

2025

# Bericht zum Stand der Cloud-Sicherheit

Wichtige Erkenntnisse und Strategien  
zum Schutz von Cloud-Umgebungen



**FORTINET®**

# Einleitung

Ob Wirtschaft oder öffentliche Hand: Cloud-Lösungen werden in allen Bereichen zunehmend eingesetzt. Neben Vorteilen wie eine einzigartige Skalierbarkeit und Flexibilität – insbesondere bei Multi-Cloud-Strategien – bringt die Cloud jedoch auch neue Sicherheitsherausforderungen mit sich. An der Implementierung innovativer Security-Lösungen, die wirksam wichtige Ressourcen schützen, führt deshalb kein Weg vorbei.

Auf den folgenden Seiten finden Sie eine detaillierte Analyse der sich entwickelnden Cloud-Sicherheitslage sowie wichtige Trends, Herausforderungen und Prioritäten für Organisationen, die sich in zunehmend komplexen Umgebungen zurechtfinden müssen. Basierend auf den Erkenntnissen von 873 Cybersecurity-Experten soll dieser Bericht ein Leitfaden für IT- und Security-Experten sein, die ihr Hybrid- und Multi-Cloud-Sicherheitsprofil stärken und gleichzeitig Innovationen vorantreiben möchten.

## Wesentliche Ergebnisse dieses Berichts:

- **Starker Trend zu Hybrid- und Multi-Cloud-Strategien:** Über 78 % der Befragten verlassen sich auf mindestens zwei Cloud-Anbieter. Das unterstreicht die wachsende Bedeutung von Multi-Cloud-Ansätzen für eine höhere Ausfallsicherheit und Spezialfunktionen. Für maximale Flexibilität und Kontrolle setzen bereits 54 % der Unternehmen auf Hybrid-Cloud-Modelle, die On-Premises- und Public-Cloud-Umgebungen integrieren.
- **Größte Bedenken bei der Sicherheit und Compliance:** Gegen die Cloud-Einführung sprechen bei 61 % der Unternehmen vor allem ungelöste Sicherheits- und Compliance-Fragen – konkret wie sich gesetzliche Anforderungen erfüllen und vertrauliche Daten zuverlässig schützen lassen.
- **Qualifikationslücken bei der Cloud-Sicherheit:** 76 % der Unternehmen berichten von mangelnden Cloud-Sicherheitskenntnissen und betonen die Notwendigkeiten von Automatisierung, gezielter Weiterbildung und Ressourcen-Optimierung.
- **Wenig Vertrauen in die Echtzeit-Bedrohungserkennung:** 64 % der Befragten bezweifeln, dass ihr Unternehmen Bedrohungen in Echtzeit erkennen kann.
- **Einheitliche Cloud-Sicherheitsplattformen:** 97 % der Befragten favorisieren eine einheitliche Plattform für die Cloud-Sicherheit mit zentralen Dashboards, um mehr Transparenz über alle Cloud-Lösungen zu gewinnen sowie einheitliche Richtlinien konfigurieren und konsequent durchsetzen zu können.
- **Schnelle Einführung eines Cloud Security Posture Management (CSPM) sowie von Cloud-Native Application Protection Platforms (CNAPP):** Um Fehlkonfigurationen und Compliance-Lücken anzugehen, implementieren derzeit 67 % der Befragten ein Sicherheitsprofil-Management für die Cloud (CSPM) und 62 % eine cloudnative Plattform für den Anwendungsschutz (CNAPP).



Dieser Bericht unterstreicht die Bedeutung einheitlicher Cloud-Sicherheitslösungen, die die Richtliniendurchsetzung optimieren, die Bedrohungserkennung automatisieren und einen konsequenten Schutz in Hybrid- und Multi-Cloud-Umgebungen gewährleisten. Wir haben für Sie die wesentlichen Ergebnisse und Best Practices zusammengestellt, damit Sie für Ihr Unternehmen ein robustes Cloud-Sicherheitsprofil realisieren können, das sich an neue Bedrohungen und dynamische Geschäftsanforderungen flexibel anpasst.

Unser besonderer Dank gilt [Fortinet](#), einem weltweit führenden Unternehmen im Bereich Cloud-Sicherheit, dessen Expertise und Insights zum Schutz von Hybrid- und Multi-Cloud-Umgebungen die Ergebnisse in diesem Bericht wesentlich gestärkt haben.

Wir hoffen, mit diesem Bericht allen IT- und Cybersecurity-Experten eine wertvolle Ressource zur Hand zu geben, damit die schnelle Einführung von Cloud-Lösungen auf sicheren Füßen steht.

Ihr

*Holger Schulze*

Gründer von Cybersecurity Insiders

# Strategiewechsel bei der Cloud-Bereitstellung

Welche Strategie ein Unternehmen für die Cloud-Bereitstellung wählt, wirkt sich direkt auf seine Sicherheitsanforderungen, Geschäftsergebnisse und Infrastrukturplanung aus. Angesichts der Vielschichtigkeit heutiger IT-Umgebungen ist dies eine zentrale Entscheidung.

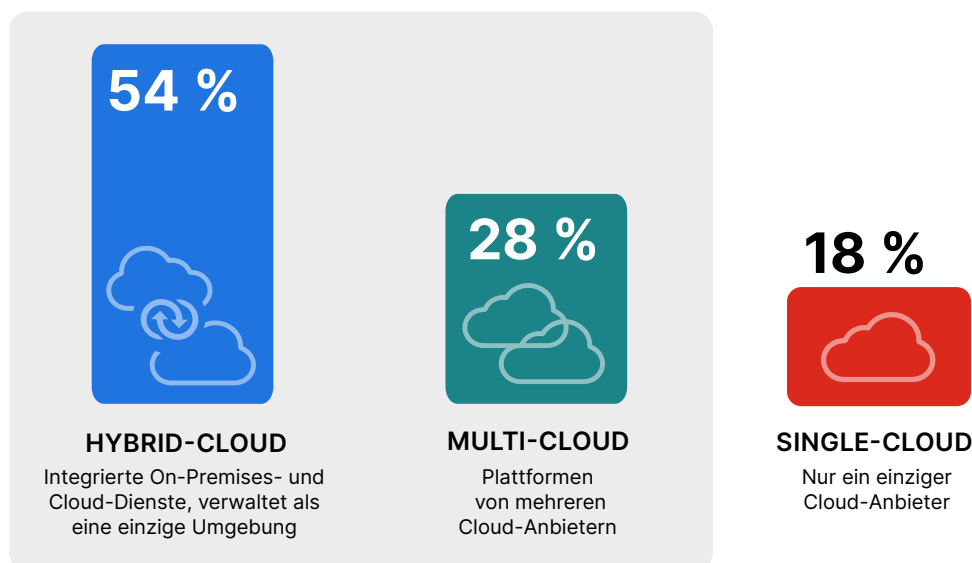
Hybrid-Cloud-Strategien sind derzeit am beliebtesten: 54 % der Befragten haben sich dafür entschieden (gegenüber 43 % im Vorjahr). Diese Zunahme zeigt eine starke Abkehr von einer einzigen Cloud-Lösung hin zur Integration mehrerer Cloud-Anbieter mit On-Premises-Systemen. Eine Einzelhandelskette kann z. B. kundenorientierte Anwendungen in der Public Cloud bereitstellen, aber wegen der Compliance-Anforderungen (wie PCI DSS) sensible Zahlungsdaten nur im eigenen On-Premises-System verarbeiten. Mit solchen hybriden Strategien profitieren Unternehmen von der Skalierbarkeit der Public Cloud, ohne die Kontrolle über wichtige Daten aus der Hand zu geben.

Auf Platz 2 folgen Multi-Cloud-Bereitstellungen mit 28 %. Unternehmen verteilen bei dieser Strategie Workloads auf mehrere Anbieter, um Abhängigkeiten zu vermeiden oder bestimmte Funktionen zu erhalten. Ein Technologieunternehmen kann z. B. rechenintensive Anwendungen auf Amazon Web Services (AWS) hosten und gleichzeitig die fortschrittlichen KI-Dienste von Google Cloud für die Datenanalyse nutzen. So lässt sich eine optimale Leistung erreichen, ohne sich an einen einzigen Anbieter zu binden.

Single-Cloud-Bereitstellungen gehen zurück: Nur noch 18 % verlassen sich auf einen einzigen Cloud-Anbieter (gegenüber 22 % in 2024). An der Verwendung eines einzigen Cloud-Anbieters wird meistens wegen des einfachen Managements festgehalten, selbst wenn das weniger Flexibilität bedeutet. Kleinere Unternehmen können dieses Modell bevorzugen, wenn z. B. ausschließlich Microsoft Azure für die Dokumentenspeicherung und das Workflow-Management genutzt wird.

## ► Welche Hauptstrategie verfolgt Ihr Unternehmens bei der Cloud-Bereitstellung?

**82 %** der Unternehmen haben eine Multi-Cloud- oder Hybrid-Umgebung

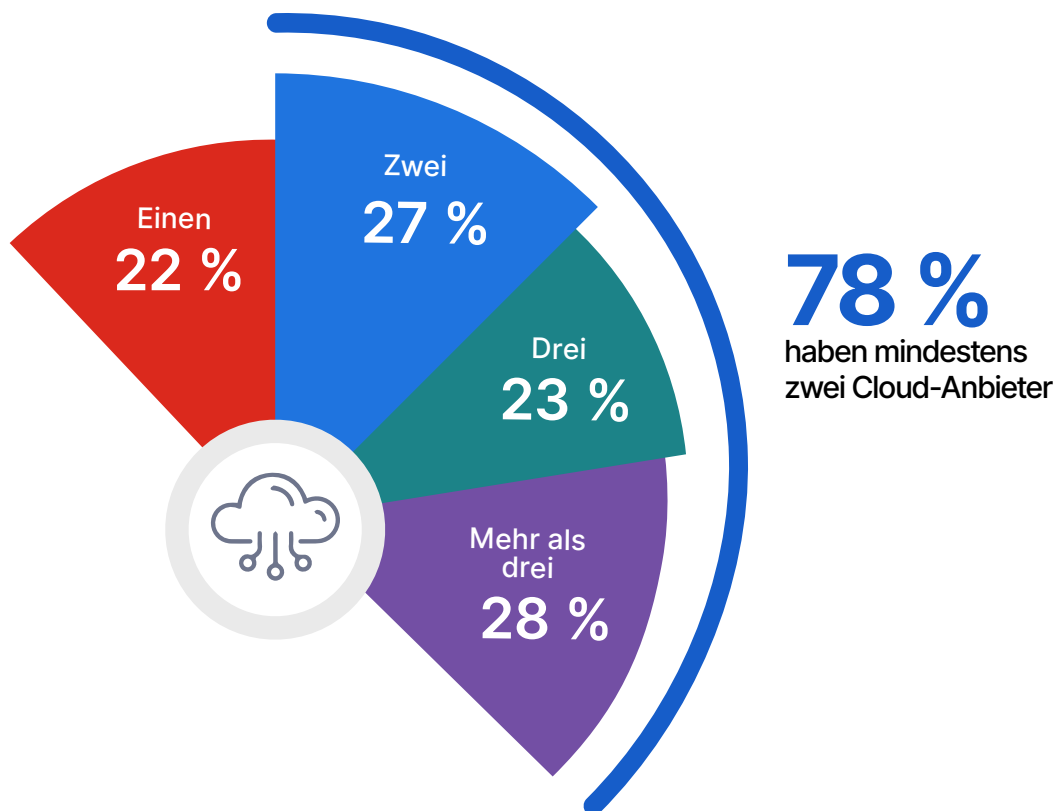


# Klarer Trend zur Multi-Cloud

Die Anzahl der Cloud-Anbieter pro Unternehmen steigt. Das spiegelt die höhere Präferenz für Hybrid- und Multi-Cloud-Strategien wider – und die damit verbundene operative Komplexität.

Die Umfrageergebnisse zeigen, dass 78 % der Unternehmen mindestens zwei Cloud-Anbieter haben (71 % im Vorjahr). Dies ist ein Anstieg um 7 %, der den zunehmenden Trend zu mehreren Clouds unterstreicht. Ein multinationales Unternehmen kann z. B. AWS für sein globales Content Delivery Network verwenden und sich in Regionen mit strengen Gesetzen für die Datenaufbewahrung auf die Compliance-fähigen Angebote von Microsoft Azure verlassen. Durch den strategischen Einsatz mehrerer Anbieter können Unternehmen spezielle Funktionen (wie KI-Dienste von Google Cloud oder die Datenbankkompetenz von Oracle Cloud) nutzen und erhalten gleichzeitig die nötige Redundanz, um die Ausfallsicherheit zu gewährleisten.

## ► Wie viele Cloud-Anbieter nutzt Ihr Unternehmen derzeit?





# Dominanz der großen Cloud-Anbieter

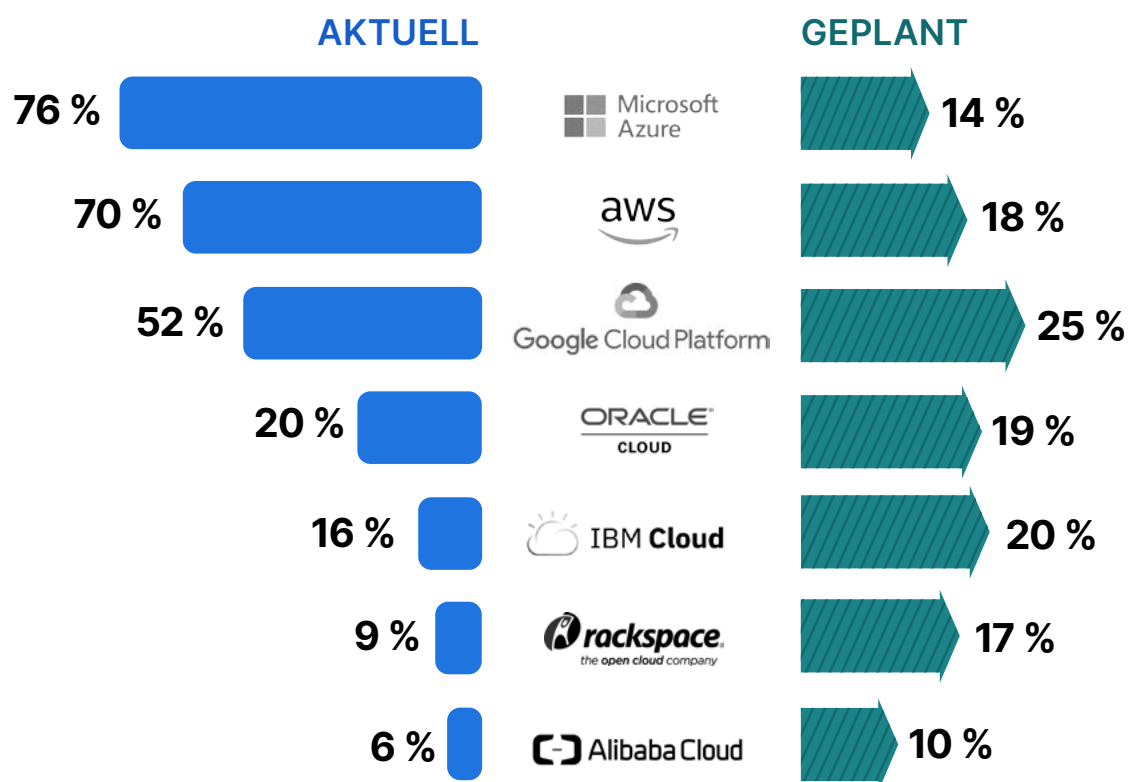
Welche Cloud-Anbieter Unternehmen derzeit nutzen und welche sie künftig einsetzen wollen, gibt Aufschluss darüber, wie Unternehmen ihre Cloud-Strategien an veränderte Workloads und spezielle Funktionen anpassen.

Microsoft Azure und AWS sind hier die dominierenden Akteure, auf die 76 % bzw. 70 % der Befragten nach eigenen Angaben vertrauen.

Aber auch die Google Cloud Platform gewinnt an Beliebtheit: 52 % der Befragten nutzen sie bereits, 25 % planen dies für die Zukunft.

Die Marktanteile von Oracle Cloud und IBM Cloud sind zwar geringer, aber das Interesse für die Zukunft ist groß. Das dürfte wahrscheinlich an der Erfahrung dieser Cloud-Anbieter bei der Integration von Legacy-Unternehmenssystemen zurückgehen.

- Welche(n) Cloud-IaaS-Anbieter nutzen Sie aktuell oder planen Sie in Zukunft zu verwenden?  
(Alle Zutreffenden auswählen)



# Überwinden von Hürden für die Cloud-Einführung

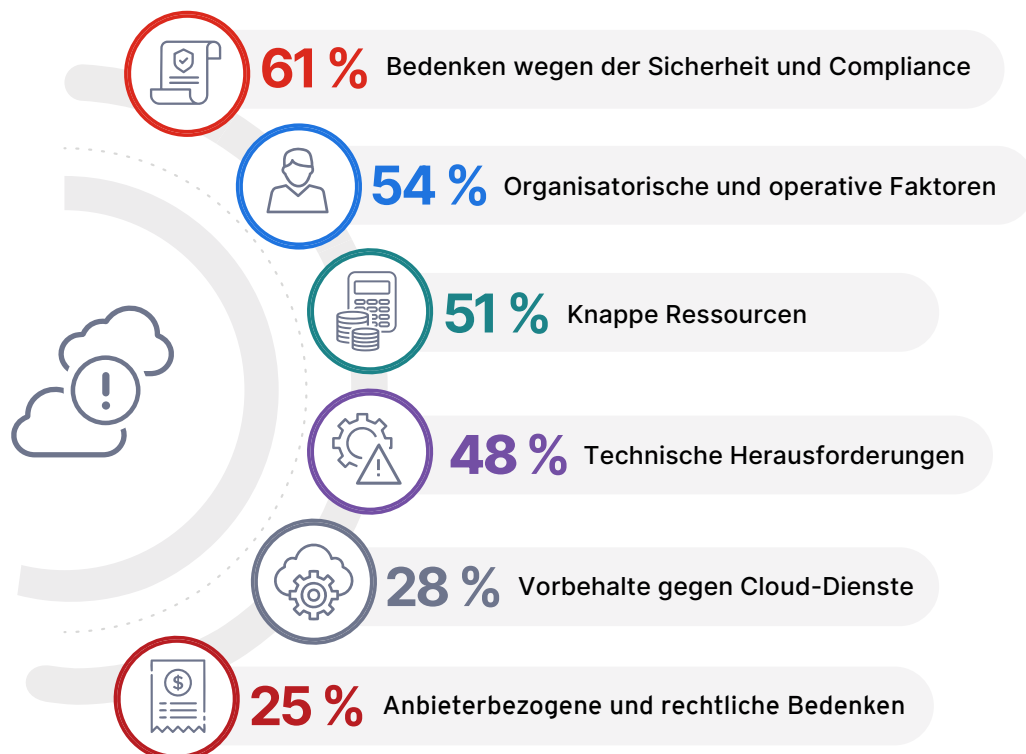
Die Ergebnisse geben Aufschluss über die größten Herausforderungen bei der Cloud-Einführung. IT- und Security-Teams müssen diese Schwierigkeiten angehen, damit das volle Potenzial von Cloud-Umgebungen zum Tragen kommt.

Am häufigsten sind Bedenken wegen der Sicherheit und Compliance, die 61 % der Befragten anführen (gegenüber 59 % im Vorjahr). Aspekte wie Datenlecks oder die Komplexität gesetzlicher Anforderungen sind immer mehr ein Thema und drohen die Cloud-Einführung auszubremsen. Denkbar ist z. B., dass Gesundheitsdienstleister die Verlagerung vertraulicher Patientendaten in die Cloud hinauszögern, weil man beim Datenschutz nichts riskieren will.

Organisatorische und operative Faktoren folgen mit 54 % dicht dahinter auf Platz 2 (49 % im Vorjahr). Herausforderungen wie Widerstand gegen Veränderungen, Bedenken wegen einer Anbieterabhängigkeit und Probleme mit der Unternehmenskultur werden hier am häufigsten genannt. Ein Fertigungsunternehmen kann z. B. bei der Migration von Altsystemen in die Cloud auf internen Widerstand stoßen, weil ein Kontrollverlust über proprietäre Prozesse befürchtet wird.

51 % der Befragten (49 % in 2024) nennen knappe Ressourcen wie begrenzte Budgets oder fehlende Mitarbeiterkenntnisse als Hürden bei der Cloud-Einführung – ebenfalls typische Schwierigkeiten, die viele Unternehmen beim Management und Schutz von Cloud-Kapazitäten haben. Technische Herausforderungen sind in diesem Jahr zwar mit 48 % etwas weniger ausgeprägt, stellen jedoch immer noch ein erhebliches Hindernis dar, insbesondere bei der Integration komplexer Hybrid-Cloud-Umgebungen.

## ► Was sind die größten Hürden für die Cloud-Einführung in Ihrem Unternehmen? (Alles Zutreffende auswählen)



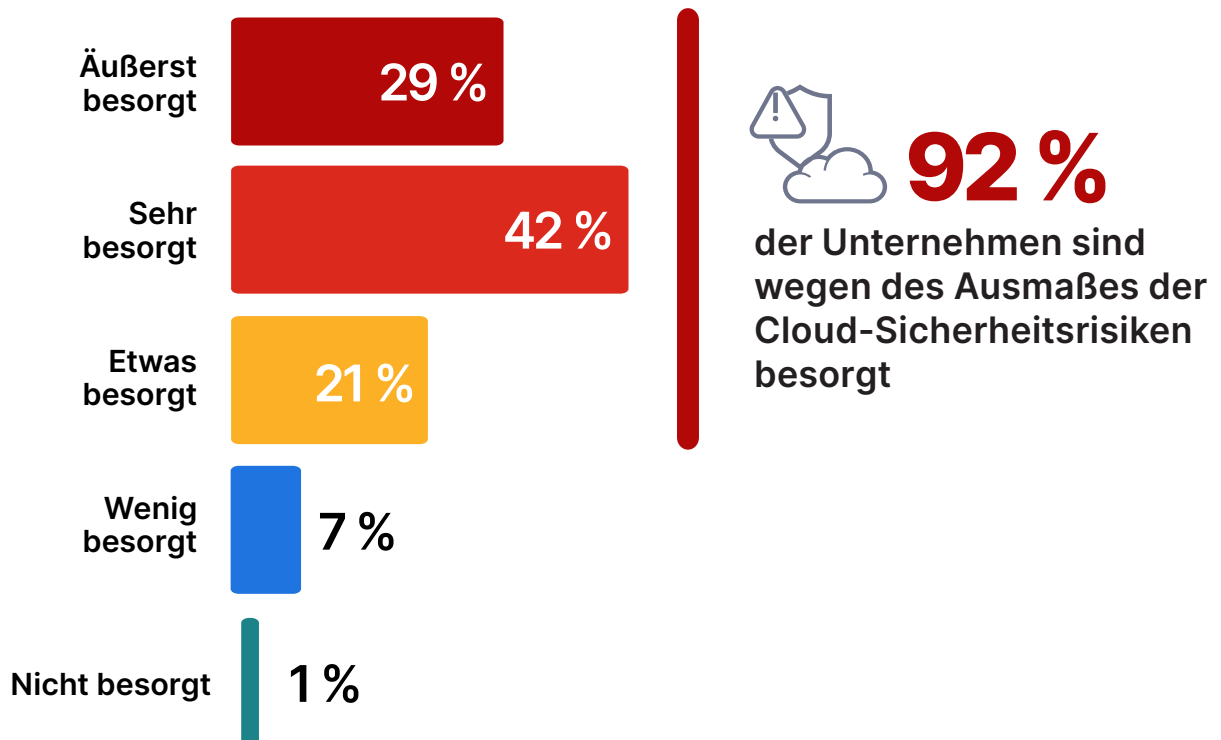
# Sicherheitsbedenken bei Public Clouds

Die anhaltenden Bedenken wegen der Sicherheit von Public Clouds spiegeln den Balance-Akt wider, die Vorteile von Skalierbarkeit und Agilität mit dem nötigen robusten Schutz unter einen Hut zu bringen.

Bemerkenswerte 92 % der Befragten sind besorgt wegen der Sicherheit von Public Clouds. Hier besteht akuter Handlungsbedarf. IT- und Cybersecurity-Experten sollten diesen wichtigen Punkt unbedingt angehen.

Diese Befürchtung deckt sich mit den Umfrageergebnissen: 61 % der Befragten nennen die Sicherheit und Compliance als Haupthindernis für die Cloud-Einführung. Ein Finanzdienstleister kann z. B. die Verlagerung von Kunden-Transaktionsdaten in die Cloud verzögern, weil man kein Risiko eingehen will, durch Fehlkonfigurationen die Compliance oder die Sicherheit sensibler Informationen zu gefährden. Dazu erschweren konkrete Bedenken den Umstieg auf die Cloud – wie das Risiko von Datenlecks, Unklarheiten bei der gemeinsamen Verantwortung oder die begrenzte Transparenz über Aktivitäten von Cloud-Anbietern.

## ► Wie besorgt sind Sie wegen der Sicherheit von Public Clouds?





# Operative Herausforderungen bei der Cloud-Sicherheit

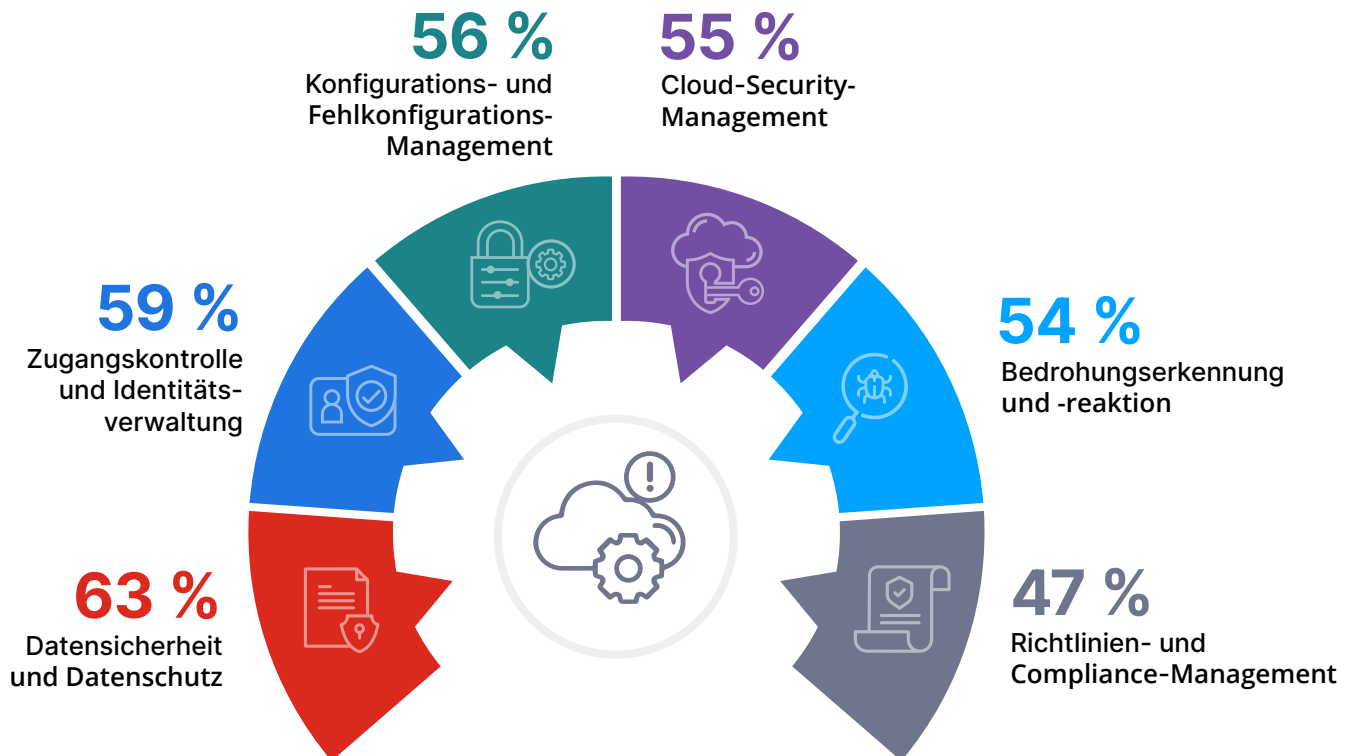
Der tägliche Aufwand, den die Cloud-Sicherheit für die Security Operations bedeutet, zeigt, mit welch komplexen, dynamischen Schwierigkeiten Unternehmen beim Schutz ihrer Umgebungen konfrontiert sind.

Datensicherheit und Datenschutz sehen 63 % der Befragten als wichtigstes Anliegen. Das spiegelt die anhaltende Sorge um den Schutz sensibler Informationen und die Verhinderung von Datenlecks wider. An zweiter Stelle folgen die Zugangskontrolle und Identitätsverwaltung (59 %), was die Notwendigkeit einer robusten Authentifizierung und Verwaltung der Zugriffsrechte unterstreicht. Bei Hybrid-Cloud-Implementierung kann es z. B. schwierig sein, die Zugriffsrichtlinien für Benutzer zwischen On-Premises-Systemen und Cloud-Plattformen zu synchronisieren.

Das Konfigurations- und Fehlkonfigurationsmanagement liegt mit 56 % knapp an dritter Stelle. Dies verdeutlicht die operativen Schwierigkeiten bei der Aufrechterhaltung korrekter Cloud-Konfigurationen, wie die Überwachung von unbeabsichtigten öffentlichen Freigaben von Cloud-Speicher-Buckets. Solche Szenarien haben in der Vergangenheit bereits zu Sicherheitsvorfällen geführt, die Schlagzeilen machten.

Aspekte wie das Cloud-Security-Management (55 %), die Bedrohungserkennung und -reaktion (54 %) sowie das Richtlinien- und Compliance-Management (47 %) unterstreichen gemeinsam den Bedarf an einheitlichen, skalierbaren Lösungen zur Verwaltung von Multi-Cloud-Umgebungen.

## ► Was sind Ihre größten Herausforderungen beim täglichen Cloud-Security-Management? (Alles Zutreffende auswählen)



Weitere Antworten sind:

Schatten-IT und unberechtigte App-Nutzung 46 % | Cloud-Integration und Automatisierung 43 % | Endpunktsicherheit 40 % | Ressourcenzuweisung 38 %  
DevSecOps-Praktiken 31 % | Operative Agilität und Komplexität 25 %

# Schutz von Multi-Cloud-Umgebungen

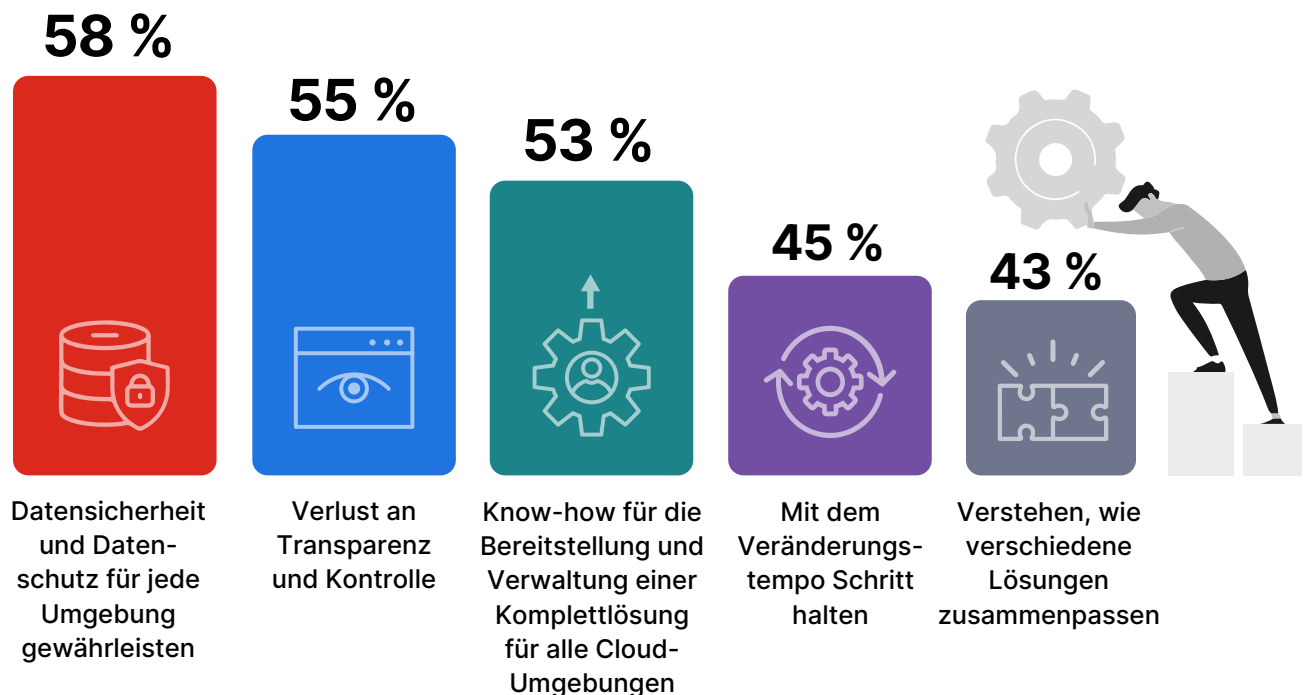
Die Sicherheit von Multi-Cloud-Umgebungen bringt besondere Schwierigkeiten mit sich. Solche Umgebungen sind komplex, nicht standardisiert und basieren auf Technologien, die sich schnell weiterentwickeln. All das verkompliziert den Schutz von vertraulichen Daten, führt regelmäßig zu ineffizienten Abläufen und erschwert das Management der verschiedenen Cloud-Ökosysteme.

Die Gewährleistung der Datensicherheit und des Datenschutzes in jeder Umgebung bleibt weiterhin die größte Herausforderung für 58 % der Befragten (55 % in 2024). Frühere Ergebnisse unserer Umfrage gingen in die gleiche Richtung: Auch da wurden die Datensicherheit und der Datenschutz als wichtigstes operatives Problem (63 %) genannt, was die Notwendigkeit einer einheitlichen Sicherheit für fragmentierte Cloud-Infrastrukturen betont.

Der Verlust an Transparenz und Kontrolle (55 %) zeigt, wie schwierig es ist, in Multi-Cloud-Konfigurationen den Überblick zu behalten – eine Sorge, die bereits zuvor geäußert wurde, als 55 % das Cloud-Security-Management als tägliche Herausforderung bezeichneten.

53 % der Befragten geben an, dass ihren Teams das nötige Know-how für die Bereitstellung und Verwaltung einer Komplettlösung für alle Cloud-Umgebungen fehlt. Herausforderungen wie Anpassungen an dynamische Entwicklungen, um mit dem Veränderungstempo Schritt zu halten (45 %), oder das Verstehen, wie verschiedene Lösungen zusammenpassen (43 %), spiegeln die operativen und strategischen Hürden wider, die die rasante Entwicklung von Cloud-Technologien oft begleitet.

## ► Was sind Ihre größten Herausforderungen beim Schutz von Multi-Cloud-Umgebungen? (Alles Zutreffende auswählen)



Weitere Antworten sind:

Kostenmanagement für unterschiedliche Lösungen 41 % | Kenntnis der Optionen für die Dienstintegration 40 % | Bereitstellung eines nahtlosen Benutzerzugangs basierend auf den Anmeldedaten 37 % | Auswahl der richtigen Dienste 30 % | Sonstiges 1 %

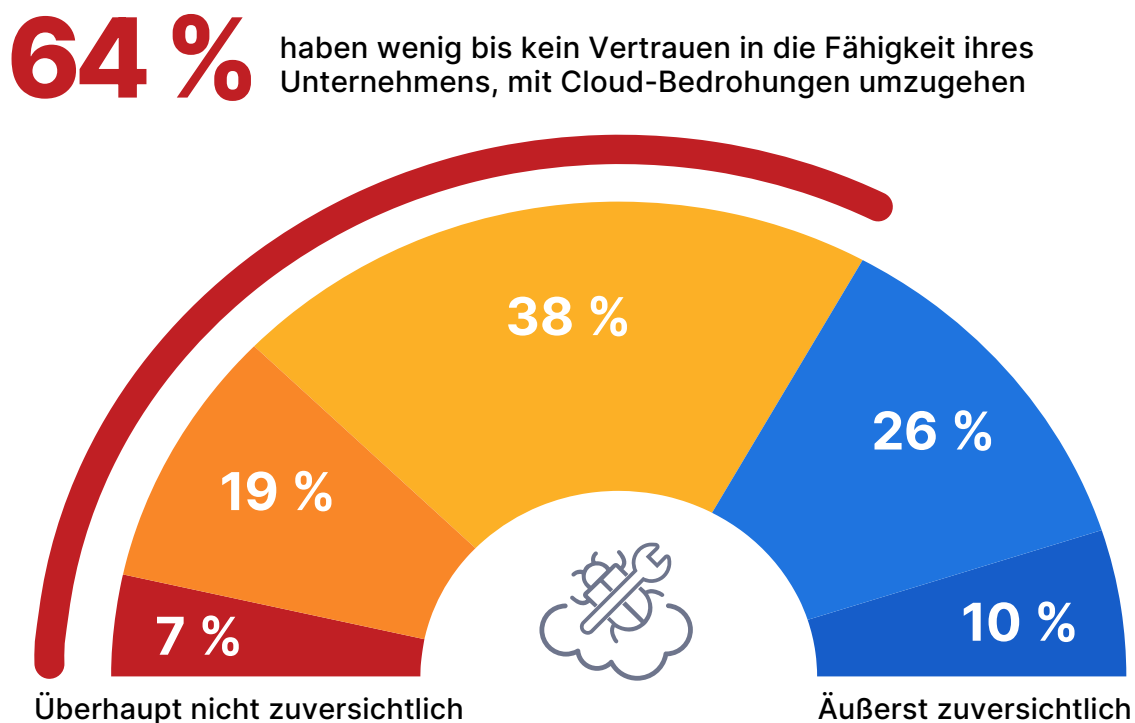
# Geringes Vertrauen in die Echtzeit-Erkennung von Bedrohungen

Die Fähigkeit, Bedrohungen in Cloud-Umgebungen in Echtzeit zu erkennen und darauf zu reagieren, ist entscheidend, wenn Unternehmen zunehmend komplexere Multi-Cloud- und Hybrid-Strategien implementieren. Diese Architekturen bringen einzigartige Herausforderungen mit sich, wenn eine nahtlose Transparenz und schnelle Reaktionsfähigkeit über unterschiedliche Plattformen hinweg erreicht werden soll.

Die Antworten der Befragten zeigen einen erheblichen Mangel an Vertrauen in die Fähigkeit ihres Unternehmens, mit Cloud-Bedrohungen umzugehen: 64 % bezweifeln, dass Bedrohungen in Echtzeit erkannt werden können. Wenn z. B. der Zusammenhang zwischen einzelnen bösartigen Aktionen nicht bemerkt wird, kann das die Identifizierung und Reaktion auf einen potenziellen Sicherheitsvorfall erheblich verzögern. Dieses fehlende Vertrauen deutet darauf hin, dass viele Unternehmen zwar grundlegende Sicherheitsmaßnahmen implementiert haben, die zunehmende Komplexität von Cloud-Bedrohungen und das schwierige Management verschiedener Umgebungen sie jedoch anfällig für hochkomplexe Angriffe und Fehlkonfigurationen machen. Die zuvor erwähnten Umfrageergebnisse belegen das und zeigen, dass der Verlust an Transparenz und Kontrolle (55 %) sowie Probleme bei der Bedrohungserkennung und -reaktion (54 %) die größten Hindernisse für die Cloud Security Operations sind.

Bei der Echtzeit-Bedrohungserkennung geben sich nur 10 % der Befragten äußerst zuversichtlich und weitere 26 % sehr zuversichtlich. Im Rückschluss bedeutet das, dass weniger als 40 % gut auf die Anforderungen eines modernen Cloud-Bedrohungsmanagements vorbereitet sind.

► Wie zuversichtlich sind Sie, dass Ihr Unternehmen Bedrohungen in allen Ihren Cloud-Umgebungen in Echtzeit erkennen und darauf reagieren kann?



■ Überhaupt nicht zuversichtlich ■ Wenig zuversichtlich ■ Etwas zuversichtlich ■ Sehr zuversichtlich ■ Äußerst zuversichtlich

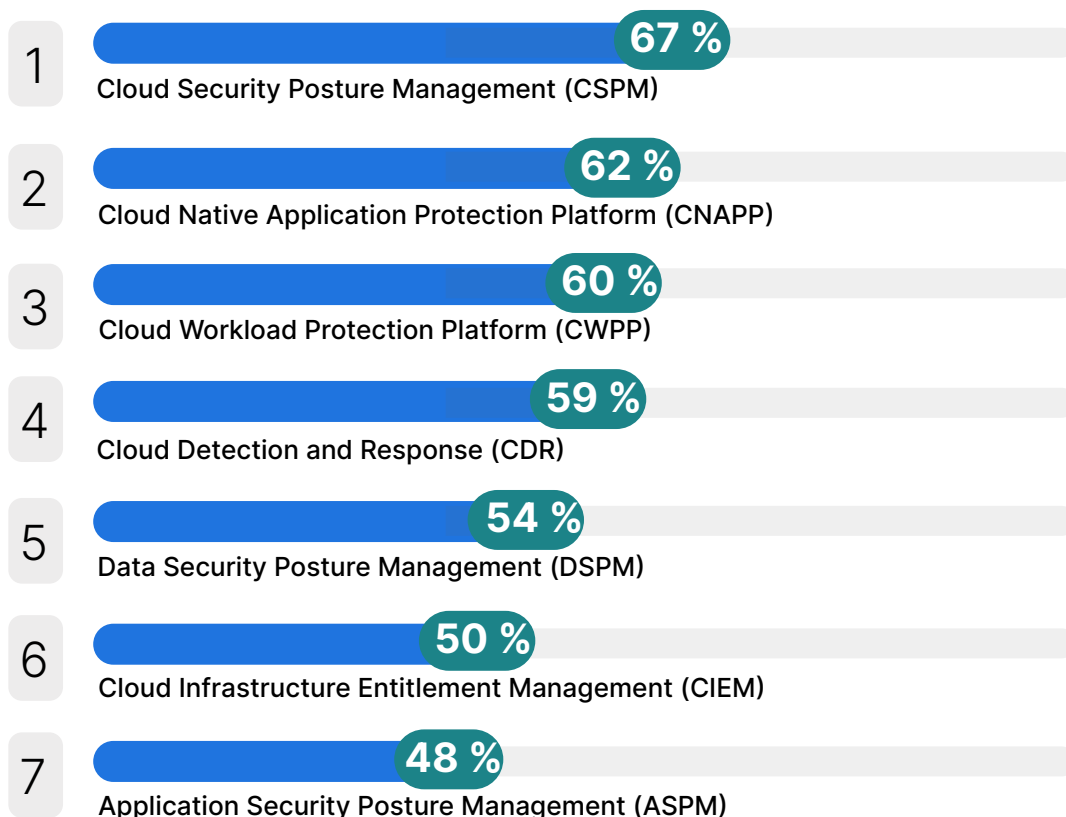
# Prioritäten bei der Cloud-Sicherheit

Je mehr Unternehmen auf die Cloud setzen, desto wichtiger wird die richtige Mischung aus Security-Funktionen, damit trotz zunehmender Bedrohungen die Resilienz, Compliance und operative Effizienz gegeben ist.

Bei den Prioritäten, welche wichtigen Cloud-Security-Tools in den nächsten 12 Monaten eingeführt werden sollen, liegt das Cloud Security Posture Management (CSPM) mit 67 % an der Spitze. Das unterstreicht die entscheidende Rolle, die ein gemanagtes Cloud-Sicherheitsprofil bei der Erkennung und Behebung von Fehlkonfigurationen in Cloud-Umgebungen spielt. Ein CSPM-Tool könnte z. B. ein Einzelhandelsunternehmen vor öffentlich zugänglichen Speicher-Buckets in AWS warnen und so kostspielige Datenverluste verhindern.

Die Notwendigkeit einer durchgängigen Sicherheit für den gesamten Lebenszyklus von Anwendungen ist ebenfalls zunehmend bekannt: 62 % der Befragten wollen mit einer Cloud Native Application Protection Platform (CNAPP) einen cloudnativen Anwendungsschutz einführen. Eine CNAPP kann z. B. proaktiv Schwachstellen in containerisierten Kubernetes-Workloads aufzeigen, bösartige Aktivitäten zur Laufzeit identifizieren und Ereignisketten erkennen, die auf eine Kompromittierung hindeuten. Knapp dahinter werden mit 60 % Cloud Workload Protection Platforms (CWPP) und Cloud Detection and Response (CDR) mit 59 % genannt. Das zeigt den zunehmenden Schwerpunkt auf den Workload-Schutz und die Bedrohungsabwehr, insbesondere in Multi-Clouds. Die Einführung eines Cloud Infrastructure Entitlement Management (CIEM), die 50 % der Befragten planen, verdeutlicht einen weiteren Sicherheitsbedarf: robuste Kontrollen für den Zugang und die Zugriffsrechte über verschiedene Cloud-Plattformen hinweg sowie die Implementierung eines Least-Privilege-Ansatzes und die Eliminierung nicht mehr benötigter Anmeldedaten.

► **Welche der folgenden Sicherheitsfunktionen verwenden Sie aktuell oder planen Sie, in den nächsten 12 Monaten zu nutzen?**  
(Alle Zutreffenden auswählen)



# Angehen von Qualifikationslücken bei der Cybersecurity

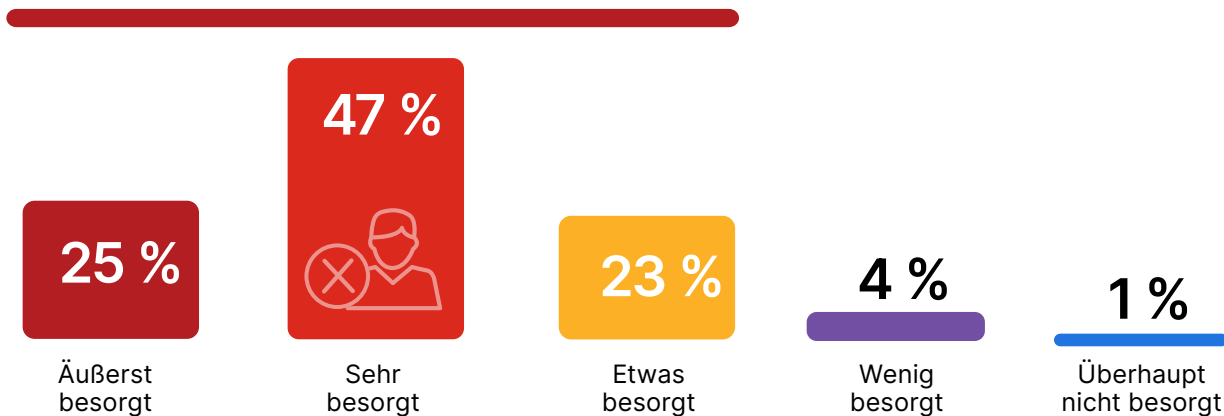
Der branchenweite Mangel an qualifizierten Cybersecurity-Experten bleibt weiterhin ein kritisches – und womöglich kostspieliges – Problem, wenn ein Unternehmen seine Ressourcen nicht richtig schützen und wirksam auf neu aufkommende Bedrohungen reagieren kann.

95 % der Befragten sind etwas bis äußerst besorgt über den anhaltenden Fachkräftemangel im Cybersecurity-Bereich. Unternehmen stehen massiv unter Druck, qualifizierte Mitarbeitende zu gewinnen und zu halten, um die immer komplexeren Cybersecurity-Probleme in den Griff zu bekommen. Nehmen wir z. B. einen Gesundheitsdienstleister, bei dem sich die Implementierung von Multi-Cloud-Sicherheitskontrollen verzögert, weil niemand im Team sich mit dem Cloud-Konfigurationsmanagement oder CIEM auskennt.

## ► Wie besorgt sind Sie wegen des branchenweiten Fachkräftemangel an qualifizierten Cybersecurity-Experten?

# 95 %

der Unternehmen sind wegen des branchenweiten Fachkräftemangels an qualifizierten Cybersecurity-Experten etwas bis äußerst besorgt



Die Sorge ist berechtigt: Laut den Umfragedaten fehlen in 76 % der Unternehmen derzeit Fachkräfte für Cybersecurity.

## ► Gibt es in Ihrem Unternehmen einen Mangel an Cybersecurity-Experten?



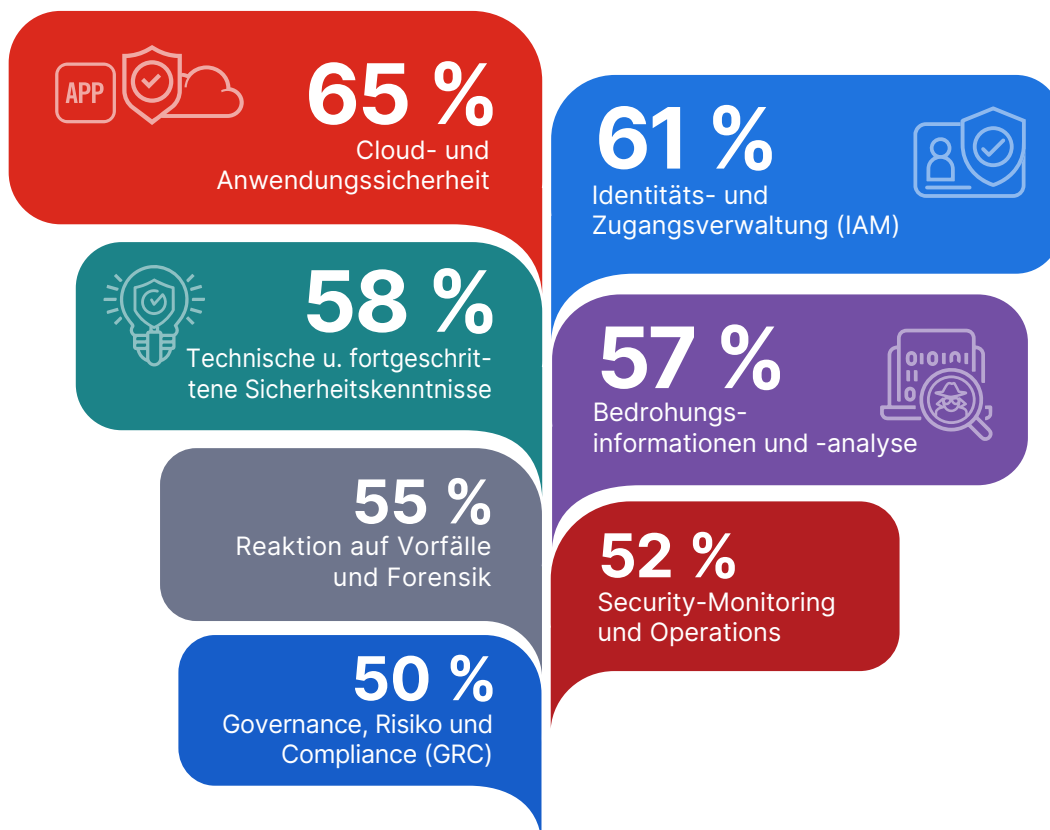
# Wichtige Sicherheitskenntnisse für den Schutz vor aktuellen Bedrohungen

Vielfältiges Fachwissen, das stets auf dem neuesten Stand ist – so lässt sich der dringende Bedarf an Sicherheitskenntnissen auf den Punkt bringen, der Unternehmen zur Bewältigung der immer komplexeren Cloud-Sicherheit fehlt.

Fachkenntnisse der Cloud- und Anwendungssicherheit haben mit 65 % oberste Priorität für Unternehmen, z. B. um Code für automatisierte Sicherheitskontrollen oder skalierbare, sichere „Landungsbereiche“ für bestimmte Cloud-Plattformen zu entwickeln und bereitzustellen.

Dicht dahinter folgt mit 61 % die Identitäts- und Zugangsverwaltung. Darin zeigt sich die Notwendigkeit von robusten Zugangskontrollen und einem einheitlichen Management der Benutzerrechte, was besonders in Hybrid- und Multi-Cloud-Umgebungen unerlässlich ist. Technische und fortgeschrittene Sicherheitskenntnisse (58 %) sowie Bedrohungsinformationen und -analysen (57 %) spiegeln die steigende Nachfrage nach Fachexperten wider, die wissen, wie man KI richtig einsetzt und wie hochkomplexe Angriffstaktiken funktionieren. Das alles ist wichtig, damit bösartige Aktivitäten schnell erkannt und eingedämmt werden, insbesondere bei kompromittierten Cloud-Administratorkonten. Auch fundiertes Fachwissen über die richtige Reaktion auf Vorfälle und Forensik-Kenntnisse (55 %) bleiben für die Eindämmung von Sicherheitsverletzungen unverzichtbar. Gleiches gilt für Fachkenntnisse im Bereich Security Monitoring und Security Operations (52 %), damit Anomalien rechtzeitig erkannt und Angriffe schnell abgewehrt werden.

## ► Welche Sicherheitskenntnisse sind in Ihrem Unternehmen am wichtigsten? (Alle Zutreffenden auswählen)



Weitere Antworten sind:

Schulung und Sensibilisierung 45 % | Kommunikation und Strategie 39 % | Nicht sicher 3 %



# Trends bei Investitionen in die Cloud-Sicherheit

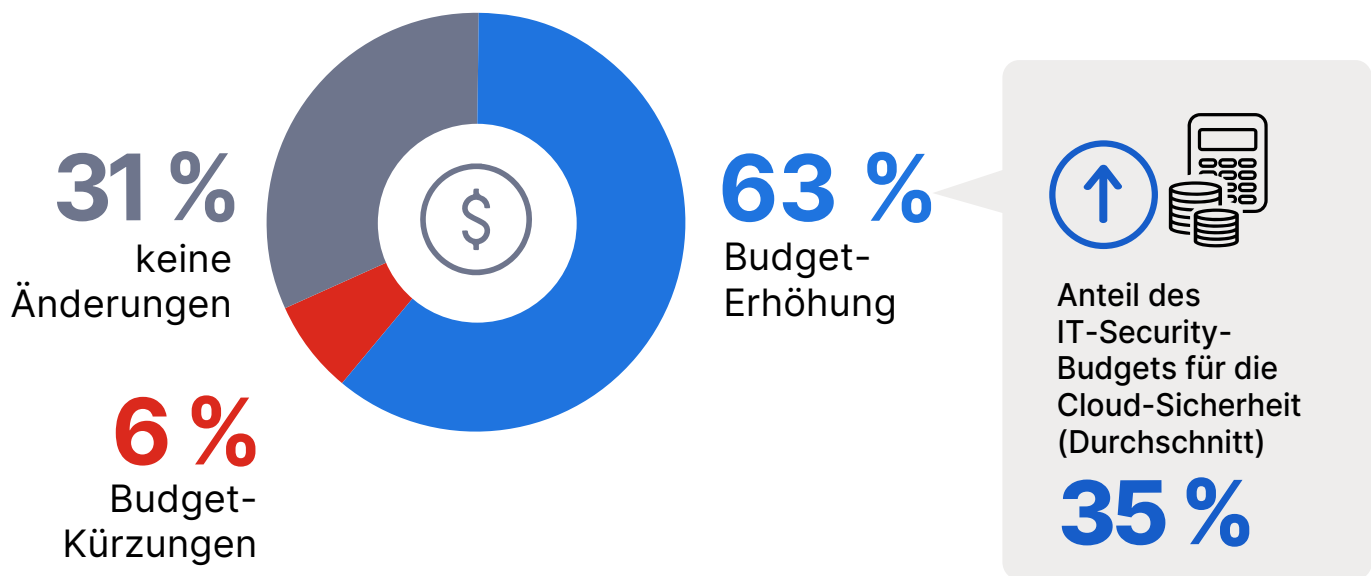
Die Umfrageergebnisse geben neuen Einblick über die finanziellen Prioritäten von Unternehmen, um Cloud-Umgebungen besser zu schützen. Die Mehrheit der Befragten (63 %) will in den nächsten 12 Monaten ihr Cloud-Security-Budget erhöhen (61 % im Vorjahr). Offensichtlich ist weithin bekannt, wie notwendig ein starker Bedrohungsschutz für Hybrid- und Multi-Clouds ist.

31 % der Befragten halten am gleichen Budget wie im Vorjahr fest (32 % in 2024). Wahrscheinlich haben diese Unternehmen gleichbleibende operative Anforderungen oder bereits stark investiert. Nur 6 % rechnen mit Budget-Kürzungen, was angesichts zunehmender Cloud-Bedrohungen und Vorschriften eher die Ausnahme ist.

Durchschnittlich 35 % der IT-Security-Budgets sind nicht mehr eigenständig, sondern fallen unter die allgemeinen Sicherheitsausgaben. Dies zeigt, dass Unternehmen infolge der stärkeren Cloud-Nutzung auch den Schutz dieser Umgebungen als finanziellen Schwerpunkt sehen.

Diese wachsende Bedeutung von Investitionen in die Cloud-Sicherheit spricht für einen proaktiven Ansatz, um Lücken bei der Transparenz, Zugangskontrolle und Bedrohungserkennung zu schließen – Herausforderungen, die in diesem Bericht immer wieder genannt werden. Unternehmen, die Budget-Erhöhungen planen, sollten sich auf Lösungen konzentrieren, die wichtige Funktionen wie CNAPP effizient integrieren, um mit ihren Investitionen in die Sicherheit eine maximale Wirkung zu erzielen.

## ► Inwiefern rechnen Sie mit Änderungen beim Budget für die Cloud-Sicherheit in den nächsten 12 Monaten?



# Der Wert einheitlicher Cloud-Sicherheitsplattformen

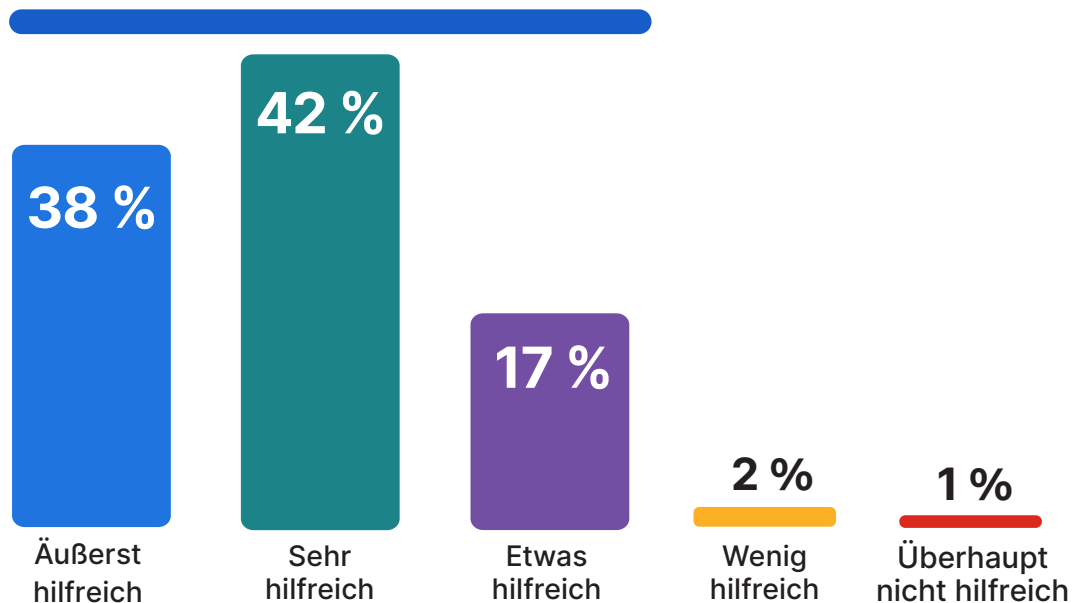
Eine einzige, gemeinsame Plattform für die Cloud-Sicherheit mit einem zentralen Dashboard bringt mehrere Vorteile, wie z. B. eine einfachere Richtlinienkonfiguration, stärkere Einheitlichkeit und höhere Transparenz über alle Cloud-Umgebungen.

Die Umfrageergebnisse zeigen ein überwältigendes Interesse an diesem Konzept: 97 % der Befragten finden eine solche Plattform etwas bis äußerst hilfreich. Mit einem einzigen, zentralen Dashboard könnte z. B. ein Finanzdienstleister einheitliche Zugangskontrollen für AWS, Azure und Google Cloud durchsetzen und die Wahrscheinlichkeit von Konfigurationsfehlern verringern. Dies steht im Einklang mit früheren Ergebnissen, bei denen 55 % der Befragten Transparenz- und Kontrollverluste als größte Multi-Cloud- und Hybrid-Herausforderungen nannten und dafür die Notwendigkeit zentraler Lösungen betonten.

- **Wie hilfreich wäre es, eine einzige Cloud-Sicherheitsplattform mit einem einzigen Dashboard zum Konfigurieren aller Richtlinien zu haben, um Daten einheitlich und umfassend in allen Clouds zu schützen?**

**97 %** 

der Unternehmen stimmen zu, dass ein einziges Dashboard für die Cloud-Sicherheit sehr bis äußerst hilfreich wäre.



# Best Practices für eine stärkere Hybrid- und Multi-Cloud-Sicherheit

Je mehr Unternehmen auf Hybrid- und Multi-Cloud-Umgebungen setzen, desto komplexer wird das Management unterschiedlicher Anbieter und die Aufrechterhaltung einer robusten Sicherheit. Ein wirksamer Schutz beginnt deshalb mit strategischen Best Practices, die aktuelle Erkenntnisse zum Thema Sicherheit berücksichtigen und fortschrittliche Sicherheitslösungen nutzen.

Im Folgenden finden Sie einige Tipps und umsetzbare Schritte, wie Sie Ihr Multi-Cloud-Sicherheitsprofil verbessern können.

1

## **AUTOMATISIERTE ERKENNUNG UND BEHEBUNG VON CLOUD-RISIKEN**

Fehlkonfigurationen sind eine häufige Schwachstelle. 67 % der Befragten gehen dieses Problem mit automatisierten Tools an oder planen deren Einführung. Mit einem ständigen Monitoring und Abhilfemaßnahmen in Echtzeit lassen sich Risiken wie falsch konfigurierte Speicherbereiche oder zu weit gefasste Berechtigungen proaktiv erkennen und effizient beheben. Automatisierte Tools vereinfachen zudem die Einhaltung von Branchenvorschriften – Stichwort „Compliance“.

2

## **SCHUTZ DER DATENFLÜSSE ZWISCHEN CLOUD-UMGEBUNGEN**

Bei Datenübertragungen zwischen Clouds muss die Sicherheit und Integrität der Daten jederzeit gegeben sein. Für 58 % der Befragten stehen deshalb die Datensicherheit und der Datenschutz ganz oben auf der Liste der Security-Prioritäten. Mit Tools, die umfassende Transparenz über Datenflüsse bieten, können Sie Informationen während der Übertragung leichter schützen, potenzielle Risiken im Blick behalten, unbefugten Zugriff verhindern, leichter Vorschriften wie die DSGVO erfüllen und so Ihre Datenschutzmaßnahmen insgesamt verbessern.

3

## **IMPLEMENTIERUNG EINHEITLICHER MECHANISMEN ZUR BEDROHUNGSERKENNUNG**

Über die Hälfte der Befragten (54 %) bezeichnen die Bedrohungserkennung und -reaktion in Multi-Cloud-Umgebungen als schwierig. Einheitliche Lösungen zur Bedrohungserkennung sind deshalb sinnvoll. IT-Teams erhalten damit zentrale Transparenz, um Anomalien schnell erkennen und darauf reagieren zu können. Lassen sich zudem Daten aus verschiedenen Cloud-Umgebungen korrelieren, bringt das noch kürzere Erkennungszeiten und präzisere Abwehrreaktionen.

4

## **INVESTITION IN CLOUD-SCHULUNGEN FÜR SECURITY-TEAMS**

In 76 % der Unternehmen fehlen Fachkräfte, die cloudnative Lösungen effektiv einsetzen und managen können. Durch die Weiterbildung von Mitarbeitern in Bereichen wie DevSecOps und Container-Sicherheit sind Teams besser in der Lage, aktuelle und künftige Sicherheits Herausforderungen zu bewältigen.

5

## **EINHEITLICHE SECURITY-DURCHSETZUNG MIT POLICY-AS-CODE**

43 % der Befragten gaben an, dass es ihnen schwerfällt, die Integration verschiedener Lösungen zu verstehen. Mit Policy-as-Code-Ansätzen lässt sich eine einheitliche Durchsetzung über alle Plattformen hinweg erreichen. Policy-as-Code vereinfacht Audits, ermöglicht ein automatisiertes Konfigurationsmanagement und sorgt so dafür, dass die Sicherheitskontrollen die Unternehmensanforderungen erfüllen.

6

**AUSRICHTUNG DER SECURITY-INVESTITIONEN AN APPLICATION-WORKLOADS**

Die Sicherheit auf Anwendungsebene wird immer wichtiger. 62 % der Befragten wollen deshalb umfassende Schutzplattformen einführen. Eine durchgängige Anwendungssicherheit – von der Entwicklung bis zur Laufzeit – sorgt für einen maßgeschneiderten Workload-Schutz und unterstützt gleichzeitig einheitliche Richtlinien in allen Umgebungen. Ideal sind Lösungen, die sich in Container-Umgebungen und in den Laufzeitschutz integrieren lassen.

7

**STANDARDISIERUNG DER ZUGANGSKONTROLLE FÜR ALLE CLOUD-PLATTFORMEN**

Die Zugangs- und Identitätsverwaltung bleibt für 59 % der Unternehmen eine der größten Herausforderungen, insbesondere in verteilten Cloud-Umgebungen. Zentrale Lösungen für die Zugangskontrolle können das Management von Benutzerberechtigungen optimieren und konsistente Sicherheitsrichtlinien in Hybrid- und Multi-Cloud-Umgebungen durchsetzen. Eine einheitliche Identitätsplattform gewährleistet zudem die nahtlose Durchsetzung von Richtlinien und minimiert zugleich das Risiko unbefugter Zugriffe.

8

**SKALIERBARKEIT MIT CLOUDBASIERTEN SECURITY-TOOLS**

Hybride Cloud-Architekturen sind das primäre Bereitstellungsmodell von 54 % der Befragten. Solche Umgebungen lassen sich nur mit skalierbaren, cloudbasierten Security-Tools wirksam schützen. Unternehmen erhalten damit einen einheitlichen Schutz für On-Premises-Systeme und Public Clouds und können so den Cloud-Einsatz jederzeit problemlos erweitern, ohne die operative Effizienz zu beeinträchtigen.

## Fazit

Dieser Bericht unterstreicht die Bedeutung strategischer Investitionen in einheitliche Tools, Schulungen und Prozesse, die auf die dynamischen Anforderungen der Hybrid- und Multi-Cloud-Sicherheit zugeschnitten sind. Indem Unternehmen aktuelle Herausforderungen wie Fehlkonfigurationen, Qualifikationslücken und mangelnde Transparenz angehen, können sie ein resilientes Sicherheitsprofil aufbauen.

Unternehmen mit komplexen Cloud-Umgebungen, die die hier genannten Best Practices umsetzen, schaffen damit ideale Voraussetzungen für mehr Wachstum und einen wirksamen Schutz wichtiger Ressourcen. Und noch mehr: Sie gewinnen die nötige Agilität und Sicherheit bei der Compliance, die sie für eine erfolgreiche Digitalisierung brauchen.

# Wichtige Begriffe zur Cloud-Sicherheit

Dieses Glossar bietet einen schnellen Überblick über die wesentlichen Cloud-Security-Technologien in diesem Bericht. Wir erklären kurz ihre Funktionen, welche Sicherheits Herausforderungen sich damit lösen lassen und warum diese Technologien für den Schutz heutiger komplexer Cloud-Umgebungen wichtig sind.

**Application Security Posture Management (ASPM):** bietet Transparenz über Anwendungsschwachstellen und Konfigurationsprobleme im gesamten Lebenszyklus der Softwareentwicklung. ASPM fördert sichere Programmierpraktiken und integriert die Sicherheit in DevSecOps-Workflows. Unverzichtbar für die Anwendungssicherheit während der Entwicklung, Bereitstellung und Laufzeit.

**Cloud Detection und Response (CDR):** spezielle Bedrohungserkennung und -abwehr für Cloud-Umgebungen, die mit Echtzeit-Einblicken in Cloud-Aktivitäten die Erkennung von Anomalien und Reaktion auf Sicherheitsvorfälle beschleunigt. Wichtig für die Aufrechterhaltung einer starken Verteidigung gegen hochkomplexe Bedrohungen in verteilten Cloud-Umgebungen.

**Cloud Infrastructure Entitlement Management (CIEM):** dient hauptsächlich zur Verwaltung von Berechtigungen und Zugangskontrollen in Cloud-Umgebungen. Identifiziert zu weit gefasste Berechtigungen, setzt das Least-Privilege-Prinzip durch (nur absolut nötige Berechtigungen) und verringert das Risiko, dass Zugriffsrechte missbraucht werden. Essentiell für die Aufrechterhaltung sicherer, regelkonformer Zugriffsrichtlinien in Multi-Cloud-Architekturen.

**Cloud Native Application Protection Platform (CNAPP):** integriert mehrere Sicherheitsfunktionen für cloudnative Anwendungen während ihres gesamten Lebenszyklus. Kombiniert den Schutz zur Laufzeit mit der Workload-Security und einem Konfigurationsmanagement, um Container, serverlose Funktionen und andere cloudnative Workloads zu schützen. Wichtig für Unternehmen mit modernen Entwicklungspraktiken wie DevOps und Microservices.

**Cloud Security Posture Management (CSPM):** erkennt automatisch Fehlkonfigurationen in Cloud-Umgebungen. Überwacht die Cloud-Infrastruktur ständig auf Sicherheitsrisiken (wie freigegebene Speicher-Buckets oder zu weit reichende Zugriffsrechte) und sorgt so für die Einhaltung gesetzlicher Rahmenbedingungen. Unverzichtbar für eine zuverlässige Transparenz und die Behebung von Schwachstellen in Multi-Cloud- und Hybrid-Umgebungen.

**Cloud Workload Protection Platform (CWPP):** schützt Workloads in Cloud-Umgebungen wie virtuellen Maschinen, Containern und serverlosen Architekturen. Zeigt Schwachstellen auf, gewährleistet einheitliche Sicherheitsrichtlinien und schützt Workloads vor hochkomplexen Bedrohungen. Wichtig für Unternehmen, die vielfältige und dynamische Cloud-Workloads verwalten.

**Data Security Posture Management (DSPM):** identifiziert, klassifiziert und schützt vertrauliche Informationen in Cloud-Umgebungen. Sorgt für eine angemessene Datensicherheit und die Handhabung von Daten nach Datenschutzbestimmungen wie der DSGVO. Entscheidend für einen zuverlässigen Schutz vertraulicher Informationen in komplexen Cloud-Ökosystemen.

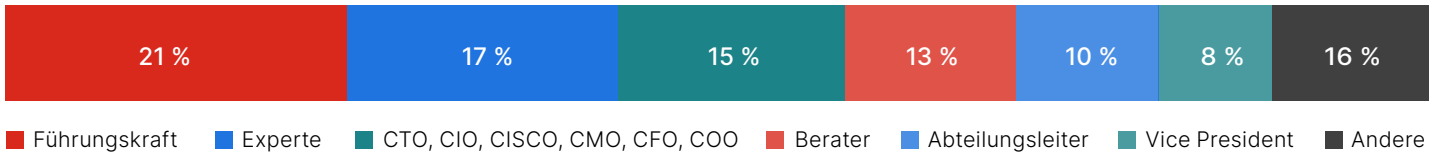
# Erhebungsmethode und demografische Daten

Der Bericht zum Stand der Cloud-Sicherheit 2025 basiert auf einer umfassenden Befragung Ende 2024 von 873 IT- und Cybersecurity-Experten aus verschiedenen Ländern und Branchen, darunter Technologie, Finanzdienstleistungen, Gesundheitswesen und öffentlicher Sektor. Die Befragten stammten aus Unternehmen und Einrichtungen jeder Größe und waren in unterschiedlichsten Positionen tätig, deren Spektrum vom Experten bis hin zum leitenden Management reichte.

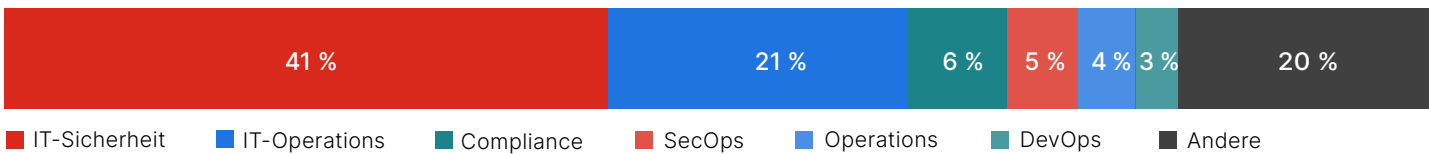
Die online durchgeführte Umfrage untersuchte die wichtigsten Trends, Herausforderungen und Prioritäten bei der Cloud-Sicherheit. Die Ergebnisse geben einen umfassenden Überblick darüber, wie Unternehmen und öffentliche Einrichtungen die Komplexität von Cloud-Umgebungen angehen und mit welchen Sicherheitstechnologien sie neuen Bedrohungen begegnen.

Bei Fragen mit mehreren möglichen Antworten kann der Gesamtprozentsatz mehr als 100 % betragen.

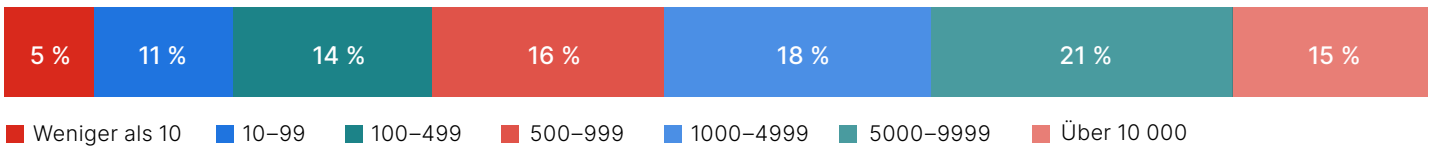
## POSITION



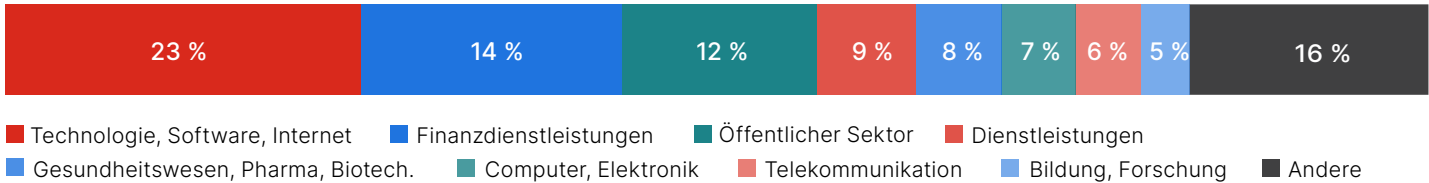
## ABTEILUNG



## UNTERNEHMENSGRÖSSE (NACH MITARBEITERN)



## BRANCHE



### Weiterverwendung von Inhalten

Wir ermutigen zur weiteren Verwendung der in diesem Bericht veröffentlichten Daten, Diagramme und Texte im Rahmen der [Creative Commons Attribution 4.0 International License](#). Sie dürfen dieses Dokument frei weitergeben und kommerziell nutzen, solange Sie den Bericht gemäß den Lizenzbedingungen als Quelle angeben. Beispiel: „Bericht zum Stand der Cloud-Sicherheit 2025 von Cybersecurity Insiders und Fortinet.“





Fortinet (NASDAQ: FTNT) schafft durch seine Mission, Menschen, Geräte, Anwendungen und Daten jederzeit zu schützen, eine digitale Welt, der wir immer vertrauen können. Aus diesem Grund entscheiden sich viele der weltweit größten Unternehmen, Service Provider und Behörden für Fortinet, um ihre digitale Transformation sicher voranzutreiben. Die Fortinet Security Fabric-Plattform bietet einen umfangreichen, integrierten und automatisierten Schutz über die gesamte digitale Angriffsfläche hinweg für kritische Geräte, Daten, Anwendungen und Verbindungen – vom Rechenzentrum über die Cloud bis hin zum Homeoffice sowie in Multi-Cloud- und Edge-Umgebungen. Fortinet ist die Nummer 1 unter den Sicherheitsunternehmen mit über 800 000 Kunden, die beim Schutz ihrer Marke auf Fortinet-Lösungen und -Services vertrauen.

[www.fortinet.com/de](http://www.fortinet.com/de)

# Cybersecurity

---

## I N S I D E R S

Cybersecurity Insiders bringt mehr als 600 000 IT-Sicherheitsexperten und erstklassige Technologieanbieter zusammen, um intelligente Problemlösungen und die Zusammenarbeit zur Bewältigung kritischer, aktueller Cybersecurity-Herausforderungen zu erleichtern.

Unser Ansatz konzentriert sich auf die Erstellung und Kuratierung einzigartiger Inhalte, die Cybersecurity-Experten über die neuesten Trends, Lösungen und Best Practices im Cybersecurity-Bereich informieren. Von umfassenden Studien und neutralen Produktbewertungen bis hin zu praktischen E-Guides, interessanten Webinaren und lehrreichen Artikeln finden Sie bei uns Ressourcen, die evidenzbasierte Antworten auf heutige komplexe Herausforderungen der Cybersecurity bieten.

Wenn Sie interessiert, wie Sie sich mithilfe von Cybersecurity Insiders in einem wettbewerbsintensiven Markt besser abheben sowie die Nachfrage, den Bekanntheitsgrad und die Wahrnehmung Ihres Unternehmens als Vordenker verbessern können, setzen Sie sich noch heute mit uns in Verbindung.

E-Mail: [info@cybersecurity-insiders.com](mailto:info@cybersecurity-insiders.com) Website: [cybersecurity-insiders.com](https://cybersecurity-insiders.com)