

DATENBLATT

Identity Manager

Weniger Risiko beim Identitäts- und Zugriffsmanagement in Unternehmen

Vorteile

- Steuerung des Zugriffs auf lokale, Cloud- und Hybridressourcen von der Anforderung bis zur Genehmigung für Benutzer und Daten
- Reduzierung des Risikos durch Sicherstellung, dass Benutzer nur den erforderlichen Zugriff haben
- Erfüllung von Audi- und Complianceinitiativen durch Richtlinien zur Bestätigung bzw. Rezertifizierung
- Verlagerung von Zugriffsentscheidungen in die richtigen Hände (Geschäftsebene)
- Aufbau auf vorhandenen Investitionen und vorhandener Infrastruktur mit entsprechender Erweiterung

Überblick

Der Aufbau herkömmlicher IAM-Frameworks (Identity and Access Management; Identitäts- und Zugriffsverwaltung) ist kostspielig und ihre Implementierung und Wartung sind zeitaufwendig. Da die IT-Abteilungen in der Regel für das Lifecycle-Management von Benutzeridentitäten zuständig sind, sehen sich diese unter Druck gesetzt. Um auf die unterschiedlichen IAM-Anforderungen der einzelnen Geschäftseinheiten eingehen zu können, arbeiten IT-Abteilungen häufig mit isolierten, spezifischen Tools und Sicherheitsrichtlinien und verlassen sich bei der Durchsetzung auf manuelle Prozesse. Die Umgebung ist dadurch leicht angreifbar, die Risiken steigen und das Einhalten von SLAs gestaltet sich als schwierig.

Sie können die Produktivität steigern, indem Sie Benutzern nur den für ihre Arbeit benötigten Zugriff auf Daten und Anwendungen gewähren.

Mindern Sie Risiken, sichern Sie Daten, erfüllen Sie Verfügbarkeitsanforderungen und sorgen Sie für Compliance, indem Sie Benutzern den Zugriff auf Daten und Anwendungen bereitstellen, die sie benötigen. Das Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) basiert nun auf den Geschäftsanforderungen anstatt auf den Kapazitäten der IT. Mit Identity Manager können Sie Sicherheitsrichtlinien vereinheitlichen und Governance-Anforderungen erfüllen – heute und auch in der Zukunft.

Sie sorgen gleichzeitig für die Verbesserung der Unternehmensflexibilität für heutige und zukünftige Anforderungen – mit einer modularen und skalierbaren IAM-Lösung.

**MINDERN SIE RISIKEN.
STEUERN SIE DEN
ZUGRIFF.
IMPLEMENTIEREN
SIE IDENTITY
GOVERNANCE.
SICHERN SIE DATEN.**

Jetzt basiert das Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) endlich auf den Geschäftsanforderungen.

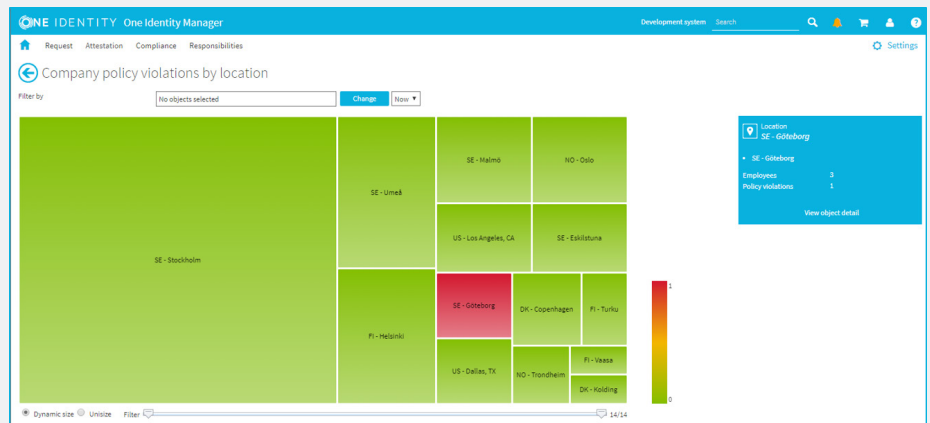


Abbildung 1. Governance-Heatmap ermöglicht schnelle Drilldowns für Richtlinienverstöße

Funktionen und Merkmale

SAP-zertifiziert

Stellen Sie zertifizierte und umfassende SAP-Integrationen mit differenzierten Funktionen bereit, um vorhandene SAP-Sicherheitsmodelle zu erweitern und sogar zu verbessern.

Risikoreduzierung

Treffen Sie bessere Sicherheitsentscheidungen, indem Sie Sicherheitsinformationen und -richtlinien aus mehreren Quellen kombinieren, um Risiken und Informationssilos zu reduzieren.

Cloud

Mit dieser Lösung können Sie Ihre Investition in Identity Governance nicht nur für lokale, sondern auch für hybride und SaaS-Anwendungen nutzen – mit einem Cloud-basierten, verwalteten Add-on-Service.

Umfassende Governance

Stellen Sie Auditoren detaillierte Governance-Berichte in Echtzeit zur Verfügung, die beschreiben, welche Ressourcen sich in Ihrer Umgebung befinden, wer zu welchem Zeitpunkt Zugriff auf sie hat und warum dieser Zugriff gewährt und beendet wurde.

Korrekte Bereitstellung

Vermeiden Sie manuelle Fehler durch die Automatisierung der Bereitstellung auf jedem beliebigen System, jeder beliebigen Plattform und jeder beliebigen Anwendung – lokal oder in der Cloud. Erweitern Sie die Bereitstellung auf Unternehmensanwendungen wie Exchange Online, SharePoint und Oracle E-Business Suite.

Richtige Zugriffsbereitstellung

Erhöhen Sie die Sicherheit, indem Sie Mitarbeitern, Subunternehmern, Partnern, Kunden, Studenten, Absolventen, Auftraggebern und Patienten nur die unbedingt benötigten Zugriffsrechte gewähren – nicht mehr und nicht weniger.

Compliance

Externe Vorschriften? Kein Problem. Interne Richtlinien? Kein Problem. Sorgen Sie für die vollständige Transparenz, die Sie benötigen, und erfüllen Sie gleichzeitig die Anforderungen aller anderen Gruppen.

Systemanforderungen

Eine vollständige Liste der Systemanforderungen finden Sie unter <https://support.oneidentity.com/identity-manager/8.1>.

Daten-Governance

Kontrolle und Transparenz für Ihre Daten.

Self-Service-Zugangsportal

Ermöglicht Unternehmen, Zeit zu sparen und Probleme selbst zu lösen. Über den intuitiven "Online-Warenkorb", der individuell angepasst werden kann, verringern Sie den IT-Aufwand. Dadurch haben Benutzer die Möglichkeit, Zugriff auf Sicherheitsassets wie physische Assets, Gruppen und Verteilerlisten anzufordern sowie Zugriffsrechte und Berechtigungen für ihren gesamten Identitäts-Lebenszyklus zu kontrollieren. Gleichzeitig können sie vordefinierte Genehmigungsprozesse und Workflows nutzen.

Steuerung des privilegierten Zugriffs

Einheitliche Governance, wobei Benutzer privilegierten und allgemeinen Benutzerzugriff in der gleichen Konsole anfordern, bereitstellen und bestätigen können.

Dashboard zur Bestätigungsprüfung

Mit dieser Funktion können Sie die On-Demand- oder Routine-Bestätigung planen und den Status von Gruppen- oder Verteilerlisten in einer klaren, einheitlichen Dashboard-Übersicht anzeigen. Zudem sind Sie in der Lage, detaillierte Berichte für die Erkennung zu generieren und für Compliance zu sorgen.

Zurücksetzen von Kennwörtern

Setzen Sie Kennwörter von Benutzerkonten zurück und legen Sie Benutzerrichtlinieneinstellungen so fest, dass sie den Kennwortregeln und -anforderungen des Unternehmens entsprechen. Sie können je nach Benutzerrollen mehrere Kennwortrichtlinien festlegen.

Multi-Faktor-Authentifizierung

Mit Identity Manager können Sie Zwei-Faktor-Authentifizierung mit Bereitstellung für alle Unternehmensanwendungen durchsetzen. Diese ist zudem mit One Identity Starling Two-Factor Authentication (2FA) integriert.

Umfassende Skalierungsmöglichkeiten

Bauen Sie auf den Investitionen und der Infrastruktur auf, über die Sie bereits verfügen, und setzen Sie mit Ihrem Wachstum dort an.

Über One Identity

One Identity unterstützt Unternehmen bei der erfolgreichen Umsetzung von Identitäts- und Zugriffsmanagement (IAM). Mit unserem einzigartigen Portfolio an Lösungen für Identity Governance, Zugriffsverwaltung, Verwaltung privilegierter Konten und Identity-as-a-Service-Lösungen können Organisationen ihr volles Potenzial entwickeln, ohne Einschränkung durch Sicherheit, und profitieren dabei vom Schutz vor Bedrohungen. Weitere Informationen finden Sie unter [OneIdentity.com](https://www.oneidentity.com).

© 2019 One Identity LLC. Alle Rechte vorbehalten. One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC in den USA und anderen Ländern. Eine vollständige Liste der Marken von One Identity finden Sie auf unserer Website unter www.oneidentity.com/legal. Alle übrigen Marken, Dienstleistungsmarken, eingetragenen Marken und eingetragenen Dienstleistungsmarken sind Eigentum der jeweiligen Markeninhaber. Datasheet_2019_IdentityMgr_US_RS_DE-WL-39628