SailPoint

Interaktives E-Book

2024-2025

Die Horizonte der Identitätssicherheit

Mit Identity Security zu einer positiven Wertkurve in der Cybersicherheit

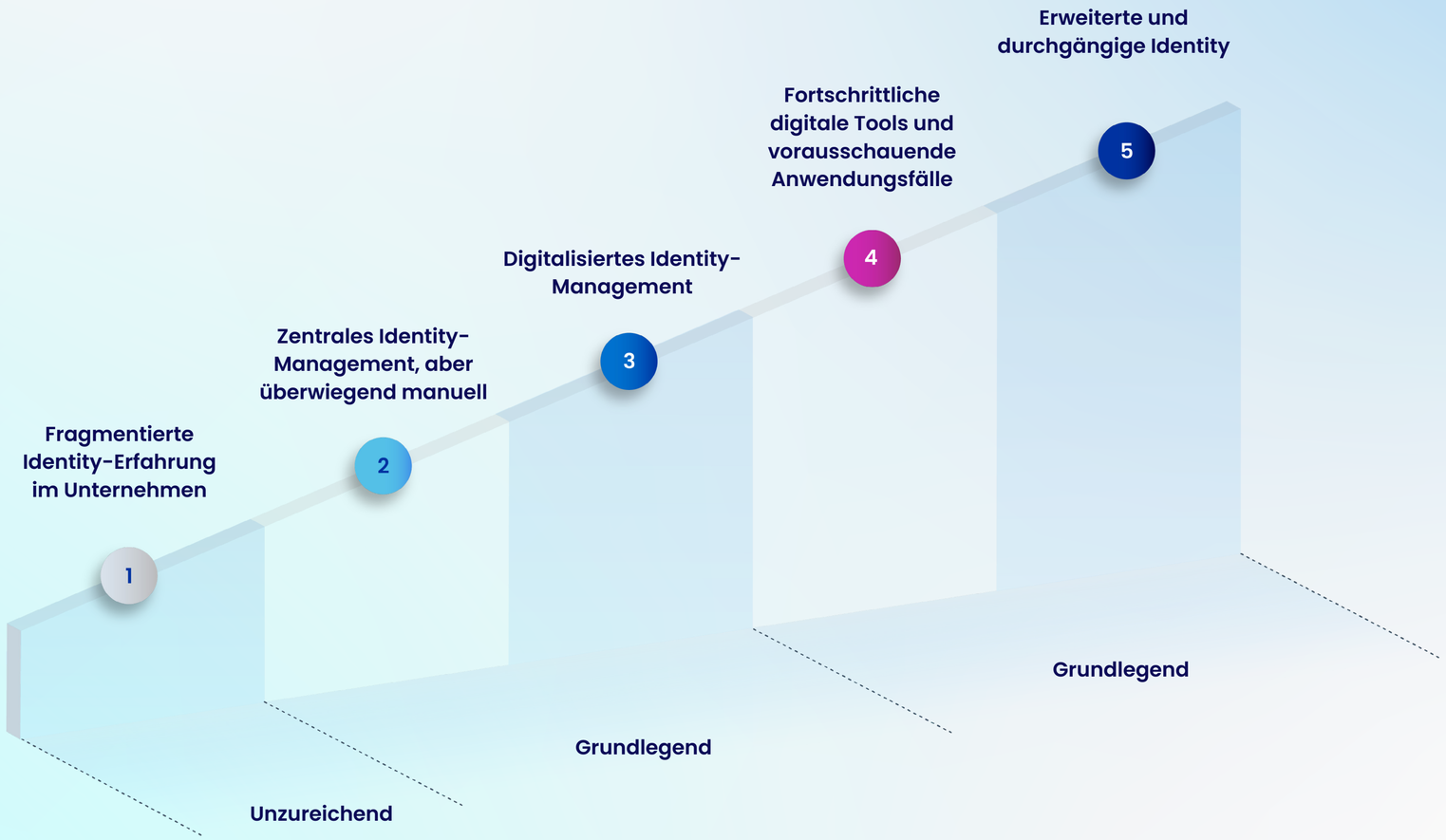
Erste Schritte →

Die Reise zu ausgereifter Identity Security antreten

Weltweit stehen Unternehmen aus allen Branchen vor der doppelten Herausforderung, zunehmend raffinierten und weitreichenden Cyberbedrohungen entgegenzuwirken und gleichzeitig knappe Budgets und unerbittliche Kosteneinsparungen zu meistern.

Besonders groß ist der Druck in der Identity Security, wo die Angriffsflächen im Zuge der Expansion von Unternehmen immer größer und die IT-Budgets immer kleiner werden. Zugleich fordern interne und externe Stakeholder robustere Sicherheit und bessere digitale Erlebnisse.

In den letzten drei Jahren hat SailPoint Entscheidungsträger für Identity and Access Management (IAM) rund um den Globus befragt, um ihre Kompetenzen entlang der fünf Horizonte der Identity Security zu bewerten. Zu den im Juli 2024 befragten 350 Entscheidungsträgern gehörten Führungskräfte aus den Bereichen IT, Cybersicherheit und Risikomanagement. Mehr als die Hälfte von ihnen arbeitet für Unternehmen mit über 10.000 Mitarbeitern und ebenfalls gut die Hälfte ist im Finanz- oder Technologiesektor tätig.



Quelle: Sämtliche Abbildungen in diesem Dokument sind dem Bericht **Die Horizonte der Identity Security 2024-2025** entnommen

KAPITEL 1

Technologische Fortschritte prägen die Zukunft der Identity Security.

Kapitel starten →

Die Zukunft der Identity wird von vier zentralen Elementen geprägt

Unsere Erfahrungen und Untersuchungen der letzten Jahre haben bestätigt, dass die Zukunft der Identity Security von integrierten Identity-Programmen geprägt sein wird.

Hier sind die wichtigsten Elemente zusammen mit den Trends, die sich aus diesen Elementen ergeben, dargestellt.

Die Weiterentwicklung der Aufsichts- und Risikolandschaft beeinflusst diese vier Elemente weiter

Identity-Security-Systeme werden zum Dreh- und Angelpunkt zukünftiger Sicherheitsmaßnahmen..

Die weltweite und branchenübergreifende Zunahme von Vorschriften und Industriestandards in Bezug auf Identity Security lässt die Erwartungen an Identity Security steigen.

Die Zukunft der Identity wird von vier zentralen Elementen geprägt

Unsere Erfahrungen und Untersuchungen der letzten Jahre haben bestätigt, dass die Zukunft der Identity Security von integrierten Identity-Programmen geprägt sein wird.

Hier sind die wichtigsten Elemente zusammen mit den Trends, die sich aus diesen Elementen ergeben, dargestellt.

Die Weiterentwicklung der Aufsichts- und Risikolandschaft beeinflusst diese vier Elemente weiter

Identity-Security-Systeme werden zum Dreh- und Angelpunkt zukünftiger Sicherheitsmaßnahmen..

Die weltweite und branchenübergreifende Zunahme von Vorschriften und Industriestandards in Bezug auf Identity Security lässt die Erwartungen an Identity Security steigen.

Die Zukunft der Identity wird von vier zentralen Elementen geprägt

Unsere Erfahrungen und Untersuchungen der letzten Jahre haben bestätigt, dass die Zukunft der Identity Security von integrierten Identity-Programmen geprägt sein wird.

Hier sind die wichtigsten Elemente zusammen mit den Trends, die sich aus diesen Elementen ergeben, dargestellt.

Die Weiterentwicklung der Aufsichts- und Risikolandschaft beeinflusst diese vier Elemente weiter

Identity-Security-Systeme werden zum Dreh- und Angelpunkt zukünftiger Sicherheitsmaßnahmen..

Die weltweite und branchenübergreifende Zunahme von Vorschriften und Industriestandards in Bezug auf Identity Security lässt die Erwartungen an Identity Security steigen.

Die Zukunft der Identity wird von vier zentralen Elementen geprägt

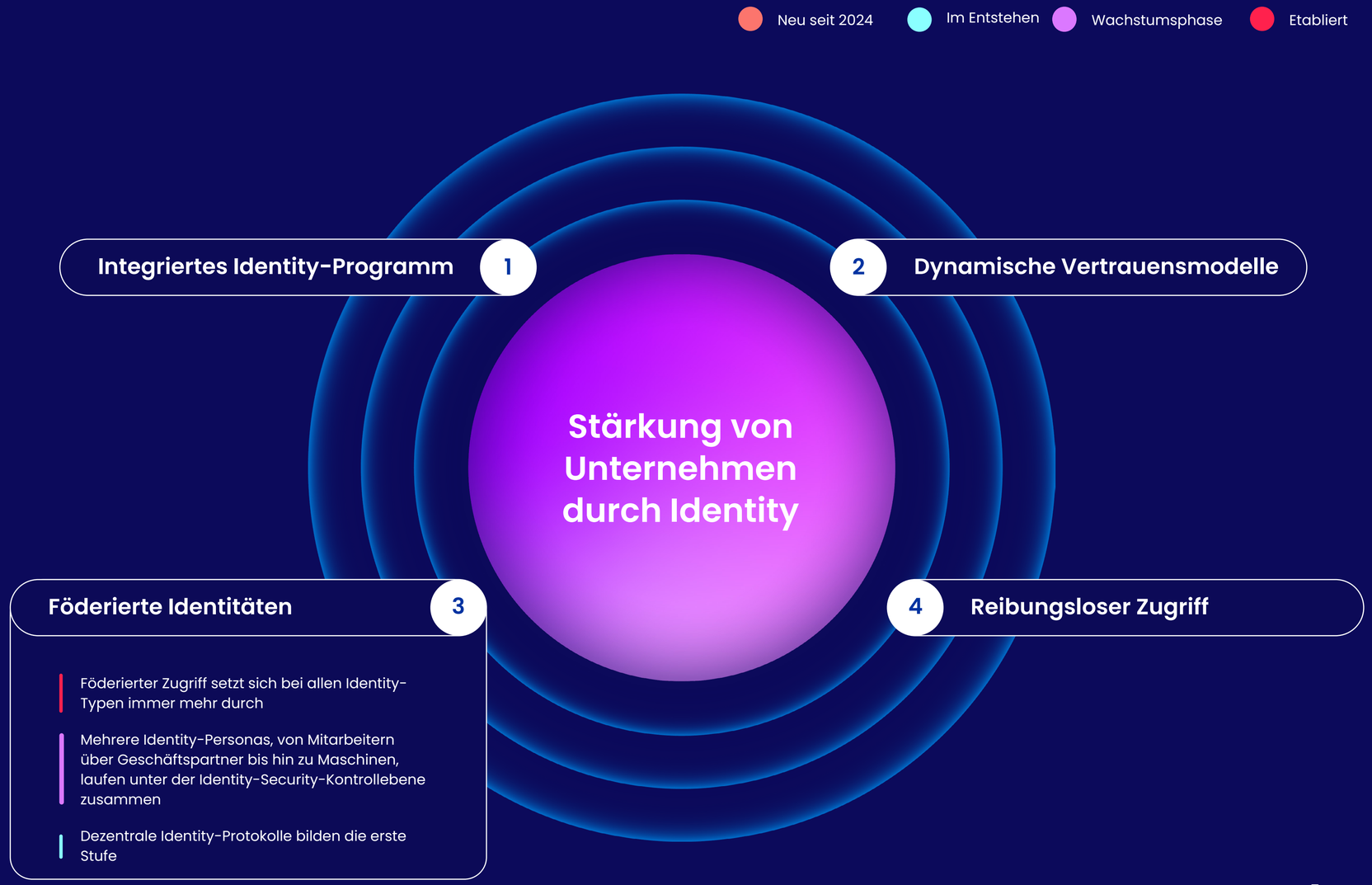
Unsere Erfahrungen und Untersuchungen der letzten Jahre haben bestätigt, dass die Zukunft der Identity Security von integrierten Identity-Programmen geprägt sein wird.

Hier sind die wichtigsten Elemente zusammen mit den Trends, die sich aus diesen Elementen ergeben, dargestellt.

Die Weiterentwicklung der Aufsichts- und Risikolandschaft beeinflusst diese vier Elemente weiter

Identity-Security-Systeme werden zum Dreh- und Angelpunkt zukünftiger Sicherheitsmaßnahmen..

Die weltweite und branchenübergreifende Zunahme von Vorschriften und Industriestandards in Bezug auf Identity Security lässt die Erwartungen an Identity Security steigen.



Die Zukunft der Identity wird von vier zentralen Elementen geprägt

Unsere Erfahrungen und Untersuchungen der letzten Jahre haben bestätigt, dass die Zukunft der Identity Security von integrierten Identity-Programmen geprägt sein wird.

Hier sind die wichtigsten Elemente zusammen mit den Trends, die sich aus diesen Elementen ergeben, dargestellt.

Die Weiterentwicklung der Aufsichts- und Risikolandschaft beeinflusst diese vier Elemente weiter

Identity-Security-Systeme werden zum Dreh- und Angelpunkt zukünftiger Sicherheitsmaßnahmen..

Die weltweite und branchenübergreifende Zunahme von Vorschriften und Industriestandards in Bezug auf Identity Security lässt die Erwartungen an Identity Security steigen.

KAPITEL 2

Identity-Security-Investitionen können die Wertkurve positiv beeinflussen.

Kapitel starten →

Wert-kurve

Risiko-minderung

Geschäfts-wert

Produktivität

Unternehmen mit ausgereifter Identity Security erzielen für jeden ausgegebenen Dollar überproportional höhere Renditen

Der Sprung zu Horizont 3 und 4 wirkt sich bei Identity Security überproportional aus und „biegt die Wertkurve“ exponentiell.

Der Durchmesser der Kugeln gibt die Verteilung des jeweiligen Horizonts an

Wert-kurve

Risiko-minderung

Geschäfts-wert

Produktivität

Mit der Erschließung neuer Identity-Security-Horizonte verkleinert sich die Angriffsfläche für potenzielle Verstöße

83% der Unternehmen verzeichneten weniger identitätsbezogene Sicherheitsprobleme aufgrund ihrer Investitionen in Identity Security im Jahr 2023

Der Durchmesser der Kugeln gibt die Verteilung des jeweiligen Horizonts an

Wert-kurve

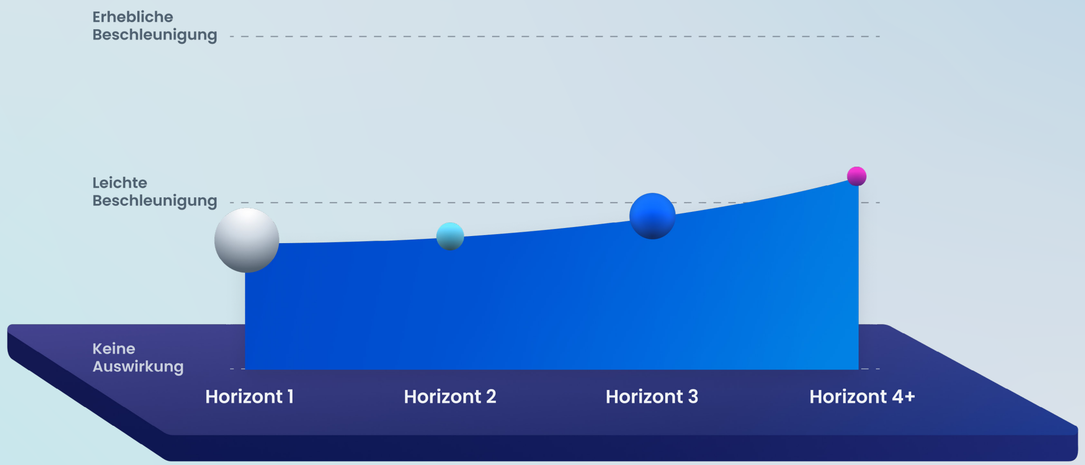
Risiko-minderung

Geschäfts-wert

Produktivität

Unternehmen mit fortschrittlichen Identity-Funktionen profitieren von einer schnelleren Markteinführung und weniger Reibung

Umsatzerlöse steigern: Fortschrittliche Identity Security fördert den digitalen Wandel, ermöglicht kürzere Entwicklungszyklen und eine schnellere Markteinführung und steigert so den Umsatz.



Der Durchmesser der Kugeln gibt die Verteilung des jeweiligen Horizonts an

Wert-kurve

Risiko-minderung

Geschäfts-wert

Produktivität

Unternehmen in den Horizonten 3 und 4+ dürften erhebliche Produktivitäts-steigerungen verzeichnen

Unternehmen ab Horizont 4 verzeichnen erhebliche Produktivitätssteigerungen durch einen integrierten Identity-Security-Ansatz und die Einführung neuer **Anwendungsfälle, wie z. B.** Copiloten als Orientierungshilfe, Services für Endbenutzer und automatisierte Genehmigung des Benutzerzugriffs.

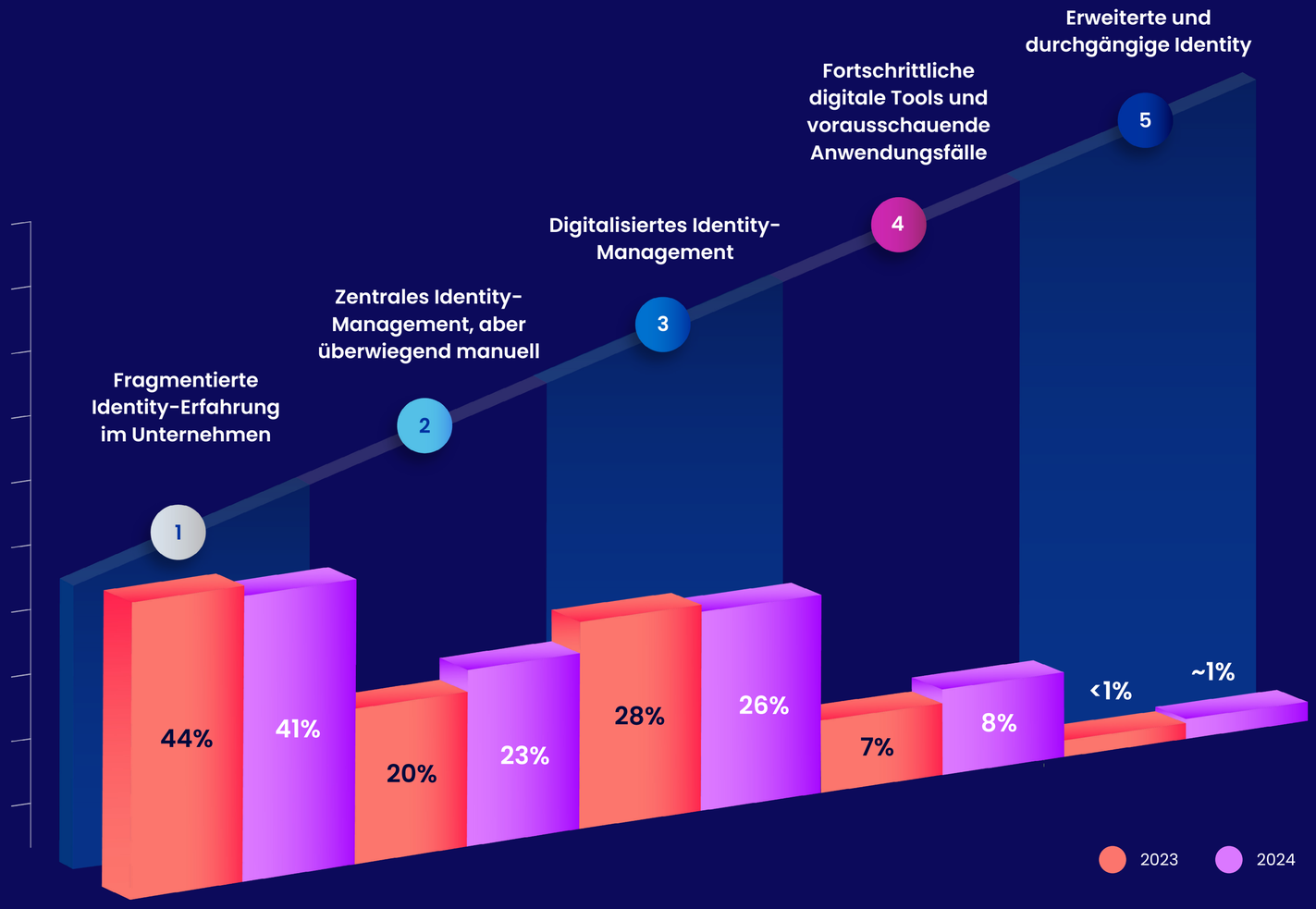
Der Durchmesser der Kugeln gibt die Verteilung des jeweiligen Horizonts an

KAPITEL 3

Wo sich Unternehmen auf ihrer Entwicklungsreise befinden und warum reife Unternehmen höhere Renditen erzielen.

Kapitel starten →

41 % der Unternehmen befinden sich weiterhin in Horizont 1, was noch viel Spielraum für die Erschließung des vollen Potenzials von Identity Security bietet.



Unternehmen in Horizont 4+ senken ihr Risiko durch eine 70%ige Abdeckung aller Identity-Typen; Horizont 3 liegt knapp dahinter

Unternehmen der Horizonte 1 und 2 weisen **große Lücken bei der Identity- Abdeckung** auf.

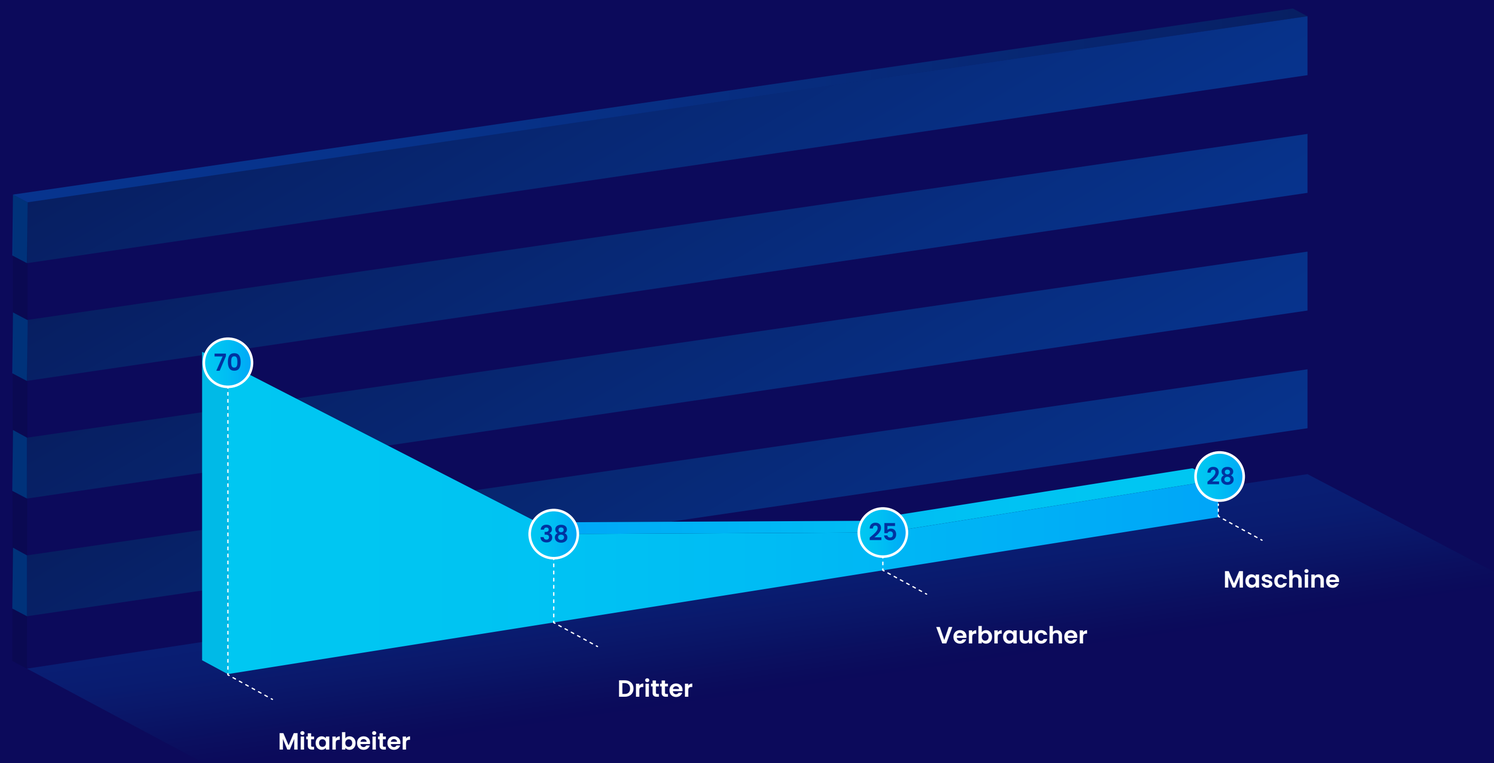
30% der Mitarbeiter

62% der Dritten

72% der Maschinen-identitäten

Letzteres ist besonders besorgniserregend, da Maschinenidentitäten typischerweise ca. 40 % bis 65 % der gesamten Identitäten in einem Unternehmen ausmachen.

Horizon 1-2 | Horizon 3 | Horizon 4+ | Gesamt | Alle Daten



Unternehmen in Horizont 4+ senken ihr Risiko durch eine 70%ige Abdeckung aller Identity-Typen; Horizont 3 liegt knapp dahinter

Unternehmen der Horizonte 1 und 2 weisen **große Lücken bei der Identity- Abdeckung** auf.

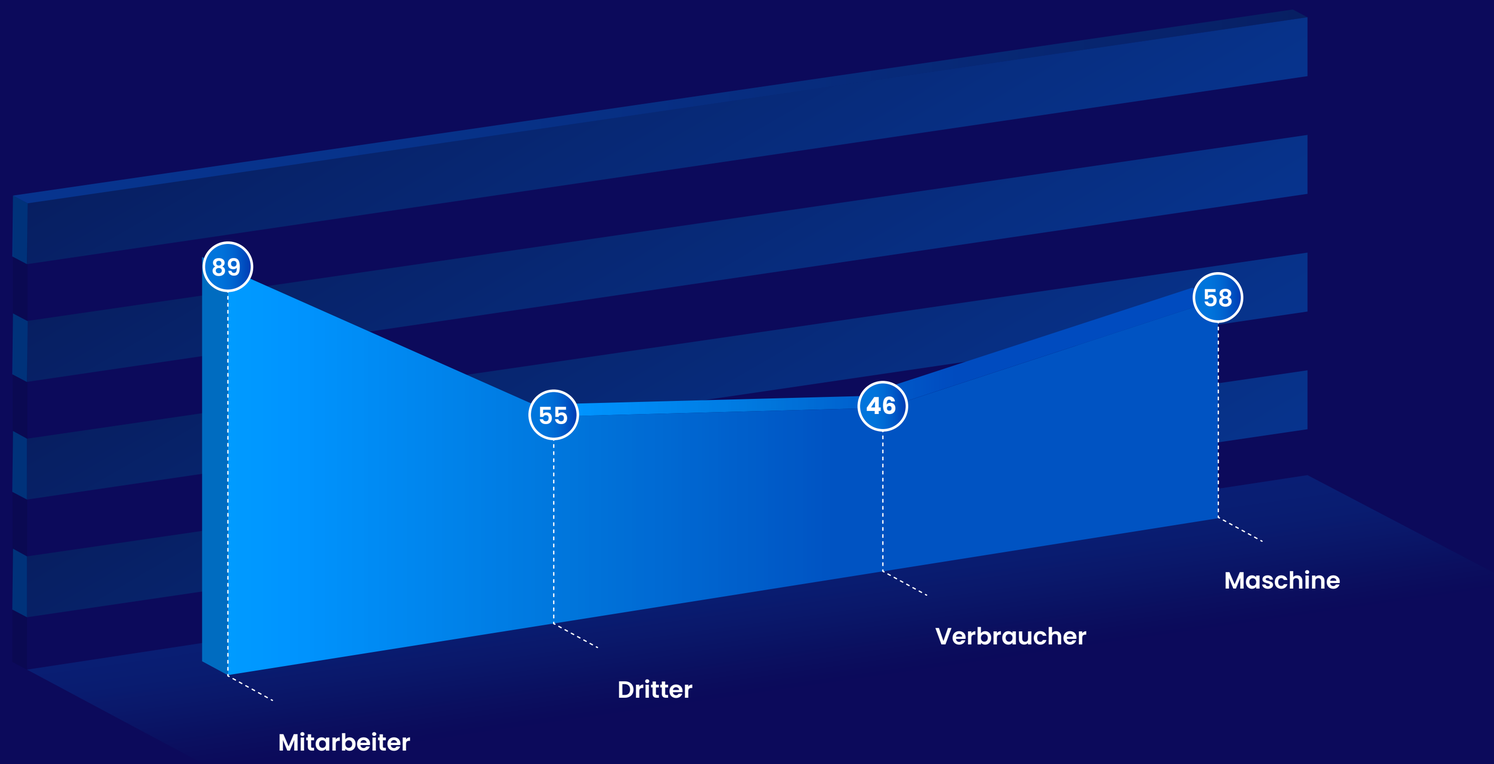
30% der Mitarbeiter

62% der Dritten

72% der Maschinen-identitäten

Letzteres ist besonders besorgniserregend, da Maschinenidentitäten typischerweise ca. 40 % bis 65 % der gesamten Identitäten in einem Unternehmen ausmachen.

Horizon 1-2 | **Horizon 3** | Horizon 4+ | Gesamt | Alle Daten



Unternehmen in Horizont 4+ senken ihr Risiko durch eine 70%ige Abdeckung aller Identity-Typen; Horizont 3 liegt knapp dahinter

Unternehmen der Horizonte 1 und 2 weisen **große Lücken bei der Identity- Abdeckung** auf.

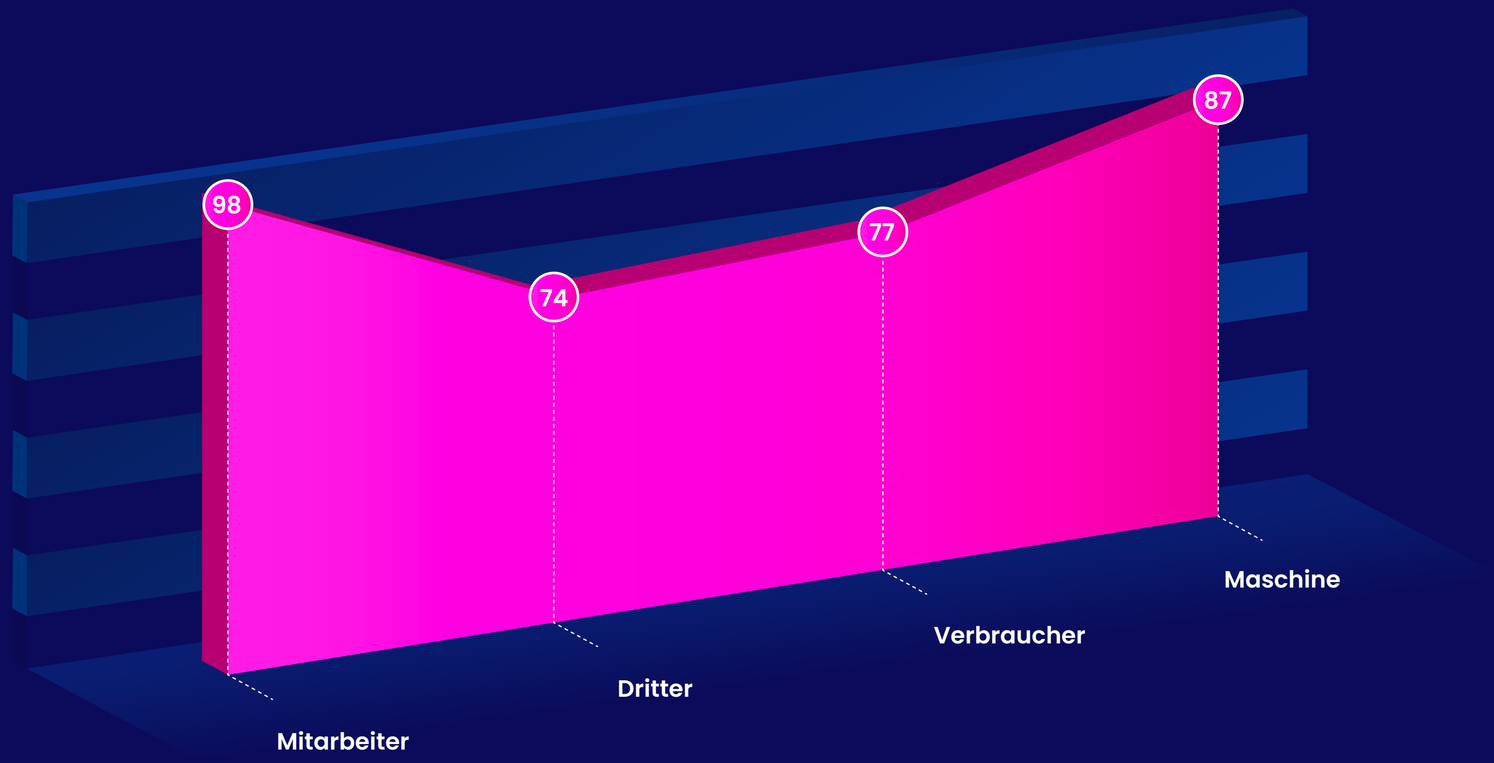
30% der Mitarbeiter

62% der Dritten

72% der Maschinen-identitäten

Letzteres ist besonders besorgniserregend, da Maschinenidentitäten typischerweise ca. 40 % bis 65 % der gesamten Identitäten in einem Unternehmen ausmachen.

Horizon 1-2 | Horizon 3 | **Horizon 4+** | Gesamt | Alle Daten



Unternehmen in Horizont 4+ senken ihr Risiko durch eine 70%ige Abdeckung aller Identity-Typen; Horizont 3 liegt knapp dahinter

Unternehmen der Horizonte 1 und 2 weisen **große Lücken bei der Identity- Abdeckung** auf.

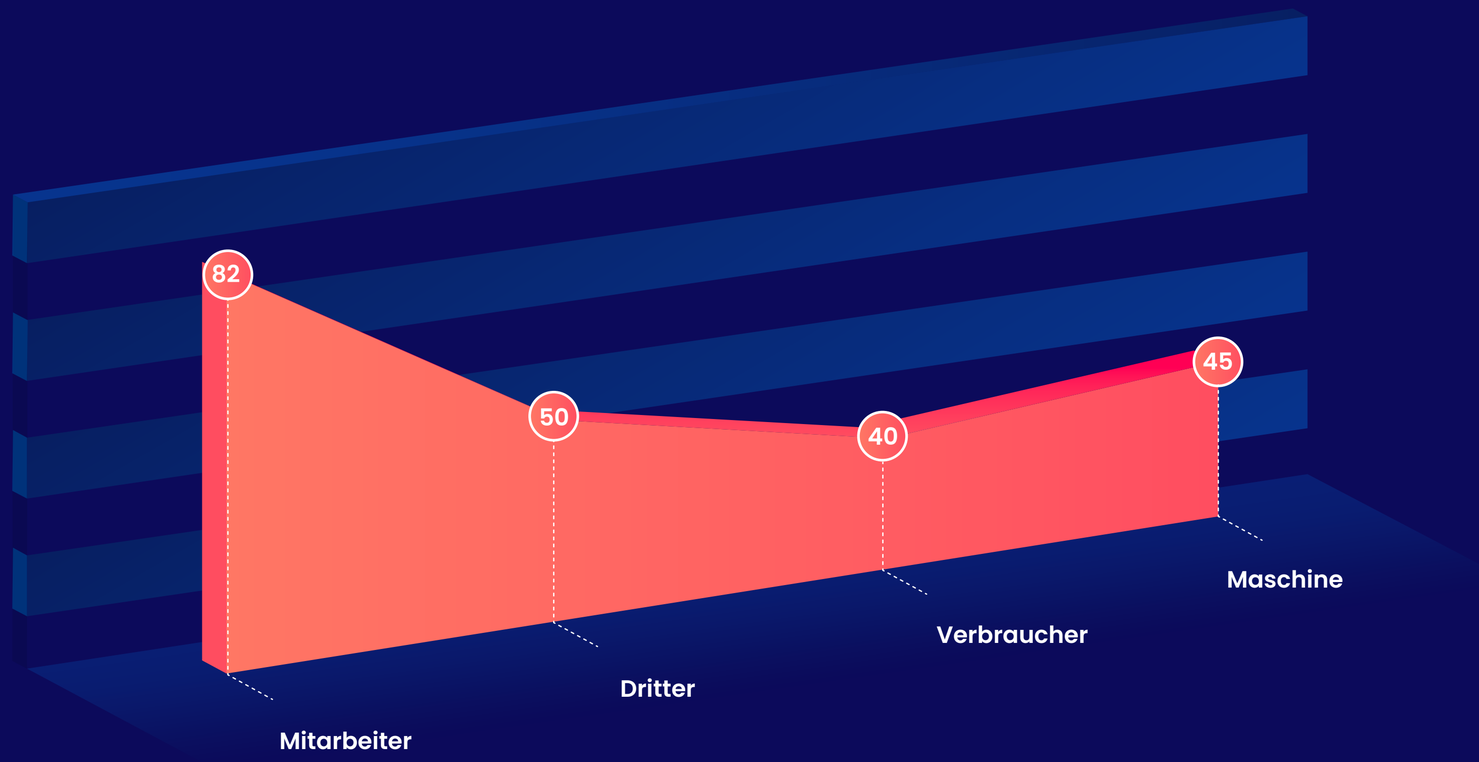
30% der Mitarbeiter

62% der Dritten

72% der Maschinen-identitäten

Letzteres ist besonders besorgniserregend, da Maschinenidentitäten typischerweise ca. 40 % bis 65 % der gesamten Identitäten in einem Unternehmen ausmachen.

Horizon 1-2 | Horizon 3 | Horizon 4+ | **Gesamt** | Alle Daten



Unternehmen in Horizont 4+ senken ihr Risiko durch eine 70%ige Abdeckung aller Identity-Typen; Horizont 3 liegt knapp dahinter

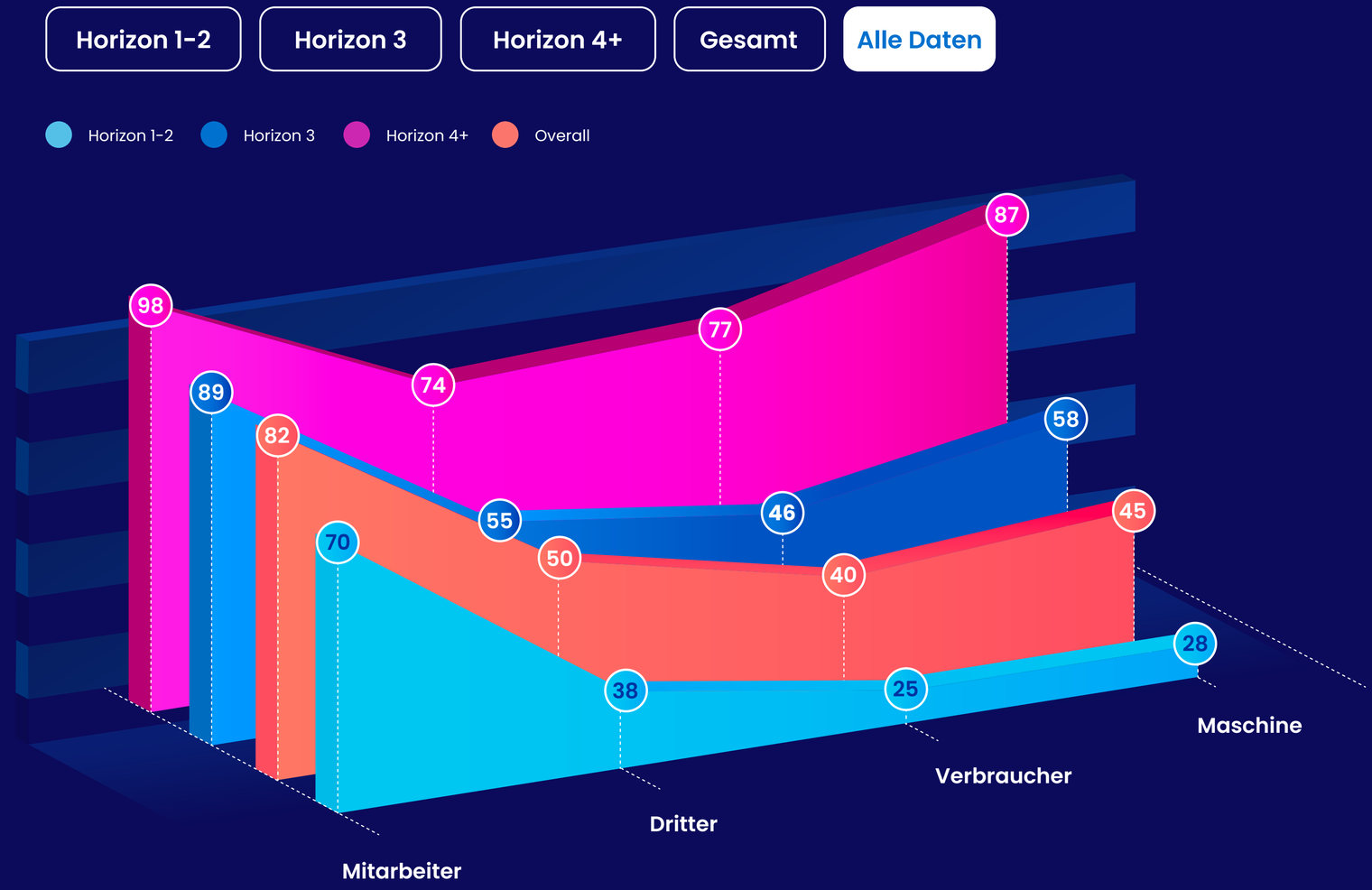
Unternehmen der Horizonte 1 und 2 weisen **große Lücken bei der Identity- Abdeckung** auf.

30% der Mitarbeiter

62% der Dritten

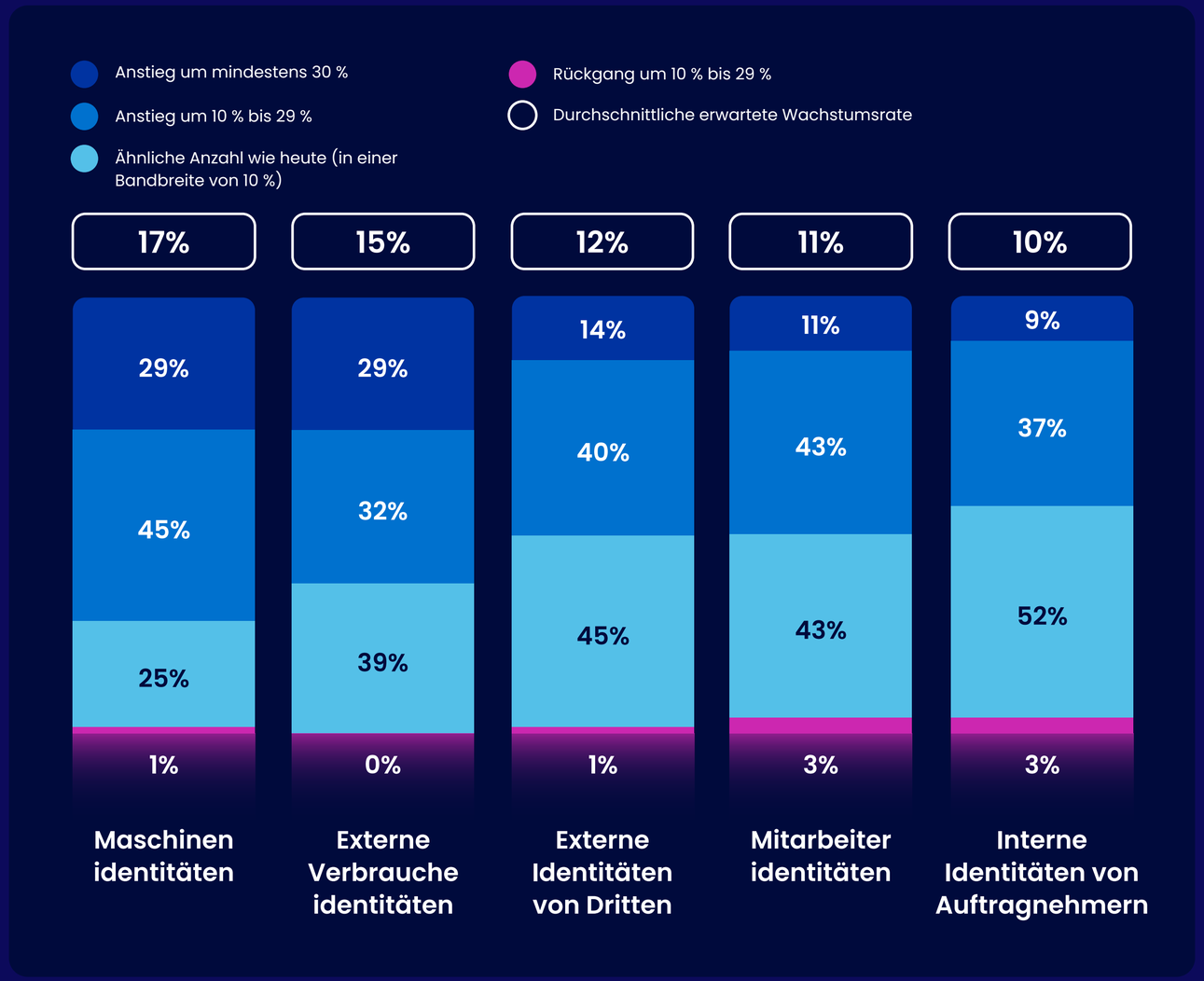
72% der Maschinen-identitäten

Letzteres ist besonders besorgniserregend, da Maschinenidentitäten typischerweise ca. 40 % bis 65 % der gesamten Identitäten in einem Unternehmen ausmachen.

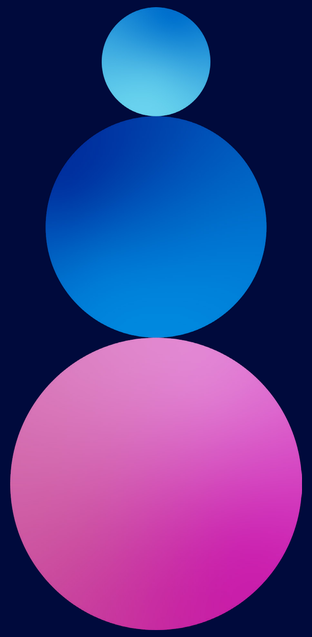


Die Anzahl aller Identitäten wird in den nächsten drei bis fünf Jahren voraussichtlich um etwa 14 % zunehmen, wobei Maschinenidentitäten am schnellsten wachsen werden.

Die Zunahme der **Maschinenidentitäten** könnte die Zunahme der menschlichen Identitäten übertreffen



Unternehmen in Horizont 4+ nutzen mit einer doppelt so hohen Wahrscheinlichkeit Identity-Daten zur Gewinnung umsetzbarer Erkenntnisse und neuer Anwendungsfälle



<20%

der Unternehmen in Horizont 1–2
nutzen Identity-Daten in großem Umfang

<40%

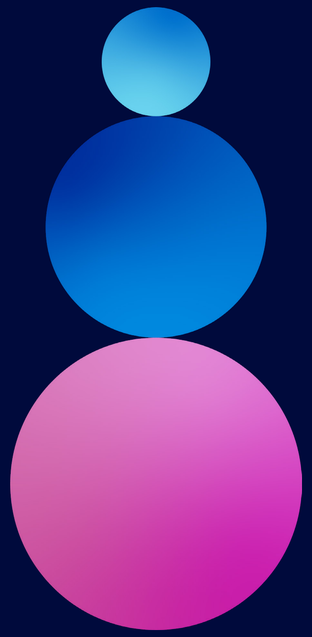
der Unternehmen in Horizont 3
nutzen Identity-Daten in großem Umfang

~50%

der Unternehmen in Horizont 4+
verwenden für Benutzerzugriff, Sicherheitsrichtlinien und Zugriffsbewertungen Erkenntnisse aus strukturierten und unstrukturierten Daten

Horizon 1-2 | Horizon 3 | Horizon 4+ | Gesamt | Alle Daten

Unternehmen in Horizont 4+ nutzen mit einer doppelt so hohen Wahrscheinlichkeit Identity-Daten zur Gewinnung umsetzbarer Erkenntnisse und neuer Anwendungsfälle



<20%

der Unternehmen in Horizont 1–2
nutzen Identity-Daten in großem Umfang

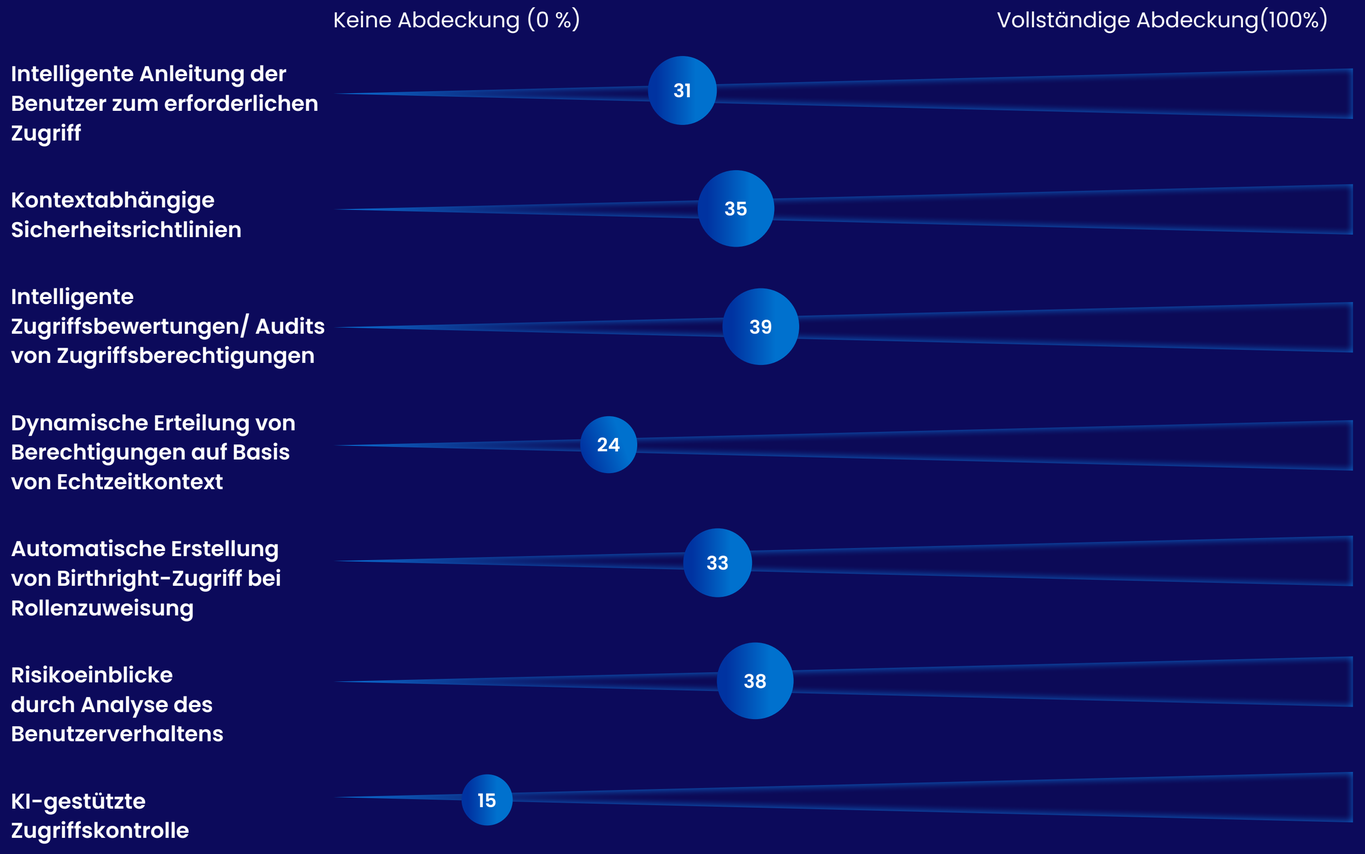
<40%

der Unternehmen in Horizont 3
nutzen Identity-Daten in großem Umfang

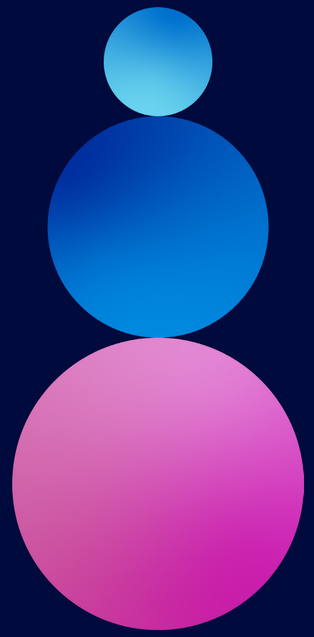
~50%

der Unternehmen in Horizont 4+
verwenden für Benutzerzugriff, Sicherheitsrichtlinien und Zugriffsbewertungen Erkenntnisse aus strukturierten und unstrukturierten Daten

Horizon 1-2 | Horizon 3 | Horizon 4+ | Gesamt | Alle Daten



Unternehmen in Horizont 4+ nutzen mit einer doppelt so hohen Wahrscheinlichkeit Identity-Daten zur Gewinnung umsetzbarer Erkenntnisse und neuer Anwendungsfälle



<20%

der Unternehmen in Horizont 1–2
nutzen Identity-Daten in großem Umfang

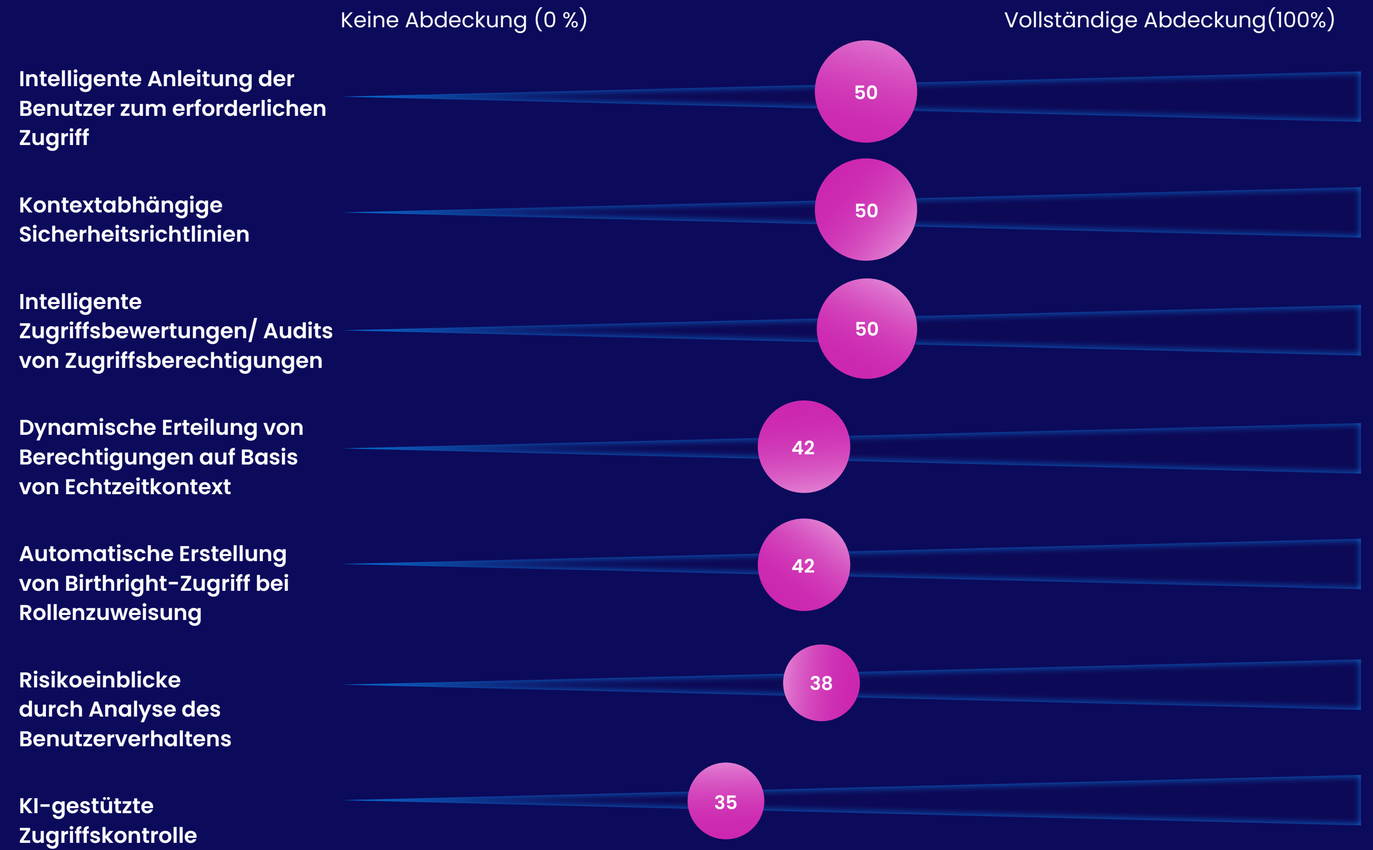
<40%

der Unternehmen in Horizont 3
nutzen Identity-Daten in großem Umfang

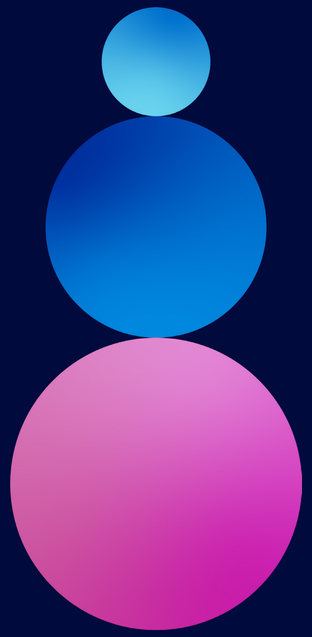
~50%

der Unternehmen in Horizont 4+
verwenden für Benutzerzugriff, Sicherheitsrichtlinien und Zugriffsbewertungen Erkenntnisse aus strukturierten und unstrukturierten Daten

Horizon 1-2 | Horizon 3 | **Horizon 4+** | Gesamt | Alle Daten



Unternehmen in Horizont 4+ nutzen mit einer doppelt so hohen Wahrscheinlichkeit Identity-Daten zur Gewinnung umsetzbarer Erkenntnisse und neuer Anwendungsfälle



<20%

der Unternehmen in Horizont 1–2
nutzen Identity-Daten in großem Umfang

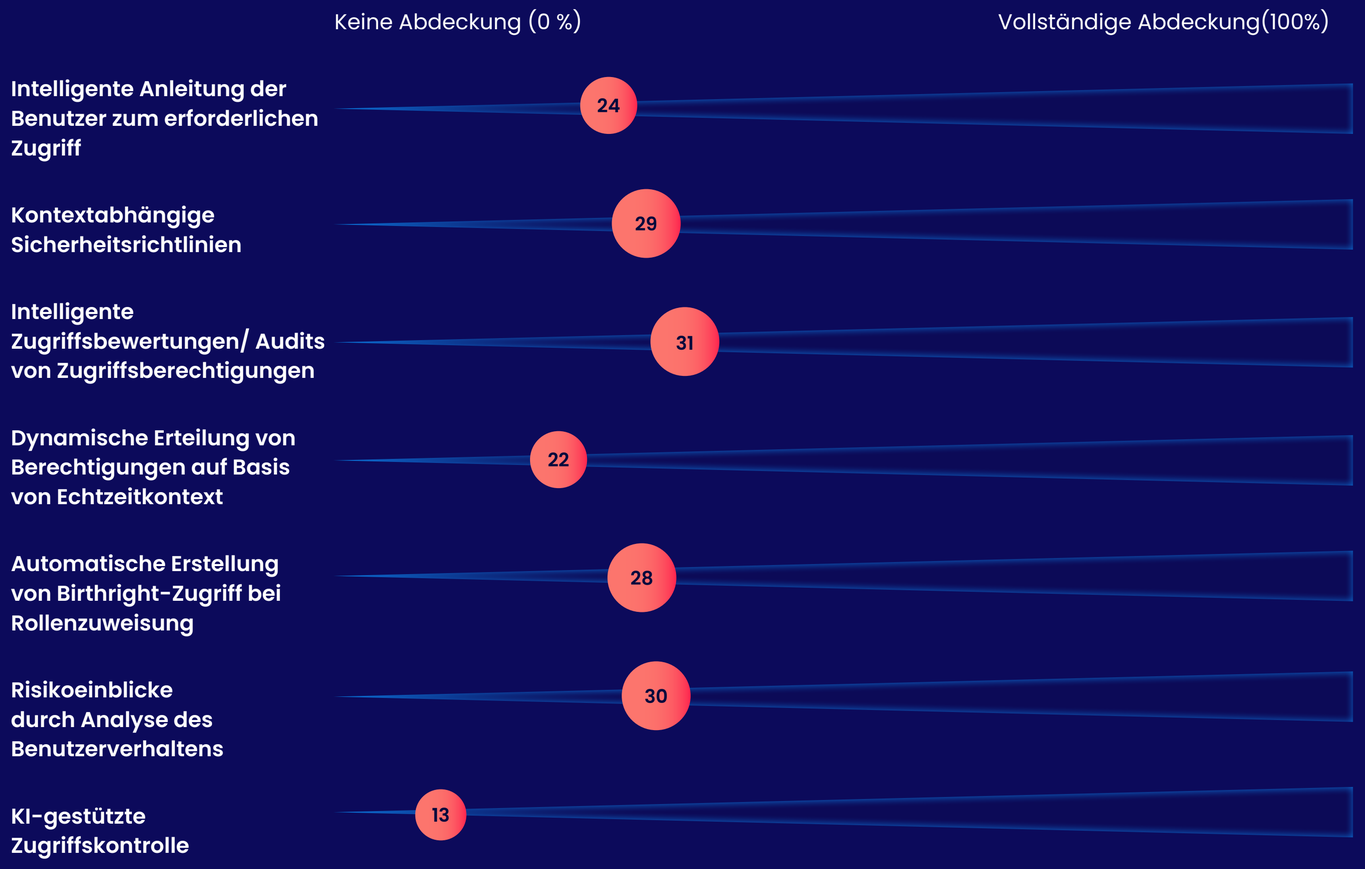
<40%

der Unternehmen in Horizont 3
nutzen Identity-Daten in großem Umfang

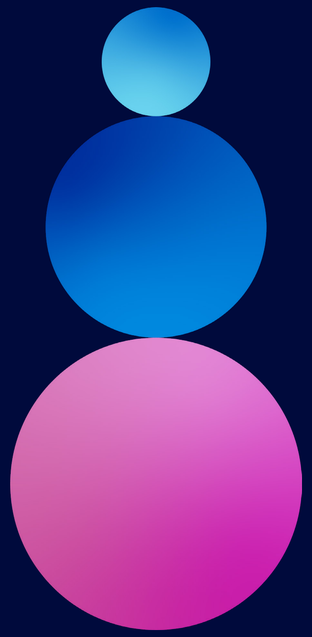
~50%

der Unternehmen in Horizont 4+
verwenden für Benutzerzugriff, Sicherheitsrichtlinien und Zugriffsbewertungen Erkenntnisse aus strukturierten und unstrukturierten Daten

Horizon 1-2 | Horizon 3 | Horizon 4+ | Gesamt | Alle Daten



Unternehmen in Horizont 4+ nutzen mit einer doppelt so hohen Wahrscheinlichkeit Identity-Daten zur Gewinnung umsetzbarer Erkenntnisse und neuer Anwendungsfälle



<20%

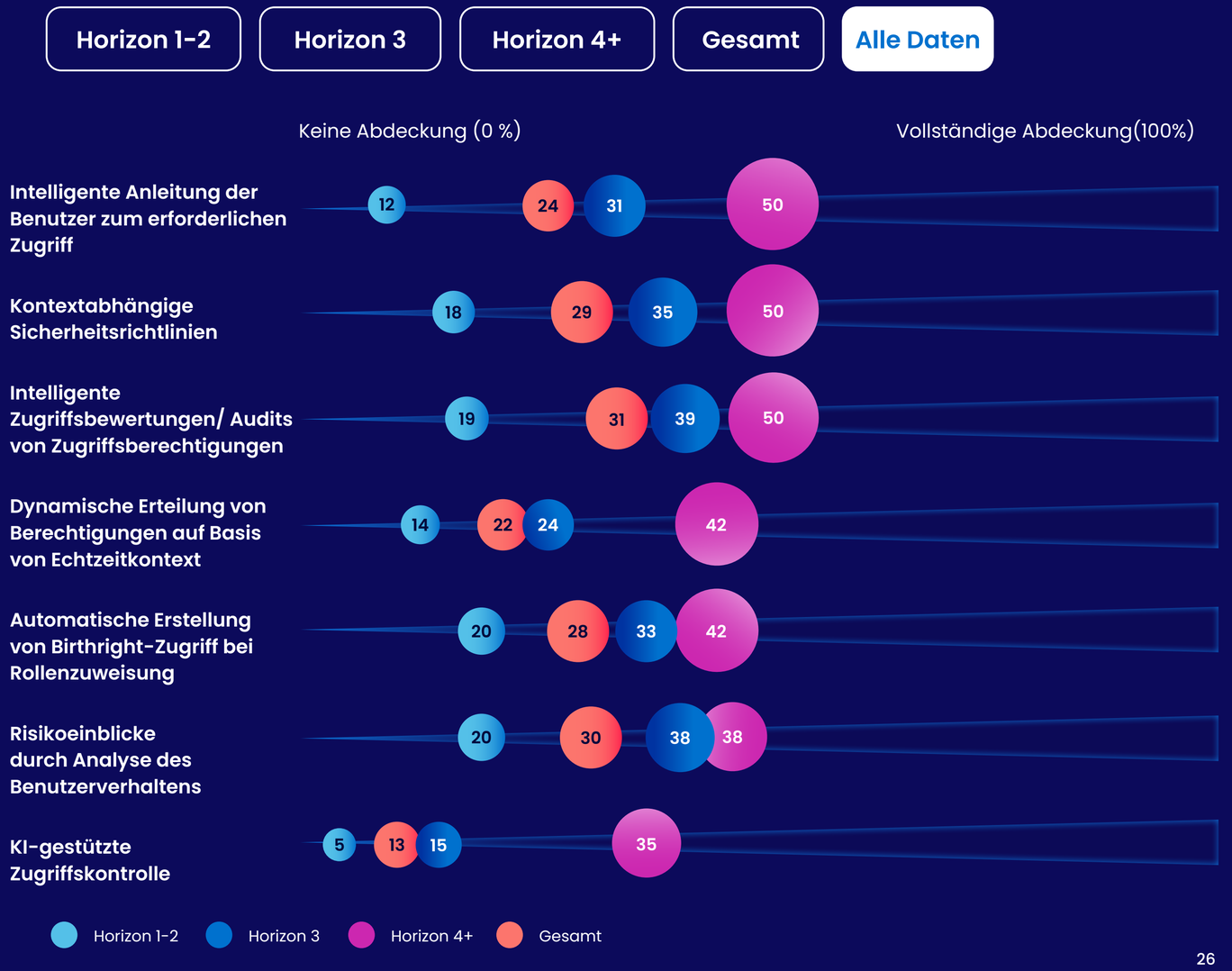
der Unternehmen in Horizont 1–2
nutzen Identity-Daten in großem Umfang

<40%

der Unternehmen in Horizont 3
nutzen Identity-Daten in großem Umfang

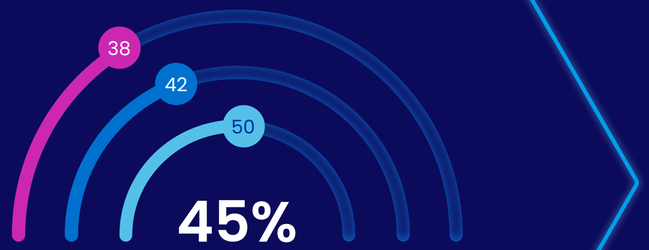
~50%

der Unternehmen in Horizont 4+
verwenden für Benutzerzugriff, Sicherheitsrichtlinien und Zugriffsbewertungen Erkenntnisse aus strukturierten und unstrukturierten Daten

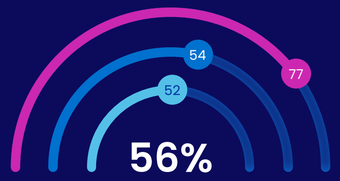


Unternehmen mit ausgereifter Identity Security haben die Grundlagen, um in skalierbare, GenAI-gestützte Anwendungsfälle zu investieren

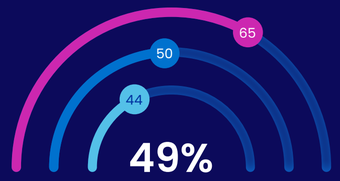
Unternehmen in Horizont 3+ konzentrieren sich auf die Entwicklung skalierbarer Lösungen zur Verbesserung und Erweiterung ihrer Identity Security. Unternehmen in den Horizonten 1–2 fokussieren sich dagegen auf die Automatisierung repetitiver Helpdesk-Tätigkeiten



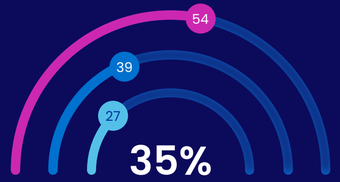
KI-Chatbots für sofortigen IAM-Support und Aufgabenmanagement



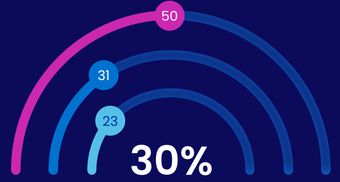
KI-gestützte Workflow-Erstellung (inkl. Benutzerbereitstellung, Zugriffsüberprüfungen und Rollenverwaltung)



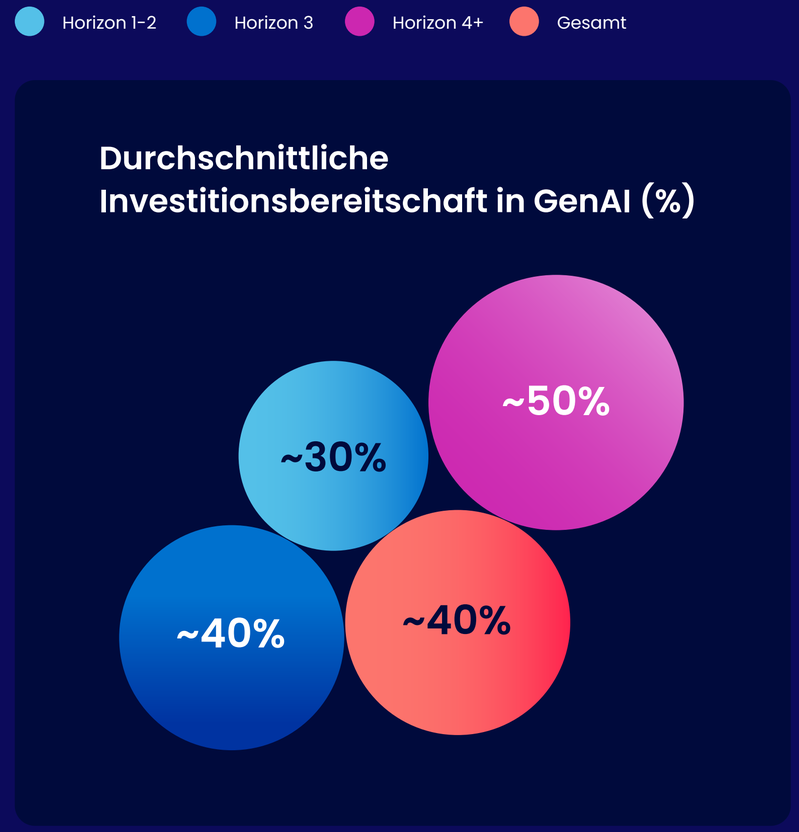
KI-generierte Berechtigungen und Rollenbeschreibungen für Benutzer (inkl. Rechte, Privilegien und Zugriffsebenen)



Suche in natürlicher Sprache zum einfachen Abrufen von IAM-Daten

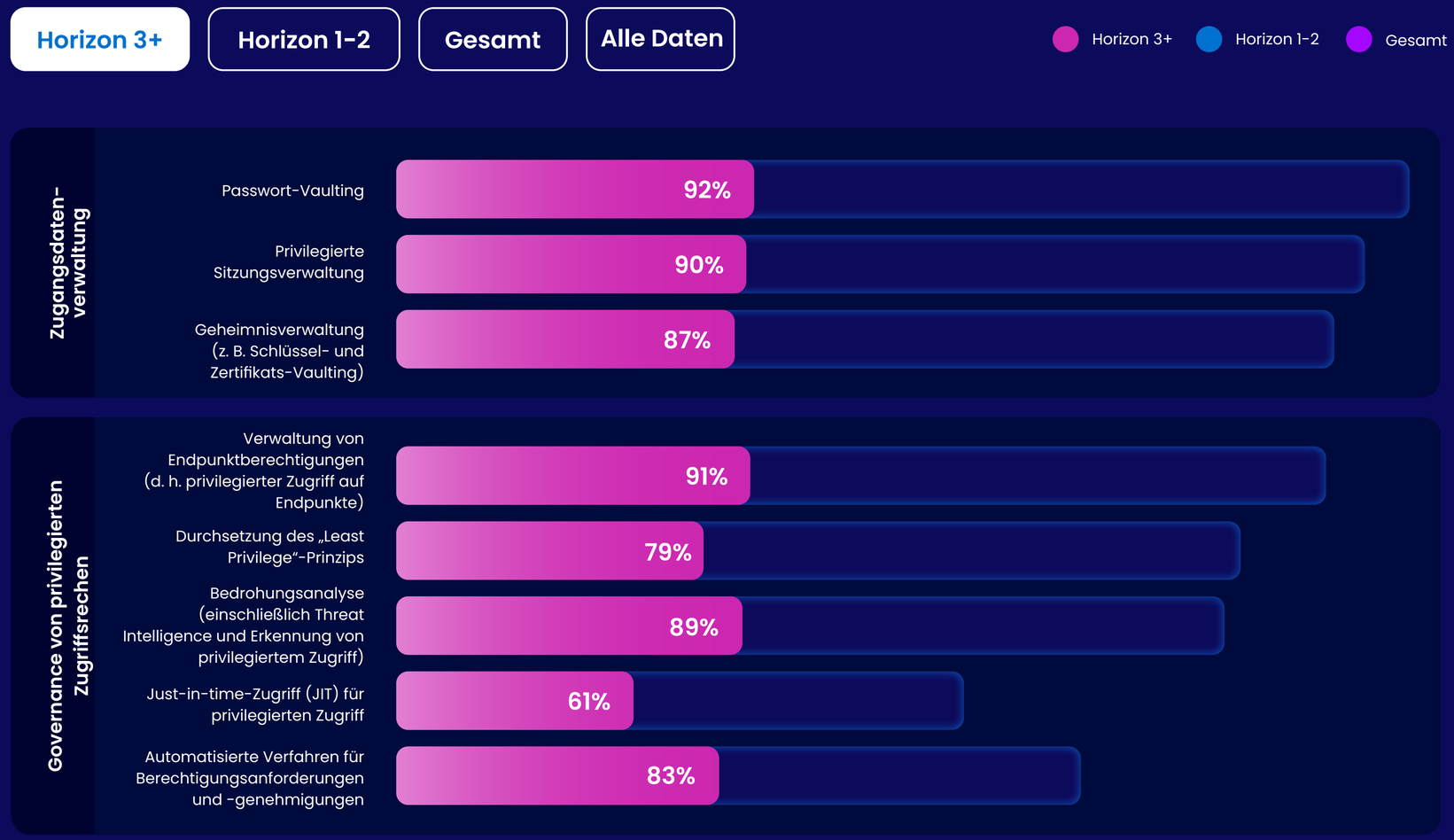


Copiloten für die automatisierte Entwicklung von Konnektoren



Unternehmen in Horizont 3+ weisen im Vergleich zu den Horizonten 1–2 eine um bis zu 50 % höhere Nutzung von Governance-Funktionen für den privilegierten Zugriff auf

Durch Investitionen in Lösungen, die über das alleinige Verwahren von Zugangsdaten und das Session-Management hinausgehen, können Unternehmen die Anforderung und Genehmigung von Zugriffsrechten vereinfachen und gleichzeitig die Bedrohungsanalyse für privilegierte Konten verbessern



Unternehmen in Horizont 3+ weisen im Vergleich zu den Horizonten 1–2 eine um bis zu 50 % höhere Nutzung von Governance-Funktionen für den privilegierten Zugriff auf

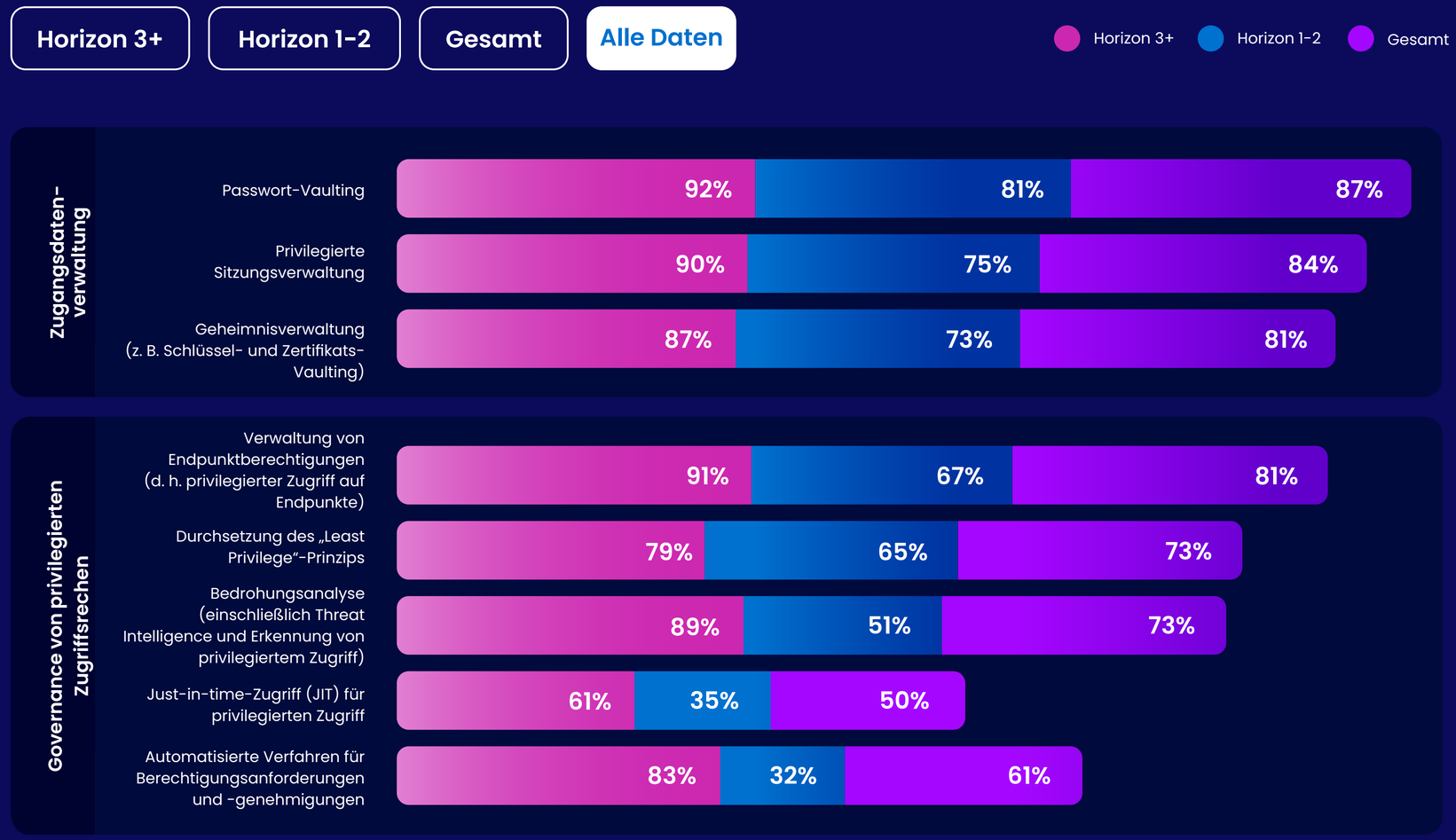
Durch Investitionen in Lösungen, die über das alleinige Verwahren von Zugangsdaten und das Session-Management hinausgehen, können Unternehmen die Anforderung und Genehmigung von Zugriffsrechten vereinfachen und gleichzeitig die Bedrohungsanalyse für privilegierte Konten verbessern

Unternehmen in Horizont 3+ weisen im Vergleich zu den Horizonten 1–2 eine um bis zu 50 % höhere Nutzung von Governance-Funktionen für den privilegierten Zugriff auf

Durch Investitionen in Lösungen, die über das alleinige Verwahren von Zugangsdaten und das Session-Management hinausgehen, können Unternehmen die Anforderung und Genehmigung von Zugriffsrechten vereinfachen und gleichzeitig die Bedrohungsanalyse für privilegierte Konten verbessern

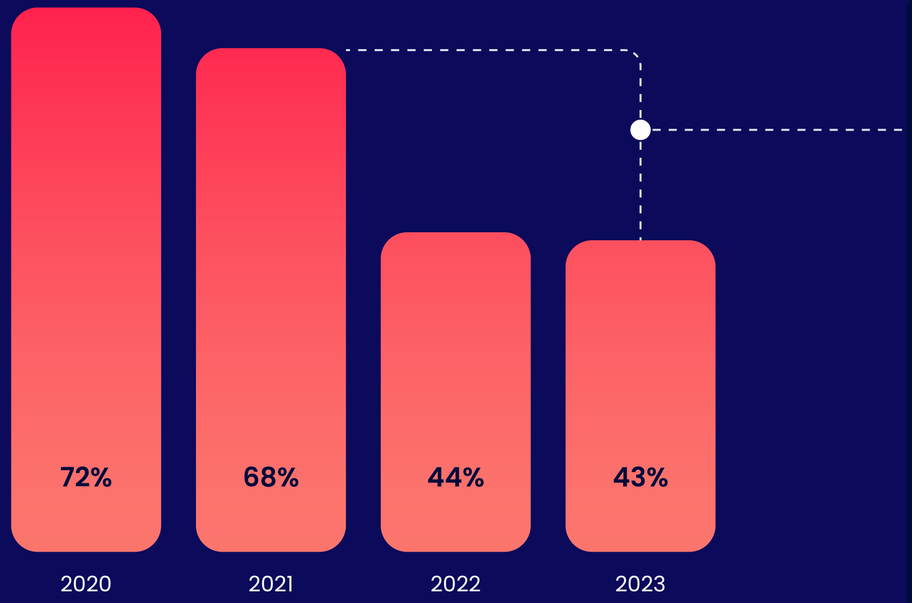
Unternehmen in Horizont 3+ weisen im Vergleich zu den Horizonten 1–2 eine um bis zu 50 % höhere Nutzung von Governance-Funktionen für den privilegierten Zugriff auf

Durch Investitionen in Lösungen, die über das alleinige Verwahren von Zugangsdaten und das Session-Management hinausgehen, können Unternehmen die Anforderung und Genehmigung von Zugriffsrechten vereinfachen und gleichzeitig die Bedrohungsanalyse für privilegierte Konten verbessern



Cyberversicherer entwickeln ausgereiftere Methoden, um die Steuerung von Cyberrisiken zu bewerten, und die Prämien für Cyberversicherungen sind gestiegen

Cyberversicherer haben ihre Schadenquoten gesenkt und an Reife bei der Risikobewertung und -verwaltung gewonnen. . .

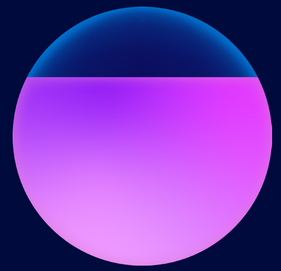


Eigenständige Schadenquoten in der Cyberdeckung, Anteil der Prämien, die für Schadenfälle ausgezahlt werden

40%

Geringere Verluste bei Cyberversicheren deuten auf ein verbessertes Cyberrisikomanagement auf

. . . und die Prämien an das gestiegene Risikoprofil angepasst



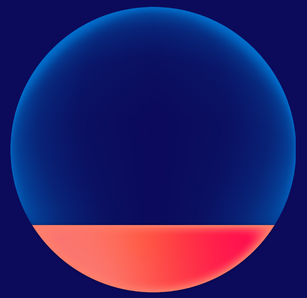
77%

der Unternehmen verzeichneten einen Prämienanstieg in den letzten drei Jahren

> Versicherungsgesellschaften prüfen jetzt genauer, welche Sicherheitskontrollen ein Unternehmen vorweisen kann … und geben unter Umständen Anreize für die Einführung neuer Sicherheitskontrollen.

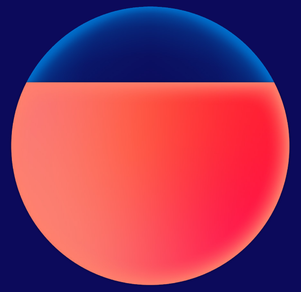
Experte für Cyberversicherungen bei einem führenden Versicherungsmakler

Cyberversicherte berichten, dass Identity-Security-Funktionen den größten Einfluss auf Bewertungen haben



25%

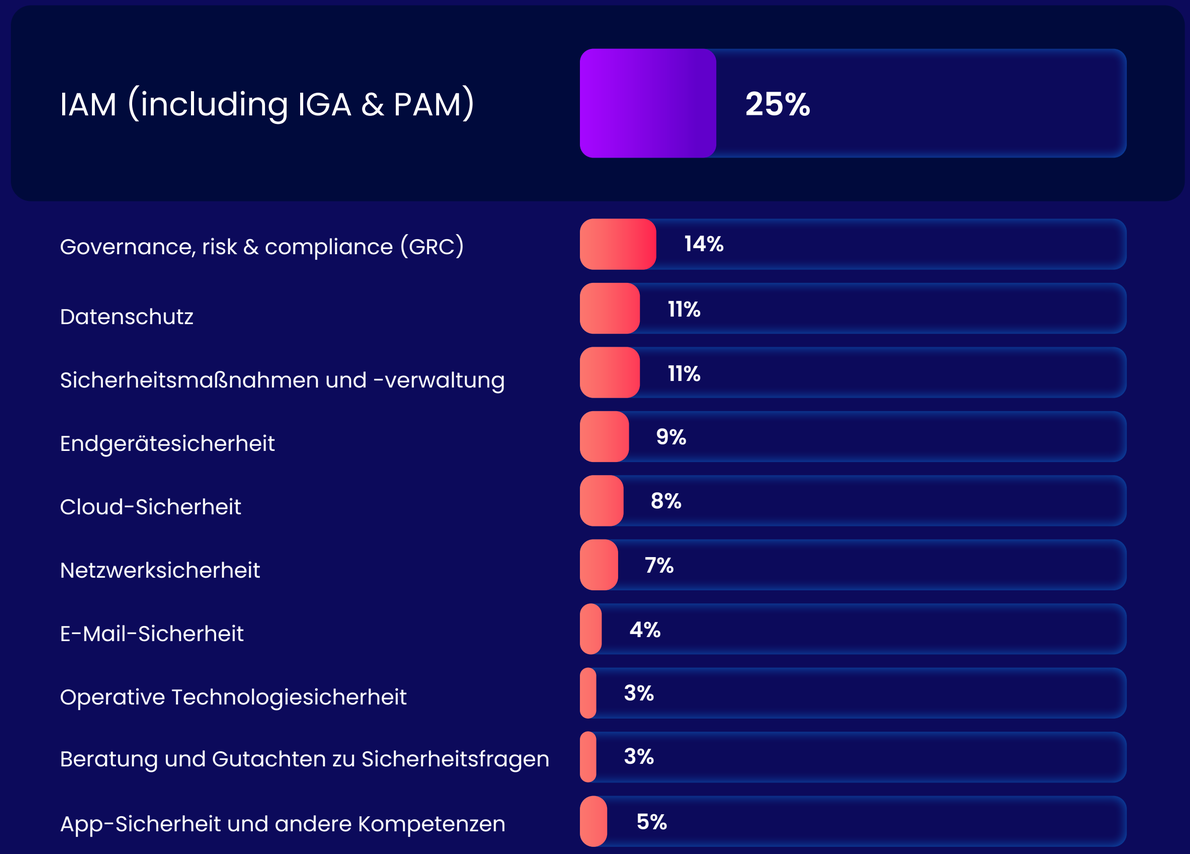
der Befragten betrachten IAM als den wichtigsten Aspekt bei der Bewertung von Cyberversicherungen, der größte Anteil



73%

der Cyberversicherten betrachten IAM-Funktionen als einen der drei wichtigsten Einflussfaktoren für die Versicherungsbewertung

Kompetenzen im Bereich Cybersicherheit, die sich am stärksten auf die Risikobewertung von Cyberversicherungen auswirken, % der Befragten, die der Fähigkeit die größte Wirkung zuschreiben



Einschließlich Web-Sicherheit und MSSP/Outsourcing

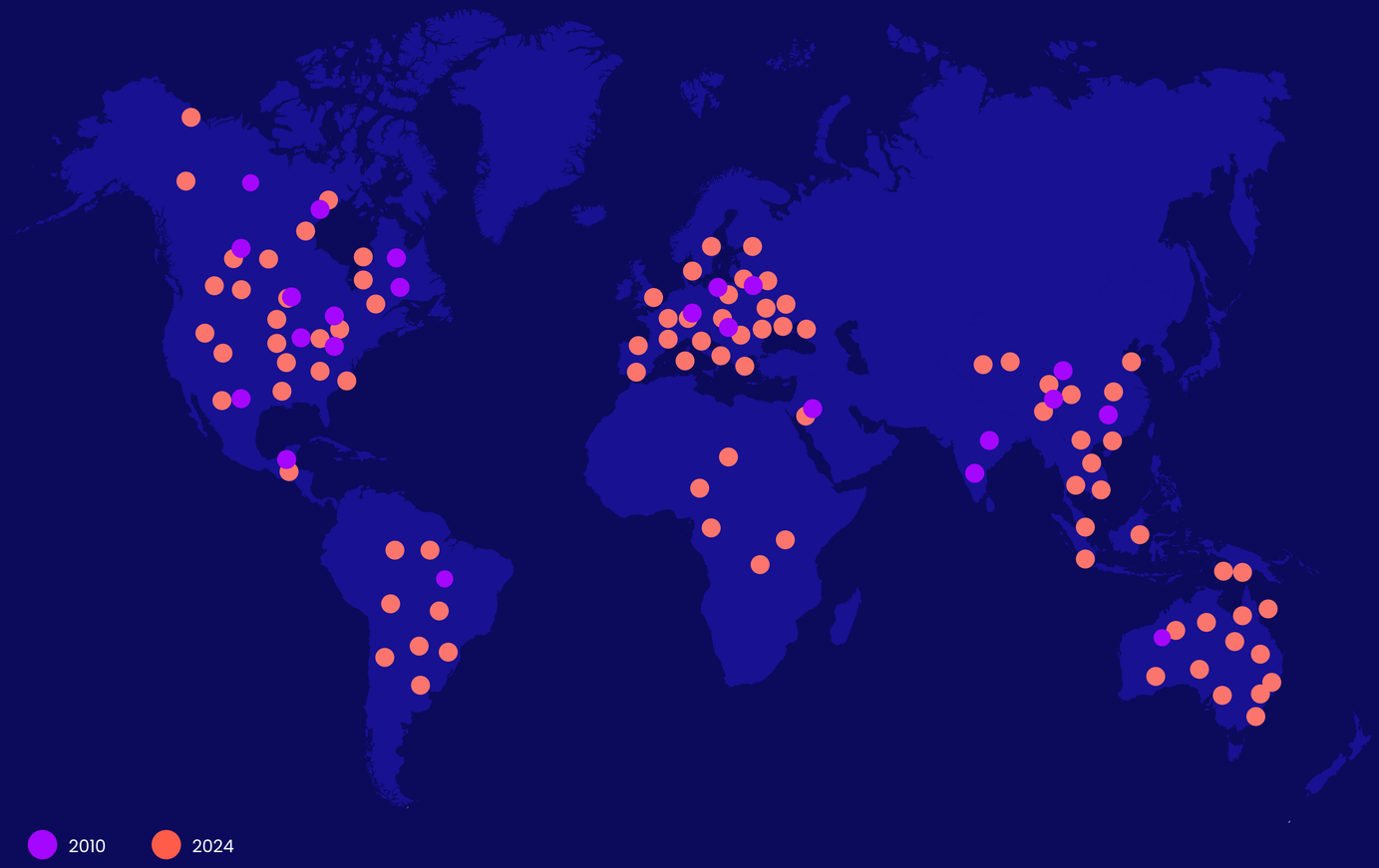
Identity-bezogene Vorschriften haben sich seit 2010 regions- und branchenübergreifend versiebenfacht

Mehr als 5-fache Zunahme

der Vorschriften für Branchen außerhalb des Finanz- und Gesundheitswesens

Mehr als 13-fache Zunahme

der Vorschriften außerhalb von Nordamerika, APAC und Europa

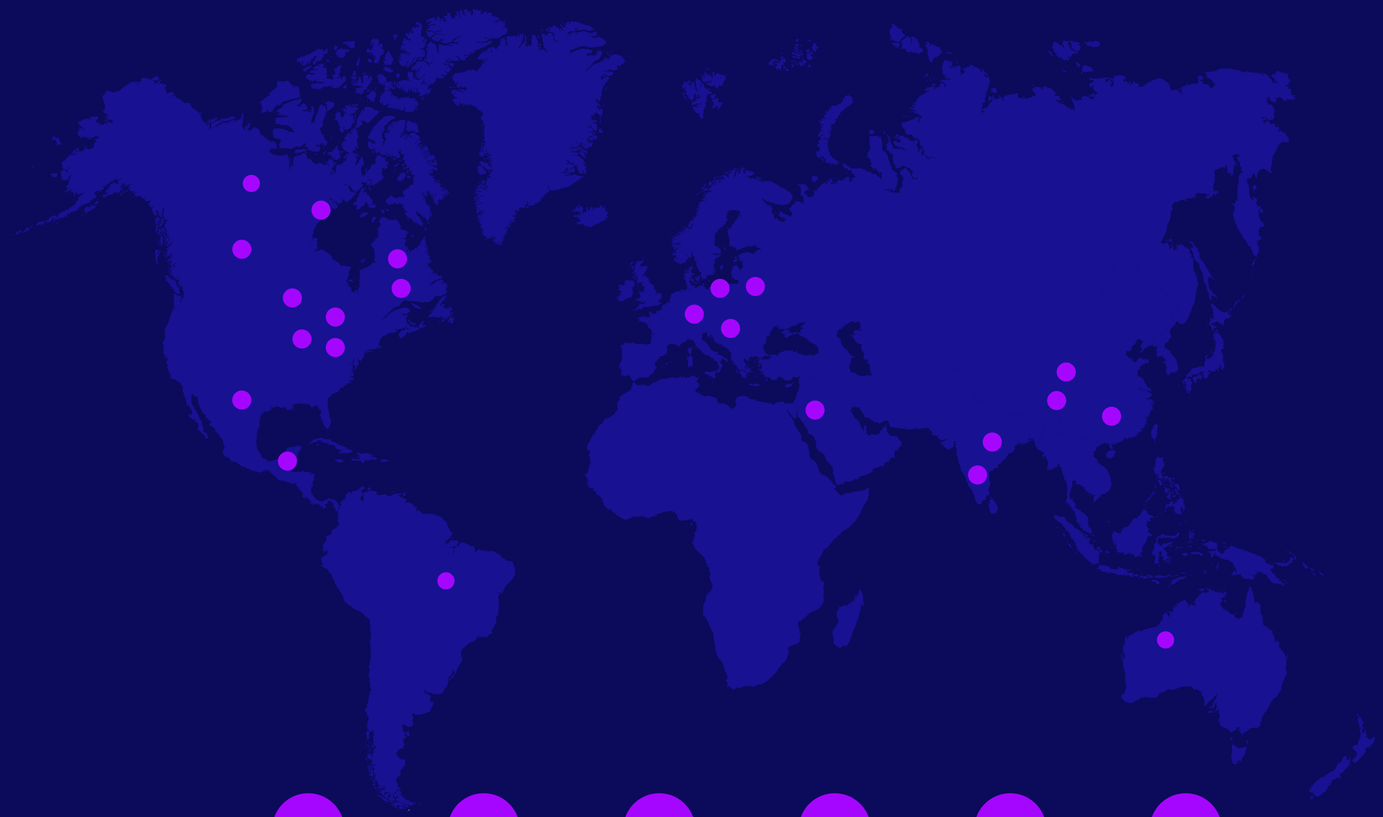


Identity-bezogene Vorschriften haben sich seit 2010 regions- und branchenübergreifend versiebenfacht

~25

Vorschriften und Frameworks konzentrierten sich 2010 auf entwickelte Regionen und ausgewählte Branchen

Alle | 2010 | 2024



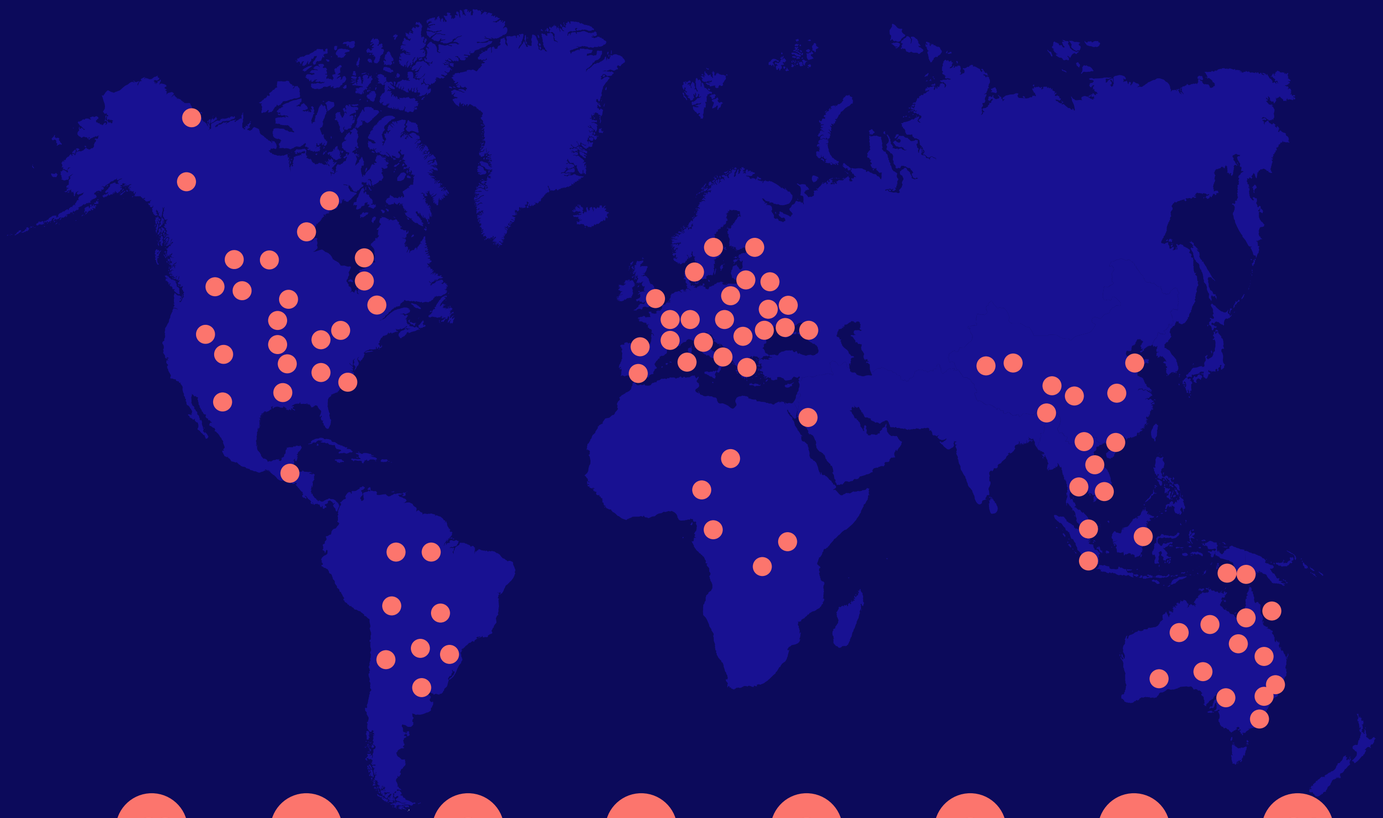
18	2	2	1	1	23
Nicht branchen-zugehörig	Telecom	Gesundheits-wesen	Finanzwesen	Fertigung	Gesamt

Identity-bezogene Vorschriften haben sich seit 2010 regions- und branchenübergreifend versiebenfacht

~135

Vorschriften und Frameworks im Jahr 2024 mit erheblichem Wachstum in allen Regionen und Branchen

Alle | 2010 | 2024



103	11	9	5	3	2	1	134
~6x	~5x	9x	~3x	3x			
Nicht branchen-zugehörig	Telecom	Finanz-wesen	Gesundheits-wesen	Fertigung	Sonstige	Regierung	Gesamt

KAPITEL 4

Wie es führenden Unternehmen gelingt, den Trend umzukehren.

Kapitel starten →

Fallstudien von Unternehmen

Überall auf der Welt und in allen Branchen investieren führende Unternehmen in Identity Security, um die Wertkurve der Cybersecurity zu „biegen“. Sie erzielen überdurchschnittliche Renditen in den Bereichen Compliance, betriebliche Effizienz, Benutzerproduktivität und Sicherheit.

BNP PARIBAS

Ziel:

Cyberrisiko senken und Produktivität steigern

BNP Paribas Bank Polska konnte durch die weitreichende Automatisierung manueller IAM-Aufgaben die Produktivität steigern.

Nach mehreren Fusionen verwaltete die Bank 10.000 Benutzer und etwa 1.000 Anwendungen über getrennte IAM- Programme. Das IT-Team war ohne Automatisierung nicht in der Lage, die zahlreichen Benutzeranfragen und IAM-Aufgaben zu bewältigen. Dank Automatisierung werden nun alle Zertifizierungskampagnen von nur zwei Mitarbeitern verwaltet, die jeweils nur etwa 15 % ihrer Arbeitszeit dafür aufwenden müssen.

Fallstudie ansehen →

40K

automatisierte Identity-Aufgaben im Monat

90%

der Berechtigungs-anforderungen werden automatisch ausgeführt

4K

automatische Zurücksetzungen und Passwortänderungen im Monat

Ziel:

Produktivität

Ein führendes Pharmaunternehmen mit 72.000 Mitarbeitern steigerte seine Produktivität und Effizienz durch die Automatisierung von IAM-Aufgaben.

Das Unternehmen war auf der Suche nach einem skalierbaren, Cloud-basierten System zur Ablösung seiner veralteten On-Premise-Identity-Lösung, die einen erheblichen manuellen Wartungsaufwand erforderte. Durch das Onboarding eines neuen Cloud-basierten Systems konnte das Unternehmen die regulatorische Compliance vereinfacheund den Zeitaufwand für Zugriffsbewertungen und Wartezeiten auf Zugriffsrechte erheblich reduzieren.

40%

weniger Zeitaufwand für Zugriffs-bewertungen

20%

kürzere Wartezeit auf den Zugriff

30%

weniger manuelle Aufgaben für die IT-Abteilung

Ziel:

Gesteigerter Geschäftswert

Absa, ein panafrikanisches Finanzinstitut mit über 35.000 Mitarbeitern, konnte das Onboarding und die Verwaltung von externen Identitäten optimieren und gleichzeitig die Kosten senken.

Um die Anforderungen der DSGVO und des POPIA zu erfüllen, setzte die Bank ein KI-gestütztes Risikomanagement-Tool mit zeitgerechter Bereitstellung und standardisierter Zertifizierung für Identitäten für Dritte ein. Durch dieses risikobasierte Zugriffsmodell konnten die Betriebskosten gesenkt und die Identity Governance für Auftragnehmer und Nicht-Mitarbeiter vereinfacht werden.

Fallstudie ansehen →

$300
Einsparungen je eingerichteter Identity

15
Tage kürzeres Onboarding für Identitäten Dritter

12K
Nicht-Mitarbeiter mit sicheren Identitäten ausgestattet

currys

Ziel:

Geringeres Cyberrisiko

Currys, ein britischer Elektronikhändler mit über 800 Filialen, konnte sein Risikoprofil durch eine bessere Identity Governance und automatisierte Identity Security senken.

Sein bisheriger Ansatz, bei dem ein ständig wechselnder Mitarbeiterpool Excel-basierte manuelle Prozesse durchführte, führte zur Einrichtung von übermäßigen Berechtigungen und zu Compliance-Risiken. Dank der Automatisierung ist nun ein vollständiger Audit-Pfad vorhanden, wodurch Compliance-Probleme und nicht umgesetzte Berechtigungen minimiert werden und gleichzeitig die allgemeine Sicherheitslage verbessert wird.

Fallstudie ansehen →

3-fache

Risikoreduzierung durch die Vergabe angemessener Berechtigungen für etwa 6.000 Konten

210

eingesparte Stunden manueller Arbeit pro Jahr

24K

verwaltete Identitäten

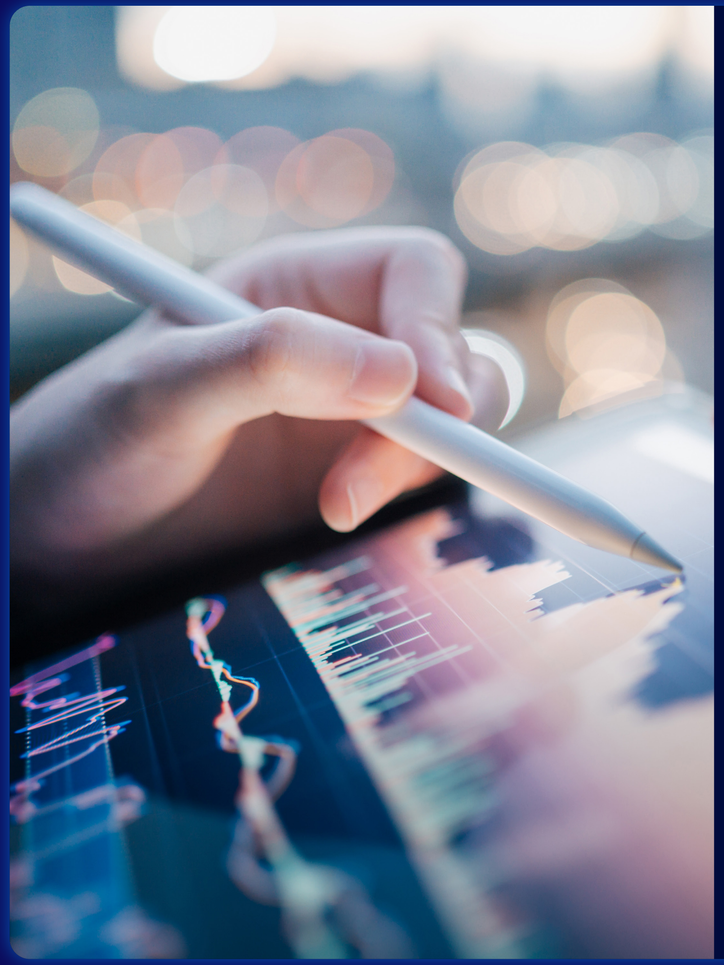
Dem globalen Technologiekonzern Aboitiz gelang es mit einer umfassenden Transformationsinitiative, innerhalb von 24 Monaten von Horizont 1 zu Horizont 3+ aufzusteigen

Bewegen Sie den Cursor über die einzelnen Abschnitte, um die ergriffenen Maßnahmen anzuzeigen

0 formale Verfahren für das Identity & Access Management	**21** Tage für die Deaktivierung und 5 Tage für die Aktivierung von Benutzerkonten	**<5** Geschäftseinheiten mit zentralisierter Identity Governance	**<1K** Konten, die mit automatisierten Prozessen verwaltet werden
1 durchgängiges Identity-and-Access-Management-Programm zur Verwaltung aller Mitarbeiterkonten	**0** Wartezeit mit sofortiger Bereitstellung und Aufhebung von Zugriffsrechten	**47** Geschäftseinheiten mit zentraler Verwaltung von etwa 23.000 Anwendungskonten	**144K** automatisierte Kontoänderungen und-überprüfungen

Horizon 1 (2020)
Horizon 3+ (2022)

Fallstudie ansehen →



“

Wir fingen bei null an. Aber das eröffnete uns die Möglichkeit, mithilfe von Technologie einen Sprung nach vorne zu machen … Wir fassten den Entschluss, Zeit und Arbeit in das wertvollste Asset unseres Unternehmens zu investieren: die Identität.

CISO, Aboitiz Equity Ventures

aboitiz

KAPITEL 5

Ihr Weg zum nächsten Horizont.

Kapitel starten →

Ihr Weg zum nächsten Horizont

1. Eine Vision festlegen
2. In die richtigen Lösungen investieren, vor allem in KI-gestützte Lösungen, die eine rasche Fortentwicklung über die Horizonte und höhere Renditen ermöglichen
3. Alle Arten von Identitäten sichern
4. IAM mit breiter angelegten Sicherheitsmaßnahmenum eine kontinuierliche Überwachung und Steuerung von Versicherungsprämien zu ermöglichen
5. Identity-Daten zur Gewinnung umsetzbarer Erkenntnisse und anpassungsfähiger Sicherheitsrichtlinien nutzen
6. Neuen Vorschriften und Standards einen Schritt vorausbleiben, um die Compliance zu wahren

SailPoint

Erfahren Sie mehr über den Reifegrad Ihrer Identity Security und den Horizont Ihres Unternehmens.

Bewertung vornehmen

Vollständigen Bericht herunterladen

IB2568-2502