

2024

Cloud-Security-Bericht



Einleitung

Immer mehr Unternehmen setzen mit der Entwicklung und Bereitstellung cloudnativer Anwendungen eine Cloud-First-Strategie um. Da sie dabei vornehmlich Hybrid- oder Multi-Cloud-Infrastrukturen nutzen, um eine Vielfalt an Anwendungsfällen und Arbeitsmodellen zu unterstützen, vergrößert sich ihre Angriffsfläche. Da überrascht es nicht, dass der Schutz moderner Cloud-Umgebungen zu einer geschäftskritischen, aber extrem komplexen Aufgabe geworden ist.

Im Cloud-Security-Bericht 2024, der auf einer weltweiten Umfrage unter 927 Cybersecurity-Experten basiert, haben wir wichtige Erkenntnisse zu aktuellen Trends in der Cloud-Sicherheit für Sie zusammengefasst. Unter anderem identifizieren wir die zentralen Herausforderungen beim Schutz komplexer Cloud-Umgebungen und sehen uns an, welche Lösungen und Strategien Cybersecurity-Experten priorisieren, wie sie ihre Ressourcen aufteilen und mit welchen Best Practices sie die Sicherheit von cloudbasierten Workloads stärken.

Hier ein Vorgeschmack auf die Umfrageergebnisse:

- **Multi-Cloud-Umgebungen sind die erste Wahl:** Die meisten Unternehmen (78 %) nutzen Hybrid- und Multi-Cloud-Strategien, um von einem Höchstmaß an Flexibilität, Kontrolle und den spezifischen Vorteilen verschiedener Cloud-Dienste zu profitieren.
- **Hürden bei der Cloud-Nutzung:** Bedenken in puncto Sicherheit und Compliance hemmen in 59 % der befragten Unternehmen die Einführung von Multi-Cloud-Strategien. Technische Herausforderungen (52 %) und knappe Ressourcen (49 %) wurden als zwei der wichtigsten Gründe genannt, warum komplexe Multi-Cloud-Infrastrukturen oft nicht so transparent und richtlinienkonform sind wie gewünscht. Damit unterstreichen die Umfrageteilnehmer, wie wichtig solides Fachwissen bezüglich der Cloud-Sicherheit ist.
- **Fachkräftemangel:** Unternehmen haben mit dem verschärften Mangel an Cybersecurity-Experten zu kämpfen: 93 % der Umfrageteilnehmer sind der Meinung, dass es nicht genügend qualifizierte Fachkräfte für den Schutz komplexer Multi-Cloud-Umgebungen gibt. Das wirkt sich nicht nur auf ihr Sicherheitsniveau, sondern auch auf ihre strategischen Entscheidungen aus und behindert die flächendeckende Einführung von Multi-Cloud-Lösungen.
- **Wunsch nach einer einheitlichen Cloud-Security-Plattform:** 95 % der befragten Cybersecurity-Experten sprechen sich für eine zentrale Plattform aus, um das Security-Management zu vereinfachen und zu automatisieren, den Fachkräftemangel auszugleichen, Richtlinien konsistent durchzusetzen und die Transparenz zu erhöhen, damit sie die Sicherheit stärken und den ineffizienten Prozessen entgegenwirken können, die sich durch die Verwaltung voneinander isolierter Sicherheitssysteme ergeben.

Wir bedanken uns bei [Fortinet](#) für die wertvolle Unterstützung dieses für unsere Branche wichtigen Forschungsprojekts und hoffen, dass dieser Bericht Ihnen als Entscheidungsträgern und Fachkräften im Bereich Cybersecurity als praktischer Leitfaden dabei hilft, den komplexen Herausforderungen der Cloud-Sicherheit effektiv zu begegnen und Ihr Unternehmen erfolgreich vor neuen Cyberbedrohungen zu schützen.

Im Voraus schon einmal vielen Dank für Ihr Interesse!

Holger Schulze

Founder, Cybersecurity Insiders

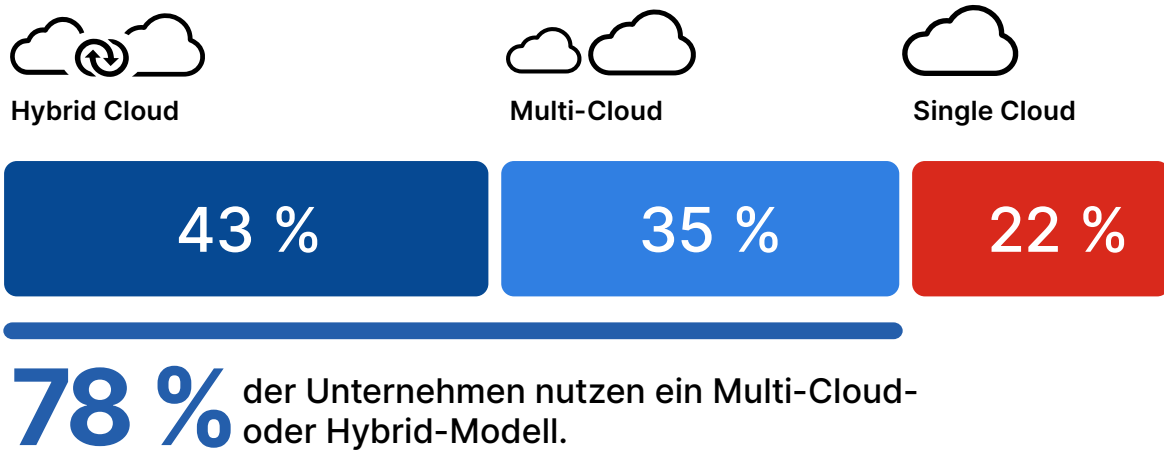
Cybersecurity
INSIDERS

Cloud-Deployment-Strategien

In welchem Umfang Sie von den Vorteilen des Cloud-Computings profitieren und die damit verbundenen Risiken senken können, hängt stark von der Auswahl der richtigen Cloud-Deployment-Strategie ab.

Die meisten Unternehmen (78 %) entscheiden sich für einen Hybrid- oder Multi-Cloud-Ansatz, um mehrere Deployments in einer einzigen Betriebsumgebung zu kombinieren. Von dieser Gruppe nutzen 43 % ein heterogenes Gefüge aus Cloud- und On-Premises-Infrastrukturen. 35 % der Unternehmen verfolgen eine Multi-Cloud-Strategie, um unterschiedliche Anwendungsfälle abzudecken und dabei die Stärken verschiedener Cloud-Service-Anbieter zu nutzen. Nur 22 % beschränken sich auf die Dienste eines einzigen Anbieters, womit sie zwar ihren Verwaltungsaufwand reduzieren, sich aber gleichzeitig von diesem Service Provider abhängig machen.

► Welchen Ansatz nutzt Ihr Unternehmen in erster Linie bei Cloud-Bereitstellungen?



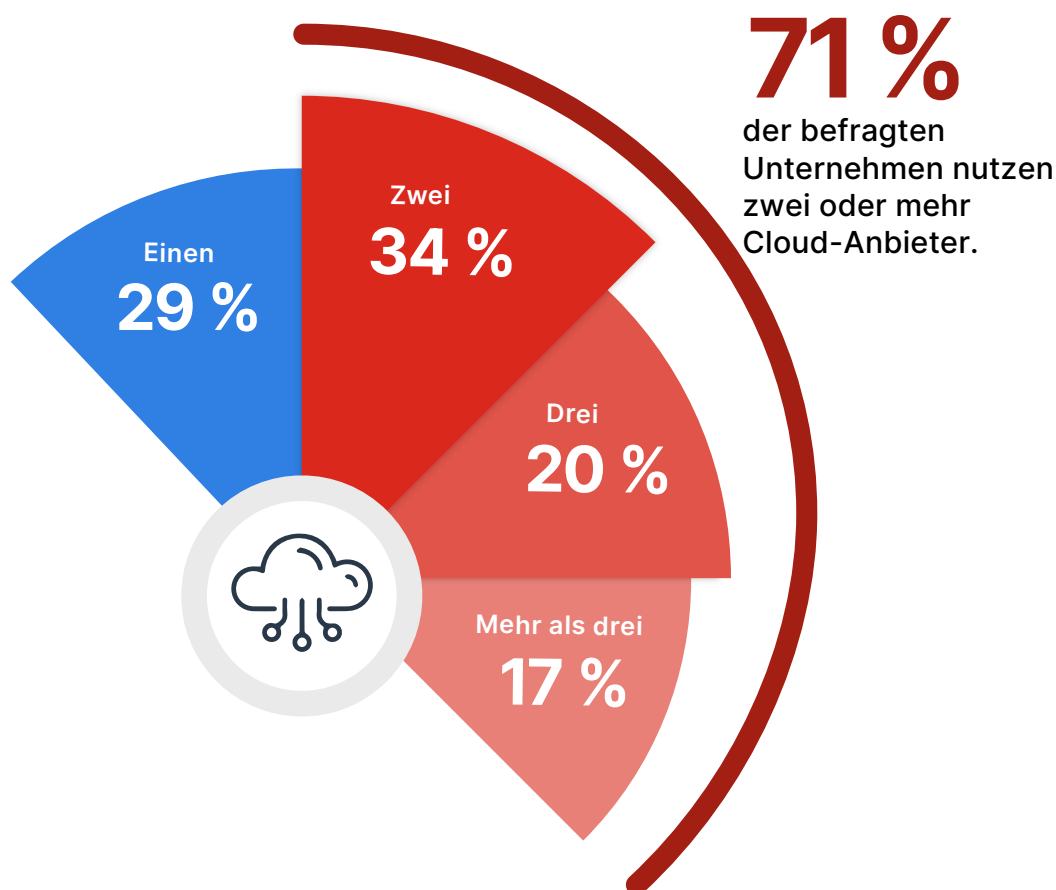
Um die komplexen Anforderungen von Hybrid- und Multi-Cloud-Deployments zu bewältigen, sollten Unternehmen ein integriertes Sicherheitskonzept anstreben, mit dem sich ihr gesamtes digitales Ökosystem nahtlos schützen lässt. Nur so erlangen sie die für die Abwehr dynamischer Cyberbedrohungen erforderliche Agilität, Skalierbarkeit und Sicherheit.

Multi-Cloud-Nutzung

In Bezug auf die betriebliche Flexibilität, das Risiko-Management und die Komplexität des Sicherheitsprogramms macht es einen großen Unterschied, wie viele Cloud-Anbieter ein Unternehmen nutzt. Der Großteil der Unternehmen (71 %) hat sich für zwei oder mehr Anbieter entschieden, um von einem Höchstmaß an Flexibilität, Kontrolle und den spezifischen Vorteilen verschiedener Service-Anbieter zu profitieren. Dies ist ein Anstieg von zwei Prozent gegenüber dem Vorjahr und diese wachsende Beliebtheit von Multi-Cloud-Strategien lässt sich durch die Nachfrage nach spezialisierten Cloud-Diensten, regionale Verfügbarkeit und Redundanz erklären.

Interessanterweise beschränken sich nur 29 % der befragten Unternehmen auf die Dienste eines einzigen Cloud-Anbieters, für den sie sich vermutlich aufgrund einer strategischen Partnerschaft oder im Bestreben nach weniger Komplexität entscheiden.

► Wie viele Cloud-Anbieter nutzt Ihr Unternehmen derzeit?



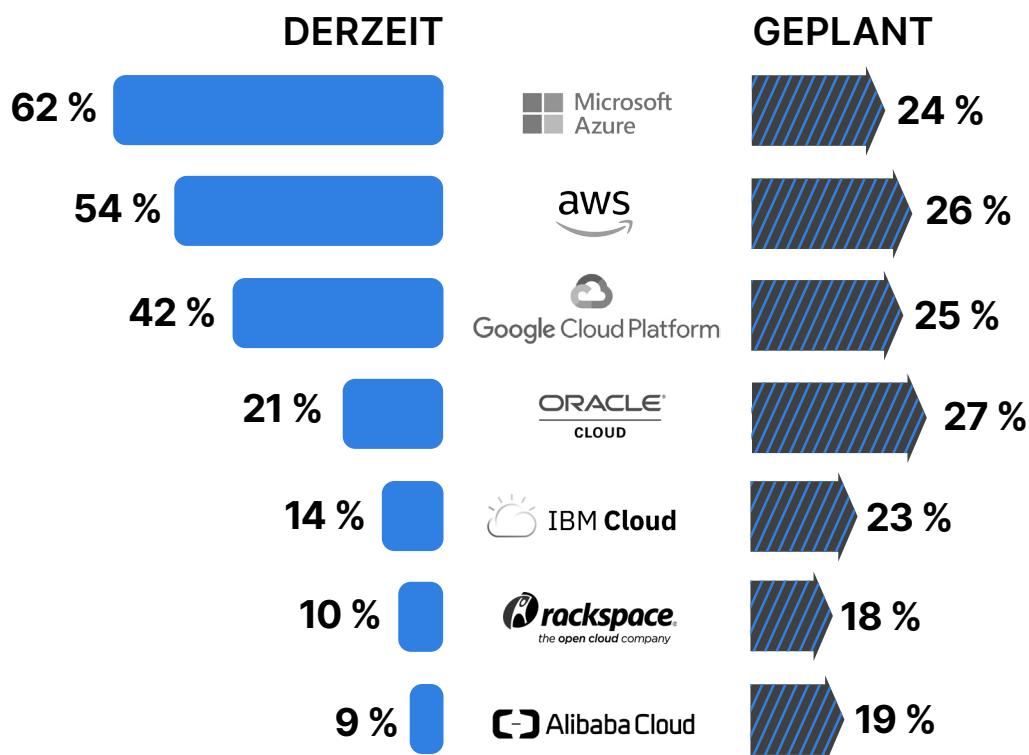
Beim Schutz mehrerer Cloud-Umgebungen sollten Unternehmen einen cloudübergreifenden Ansatz verfolgen, mit dem sie konsistente Sicherheitsrichtlinien durchsetzen können und einen umfassenden Überblick über ihr digitales Ökosystem erhalten. So reduzieren sie Komplexität und stärken die Abwehr immer vielschichtiger werdender Angriffe.

Bevorzugte Cloud-Anbieter

Als Nächstes haben wir die Cybersecurity-Experten nach ihren Cloud-Anbietern gefragt, um die wechselhafte Marktdynamik im Cloud-Segment besser beurteilen zu können. 62 % der Umfrageteilnehmer nutzen die Services des Marktführers Microsoft Azure, Amazon Web Services (AWS) liegt mit 54 % auf Platz zwei. Unternehmen zeigen also eine klare Vorliebe für diese beiden etablierten Cloud-Giganten.

Die Umfrageergebnisse lassen aber auch ein deutliches Interesse an anderen Anbietern erkennen: 27 % der Befragten geben an, die Nutzung von Oracle Cloud zu planen, und 25 % visieren in Zukunft den Einsatz der Google Cloud Platform an. Das deutet darauf hin, dass die Cloud-Landschaft im Begriff ist, diverser zu werden.

► Welche(n) IaaS-Anbieter nutzen Sie derzeit oder planen Sie, in Zukunft zu nutzen? (Bitte alle gültigen Antworten auswählen.)



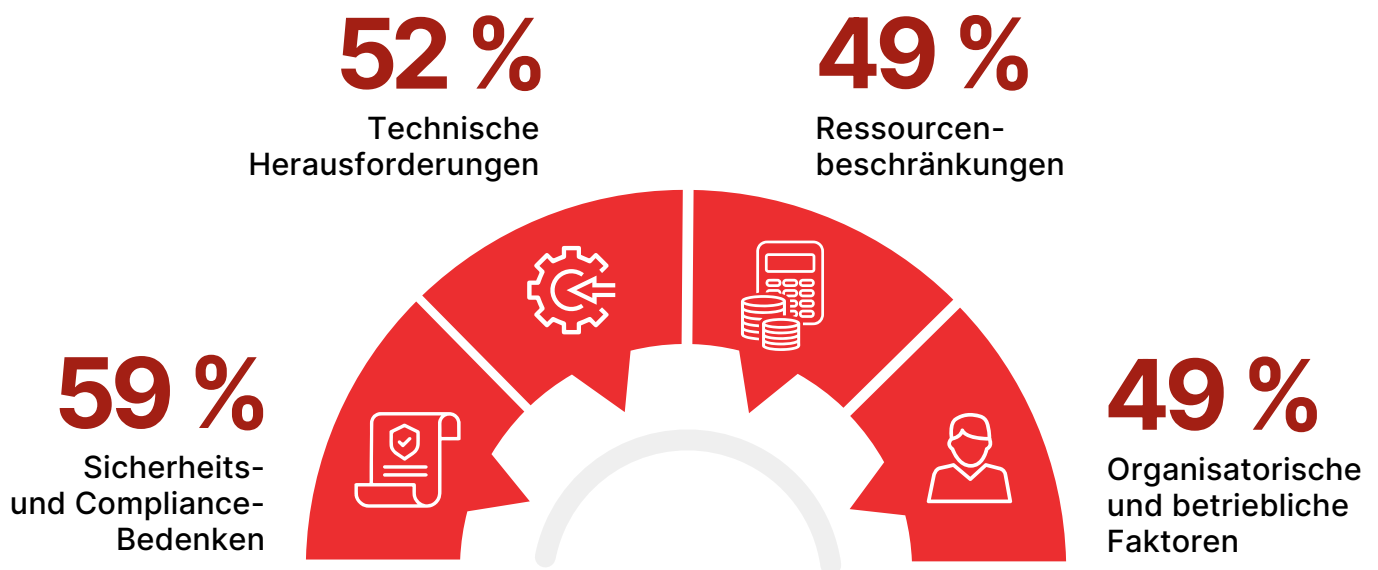
Hürden bei der Cloud-Nutzung

Damit Unternehmen die Umstellung auf cloudbasierte Lösungen möglichst schnell und mühelos bewältigen, müssen sie wissen, welche Hindernisse auf dem Weg in die Cloud zu erwarten sind.

An erster Stelle nennen 59 % der befragten Unternehmen Sicherheits- und Compliance-Bedenken. Dies verdeutlicht, dass diese beiden Bereiche bei der Einführung einer Cloud-Strategie unbedingt berücksichtigt werden müssen. Mit 52 % liegen die technischen Herausforderungen auf Platz drei, was zeigt, dass Einrichtung einer Cloud-Umgebung nicht trivial ist.

49 % der Befragten geben Ressourcenbeschränkungen wie Fachkräftemangel und knappe Budgets als Hürde für die Umstellung auf die Cloud an. Das unterstreicht, wie wichtig es ist, in personelle und finanzielle Ressourcen zu investieren, um Cloud-Initiativen voranzutreiben. Die Nennung von organisatorischen und betrieblichen Faktoren (49 %) hebt hervor, dass Cloud-Computing nicht einfach nur eine neue Technologie ist, sondern ein ganz eigenes Betriebsmodell mit innovativen Arbeitsmethoden. Die zu erwartende Änderungsresistenz wird sich nur mit Unterstützung durch die Führungsriege überwinden lassen.

► Was sind die größten Hürden in Bezug auf die Cloud-Nutzung in Ihrem Unternehmen? (Bitte alle gültigen Antworten auswählen.)



Weitere Nennungen:

Bedenken im Hinblick auf Cloud-Services 28 % | Anbieterspezifische und rechtliche Fragen 27 %

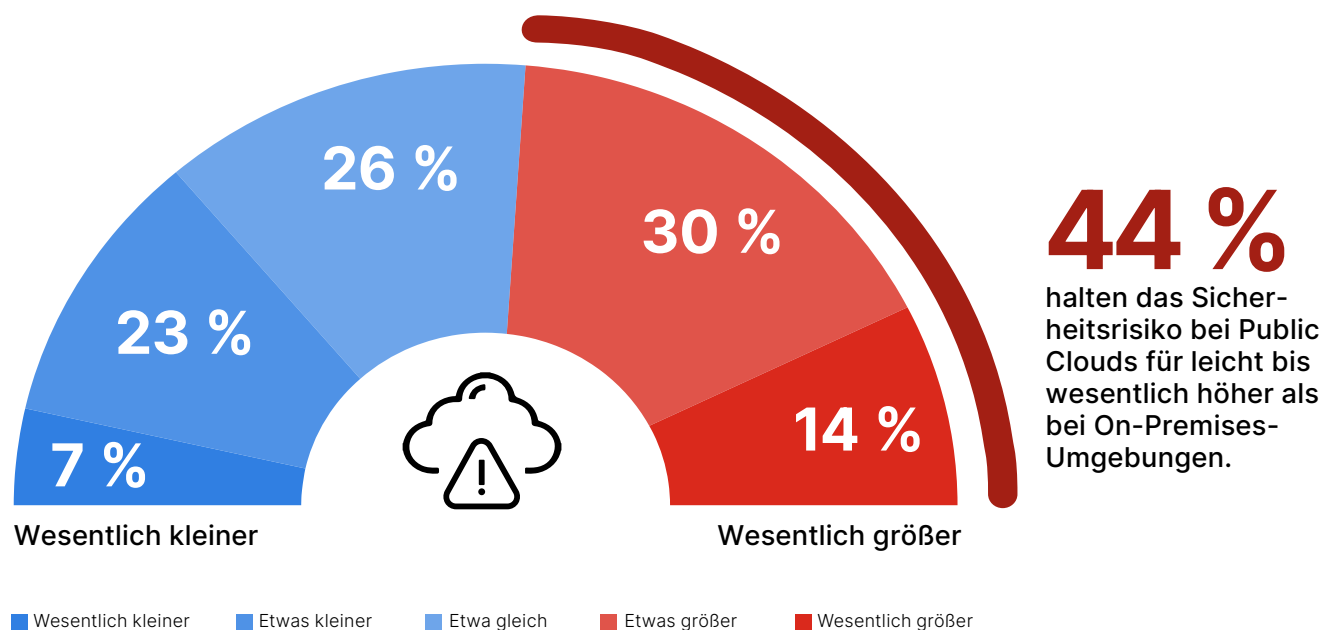
Einschätzung von Cloud-Sicherheitsrisiken

Wie hoch das Risiko von Sicherheitsverletzungen in Public-Cloud-Umgebungen im Vergleich zu traditionellen On-Premises-Infrastrukturen eingeschätzt wird, verrät viel über die potenziellen Gefahren und inhärenten Sicherheitsprobleme des Cloud Computing.

Insgesamt 44 % der Umfrageteilnehmer halten Public-Cloud-Umgebungen für weniger sicher. Im Einzelnen gehen 30 % von einem leicht höheren und 14 % von einem wesentlich höheren Risiko aus.

Gleichzeitig scheinen 30 % der befragten Experten Vertrauen in die Sicherheitsmaßnahmen und Lösungen von Cloud-Anbietern zu haben und schätzen das Sicherheitsrisiko einer Public-Cloud-Umgebung als niedriger ein. Nennenswerte 26 % sind der Meinung, dass sich das Risiko durch die Umstellung nicht ändert. Sicherheitsherausforderungen sind also nach Ansicht dieser Gruppe ein umgebungsunabhängiges Problem.

► Halten Sie das Risiko eines Datenlecks in einer Public Cloud für größer oder kleiner als in einer konventionellen IT-Umgebung, die sich auf Ihrem Unternehmensgelände befindet?



Public Clouds bieten Unternehmen die Möglichkeit, auf einen proaktiven, automatisierten Sicherheitsansatz umzustellen. Die nativen Sicherheitsmechanismen cloudbasierter Umgebungen machen es möglich, Risiken effektiv zu mindern und zugleich die Vorteile dieser Umgebungen im Hinblick auf Skalierbarkeit, Flexibilität und Innovationskraft zu nutzen.

Bedenken hinsichtlich der Cloud-Sicherheit

Wie hoch die Bedenken in Bezug auf die Sicherheit von Public-Cloud-Umgebungen sind, ist ein klarer Indikator dafür, wie es um das Vertrauen in Cloud-Sicherheit unter den Cybersecurity-Experten bestellt ist und inwieweit sie bereit sind, potenziellen Gefahren und Bedrohungen zu begegnen.

Trotz der steigenden Cloud-Nutzung bleiben Sicherheitsbedenken unvermindert bestehen. Nahezu alle untersuchten Unternehmen (96 %) sind sehr über das Sicherheitsniveau von Public-Cloud-Umgebungen besorgt (37 % davon extrem und 41 % sehr besorgt). Dieses Maß an Besorgnis besteht seit drei Jahren unverändert und ist einer der wichtigsten Gründe dafür, dass die Nutzung von Cloud-Infrastrukturen nicht schneller steigt. Die vermeintlichen Risiken und Schwierigkeiten beim Schutz von Cloud-Umgebungen halten offenbar noch immer viele Unternehmen von deren Nutzung ab. Nur ein kleiner Teil (22 %) der Umfrageteilnehmer gab an, sich in dieser Hinsicht nur begrenzt oder gar keine Sorgen zu machen. Es zeigt sich also, wie wichtig den meisten Unternehmen zuverlässige Sicherheitsvorkehrungen bei Public-Cloud-Bereitstellungen sind.

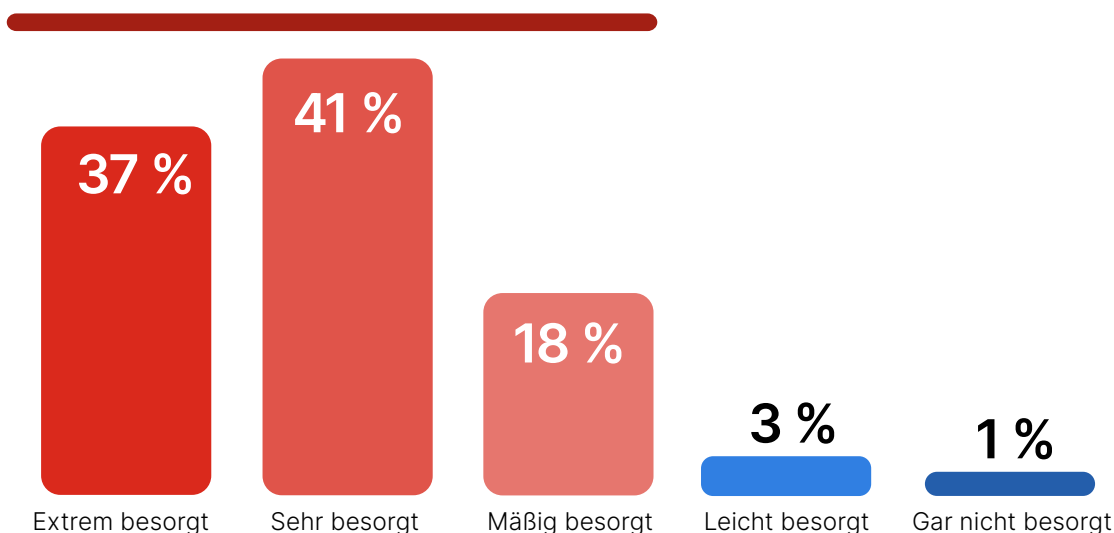
Diese Wahrnehmung hat sich gegenüber dem Vorjahr nicht verändert, als insgesamt 44 % der Umfrageteilnehmer das Risiko von Sicherheitsverletzungen in Public Clouds höher als in einer konventionellen On-Premises-Umgebung einschätzten. Das bestätigt einmal mehr, dass die zahlreichen Vorteile des Cloud Computing zwar allgemein bekannt sind, aber nicht ausreichen, um die Bedenken hinsichtlich der Sicherheit aufzuwiegen.

► Wie besorgt sind Sie über die Sicherheit öffentlicher Clouds?



96 %

der Unternehmen sind mäßig bis extrem besorgt über das Sicherheitsniveau von Cloud-Umgebungen.



Daher sollten Unternehmen das Security-by-Design-Prinzip umsetzen und in cloudspezifische kontinuierliche Überwachungs-, Threat-Intelligence- und Incident-Response-Funktionen investieren. Branchenführende Sicherheitslösungen und die enge Zusammenarbeit mit Cloud-Anbietern können helfen, die Angst vor den vermeintlichen Risiken und Gefahren von Public Clouds zu mindern und eine sichere, zuverlässige Cloud-Infrastruktur aufzubauen.

Herausforderungen bei Cloud-SecOps

Das alltägliche Management des cloudspezifischen Sicherheitsbetriebs stellt Unternehmen vor vielfältige Herausforderungen und kann nur gelingen, wenn das richtige Gleichgewicht zwischen Technologie, Abläufen und Rücksicht auf menschliche Bedürfnisse gefunden wird. Datensicherheit und Datenschutz sind die Hauptsorge bei den Umfrageteilnehmern und 58 % betonen dabei den Schutz sensibler Daten und die Prävention von Datenlecks in der Cloud. Dies zeigt, wie wichtig eine zuverlässige Daten-Governance und solide Verschlüsselungsmaßnahmen sind. An zweiter Stelle steht das Konfigurationsmanagement mit 55 % als Spiegel der Komplexität und potenziellen Risiken von Cloud-Konfigurationen – schließlich kann eine einzelne Fehlkonfiguration erhebliche Sicherheitsrisiken zur Folge haben.

Die kombinierte Herausforderung von Zugriffskontrolle und Identitätsverwaltung wird von 54 % der Befragten als Problem betrachtet. Dies macht deutlich, wie wichtig die strikte Kontrolle des Benutzerzugriffs und der Berechtigungen zur Verhinderung des unbefugten Zugriffs sind. Die Nennung von Bedrohungserkennung und -abwehr (50 %) sowie der Endpunktsicherheit (45 %) deuten auf die andauernden Schwierigkeiten beim Aufdecken und Blockieren von Bedrohungen in Echtzeit sowie beim Schutz der unzähligen Geräte mit Zugang zu Cloud-Diensten hin. Die Angabe von Richtlinien- und Compliance-Management (45%) sowie der Verwaltung der Sicherheit (45 %) unterstreicht, wie schwer es Unternehmen fällt, konsistente Sicherheitsrichtlinien umgebungsübergreifend durchzusetzen und die Security-Features von Cloud-Umgebungen in Einklang mit denen der On-Premises-Lösungen zu bringen.

► Worin bestehen Ihre größten Herausforderungen bei der tagtäglichen Verwaltung des Security-Betriebs in der Cloud? (Bitte alle gültigen Antworten auswählen.)



Unternehmen sollten daher eine einheitliche Sicherheitsstrategie mit Automatisierung, erweiterten Analysen und einer integrierten Plattform priorisieren, um den Schutz von Daten, die Durchsetzung von Richtlinien, das Zugriffsmanagement sowie die Erkennung und Abwehr von Bedrohungen zu vereinfachen. Unternehmen, die ihre Security-Teams beim Erwerb und der Vertiefung von Kenntnissen und Fähigkeiten rund um die cloudnative Sicherheit unterstützen und das Sicherheitsbewusstsein aller Mitarbeitenden wachhalten, haben bessere Voraussetzungen für das effektive Management der Cloud-SecOps.

Weitere Nennungen:

Schatten-IT und Nutzung nicht autorisierter Apps 36 % | Cloud-Integration und Automatisierung 35 % | Betriebliche Agilität und Komplexität 32 % | Zuweisung von Ressourcen 30 % | DevSecOps-Abläufe 28 %

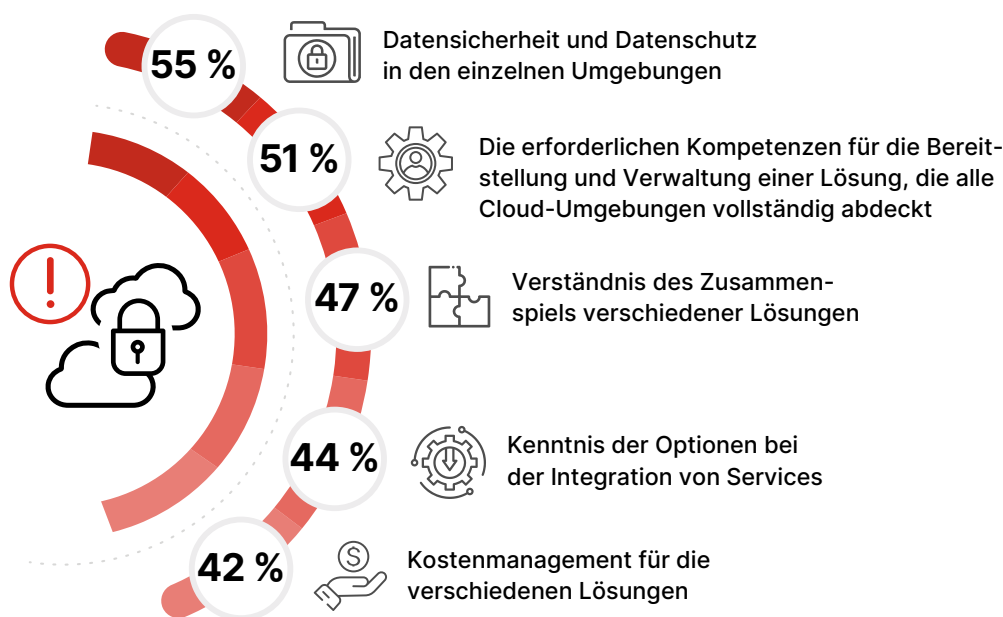
Herausforderungen rund um Cloud Security

Durch Multi-Cloud-Umgebungen nehmen die Komplexität und die Herausforderungen rund um die Sicherung von Cloud-Workloads erheblich zu. In jeder Umgebung Datensicherheit und Datenschutz zu gewährleisten, wurde von 55 % der Umfrageteilnehmer als schwierige Aufgabe identifiziert und stellt damit die meistgenannte Herausforderung in Multi-Cloud-Architekturen dar. Dies steht im Einklang mit den zuvor erwähnten Bedenken in puncto Datensicherheit und Datenschutz und unterstreicht die zunehmende Komplexität, die sich aus der Verteilung von Daten auf mehrere Cloud-Umgebungen ergibt.

Das nötige Fachwissen für die Bereitstellung und Verwaltung von Lösungen in sämtlichen Cloud-Umgebungen empfinden 51 % der Befragten als eine große Herausforderung. Dies spiegelt den bereits erwähnten Bedarf an Expertise im Bereich der cloudnativen Sicherheit wieder – eine wichtige Voraussetzung für den erfolgreichen Umgang mit einer vielschichtigen Cloud-Security-Landschaft. Das Verständnis sowohl des Zusammenspiels verschiedener Lösungen als auch der Optionen für die Integration von Services wurde jeweils von 47 % bzw. 44 % der Umfrageteilnehmer als kritische Herausforderung eingestuft.

Diese Bedenken verleihen dem Empfinden Nachdruck, dass die nahtlose Integration und Interoperabilität der verschiedenen Cloud-Umgebungen für einen effizienten Betrieb und belastbare Sicherheit unerlässlich, aber bislang keineswegs selbstverständlich sind. Die Tatsache, dass 42 % der Teilnehmer das Kosten-Management für verschiedene Lösungen als Herausforderung empfinden, lässt den Balanceakt zwischen betrieblichen und finanziellen Interessen erkennbar werden, den eine Multi-Cloud-Strategie erfordert.

► Was sind Ihre größten Herausforderungen bei der Sicherung von Multi-Cloud-Umgebungen? (Bitte alle gültigen Antworten auswählen.)



Unternehmen können diese Herausforderungen mit integrierten Security-Lösungen meistern, die Transparenz und Kontrolle in Multi-Cloud-Umgebungen bieten und mit denen sich Datensicherheits- und Datenschutzstandards aufrechterhalten lassen. Durch Partnerschaften mit Anbietern, die umfassende Sicherheitsfunktionen für Multi-Cloud-Architekturen bieten, und durch die Weiterbildung der eigenen Mitarbeitenden können Unternehmen die Komplexität der Multi-Cloud-Security bewältigen. Darüber hinaus lässt sich mit einem solchen Ansatz das Potential von Multi-Cloud-Umgebungen effektiv nutzen, um ein höheres Maß an Agilität, Skalierbarkeit und Innovationskraft zu erzielen.

Weitere Nennungen:

Reibungsloser Zugang für befugte Nutzer im Rahmen ihrer Zugriffsrechte 38 % | Fehlende Transparenz und Kontrolle 37 % | Auswahl der richtigen Services 36 % | Mit dem Tempo der Änderungen Schritt halten 33 %

Mangel an Cybersecurity-Fachkräften

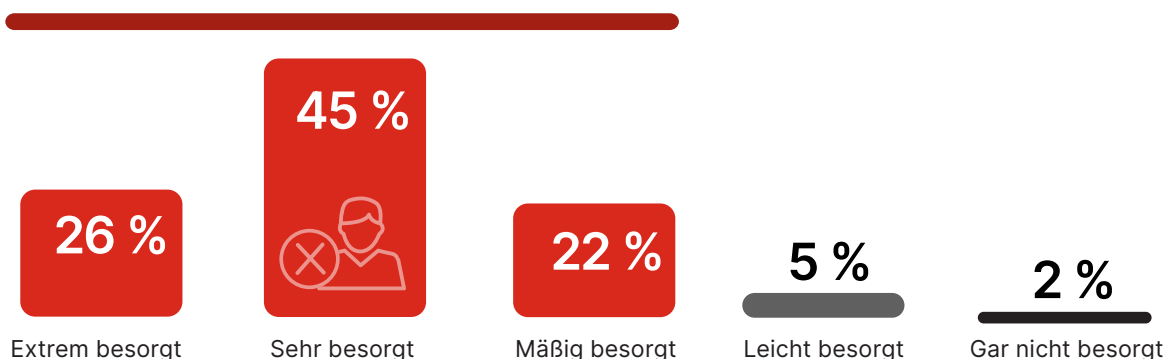
Die oben genannten Herausforderungen bei der Sicherung von Multi-Cloud-Umgebungen spiegeln sich auch in der Sorge über den anhaltenden Mangel an entsprechend qualifizierten Fachkräften in der Branche als Ganzes wider.

Eine überwältigende Mehrheit (93 %) der Befragten äußert sich besorgt über den branchenweiten Mangel an qualifizierten Cybersecurity-Fachkräften. Diese Sorge ergibt sich aus der Diskrepanz zwischen der wachsenden Nachfrage nach Experten auf diesem Gebiet und den verfügbaren Arbeitskräften. Durch dieses Missverhältnis verschärfen sich die sicherheits- und betriebstechnischen Probleme in einer zunehmend komplexen Cyberlandschaft.

► Wie besorgt sind Sie über den branchenweiten Fachkräftemangel im Cybersecurity-Bereich?

93 %

der Unternehmen sind mäßig bis extrem besorgt über den branchenweiten Mangel von qualifizierten Cybersecurity-Fachkräften.



74 % der Umfrageteilnehmer bestätigen, dass ihr Unternehmen derzeit mehr Cybersecurity-Experten bräuchte. Die Teilnehmerangaben zu dieser Frage lassen erkennen, in welchem Ausmaß diese Unterversorgung den tagtäglichen Security-Betrieb und die strategischen Initiativen beeinträchtigt.

► Herrscht in Ihrem Unternehmen ein Mangel an Cybersecurity-Fachkräften?



Um den Auswirkungen des andauernden Fachkräftemangels entgegenzuwirken, bietet sich ein mehrgleisiger Ansatz an: Zum einen begünstigen Partnerschaften mit akademischen Einrichtungen die Talentbeschaffung, zum anderen fördern eigene Schulungs- und Weiterbildungsprogramme die unternehmensinternen Kompetenzen. So können Unternehmen den dynamischen Anforderungen der Cloud Security besser gerecht werden. Ferner reduziert die Umstellung von isolierten Punktlösungen auf einheitliche, KI-gestützte Sicherheitslösungen die betriebliche Komplexität, minimiert das Kompetenzdefizit, verbessert die Bedrohungserkennung und -abwehr und stärkt das Sicherheitsniveau im Gesamten.

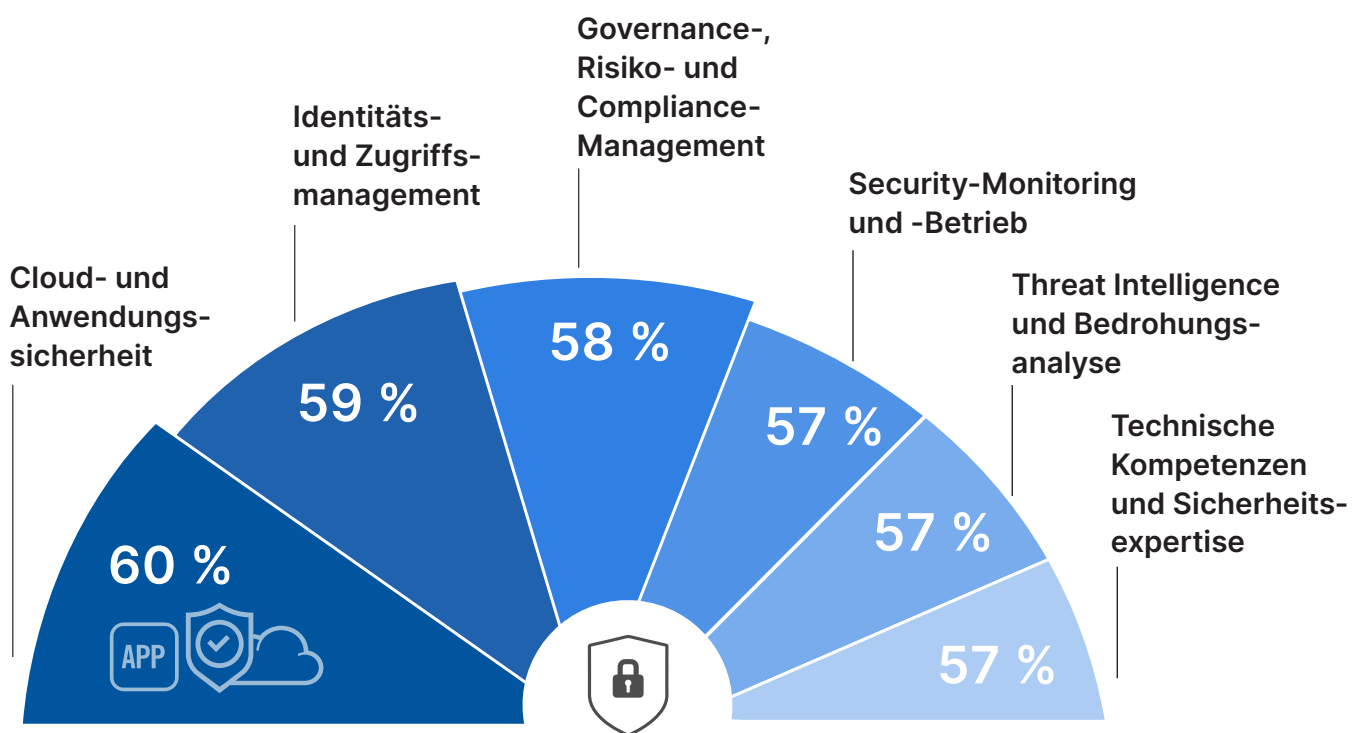
Wichtige Cybersecurity-Kompetenzen

Vor dem Hintergrund des ausgeprägten Fachkräftemangels haben wir die Umfrageteilnehmer gefragt, welche konkreten Cybersecurity-Kompetenzen ihrer Meinung nach zur Bewältigung aktueller Sicherheitsherausforderungen am wichtigsten sind.

Mit 60 % liegt die Expertise im Bereich Cloud- und Anwendungssicherheit an erster Stelle – aufgrund der beschleunigten Umstellung auf Cloud-Dienste und der Notwendigkeit für zuverlässige Sicherheitspraktiken bei der Entwicklung und bei der Bereitstellung von Anwendungen. Auf Platz zwei liegt das Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM), das für 59 % der Unternehmen angesichts der zunehmend komplexen Sicherung des Benutzerzugriffs in verteilten IT-Umgebungen unerlässlich ist.

Governance-, Risiko- und Compliance-Management (GRC) wird von 58 % der Umfrageteilnehmer als wichtige Kompetenz eingeschätzt, was sich auf die heutige zentrale Rolle von gesetzlichen Auflagen und Risiko-Management-Frameworks zurückführen lässt. Jeweils 57 % der Befragten stufen Kenntnisse im Bereich Security-Monitoring und -Betrieb, Threat-Intelligence-Expertise und erweiterte technische Sicherheitskompetenzen als wichtig ein. Das zeigt, dass der proaktiven Bedrohungserkennung, der Kenntnis der Angreifer und dem Einsatz innovativer Technologien ein gleich hoher Stellenwert beim Erreichen eines hohen Sicherheitsniveaus zukommt.

► Welche Security-Kompetenzen werden in Ihrem Unternehmen am dringendsten benötigt? (Bitte alle gültigen Antworten auswählen.)



Weitere Nennungen:

Incident Response und Forensik 55 % | Kommunikation und Strategie 39 % | Schulung und Sensibilisierung 38 %

Trends beim Cloud-Security-Budget

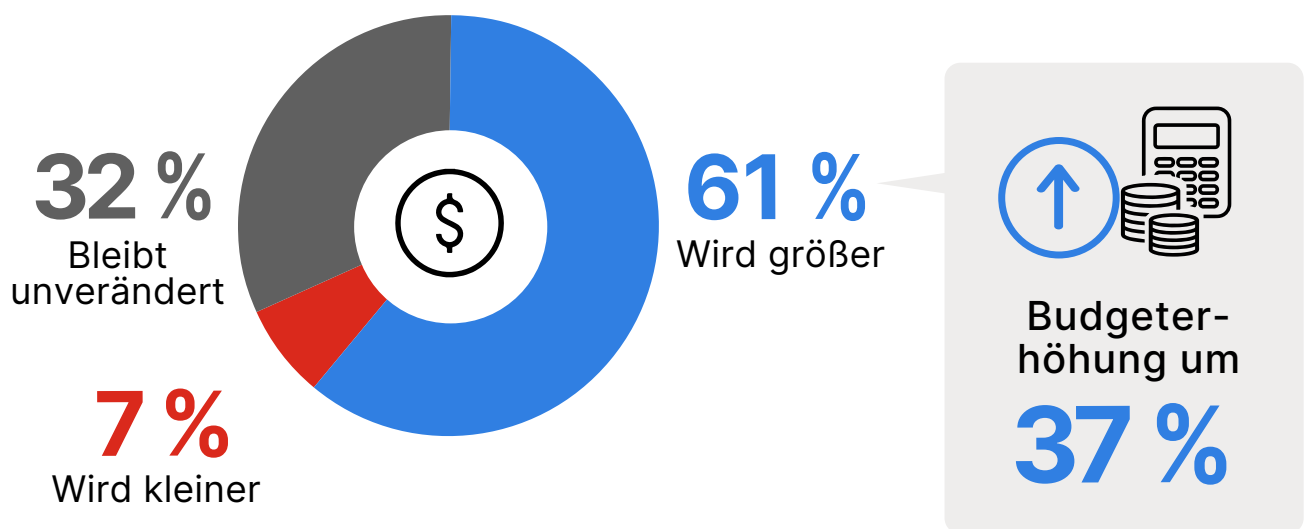
In welchem Maß Ressourcen dem Cloud-Security-Bereich zugewiesen werden, lässt Rückschlüsse auf die Prioritäten des Unternehmens zu und zeigt, wie wichtig der Unternehmensleitung die Sicherung der Cloud-Infrastruktur vor dem Hintergrund technologischer Entwicklungen und der dynamischen Bedrohungslandschaft ist.

61 % der Umfrageteilnehmer gehen davon aus, dass das Cloud-Security-Budget in den nächsten 12 Monaten erhöht wird, und zwar um bis zu 37 %. Dies signalisiert ein Zugeständnis an die steigende Tendenz bei den Herausforderungen in der Cybersecurity und die Notwendigkeit besserer Sicherheitsmaßnahmen in Cloud-Umgebungen.

Die Bereitschaft, bis zu 37 % mehr in die Cloud-Sicherheit zu investieren, zeigt, dass Unternehmen die Bedeutung zuverlässiger Abwehrmechanismen für den Schutz sensibler Daten und die Einhaltung regulatorischer Vorgaben anerkennen.

Ein Drittel der Befragten (32 %) vermutet, dass ihr Cloud-Security-Budget unverändert bleibt, und nur 7 % erwarten eine Budgetkürzung.

► Wie wird sich Ihr Cloud-Security-Budget in den nächsten 12 Monaten verändern?

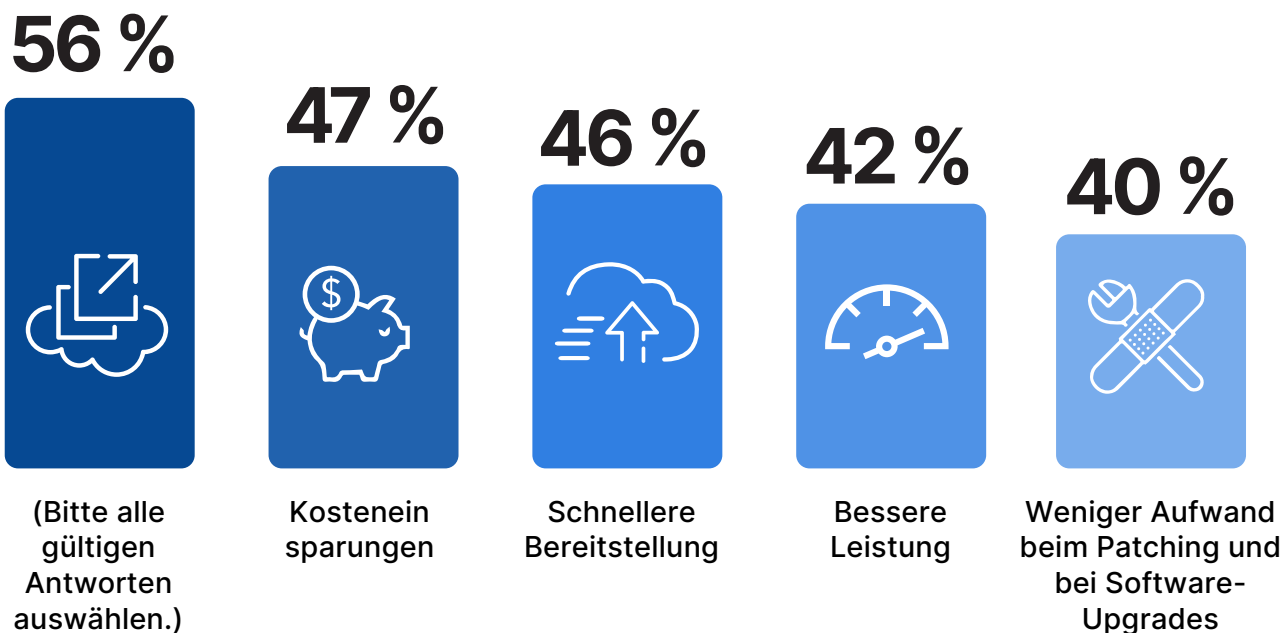


In Anbetracht der in der Mehrzahl der Unternehmen zu erwartenden Budgeterhöhungen sind Entscheidungsträger im Bereich Cybersecurity gut beraten, den Bereichen mit dem größten Risiko- und Auswirkungspotenzial zusätzliche Ressourcen zuzuweisen. Dazu gehören die erweiterte Bedrohungserkennung, das Identitäts- und Zugriffsmanagement sowie die Sicherheitsautomatisierung. Mit diesem Ansatz bereiten sie ihre Unternehmen besser auf komplexe Cyberbedrohungen vor und stärken ihr allgemeines Sicherheitsniveau mit zeitgemäßen Technologieinnovationen.

Erwartungen an cloudbasierte Sicherheitslösungen

In der Regel führen mehrere Beweggründe zum Einsatz einer cloudbasierten Security-Lösung, die aber alle mit Unternehmenszielen wie Agilität, Effizienz und stärkeren Schutz zusammenhängen. An erster Stelle steht (mit 56 %) der Wunsch nach mehr Skalierbarkeit, denn Cloud-Umgebungen lassen sich bekanntlich dynamisch an schwankende Erfordernisse anpassen. Auf den Plätzen zwei und drei folgen Kosteneinsparungen (47 %) und schnellere Bereitstellung (46 %), eine klare Anerkennung der wirtschaftlichen und betrieblichen Vorteile cloudbasierter Sicherheitslösungen. Der Trend hin zu cloudbasierter Sicherheit, insbesondere angesichts des chronischen Fachkräftemangels, wird dadurch weiter belegt, dass sich 42 % der Befragten Leistungssteigerungen und 40 % eine Reduzierung des manuellen Aufwands beim Patching und bei Software-Upgrades erhoffen.

► Was sind die wichtigsten Beweggründe für die Nutzung cloudbasierter Sicherheitslösungen? (Bitte alle gültigen Antworten auswählen.)



Unternehmen, die die Einführung einer cloudbasierten Sicherheitslösung planen, sollten bei ihrer Entscheidung Skalierbarkeit, Kosteneffizienz und Deployment-Geschwindigkeit priorisieren, um die betrieblichen und wirtschaftlichen Vorteile der Cloud optimal zu nutzen. Lösungen, die Funktionen zur Straffung des Richtlinien-Managements und zur Gewährleistung der kontinuierlichen Einhaltung von Vorgaben bieten, können die Sicherheit insgesamt stärken und Resilienz bei der Reaktion auf neue Bedrohungen und Vorschriften aufbauen.

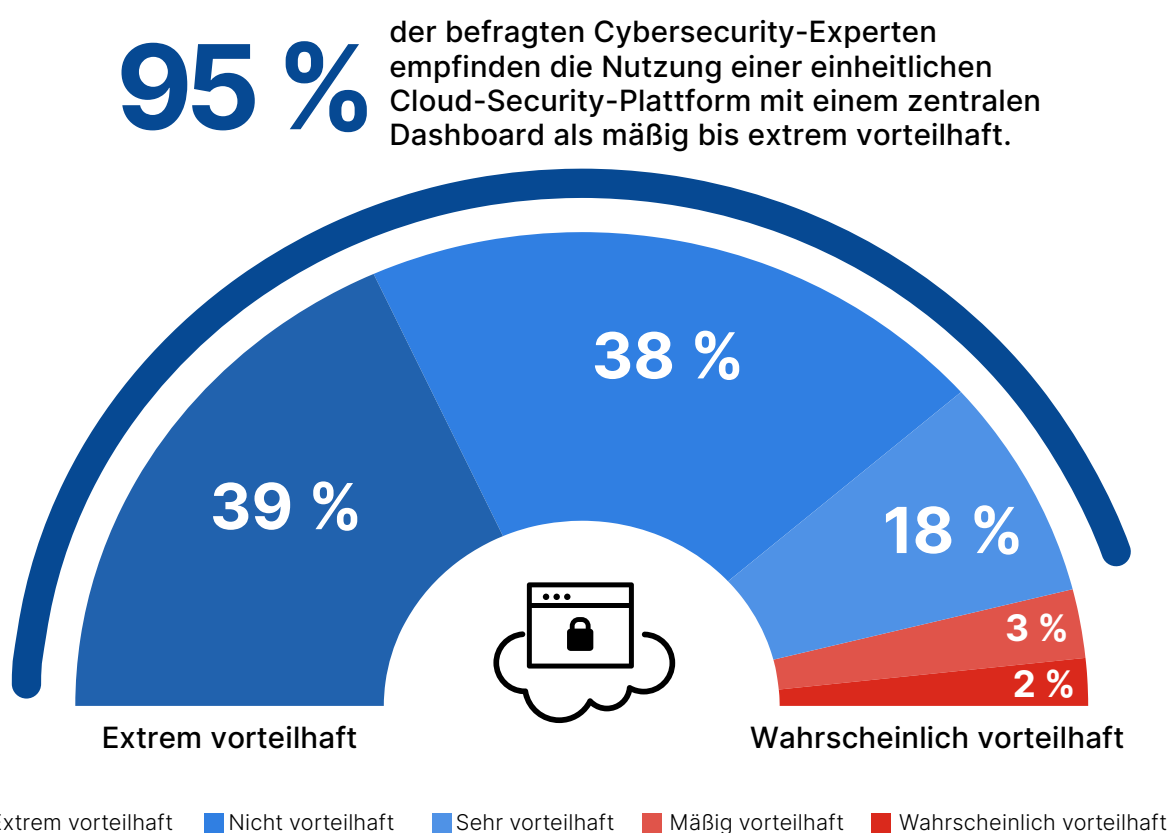
Weitere Nennungen:

Einfachere Richtlinienverwaltung 39 % | Bessere Verfügbarkeit 38 % | Erfüllung von Erwartungen bezüglich der Cloud-Compliance 34 % | Bessere Übersicht über Nutzeraktivitäten und das Systemverhalten 33 % | Sicherer Anwendungszugriff von beliebigen Standorten aus 32 % | Daten/Workloads befinden sich in der Cloud 28 % | Reduzierung der Anzahl der Appliances in Filialen 27 %

Eine einheitliche Cloud-Security-Plattform

Angesichts der bereits erwähnten Komplexität, des betrieblichen Aufwands und der Kompetenzlücken überrascht es nicht, dass sich Unternehmen eine einheitliche Sicherheitsplattform wünschen, mit der sie das Security Management über alle Cloud-Umgebungen hinweg zusammenführen und vereinfachen können. Beeindruckende 95 % der Befragten bestätigen, dass eine solche Plattform den konsistenten und umfassenden Schutz von Daten in der Cloud erleichtern würde.

- **Wie vorteilhaft wäre es für Sie, eine Cloud-Security-Plattform zu haben, auf der Sie von einem einzigen Dashboard aus alle Richtlinien konfigurieren könnten, die zum konsistenten und umfassenden Schutz aller Daten in Ihren Cloud-Umgebungen erforderlich sind?**



Dieser Wunsch nach einer zentralen, integrierten Lösung spiegelt den branchenweiten Trend zu plattformbasierter Konsolidierung wider, der von dem Streben nach effektiverer Sicherheit, unkomplizierten Integrationen und vermindertem Verwaltungsaufwand getrieben wird. Eine solche Plattform bietet den einzig sinnvollen Ansatz, mit dem Unternehmen dem Fachkräftemangel entgegenwirken und zunehmend komplexe, automatisierte Angriffe abwehren können. Mit einer konsolidierten Plattform wird die Verwaltung mehrerer Sicherheitsschnittstellen überflüssig und der Betrieb vereinfacht. Dank konsistenter Richtliniendurchsetzung und umfassenden Einblicken in alle Cloud-Umgebungen wird das Sicherheitsniveau unternehmensweit verbessert.

Sichere Cloud-Nutzung: Wichtige Cloud-Security-Strategien

Ein hohes Cloud-Sicherheitsniveau ist in der heutigen dynamischen Cloud-Landschaft für Unternehmen jeder Größenordnung unerlässlich. Die in diesem Leitfaden vorgestellten Best Practices zur Sicherung von Cloud-Umgebungen – von der Umstellung auf eine konsolidierte Security-Plattform bis zur Investition in Fachkompetenzen – helfen beim Schutz vor den komplexen Bedrohungen von heute und morgen.



EINHEITLICHE SECURITY-PLATTFORM:

Ermöglichen Sie die zentrale Kontrolle und Transparenz für alle Cloud-Umgebungen, um die betrieblichen Abläufe zu straffen und bessere Einblicke zu gewähren. Diese Strategie wird von 95 % der Unternehmen bevorzugt.



UMGEBUNGSUNABHÄNGIGE SICHERHEIT:

Da 78 % der Unternehmen eine Hybrid- oder Multi-Cloud-Infrastruktur nutzen, benötigen sie ein Sicherheitskonzept, das den diesen Umgebungen eigenen Herausforderungen begegnet und die konsistente Verwaltung und Durchsetzung von Sicherheitsrichtlinien ermöglicht.



AUTOMATISIERTES RICHTLINIEN- UND COMPLIANCE-MANAGEMENT:

Implementieren Sie Systeme, mit denen Sie Sicherheitsrichtlinien vereinheitlichen und in allen Cloud-Umgebungen automatisch anwenden können und die Ihnen die konsistente Einhaltung regulatorischer Vorgaben ermöglichen.



DATENSICHERHEIT ALS OBERSTE PRIORITÄT:

Etablieren Sie zuverlässige Daten-Governance- und Verschlüsselungspraktiken, um sensible Daten in allen Cloud-Services zu schützen. Damit adressieren Sie ein wichtiges Sicherheitsbedenken, das 58 % der Unternehmen teilen.



UNKOMPLIZIERTES KONFIGURATIONSMANAGEMENT:

Verhindern Sie Fehlkonfigurationen und schützen Sie Ihre Infrastruktur vor Sicherheitslücken, indem Sie Cloud-Konfigurationen aktiv verwalten.



BESSERE ZUGRIFFSKONTROLLE:

Effektives Identitäts- und Zugriffsmanagement bietet Ihnen die Vorteile des Zero-Trust-Prinzips und verhindert unbefugten Zugriff.



EFFEKTIVE BEDROHUNGSERKENNUNG UND -ABWEHR:

Mit erweiterten Analysefunktionen und automatisierter Bedrohungsabwehr lassen sich Angriffe in Echtzeit erkennen und stoppen.



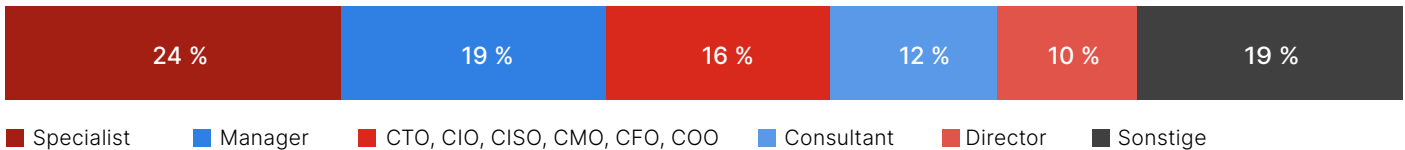
KOMPETENZEN BEI DER CLOUDNATIVEN SICHERHEIT:

93 % der befragten Unternehmen bereitet der Mangel an Cybersecurity-Fachkräften große Sorge. Daher ist es wichtig, den Ausbau cloudspezifischer Sicherheitskompetenzen unternehmensintern zu fördern, um effektiver durch die komplexe Cloud-Security-Landschaft zu navigieren.

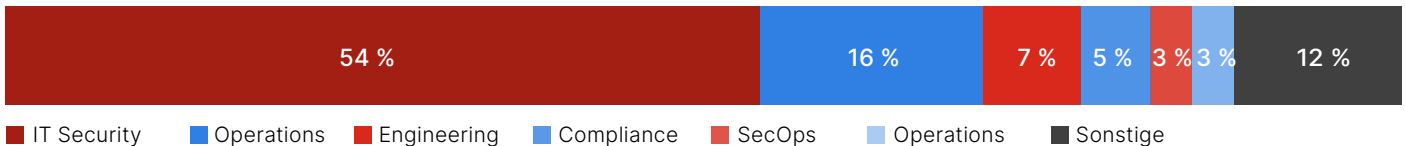
Methodik und Demographie

Der Cloud-Security-Bericht 2024 basiert auf einer ausführlichen globalen Umfrage im Februar 2024, an der 927 Cybersecurity-Experten teilnahmen. Durch diese Befragung sollte ermittelt werden, wie Unternehmen Clouds nutzen, wie sie die Entwicklung der Cloud-Sicherheit beurteilen und welche Best Practices für Manager mit Verantwortung für die IT-Cybersecurity bei der Migration in die Cloud Priorität haben. Bei der Auswahl der Umfrageteilnehmer wurde darauf geachtet, dass alle Hierarchieebenen von der Führungsriege bis zur IT-Fachkraft ohne Management-Verantwortung sowie diverse Unternehmensgrößen und mehrere Branchen vertreten waren.

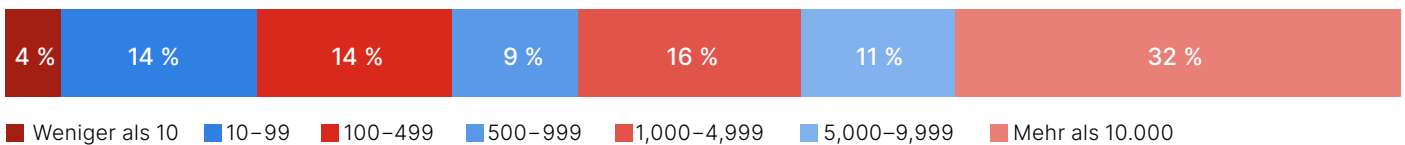
POSITION



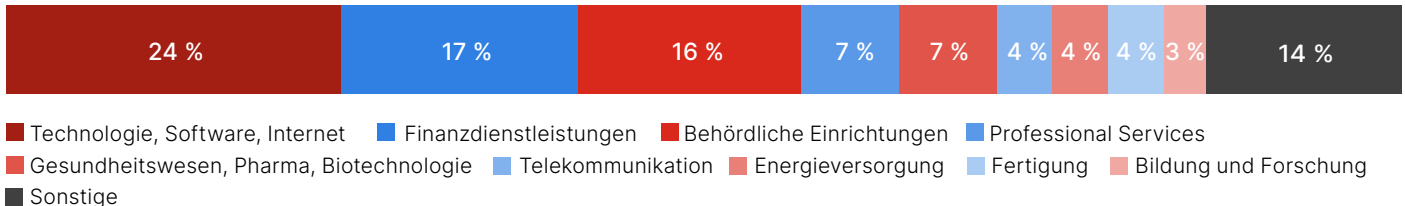
ABTEILUNG/BEREICH



UNTERNEHMENSGRÖÖE



BRANCHE



Reproduktion von Inhalten

Wir freuen uns, wenn Sie die Daten, Grafiken und Texte aus diesem Bericht für Ihre Zwecke verwenden. Wir bitten lediglich darum, die Bestimmungen der [Creative Commons Attribution 4.0 International License](#) zu beachten. Sie können dieses Dokument oder Teile davon gern teilen und gewerblich nutzen, solange Sie den Bericht gemäß den Lizenzbestimmungen als Quelle nennen, zum Beispiel als „Cloud-Security-Bericht 2024 von Cybersecurity Insiders und Fortinet“.



Fortinet (NASDAQ: FTNT) sichert einige der größten Unternehmen, Service Provider und Behörden in aller Welt. Fortinet gibt seinen Kunden umfassende Einblicke und Kontrolle über ihre wachsenden Angriffsflächen und versetzt sie damit in die Lage, die stetig steigenden Anforderungen bezüglich der Leistung zu erfüllen – heute und in Zukunft. Nur die Fortinet Security Fabric Platform ist den größten Herausforderungen gewachsen und kann Daten in kompletten digitalen Infrastrukturen schützen, darunter beispielsweise in Netzwerk-, Anwendungs-, Multi-Cloud- und Edge-Umgebungen. Als die Nummer 1, was die am häufigsten ausgelieferten Security Appliances angeht, vertrauen mehr als 730.000 Kunden Fortinet den Schutz ihrer Marke an.

www.fortinet.com/de

Cybersecurity

I N S I D E R S

Cybersecurity Insiders bringt mehr als 600.000 IT-Sicherheitsexperten und branchenführende Technologieanbieter zusammen, um smarte Lösungen für komplexe Probleme zu finden und gemeinsam die dringendsten Herausforderungen rund um Cybersecurity anzugehen.

Wir haben uns auf die Erstellung und Auswahl einzigartiger Inhalte spezialisiert, mit denen wir Cybersecurity-Experten über aktuelle Trends, Lösungen und Best Practices informieren. Von umfassenden Forschungsprojekten und unvoreingenommenen Produktrezensionen bis hin zu praxisbezogenen Leitfäden, spannenden Webinaren und informativen Artikeln stellen wir Ressourcen zur Verfügung, die evidenzbasierte Lösungskonzepte für unsere komplexe Cybersecurity-Landschaft bieten.

Kontaktieren Sie uns noch heute, um zu erfahren, wie Cybersecurity Insiders Sie dabei unterstützen kann, sich von der Masse abzuheben, die Nachfrage in einem wettbewerbsintensiven Markt anzukurbeln, die Bekanntheit Ihrer Marke zu steigern und eine Vordenkerposition einzunehmen.

Schicken Sie uns eine E-Mail an info@cybersecurity-insiders.com oder besuchen Sie cybersecurity-insiders.com.