PRISMA® CLOUD | paloalto® NETWORKS

Bericht zum Stand der cloudnativen Sicherheit 2022

So stellen Sie erfolgreich auf die Cloud um

Inhalt

Einleitung

Für unsere jährlichen Berichte zum Stand der cloudnativen Sicherheit werden mehr als 3.000 Personen auf der ganzen Welt zu Ihren Strategien, Ihrem Budget, Ihren Erfahrungen und Ihren Plänen bezüglich der Cloud-Einführung befragt. Ihre Antworten werfen ein Licht auf die Praktiken, Tools und Technologien, die zur Einrichtung von Cloud-Workloads und für das Management der Sicherheit cloudnativer Architekturen verwendet werden. Wie im Bericht für 2020 ist es dabei unser Ziel, die Maßnahmen und die damit korrelierenden Ergebnisse von Unternehmen, die ihre Cloud-Initiative erfolgreich umgesetzt haben, sowie von Unternehmen, die damit weniger erfolgreich waren, hervorzuheben. Eine entscheidende Rolle scheint dabei das Vorgehen der Unternehmen in puncto Cloud-Sicherheit zu spielen. Dazu zählen Unterschiede bei der Implementierung von Technologien und Prozessen zur Unterstützung eines hohen Sicherheitsniveaus (definiert als die Wirksamkeit der Maßnahmen für die Cloud-Sicherheit) und niedriger Nebenwirkungen der Sicherheitsmaßnahmen (definiert als das Maß, in dem die Cloud-Sicherheit den Betrieb einschränkt).

Es überrascht wahrscheinlich nicht, dass die COVID-19-Pandemie sowohl die Erweiterung der Cloud als auch die resultierenden Ergebnisse beeinflusst hat (siehe hierzu den Kasten „Die anhaltende Wirkung von COVID-19“). Zwar reagierten Unternehmen während der Pandemie schnell auf den erhöhten Bedarf an Cloud-Bereitstellungen, doch mühen sich viele immer noch damit ab, die Cloud-Sicherheit zu automatisieren und Cloud-Sicherheitslücken zu bekämpfen. Trotzdem hält die Migration in die Cloud für Unternehmen in jeder Phase an – von jenen, die sich Cloud-Funktionen neu erschließen, bis hin zu jenen, die in der Cloud gegründet wurden.

Dieser Bericht identifiziert Muster bei den Ansätzen und Ergebnissen, die eine Kategorisierung in drei repräsentative Gruppen ergeben: moderate Nutzer, schnelle Erweiterer und etablierte Nutzer. Diese Gruppen ergeben sich aufgrund von Merkmalen wie der Größe der Cloud-Umgebung, den Zielen bei der Transformation und betrieblichen Strategien. Wir stellen diese Gruppen hier in Zusammenhang mit umfangreichen Daten und Analysen ihrer Verhaltensweisen vor. Dies soll den Lesern dabei helfen, ihr eigenes Unternehmen einzuordnen und gängige Herausforderungen und Strategien zu identifizieren, die sich auf die Ergebnisse auswirken. Unabhängig vom Reifegrad der Cloud-Bereitstellung Ihres Unternehmens, von der Branche, der Region oder den Zielen bei der Cloud-Migration, geben Ihnen die Erkenntnisse in diesem Bericht wertvolle Informationen für die Planung Ihrer Cloud-Erweiterung.

Kurzfassung

So wie sich die besonderen Funktionen der Cloud weiterentwickeln, entwickelt sich auch die Art und Weise, wie wir die Cloud nutzen, um unser Geschäft voranzubringen. Aus diesem Grund enthält dieser Bericht auch Untersuchungsergebnisse, die sich speziell auf die wichtigsten Bedenken und Routinesituationen in Zusammenhang mit cloudnativer Sicherheit beziehen, darunter Automatisierung, DevSecOps, Sicherheitsniveau, Nutzung von Open-Source-Lösungen und weitere. Unser Ziel bei der Verfassung dieses Berichts ist jedes Jahr dasselbe: Ihnen wertvolle Erkenntnisse für die Ausrichtung Ihrer Cloud- und Sicherheitsstrategie an die Hand zu geben – so auch 2022 und darüber hinaus.

Cloud-Erweiterung und -Strategie

- Unternehmen haben ihre **Nutzung der Cloud während der Pandemie** schnell **um insgesamt mehr als 25 Prozent ausgebaut**, hatten dabei aber Mühe mit umfassender Sicherheit, Compliance und technischer Komplexität.
- Unternehmen stand für die Erweiterung ein kleineres Budget zur Verfügung: **39 Prozent der Unternehmen investierten weniger als 10 Mio. USD in ihre Cloud** (ein Anstieg um 16 Prozentpunkte gegenüber 2020) und **nur 26 Prozent investierten mehr als 50 Mio. USD** (ein Rückgang um 17 Prozentpunkte gegenüber 2020).
- Unternehmen nutzen weiterhin verschiedene IT-Optionen, doch **Platform-as-a-Service-(PaaS-) und serverlose Ansätze nahmen um 20 Prozentpunkte zu**, wahrscheinlich zur Unterstützung der raschen Umstellung auf die Cloud, während die Nutzung von Containern und Containers-as-a-Service (CaaS) ein mäßigeres Wachstum verzeichneten.

Sicherheitsniveau und Nebenwirkungen

- **Unternehmen mit einem hohen Sicherheitsniveau sind mit mehr als doppelt so hoher Wahrscheinlichkeit weniger von Nebenwirkungen der Sicherheitsmaßnahmen betroffen**, d. h. förderlichen oder beschränkenden Auswirkungen auf den Geschäftsbetrieb. Dies unterstreicht die Notwendigkeit eines zweigleisigen Ansatzes für die Cloud-Sicherheit mit wirksamen Sicherheitsfunktionen, die andere Teams außerhalb der Sicherheitsdienste nicht beeinträchtigen.
- Unternehmen mit erstklassigen Sicherheitsprozessen haben den größten Nutzen hinsichtlich der Produktivität und Zufriedenheit ihrer Mitarbeiter. **80 Prozent der Unternehmen mit hohem Sicherheitsniveau und 85 Prozent der Unternehmen mit geringen Nebenwirkungen berichteten von einer Steigerung der Mitarbeiterproduktivität**.
- 55 Prozent der befragten Unternehmen schätzen ihr Sicherheitsniveau als schwach ein. Sie sind zudem davon überzeugt, dass sie zur Stärkung ihrer Sicherheitslage bestimmte grundlegende Ziele erreichen müssen, darunter cloudübergreifende Transparenz, konsistente Governance für alle Konten oder straffere Incident-Response- und Untersuchungsprozesse.
- **80 Prozent der Unternehmen, die hauptsächlich Open-Source-Sicherheitstools verwenden, haben ein niedriges oder sehr niedriges Sicherheitsniveau** gegenüber 26 Prozent der Unternehmen, die hauptsächlich die Sicherheitstools ihres Cloud-Serviceanbieters nutzen, und 52 Prozent der Unternehmen, die Lösungen von Drittanbietern einsetzen. Diese Zahlen unterstreichen, dass eine Plattform, die ein Flickwerk aus unterschiedlichen Tools ist, für das Unternehmen ein höheres Risiko bedeutet.

Sicherheitsfördernde Faktoren

- Unternehmen konsolidieren ihren Sicherheitsansatz. **Knapp drei Viertel verwenden höchstens zehn Sicherheitstools** und die **Zahl der Unternehmen, die höchstens fünf Sicherheitsanbieter nutzen, ist gegenüber 2020 um 27 Prozentpunkte gestiegen**. Dies legt nahe, dass sie mehr Sicherheitsdienste von weniger Sicherheitsanbietern beziehen.
- **Unternehmen mit einem hohen Grad der Sicherheitsautomatisierung haben mit doppelt so hoher Wahrscheinlichkeit geringe Nebenwirkungen und ein hohes Sicherheitsniveau** wie Unternehmen mit einem niedrigen Grad der Sicherheitsautomatisierung.
- Wie gut Unternehmen DevSecOps-Methoden übernommen und umgesetzt haben, ist der Hauptindikator für erstklassige Sicherheit. **Unternehmen, die DevSecOps-Prinzipien eng integriert haben, haben mit einer mehr als 7-fachen Wahrscheinlichkeit ein hohes oder sehr hohes Sicherheitsniveau und mit einer mehr als 9-fachen Wahrscheinlichkeit nur geringe Nebenwirkungen der Sicherheitsmaßnahmen**.

Die anhaltende Wirkung von COVID-19

„Schnelle Cloud-Skalierung und Komplexität ohne automatisierte Sicherheitsmaßnahmen, die in die gesamte Entwicklungspipeline integriert sind, sind eine gefährliche Kombination."

Die diesjährige Befragung wurde im Mai 2021 durchgeführt, also gut ein Jahr nachdem die COVID-19-Pandemie die Bevölkerungen ganzer Länder in die Selbstabschottung zu Hause geschickt hatte. Die Umfrageteilnehmer berichteten von Geschäftsentscheidungen im Verlauf der letzten zwölf Monate (Juni 2020 bis Juni 2021), einem Zeitraum mit den weltweit schwersten gesellschaftlichen und wirtschaftlichen Umwälzungen seit dem Zweiten Weltkrieg. Die Entscheidungen dieser Unternehmen erfolgten in Reaktion auf dramatische und unerwartete Veränderungen der Nachfrage nach Servicebereitstellung in der Cloud, die nahezu gleichzeitig die ganze Welt und alle Branchen betrafen:

- Die schnelle Umstellung auf Onlinearbeit und -unterricht sowie Remote-Gesundheitsversorgung führte zu einem rapiden Anstieg der Nutzung von Tools für Onlinezusammenarbeit und -meetings.
- Die Nachfrage nach Bereitstellung wichtiger Geschäftsanwendungen in der Cloud stieg plötzlich steil an.
- Verbraucher wechselten flächendeckend zu Onlineshopping und Gastronomielieferdiensten.
- Die Nachfrage nach Support für die Cloud-Infrastruktur für alles Mögliche von sozialen Dienstleistungen bis hin zum Lieferkettenmanagement nahm stark zu.

Und während sich Unternehmen bemühten, dieser neuen und unerwarteten Anforderungen möglichst schnell Herr zu werden, sahen sie sich zugleich einer weiteren globalen Bedrohung ausgesetzt: Cyberattacken. Wie Unit 42 von Palo Alto Networks in einem Cloud Threat Report über COVID feststellte, korrelierte ein explosionsartiger Anstieg der Sicherheitsvorfälle mit den erhöhten Investitionen von Unternehmen in die Cloud, die in den ersten sechs Monaten der Pandemie einsetzten. Dies führte zu dem Schluss, dass „schnelle Cloud-Skalierung und Komplexität ohne automatisierte Sicherheitsmaßnahmen, die in die gesamte Entwicklungspipeline integriert sind, eine gefährliche Kombination sind". Zum Zeitpunkt der Verfassung des vorliegenden Berichts dauert die Pandemie noch an. Unternehmen migrieren weiterhin Workloads in die Cloud, während sie immer noch Mühe mit der Automatisierung der Cloud-Sicherheit und Eindämmung von Cloud-Risken haben.

Der weltweite Stand der Cloud und cloudnativen Sicherheit

Im ersten Abschnitt dieses Berichts untersuchen wir die allgemeinen Trends bei der Cloud-Nutzung und Sicherheitsmaßnahmen in der Cloud, wie Unternehmen auf der ganzen Welt sie uns berichtet haben. (Weitere Angaben zu den Umfrageteilnehmern finden Sie im Abschnitt „Methodik und demografische Daten".)

Wachstum der Cloud in der Pandemie

Im Verlauf der Pandemie kam es zu einem signifikanten **Anstieg des Anteils der Workloads in der Cloud auf durchschnittlich 59 Prozent** der gesamten Workloads gegenüber durchschnittlich 46 Prozent im Jahr 2020. **Außerdem führen 69 Prozent der Unternehmen mehr als die Hälfte ihrer Workloads in der Cloud aus.** 2020 lag dieser Anteil noch bei nur 31 Prozent.

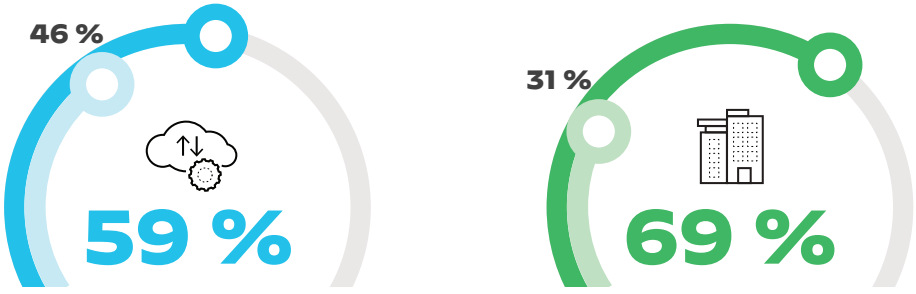


Abbildung 1: Veränderung des Anteils der Cloud-Workloads gegenüber 2020

Die Erwartungen der Unternehmen bezüglich der zukünftigen Cloud-Nutzung haben sich gegenüber dem Vorjahr nicht wesentlich verändert. Im Durchschnitt gehen Unternehmen davon aus, binnen zweier Jahre 68 Prozent ihrer Workloads in der Cloud bereitzustellen, was in etwa dem Vorjahreswert (65 Prozent) entspricht. Dies lässt vermuten, dass Unternehmen zwar infolge der Pandemie schneller als erwartet zur Cloud wechselten, der maximale geplante Umfang der Umstellung hingegen nicht signifikant zugenommen hat.

Auch die Zusammensetzung der Cloud hat sich im Verlauf eines Jahres verändert, da Unternehmen zu privatem Hosting ihrer Cloud-Workloads wechselten. Im Durchschnitt werden nun 55 Prozent der Cloud-Workloads in privaten Clouds bereitgestellt, ein Plus von 7 Prozentpunkten gegenüber 2020. Unternehmen nutzen zwar weiterhin verschiedene IT-Optionen, doch **nahmen PaaS- und serverlose Ansätze um 20 Prozentpunkte zu, während die Nutzung von Containern und CaaS ein mäßigeres Wachstum verzeichnete**. PaaS- und serverlose Strategien, die es Entwicklungsteams ermöglichen, Anwendungen in die Cloud zu verlegen, ohne notwendigerweise zugleich die Infrastruktur einrichten und skalieren zu müssen, haben wahrscheinlich die schnelle Umstellung auf die Cloud im vergangenen Jahr unterstützt. Wir gehen davon aus, dass dieser Trend anhalten wird, und werden ihn genau beobachten.

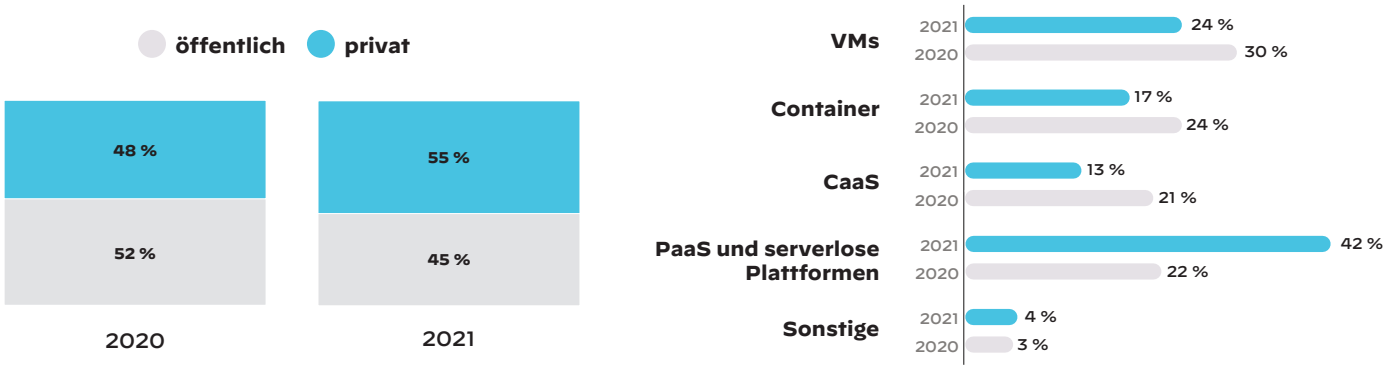


Abbildung 2: links: Anteil der in öffentlichen und privaten Clouds bereitgestellten Workloads; rechts: Anteil der Workloads nach IT-Umgebung

Die Untersuchung der Gründe, warum Unternehmen ihre Cloud-Funktionen ausbauten, ergab strategische Überlegungen als Antriebsfaktoren: Anwendungsmodernisierung, Bewahrung der Wettbewerbsfähigkeit und Eindämmung der Infrastrukturkosten. Während die Pandemie also sicherlich zu den Veränderungen im Berichtszeitraum beitrug, überwiegen diese Gründe bei der Entscheidung der Unternehmen, die Cloud überhaupt zu nutzen. Die Flexibilität und Agilität, die die Cloud Unternehmen verschafft, ermöglichen es ihnen, ihr Geschäft immer schneller weiterzuentwickeln.

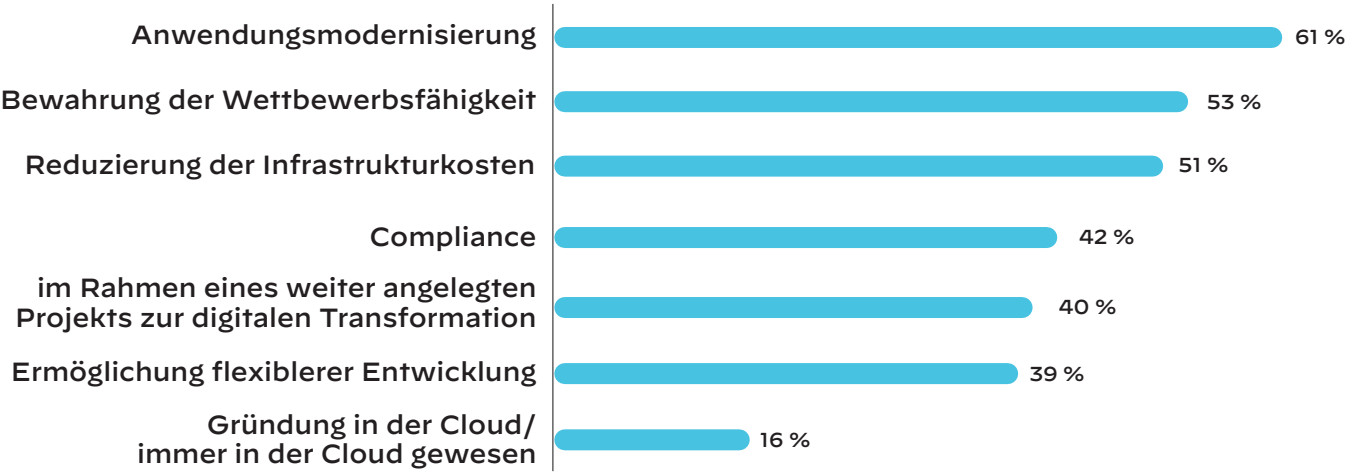
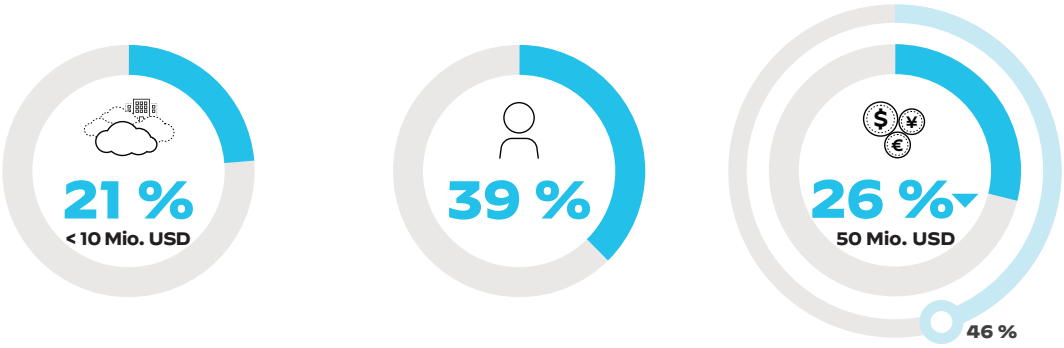


Abbildung 3: Gründe für den Ausbau der Cloud-Funktionen

Trotz des massiven Trends, mehr Workloads in die Cloud zu verlagern, stand den Unternehmen hierfür ein kleineres Budget als im Vorjahr zur Verfügung. **Im Jahr 2021 investierten 39 Prozent der Unternehmen weniger als 10 Mio. USD in ihre Cloud**, ein Anstieg um 16 Prozentpunkte gegenüber 2020, **während nur 26 Prozent mehr als 50 Mio. USD investierten**, ein Rückgang um 17 Prozentpunkte gegenüber 2020. Diese Senkung der Ausgaben für die Cloud kann die Folge allgemeiner Budgetkürzungen oder Umwidmungen von Mitteln infolge der Pandemie sein. Sie kann auch einfach eine „Normalisierung" der Cloud-Aktivitäten widerspiegeln, wobei das Budget natürlicherweise schrumpft, da die Teams mit zunehmender Erfahrung routinierter und effizienter werden.



2020 gaben **21 %** der Unternehmen weniger als 10 Mio. USD für ihre Cloud aus.

2021 galt dies für **39 %** der befragten Unternehmen.

Der Anteil der Unternehmen mit einem Cloud-Budget von über **50 Mio. USD** sank von **46 % auf 26 %**.

Abbildung 4: Veränderung der Budgets für die Cloud

Bezogen auf Branche, Region und Umsatz lassen sich zwar kleine Unterschiede bei der Cloud-Nutzung erkennen, doch weisen die Daten darauf hin, dass diese Variabilität keine wesentliche Rolle für die Gesamtergebnisse spielt. In Abbildung 5 ist dennoch eine Auswahl der auffälligeren Abweichungen zusammengefasst.

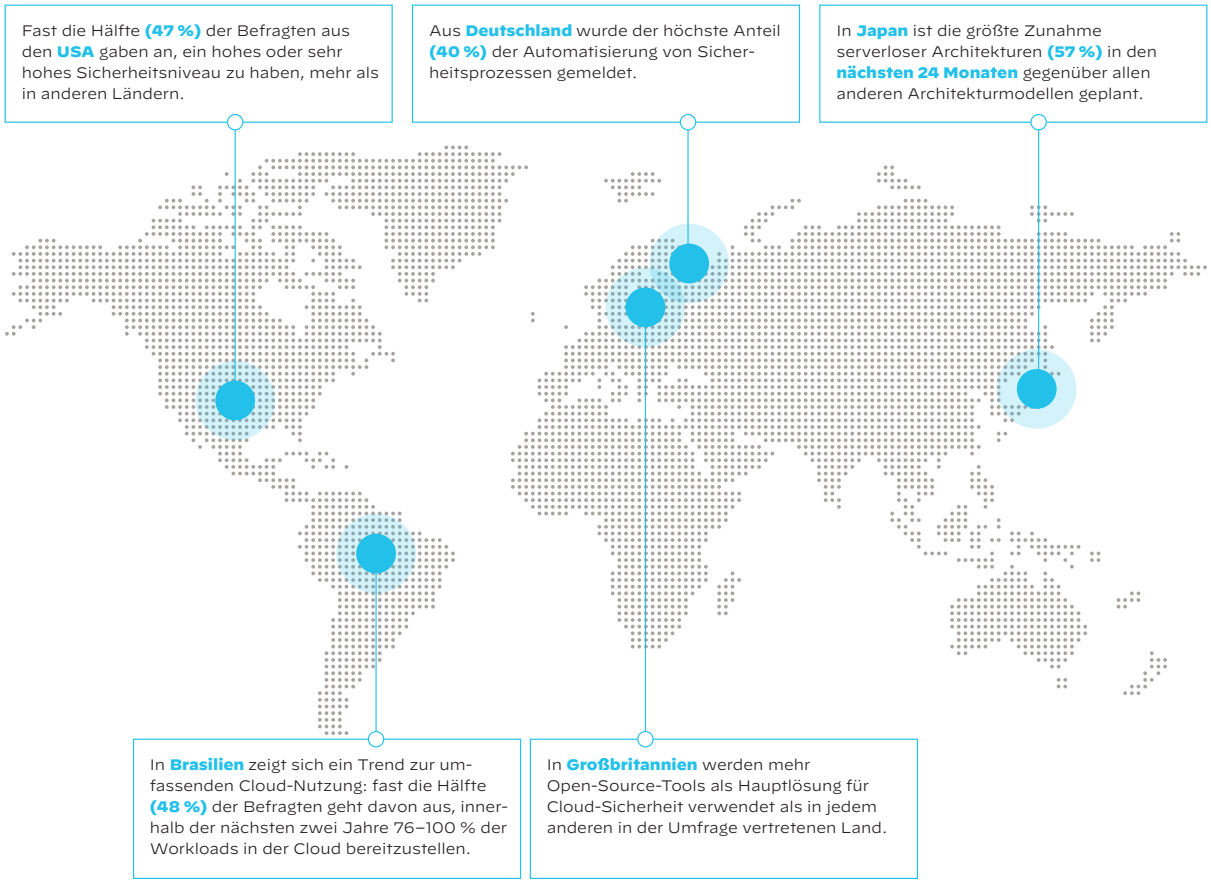


Abbildung 5: Cloud-Trends nach Weltregion

Sicherheitsherausforderungen bei der Cloud-Migration

Während der schnellen Erweiterung der Cloud-Nutzung im vergangenen Jahr stießen Unternehmen auf dieselben häufigsten Herausforderungen wie die Befragten im Vorjahr: Gewährleistung der Sicherheit, Compliance und technische Komplexität.

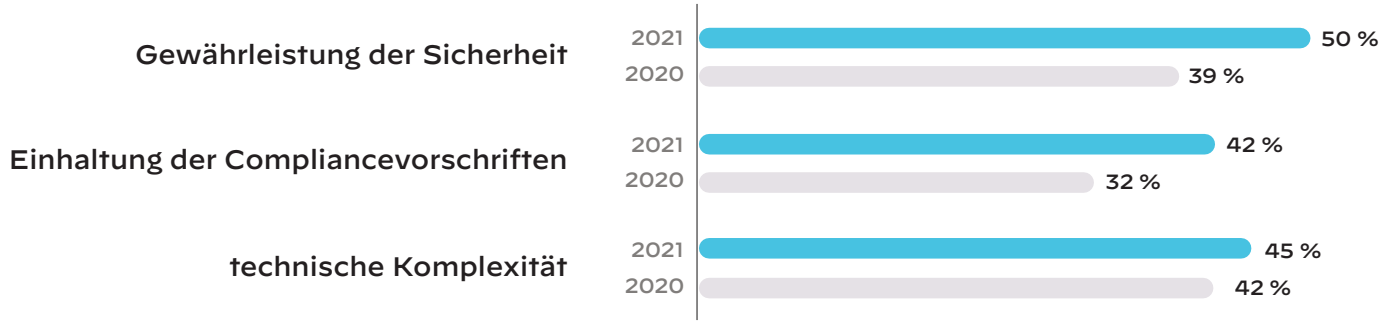


Abbildung 6: Herausforderungen bei der Cloud-Migration

Während die Cloud-Budgets insgesamt schrumpften, blieben die Budgets für die Cloud-Sicherheit gleich. Wir interpretieren dies so, dass Unternehmen ihre Gesamtausgaben für die Cloud zwar drosselten, ihr Sicherheitsbudget jedoch davon ausnahmen. Dies verdeutlicht, dass Unternehmen den Wert der Cloud-Sicherheit, um den vollen Nutzen aus der Cloud ziehen zu können, kennen.

Im Berichtszeitraum **vergrößerten Unternehmen ihre Cloud-Sicherheits-teams während der Pandemie. 53 Prozent der Unternehmen gaben an, dass ihr Sicherheitsteam aus mehr als 30 Mitarbeitern bestehe, gegenüber 41 Prozent im Jahr zuvor.** Unternehmen konsolidierten im Rahmen der Erweiterung ihrer Cloud-Umgebungen auch ihre Anbieter von Cloud-Sicherheit. Die Daten zeigen, dass die Zahl der Unternehmen, die höchstens fünf Sicherheitsanbieter nutzen, um 27 Prozentpunkte anstieg, während die Zahl derjenigen, die sechs bis zehn Sicherheitsanbieter nutzen, gegenüber dem Vorjahr um 19 Prozentpunkte gesunken ist.

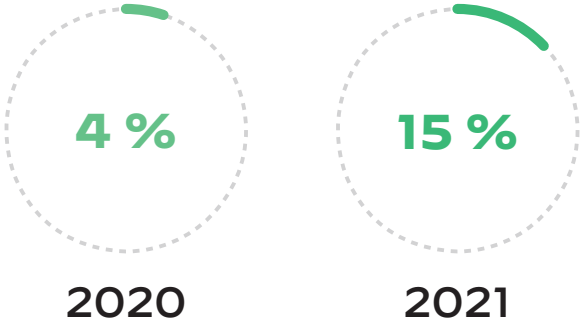


Abbildung 7: Anteil der Befragten, die mehr als 20 % ihres Cloud-Budgets für Sicherheit ausgeben

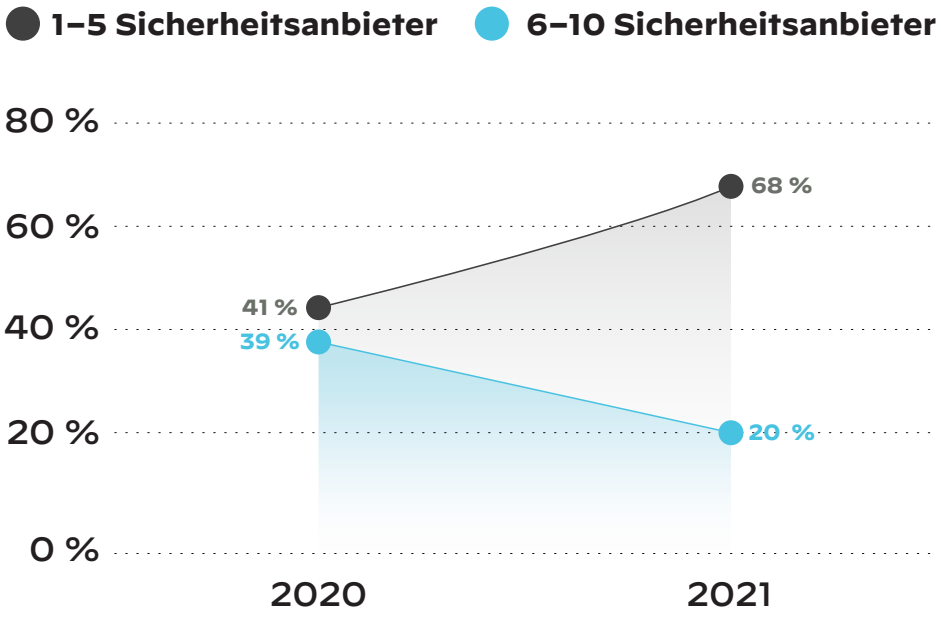


Abbildung 8: Veränderungen der Zahl der Sicherheitsanbieter

Zwar reduzierten Unternehmen die Zahl der Sicherheits*anbieter*, mit denen sie zusammenarbeiten, die Zahl der Sicherheits*tools*, die sie nutzen, hat sich hingegen im Vergleich zum Vorjahr nur minimal verändert. Wir definieren Cloud-Sicherheitsanbieter als jedes Unternehmen, mit dem ein Unternehmen zum Schutz seiner Clouds zusammenarbeitet, und Sicherheitstools als die Zahl der Fähigkeiten und Funktionen, die diese Cybersicherheitsunternehmen anbieten. **Knapp drei Viertel der Unternehmen verwenden höchstens zehn Sicherheitstools**, was darauf hindeutet, dass sie mit weniger Sicherheitsanbietern zusammenarbeiten, um ein breites Spektrum von Sicherheitsanforderungen zu erfüllen. Diese Konsolidierung untermauert Beobachtungen, dass es bei Unternehmen, die unterschiedlichste Tools von zahlreichen Anbietern nutzen, zu „blinden Flecken" kommen kann, die ein erhöhtes Risiko mit sich bringen und zusätzliche Anstrengungen erforderlich machen, um die Lücken zu schließen. Die 28 Prozent der Unternehmen, die immer noch eine große Zahl unterschiedlicher Tools verwenden, darunter 8 Prozent, die 21 bis über 50 Tools nutzen, möchten wir an dieser Stelle vor den möglichen Folgen warnen.

Von den Unternehmen, die 21 oder mehr Sicherheitstools verwenden, beziehen fast alle (91 Prozent) ihre Tools von sechs oder mehr Anbietern. Um so viele Tools gleichzeitig managen zu können, setzen diese Unternehmen größere Teams für die Verwaltung und Unterstützung der Sicherheit ihrer Cloud-Workloads ein. Knapp die Hälfte (49 Prozent) beschäftigt sogar über 50 Mitarbeiter für die Verwaltung der Cloud-Sicherheit. Daher überrascht es wahrscheinlich nicht, dass eine höhere Zahl von Tools mit größerer Wahrscheinlichkeit bei Unternehmen mit höherem Umsatz zu finden ist. Von den Befragten, die für Unternehmen mit einem Umsatz von 1 Milliarde USD oder mehr arbeiten, gaben 11 Prozent an, 21 oder mehr Tools zu nutzen, während dies nur bei 3 Prozent der Befragten, die für Unternehmen mit einem Umsatz von weniger als 1 Milliarde USD arbeiten, der Fall war.

Organisatorische Merkmale einer hohen Erfolgsquote

Neben der variierenden Nutzung von Sicherheitsanbietern und -tools untersuchten wir auch die organisatorischen Sicherheitsmerkmale, die das Fundament einer erfolgreichen Cloud-Erweiterung bilden. Die Untersuchungen unterstreichen die wesentlichen Elemente cloudnativer Sicherheit, Antriebsfaktoren für erstklassige Sicherheit und die Bedeutung der Sicherheit für den unternehmerischen Erfolg im Großen und Ganzen.

Um an und für sich sehr unterschiedliche Unternehmen vergleichbar zu machen, betrachteten wir zwei entgegengesetzte Sicherheitsattribute:

- Das Sicherheitsniveau gibt an, wie die Unternehmen die Wirksamkeit ihrer Maßnahmen für die Cloud-Sicherheit beurteilen.
- Nebenwirkungen sind ein Maß dafür, wie sehr die Cloud-Sicherheit nach Einschätzung des Unternehmens den Geschäftsbetrieb unterstützt oder beschränkt.

Zur Ermittlung des Cloud-Sicherheitsniveaus wurden die Umfrageteilnehmer gebeten, den Grad ihrer Zustimmung zu sechs Aussagen anzugeben. Je stärker die Zustimmung zu den Aussagen ausfiel, desto höher wurde das Cloud-Sicherheitsniveau des Unternehmen wahrgenommen. Die Befragung ergab für eine leichte Mehrheit (55 Prozent) der Unternehmen ein niedriges Sicherheitsniveau. Genauer gesagt, glaubt diese Mehrheit, dass die Grundlagen effektiver sein müssten, etwa cloudübergreifende Transparenz, konsistentere Governance aller Konten oder Vereinheitlichung von Bedrohungsabwehr und -untersuchung.

Sicherheitsniveau und -ausgaben

Unternehmen mit einem hohen Sicherheitsniveau haben in der Regel höhere Sicherheitsausgaben. Mehr als zwei Drittel der Unternehmen mit hohem oder sehr hohem Sicherheitsniveau investierten mindestens 16 Prozent ihres Cloud-Budgets in die Sicherheit. Von den Unternehmen mit einem niedrigen oder sehr niedrigen Sicherheitsniveau gaben weniger als ein Fünftel einen ebenso hohen Anteil ihres Cloud-Budgets für die Sicherheit aus. Die Gruppe mit „hohem Sicherheitsniveau" scheint auch eine Erhöhung ihrer Ausgaben für die Sicherheit zu planen. Fast drei Viertel (71 Prozent) der Unternehmen mit einem hohen oder sehr hohen Sicherheitsniveau beabsichtigen, in den nächsten zwölf Monaten mindestens 16 Prozent ihres Cloud-Budgets in die Sicherheit zu investieren, gegenüber 46 Prozent aus der Gruppe mit einem niedrigen oder sehr niedrigen Sicherheitsniveau.

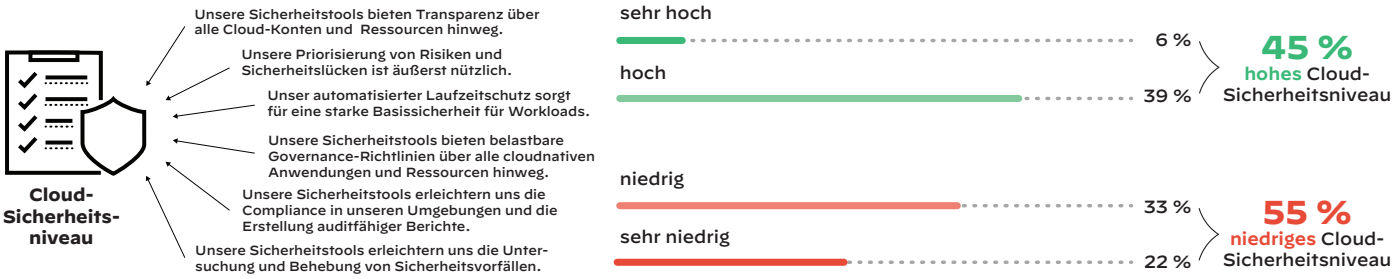


Abbildung 9: links: Faktoren, die das Sicherheitsniveau beeinflussen; rechts: Anteil der Unternehmen mit einem hohen bzw. niedrigen Sicherheitsniveau

Zur Untersuchung von Nebenwirkungen der Cloud-Sicherheit fragten wir die Umfrageteilnehmer, inwieweit sie zwei Aussagen über geschäftliche Auswirkungen infolge der Cloud-Nutzung und -Sicherheit zustimmen. Je stärker die Zustimmung zu den Aussagen ausfiel, desto stärker war der Gesamteindruck von Nebenwirkungen der Cloud-Sicherheit im Unternehmen. Die Befragung ergab, dass **nur knapp die Hälfte (48 Prozent) der Unternehmen die Nebenwirkungen der Sicherheit als gering beurteilt**.

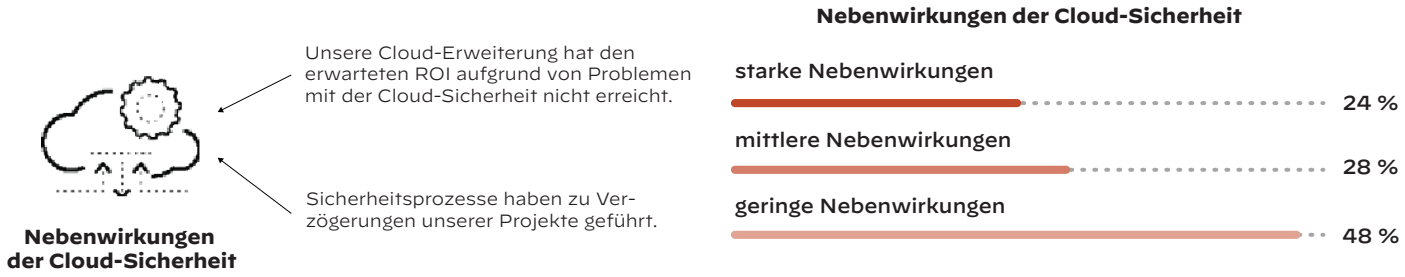


Abbildung 10: links: Faktoren, die zu Beeinträchtigungen der geschäftlichen Ziele führen; rechts: Anteil der Unternehmen mit starken, mittleren oder geringen Nebenwirkungen

Betrachtet man diese beiden Kriterien zusammen, wird deutlich, dass geringe Nebenwirkungen ganz wesentlich sind, um ein höheres Sicherheitsniveau zu erreichen. **Unternehmen mit einem hohen Sicherheitsniveau sind mit mehr als doppelt so hoher Wahrscheinlichkeit weniger von Nebenwirkungen der Sicherheitsmaßnahmen betroffen.** Dies unterstreicht die Notwendigkeit eines zweigleisigen Ansatzes: Unternehmen sollten zwar möglichst wirksame Sicherheitsfunktionen anstreben, müssen dabei aber sicherstellen, dass diese Tools und Prozesse die Geschäftsabläufe nicht behindern.

Abbildung 11: Anteil der Unternehmen mit „geringen Nebenwirkungen" mit niedrigem bzw. hohem Sicherheitsniveau

Abgesehen von einem optimalen Betrieb gibt es weitere Vorteile erstklassiger Sicherheit. Unternehmen, die ein hohes Sicherheitsniveau und geringe Nebenwirkungen ermöglichen, gewinnen am meisten hinsichtlich der Produktivität und Zufriedenheit ihrer Mitarbeiter: **Mehr als 80 Prozent der Unternehmen mit geringen Nebenwirkungen ihrer Sicherheitsmaßnahmen berichteten von einer Zunahme oder deutlichen Zunahme der Mitarbeiterzufriedenheit.**

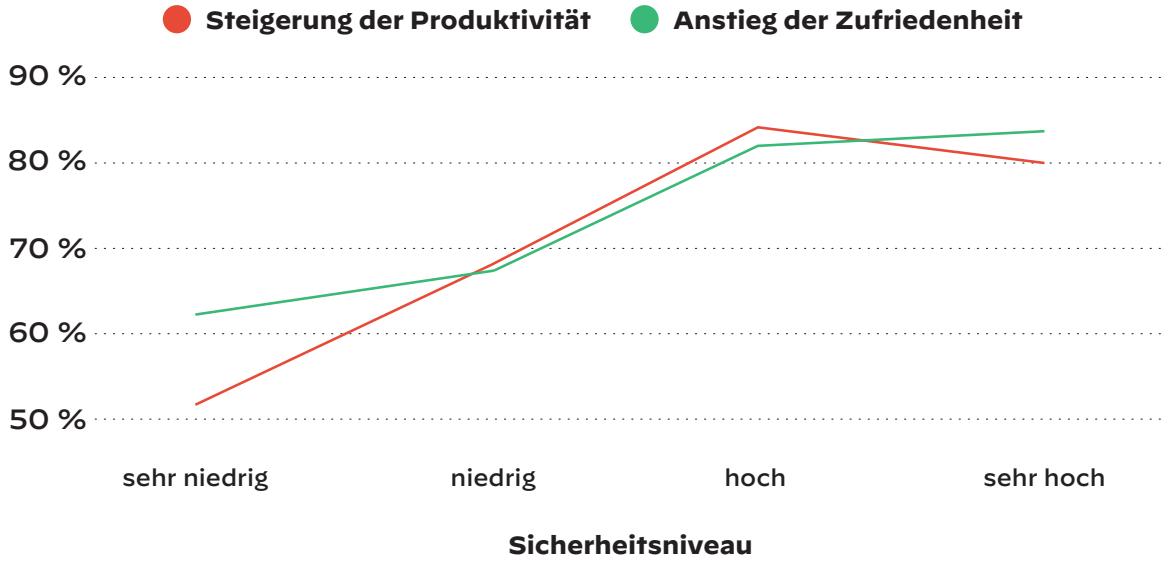


Abbildung 12: Korrelation betrieblicher Auswirkungen mit dem Gesamtsicherheitsniveau

Wie Unternehmen ein hohes Sicherheitsniveau erreichen

Als Nächstes untersuchen wir, welche Ansätze Unternehmen unter den Spitzenreitern verfolgen, um Beeinträchtigungen des Geschäftsbetriebs zu reduzieren und das Sicherheitsniveau insgesamt zu verbessern. Die Unternehmen, die diese ausgewogene, erstklassige Sicherheit erreichen, stechen in zwei miteinander verwandten Disziplinen hervor:

- **DevSecOps-Integration:** der Grad, zu dem Berührungspunkte mit der Cloud-Sicherheit in den Entwicklungszyklus insgesamt integriert wurden, d. h. von der Programmierung bis zum Ende der Laufzeit.
- **Automatisierung der Cloud-Sicherheit:** der Grad, zu dem die Cloud-Sicherheit automatisiert wurde.

Wir baten die Umfrageteilnehmer, den Grad der DevSecOps-Integration in ihrem Unternehmen durch Beantwortung von vier Fragen anhand einer Skala von „nie“ bis „immer“ zu beurteilen.

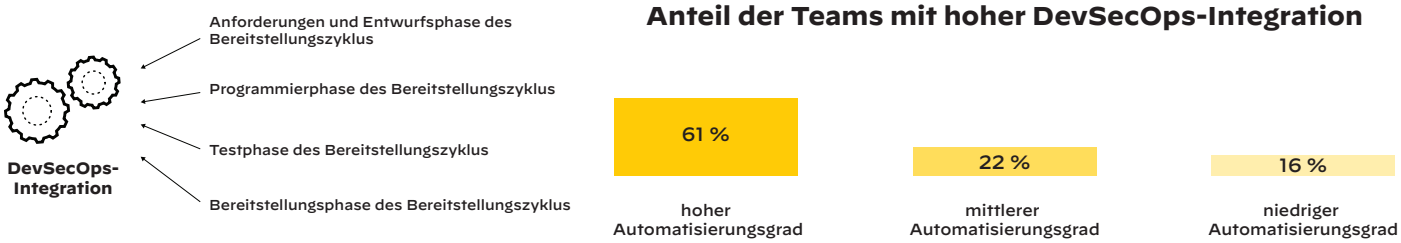


Abbildung 13: links: Faktoren zur Bestimmung der DevSecOps-Integration; rechts: Korrelation der DevSecOps-Integration mit dem Automatisierungsgrad

Als Hauptindikator für erstklassige Sicherheit wurde herangezogen, wie gut Unternehmen DevSecOps-Methoden übernommen und umgesetzt haben. **Unternehmen, die DevSecOps-Prinzipien eng in ihren Entwicklungslebenszyklus integrieren, haben mit einer mehr als siebenfachen Wahrscheinlichkeit ein hohes oder sehr hohes Sicherheitsniveau und mit einer mehr als neunfachen Wahrscheinlichkeit nur geringe Nebenwirkungen der Sicherheitsmaßnahmen.**

Um die Automatisierung zu messen, baten wir die Umfrageteilnehmer, auf einer Skala von „vollständig manuell“ bis „vollständig automatisiert“ anzugeben, wie umfassend fünf Sicherheitspraktiken in ihrem Unternehmen automatisiert sind.

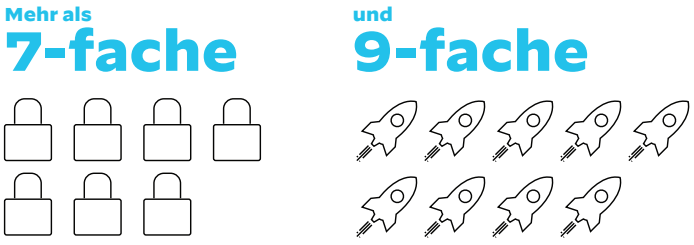


Abbildung 14: Ergebnisse für Unternehmen mit enger Integration von DevSecOps-Prinzipien

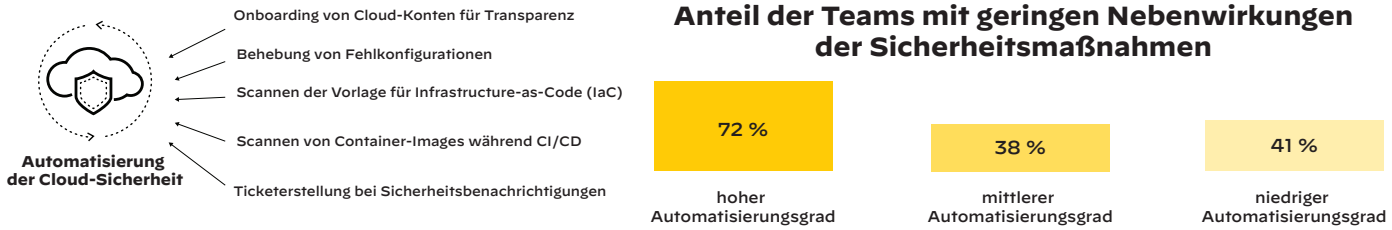


Abbildung 15: links: Faktoren zur Messung des Automatisierungsgrades; rechts: Korrelation der Nebenwirkungen von Sicherheitsmaßnahmen mit dem Automatisierungsgrad

Es zeigte sich, dass **Unternehmen mit einem hohen Grad der Sicherheitsautomatisierung mit etwa doppelt so hoher Wahrscheinlichkeit geringe Nebenwirkungen und ein hohes Sicherheitsniveau haben als Unternehmen mit einem niedrigen Grad der Sicherheitsautomatisierung**. Insbesondere ein „überdurchschnittlicher" Automatisierungsgrad führt zu einer signifikanten Verbesserung der Sicherheit.

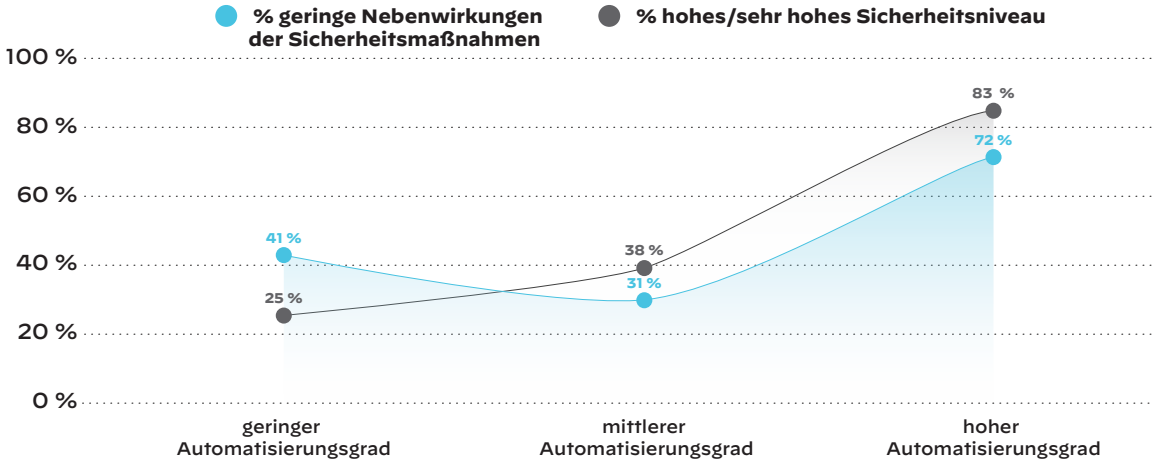


Abbildung 16: Automatisierung als Sicherheitsmotor

Die Folgen von Open-Source-Sicherheitstools

Unternehmen verfolgen viele verschiedene Ansätze bezüglich der Anbieter ihrer Sicherheitstools und nutzen gleichermaßen Cloud-Service-Anbieter (CSPs), Drittanbieter und Open-Source-Sicherheitstools. Allerdings zeigen die Daten, dass Unternehmen, die hauptsächlich Open-Source-Tools einsetzen, anhaltende Probleme haben.

Diese Gruppe verfügt in der Regel über ein kleineres Budget als Unternehmen, die Lösungen von Drittanbietern oder CSPs verwenden, dennoch sind die Teams größer als die der beiden anderen Gruppen: **70 Prozent der Unternehmen, die hauptsächlich Open-Source-Tools nutzen, gaben an, dass ihr Sicherheitsteam aus 30 oder mehr Mitarbeitern bestehe**.

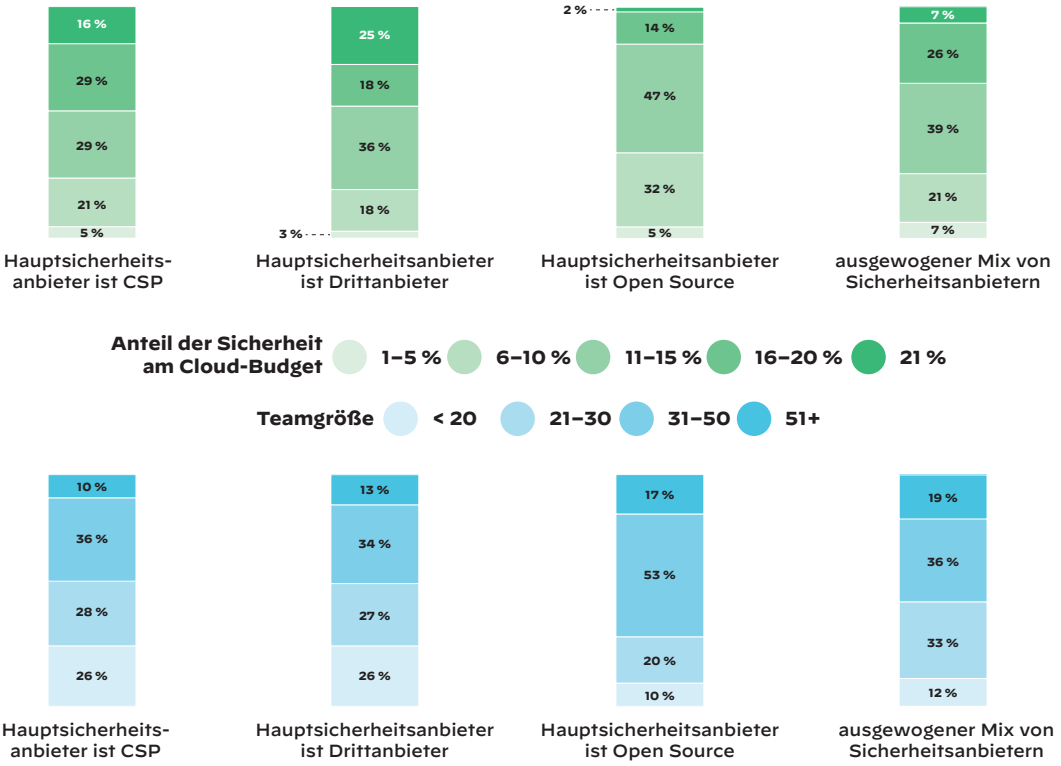


Abbildung 17: Sicherheitsanbieter und Budget (oben) bzw. Größe (unten) des Teams

Von jenen, die hauptsächlich Open-Source-Sicherheitstools nutzen, haben außerdem 80 Prozent ein niedriges oder sehr niedriges Sicherheitsniveau.

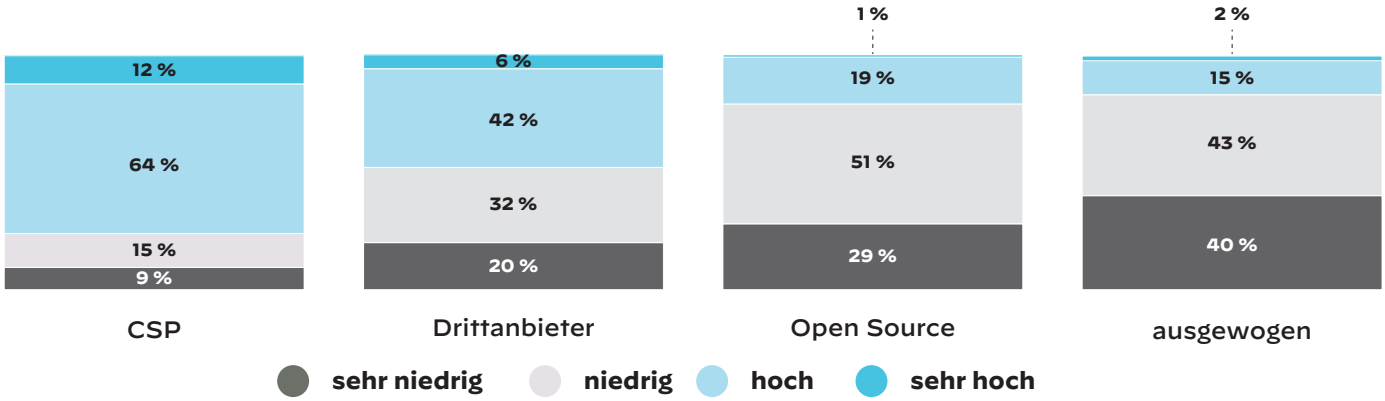


Abbildung 18: Sicherheitsanbieter und Sicherheitsniveau

Insgesamt legen die Daten nahe, dass Open-Source-Sicherheitstools keinen integrierten, umfassenden Ansatz bieten, der das ganze Spektrum von Funktionen und Merkmalen umfasst, die Unternehmen brauchen. Unternehmen, die mit Open-Source-Sicherheitstools erfolgreich sind, scheinen lediglich die Kosten auf ein größeres Team zu verlagern, das zur Stützung der Maßnahmen wichtig ist. Unternehmen, die Open-Source-Tools in Erwägung ziehen, sollten sich darauf einstellen, dass sie eine hochgradig individuelle Bereitstellung haben werden – mit erforderlichen laufenden Investitionen in die interne Pflege, die ansonsten in den Händen eines spezialisierten Lösungsanbieters läge.

Identifizieren Sie Ihren Nutzertyp und lernen Sie von Kollegen

Um zu ermitteln, ob bestimmte Rahmenbedingungen auch ohne DevSecOps-Methoden und Sicherheitsautomatisierung wie oben beschrieben erstklassige Sicherheit unterstützen können, suchten wir in den von den Unternehmen während der Pandemie zur Entwicklung ihrer Cloud-Umgebungen und Cloud-Sicherheit eingeschlagenen Wege nach Mustern. Diese Zeit stellt gewissermaßen ein natürliches Experiment dar, bei dem wir sozusagen im Zeitraffer verschiedene Ansätze und ihre Auswirkungen beobachten konnten. Anstatt mehrere Jahre warten zu müssen, führte diese konzentrierte Bewegung in die Cloud binnen weniger Monate zu schnellen Ergebnissen.

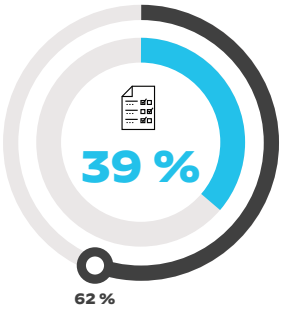
Aus den Daten konnten wird anhand organisatorischer Verhaltensmuster und Ansätze für die Cloud-Sicherheit drei repräsentative Gruppen ermitteln. Beachtenswert ist, dass unsere **Ergebnisse für diese Gruppen unabhängig von geografischer Lage, Branche und Umsatz konstant** sind. Damit verfügen wir über einen einmaligen Einblick in die Faktoren für die erfolgreiche Cloud-Nutzung – und Ansätze, die fehlschlagen – auf der Grundlage, wie Unternehmen ihre Cloud-Projekte und Cloud-Sicherheit umsetzen, und nicht ihres geschäftlichen Hintergrunds.

> „Damit verfügen wir über einen einmaligen Einblick in die Faktoren für die erfolgreiche Cloud-Nutzung – und Ansätze, die fehlschlagen – auf der Grundlage, wie Unternehmen ihre Cloud-Projekte und Cloud-Sicherheit umsetzen, und nicht ihres geschäftlichen Hintergrunds."

Die erste Gruppe sind die **moderaten Nutzer** – Unternehmen, in denen die Cloud sowohl vor als auch während der Pandemie eine untergeordnete Rolle spielte. Die zweite Gruppe sind die **schnellen Erweiterer** – Unternehmen, die die Cloud vor der Pandemie wenig nutzten, aber während der Pandemie die Cloud-Nutzung schnell und weitreichend ausbauten. Die **etablierten Nutzer** schließlich sind Unternehmen, die bereits vor der Pandemie die Cloud in großem Umfang nutzten und während der Pandemie die Nutzung moderat erweiterten.

Sehen Sie sich die Merkmale und Erfahrungen jeder dieser Gruppen genau an. Zu welcher gehört Ihr Unternehmen? Sie können die Daten nutzen, um sich mit Ihren Kollegen zu vergleichen, Erfahrungen zu überprüfen und Unterschiede zu bestimmen. Mithilfe dieser Analyse können Sie auch eine Gruppe identifizieren, die Ihren Cloud-Plänen am nächsten kommt, und anhand ihrer Entscheidungen und Verhaltensmuster Ihre eigene Strategie für langfristigen Erfolg entwickeln.

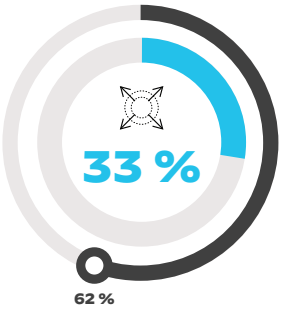
Welche Gruppe beschreibt Ihr Unternehmen am besten?



Moderate Nutzer: 39 % der Gesamtheit
wahrscheinlich eher niedriger Umsatz
Vor der Pandemie: geringe Cloud-Nutzung

Während der Pandemie:
gleichmäßige Cloud-Erweiterung
Erweiterung angetrieben von taktischem Nutzen
niedrige Priorität der Cloud, geringe Investitionen

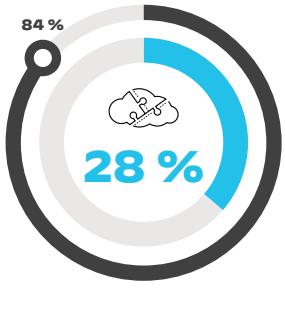
Aktuell: serverlose Architekturen
Planung: durchschnittliches Ziel für Cloud-Nutzung (62 %)



Schnelle Erweiterer: 33 % der Gesamtheit
tendenziell höherer Umsatz
Vor der Pandemie: geringe Cloud-Nutzung

Während der Pandemie:
schnelle Cloud-Erweiterung
Erweiterung angetrieben von strategischem und taktischem Nutzen
durchschnittliche Priorität der Cloud, durchschnittliche Investitionen

Aktuell: PaaS-Architekturen
Planung: durchschnittliches Ziel für Cloud-Nutzung (62 %)



Etablierte Nutzer: 28 % der Gesamtheit
überwiegend große Unternehmen (nach Umsatz)
Vor der Pandemie: umfangreiche Cloud-Nutzung

Während der Pandemie:
gleichmäßige Cloud-Erweiterung
Erweiterung angetrieben von taktischem Nutzen
hohe Priorität der Cloud, hohe Investitionen

Aktuell: ausgewogene Nutzung von IT-Umgebungen
Planung: hohes Ziel für Cloud-Nutzung (84 %)

Abbildung 19: Merkmale der verschiedenen Gruppen von Cloud-Nutzern

Der aktuelle Stand der Cloud-Nutzungsgruppen

Wie bereits angemerkt, sind die cloudbezogenen Merkmale und Verhaltensweisen dieser Gruppen im Allgemeinen konsistent, unabhängig von geografischer Lage, Branche oder Größe des Unternehmens.

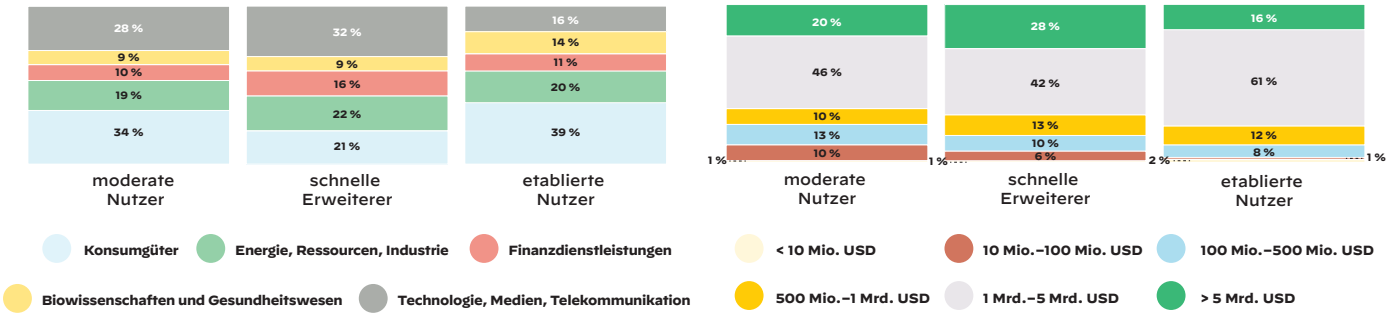


Abbildung 20: links: Cloud-Nutzungsgruppen nach Branche; rechts: Cloud-Nutzungsgruppen nach Umsatz

Cloud-Nutzung

Moderate Nutzer nutzten die Cloud zu Beginn der Pandemie relativ wenig und erhöhten die Nutzung in den folgenden zwölf Monaten kaum. Schnelle Erweiterer nutzten die Cloud zu Beginn der Pandemie ähnlich wenig, erhöhten die Nutzung aber deutlich schneller. Im Gegensatz dazu nutzten die etablierten Nutzer die Cloud bereits vor der Pandemie in großem Umfang und erhöhten die Nutzung nur wenig, ähnlich wie die moderaten Nutzer.

Zukunftspläne für die Cloud

Auf die Frage nach ihren Zukunftsplänen gaben beide Gruppen mit geringer Cloud-Nutzung vor der Pandemie – die moderaten Nutzer und die schnellen Erweiterer – an, dass sie innerhalb von zwei Jahren voraussichtlich 62 Prozent ihrer Workloads in die Cloud verlagert haben werden. Im Gegensatz dazu gehen die etablierten Nutzer davon aus, ihre intensive Cloud-Nutzung fortzusetzen und innerhalb von zwei Jahren 82 Prozent ihrer Workloads in die Cloud verlagert zu haben.

	2020	2021	aktueller Gesamtanteil	Ziel für 2022
moderate Nutzer	35 %	14 %	49 %	62 %
schnelle Erweiterer	26 %	33 %	59 %	62 %
etablierte Nutzer	61 %	13 %	74 %	84 %

Abbildung 21: Anteil der Workloads in der Cloud nach Nutzungsgruppe

Cloud-Ausgaben

Über alle Gruppen hinweg variierten die Cloud-Ausgaben stark. Nur 42 Prozent der moderaten Nutzer gaben mehr als 10 Mio. USD für die Cloud aus, verglichen mit 69 Prozent der schnellen Erweiterer und 70 Prozent der etablierten Nutzer. Etablierte Nutzer haben auch das größte Budget für die Cloud: 10 Prozent gaben mehr als 100 Mio. USD aus gegenüber lediglich 2 Prozent der moderaten Nutzer und 1 Prozent der schnellen Erweiterer.

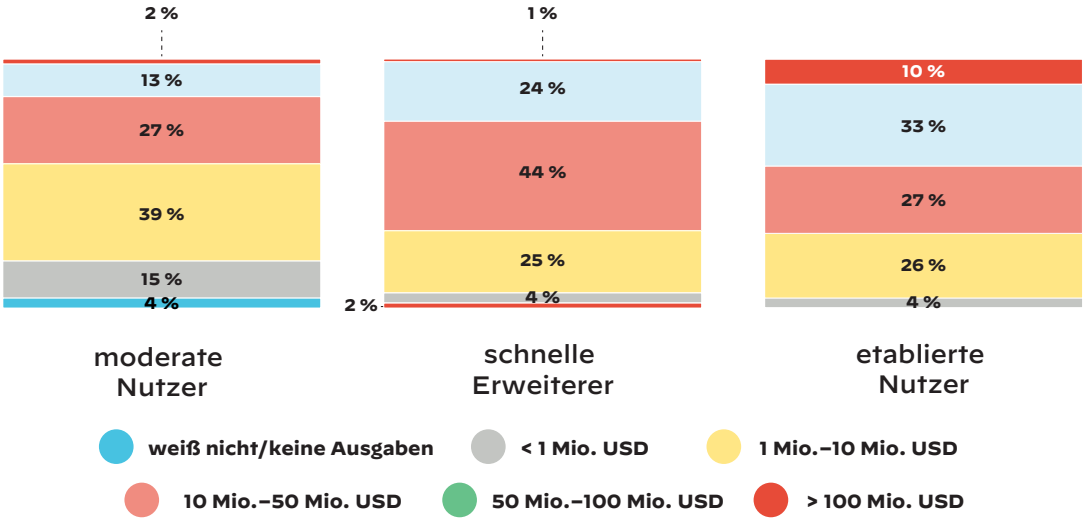


Abbildung 22: Gesamtausgaben für die Cloud nach Nutzungsgruppe

Ansatz für die IT-Umgebung

Auch bei den Ansätzen für Cloud-Architekturen stellen sich Unterschiede heraus. Etablierte Nutzer nutzen mit deutlich größerer Wahrscheinlichkeit einen Mix von IT-Umgebungen mit virtuellen Maschinen (VMs), Containern/CaaS, PaaS und serverlosen Plattformen. 65 Prozent dieser Gruppe nutzen alle vier gleichermaßen. **Auch schnelle Erweiterer verfolgen überwiegend einen ausgewogenen Ansatz (48 Prozent), nutzen PaaS aber doppelt so häufig wie etablierte Nutzer (28 Prozent gegenüber 14 Prozent)**. Diese Entscheidung, die Verwaltung der Infrastruktur zu vermeiden, hat möglicherweise das schnelle Wachstum der schnellen Erweiterer erst ermöglicht.

In unserer Analyse kommen wir zu dem Schluss, dass die moderaten Nutzer mit mäßiger Cloud-Nutzung und Plänen für einen langsameren Ausbau nicht die Cloud an und für sich priorisieren, sondern ihre Cloud-Nutzung von anderen unternehmerischen Strategien leiten lassen. Die IT-Entscheidungen dieser Gruppe (47 Prozent nutzen hauptsächlich serverlose Plattformen und 32 Prozent nutzen einen ausgewogenen Technologiemix) spiegeln dies ebenfalls wider: Ihr Ansatz vermeidet Verwaltungskosten und konzentriert sich auf die Entwicklung von Anwendungscode statt die Einrichtung und Pflege einer Cloud-Infrastruktur.

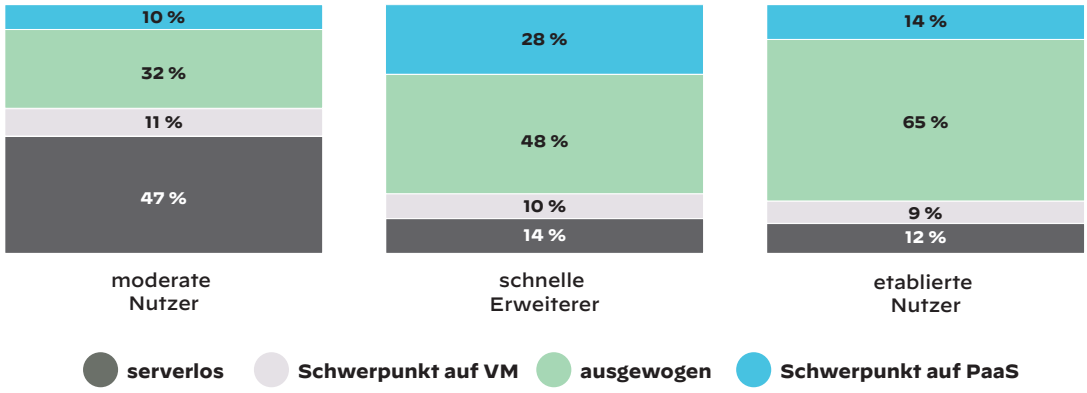


Abbildung 23: Mix der IT-Architektur nach Nutzungsgruppe

Schnelle Cloud-Erweiterung hat entgegengesetzte Ergebnisse

Bei näherer Untersuchung der Cloud-Ziele unserer drei Gruppen stießen wir auf ein überraschendes Muster. Die Gruppe der schnellen Erweiterer teilte sich in zwei klar abgrenzbare Untergruppen auf. **Die Mehrheit der schnellen Erweiterer (74 Prozent) baute ihre Cloud-Nutzung schnell und erfolgreich aus**. Dabei migrierten sie im letzten Jahr 35 Prozent ihrer Workloads in die Cloud und planen die Migration weiterer 12 Prozent ihrer Workloads im Verlauf der beiden nächsten Jahre.

Im Gegensatz dazu migrierten **die anderen 26 Prozent der schnellen Erweiterer** während der Pandemie 28 Prozent ihrer Workloads in die Cloud, haben aber überraschenderweise vor, **in den nächsten beiden Jahren ihre Cloud-Workload um 26 Prozent zu verringern**. Das lässt vermuten, dass sie planen, Workloads wieder aus der Cloud zurückzuholen oder netto keine neuen Workloads in die Cloud zu migrieren.

Diese Aufteilung der schnell erweiternden Gruppe ließ neue Fragen aufkommen: Was ist die Ursache für diesen auffälligen Unterschied? Welche Lehren können aus den Erfahrungen dieser Unternehmen gezogen werden? Wie können diese Lehren zum Erfolg künftiger Cloud-Projekte beitragen?

	2020	2021	die nächsten beiden Jahre
moderate Nutzer	35 %	14 %	+13 %
schnelle Erweiterer mit Schwierigkeiten	34 %	28 %	-26 %
schnelle Erweiterer mit erfolgreicher Umsetzung	24 %	35 %	+12 %
schnelle Erweiterer	61 %	13 %	+10 %

Abbildung 24: Veränderung der Cloud-Workload im Zeitraum 2020–2021 und Prognose für 2022–2023

Bei eingehender Betrachtung kann diese Aufteilung dadurch erklärt werden, dass ein Teil der schnellen Erweiterer ihre Cloud-Nutzung erfolgreich ausbauen konnte, während andere erhebliche Schwierigkeiten hatten. Die schnellen Erweiterer, die sich Schwierigkeiten gegenübersahen, investierten deutlich höhere Summen in die Cloud als ihre erfolgreicheren Kollegen: **45 Prozent gaben 2021 mehr als 50 Millionen USD für die Cloud aus gegenüber nur 13 Prozent der schnellen Erweiterer, die mit dieser Strategie fortfahren**. Dies legt nahe, dass einige der schnellen Erweiterer möglicherweise versucht haben, die Schwierigkeiten mit Geld zu lösen, anstatt die zugrunde liegenden Probleme zu beheben.

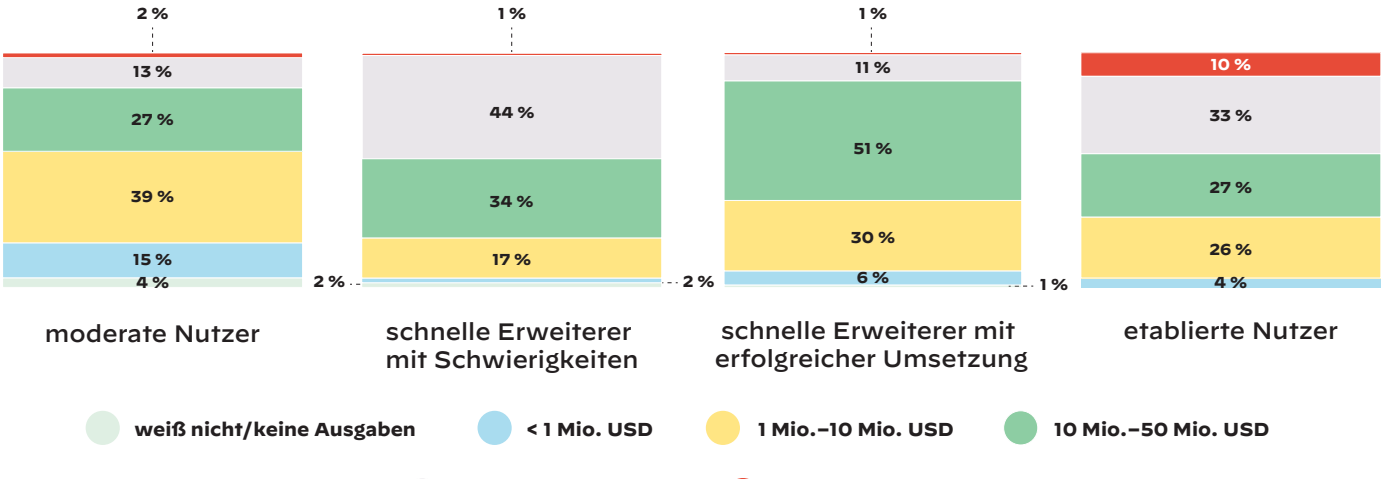


Abbildung 25: Ausgaben nach Nutzungsgruppe

Auch bei den Cloud-Zielen der Gruppen sind deutliche Unterschiede erkennbar. Für alle Gruppen waren kurzfristige Ziele wie die Anwendungsmodernisierung und Bewahrung der Wettbewerbsfähigkeit die Hauptgründe für die Erweiterung der Cloud-Nutzung, während strategische Überlegungen zurückgestellt wurden. Allerdings gab es große Unterschiede bei der geschäftlichen Ausrichtung. Bei den erfolgreichen schnellen Erweiterern war die Cloud-Entwicklung mit deutlich höherer Wahrscheinlichkeit Teil eines größeren strategischen Projekts zur digitalen Transformation. **Schnelle Erweiterer, die ihre Cloud-Infrastruktur im letzten Jahr erfolgreich ausbauten, taten dies mit mehr als doppelt so hoher Wahrscheinlichkeit im Rahmen eines umfassenderen strategischen Projekts der digitalen Transformation**.

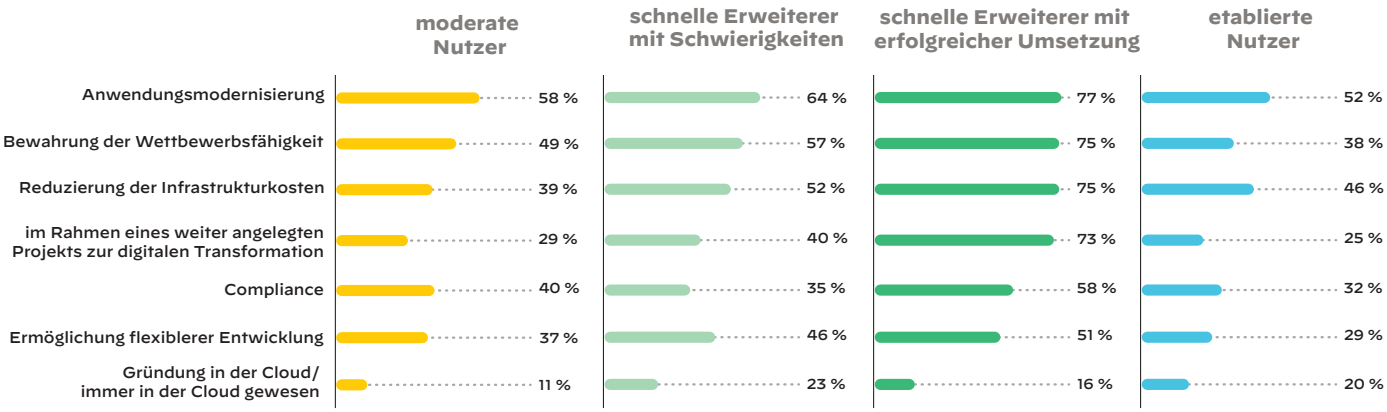


Abbildung 26: Gründe für die Migration von Workloads in die Cloud

Umfassende Sicherheit und die Einhaltung von Vorschriften zählten ebenfalls zu den häufigsten Herausforderungen für alle Gruppen, aber ein wichtiges Muster ist erkennbar: **Die schnellen Erweiterer nannten umfassende Sicherheit häufiger als eine der größten Herausforderungen als andere Gruppen**. Sie berichteten auch deutlich häufiger von Schwierigkeiten im Zusammenhang mit Strategie, Budget und der Gewinnung und Haltung qualifizierter Mitarbeiter. **Dies spricht für die Vorstellung, dass ein erfolgreiches Cloud-Projekt Teil einer größeren strategischen Umstellung im Unternehmen sein muss, weil die Cloud viele Geschäftsprozesse betrifft und das Unternehmen insgesamt darauf vorbereitet sein muss, diese Veränderungen zu tragen**. Die schnellen Erweiterer, die sich wieder aus der Cloud zurückziehen wollen, machen zwar nur 8 Prozent der untersuchten Unternehmen aus, doch verdeutlichen sie die Herausforderungen bei der Integration von Sicherheit in Projekte zur Erweiterung der Cloud-Nutzung.

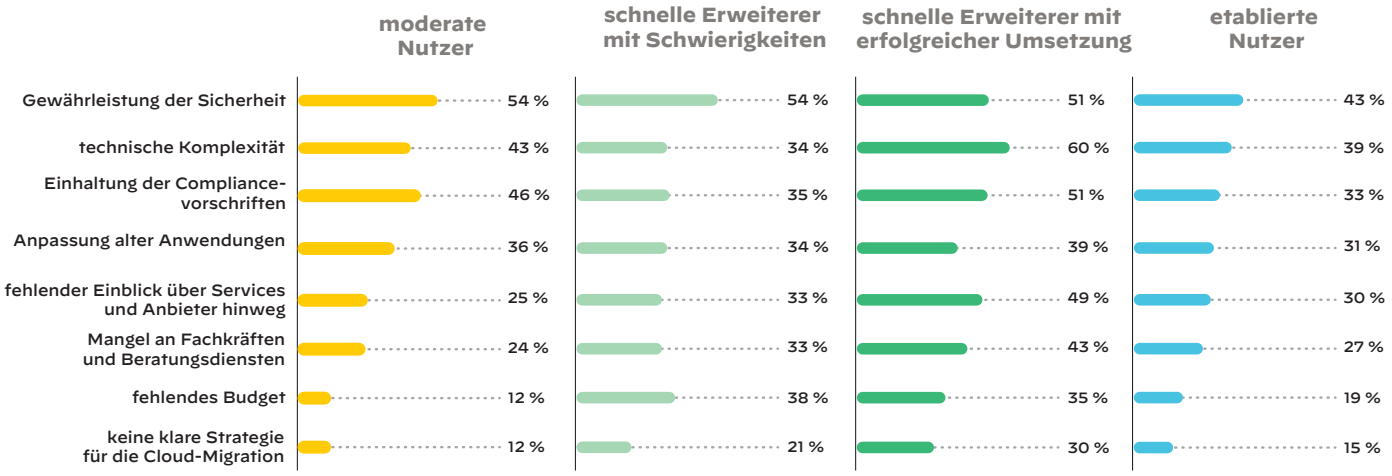


Abbildung 27: Die größten Herausforderungen bei Programmen zur Erweiterung der Cloud-Nutzung

Die Rolle von Sicherheitsanbietern, Teams und Tools

Die beiden Gruppen schneller Erweiterer verfolgten unterschiedliche Ansätze bei der Zusammenarbeit mit Sicherheitsanbietern. **83 Prozent der erfolgreichen Gruppe nutzten höchstens fünf Anbieter. In der Gruppe der schnellen Erweiterer, die auf Probleme stießen, trifft dies nur auf 45 Prozent zu.**

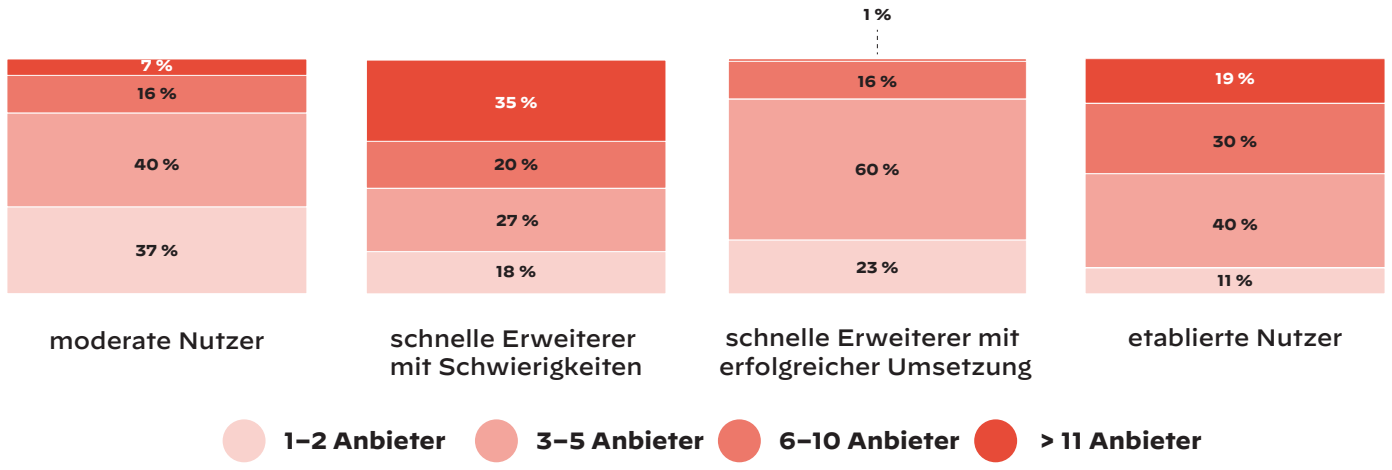


Abbildung 28: Zahl der einzelnen genutzten Sicherheitsanbieter

Als Nächstes betrachten wir die Sicherheitsteams. Die erfolgreichen schnellen Erweiterer haben in der Regel ein relativ kleines Team und ein kleineres Anbieternetz, nutzen aber mehrere Sicherheitstools (Sicherheitstools werden hier wieder als die Zahl der Fähigkeiten und Funktionen, die Cybersicherheitsunternehmen anbieten, definiert). Schnelle Erweiterer, die auf Schwierigkeiten stießen, hatten hingegen eher größere Teams, ein größeres Anbieternetz und weniger Sicherheitstools.

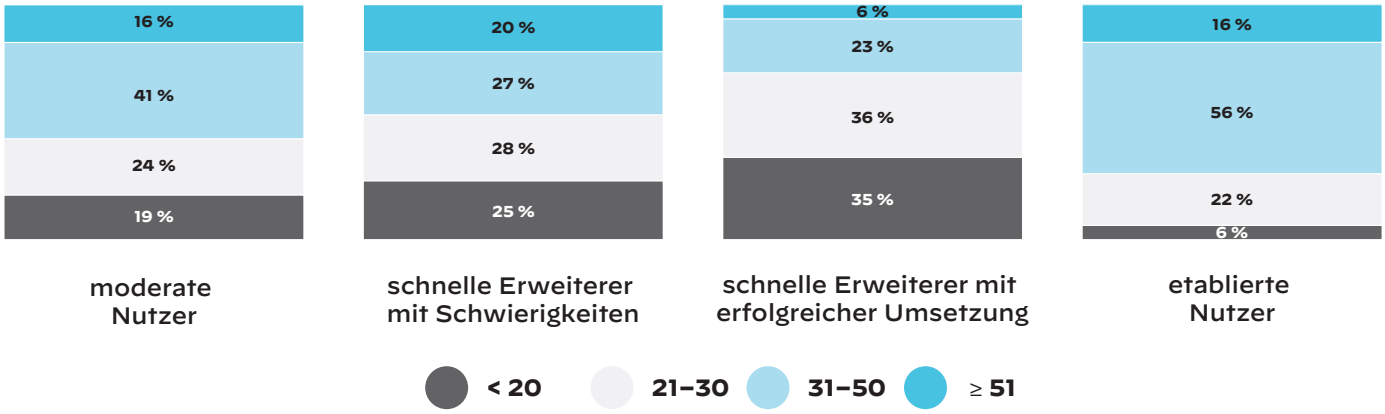


Abbildung 29: Größe des Teams für die Cloud-Sicherheit

Die Untersuchung zeigt, dass alle Gruppen eine hohe Zahl von Sicherheitstools verwenden und mehr als die Hälfte der Unternehmen in jeder Gruppe mehr als fünf Tools nutzt. Dies könnte bedeuten, dass es eine Variablengleichung für die optimale Zahl von Sicherheitstools gibt, die für eine bestimmte Umgebung notwendig sind, wobei größere Cloud-Umgebungen notwendigerweise mehr Tools erfordern oder unterschiedliche Teams unterschiedliche Sätze von Tools bevorzugen. Ein zu starker Fokus auf Einfachheit kann jedoch nachteilig sein und das Scheitern mancher Cloud-Projekte scheint eher auf ein Fehlen von Sicherheitsdaten und -steuerungen zurückzuführen zu sein als auf die mangelnde Verfügbarkeit von Tools.

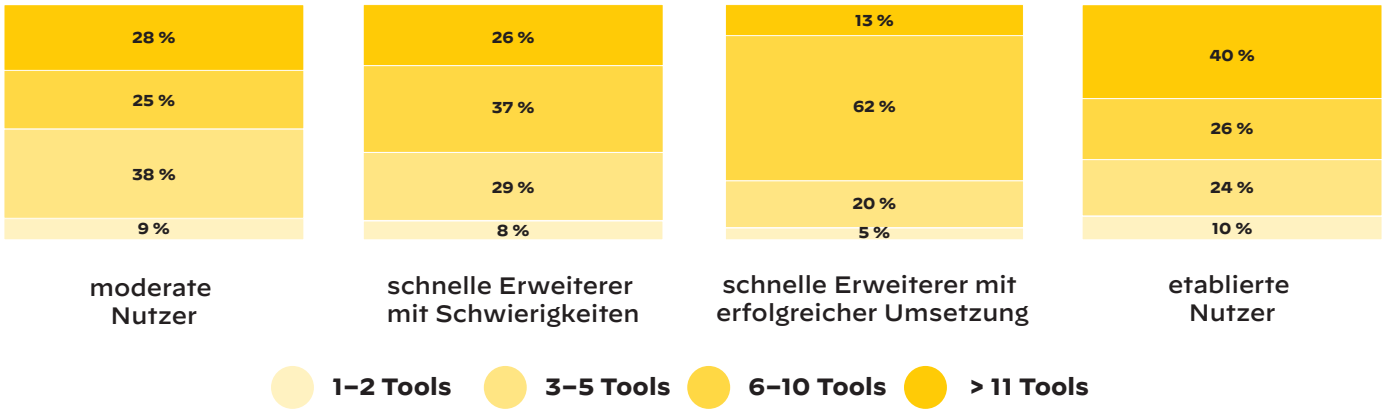


Abbildung 30: Zahl der verwendeten Tools, unabhängig vom Anbieter

Falls es eine solche Variablengleichung gibt, weisen die Daten darauf hin, dass auch die Integration der Sicherheitstools ein wichtiger Faktor ist. Unternehmen, die weniger als fünf Sicherheitstools nutzen, haben Mühe damit, ein hohes oder sehr hohes Sicherheitsniveau zu erreichen, – die reibungslose Zusammenarbeit verschiedener Teams scheint jedoch von der Zahl der Tools unabhängig zu sein. Vielmehr ist es die Fähigkeit, Sicherheitstools mit DevSecOps-Methoden zu verknüpfen und so umfassendere Transparenz und Kontrolle zu erhalten, die zu besseren Ergebnissen führt. Dies passt mit den Branchentrends zu konsolidierten, umfassenden Sicherheitsplattformen zusammen.

„Es ist die Fähigkeit, Sicherheitstools mit DevSecOps-Methoden zu verknüpfen und so umfassendere Transparenz und Kontrolle zu erhalten, die zu besseren Ergebnissen führt.“

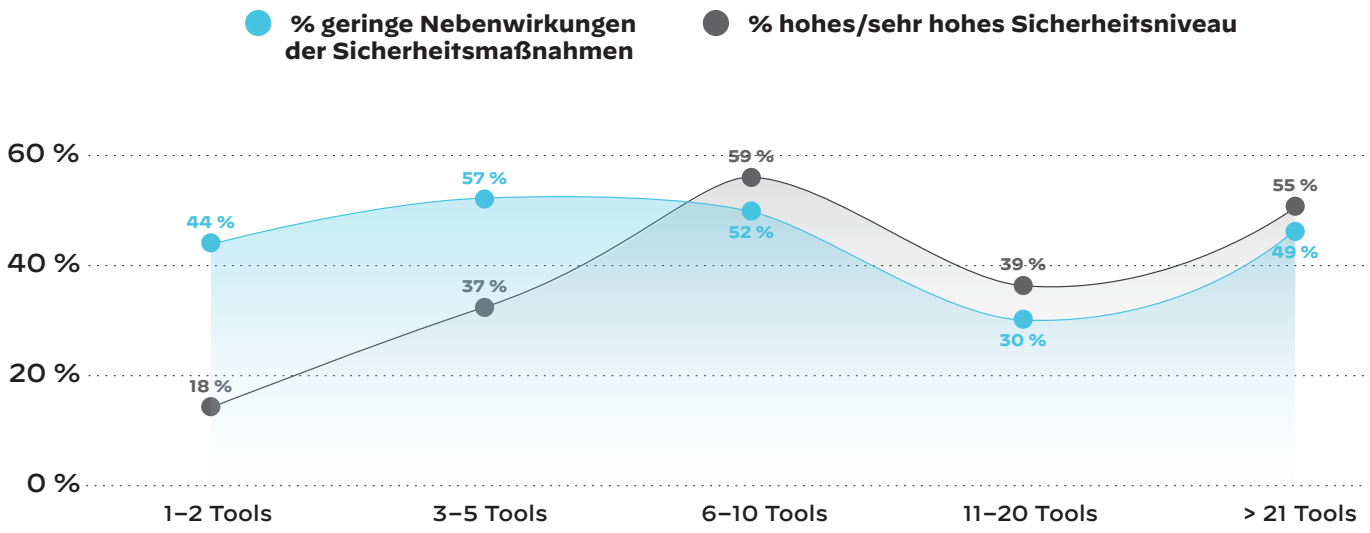


Abbildung 31: Zahl der Sicherheitstools und Auswirkungen auf die Sicherheit

Umsetzung erstklassiger Sicherheit in den Gruppen

An anderer Stelle in diesem Bericht wurde auf die Bedeutung der DevSecOps-Integration und Sicherheitsautomatisierung als wichtige Elemente für eine erstklassige Cloud-Sicherheit eingegangen. Unsere Gruppen zeigen, dass **63 Prozent der schnellen Erweiterer, die erfolgreich ihre Cloud-Nutzung ausgebaut haben, auch DevSecOps-Prinzipien integrierten**. Dieser Anteil ist selbst im Vergleich zu etablierten Nutzern beträchtlich höher, was darauf hinweist, dass **erfolgreiche schnelle Erweiterer** beim Ausbau ihrer Cloud-Funktionen **der Integration von Sicherheit während des gesamten Entwicklungslebenszyklus besondere Aufmerksamkeit schenkten**.

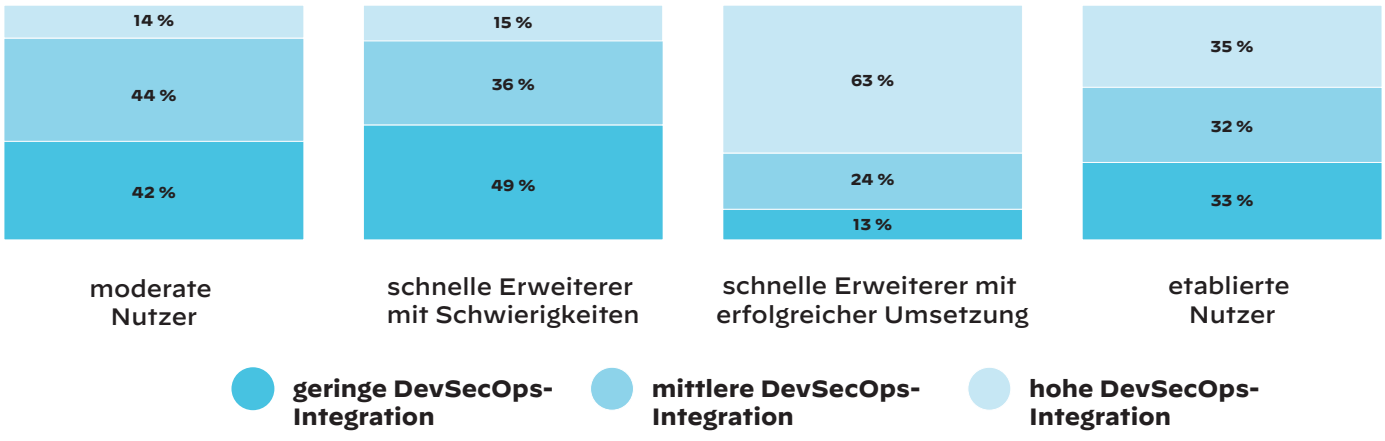


Abbildung 32: Grad der DevSecOps-Integration in den Anwendungslebenszyklus

Ganz ähnlich sind Gruppen mit starker Cloud-Nutzung – etablierte Nutzer und erfolgreiche schnelle Erweiterer – auch eher zur Automatisierung bereit: 44 Prozent bzw. 40 Prozent der beiden genannten Gruppen weisen einen hohen Automatisierungsgrad auf. Im Gegensatz dazu liegen **schnelle Erweiterer, die mit der Cloud-Erweiterung Schwierigkeiten hatten, mit einem niedrigen Automatisierungsgrad bei 40 Prozent weit zurück.**

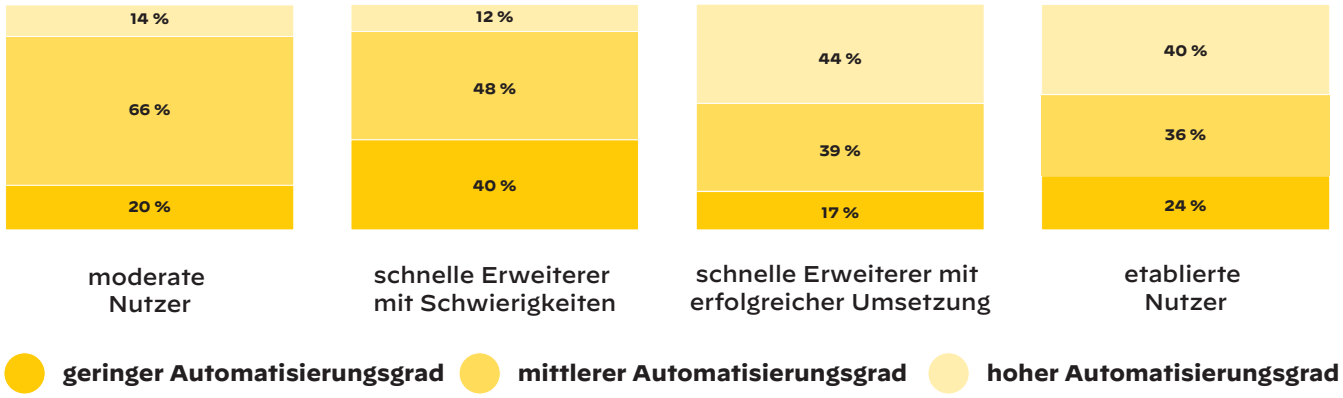


Abbildung 33: Grad der Sicherheitsautomatisierung während des gesamten Entwicklungslebenszyklus

Schließlich ist festzuhalten, dass **erfolgreiche schnelle Erweiterer beim Sicherheitsniveau am besten abschneiden: 81 Prozent von ihnen haben ein hohes oder sehr hohes Sicherheitsniveau**. Die etablierten Nutzer liegen mit 50 Prozent an zweiter Stelle, während **das Sicherheitsniveau bei 69 Prozent der schnellen Erweiterer, die Schwierigkeiten hatten, niedrig oder sehr niedrig war**. Auch bei den moderaten Nutzern ist das Sicherheitsniveau niedrig, aber wie bereits angemerkt, beurteilt diese Gruppe, die die Cloud weiterhin nur wenig nutzt, den Erfolg oder das Scheitern ihrer Cloud-Nutzung möglicherweise nach anderen Maßstäben.

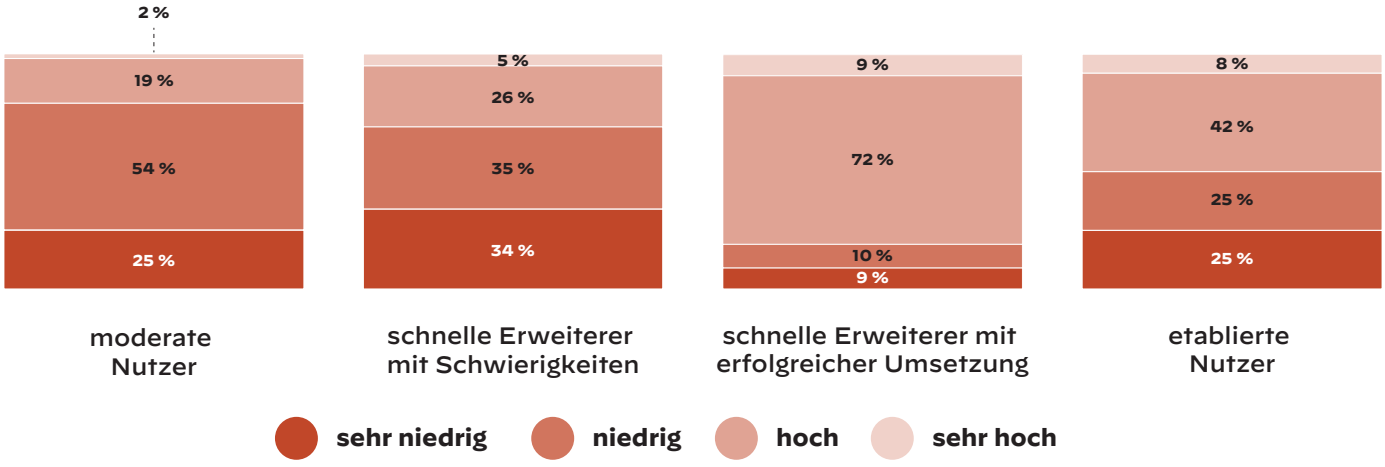


Abbildung 34: Sicherheitsniveau nach Nutzungsgruppe

Hier sehen wir weitere Anzeichen, dass eine organisatorische Anpassung für eine erfolgreiche Umstellung auf die Cloud wichtig ist – Gruppen mit einem niedrigen Sicherheitsniveau haben im Allgemeinen auch viele störende Nebenwirkungen ihrer Sicherheitsmaßnahmen. **Bei der Hälfte der schnellen Erweiterer, die Schwierigkeiten hatten, traten starke Nebenwirkungen der Sicherheitsmaßnahmen auf, verglichen mit nur 13 Prozent der erfolgreichen schnellen Erweiterer und 14 Prozent der etablierten Nutzer.**

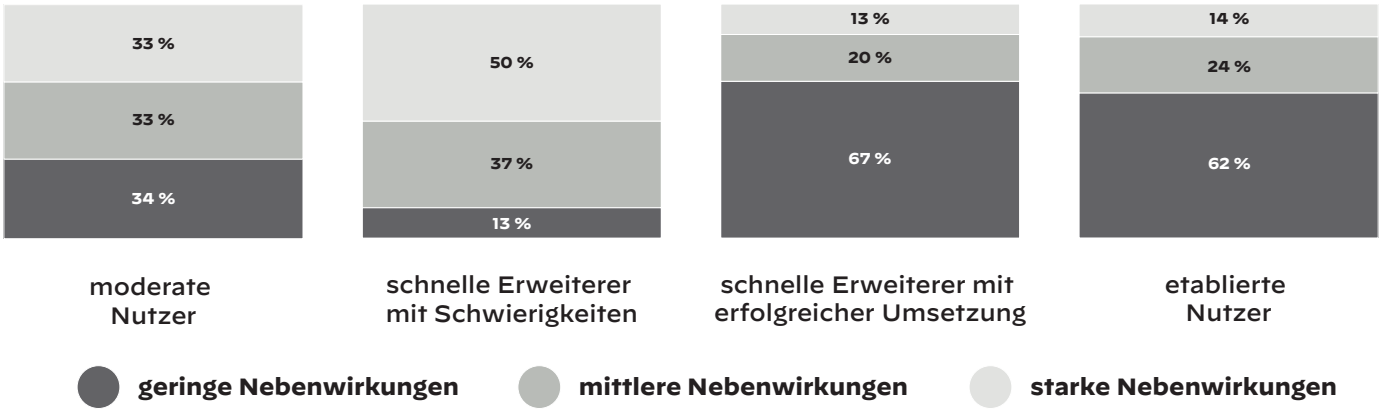
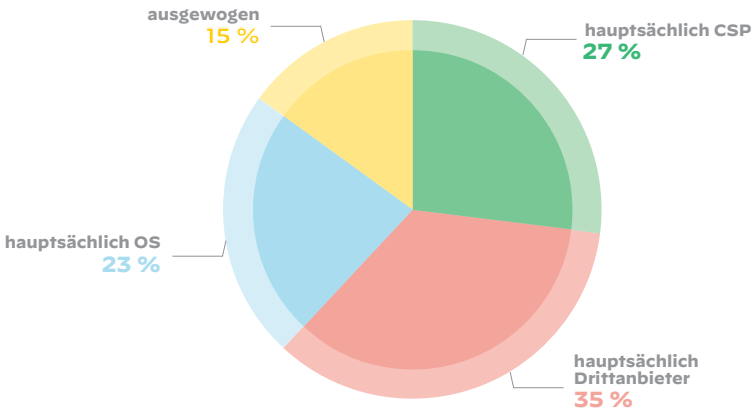


Abbildung 35: Menge an Nebenwirkungen auf den Geschäftsbetrieb nach Nutzungsgruppe

Zwar nutzten die meisten Unternehmen mehrere Sicherheitsanbieter, doch waren dies bei den schnellen Erweiterern, die auf Schwierigkeiten stießen, häufiger Open-Source-Sicherheitsanbieter. **Im Gegensatz dazu vermieden Unternehmen, die ihre Cloud-Nutzung erfolgreich schnell erweiterten, Open-Source-Anbieter und auch einen ausgewogenen Mix. Vielmehr nutzten 87 Prozent entweder die Sicherheitsdienste von CSPs oder Drittanbietern.**



Unternehmen verfolgten viele verschiedene Ansätze bei der Auswahl der Art ihres Sicherheitsanbieters und nutzen gleichermaßen CSP, Drittanbieter und Open-Source-Material.

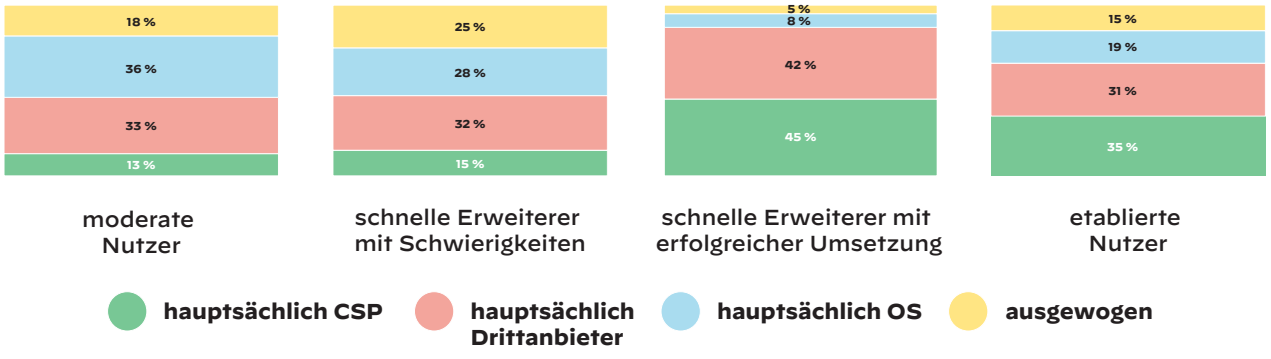


Abbildung 36: Haupt-Toolanbieter insgesamt (oben) und nach Nutzungsgruppe (unten)

Die Unterteilung der schnellen Erweiterer gab uns die Möglichkeit, zu untersuchen, was für eine erfolgreiche schnelle Migration in die Cloud wichtig ist. Insgesamt gelangten wir zu den folgenden Erkenntnissen:

- Hohe Cloud-Ausgaben sind nicht gleichbedeutend mit erfolgreicher Cloud-Nutzung.
- Die Einbindung der Cloud-Nutzung in eine umfassendere strategische digitale Transformation ist der Schlüssel zum Erfolg.
- Die Konsolidierung von Sicherheitsanbietern, die vielfältige Sicherheitstools anbieten, führt zum Erfolg von Projekten zur Erweiterung der Cloud-Nutzung.
- Größere Sicherheitsteams sind nicht gleichbedeutend mit größerer Sicherheit des Unternehmens.
- DevSecOps-Integration und Sicherheitsautomatisierung sind notwendige Komponenten für die erfolgreiche Cloud-Nutzung.
- Sicherheitsdienste von CSPs oder Drittanbietern führen mit größter Wahrscheinlichkeit zu einer erfolgreichen und sicheren Cloud-Nutzung.

Abschließende Gedanken

Die Pandemie hat dem diesjährigen Bericht zum Stand der cloudnativen Sicherheit einen unverwechselbaren Stempel aufgedrückt und wir gehen davon aus, dass sich ihr Einfluss auch in Zukunft bemerkbar machen wird. Trotz rapider Veränderungen hinsichtlich der Geschäftsstrategien und -ressourcen konnten die meisten Unternehmen ihre Projekte zur Cloud-Erweiterung in dieser unruhigen Zeit dennoch erfolgreich umsetzen. Selbst für die heutigen komplexen und heterogenen Cloud-Umgebungen, die eine Mischung von öffentlichen und privaten Clouds, verschiedenen IT-Konstellationen und einer wachsenden Zahl von Cloud-Service-Anbietern umfassen, lassen unsere Untersuchungen einen bewährten Weg für die weitere Entwicklung erkennen.

Insgesamt waren **Unternehmen, die ihre Cloud-Infrastruktur zu einem strategischen Kernthema für den gesamten Geschäftsbetrieb machten, erfolgreicher**. Außerdem ist die **Cloud-Sicherheit ein klarer Faktor zur Förderung der geschäftlichen Entwicklung**. Für jeden Unternehmenstyp auf der ganzen Welt sind die Best Practices für die Sicherheit gleich und können als zentrale Faktoren für den Erfolg der Cloud-Nutzung umgesetzt werden. Natürlich führt größere Sicherheit nicht notwendigerweise zu einem bestimmten Kennwert. Doch ist die Sicherheit im Griff – durch Konsolidierung von Tools und Anbietern sowie durch Nutzung bewährter Strategien für DevSecOps und Sicherheitsautomatisierung –, schafft dies die Grundlage, auf der Entwicklungsteams ihre Aufgaben besser erledigen und Unternehmen ihre Cloud-Transformationen erfolgreich umsetzen können.

Methodik und demografische Daten

Diese Umfrage wurde online zwischen dem 3. Mai und dem 1. Juni 2021 durchgeführt. Die Umfrageteilnehmer kamen aus der ganzen Welt, unter anderem aus Deutschland, den USA, Großbritannien, Brasilien und Japan. Die Stichprobe umfasste alle größeren Branchen, wobei insbesondere Konsumgüter und Dienstleistungen, Energie, Ressourcen und Industrie, Finanzdienstleistungen, Technologie, Medien und Telekommunikation sowie Biowissenschaften und Gesundheitswesen vertreten waren. Mehr als zwei Drittel der Befragten arbeiten in Unternehmen der Enterprise-Klasse (Jahresumsatz über 1 Milliarde USD) und repräsentieren beide Bereiche der organisatorischen Struktur: Die Befragten haben zu etwa gleichen Teilen Rollen in der Geschäftsführung und eher praxisorientierte Rollen inne, um die Einstellungen im gesamten Unternehmen einschätzen zu können. Die Befragten aus der Praxis sind ausschließlich in den Bereichen Entwicklung, IT und Informationssicherheit tätig. Die Befragten wurden aus professionellen Umfragepanels ermittelt und alle gaben an, sich mit dem Cloud-Betrieb und der Cloud-Sicherheit in ihrem Unternehmen auszukennen.

Über uns

Palo Alto Networks

Palo Alto Networks ist ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, das mit seinen bahnbrechenden Technologien die Weichen für eine cloudorientierte Zukunft stellt und die Arbeitsweise von Unternehmen und ihren Mitarbeitern von Grund auf modernisiert. Wir haben uns das Ziel gesetzt, zum bevorzugten Cybersicherheitspartner für Unternehmen zu werden und gemeinsam mit ihnen unseren digitalen Lebensstil zu schützen. Dazu gehen wir durch kontinuierliche Innovation die größten Herausforderungen rund um die Cybersicherheit an, mit denen Unternehmen derzeit konfrontiert sind. Dabei kommen die neuesten Forschungsergebnisse aus den Bereichen künstliche Intelligenz, Analyse, Automatisierung und Orchestrierung zum Einsatz. Mit einer integrierten Plattform und einem wachsenden Partnernetzwerk schützt Palo Alto Networks die Clouds, Netzwerke und Mobilgeräte Zehntausender Unternehmen und arbeitet unermüdlich für eine Welt, in der jeder Tag ein bisschen sicherer ist als der Tag zuvor. Weitere Informationen erhalten Sie unter www.paloaltonetworks.de.

Prisma Cloud

Prisma Cloud ist eine umfassende cloudnative Sicherheitsplattform, die mit branchenführenden Sicherheits- und Compliancefunktionen Anwendungen, Daten und cloudnative Technologien während des gesamten Entwicklungslebenszyklus in Multi-Cloud- und Hybridbereitstellungen schützt. Der integrierte Ansatz von Prisma Cloud bietet Sicherheits- und DevOps-Teams das nötige Maß an Flexibilität und ermöglicht es ihnen, effektiv zusammenzuarbeiten sowie cloudnative Anwendungen schnell und sicher zu entwickeln und bereitzustellen. Weitere Informationen erhalten Sie unter www.paloaltonetworks.de/prisma/cloud.

PRISMA® CLOUD | paloalto® NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de

the-state-of-cloud-native-security-report-2022_011422-de