

Steigern Sie das Wachstum, indem Sie den Zugriff Dritter auf Unternehmensinformationen in skalierter Form automatisieren

Optimieren Sie Initiativen zur digitalen Transformation, und schützen Sie gleichzeitig das Unternehmen vor der Haupt- Ursache für Datenschutzverletzungen: „Vertrauenswürdige“ Dritte



Inhalt

Zusammenfassung	3
Zugriff durch Dritte: Einführung	4
Identity and Access Management definiert	6
Enterprise IAM vs. Erweitertes Enterprise-IAM	7
Welche Innovationen können die Sicherheit und Agilität Ihrer Wertschöpfungskette erhöhen?	8
Fazit	14

Zusammenfassung

Digitale Initiativen beschleunigen sich in Rekordgeschwindigkeit. Traditionelle Wertschöpfungsketten versuchen, ihre externen Geschäftsnetzwerke in hochgradig vernetzte digitale Ökosysteme umzuwandeln, die in der Lage sind, Wachstum, Effizienz, Wettbewerbsfähigkeit und andere Geschäftsergebnisse zu skalieren und gleichzeitig die operativen Investitionen zu senken. So reduzieren Lebensversicherungsunternehmen beispielsweise den Zeit- und Kostenaufwand für die Kontaktaufnahme mit potenziellen Kunden, indem sie über ein verteiltes Ökosystem von externen Vertretern, Maklern, Beratern, Marketingorganisationen, Versicherungsträger und anderen verkaufen. Digitale Produkt- und Serviceprovider bieten Kunden und Abonnenten einen neuen Wert, indem Partnerservices nahtlos in Kernangebote integriert werden.

Bei diesen und ähnlichen digitalen B2B-Strategien hängt der Erfolg von der Fähigkeit ab, Partner, Lieferanten, Kunden und andere Drittorganisationen sicher und vorhersehbar mit Unternehmenssystemen und -ressourcen zu verbinden.

Leider sind die meisten Tools, die den Benutzerzugriff auf Unternehmenssysteme sichern und erzwingen, für interne Mitarbeiter und nicht für Dritte bestimmt. Wenn solche Lösungen komplexen, unternehmensübergreifenden Anwendungsfällen untergeordnet sind, kommt es schnell zu Verzögerungen, zusätzlichen Kosten und Abstrichen.

In diesem Dokument werden die Komplexität und die Herausforderungen bei der Sicherung des Zugriffs Dritter und die wichtigen Funktionen beschrieben, die erforderlich sind, um diesen Zugriff zu skalieren. Darüber hinaus wird eine Cloud-native Plattform-als-Service-Lösung eingeführt, die den Zugriff auf Unternehmenssysteme über globale Wertschöpfungsketten hinweg sichert, wofür in der Regel nur zwei bis drei VZÄ benötigt werden.



Zugriff durch Dritte: Einführung

Unternehmen stützen sich seit Jahren auf partnerschaftliche Beziehungen mit Dritten, um durch Zusammenarbeit Kosten zu senken. So erzielten beispielsweise die „Big Three“ der nordamerikanischen Automobilhersteller im Jahr 2000 durch die Zusammenarbeit mit ihrer gemeinsamen Lieferantenbasis enorme Effizienzsteigerungen. Die Lieferanten erhielten Zugang zu den Backend-Systemen der Hersteller, um die Procure-to-Pay-Prozesse zu erfüllen, die zuvor intern durchgeführt wurden.

Die Zunahme der Zusammenarbeit zeigt sich vor allem in globalen Wertschöpfungsketten, da die digitale Verknüpfung von Wertschöpfungspartnern mit den Kerngeschäftsprozessen des Unternehmens entscheidend ist, um Effizienz zu erreichen, Kosten zu reduzieren und das Risiko von Unterbrechungen zu verringern. (Siehe Abbildung 1).

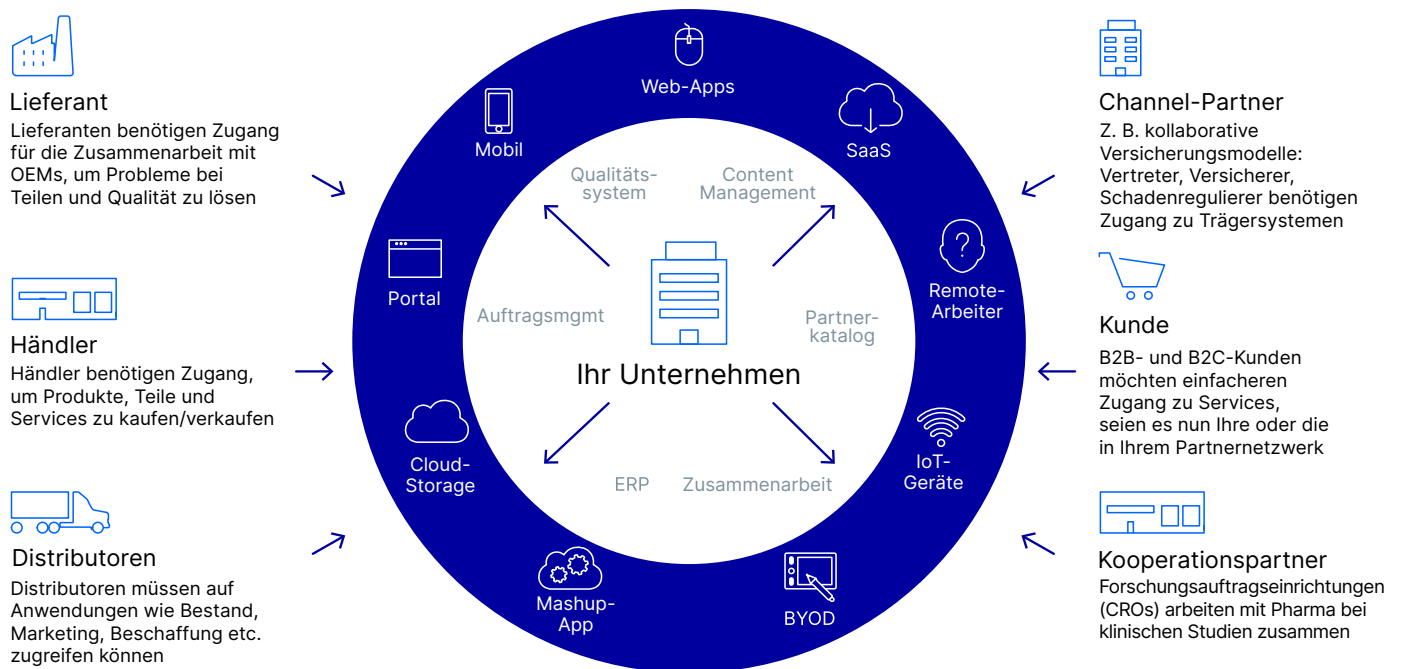


Abbildung 1. Das kollaborative Ökosystem

Mit der Ausweitung der Wertschöpfungsketten müssen digitale Bestände und Informationen, die bisher nur Mitarbeitern zugänglich waren, einer sich ständig verändernden Community von Lieferanten, Partnern, Distributoren, B2B-Kunden und anderen Dritten zur Verfügung gestellt werden. In der Vergangenheit haben Unternehmen Ad-hoc-1:1-Verbindungen eingerichtet, um Handelspartner zu internen Ressourcen weiterzuleiten, und Identitäten und Zugang direkt als Mesh-Netzwerk verwaltet.

Dieser Ansatz führt jedoch schnell zu einer unhaltbaren Situation, da jeder neue Endpunkt eine exponentielle Zunahme der Angriffsfläche darstellt und einen oder mehrere Faktoren einer Unternehmensarchitektur auf die Probe stellt: Skalierbarkeit, Verfügbarkeit, Sicherheit und andere. (Siehe Abbildung 2).

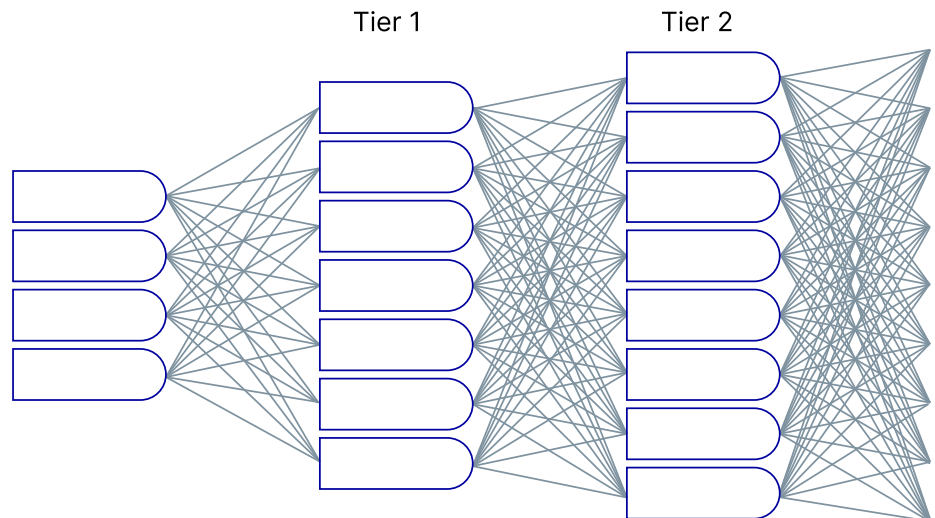


Abbildung 2. Hohe Komplexität mit multi-tiered Partner- und Nutzerbeziehungen

Der aktuelle Stand des Zugriffs durch Dritte ist bei Weitem nicht ideal. Die zunehmende Anzahl von Dritten, die Zugriff auf Backend-Systeme ohne orchestriertes Identity Management oder Governance erhalten haben, hat zu erheblichen Risiken und Kosten geführt.

Chancen bieten sich denjenigen, die in der Lage sind, wirksame Kontrollen zu implementieren, um Risiken zu überwinden und die Möglichkeiten externer Ökosysteme zu nutzen. Die Abhängigkeit von kooperativen Beziehungen mit Dritten wird voraussichtlich noch zunehmen, und zwar in einem deutlich schnelleren Tempo, da die Initiativen zur digitalen Transformation reifen.

- Digitale Ökosysteme werden bis 2030 weltweit \approx 60 Billionen € Umsatz ausmachen¹
- 53 % der Supply Chains werden bis 2026 weiterhin erhebliche Änderungen an ihrer Lieferantenbasis vornehmen²
- Bis 2025 werden die Führungskräfte die Produktentwicklung des Ökosystems nutzen, um die Erwartungen neuer Kunden zu erfüllen³

Ohne wirksame Kontrollen zur Minderung des Risikos durch Dritte erhöhen solche Initiativen jedoch nur das Risiko einer Verletzung.

1 McKinsey, Digital ecosystems for insurers: No one size fits all. (2021)

2 Ernst & Young, Why global industrial supply chains are decoupling. (2022)

3 Gartner, Rebound Quickly From the Current Downturn by Using Collaborative Ecosystem Product Development (2021)

Identity and Access Management definiert

Identity and Access Management (IAM) ist eine Technologie, die die Abstimmung von Benutzerberechtigungen und Zugriff auf die Sicherheits- und Datenschutzrichtlinien eines Unternehmens automatisiert. Die folgende einfache Definition ist ideal für diejenigen außerhalb der Informationssicherheit, lässt sich aber problemlos mit den zugrunde liegenden IAM-Frameworks und -Komponenten verbinden, wie in Abbildung 3 unten dargestellt:

Wer hat Zugang wozu, warum, wer hat ihn genehmigt und wird er noch gebraucht?

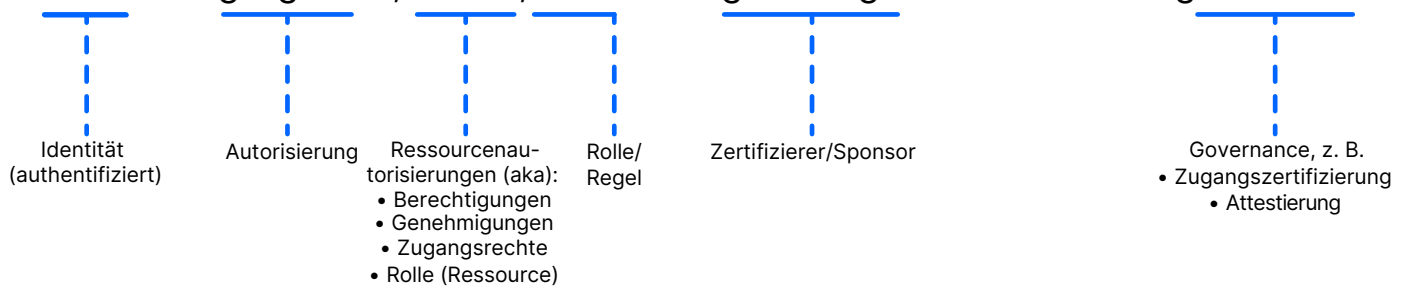


Abbildung 3. IAM definiert

IAM umfasst neben der grundlegendsten Funktion der Verzeichnisdienste, bei der die mit einer Identität verbundenen Metadaten verwaltet werden, zwei Hauptfunktionen:

Authentifizierung: Der Mechanismus zur Ermittlung der Zuverlässigkeit der Anmeldeinformationen eines Benutzers, um effektiv zu bestimmen, ob es sich bei dem Benutzer tatsächlich um ihn selbst handelt, und anschließend die Authentifizierung über Sicherheitsdomänen hinweg über verbundenes Single Sign-on oder andere Mittel zu kommunizieren.

Autorisierung: Der Mechanismus für die Verwaltung von Zugriffsrechten/-berechtigungen für geschützte Ressourcen, typischerweise im Zusammenhang mit der Implementierung einer Kontrollstelle für die Informationssicherheit, dem Anwendungszugriff und der Rollenverwaltung. Autorisierungen werden in der Regel über eine definierte Zugriffsrichtlinie geregelt, die Workflow und Zertifizierung umfasst.



Das Berechtigungsmanagement ist das Herzstück einer IAM-Lösung, da es letztendlich steuert, auf welche Anwendungen jeder Benutzer Zugriff hat, welche Aufgaben innerhalb der Anwendung ausgeführt werden können, wer den Zugriff genehmigen muss und wer diesen Zugriff neu zertifizieren muss, damit er beibehalten oder widerrufen werden kann. IAM-Lösungen automatisieren diese Prozesse, indem sie geplante oder Echtzeit-Ereignisse erkennen und darauf reagieren, z. B. wenn eine Person bei einem Unternehmen eintritt, zu einer neuen Stelle innerhalb des Unternehmens wechselt oder das Unternehmen verlässt. Der End-to-End-Prozess zur Verwaltung von Identitäten und Zugriff für neue Mitarbeiter, wechselnde Mitarbeiter und ausscheidende Mitarbeiter wird als Identitätslebensdauer-Verwaltung bezeichnet. In Abbildung 4 unten sind die drei Phasen des Identitätslebenszyklus dargestellt und Beispielergebnisse dargestellt, die standardmäßig IAM-Prozesse auslösen.

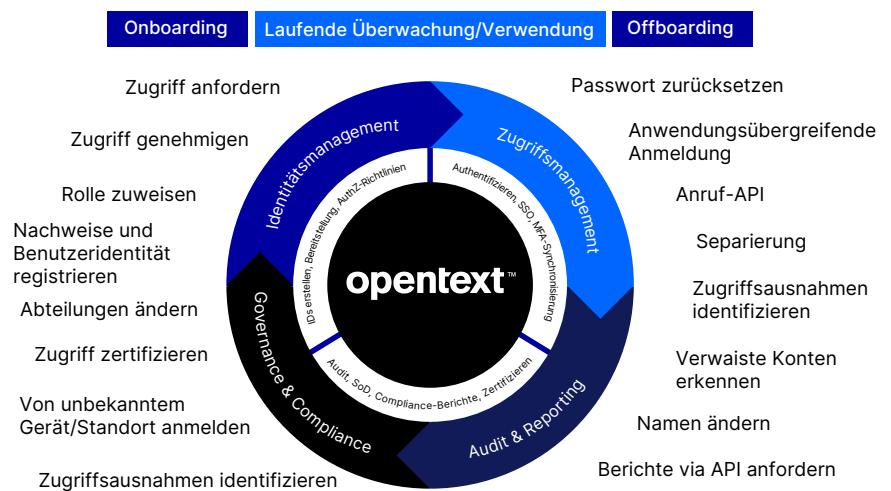


Abbildung 4. Identitätslebenszyklus-Verwaltung

Enterprise IAM vs. Erweitertes Enterprise-IAM

IAM ist zwar eine Sicherheitstechnologie, das ursprüngliche Wertversprechen der frühen 2000er Jahre bestand jedoch darin, die Kosten für die Verwaltung des Mitarbeiterzugriffs zu senken – Sicherheit war eher ein „Vorteil“. Bei der Einführung von Vorschriften zur Betrugsbekämpfung und Unternehmensverantwortung (z. B. Sarbanes Oxley, Graham Leach Bliley usw.) war „Enterprise IAM“ ein natürlicher Ansatz, da es einen Rahmen für Kontrollen bot, um das Risiko rechtswidriger oder unangemessener Handlungen von Mitarbeitern zu mindern. Beispielsweise ermöglichte die Durchsetzung der Aufgabentrennung Unternehmen, toxische Kombinationen von Autorisierungen zu untersagen, die Betrug ermöglichen, z. B. einen Mitarbeiter, der zur Erstellung eines Lieferanten, zur Ausstellung einer Bestellung und zur Bezahlung von Rechnungen berechtigt ist.

Enterprise-IAM ist seitdem gewachsen, um mehr Lebenszyklusereignisse zu automatisieren, mehr Systeme zu unterstützen und als Cloud-Service (IDaaS) bereitgestellt zu werden. Der primäre Use Case bleibt jedoch für die meisten Anbieter gleich: Der Zugriff der Mitarbeiter (Belegschaft) auf On-Premise- und Cloud-Ressourcen wird gesichert.

Erweiterte Enterprise-IAM hingegen konzentriert sich auf die viel größere Anzahl externer Nutzer – Lieferanten, Partner, Anbieter, B2B-Kunden, Agenten, Auftragnehmer und andere Benutzer AUSSERHALB des Unternehmens, die Zugriff auf Ressourcen INNERHALB des Unternehmens benötigen.



Beide IAM-Varianten dienen der sicheren Verwaltung von Benutzerautorisierungen und -zugriffen, doch dies gilt für sehr unterschiedliche Zielgruppen, Zwecke und Umgebungen. Unternehmen, die ihre Enterprise-IAM-Investitionen zur Verwaltung von Handelspartnern und B2B-Kundenidentitäten nutzen, sehen in der Regel eine sofortige Reduzierung (oder Mangel) in den Bereichen Automatisierung, Sicherheit, Compliance und Standardisierung sowie eine Zunahme manueller Vorgänge. Aber warum? Die Enterprise-IAM-Produkte sind so konzipiert, dass sie die internen Unternehmensprozesse, Konventionen und Daten nutzen und wie angekündigt funktionieren. Beispiel: Ein einheitliches und kuratiertes Aufzeichnungssystem für Benutzer und Attribute, eine definierte Unternehmenshierarchie zur Erleichterung von Bereitstellungs- und Sicherheitsentscheidungen, vom Unternehmen ausgegebene Geräte usw. Wenn Enterprise-IAM-Produkte auf B2B-Unternehmen abzielen, sind diese Voraussetzungen nicht mehr verfügbar oder unzureichend, um Vertrauen aufzubauen, den Zugriff bereitzustellen oder den externen Zugang auf automatisierte, skalierbare Weise zu sichern.

B2B-IAM-Produkte, die eine Investition wert sind, bieten Technologien und Innovationen, die Transparenz bei externen Unternehmen schaffen, um die Verwaltung von Identitätslebenszyklen für alle Personen, Systeme und Dinge innerhalb des Ökosystems zu vereinfachen und zu skalieren: Lieferanten, Kunden, Mitarbeiter, Anwendungen für Bürger, Geräte und Betriebstechnologie.

Erweiterte Enterprise-IAM-Lösungen heben sich von mitarbeiterorientierten Produkten ab, indem sie Technologien und digitale Prozesse umfassen, die:

- Transparenz in Drittanbieter-Organisationen schaffen.
- Den Zugriff über mehrere Sicherheitsdomänen und komplexe Ökosysteme hinweg sichern.
- die Anmeldedaten mithilfe verschiedener Signale validieren, um die Identität zu bestätigen.
- APIs vor Veröffentlichung schützen.
- Eine 360-Grad-Ansicht aller Personen, Systeme oder Dinge erstellen, die auf das Unternehmen zugreifen.
- Das Hinzufügen externer Organisationen ermöglichen, ohne die internen Ressourcen zu erhöhen.
- einen Endpunkt für den gesamten externen Zugriff darstellen.

Welche Innovationen können die Sicherheit und Agilität Ihrer Wertschöpfungskette erhöhen?

Das IAM-Produkt von OpenText, OpenText Core Secure Access bietet innovative Lösungen zur Vereinfachung und Standardisierung der Zugriffsverwaltung in großen Ökosystemen von Dritten. Im Folgenden finden Sie einige Innovationen von OpenText Core Secure Access, die die Führungsposition des Unternehmens in diesem Bereich demonstrieren.

Entitätsbeziehungsmanagement: einheitliches Datenmodell

Die Sicherung des Zugriffs von Ökosystemen auf Unternehmensinformationen ist mehr als nur die Verwaltung von Benutzern. Unternehmen müssen alle externen Zugriffe auf das Unternehmen, einschließlich Menschen, aber auch Systeme, Sensoren, Fahrzeuge und andere nicht-kohlenstoffintensive Einheiten, inventarisieren, prüfen und zertifizieren.

OpenText Core Secure Access verfügt über ein einheitliches Datenmodell, das einen einheitlichen Ansatz zur Sicherung des Zugriffs für alle Personen, Systeme und Dinge schafft. Jede dieser Entitäten erhält eine eindeutige digitale Identität, die alle bekannten Konten, Autorisierungen, Beziehungen, Profildaten und anderen Informationen widerspiegelt. Das einheitliche Datenmodell ist eine kanonische Darstellung von Identitätsinformationen für jeden Entitätstyp. Es beschreibt die Beziehung der Entität zu anderen Entitäten (Knoten), die explizit oder abgeleitet sein können. Diese Beziehungsknoten werden dann für die Authentifizierung und Autorisierung verwendet und bieten eine hochgradig skalierbare und sichere Methode zur Zugriffskontrolle in großen Ökosystemen (siehe Abbildung 5).

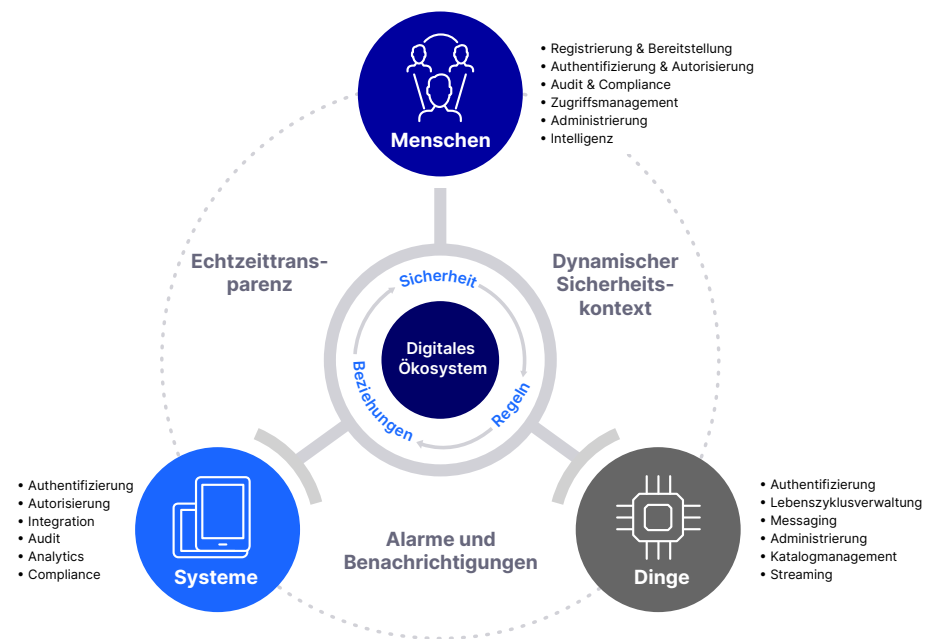


Abbildung 5: Modell der Entitätsbeziehungsverwaltung

Das „erweiterte“ Unternehmensverzeichnis

Unternehmensverzeichnisse pflegen und verwalten Informationen, die letztendlich die Zugriffsberechtigungen für jeden Benutzer festlegen und so eine „einzige Version der Wahrheit“ für Mitarbeiter- und Personalbenutzer schaffen. Die Einrichtung des gleichen Konstrukts für erweiterte Unternehmensbenutzer ist ebenso wichtig, aber wesentlich komplexer.

Externe Benutzeridentitäten werden in der Regel in jedem System erstellt, auf das ein Benutzer zugreifen darf (z. B. ERP, Qualität, CRM), und werden vom Eigentümer des Systems oder dem unterstützten Geschäftsprozess verwaltet. Dies führt zu Silos von Identitätsdaten, die die Sicherheit beeinträchtigen und die betrieblichen Vorgänge untergraben. Beispielsweise werden der Wert und der Schutz durch risikobasierte Authentifizierungstools reduziert, wobei nur ein Teil der Informationen zur Bestimmung des Risikos und der Faktoren zur Risikominderung zur Verfügung stehen.

Einige Unternehmen entscheiden sich dafür, Daten externer Benutzer im Unternehmensverzeichnis zu speichern. Analysten sind sich einig, dass die Verwaltung von Identitäten Dritter im Unternehmensverzeichnis aufgrund des inhärenten Risikos bei der Vermischung von internen und externen Benutzern die „schlechteste Methode“ sein kann. Dies wird in einem internen Auditbericht aus dem Jahr 2020 zum Zugriff von Dritten auf die Daten- und Informationssysteme des World Food Programmes beschrieben.¹⁰ Insbesondere führte die Konfiguration des Unternehmensverzeichnisses dazu, dass interne und externe Benutzer „denselben Standardzugriff auf Anwendungen, Services und Daten haben, die über AD verfügbar sind, einschließlich der virtuellen privaten Netzwerkverbindungen des WFP-Intranets und einiger gemeinsamer Laufwerke usw.“



OpenText Core Secure Access ist die „einzige wahre Version bezüglich Dritter“, die sich einfach in On-Premise- und Cloud-Systeme integrieren lässt, um sicherzustellen, dass das Benutzerprofil und die Autorisierungsinformationen korrekt, aktuell und in dem richtigen Format über alle Wertschöpfungs-systeme und Geräte hinweg bereitgestellt werden. Messaging und Orchestrierung, Event-Streaming und andere Services auf Integrationsebene vereinfachen die Verbindung und Verwaltung von Identitätsspeichern und beseitigen Silos.

Dieser Best-Practice-Ansatz führt zu einer 360-Grad-Ansicht aller Dritten, um:

- das Vertrauen während der Authentifizierung zu skalieren, indem das tatsächliche Risiko eines Benutzers festgestellt wird.
- Zugriffsentscheidungen zu verbessern.
- die Journeys in den Geschäftsprozessen zu personalisieren.
- um Probleme mit dem Kundenservice schnell und zufriedenstellend zu lösen, wenn Kundenservice-Mitarbeiter alle relevanten Services kennen und disjunkte Erfahrungen eliminieren.
- Strategien für das Risikomanagement Dritter (TPRM) durch die Abstimmung der Zugriffsrichtlinien und -kontrollen von OpenText Core Secure Access mit TPRM zu operationalisieren.
- Die Remote-Nutzung durch Drittanbieter und Mitarbeiter sicher mit Unternehmenssystemen zu verbinden, ohne dass ein VPN erforderlich ist.
- mit granularen Zugriffen in Partner-Ökosystemen zusammenzuarbeiten.

Konzept der Organisationshierarchie

Eine Schlüsselkomponente von Unternehmensprodukten ist das Konzept einer Organisationsstruktur oder -hierarchie. Eine Organisationshierarchie bietet eine effiziente Möglichkeit, die Zugriffsrechte, Administratorrechte und andere Berechtigungen eines Benutzers basierend auf seiner Position innerhalb der Hierarchie zu bestimmen.

OpenText Core Secure Access nutzt dasselbe Konzept, um eine logische Ansicht der Organisationshierarchie eines Dritten darzustellen. Die Plattform ermöglicht es delegierten Administratoren, einen „digitalen Zwilling“ der Teile ihres Unternehmens zu erstellen und zu pflegen, für die ein Zugriff erforderlich ist – ohne die Einbeziehung von Unternehmensadministratoren. Die Organisationshierarchie bietet auch die Möglichkeit, organisatorische Änderungen bei Drittorganisationen zu erkennen: Siehe Hierarchieverwaltung und -synchronisierung, die später erläutert werden.

Verteilte Entscheidungen: Delegierte Verwaltung

Skalierbarkeit ist der einschränkende Faktor bei der Verwaltung von Dritt-Benutzern. Der Zeit-, Kosten- und Risikoaufwand für die Verwaltung von Identitäten und Zugriffen für Tausende von Unternehmen und Millionen von Benutzern kann unerschwinglich sein, wenn eine Mischung aus Unternehmenstools und manuellen Prozessen angewendet wird. Darüber hinaus birgt die fehlende Übersicht über das Kommen und Gehen von Mitarbeitern bei Drittanbietern ein erhebliches Risiko, da sich die Bereitstellungsrücknahme ausgeschiedener Benutzer bis zur nächsten vertraglichen Neuzertifizierung in ein bis zwei Jahren hinauszögern kann.

Die skalierbare Verwaltung von Identity and Access Management erfordert eine verteilte Entscheidungsfindung und die zentrale Durchsetzung von Richtlinien, Überprüfung, Protokollierung, Compliance und Reporting. Dennoch muss die Aufsicht über Aktivitäten mit hohem Risiko behalten werden, wie z. B.:

- Spezifische Anwendungen, die für jede Partnerorganisation verfügbar sind.
- Endgültige Genehmigung der Anwendungen, auf die ein Benutzer zugreifen kann.
- Entfernen des Anwendungszugriffs durch den Benutzer oder den Partner des Kunden.
- Überwachung der Durchführung von Benutzeraudits nach Bedarf.
- Anpassung der Partnerorganisationen an die Unternehmensstruktur.

OpenText Core Secure Access umfasst ein umfassendes, delegiertes Verwaltungsmodell, das Einblicke in Tausende von Drittunternehmen bietet. Dabei werden externe Organisationen beauftragt, ihren eigenen Benutzerzugriff durch autorisierte Unternehmensressourcen zu verwalten. Delegierte Administratoren (z. B. Lieferanten) haben die besten Kenntnisse darüber, „wer Zugriff auf was haben sollte“ und welche Benutzer keinen Zugriff mehr benötigen. Dies bietet Unternehmen eine kontinuierliche Überwachungsfunktion für den Zugriff durch Dritte, die praktisch kostenlos ist.

Das bereitstellende Unternehmen ist die oberste Organisation innerhalb des Bereichs, die die endgültige Kontrolle und Aufsicht über alle Lieferanten, Partner, Kunden und andere Dritte, die Zugriff auf Unternehmenssysteme haben, gewährleistet (siehe Abbildung 6). Die tägliche Benutzerverwaltung, der Helpdesk-Support, Zugriffszertifizierungen und andere Funktionen werden jedoch an Administratoren, Manager, Datenverantwortliche und andere Personen in jeder externen Partnerorganisation delegiert. Es werden mehrere Rollen bereitgestellt, die die Aktivitäten festlegen, die jeder delegierte Administrator ausführen kann.

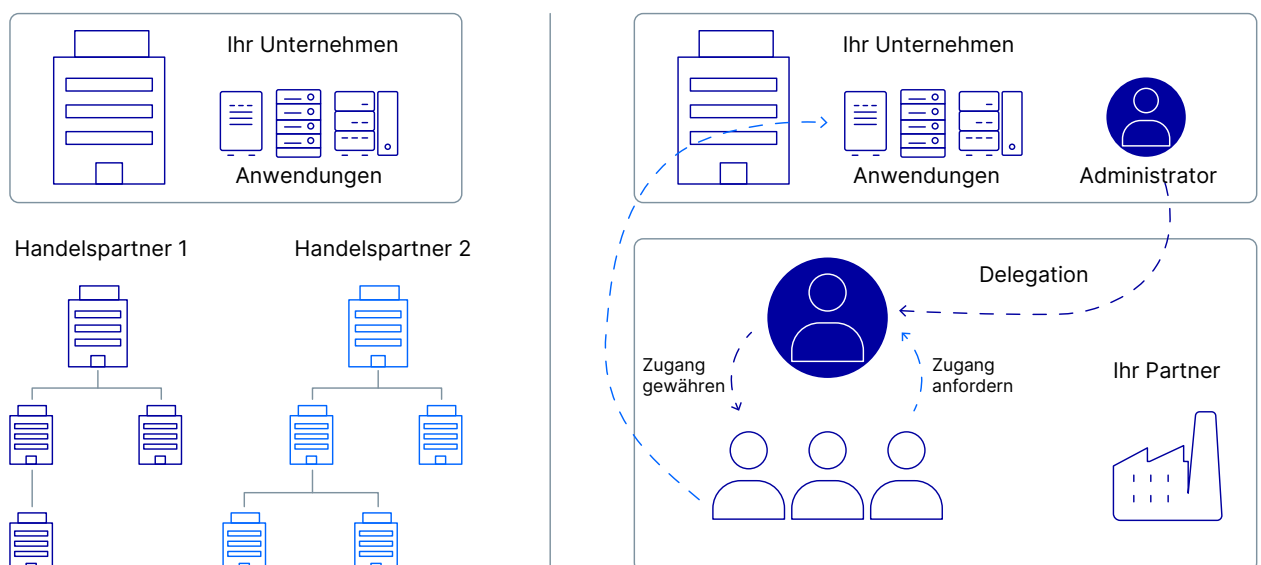


Abbildung 6. Das Modell der delegierte Verwaltung von OpenText Core Secure Access

Das delegierte Verwaltungsmodell etabliert automatisierte, wiederholbare Prozesse zur Verwaltung der Organisationshierarchie, von Benutzerzugriffen und -anforderungen, des Supports, der Governance und anderer Funktionen. Beispiel:

- Neue Benutzer und Administratoren einladen.
- Daten externer Organisationen aktualisieren (z. B. Standort ändern, übergeordnete Einheit ändern).
- Zugriff anfordern.
- Genehmigen von Anforderungen.
- Zuweisen von Verwalterrollen.
- [Neu]Zertifizierung von Rollen und Benutzerberechtigungen.
- Autorisierungen verwalten.
- Profile verwalten.
- Passwort zurücksetzen.

Hinweis: Die delegierte Verwaltung wird in vielen anderen OpenText Core Secure Access und Internet of Things Kontexten verwendet, wie z. B. dem Use Case „verbundenes Fahrzeug“, bei dem der Fahrzeugeigentümer die Erlaubnis eines Zweitfahrers zur Anforderung einer Fahrzeugfunktion entfernen kann.

Erkennen und Aufnehmen von Änderungen: Hierarchieverwaltung und -synchronisierung

Organisationen ändern sich ständig: neue Versandstandorte, Arbeitskämpfe, organisatorische Umstrukturierungen, Verkäufe, Übernahmen, Personalwechsel und ähnliches. Wenn sie nicht erkannt werden, können diese Änderungen zu Betriebsunterbrechungen, Sicherheitsvorfällen und anderen unerwünschten Ergebnissen führen, die durch nicht synchronisierte Partner- oder Lieferantendaten verursacht werden.

OpenText Core Secure Access überwacht automatisch die Lieferantenstammdaten, um Unstimmigkeiten zu erkennen und entsprechende Maßnahmen zu ergreifen. Kunden können die Lösung so einrichten, dass Zugriffsrichtlinien auf der Grundlage der neuen Stammdaten automatisch erneut angewendet und der Zugriff nach Bedarf geändert wird, oder den entsprechenden Mitarbeiter benachrichtigen, der dann bestimmte Workflows anwenden kann, um erforderliche Benutzerbewegungen, Änderungen von Codezuteilungen oder andere autorisierte Vorgänge nach Bedarf durchzuführen (siehe Abbildung 7).

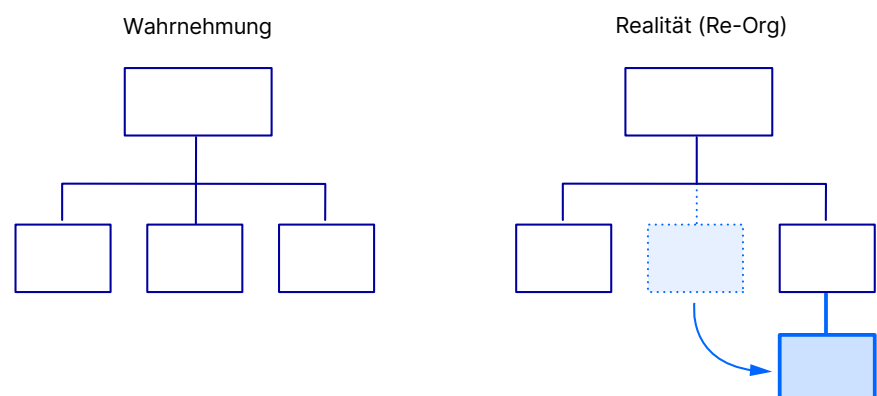


Abbildung 7. Hierarchieverwaltung und Synchronisierung

Diese wichtige Funktion verbessert den Zustand und die Vorhersehbarkeit von Wertschöpfungsketten, indem sie Kunden von OpenText Folgendes ermöglicht:

- Schnelle Reaktion auf organisatorische Veränderungen bei den Partnern in der Wertschöpfungskette
- Skalieren des Identity and Access Management für Tausende von Drittunternehmen und Millionen von Benutzern.
- Vermeiden von Tausenden von Routineaufgaben, um Partner- und Lieferantendaten zu aktualisieren.
- Verwenden der stets aktuellsten Partner- und Lieferanteninformationen.

OpenText Core Secure Access as a Service

OpenText Core Secure Access ist eine speziell entwickelte Plattform-als-Service-Lösung, die eine sichere, effiziente Interaktion und Zusammenarbeit über große Ökosysteme von Dritten ermöglicht – und zwar in großem Umfang (siehe Abbildung 8). Die Plattform besteht aus Cloud-nativen Technologien, integrierten Sicherheits-Frameworks und digitalen Prozessen zur nicht linearen Skalierung des Zugriffs durch Dritte.

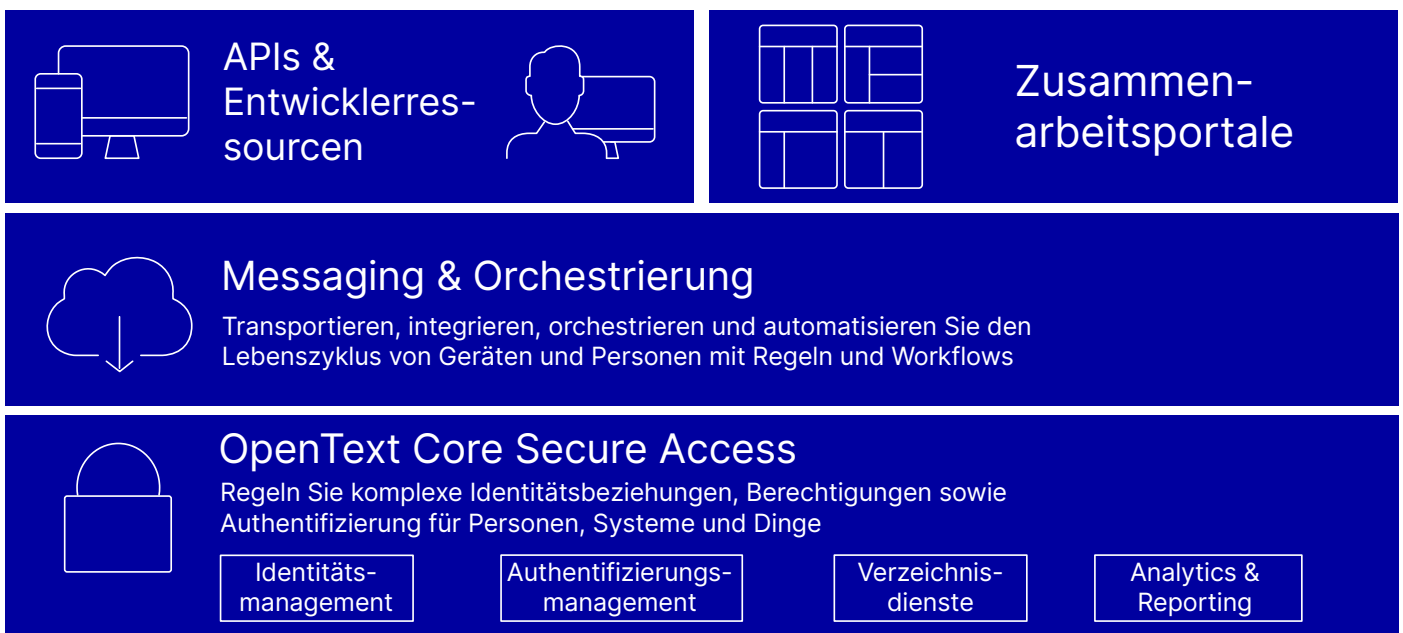


Abbildung 8. OpenText Core Secure Access as a Service

Identity and Access Management

OpenText Core Secure Access bietet eine umfassende Plattform mit Funktionen für Zugriffsmanagement, Bereitstellung, Identity Governance and Administration, Identitäts-Brokering, Verifizierung und andere Bereiche, um Remote- und Drittanbieterzugriff auf On-Premise- und Cloud-Systeme des Unternehmens zu sichern.

OpenText Core Secure Access Admin

Dank Self-Service-Verwaltung und -Konfiguration können Sie digitale Ökosysteme ganz einfach ohne kostspielige professionelle Services erstellen, erweitern und verwalten. Unternehmen können für das Hinzufügen neuer Systeme, Organisationen und Benutzer zu Ökosystemen den Zeit- und Personalbedarf reduzieren und gleichzeitig Zero-Trust-Prinzipien über eine Wertschöpfungskette jeder Größe hinweg durchsetzen.

Weitere Informationen:

[Lösungsübersicht:](#)

[OpenText Core](#)

[Secure Access](#) ›

[Produktseite:](#)

[OpenText Core](#)

[Secure Access](#) ›

[Video zur Erläuterung:](#)

[So sichern Sie](#)

[Drittanbieter-IAM](#) ›

[Blog: Beseitigung von Lücken](#)

[in der Cyber-Resilienz in](#)

[wichtigen Infrastrukturanlagen](#) ›

[Produktübersicht:](#)

[OpenText Core](#)

[Collaboration Access](#) ›

APIs und Entwicklerressourcen

APIs und Entwicklertools von OpenText beschleunigen die Entwicklung neuer Lösungen und Anwendungen und erhöhen gleichzeitig die Sicherheit. OpenText ermöglicht Unternehmen die Erstellung von Frameworks zur Verwaltung der komplexen Beziehungen zwischen Identitäten und wichtigen Geschäftsressourcen.

Collaboration-Portals

Portale ermöglichen eine sichere und effiziente Zusammenarbeit zwischen mehreren Unternehmen. Die Portale von OpenText umfassen intelligente, flexible Funktionen zur Steigerung der Geschwindigkeit und Ergebnisse der Wertschöpfungskette und reduzieren gleichzeitig die Kosten und Verzögerungen, die mit kollaborativen Arbeitsprozessen einhergehen, wie P2P, O2C, WIP und andere.

Messaging & Orchestrierung

Unternehmen können die automatisierte, ereignisgesteuerte Identitätslebensdauer-Verwaltung im gesamten Ökosystem vereinfachen. Systeme und Anwendungen beziehen einen Strom ereignisbasierter Nachrichten, die durch Aktionen innerhalb von OpenText Core Secure Access ausgelöst werden (z. B. Benutzer erstellen, Profil aktualisieren, Servicepaket erteilen, Lebenszyklusstatus des Benutzers aktualisieren), und ergreifen dann die entsprechende Maßnahme. Mit OpenText können Unternehmen beliebige externe Benutzer mit jedem Unternehmenssystem verbinden.

Fazit

OpenText Core Secure Access ist das Front-End aller digitalen Produkte, Services und Geschäftsprozesse. Da Unternehmen ihren digitalen Fokus über interne Effizienzen hinaus ausweiten, um Wachstum zu steigern und Mehrwert zu schaffen, werden herkömmliche OpenText Core Secure Access Lösungen zum einschränkenden Faktor: Time to Value, Skalierbarkeit, Kosten, Fähigkeit zur Integration in unbekannte Systeme und vieles mehr.

OpenText Core Secure Access sichert den Zugriff und das Risiko für einige der weltweit größten Wertschöpfungsketten, Distributionsnetzwerke und Kundenökosysteme. Unser Cloud-Service verbindet mehr als 30 Millionen Lieferanten, Kunden, Partner, Anbieter und andere Dritte mit On-Premise- und Cloud-Informationssystemen – und zwar großem Maßstab. Die bewährte Technologie von OpenText und die 30-jährige Innovation in der Identitäts- und Multi-Enterprise-Collaboration schaffen Transparenz bei Dritten, um IAM und Governance in komplexen Ökosystemen zu vereinfachen und zu automatisieren.