

# Identity Manager – Data Governance Edition

Daten-Governance-Lösung für volle Kontrolle über den Zugriff auf Ihre vertraulichen Daten

## Vorteile

- Ermittlung und Zuweisung der Eigentümer unstrukturierter Daten
- Einheitlicher Überblick über zuvor fehlende Informationen zur Datennutzung
- Reduzierte Gefahr von Sicherheitsverletzungen durch die Möglichkeit für Dateneigentümer, den Zugriff auf vertrauliche Daten auf bestimmte Benutzer zu beschränken
- Verbesserte Effizienz dank geringerer Belastung der IT durch Zugriffsanfragen
- Beweis der Compliance gegenüber Revisoren durch Benutzerzugriffs- und Nachweisberichte

## Systemanforderungen

Eine vollständige Liste der Systemanforderungen finden Sie unter [oneidentity.com/products/identity-manager-data-governance/](https://oneidentity.com/products/identity-manager-data-governance/)

Zahlreiche Unternehmen sind heute durch unzureichende Datensicherung gefährdet. Sicherheits- und Compliance-Beauftragte haben zunehmend Schwierigkeiten, vertrauliche Daten zu schützen, da kein geeignetes Zugriffssystem installiert ist. Dadurch kommt die Compliance zu kurz, was die Sicherheit der Unternehmen gefährdet.

Auch wenn IT-Manager berechtigt sind, Zugriff auf bestimmte Daten zu gewähren, sind sie sich häufig der Auswirkungen nicht bewusst. So können durch nicht autorisierte Zugriffe von Personen im Unternehmen weitere Konten externen Bedrohungen ausgesetzt werden. Zusätzliche interne Kontrollen sorgen dafür, dass der Zugang zu unstrukturierten Daten auf die betreffenden Personen beschränkt bleibt, sodass die Sicherheit gewahrt wird und Bestimmungen eingehalten werden. Identity Manager – Data Governance Edition, Teil der One Identity Lösungen, schützt Ihre Organisation, indem die Zugriffssteuerung den Geschäftsinhabern übertragen wird, die wissen, wer Zugriff auf welche vertraulichen Daten benötigt. Dafür stehen ihnen Funktionen zur Analyse, Genehmigung und Erfüllung von Zugriffsanfragen für unstrukturierte Daten in Dateien, Ordnern und Freigaben in NTFS, auf NAS-Geräten und in SharePoint zur Verfügung.

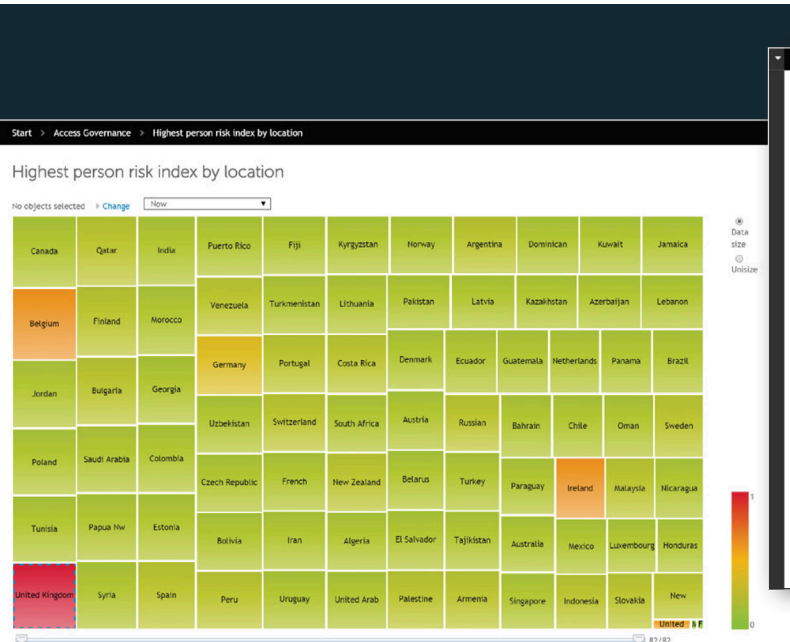


Abbildung 1. Heatmap: Heatmaps zeigen einen Risikoindex und Richtlinienverletzungen der aktuellen Daten sowie einen historischen Vergleich mit vorherigen Daten.

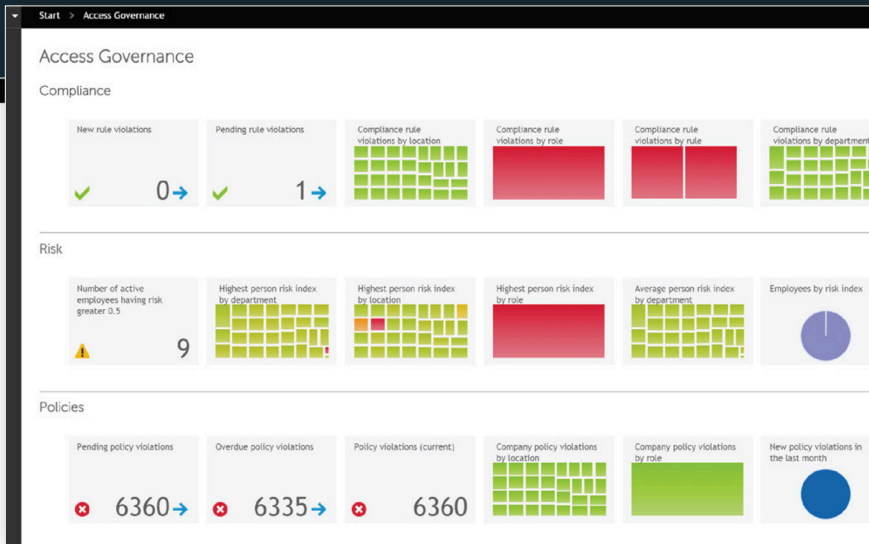


Abbildung 2. Verwaltete Daten: Der Dateneigentümer genehmigt Zugriffsanfragen, erstellt Berichte, überwacht und verwaltet den Lebenszyklus für verwaltete Daten.

Identity Manager – Data Governance Edition hilft Dateneigentümern (nicht der IT) bei der Bestimmung der Zugriffsberechtigten und automatisiert den Anfrage-Genehmigungs-Workflow. So wird Ihr Unternehmen vor Sicherheitsverletzungen bewahrt und gleichzeitig die IT entlastet.

**Funktionen und Merkmale**

**Cloud-Governance**  
Die Lösung unterstützt Microsoft SharePoint Online sowie OneDrive und ermöglicht so Cloud-Governance. Außerdem bietet sie Reporting-Funktionen zur Erstellung von Zugriffsberichten.

**Klassifizierung von Daten**  
Klassifizieren Sie verwaltete Daten manuell. Die Klassifizierungseinstellungen kann der Geschäftsinhaber im Webportal festlegen. Die Lösung bringt vordefinierte Richtlinien mit und berechnet Risikoniveaus auf Basis der zugewiesenen Klassifizierungsstufe.

**Beschränkter Zugriff**  
Definieren Sie Zugriffsrichtlinien für Ihre Organisation, um sicherzustellen, dass nur autorisierte Benutzer auf vertrauliche unstrukturierte Daten zugreifen können. Identity Manager –

Data Governance Edition sperrt vertrauliche Daten, wie Dateien, Ordner und Freigaben in NTFS, auf NAS-Geräten und in SharePoint.

**Zuweisung von Dateneigentümern**  
Bestimmen Sie durch Auswertung von Nutzungsmustern und Lese-/Schreibzugriffen den geeigneten Dateneigentümer und weisen Sie ihn für alle zukünftigen Zugriffsanfragen zu.

**Vereinfachte Überwachung**  
Erkennen Sie Benutzerzugriffe auf Unternehmensressourcen wie Dateien, Ordner und Freigaben auf NAS-Geräten sowie in NTFS und SharePoint. Dies bietet Ihnen Schlüsselinformationen zur Vorbereitung auf Audits.

**Automatisierte Zugriffsanfragen**  
Verwenden Sie integrierte Workflows zur automatischen Umleitung von Zugriffsanfragen vom Anfrageportal zum betreffenden Dateneigentümer. Genehmigte Anfragen werden automatisch korrekt erfüllt, ohne die IT zu belasten.

**Zugriffsüberprüfung**  
Stellen Sie sicher, dass nur autorisierte Benutzer Zugriff auf bestimmte Ressourcen erhalten. Dies gilt auch für Benutzer, welche

die Organisation bzw. Abteilung verlassen haben oder deren Rollen sich geändert haben. Mit Identity Manager – Data Governance Edition lassen sich Benutzer- und Ressourcenaktivitäten überwachen. Zudem können Sie einen Rezertifizierungsprozess für Dateneigentümer konfigurieren und planen, mit dem der Zugriff durch Mitarbeiter überprüft und nachgewiesen werden kann.

**Personalisiertes Dashboard**  
Zeigen Sie Trends, historische und aktuelle Datenzugriffsaktivitäten sowie den Nachweisstatus auf einem personalisierten Dashboard an. Die Berichte können zum Nachweis der Compliance gegenüber Revisoren verwendet werden.

**Infos über One Identity**

Die One Identity Lösungen für Identitäts- und Zugriffsmanagement bieten Identitäts- und Zugriffsmanagement für den Praxiseinsatz und umfassen geschäftsorientierte, modulare, integrierte und zukunftsfähige Lösungen für Identity Governance, Zugriffsverwaltung und Verwaltung privilegierter Konten.

Weitere Informationen finden Sie unter [OneIdentity.com](http://OneIdentity.com)

