# Report zum Stand der Anwendungs-strategie 2023

# Inhalt

# Einleitung
# Entweder-Oder hat ausgedient

**IN DER HEUTIGEN GLOBALEN KULTUR** geht es darum, geografische und andere Grenzen zu überwinden, um Konflikte abzubauen und Menschen, Ideen und Ressourcen zusammenzubringen. Dies gilt auch auf persönlicher Ebene, wo wir mit einer Vielzahl von Rollen jonglieren. Wir sind Berufstätige und Familienmitglieder, Bürger von Nationen und einer multikulturellen globalen Gemeinschaft. Das lässt sich auch auf Organisationen übertragen, die Ressourcen und Menschen verknüpfen müssen, um ihre Ziele zu erreichen. Um in all ihren Rollen erfolgreich zu sein, müsse Organisationen auf Agilität setzen. Die wird durch Anwendungen und APIs bereitgestellt, die alle Prozesse mit prompten und effizienten digitalen Helfern unterstützen.

# Hybride IT ist schwierig aber nachhaltig.

Heute sind 40% dieser Anwendungen modern oder nutzen moderne Komponenten. Neun von zehn Unternehmen treiben die digitale Transformation voran, um ihre IT-Stacks zu modernisieren, besser zu integrieren und die Vorteile zu nutzen, die am Edge möglich sind. Überraschender aber sind andere Ergebnisse der neunten jährlichen F5-Umfrage zum Stand der Anwendungsstrategie, denn sie haben das Zeug dazu, Anregungen zu geben, die sich sogar auf die Unternehmensstrategie vieler auswirken könnten.

Wenn sich in diesem Jahr eine Erkenntnis herauskristallisiert hat, dann die, dass der typische IT-Stack hybrid bleiben wird, d. h. dass Funktionen wie Rechenleistung, Netzwerk, Speicher und Anwendungen über Kern-, Cloud- und Edge-Umgebungen verteilt sind. Es sind nicht nur Clouds, die als “hybrid” bezeichnet werden können. Unternehmen werden auch weiterhin mehrere, unterschiedliche Technik-Stacks verwalten und verschiedene Generationen von Infrastrukturen und Anwendungen betreiben. (Ein bekanntes Beispiel ist der nach wie vor bestehende, milliardenschwere Markt für Faxgeräte, selbst im Zeitalter von E-Mail, SMS und Apps).

Viele CIOs kennen diesen Balanceakt. Sie müssen gleichzeitig ein digitales Geschäft ermöglichen und die Kundenerwartungen erfüllen und gleichzeitig mit Ressourcenbeschränkungen, den Herausforderungen technischer Schulden und den organisatorischen Anforderungen an Stabilität, Ausfallsicherheit und effektivem Änderungsmanagement jonglieren. Als Folge müssen IT-Experten immer besser mit unterschiedlichen und sich dynamisch wandelnden Systemen und Technologien zurechtkommen.

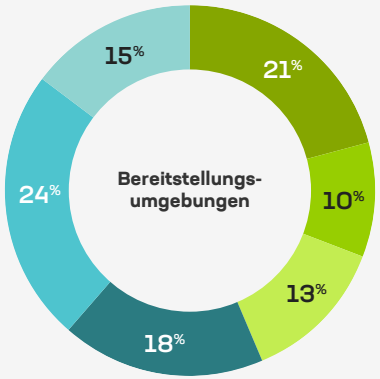
Die gute Nachricht: Hybride IT hat sich als nachhaltig erwiesen und wie in vielen anderen Bereichen unseres heutigen Lebens lautet das entscheidende Wort nicht “oder”, sondern “und”. Geschäftserfolg und -wachstum hängen davon ab, dass man Anwendungen und APIs standortübergreifend verbindet und gleichzeitig die Verwaltung komplexer hybrider Umgebungen vereinfacht. Diese Realität verändert die Anwendungssicherheit und -bereitstellung. Die aktuelle jährliche Umfrage von F5 unter IT-Entscheidern zeigt, welche Ansätze immer beliebter werden und was Ihr Unternehmen tun muss, um dabei Schritt zu halten.

01

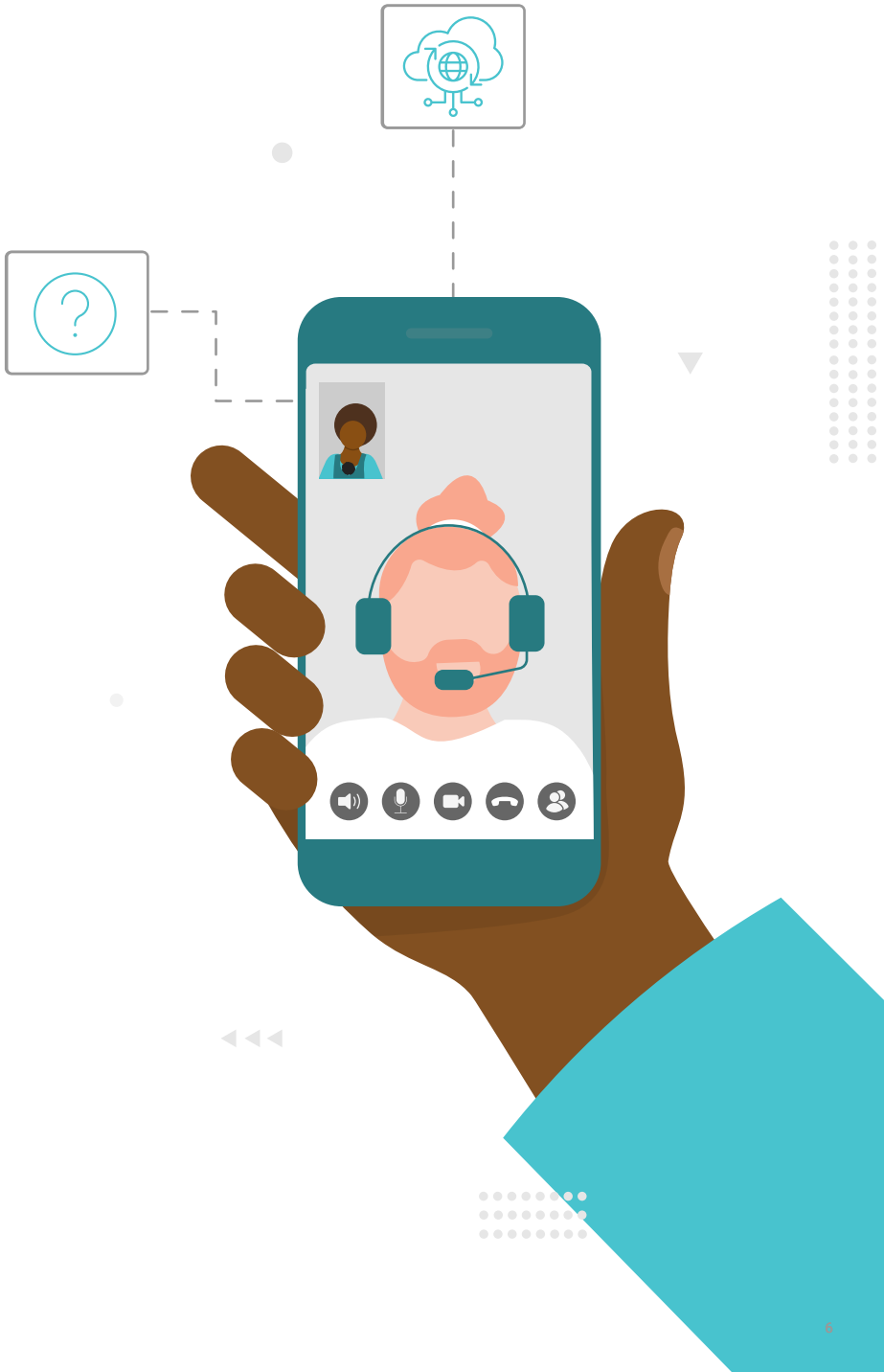
# IT wird für immer hybrid bleiben

**DIE AKTUELLEN DATEN ZEIGEN:** Die hybride IT ist auf dem Vormarsch. Nur 15% der Befragten betreiben Anwendungen in einer einzigen Umgebung. Die Mehrheit ist breiter verteilt und mehr als ein Fünftel der Anwendungen wird sogar in sechs verschiedenen Umgebungen gehostet. Unternehmen haben erkannt, dass es nicht die eine Umgebung gibt, die für alle Apps die beste ist. Einige benötigen ein Rechenzentrum vor Ort, während andere die Geschwindigkeit, Skalierbarkeit und Effizienz einer oder mehrerer Clouds benötigen, um App-spezifische Ziele zu erreichen.

## Apps sind weitestgehend verteilt




Ein
Zwei
Drei
Vier
Fünf
Sechs



**Public-Cloud-Bereitstellungen sind nicht die Regel.**

Wir haben auch festgestellt, dass sich der Run auf die Public Cloud beruhigt hat. Im Jahr 2018, gaben 74% der Befragten an, dass sie planten, “bis zur Hälfte” ihrer Anwendungen in einer “Cloud” bereitzustellen. Zwei Jahre später hat nur etwa ein Viertel diese Pläne umgesetzt – trotzdem ist Cloud Computing immer noch der mit Abstand spannendste Technologietrend.

Heute gibt knapp die Hälfte (48%) an, dass sie derzeit irgendeine Anwendung in der Cloud betreiben und im Durchschnitt setzen Unternehmen nur 15% ihres Anwendungsportfolios in der Cloud ein. Der Grund dürften Bedenken hinsichtlich der Datenkontrolle, der Sicherheit oder über ausufernde Kosten sein.

# Sicherheit ist das vorrangige Motiv für die Public Cloud.

Public Clouds sind für viele Unternehmen vor allem eine Option für die Sicherung und Ausfallsicherheit, aber nicht immer die erste Wahl für das Hosting von Anwendungen. Dieses Vorrecht geniessen On-Premise-Bereitstellungen: Nach einer Phase der Konsolidierung ist das Pendel nun zurückgeschwungen und die lokalen Installationen nehmen wieder zu.

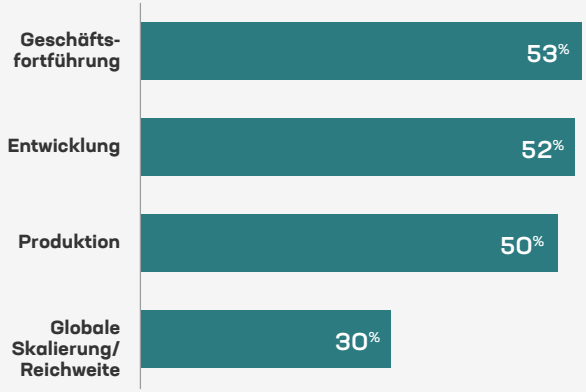
**On-premise-Bereitstellungen bleiben die Grundlage heutiger Anwendungsarchitekturen.**

Nach Jahren des Rückgangs stieg der Anteil der Anwendungen, die in traditionellen, lokalen Rechenzentren gehostet werden, gegenüber 2022 um zwei Prozentpunkte auf 37%. Der Anteil der On-Premises-Bereitstellungen übersteigt insgesamt die Hälfte, denn während viele bei On-Premises-Rechenzentren an eine monolithische Umgebung denken, ist es in Wirklichkeit so, dass dort sowohl traditionelle als auch Cloud-Umgebungen existieren. Obwohl die meisten anderen Bereitstellungsmodelle – wie Public Cloud und SaaS – in den letzten Jahren auf dem Vormarsch waren, ist ihr Anteil im Jahr 2023 gleichbleibend oder leicht rückläufig.

## Public Cloud bietet vor allem Ausfallsicherheit

**Gefragt wurde:**
Wie nutzen Sie die Public Cloud (IaaS)?
Wählen Sie alle zutreffenden Punkte aus.

**Das Ergebnis:**
**Für rund die Hälfte der Befragten, die eine Public Cloud nutzen, sind Backup und Disaster Recovery die wichtigsten Anwendungsfälle.**



Rückzug aus der Cloud ist eine der Ursachen für diesen Trend. Mehr als ein Drittel (43%) der Befragten gab an, dass sie in letzter Zeit Apps repatriiert haben oder dies planen. Die Notwendigkeit, den Wildwuchs von Apps in einer Multi-Cloud-Welt in Zaum zu halten, ist das Hauptmotiv, das von 54% derjenigen genannt wird, die Anwendungen repatriieren.

Führend bei der Rückführung von Anwendungen sind die Branchen Finanzdienstleistungen, Telekommunikation und Technologie – also genau diejenigen, die am ehesten mit mehreren Clouds jonglieren und vermutlich meist über die erforderlichen Fähigkeiten verfügen, um ihre Anwendungen on-premise effizient verwalten zu können.

Nach der Bereitstellung vor Ort sind mit mit deutlichem Abstand Private Clouds das nächsthäufige Bereitstellungsmodell: Nur 17% des durchschnittlichen Unternehmensportfolios wird so gehostet, also nicht einmal halb so viel, wie in lokalen Rechenzentren.

SaaS-Angebote liegen mit 16% dicht dahinter (obwohl technisch gesehen ein Verbrauchsmodell und kein Bereitstellungsmodell). Im Gesamtbild ergibt sich eine hybride Vielfalt mit lokalen Rechenzentren als Schwergewicht.

## Moderne App-Architekturen sind überall.

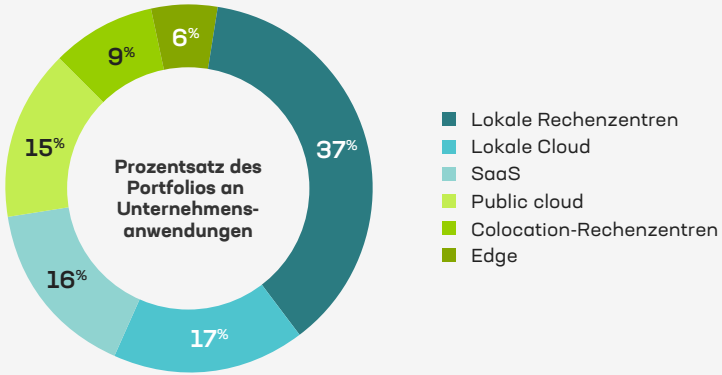
Eine Gemengelage auch bei den App-Architekturen: Jeder Umfrageteilnehmer betreibt moderne Apps, nutzt SaaS oder beides. Die Befragten berichten, dass unabhängig vom Einsatzort im Schnitt mehr als ein Drittel (40%) ihres App-Portfolios (ohne SaaS) als modern bezeichnet werden kann, was mobile Apps und die Nutzung von Microservices einschließt. Dieser Prozentsatz ist stetig gewachsen und wir erwarten, dass er bis 2025 50% (oder sogar 60%) übersteigen wird. Aber heute betreiben mit 95% fast alle Unternehmen auch noch traditionelle Apps. Infolgedessen steht die große Mehrheit (85%) der Unternehmen vor der Herausforderung, sowohl moderne als auch herkömmliche Anwendungen zu verwalten und zu sichern – und das oft in einer Vielzahl von Hosting-Umgebungen.

## Multi-Cloud-Umgebungen werden überleben

2023

**Gefragt wurde:**
Wie viel Prozent ihrer heute eingesetzten Anwendungen nutzen die folgenden Bereitstellungsmodelle? Bitte geben Sie Werte ein, die sich zu 100% addieren.

**Das Ergebnis:**
**Eine Vielfalt von App-Standorten ist die Norm.**



Da App-Portfolios im Laufe der Zeit immer moderner werden, erwarten wir einen Rückgang bei der Zahl der Unternehmen, die sowohl moderne als auch traditionelle Apps einsetzen. Dieser Prozentsatz dürfte 2022 mit 88% seinen Höhepunkt erreicht haben. Ganz auf Null wird er aber wohl nie sinken, da viele CIOs traditionelle Anwendungen mit Mehrwert intakt lassen.

Wenn es darum geht, herkömmliche Anwendungen aus dem Verkehr zu ziehen, ersetzen 59% der Befragten diese durch moderne Apps. Unternehmen in der Fertigungsindustrie und in der öffentlichen Verwaltung entwickeln dabei am ehesten selbst Apps. 46% der Unternehmen dagegen – vor allem im Gesundheitswesen – wechseln stattdessen zu SaaS-Angeboten. Generell wird die Modernisierung oft ausgelagert, weil so gleichzeitig weniger entwickelt und mehr bereitgestellt werden kann. Einer von fünf Befragten erwartet, dass er nicht mehr benötigte Anwendungen einfach stillegt.

Aber immerhin 16% der Teilnehmer haben keine Pläne, herkömmliche Apps außer Betrieb zu nehmen. Vor allem im Bank- oder Versicherungswesen bieten diese die Kernfunktionen des Unternehmens. In Branchen wie dem Energiesektor, dem Gesundheitswesen oder der Telekommunikation, in denen Regulatorien nur langsamen Fortschritt bedingen, erwarten bis zu 33% der Befragten die Beibehaltung herkömmlicher Anwendungen. Daraus folgt, dass der Prozentsatz moderner Anwendungen im durchschnittlichen Portfolio aller Branchen in diesem Jahrzehnt wahrscheinlich bei 85% liegen wird. Und ein erheblicher Teil davon sind möglicherweise Microservices, die nur eine Schnittstelle zu einer traditionellen Anwendung darstellen.

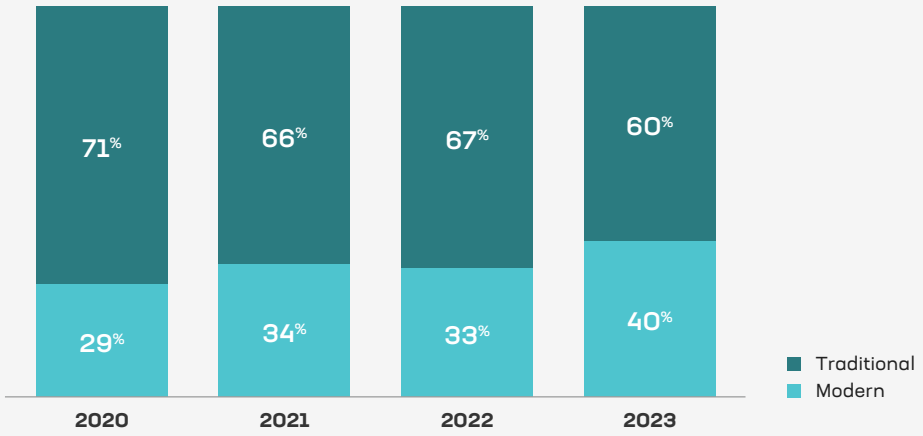
Kurz gesagt, die Mehrheit der CIOs wird in absehbarer Zukunft hybride App-Architekturen und über hybride Umgebungen verteilte Apps mehrerer Generationen zu betreuen haben.

## Moderne App-Architekturen weiterhin auf dem Vormarsch

2023

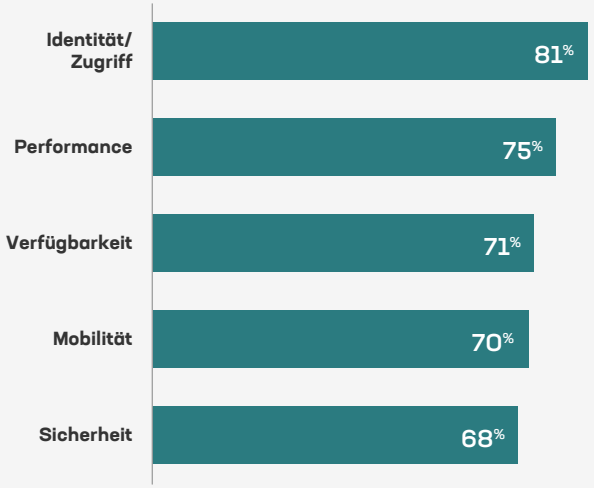
**Gefragt wurde:**
Wie viel Prozent Ihrer aktuellen Anwendungen fallen in in die beiden Kategorien? Bitte geben Sie Werte ein, die sich zu 100% addieren.

**Das Ergebnis:**
**Moderne App-Architekturen machen fast die Hälfte des durchschnittlichen Portfolios aus.**



**Auch die Technologien der Sicherheit und Bereitstellung von Anwendungen sind in den Unternehmen verteilt.**
Die Technologien, die die Anwendungssicherheit und -bereitstellung unterstützen, sind ebenso wie die Apps selbst verteilt. Meist entscheidet ihr Zweck über den Einsatzort und die Umgebung wiederum beeinflusst die Technologie. So eignet sich etwa die Hardware einer Web Application Firewall (WAF) am besten für ein Rechenzentrum vor Ort, während Apps in der Cloud, durch ein Security-as-a-Service-Angebot (SECaaS) effizienter geschützt werden können. In anderen Situationen wird die Security am besten so nah wie möglich am Benutzer platziert, da ein früheres Stoppen von Angriffen Ressourcenüberlastung verhindert, während Layer-7-Routing-Dienste am besten in der Nähe der Anwendung selbst arbeiten. Darum sind in hybriden Umgebungen mehrere Bereitstellungen von Technologien für die Sicherheit und Bereitstellung von Anwendungen sinnvoll.

**Die Befragten verlassen sich am meisten auf Identitäts- und Zugriffs-Technologien**




# Technologien für die App-Sicherheit werden besonders häufig in der Cloud eingesetzt.

Infolgedessen setzt die Mehrheit der Befragten (59%) solche Dienste vor Ort ein und ähnlich viele nutzen mindestens einen in der Cloud. Cloud-Bereitstellungen sind besonders bei Sicherheitstechnologien üblich. Die Bereitstellung von Anwendungssicherheits- und Bereitstellungstechnologien über SaaS von Drittanbietern wird jedoch immer beliebter und ist die zweithäufigste Art der Bereitstellung. Fast ein Drittel (30%) der Befragten gibt an, diese Methode zu verwenden, die es ihnen ermöglicht, Anwendungen über Clouds oder andere Umgebungen hinweg zu erweitern und zu skalieren, ohne die Komplexität zu erhöhen oder die Kontrolle zu verringern.

Unabhängig davon, wo sie gehostet werden, nimmt die Verwendung von Technologien für die Sicherheit und Bereitstellung von Anwendungen zu, da Unternehmen die digitale Transformation vorantreiben und daran arbeiten, ein Gleichgewicht zwischen digitaler Geschwindigkeit und Sicherheit und betrieblicher Stabilität herzustellen. Identitäts- und Zugriffsmanagement-Technologien (IAM) wie SSL VPN, Single Sign-On (SSO) und Id-Federation sind heute die am häufigsten eingesetzten App-Services. Dabei hat sich die Gesamtzahl derer, die diese Services einsetzen seit 2017 mehr als verdoppelt. Dies ist ein Maß für ihre Bedeutung, denn die von Anwendungen bereitgestellten digitalen Dienste sind nicht nur das Gesicht des Unternehmens, sondern wirken auch direkt auf sein Portemonnaie ein.

**Multi-Clouds bleiben schwierig - aber es gibt Lösungen.**
Nicht überraschend, dass in dieser hybriden und verteilten Anwendungslandschaft fast neun von zehn Befragten, die in Multi-Clouds arbeiten, weiterhin Herausforderungen in Bezug auf Sicherheit, Leistung und Kosten sehen. Die größte Herausforderung im Jahr 2023 ist die Komplexität von Tools und APIs, die sich aus der fehlenden Standardisierung oder Interoperabilität der genutzten Tools ergibt. Knapp dahinter folgt die Umsetzung konsistenter Sicherheitsrichtlinien und die Leistungsoptimierung der Apps.

# Zunehmende Angriffsfläche von APIs erschwert Einsatz von Multi-Clouds.

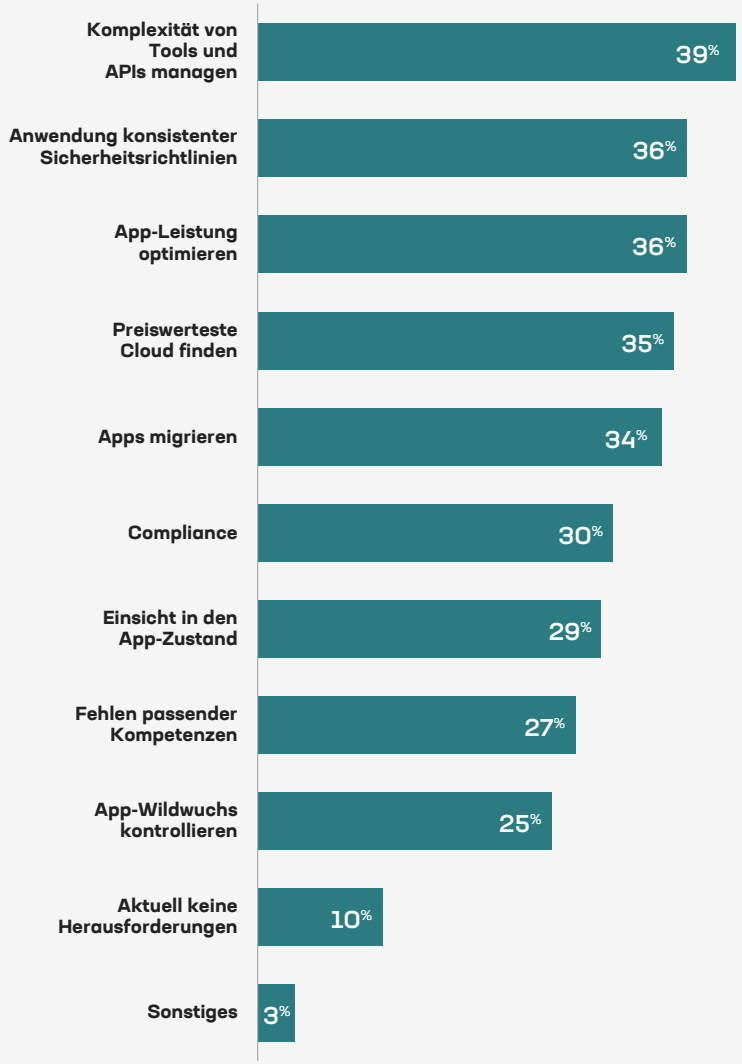
Diese Herausforderungen sind zweifellos der Grund dafür, dass Unternehmen in Nord- und Südamerika sowie in Europa, dem Nahen Osten und Afrika Multi-Cloud-Networking als den aufregendsten Trend der nächsten Jahre bezeichneten. Die Befragten im asiatisch-pazifischen Raum dagegen begeistern sich mehr für die Konvergenz von IT- und Betriebstechnologien (IT/OT). Dies hängt wahrscheinlich mit dem Status der Region als globales Fertigungszentrum zusammen, spricht aber auch für die Notwendigkeit einer besseren Integration von Maschinensteuerungen mit anderen Geschäftssystemen, um die Effizienz zu verbessern.

Andere Lösungen, die jetzt für die Verbindung, den Schutz und die Verwaltung einer Multi-Cloud-Realität verfügbar sind, umfassen eine stärkere Automatisierung, Ökosystemansätze und Partner, die zur Vereinfachung beitragen können. Deklarative Bereitstellungsrichtlinien, die konsistente Sicherheit bieten, können globalen Schutz bieten und gleichzeitig die Reibung zwischen funktionalen Silos beseitigen. Und da die hybride IT nicht verschwinden wird, werden sich dieselben Lösungen, die das Multi-Cloud-Management erleichtern, für die meisten Unternehmen als zunehmend hilfreich erweisen.

## Komplexität ist die größte Bürde der Multi-Cloud

**Gefragt wurde:**
Vor welchen Herausforderungen stehen Sie derzeit bei der Bereitstellung von Anwendungen in Multi-Clouds?

**Das Ergebnis:**
**Weiterhin Probleme bei Komplexität und Sicherheit, aber die fehlende Sichtbarkeit von App-Problemen fällt auf Platz 7.**



# Erkenntnisse von F5

Die meisten Unternehmen möchten bei der Infrastruktur die Komplexitäten verringern und den Lebenszyklus verlängern, die Zielumgebungen zusammenlegen und die Zahl der Einzellösungen reduzieren. Da sie jedoch ihre Anwendungen modernisieren, verlagern und häufig ihr Anwendungsportfolio erweitern, beseitigen sie in der Regel keine Architekturen oder Standorte, sondern ändern nur Proportion und Zweck jeder Umgebung und so die Art der daraus resultierenden Herausforderungen. Darüber hinaus gehen wir davon aus, dass der Anteil moderner App-Architekturen im durchschnittlichen Portfolio bis 2030 bei 85% liegen wird. Da Kosten, Kontrolle, Latenz, Geschäftskontinuität und Skalierbarkeit ein ständiges Anliegen sind, wird es immer gute Gründe geben, mehr als eine Bereitstellungsoption beizubehalten. Keine einzelne Umgebung wird für jeden Zweck geeignet sein.

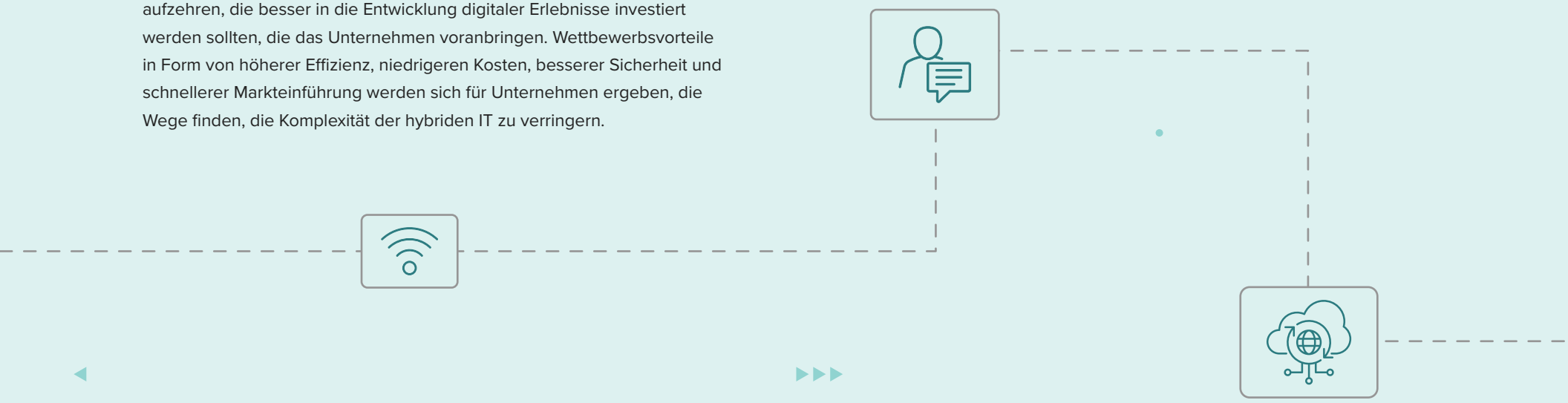
### Was das für Sie bedeutet

Das digitale Geschäft erfordert eine anpassungsfähige IT-Infrastruktur. Um ihre Ziele zu erreichen, benötigen Unternehmen Lösungen, die die Herausforderungen des Betriebs in hybriden und Multi-Cloud-Landschaften bewältigen helfen. Andernfalls wird der Verwaltungsauwand Zeit und Ressourcen aufzehren, die besser in die Entwicklung digitaler Erlebnisse investiert werden sollten, die das Unternehmen voranbringen. Wettbewerbsvorteile in Form von höherer Effizienz, niedrigeren Kosten, besserer Sicherheit und schnellerer Markteinführung werden sich für Unternehmen ergeben, die Wege finden, die Komplexität der hybriden IT zu verringern.

Sieger wird, wer ergänzende Ansätze kombinieret, wie etwa:

- IT-Praktiker, die kein isoliertes Fachwissen haben, sondern system- und technologieübergreifend arbeiten können.
- Prozessmethoden nutzt, wie das Site Reliability Engineering (SRE).
- Werkzeuge wie deklarative Bereitstellungsrichtlinien einsetzt.
- Technologien für die Sicherheit und Bereitstellung von Anwendungen beherrscht, die modellübergreifend sind, als Service bereitgestellt werden können, in allen verteilten Anwendungen und Architekturen des Unternehmens einheitlich funktionieren – und sowohl für die derzeitige Architektur als auch eventuelle zukünftige Anpassungen geeignet sind.

Für viele Unternehmen wird der Schlüssel zum Erreichen dieser Ziele in der Zusammenarbeit mit Partnern liegen, deren Lösungen die Konnektivität von Multi-Cloud-Netzwerke erweitern. So können sie alle Arten von Anwendungen und APIs, die über verschiedene Clouds, Rechenzentren und Edge-Standorte verteilt sind, sichern und bereitstellen.



02

# Die digitale Transformation wird zur Unternehmensstrategie

2023

**IM JAHR 2023** berichten etwa neun von zehn Befragten quer über alle Branchen von laufenden Projekten zur digitalen Transformation – genau wie in jedem der drei Vorjahre. Und obwohl die digitale Transformation in unserer hybriden Welt nicht mehr neu ist, bleibt sie aus guten Gründen aktuell.

Für Unternehmen verspricht sie einen deutlichen Mehrwert durch verbesserte Effizienz, neue Möglichkeiten, optimierte Kundenerfahrungen und -beziehungen sowie die Fähigkeit, schneller skalieren zu können. Diese Vorteile machen die digitale Transformation zu einer Unternehmensstrategie auf höchster Ebene und nicht nur zu einer IT-Angelegenheit.

## Modernisierung ist der Motor der digitalen Transformation.

Dabei erfolgt die digitale Transformation in drei Phasen: Aufgabenautomatisierung, digitale Erweiterung (einschließlich Skalierung und Integration von Automatisierungen) und Entscheidungsfindung mit Hilfe von Telemetrie, künstlicher Intelligenz und maschinellem Lernen.

Im aktuellen Jahr 2023 sind die meisten Befragten in Phase zwei, überarbeiten also ihre Systeme und Anwendungen für die Zukunft.

Genau genommen arbeiten mehr als acht von zehn Organisationen derzeit an der Modernisierung und digitalen Erweiterung. Das ist eine Verdopplung gegenüber der Zeit vor COVID-19, als nur etwas mehr als ein Drittel der Unternehmen (37%) in Phase zwei war. Die Pandemie hat die digitale Transformation also um einen großen Schritt vorangebracht.

Zu den aktuellen Modernisierungsaktivitäten gehören die Entwicklung moderner Anwendungen und das Hinzufügen moderner Komponenten zu herkömmlichen Anwendungen, die Kerngeschäftsfunktionen bereitstellen. Was dabei geändert wird, ist die Art und Weise wie auf diese Anwendungen zugegriffen wird und wie sie erlebt werden. Beispiele hierfür sind mobile Apps, die eine Schnittstelle zur grundlegenden Logik von Branchen wie dem Bank- und Versicherungswesen bilden oder Integrationen für die Auftragserfassung und -verfolgung bei der Steuerung von Produktionsanlagen.

Obwohl mehr als die Hälfte der Unternehmen auch in der dritten Phase der digitalen Transformation, dem KI-gestützten Teil, arbeiten, ist dieser Anteil seit 2021 gesunken – dies wahrscheinlich aus zwei Gründen.

### Bei der Modernisierung sind fast alle mit an Bord

**27%**

**Phase 1**
Aufgabenautomatisierung: Apps

**81%**

**Phase 2**
Digitale Erweiterung: Modernisierung

**54%**


**Phase 3**
KI-gestütztes Business: Daten & Analytik

Die Herausforderungen bei der Implementierung von KI oder ML im großen Maßstab können die Begeisterung dafür abkühlen. Generell ist die digitale Transformation ein iterativer Prozess. Es ist üblich, dass Unternehmen in allen drei Phasen gleichzeitig arbeiten oder in einer Phase Fortschritte machen, bevor sie zu einer früheren Phase zurückkehren, um sie weiter zu automatisieren. Insbesondere bei der KI-Unterstützung kann das, was wie ein Rückschritt aussehen mag, die Grundlage für einen weiteren Sprung nach vorn bilden. Dies ist auch der Grund, warum die Arbeit in Phase eins, der Aufgabenautomatisierung, gegenüber dem Jahr 2020 (damals 46%) zurückgegangen ist, aber wahrscheinlich noch einige Zeit weitergehen wird, wenn Unternehmen verstärkt ihre Back-Office-Funktionen automatisieren.

**IT Ops bleiben die Priorität der Digitalen Transformation.**
Fast zwei Drittel der Befragten (64%) modernisieren derzeit den IT-Betrieb, sogar mehr als in den Vorjahren. Die Modernisierung ist nicht nur notwendig, um die Unterstützung durch KI zu ermöglichen, sondern auch, um die Belastung der IT-Teams abzumildern, denn eine Transformation, die sich über das gesamte Unternehmen erstreckt, erhöht die Anforderungen an die begrenzten IT-Ressourcen. Auch die damit verbundenen IT-Prozesse müssen modernisiert werden, um Engpässe zu vermeiden.

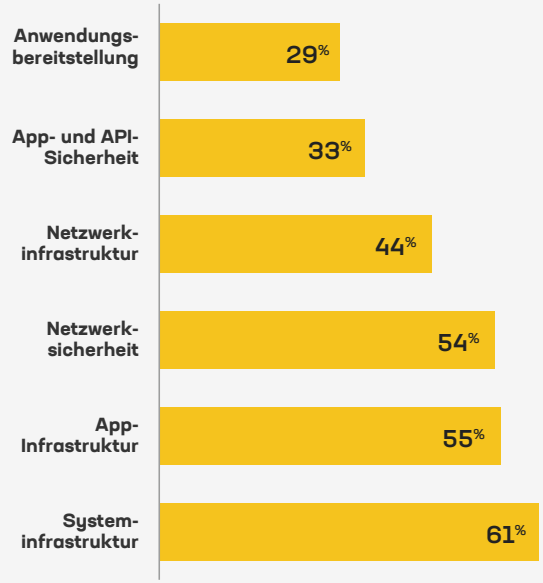
## Die Automatisierung bewirkt in der Regel eine höhere Effizienz der IT.

Das Bewusstsein für diese Notwendigkeit spiegelt sich auch in den Plänen von mehr als der Hälfte der Befragten (59%) wider, SRE-Praktiken (Site Reliability Engineering) einzuführen, die die Verwendung digitaler Tools und Automationen bedingen, um alle Prozesse flexibler und leistungsfähiger zu machen.

### Der Grad der Automations vaiiert stark

**Gefragt wurde:**
Welche IT-Funktionen haben Sie bereits automatisiert? Mehrere Antworten sind erlaubt.

**Das Ergebnis:**
**Die Automatisierung der Anwendungssicherheit und -bereitstellung bleibt eine Chance.**



Der wichtigste Weg zur Steigerung der IT-Effizienz ist jedoch die Automatisierung und nicht die Modernisierung. Die Automatisierung kann in jeder der sechs IT-Kernfunktionen erreicht werden: Systeminfrastruktur, Netzwerkinfrastruktur, App-Infrastruktur, Netzwerksicherheit, App-Bereitstellung und App-Sicherheit. Der Fokus der Automatisierung lag bisher auf der Systeminfrastruktur, der Netzwerksicherheit und der App-Infrastruktur.

- Die Automatisierung der Systeminfrastruktur – wie virtuelle Maschinen und Kubernetes – profitiert von der Reife der Virtualisierung und der soliden Unterstützung der Industrie für Container-Ökosysteme.
- Die Automatisierung der Netzwerksicherheit, die zunehmend auf Servicemodelle verlagert wird, wird durch KI und das Vorhandensein genau definierter Szenarien unterstützt.
- Der Treiber bei der Automatisierung der App-Infrastruktur sind Sicherheitsbedrohungen und die Notwendigkeit, die Markteinführungszeiten neuer Funktionen und Apps zu verkürzen.

Zwei Drittel der Unternehmen geben an, dass sie die IT-Effizienz bereits gesteigert haben, was 2018 als wichtigstes Ziel der digitalen Transformation angesehen wurde. Fünf Jahre später ist dieses Ziel erreicht.

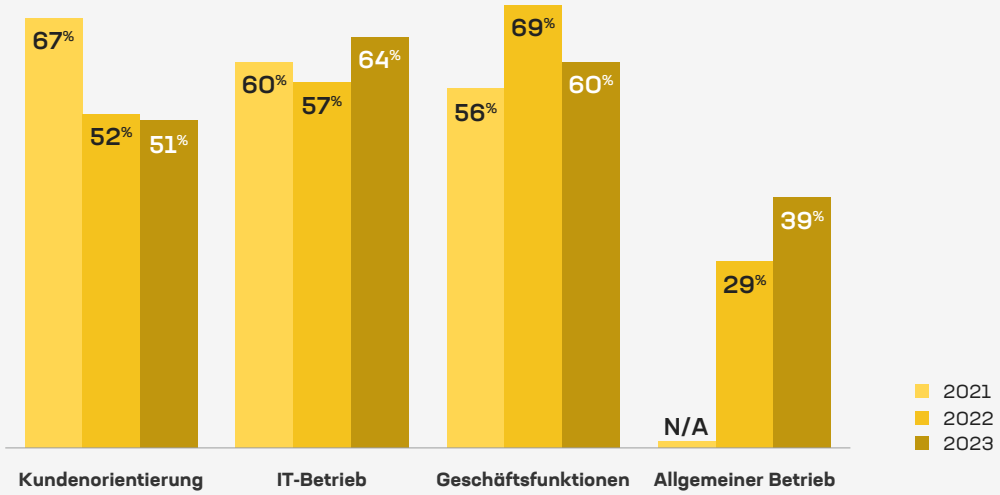
Die Umfrageteilnehmer, die von einer gesteigerten IT-Effizienz berichten, haben im Durchschnitt in mindestens drei der sechs Bereiche automatisiert. Natürlich berichten sie von den größten Effizienzvorteilen in den drei Bereichen mit der größten Aktivität und Automatisierungsreife, d. h. in den Bereichen System- und Anwendungsinfrastrukturen sowie Netzwerksicherheit. Da ein höherer Automatisierungsgrad jedoch in der Regel mit einer höheren Effizienz einhergeht, sollten Unternehmen, die einen Wettbewerbsvorteil anstreben, in allen sechs Bereichen automatisieren.

Die Vorteile sind besonders groß für Unternehmen, deren Betrieb in erster Linie digital ist. Ein traditioneller Fertigungsbetrieb verursacht Fixkosten, die von Investitionen in Anlagen bis hin zu Lagerflächen reichen.

## Die Prioritäten der digitalen Transformation verschieben sich

**Gefragt wurde:**
Welche Unternehmensfunktionen haben bei Ihren Initiativen zur digitalen Transformation Priorität? Mehrfachantworten sind möglich .

**Das Ergebnis:**
**Die digitale Transformation von Geschäftsfunktionen und des allgemeinen Betriebs hat seit 2021 zugenommen.**



Im Gegensatz dazu stellen für ein digitales Unternehmen – selbst für Einzelhändler, die überwiegend online verkaufen – die variablen Arbeits- und IT-Kosten in der Regel einen bedeutenden oder sogar die Hauptkosten für das „Produkt“ dar, das häufig eine Dienstleistung ist. In solchen Fällen wirkt sich eine höhere IT-Effizienz direkt und deutlich auf das Endergebnis aus.

## Digitale Transformation kommt allen Aspekten des Unternehmens zugute.

Natürlich ist die IT-Effizienz nicht der einzige Vorteil der Automatisierung, und die Vorteile der Modernisierung gelten auch für andere Geschäftsprozesse. Während der Kundenservice nach wie vor eine wichtige Modernisierungspriorität darstellt, sind die kundenorientierten Anwendungen und Prozesse insgesamt (einschließlich Vertrieb und Marketing) in den letzten zwei Jahren als Priorität deutlich zurückgegangen.

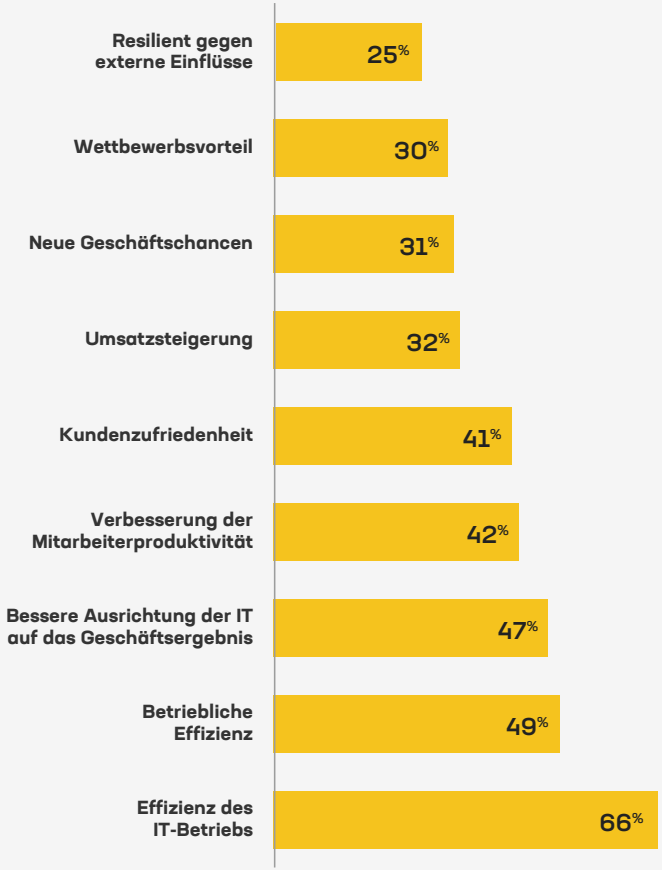
Dies mag zum Teil daran liegen, dass in diesen Bereichen bereits erhebliche Anstrengungen unternommen wurden, aber es ist auch klar, dass die Führungskräfte ihre Aufmerksamkeit zunehmend auf ineffiziente interne Prozesse und isolierte Legacy-Apps richten, damit sie die Leistung unter den heutigen unsicheren wirtschaftlichen Bedingungen nicht beeinträchtigen.

Erfreulicherweise berichtet fast die Hälfte der Befragten, die sich mit der digitalen Transformation befassen, von einer gesteigerten betrieblichen Effizienz im gesamten Unternehmen, nicht nur in der IT. Die allgemeine Mitarbeiterproduktivität und die Kundenzufriedenheit sind nicht weit entfernt. Ebenso berichtet fast ein Drittel der Befragten über höhere Umsätze und neue Geschäftsmöglichkeiten.

## Auf die Digitale Transformation folgt operative Effizienz

**Gefragt wurde:**
Welche Vorteile sehen Sie in Ihren Bemühungen um die digitale Transformation?

**Das Ergebnis:**
**Zwei Drittel der Befragten beobachten eine verbesserte IT-Effizienz, aber auch andere Vorteile sind wichtig.**



## Die Transformation hat viele Gesichter.

Ob Ihr Unternehmen von den Vorteilen der digitalen Transformation profitiert, hängt unter anderem auch davon ab, wie digital Ihr Geschäftsmodell ist. Heute geben mehr als drei Viertel der Befragten (79%) an, dass sie digitale Dienstleistungen für Verbraucher, andere Organisationen oder beides erbringen. Nur einer von fünf (21%) bietet diese Dienste einzig alleine für seine eigenen Mitarbeiter an.


Wir definieren digitale Dienstleistungen als eine Sammlung von Apps, APIs, App-Bereitstellungs- und Sicherheitstechnologien sowie Daten und anderen Ressourcen, die nahtlos zusammengefügt werden. Ziel ist es, digitale Erlebnisse zu schaffen, die dem anbietenden Unternehmen ein Ergebnis liefert. Die Beispiele reichen von Gigworker-Apps und Zeiterfassung für Mitarbeiter bis hin zu digitalen Medienabonnements, mobilem Check-in am Flughafen und mobilen Zahlungen. Sie können den Nutzern ohne Extrakosten zur Verfügung gestellt werden oder auf verschiedenen Einnahmemodellen beruhen, darunter On-Demand, Pay-as-you-go oder Abonnements.

Aber während fast alle Befragten digitale Dienstleistungen anbieten, nutzt nur etwas mehr als die Hälfte (58%) diese, um das Geschäft wesentlich voranzutreiben, wobei diese Dienstleistungen die Hälfte oder mehr des Jahresumsatzes des Unternehmens ausmachen. Darüber hinaus gibt es einen Unterschied zwischen den Unternehmen, die den digitalen Dienstleistungen den Vorrang geben, und denen, die ihr Geld eher durch analoge Interaktionen verdienen. Insbesondere die digitalen Umsatzträger haben eine höhere Wahrscheinlichkeit dafür, dass sie:

- Moderne App-Portfolios betreiben
- Technologien für Anwendungssicherheit und -bereitstellung nutzen.
- Public Clouds für jeden Zweck einsetzen, insbesondere aber in der Produktion zur schnellen globalen Skalierung von Infrastruktur und Anwendungen sowie zur Gewährleistung der Geschäftskontinuität.
- SaaS- und SECaaS-Dienste einkaufen.
- Den Edge verwenden, vor allem um ihre Kunden besser zu erreichen.

Mehr als die Hälfte der Unternehmen sind also digitale Dynamos, die mehr oder weniger mit den neuesten IT-Technologien Schritt halten. Die andere Hälfte setzt andere Prioritäten und leitet die Ressourcen anderswo hin, von der geografischen Expansion über die Produktentwicklung bis hin zur Sicherheit. Es ist ein Balanceakt. Hinzu kommt, dass sich keine zwei Unternehmen, selbst in derselben Branche, zur selben Zeit auf dieselben Prioritäten konzentrieren – oder dieselben Fortschritte machen, wenn doch.

Die Digitalisierung des heutigen Lebens wird sich nicht mehr umkehren. Je nach ihren Zielen sollten CIOs und andere Unternehmensleiter darauf achten, dass ein erheblicher Rückstand gegenüber dem Stand der Technik oder ein zu langes Verharren in einem hauptsächlich analogen Umsatzmodell es schwierig machen könnte, diesen Rückstand später aufzuholen. Die Modernisierung kann ein langer Weg sein, der für jedes Unternehmen anders aussieht, aber kluge CIOs wollen immer weiter vorankommen, auf die eine oder andere Weise, um nicht zu weit in Rückstand zu geraten.

# Erkenntnisse von F5

Unabhängig davon, wie viel Umsatz sie mit digitalen Diensten erzielen, müssen Unternehmen, die in der App- und API-gesteuerten Wirtschaft der Zukunft wettbewerbsfähig sein wollen, über die Aktivitäten, Technologien und Strategien derjenigen auf dem Laufenden bleiben, die digitale Dienste am effektivsten monetarisieren.

Es ist nicht nur so, dass es sich niemand leisten kann, von der Konkurrenz abgehängt zu werden. Selbst die traditionellsten Branchen werden in Zukunft wahrscheinlich digitale Dienstleistungen anbieten. Das kann alles bedeuten, von neuen virtuellen Angeboten im Bildungsbereich über Robotik in der Altenpflege bis hin zu drohnengestütztem Ressourcenabbau.

Selbst wenn ein Unternehmen auf digitale Erfahrungen setzt, besteht immer noch die Gefahr, dass öffentlichkeitswirksame Sicherheits- oder Betriebsfehler auftreten, die den Ruf schädigen oder zu rechtlichen Konsequenzen führen. Führungspersönlichkeiten, die die in Automatisierung und Modernisierung – und damit in Effizienz – investieren, während andere sich mit dem Status quo zufrieden geben, werden besser für Innovationen positioniert sein und vielleicht die Konkurrenz angesichts des Wandels überflügeln.

### Was das für Sie bedeutet

Jedes Unternehmen, dessen IT-Betriebsteam die Systeminfrastruktur, die App-Infrastruktur und die Netzwerksicherheit noch nicht automatisiert hat, kann immer noch erhebliche Vorteile erzielen – Vorteile, von denen viele Mitbewerber vielleicht schon profitieren. Wer die Nase vorn hat, sollte auch die Automatisierung der anderen drei IT-Kernfunktionen erkunden: Netzwerkinfrastruktur, App-Bereitstellung und App-Sicherheit. Insbesondere die Automatisierung der App-Bereitstellung und der App- und API-Sicherheit bietet für die meisten Unternehmen enorme Möglichkeiten. Natürlich kann es schwieriger sein, diese Bereiche zu automatisieren, da einzelne Anwendungen oft einzigartige Umstände aufweisen, die eine einfache Nutzung vorhandener Ressourcen oder Tools ausschließen. Aber die Automatisierung in diesen Bereichen steht in engerem Zusammenhang mit höherer Kundenzufriedenheit, größeren Umsätzen und der Erschließung neuer Geschäftsmöglichkeiten als die Automatisierung in anderen IT-Kernbereichen. Diese Vorteile, die über die IT-Effizienz hinausgehen und sich auf das gesamte Unternehmen auswirken, können den Aufwand wert sein.

Abschließend wird immer deutlicher, dass Unternehmen, die langfristig erfolgreich sein wollen, im Rahmen dieser Automatisierung und Modernisierung integrierte Technologien für die Sicherheit und Bereitstellung von Anwendungen benötigen, einschließlich fortschrittlicher und anpassungsfähiger Schutzmechanismen, die dabei helfen, die vom Kern bis zum Rand verteilten Anwendungen zu verbinden. Die Reaktionsgeschwindigkeit und die einfache Verwaltung, die mit SaaS-basierten Lösungen möglich sind, können Unternehmen dabei helfen, die digitale Geschwindigkeit mit Kontrolle und Leistung in Einklang zu bringen und Webanwendungen und APIs sowie die Infrastruktur, die diese Anwendungen hostet, zu sichern.

03

# Zeitdruck prägt die Sicherheits-strategien

**DIE ABSICHERUNG DIESER** hybriden und sich schnell modernisierenden digitalen Welt wird immer schwieriger. In einer zunehmend App- und API-gesteuerten Wirtschaft ist es ein strategischer Marathon, Risiken und Chancen abzuwägen, um aufkommende Bedrohungen erfolgreich zu erkennen und zu entschärfen – ohne zusätzliche Reibungsverluste, die Kunden abschrecken. Doch auch Cybersecurity-Aktivitäten müssen im Eiltempo erfolgen, um den sich schnell entwickelnden Angriffen immer einen Schritt voraus zu sein, was sich auf die Sicherheitsstrategien auswirkt. So nannten Unternehmen, die auf SECaaS umsteigen, ein bewährtes Mittel zur schnellen Behebung neuer Angriffe und Schwachstellen, die Geschwindigkeit als wichtigsten Faktor. Diejenigen, die in Sicherheitsfunktionen oder mit SRE- und DevOps-Verantwortung tätig sind, gaben besonders häufig Geschwindigkeit als Motivation an. Natürlich bietet SECaaS auch andere Vorteile, indem es Sicherheitsexperten bereitstellt und gleichzeitig den Betrieb vereinfacht und die Verwaltung erleichtert. Das macht den Mangel an ausreichend qualifizierten Mitarbeitern zu einem weiteren Treiber für die Einführung. Infolgedessen vertrauen immer mehr Unternehmen ihren SaaS-Anbietern, dass sie Sicherheit in kürzester Zeit bereitstellen und aufkommende Bedrohungen schneller und fachkundiger abwehren, als dies intern möglich ist.

Unternehmen, die sich noch selbst um ihre Sicherheit kümmern, bewegen sich. Ihr Fokus zeigt sich in der Einführung von App-Sicherheitstechnologien zwischen dem Beginn der COVID-19-Pandemie und heute:

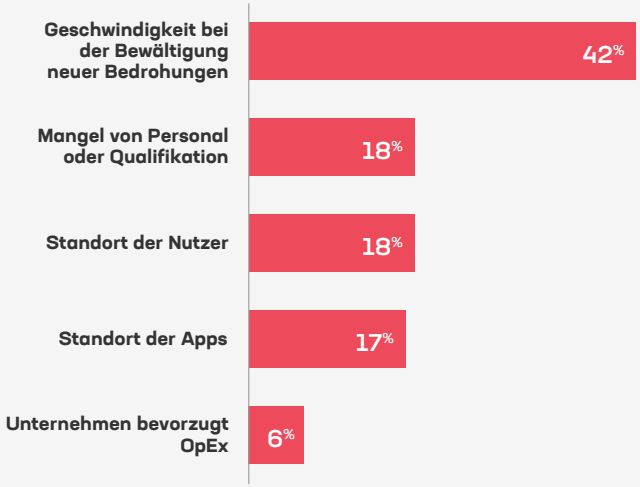
- Die Nutzung von API-Gateways hat sich mehr als verdoppelt, von 35% auf 78% der Befragten.
- Der Einsatz von Diensten für Id-Federation stieg von 52% auf 75%.
- Die Verwendung von Endpunktsicherheit nahm von 65% auf 86% zu.
- Sichere Web-Gateway-Dienste (SWG) kletterten von 61% auf 85%.
- Der Einsatz von WAFs stieg deutlich von 6% auf 82%.

Der zunehmende Einsatz von App-Sicherheitstechnologien spiegelt das wachsende Bewusstsein für ihre wichtige Rolle bei der schnellen Beseitigung von Risiken in einer sich verändernden Bedrohungslandschaft wider.

## SECaaS glänzt mit Geschwindigkeit

**Gefragt wurde:**
Was ist Ihr Hauptgrund für die Verwendung von Security as a Service (WAAP, WAF, DDoS, API-Schutz usw.)? Nur eine Antwort ist erlaubt.

**Das Ergebnis:**
**Hauptmotiv ist schnelle Abwehr von Bedrohungen.**



**Die Unternehmen stürzen sich auf Zero Trust.**

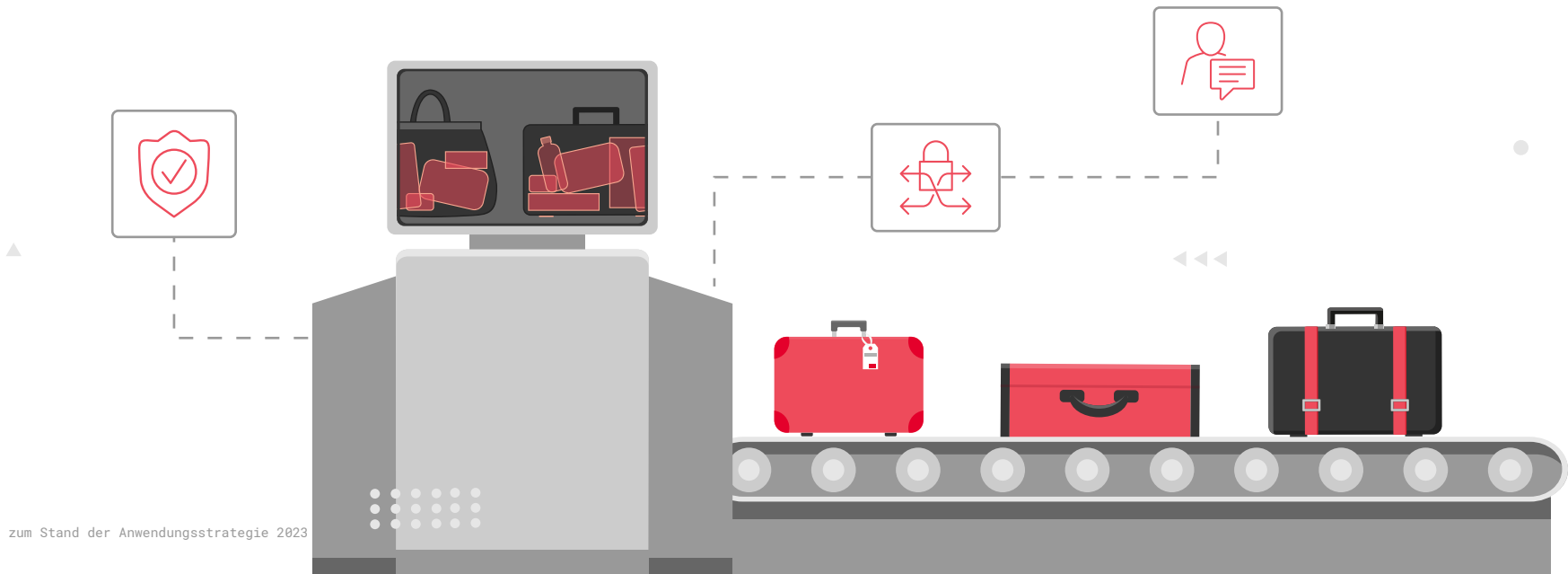
Die Geschwindigkeit ist auch ein Faktor für die Zunahme von Zero-Trust-Sicherheitsmodellen, die verschiedene Architekturen und hybride Bereitstellungen überwinden und den Sicherheitsaspekt von Entwicklungs- und Bereitstellungsprozessen vereinfachen können. Mehr als 80% der Befragten geben an, dass sie Zero-Trust einführen oder dies planen.

# Über 80% der Unternehmen führen Zero Trust ein

Tatsächlich war Zero Trust zusammen mit der Konvergenz von IT- und Betriebstechnologien (IT/OT) als der spannendste globale Trend der nächsten Jahre. Das ist eine Verbesserung gegenüber dem dritten Platz im Jahr 2022. Die kontinuierliche Überprüfung von Zero-Trust-Modellen verhindert unter anderem Session-Attacken und die zwangsweise Nutzung autorisierter Zugriffe für nicht autorisierter Ressourcen. Der Einsatz dieses identitätszentrierten Sicherheitsansatzes kann die Markteinführungszeit für neue Funktionen und Funktionen und Anwendungen verkürzen und Schwachstellen verhindern, die manuell entschärft oder gepatcht werden müssen. Das ist einer der Gründe, warum der Einsatz von IAM-Technologien zugenommen haben.

Die Aussicht auf schnellere Reaktionszeiten treibt auch die Nutzung von KI/ML für die Sicherheit voran. Fast zwei Drittel der Unternehmen planen (41%) oder haben bereits KI-Unterstützung implementiert (23%). Diejenigen, die KI oder ML bereits einsetzen, nennen Sicherheit als primären Use Case und auch bei denjenigen, die noch in der Planung sind, wird Sicherheit als Hauptantrieb genannt. AIOps rangiert an zweiter Stelle.

Auch die Geschwindigkeit motiviert die laufenden Bemühungen um Automatisierung. Der Bedarf ist offensichtlich: Die App-Entwicklung wird damit immer schneller, während Sicherheit und Risikomanagement in der Regel immer noch einen hohen manuellen Aufwand, Überwachung und Eingriffe erfordern. Aber die Unternehmen machen Fortschritte. Im Jahr 2023 rangiert die Netzwerksicherheit nicht weit hinter der Systeminfrastruktur als die am dritthäufigsten automatisierte der sechs IT-Kernfunktionen. Die Netzwerksicherheit wird zunehmend in Servicemodelle verlagert,



## Plattformen und Zero Trust gehen meist Hand in Hand.

Fast neun von zehn Befragten (88%) geben an, dass ihre Unternehmen eine Sicherheitsplattform einführen, was praktisch dem Anteil derjenigen entspricht, die auf ein Zero-Trust-Modell hinarbeiten. Die Trends überschneiden sich. Beide spiegeln die Komplexität der Sicherung einer hybriden Multi-Cloud-Welt wider. Plattformsicherheit entspricht aber auch dem Wunsch, die Verbreitung verschiedener Lösungen und Anbieter zu begrenzen und gleichzeitig konsistente Sicherheit für hybride Infrastrukturen, ältere und moderne Anwendungen und verteilte APIs zu bieten.

Organisationen, die digitale Dienste für externe Nutzer bereitstellen, setzen besonders häufig auf einen Plattformansatz, ebenso wie Unternehmen in Nord- und Südamerika und in der Technologiebranche, möglicherweise weil diese auch eher eine globale Reichweite und Skalierung benötigen.

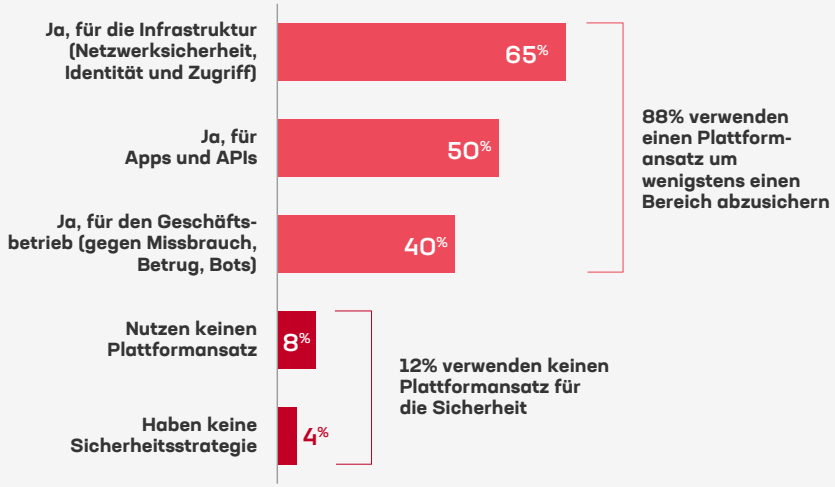
Was die Art der Anwendung betrifft, so wird der Plattformansatz am häufigsten zur Sicherung der Infrastruktur eingesetzt: Fast zwei Drittel (65%) wollen eine Plattform für die Netzwerksicherheit oder das Identitäts- und Zugangsmanagement nutzen. Die Hälfte der Befragten will eine Plattform auch für die Sicherung von Web-Apps und APIs vom Rechenzentrum bis zum Edge einsetzen. Weitere 40% wollen eine Plattform für geschäftliche Sicherheitsanforderungen wie Anti-Bot- und Anti-Fraud-Lösungen.

Unabhängig davon, was genau sie zu schützen hoffen, ist es für die 40% der Befragten, die bei der Auswahl ihrer Sicherheitsplattform einen Ökosystemansatz verfolgen, besonders wichtig, schnell auf neue Bedrohungen reagieren zu können. Der Ökosystem-Ansatz (z. B. die Nutzung der Partner-Marktplätze eines öffentlichen Cloud-Anbieters) bietet zwei Vorteile. Erstens können Unternehmen durch die Auswahl unter mehreren Anbietern die effizienteste Lösung wählen, die mit dem Ökosystem kompatibel ist. Zweitens verkürzt das Wissen, dass Public-Cloud-Anbieter auf grundlegende Integrationen für Dritte im Ökosystem bestehen, die Zeit bis zur Wertschöpfung für Sicherheitslösungen.

## Sicherheitsplattformen zielen vor allem auf die Infrastruktur ab

**Gefragt wurde:**
Verfolgen Sie bei Ihrer Sicherheitsstrategie einen Plattformansatz? Mehrfachantworten sind erlaubt.

**Das Ergebnis:**
**Fast 90% setzen auf einen Plattformansatz und viele planen die Nutzung einer Plattform zur Sicherung von mehr als einem Bereich.**



Interessanterweise tendieren vor allem leitende IT-Manager zu einem Ökosystemansatz. SecOps-Teams hingegen bevorzugen Sicherheitsplattformen eines einzigen Anbieters. Das ist wahrscheinlich darauf zurückzuführen, dass sich die höheren Ebenen des Unternehmens der Kosten der Fragmentierung der IT-Funktionen stärker bewusst sind.

### Sicherheit ist der primäre Workload am Edge.

Von allen Unternehmen, die Workloads für den Edge-Bereich planen, erwartet die Hälfte, dass sie dort Sicherheits-Workloads platzieren. Aber fast zwei Drittel der Befragten, die derzeit Zero-Trust-Strategien verfolgen, planen die Bereitstellung von Sicherheits-Workloads am Edge, da sie erkannt haben, dass die vollständige Umsetzung von Zero-Trust – und die Erzielung der vollen Vorteile – die Nutzung des Edge zur Sicherung jedes Endpunkts voraussetzt.

Während Sicherheitsdienste der wichtigste Edge-Anwendungsfall sind, wächst die Edge-Arbeitslast seit 2022 am schnellsten beim Monitoring. Dies ist wahrscheinlich auf mehrere Faktoren zurückzuführen: die explo-

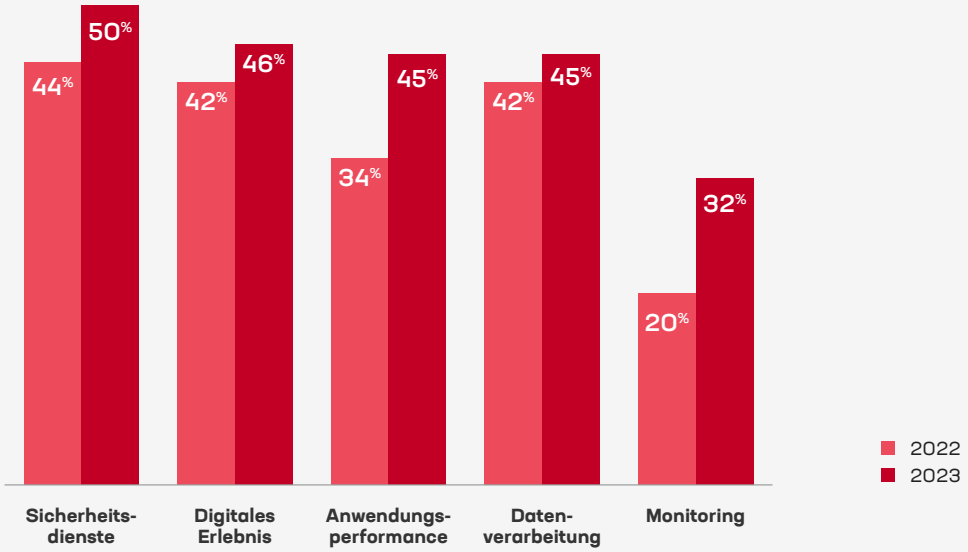
## Monitoring-Workloads legen am Edge kräftig zu

sionsartige Zunahme von Remote-Work, IoT-Anwendungen die Tendenz zur weiten Verbreitung von Anwendungen, die globale die globale Reichweite der heutigen Märkte und die Begeisterung über die IT/OT-Konvergenz, die auf Echtzeitdaten angewiesen sein wird, um Prozessanpassungen vorzunehmen..

### Sicherheit ist der vorrangige Workload am Edge

**Gefragt wurde:**
Welche Workloads sind bei Ihnen am Edge geplant? Mehrfachantworten möglich.

**Das Ergebnis:**
**Sicherheit stellt den wichtigsten Workload dar, aber Monitoring hat das größte Wachstum.**



## Immer mehr Organisationen benötigen einen sicheren Lebenszyklus für ihre Softwareentwicklung.

Starke Sicherheit beginnt jedoch lange vor der Bereitstellung, unabhängig davon, wo diese Arbeitslasten gehostet werden. Dementsprechend haben drei Viertel (75%) der Befragten einen sicheren Softwareentwicklungs-Lebenszyklus (SDLC) eingeführt oder planen ihn zumindest. Dieses Ergebnis zeigt, dass Sicherheit und Risikomanagement keine einmalige Angelegenheit sind, die nur auf der Ebene der Infrastruktur oder der Anwendungsbereitstellung stattfinden kann. Vielmehr erfordert ein umfassender und konsistenter Schutz mehrere, koordinierte Anstrengungen über einen längeren Zeitraum und über IT- und Unternehmensrollen hinweg.

Die Minderheit der Unternehmen, die sich noch keine Gedanken über den SDLC gemacht hat, ist jedoch besser dran als die 4% der Umfrageteilnehmer, die angaben, überhaupt keine Sicherheitsstrategie zu haben – weder für Software noch für das Unternehmen. Au weia!

Glücklicherweise sind die meisten Unternehmen proaktiver und suchen im Vorfeld nach Möglichkeiten, alle möglichen Risiken zu minimieren. Bedenken hinsichtlich der Sicherheit der Software-Lieferkette beispielsweise werden auf verschiedene Weise angegangen.

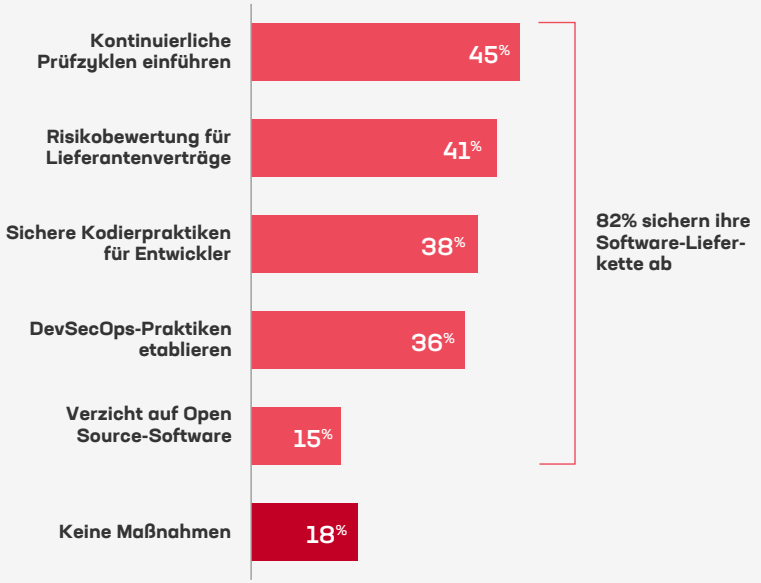
Der beliebteste Ansatz ist die Einführung eines kontinuierlichen Prüfzyklus. Mehr als ein Drittel der Unternehmen (36%) baut eine DevSecOps-Praxis auf. Etwa ein weiteres Drittel (38%) schult Entwickler in sicheren Kodierungspraktiken.

Es überrascht vielleicht nicht, dass Unternehmen in der Finanzdienstleistungs- und Gesundheitsbranche sich am ehesten mit der Sicherheit der Software-Lieferkette befassen. Fast jedes fünfte Unternehmen (18%) macht sich offenbar keine Gedanken über die Sicherheit der Software-Lieferkette und plant auch keine entsprechenden Maßnahmen.

### Software Remains a Security Risk

**Gefragt wurde:**
Wie sichert Ihr Unternehmen seine Software-Lieferkette ab? Mehrfachantworten sind erlaubt

**Das Ergebnis:**
**Während die meisten zumindest einen Ansatz verfolgen, bleibt die Software-Lieferkette für fast ein Fünftel der Befragten eine offenes Flanke.**



# Erkenntnisse von F5

In der heutigen hybriden Welt ist es schwieriger denn je, Unternehmen zu sichern und die Implementierung konsistenter Sicherheitsrichtlinien ist besonders schwierig – aber auch der Schlüssel zu mehr Geschwindigkeit, Agilität und Resilienz. Während Zero-Trust-Strategien zunehmend mit Netzwerk- oder Infrastruktursicherheit in Verbindung gebracht werden, gelten Identitätsmanagement-Technologien – einschließlich der Verwendung von Authentifizierung und Autorisierung für API-Sicherheit – nach wie vor als die wertvollsten Ansätze zur Sicherung von Anwendungen.

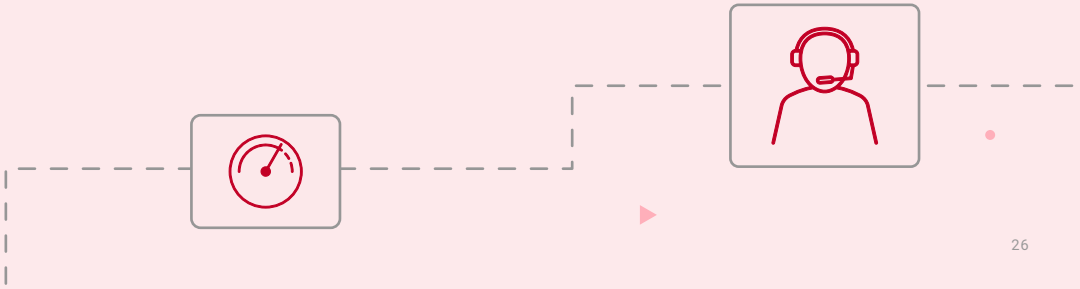
Um diese Apps zu unterstützen, sind Sicherheits- und Identitätstechnologien diejenigen Dienste, die am ehesten sowohl lokal als auch in der Cloud eingesetzt werden. Dies gilt auch zunehmend für den Edge, da Unternehmen das dortige Potenzial verstärkt nutzen. Wir gehen davon aus, dass der Unterschied zwischen den Bereitstellungsraten in den verschiedenen Umgebungen weiter schrumpfen wird, auch wenn der Anteil der Sicherheitsaufgaben am Edge zunimmt, da App- und Sicherheitstechnologien überall dort erforderlich sind, wo Anwendungen und APIs bereitgestellt werden.

### Was das für Sie bedeutet

Sicherheit kann zu einem digitalen Unterscheidungsmerkmal werden, das es App-Entwicklungsteams ermöglicht, das Innovationstempo zu erhöhen, ohne dass mehr Risiko oder der Reibungsverluste bei den IT-Funktionen entsteht. Zero-Trust-Modelle, Identitätsmanagement, sichere Softwareentwicklung und weitere Sicherheitsstrategien können und sollten nebeneinander existieren. Unternehmen tun gut daran, das Prinzip von Zero Trust auf die Tools in ihrer Softwareentwicklungspipeline auszuweiten. Um hochmotivierte Angreifer abzuwehren, müssen Unternehmen nicht nur Türen und Fenster, sondern auch den Schornstein und sogar den Briefschlitz schützen. Deshalb sollten Sicherheitsprozesse wie SDLC umgesetzt werden. Nur wenn alle möglichen Schwachstellen bedacht werden, können IT-Verantwortliche Daten, Kunden und das Unternehmen schützen.

Ein Beispiel für dieses Denken ist die Ausweitung der API-Sicherheit über ihre traditionelle Verwendung im Datenpfad hinaus. Die interessantesten API-Sicherheitslösungen betreffen dabei den Ost-West-Datenverkehr, beispielsweise über einen POST-Agenten. Dieser kreative Ansatz kann Unternehmen einen Vorsprung vor Angreifern verschaffen und IT-Ressourcen von der manuellen Schadensbegrenzung befreien, so dass stattdessen das Geschäft beschleunigt wird. Darüber hinaus sind Apps und ihre API-Fabrics nur so sicher wie die Infrastruktur, auf der sie entwickelt, bereitgestellt und betrieben werden. Der einfachste Weg, einen Komplettschutz zu erhalten, der Ausfallsicherheit und Agilität bietet, ist die Verwendung von umgebungsunabhängigen Lösungen, Nutzungsmodellen und Anbietern, die sowohl Anwendungen als auch die Infrastruktur überall schützen. SECaaS ist eine Option, die besonders Unternehmen mit dringendem Bedarf an Schutzmaßnahmen, begrenzter interner Sicherheitsexpertise oder der Bevorzugung von Betriebsausgaben gegenüber Kapitalkosten nützen können.

Die Fähigkeit, einheitliche Sicherheitsrichtlinien für jede Anwendung und jede API überall zu implementieren, ist wichtig. Sicherheitsplattformen, einschließlich SaaS-basierter Dienste, können dabei helfen, hybride Anwendungen und APIs über alle Host-Umgebungen hinweg zu sichern, vom Kern bis zum Edge, mit konsistenten Richtlinien, umfassender Transparenz und vereinfachter Verwaltung. Diese Art von Ansatz schützt sowohl moderne als auch traditionelle Architekturen und hybride Anwendungen mit WAF, DDoS-Schutz und Bot-Abwehr, die mit verhaltensbasiertem Eindringungsschutz und Angriffsabwehr für den gesamten Sicherheitsstapel integriert sind. Eine solche effektive Sicherheit, die mit der Geschwindigkeit des Unternehmens arbeitet, schützt das, was am wichtigsten ist, und setzt gleichzeitig das Wachstumspotenzial des Unternehmens frei.



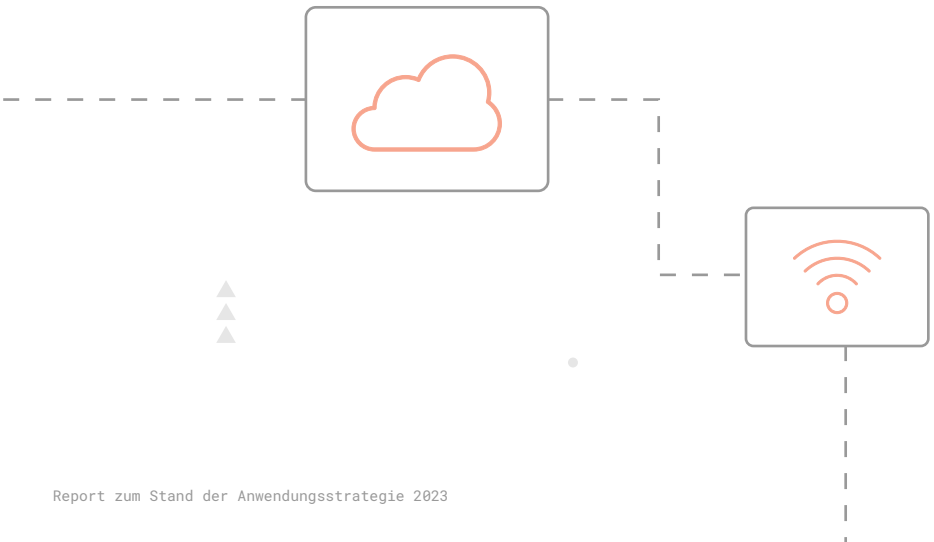
Fazit

# Es gibt Hoffnung für überlastete IT-Teams

**MIT ZUNEHMENDER MODERNISIERUNG** der App-Portfolios werden Unternehmen ihre Bereitstellungsarchitekturen immer weiter anpassen, um betriebliche und Marktanforderungen auszubalancieren und die richtige Verteilung zwischen lokaler, Cloud- und Edge-Umgebungen sowie der Nutzung von SaaS zu finden. Auch wenn sie dabei vieles konsolidieren, wird die große Mehrheit auf unbestimmte Zeit hybride und Multi-Cloud-Modelle nutzen.

Das gründet sich auf dem Tempo des technologischen Wandels, der Folgen technischer Schulden sowie der Tatsache, dass die meisten Unternehmen mit mehreren Technologiegenerationen jonglieren müssen. Diese Technologien können sich gegenseitig überholen, so wie Mobiltelefone Märkte erobert haben, in denen es nur wenige oder gar keine Festnetzanschlüsse gab, aber mehrere Paradigmen werden nebeneinander existieren.

Vielleicht wichtiger: hybride Modelle bieten die größte Flexibilität für Bereitstellungsentscheidungen, die im Allgemeinen pro Anwendung auf der Grundlage App-spezifischer Bedürfnisse, Vorteile und Ziele getroffen werden. Angesichts des Wettbewerbsdrucks bei der Markteinführung und der Bedeutung der Kundenzufriedenheit werden sich die meisten Unternehmen weiterhin für Agilität, Geschwindigkeit und die Möglichkeit zur Optimierung digitaler Erlebnisse entscheiden. Moderne Apps und Microservices erlauben die notwendigen Verbindungen, z. B. zwischen traditionellen, monolithischen Apps im Kern des Unternehmens und mobilen APIs.



Infolgedessen werden die Herausforderungen mehrerer Clouds, verteilter Bereitstellungen und hybrider IT-Stacks in der einen oder anderen Form fortbestehen. Es gibt jedoch Hoffnung für überlastete IT-Teams. Mehr Automatisierung, eine konsistente Sicherheitsebene mit deklarativen Bereitstellungsrichtlinien, KI/ML im IT-Betrieb und standardisierte Methoden wie SRE können Unternehmen dabei helfen, die Komplexität zu überwinden und die Geschäftsgeschwindigkeit zu erhöhen. Die kontinuierliche Zunahme der Echtzeitüberwachung am Edge sowie Lösungen, die diese Telemetrie verwertbar machen, können die AIOps unterstützen, die die manuelle Verwaltung reduzieren. Zero-Trust-Sicherheitsansätze und übergreifende Plattformen können Anwendungen und APIs überall dort verbinden und schützen, wo sie eingesetzt werden, ebenso wie die Infrastruktur, die sie unterstützt. Abstraktionsschichten, wie sie von App-Sicherheits- und Bereitstellungstechnologien verwendet werden, können Grenzen überschreiten und einen Nexus für eine zentralere und so vereinfachte Verbindung und Kontrolle bieten.

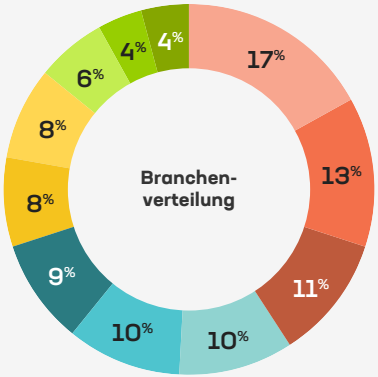
## Die meisten Unternehmen werden auf unbestimmte Zeit hybride Modelle nutzen.

Da kein Unternehmen über das nötige Fachwissen verfügt, um all dies allein zu bewältigen, können Geschäftspartner, die sich in der hybriden Welt auskennen und dort erfolgreich sind, einen erheblichen Mehrwert bieten. Insbesondere Technologieanbieter wie F5 können dazu beitragen, die Komplexität zu vereinfachen, um umfassenden Schutz und konsistente Leistung zu bieten. Der richtige Partner kann Sie bei der Bereitstellung und dem Schutz moderner und traditioneller Anwendungen unterstützen, die über hybride IT-Stacks mit einer Vielzahl von Nutzungsmodellen, einschließlich SaaS, verteilt sind. Gemeinsam können wir das das hybride Leben, das wir alle führen, einfacher, sicherer und lohnender machen.

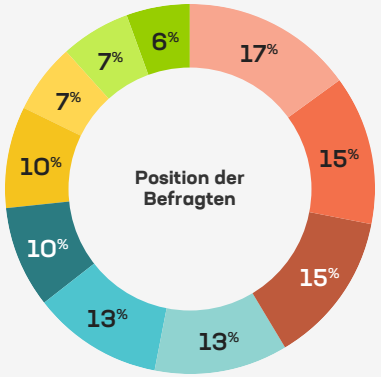
## Über diesen Report

Mehr als 1.000 IT-Entscheidungsträger aus der ganzen Welt teilten F5 in der diesjährigen Umfrage ihre Prioritäten und Anliegen mit. Die APCJ-Region war in diesem Jahr besonders gut vertreten. Wie immer repräsentierten die Befragten eine breite Mischung von Branchen, wobei der Regierungssektor stärker als in der Vergangenheit stärker vertreten als in der Vergangenheit und Technologieunternehmen etwas weniger stark vertreten.

Die Daten wurden von Personen in einem breiten Spektrum von IT- und Führungspositionen zur Verfügung gestellt, von der Chefetage bis hin zu dem Personal der App-Entwicklung, mit einem größeren Anteil von Product Ownern von Business-Apps als in den Vorjahren. F5 bedankt sich bei allen, die sich die Zeit genommen haben, ihre Aktivitäten, Interessen und Erkenntnisse über die digitale Transformation mitzuteilen




- Technologie
- Finanzdienstleistung
- Fertigung und Ressourcen
- Vertrieb und Dienstleistungen, einschließlich Groß- und Einzelhandel, Transport und Medien
- Regierung / Öffentlicher Sektor
- Cloud Service Provider
- Telekommunikation
- Bildung
- Andere
- Gesundheitswesen
- Energie und Versorgung




- IT-Leiter
- Netzwerkspezialist
- Data Scientist
- Operations
- Andere
- Sicherheit
- Betriebsleiter
- Inhaber einer Business- oder Tech-App
- Cloud- oder Enterprise-Architekt
- Site Reliability Engineer (SRE), Entwickler, DevOps oder DevOps-Manager

## Über F5

F5 ist ein Multi-Cloud-Anwendungsservice- und Sicherheitsunternehmen, das sich dafür einsetzt, eine bessere digitale Welt zu ermöglichen. F5 arbeitet mit den größten und zukunftsweisenden Unternehmen der Welt zusammen, um Anwendungen und APIs überall zu sichern und zu optimieren – vor Ort, in der Cloud oder am Edge. F5 ermöglicht es Unternehmen, ihren Kunden außergewöhnliche, sichere digitale Erlebnisse zu bieten und Bedrohungen stets einen Schritt voraus zu sein. Weitere Informationen unter f5.com. (NASDAQ: FFIV).