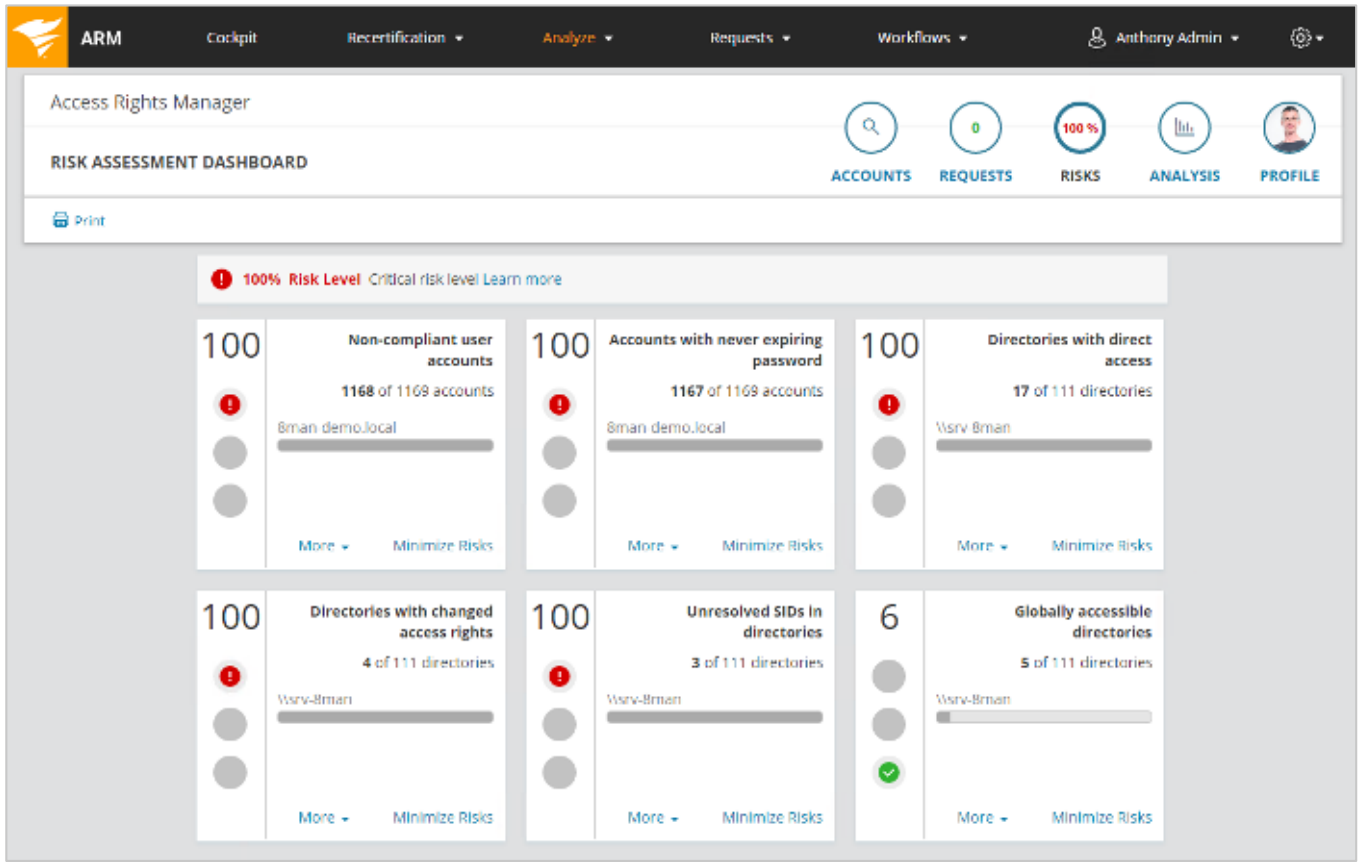
Dank des einfachen Designs können Sie Benutzerberechtigungen mit automatisierter und vorlagenbasierter Bereitstellung und Entziehung einfacher verwalten.

Produktivität steigern

Reduzieren Sie die IT-Workload, indem Sie ein Self-Service-Portal einsetzen und die Berechtigungsverwaltung an die Dateneigentümer delegieren.

Überraschend einfach

Leistungsstarke und intuitive Zugriffsrechteverwaltung und -überwachung für Unternehmen jeder Größe unterstützen beim Schutz vor internen Bedrohungen. Sicherheit war noch nie so einfach.



Was kann ARM heute für Sie tun?

Überwachung und Verwaltung ganz nach Ihren Bedürfnissen

ARM Audit Edition

- Protokollieren, Überprüfen und Überwachen von Benutzerberechtigungen für die wichtigsten Microsoft-Technologien
- Analyse und Überwachung zugriffsbasierter Risikobereiche
- Vollständiger Änderungsüberwachungs-verlauf zum Nachweis der Einhaltung von PCI DSS, DSGVO, SOX, NIST, HIPAA

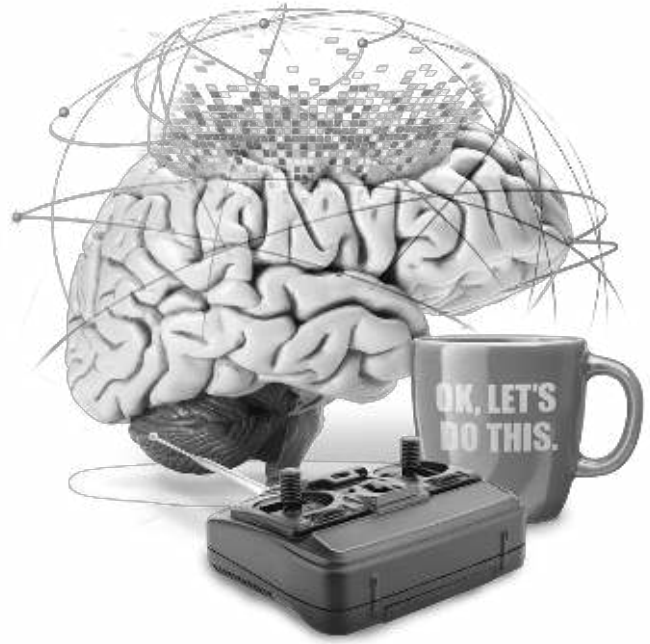
ARM

- Verwaltung von Benutzerberechtigungen
- Benutzerbereitstellung für Active Directory
- Dateneigentümer-Konzept und Delegierung von Benutzerrechten
- Risikomanagement
- Korrektur der Benutzerberechtigungen

Technologien:

- Active Directory®
- Windows®-Fileserver
- Microsoft® Exchange™
- Microsoft OneDrive®
- Microsoft SharePoint®
- SAP R/3*

*nur Überwachung



ARM-Editionen

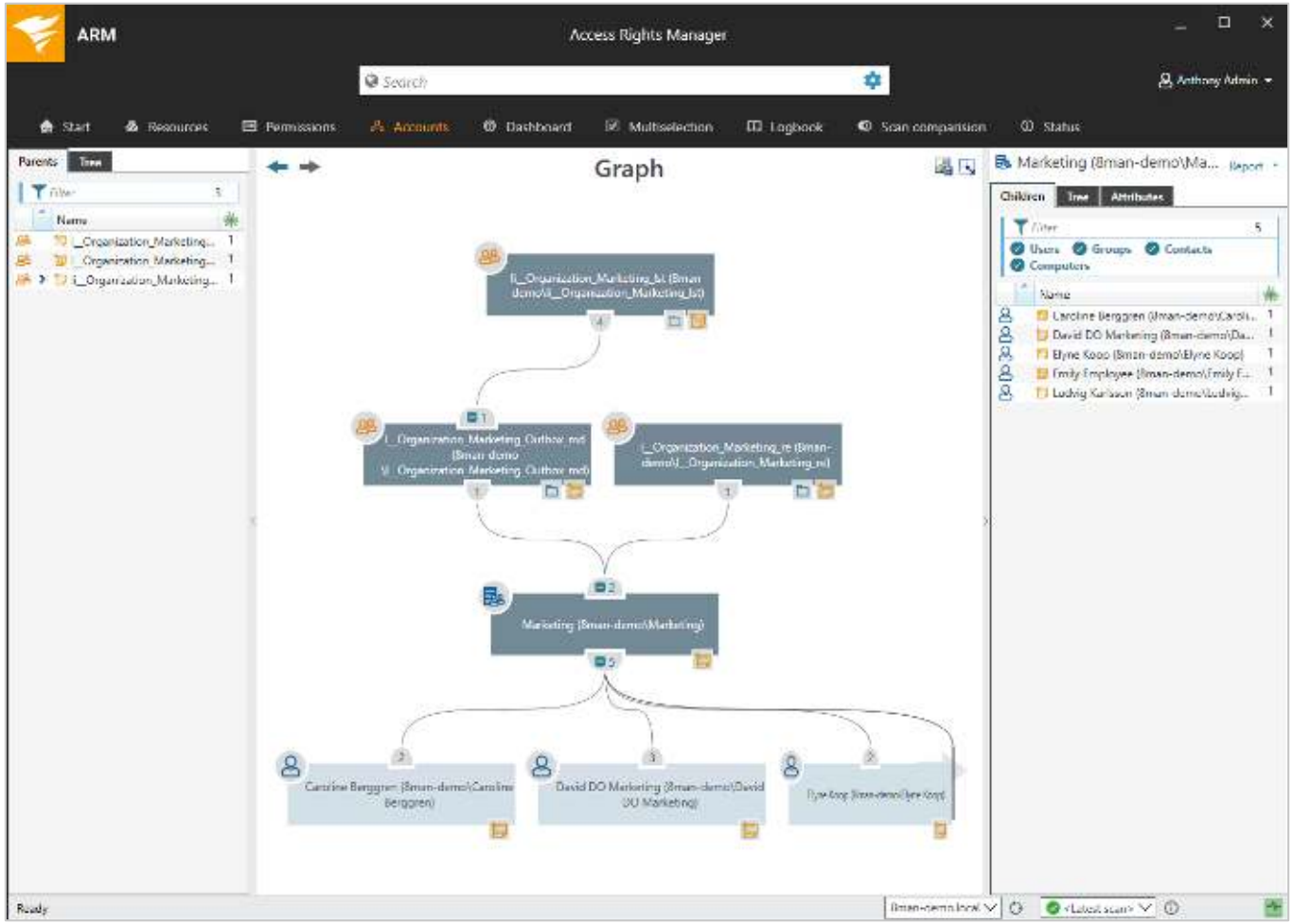
Funktionsmerkmal	ARM Audit Edition	ARM (Vollversion)
Analyse von Benutzerberechtigungen für Active Directory, Fileserver (Windows, EMC, NetApp), SharePoint, Exchange, OneDrive, SAP/R3	✓	✓
Überprüfen (Berichterstellung) für Active Directory, Fileserver (Windows, EMC, NetApp), SharePoint, Exchange, OneDrive, SAP/R3	✓	✓
Überwachen (Protokollieren) für Active Directory, Fileserver (Windows, EMC, NetApp), SharePoint Online, Exchange, OneDrive	✓	✓
Risikoanalyse-Übersicht	✓	✓
Risikomanagement		✓
Benutzerbereitstellung für Active Directory		✓
Benutzermanagement für Active Directory, Fileserver (Windows, EMC, NetApp), SharePoint, Exchange, OneDrive		✓
Dateneigentümer-Konzept (Delegierung der Zugriffsrechteverwaltung)		✓
Self-Service-Portal für Berechtigungen		✓
Problemlösung		✓

Access Rights Manager

Active Directory-Überwachung

Änderungen in Active Directory überwachen und prüfen

Sorgen Sie für mehr Sicherheit durch Überwachung, Analyse und Überprüfung von Active Directory, um festzustellen, welche Änderungen wann und von wem vorgenommen wurden.



Verfügbar in:

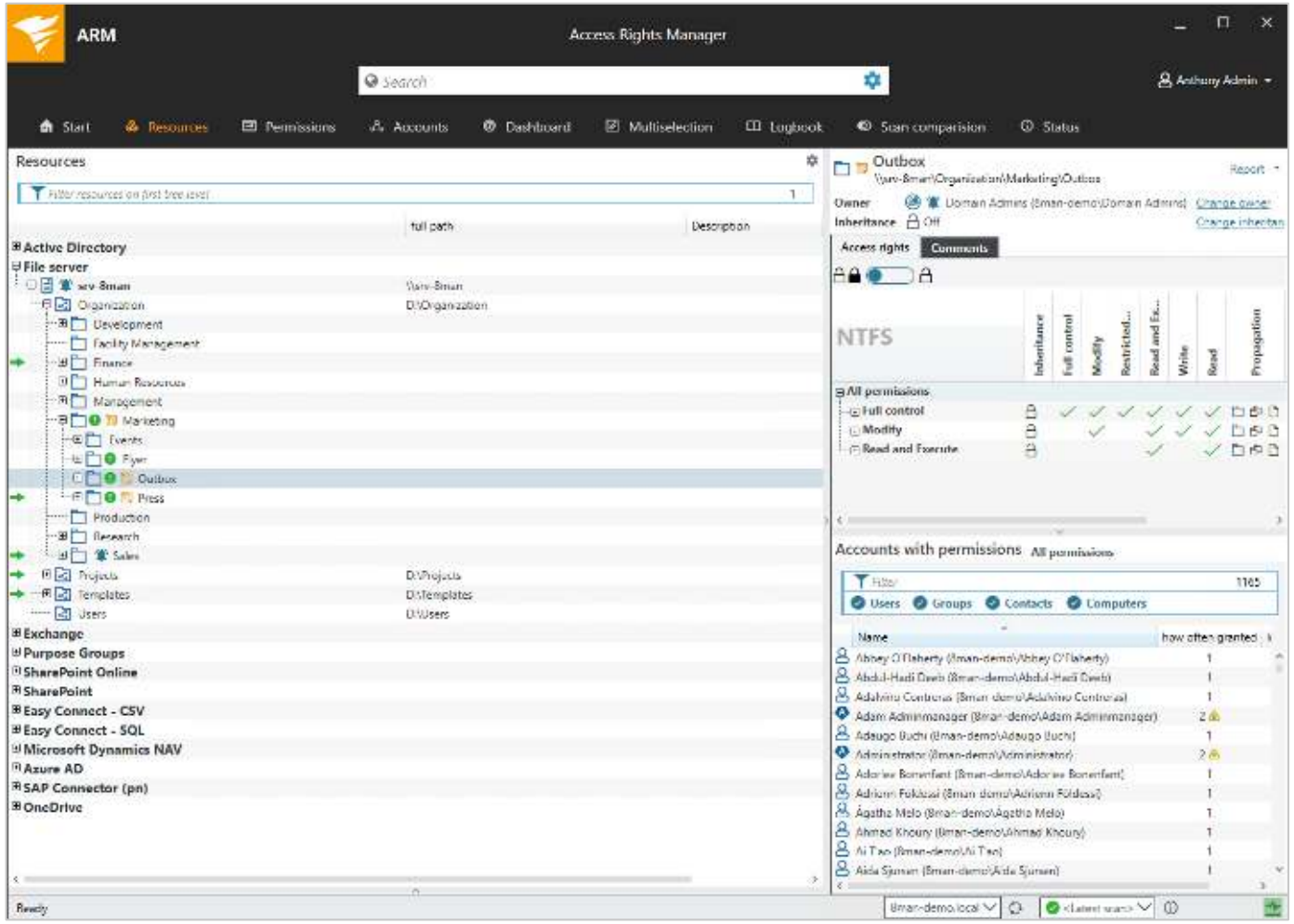
- ✓ ARM Audit Edition
- ✓ ARM

Access Rights Manager

Überprüfung für Windows-Dateifreigaben

Erhalten Sie Warnungen zu unbefugten Zugriffen oder Änderungen an Windows-Fileservern.

Verhindern Sie mithilfe der Visualisierung von Fileserver-Berechtigungen Datenlecks und unbefugte Änderungen an sensiblen Dateien und Daten.



Verfügbar in:

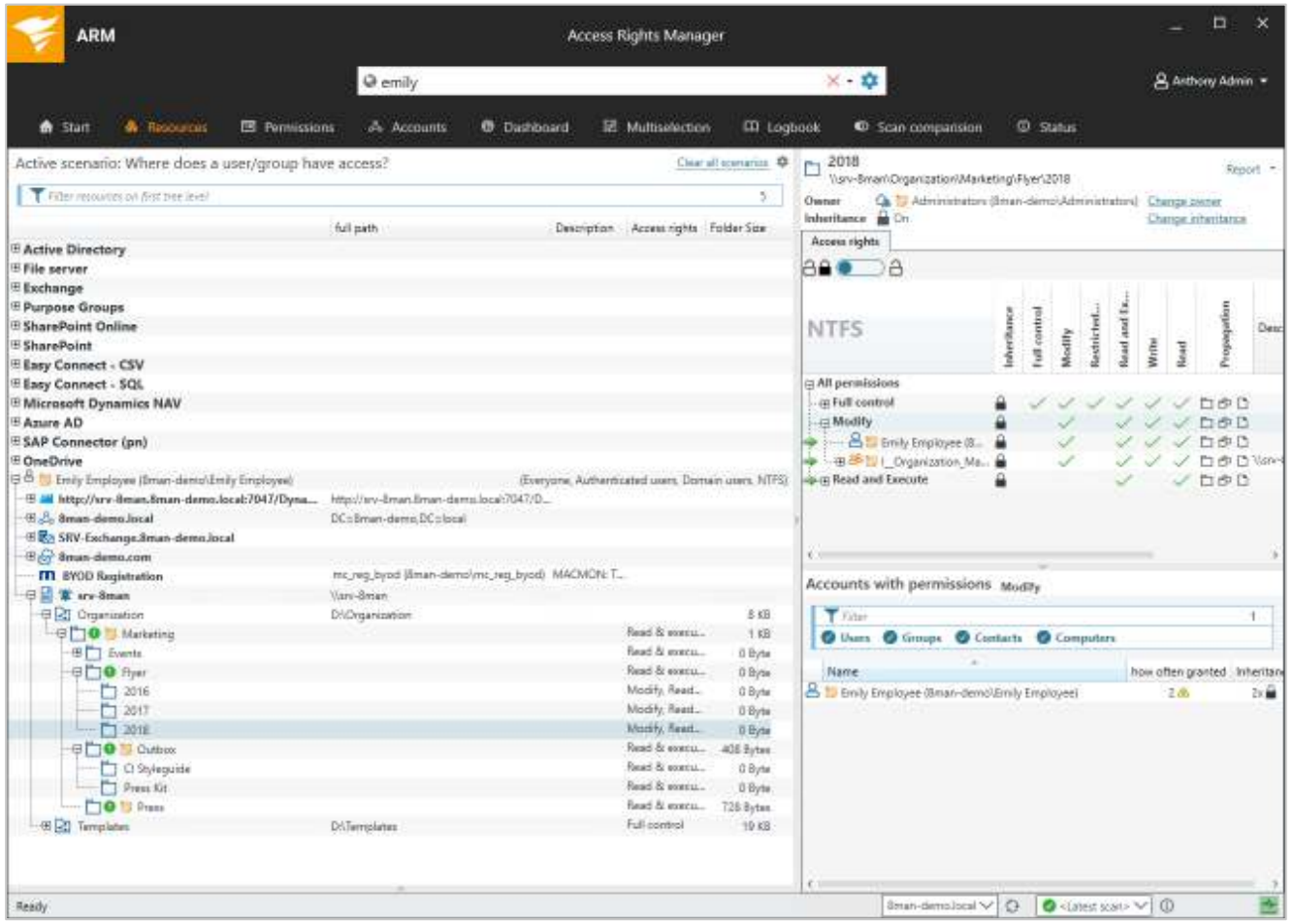
- ✓ ARM Audit Edition
- ✓ ARM

Access Rights Manager

Analyse von Benutzerberechtigungen

Verschaffen Sie sich einen Überblick über Gruppenmitgliedschaften in Active Directory und Zugriffsrechte für Fileserver.

Tragen Sie zum Schutz vor internen Sicherheitsbedrohungen bei: Nutzen Sie die Einblicke in Gruppenmitgliedschaften in Active Directory und Fileservern, um den Benutzerzugriff auf Dienste und Fileserver zu analysieren.



Verfügbar in:

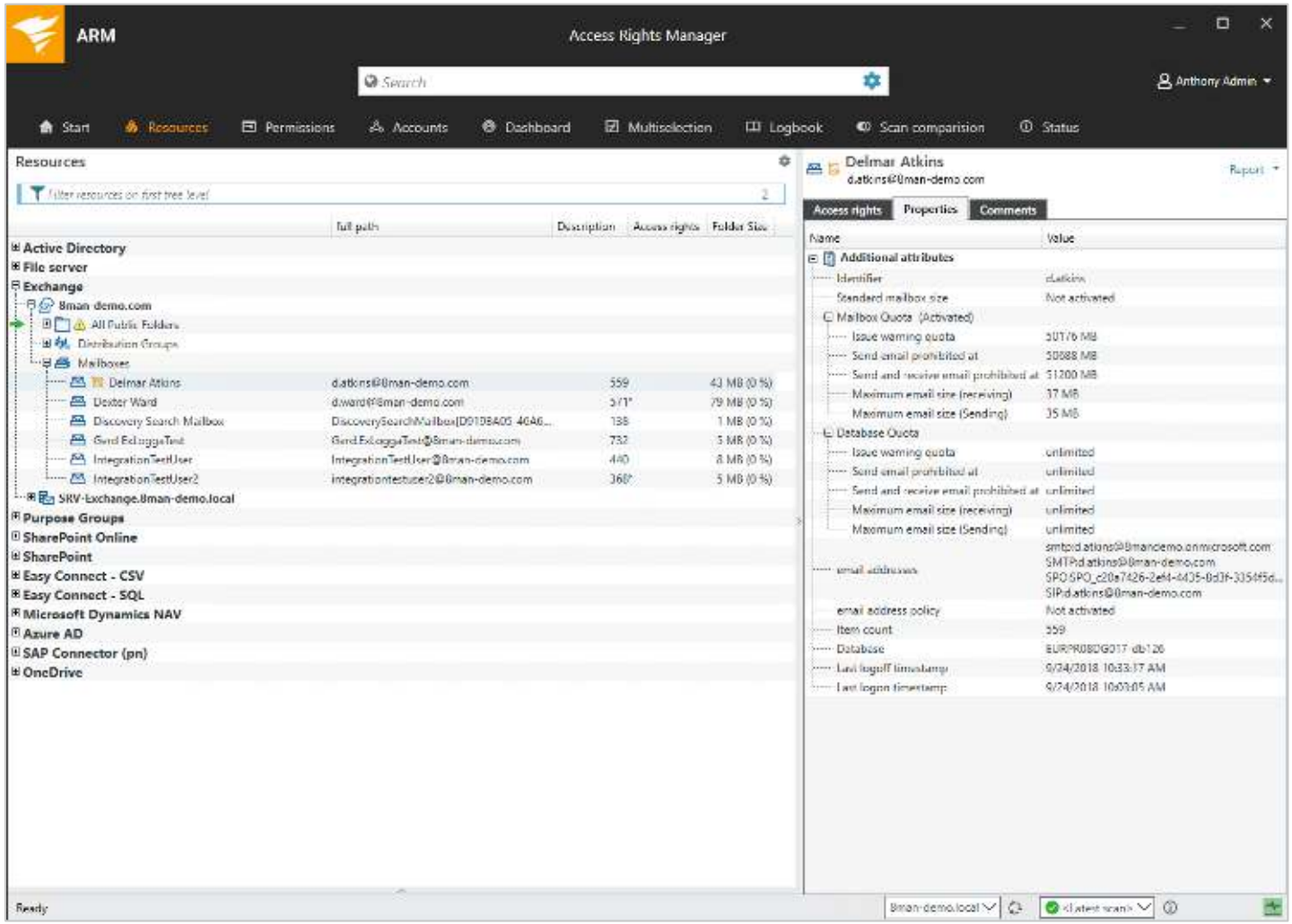
- ✓ ARM Audit Edition
- ✓ ARM

Access Rights Manager

Überwachung von Microsoft Exchange

Analysieren und verwalten Sie Exchange-Zugriffsrechte.

Vereinfachen Sie die Exchange-Überwachung und Prüfungen, um Datensicherheitsverletzungen zu verhindern. Überwachen Sie Änderungen an Postfächern, Postfachordnern, Kalendern und öffentlichen Ordnern. Verbessern Sie die Compliance und erkennen Sie nicht autorisierte Exchange-Änderungen.



Verfügbar in:

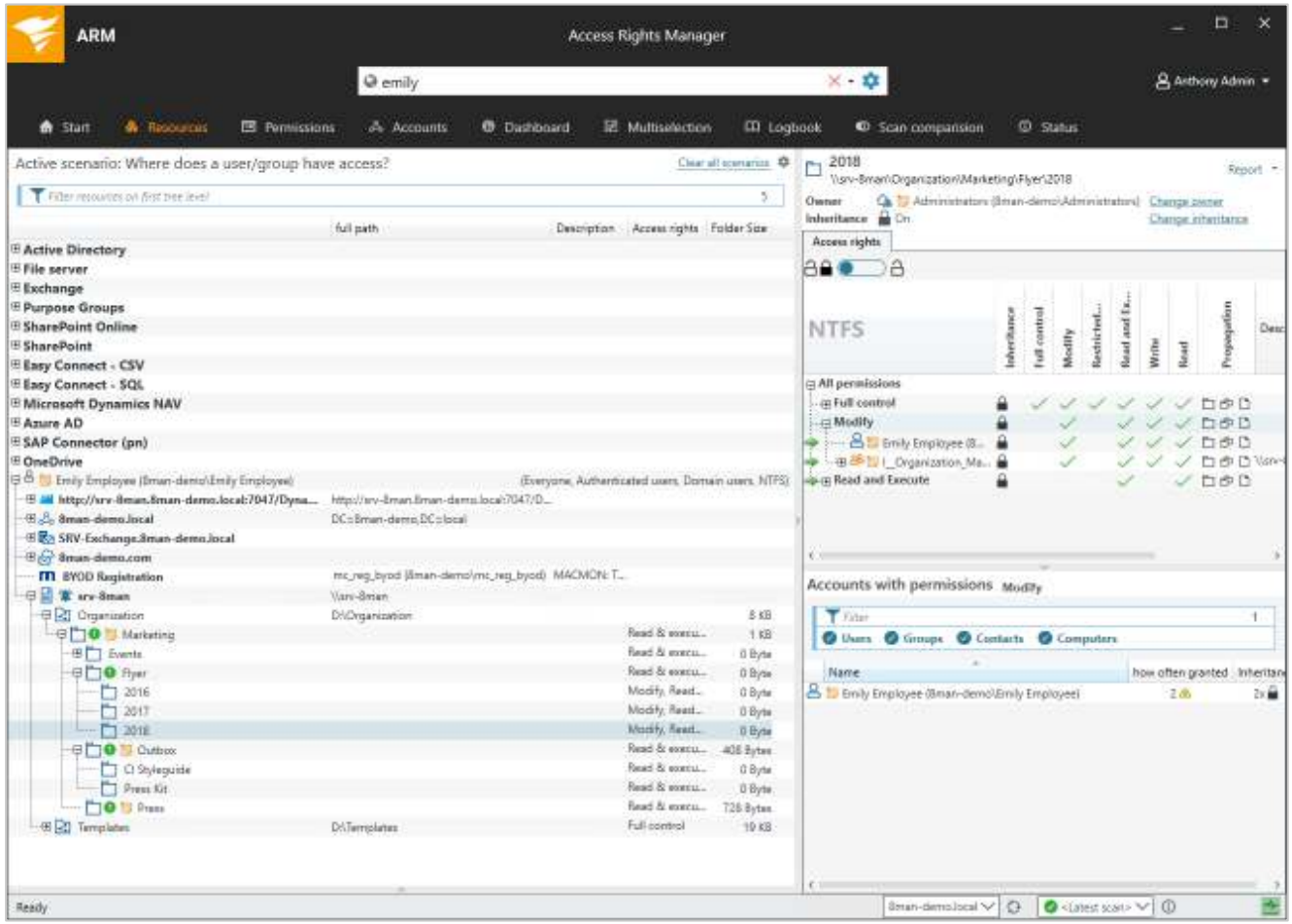
- ✓ ARM Audit Edition
- ✓ ARM

Access Rights Manager

SharePoint-Zugriffsüberwachung

Zeigen Sie Zugriffsrechte für SharePoint als Baumdiagramm an und erkennen Sie schnell, wer für eine bestimmte SharePoint-Ressource zugriffsberechtigt ist.

Mithilfe des Scan-Vergleichsberichts können Sie ermitteln, wer welche Änderungen an Berechtigungen vorgenommen hat.



Verfügbar in:

- ✓ ARM Audit Edition
- ✓ ARM

Access Rights Manager

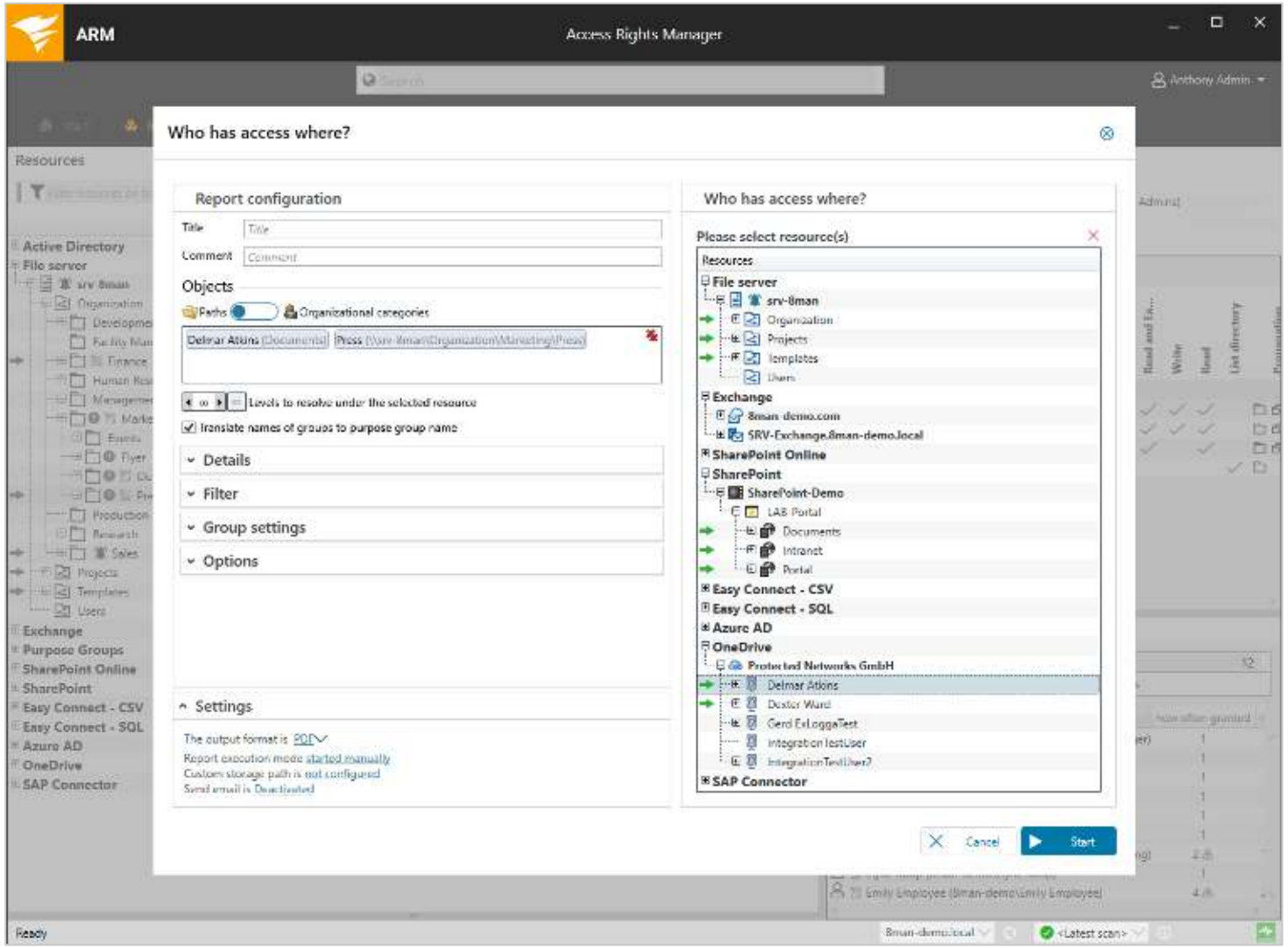
Erstellung benutzerdefinierter Berichte

Halten Sie die Anforderungen von Prüfern und gesetzlichen Vorschriften ein.

Erstellen Sie mit wenigen Mausklicks für Prüfer oder das Management Compliance-Berichte zu den Zugriffsrechten der Benutzer. Protokollieren Sie Aktivitäten in Active Directory und Fileservern je nach Benutzer.

Verfügbar in:

- ✓ ARM Audit Edition
- ✓ ARM



Access Rights Manager

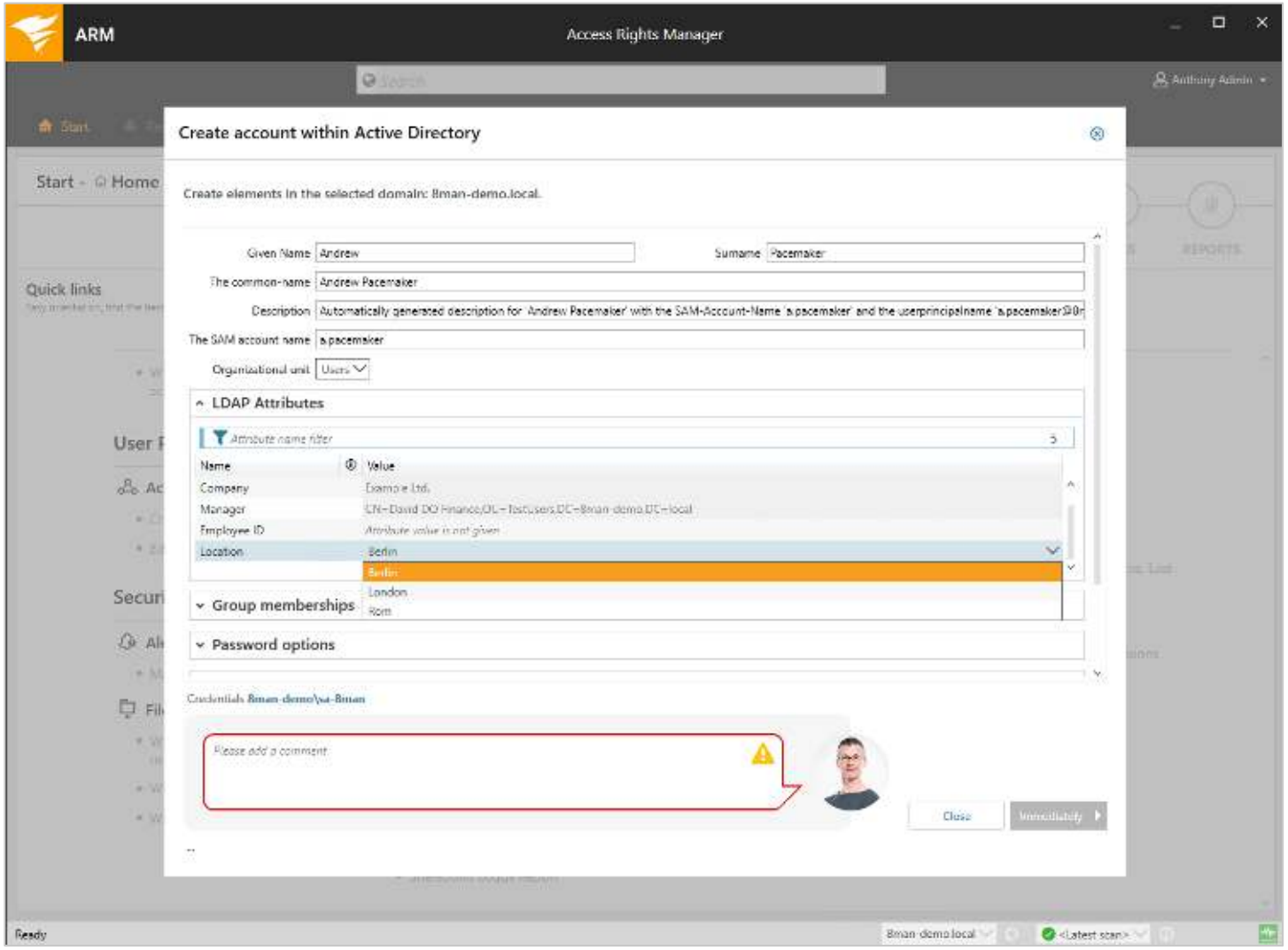
Bereitstellung und Verwaltung von Benutzerrechten

Erstellen, bearbeiten, aktivieren, deaktivieren oder löschen Sie den Benutzerzugriff auf Dienste und Dateien.

Mit standardisierten rollenspezifischen Vorlagen, die Zugriff auf Fileserver und Exchange bieten, können Sie normalerweise in Sekundenschnelle neue Benutzerkonten einrichten und verwalten.

Verfügbar in:

✓ ARM



Access Rights Manager

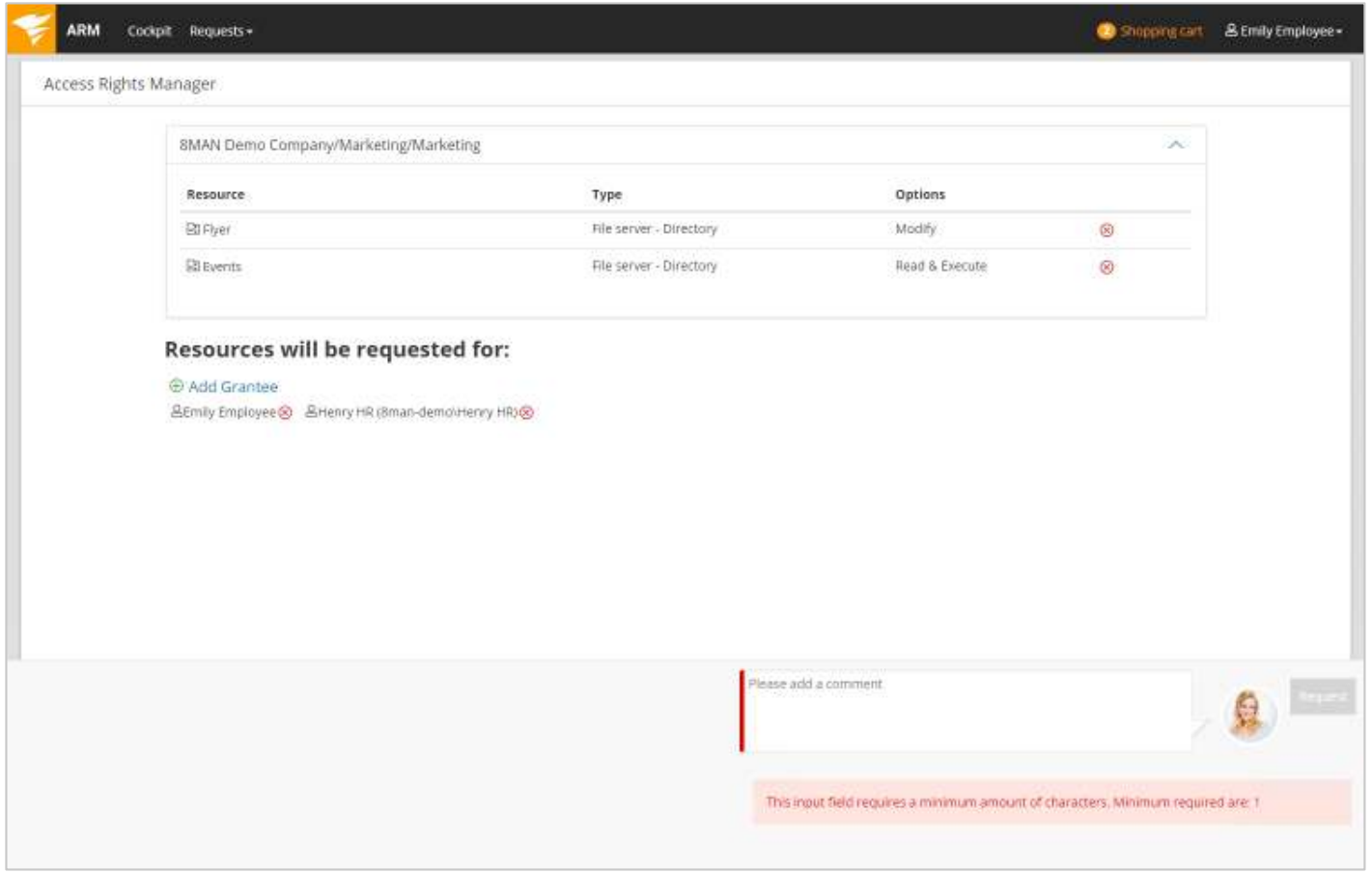
Self-Service-Portal für Berechtigungen

Fordern Sie Zugriffsrechte direkt vom Dateneigentümer an.

Legen Sie die Verantwortung für Zugriffsrechte auf Daten mit einem webgestützten Self-Service-Portal direkt in die Hand des Dateneigentümers anstatt des Administrators.

Verfügbar in:

- ✓ ARM



FAQ

Wie wird SolarWinds Access Rights Manager lizenziert?

Unkomplizierte Lizenzierung

Access Rights Manager wird entsprechend der Anzahl der aktiven Benutzerkonten in Active Directory lizenziert. Hierzu zählen Benutzer- und Dienst-/Systemkonten.

Ist die Zahl der Benutzer beschränkt, die ich mit Access Rights Manager überwachen kann?

Skalierbare Benutzerüberwachung

Access Rights Manager kann zur Überwachung kleinerer und sehr großer Umgebungen eingesetzt werden. In größeren Umgebungen sollte zunächst ein Testbetrieb durchgeführt werden.

Wie wird Access Rights Manager bereitgestellt?

Einfache und unkomplizierte Bereitstellung

Access Rights Manager wird auf einem Windows Server® Ihrer Wahl bereitgestellt und ist in der Regel innerhalb weniger Minuten einsatzbereit.

„Diese Lösung bietet uns bei der Servicequalität und der Sicherheit einen großen Mehrwert ... Nebenbei reduziert sie außerdem unseren Arbeitsaufwand: Mit Access Rights Manager brauchen wir etwa 30 Minuten weniger, um eine Autorisierung zu gewähren ... Wir sind durchweg überzeugt davon, die richtige Entscheidung getroffen zu haben."

Bjorn Pursche
Teamleiter
MPC IT User Service

„Heute habe ich mit Access Rights Manager die fehlerhafte Gruppen-Autorisierung aus dem gestrigen Beispiel entfernt. Im Vergleich dazu, wie lange das mit Standard-Tools des Betriebssystems gedauert hätte, war das eine wahre Offenbarung."

Rolf Eustergerling
Administrator
Benteler AG

Systemanforderungen

Hauptserver-Anforderungen

Server-Anforderungen (je nach Nutzung):

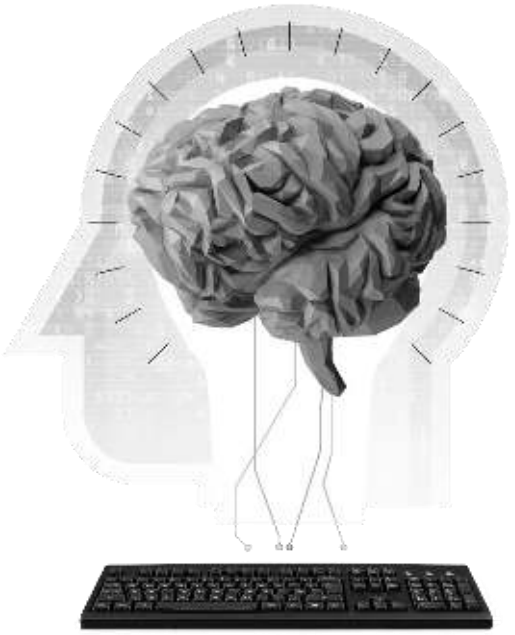
- **Bis zu 1.000 Benutzer**
  - 30 GB Festplatte
  - 4 GB Arbeitsspeicher
- **1.001 bis 4.000 Benutzer**
  - 40 GB Festplatte
  - 8 GB Arbeitsspeicher
- **Mehr als 4.000 Benutzer**
  - 40 GB Festplatte
  - 16 GB Arbeitsspeicher
- **CPU:** Dual-Core-Prozessor oder besser
- **Betriebssystem:** Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 und 2019.
- **Datenbanken:** SQL Server® 2008 SP1, 2012, 2014, 2016 (32 Bit und 64 Bit) und 2017.
- **.NET Framework:** .NET 3.5 SP1 oder .NET 4.5.2 (oder höher) ist erforderlich.

Erfassungsmodul-Anforderungen

- **Festplatte:** 5 GB
- **CPU:** Dual-Core-Prozessor oder besser
- **Arbeitsspeicher:** 4 GB
- **Betriebssystem:** Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016 und 2019.
- **.NET Framework:** .NET 3.5 SP1 oder .NET 4.5.2 (oder höher) ist erforderlich.

WEITER ZUM GRATIS-DOWNLOAD

F&A



DEMO

UMFRAGE

VIELEN DANK!