



sonio.

Mehr Clouds. Mehr Freiheit.

Und wer betreibt das alles?
Hybrid Cloud als Betriebsmodell –
was Consumer gewinnen und was
Betreiber schultern müssen.

Cloud beginnt nicht beim Rechenzentrum.

Nicht jede virtualisierte Umgebung ist eine Cloud. Entscheidend sind Automatisierung, Skalierbarkeit, Transparenz und Governance.

Bevor wir über Hybrid Cloud sprechen, braucht es eine ehrliche Antwort auf eine einfache Frage: Was ist Cloud überhaupt? Die Antwort ist weniger selbstverständlich, als viele denken.

Wir orientieren uns an NIST SP 800-145 – der international anerkannten Definition.

Die Konsequenz: Virtualisierung ist eine Grundlage, keine Cloud. Wer Ressourcen noch immer manuell bereitstellt, manuell skaliert und manuell abrechnet, betreibt keine Cloud – auch wenn er das Label verwendet. Und wer Cloud sagt, aber neue VMs per Ticket anfordert, meint damit eigentlich: virtualisiertes Rechenzentrum mit modernem Namen.

Hybrid Cloud, Multi Cloud, Trusted Cloud – was ist was?

NIST unterscheidet vier Deployment-Modelle: Eine – Private Cloud – wird exklusiv für eine Organisation betrieben, entweder intern oder durch Dritte. Eine Community Cloud teilt die Infrastruktur zwischen Organisationen mit gemeinsamen Anforderungen (z. B. Behörden oder Forschungseinrichtungen). Eine Public Cloud stellt Services einer breiten Öffentlichkeit über das Internet zur Verfügung.

Hybrid Cloud schliesslich verbindet mindestens zwei dieser eigenständigen Cloud-Infrastrukturen so, dass Daten oder Anwendungen zwischen ihnen portierbar werden. Das setzt Integration, Standards und

Fünf Merkmale machen eine Cloud aus:

NIST-MERKMAL	WAS DAS KONKRET BEDEUTET
On-Demand Self-Service	Ressourcen auf Abruf – kein Ticket, kein Warten, kein manueller Prozess.
Broad Network Access	Services über standardisierte Netzwerkmechanismen erreichbar – nicht zwingend über das Internet.
Resource Pooling	Ressourcen dynamisch aus gemeinsamen Pools zugeteilt.
Rapid Elasticity	Kapazität automatisch skalierbar – nach oben und nach unten.
Measured Service	Nutzung wird gemessen, transparent gemacht und abgerechnet.

Quelle: NIST SP 800-145, The NIST Definition of Cloud Computing

gemeinsame Governance voraus. Dieses White Paper fokussiert auf Private, Public und Hybrid Cloud – die für Unternehmen in der Praxis relevantesten Modelle.

Multi Cloud ist ein Marktbegriff für die Nutzung mehrerer Cloud-Provider. Entscheidend: Multi Cloud bedeutet nicht automatisch Integration. Sie entsteht oft ungeplant – durch Teams, Akquisitionen, Einzelentscheidungen. Mehrere Plattformen zu nutzen ist kein Betriebsmodell. Beherrschen ist es.

„ Cloud ist kein Ort. Cloud ist die Art, wie IT bereitgestellt und betrieben wird.

Trusted Cloud bezeichnet Cloud-Services, bei denen neben der Technik auch Rechtsraum, Datenhaltung, Betriebsverantwortung, Subprozessoren, Security, Transparenz und Exit-Optionen nachvollziehbar kontrolliert werden können. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) hat diesen Begriff als Qualitätsmerkmal für sichere, souveräne Cloud-Dienste geprägt (<https://trusted-cloud.de/ueber-trusted-cloud.html>). Die Sonio Cloud ist eine konkrete Ausprägung davon.

CLOUD IST KEIN ORT.

Broad Network Access bedeutet Netzwerkzugriff – nicht zwingend Internet. Eine Private Cloud kann vollständig im eigenen Rechenzentrum betrieben werden und trotzdem alle fünf Merkmale erfüllen.

ZUSAMMENFASSUNG

Hybrid Cloud verspricht Wahlfreiheit – die Freiheit, Workloads dorthin zu platzieren, wo sie am besten aufgehoben sind, und Ressourcen schneller bereitzustellen, als es klassische Infrastruktur erlaubt. Was viele Unternehmen in der Praxis bekommen: mehr Plattformen, mehr Regeln, mehr Betriebsaufwand – und am Ende neue Silos, die sich nur anders nennen.

Die Kernaussage ist so einfach wie unbequem: Für den Consumer kann Hybrid Cloud das Leben tatsächlich einfacher machen. Für den Betreiber wird es deutlich anspruchsvoller. Druck kommt von zwei Seiten gleichzeitig: Consumer verlangen mehr Einfachheit, mehr Geschwindigkeit, neue Services wie AI. Gleichzeitig verschlimmert sich die Bedrohungslage und verlangt schnellere Reaktionen, mehr Kontrolle, höhere Sicherheit.

Dieses White Paper klärt, was Cloud nach NIST wirklich bedeutet, wo die Komplexität bei Hybrid Cloud bleibt, welche Rolle AI, Kubernetes und Security spielen – und mit welchen organisatorischen Fähigkeiten und Betriebsmodellen Unternehmen das tatsächlich beherrschen können.

Einfach vorne. Komplex dahinter.

Hybrid Cloud versteckt Komplexität für den Consumer. Für die IT steigen die Anforderungen an Plattform, Automation, Security und Betrieb.

Der Consumer will keine Cluster, kein VLAN, keine Storage-Klasse. Er will einen Service. Schnell, sicher, ohne Ticket. Das ist die versprochene Welt der Hybrid Cloud. Diese Einfachheit für den Consumer hat einen Preis – und der liegt nicht auf seiner Seite. Portale, APIs und automatisierte Workflows verstecken die technische Komplexität. Dahinter muss sie jemand beherrschen: die IT-Organisation, ein Managed-Service-Partner oder eine Kombination aus beidem. Compute, Storage, Netzwerk, Identity, Security, Kosten, Lifecycle, Compliance – all das verschwindet nicht. Es wird Teil einer Plattform. Und diese Plattform muss jemand bauen, betreiben, absichern und weiterentwickeln.

» Hybrid Cloud ist dann gut, wenn der Consumer nicht wissen muss, wo sein Service läuft. Die Komplexität gehört in die Plattform – nicht zum Consumer. Sonio AG, Hybrid Cloud Praxis

Frage: Wer ist das in Ihrer Organisation? 73% der von Flexera 2026 befragten Organisationen nutzen Hybrid Cloud, 88% arbeiten mit mehreren Providern

(Flexera, [State of the Cloud Report 2026](#)). Die Frage lautet längst nicht mehr, ob Unternehmen mehrere Plattformen nutzen. Die Frage ist, ob sie diese wirklich beherrschen – oder ob sie einfach gewachsen sind.

Platform Engineering: Was dahintersteckt

Platform Engineering ist der Versuch, Komplexität in wiederverwendbare, standardisierte Services zu übersetzen. Ein Portal vor manuellen Prozessen ist kein Self-Service. Es ist Ticket-IT mit schöner Oberfläche. Echte Plattformen automatisieren den gesamten Lifecycle – Bereitstellung, Betrieb, Skalierung, Lifecycle-Management, Recovery. Wer das nicht kann, hat noch keine Cloud. Er hat eine Hoffnung auf Cloud.

DIE REALITÄT.

Für den Consumer: Portal öffnen, Service beziehen, fertig. Kein Ticket, keine Wartezeit.
Für den Betreiber: Die Anforderungen an Plattform, Automation, Security, Governance und Betrieb steigen erheblich. Cloud macht IT nicht einfacher. Sie macht sie anspruchsvoller.

Kontrolle entsteht nicht von selbst.

Hybrid Cloud braucht klare Leitplanken für Governance, Souveränität, Kosten und Exit – über alle Plattformen hinweg.

Mehrere Plattformen zu betreiben, bedeutet nicht automatisch, sie auch zu beherrschen. Governance beginnt nicht bei einem Regelwerk – sondern bei gemeinsamen Leitplanken, die für alle Plattformen gelten: Identity, Security, Logging, Backup, Datenklassifikation, Kosten, Verantwortlichkeiten. Wer diese Leitplanken pro Plattform separat erfindet, baut keine Hybrid Cloud. Er baut mehrere unabhängige Silos.

Datensouveränität: Der Serverstandort allein genügt nicht

Ein Schweizer Rechenzentrum klingt nach Sicherheit. Ist es aber nicht automatisch. Entscheidend sind Rechtsraum, Verschlüsselung, Subprozessoren und

die Frage, wer im Ernstfall Kontrolle ausüben kann. Die Schweizer Datenschutzkonferenz privatim hält in ihrer Resolution vom November 2025 fest: Der US Cloud Act kann auch Daten in Schweizer Rechenzentren betreffen – wenn der Anbieter US-amerikanischem Recht unterliegt (privatim.ch, Resolution zu internationalen Cloud-Lösungen, 24. November 2025). Der Serverstandort ist irrelevant. Die Rechtsarchitektur ist es nicht. Für regulierte Branchen wie Finanz, Pharma oder öffentliche Hand ist das keine abstrakte Datenschutzdiskussion. Es ist eine Compliance-Anforderung, die direkt in die Wahl des Cloud-Modells einfließt.

FinOps: Von Cloud-Kosten zu Technology Value

Die Frage «ist Public Cloud günstiger als eigenes Rechenzentrum?» ist 2026 die falsche Frage. FinOps entwickelt sich von reinem Cloud-Kostenmanagement zu «Technology Value»: 98% der FinOps-Praktiker managen bereits AI-Ausgaben, 57% Private Cloud und 48% Datacenter-Kosten (FinOps Foundation, State of FinOps 2026: data.finops.org). Was zählt: Welche Plattform liefert für diesen Workload den besten Wert – bei Kosten, Risiko, Performance, Souveränität und Betriebsaufwand zusammen?

EINE WICHTIGE FRAGE VOR JEDEM CLOUD-EINSTIEG.

Wie kommen wir wieder heraus?

Eine Exit-Strategie gehört an den Anfang einer Cloud-Entscheidung, nicht ans Ende. Daten, Konfigurationen, Identitäten, Schnittstellen und Betriebswissen müssen portierbar bleiben – sonst kauft man nicht Cloud, sondern Abhängigkeit.



Neue Workloads. Gleiche Grundfrage.

AI und Kubernetes verändern die Anforderungen an Hybrid Cloud – nicht ihre Grundprinzipien.

Wer glaubt, Hybrid Cloud sei eine rein infrastrukturelle Übung, unterschlägt zwei Entwicklungen, die den Anspruch fundamental verändern.

Kubernetes hat sich zur standardisierten Betriebssystemschicht für moderne Anwendungen entwickelt. Gemäss CNCF Annual Cloud Native Survey 2025 setzen 82% der Container-Nutzer Kubernetes produktiv ein; 66% der Organisationen, die generative AI-Modelle hosten, nutzen Kubernetes für Inference-Workloads. Kubernetes ist dabei in sich schon Multi Cloud – Microservices werden aus verschiedenen Quellen bezogen, Infrastrukturgrenzen verschwimmen.

AI-Infrastruktur folgt denselben Grundsätzen wie jede andere Infrastruktur: Wo sollen Daten, Modelle und GPU-Ressourcen laufen? Die Antwort hängt von Workload, Latenz, Kosten, Security und Datensouveränität ab – denselben Kriterien, die für jeden anderen Workload gelten. Was auf CPU-Ebene gilt,

gilt auf GPU-Ebene genauso.

Daraus folgt: Eine Hybrid-Cloud-Architektur, die nicht auch AI- und Container-Workloads aufnehmen kann, ist keine zukunftsfähige Hybrid-Cloud-Architektur. Sie ist der vorletzte Stand.

DER NÄCHSTE FEHLER IST VORHERSEHBAR.

Wer AI als isolierte Spezialplattform aufbaut, wiederholt exakt den Fehler, den Hybrid Cloud lösen soll: ein neues Silo, eigene Infrastruktur, eigene Governance, eigener Betrieb. AI Readiness beginnt nicht beim AI-Tool. Sie beginnt bei der Fähigkeit, Plattform, Daten, Security und Lifecycle gemeinsam zu betreiben.

Security muss schneller sein als der Angriff.

Automatisierung, Standardisierung und zentrale Kontrolle werden zur Sicherheitsanforderung – über Cloud, Kubernetes und AI hinweg.

AI beschleunigt nicht nur Unternehmensprozesse. Sie beschleunigt auch Angriffe. Während Organisationen AI nutzen, um effizienter zu werden, nutzen Angreifer dieselbe Technologie, um Angriffsflächen schneller zu identifizieren, Schwachstellen automatisiert auszunutzen und Kampagnen zu skalieren. Der Druck kommt von beiden Seiten gleichzeitig: Das Business verlangt Geschwindigkeit. Die Bedrohungslage lässt immer weniger Zeit für Reaktion.

Das BACS erhielt im zweiten Halbjahr 2025 über 29'000 Meldungen und 145 meldepflichtige Cyberfälle (BACS, [Halbjahresbericht 2025/2](#)). Ransomware bleibt dominant.

DER SECURITY-TEST.

Wenn eine kritische Schwachstelle schneller ausgenutzt wird, als Ihr Change-Prozess den Patch ausrollen kann, haben Sie nicht nur ein Patch-Problem. Zuerst ist es ein organisatorisches Problem – zu langsame Prozesse, zu wenig Automation, zu viele manuelle Hürden. Und dieses organisatorische Problem hat eine direkte architektonische Konsequenz: Eine Plattform, die Patches nicht schnell und kontrolliert ausrollen kann, ist keine sichere Plattform.

INSTANT PATCHING ALS PLATTFORMANFORDERUNG.

Kritische Patches müssen durch standardisierte, automatisierte und getestete Prozesse schnell ausrollbar – und ebenso schnell zurückrollbar sein. Rollout und Rollback sind Plattformfähigkeiten. Wer sie als Sonderprojekte behandelt, hat die Architekturanforderung noch nicht verstanden.

Phishing, Identitätsmissbrauch und Angriffe auf Software-Lieferketten werden gezielter und komplexer. Die entscheidende Veränderung ist nicht die Zahl der Angriffe – es ist ihre Geschwindigkeit.

Security-Produkte plattformweise aufzusetzen, löst das nicht. Wer Private Cloud, Public Cloud, Kubernetes und AI separat absichert, betreibt mehrere Sicherheitsmodelle ohne gemeinsame Sicht.

Security muss Teil der Plattformarchitektur sein: standardisierte Baselines, minimale Rechte, Segmentierung, Policy-as-Code, zentrale Telemetrie und getestete Recovery.

” Wenn der Patch langsamer ist als der Angriff, ist nicht nur die Technik zu langsam. Sonio AG, Hybrid Cloud Praxis

Je einheitlicher eine Plattform aufgebaut ist, desto schneller lassen sich Schwachstellen bewerten,

Policies durchsetzen und Abweichungen erkennen. Standardisierung ist nicht nur Effizienz – sie ist Security-Kontrolle.

AI-Agenten sind eine neue Kategorie: nicht einfach ein weiteres Tool, sondern digitale Identitäten mit Handlungsmacht. Wer lesen, entscheiden und über APIs handeln darf, muss begrenzt, überwacht und bei kritischen Aktionen kontrollierbar sein. OWASP dokumentiert reale Vorfälle. NIST hält fest: bewährte Cybersecurity-Prinzipien gelten weiter – müssen für autonome Agenten aber konsequent erweitert werden.

Drei Ebenen der Bedrohung, auf die Plattformarchitekturen ausgelegt sein müssen:

PRIORITÄT	BEDROHUNG	WAS DIE PLATTFORM KÖNNEN MUSS
Kritisch	Schwachstellen, gestohlene Identitäten, Ransomware	Standardisierte Baselines, Instant Patching, minimale Rechte, Segmentierung, getestete Recovery
Komplex	APIs, Cloud-Konfigurationen, Software- und AI-Supply-Chain	Policy-as-Code, Abhängigkeitstransparenz, zentrale Telemetrie, Detection und Response
Emerging	Prompt Injection, Agent Hijacking, Privilegienmissbrauch durch AI-Agenten	Eigene Agent-Identitäten, begrenzte Rechte, Approval Gates, kontinuierliches Testing

Quellen: BACS Halbjahresbericht 2025/2; OWASP GenAI Exploit Round-up Q1 2026; NIST, Security Considerations for AI Agents, Mai 2026



Der Workload entscheidet.

Nicht jede Anwendung gehört in dieselbe Cloud.

Es gibt keine universell beste Cloud. Ein globaler Webservice hat andere Anforderungen als eine Kernapplikation mit Compliance-Pflichten, ein GPU-Cluster für AI oder ein Archivierungssystem mit langen Aufbewahrungsfristen. Wer die Cloud-Entscheidung vor der Workload-Analyse trifft, trifft sie falsch – und zahlt das später in Form von Egress-Kosten, Migrationsaufwand oder Lock-in.

„Nicht Cloud First entscheidet richtig. Sondern Workload First.“

Sonio AG, Hybrid Cloud Praxis

EINE VM LÄSST SICH VERSCHIEBEN. EINE ANWENDUNG NICHT AUTOMATISCH.

Applikationen hängen an Datenbanken, Latenzen, Schnittstellen, Lizenzen, Identitäten und Betriebsprozessen. Wer diese Abhängigkeiten nicht kennt, trifft Cloud-Entscheidungen im Blindflug – und merkt das erst, wenn die Migration doppelt so viel kostet wie geplant.

Sechs Fragen, die vor jeder Workload-Entscheidung beantwortet sein müssen:

- **Daten und Compliance:** Welche Daten werden verarbeitet? Welche Regeln gelten – revDSG, FINMA, DSGVO, Branchen-spezifisches?
- **Abhängigkeiten:** Welche technischen und organisatorischen Verknüpfungen bestehen? Was läuft auf welchem Hypervisor?
- **Performance und Verfügbarkeit:** Welche SLAs sind nötig – und können sie gemessen und belegt werden?
- **Vollkosten:** Betrieb, Lizenzen, Migration, Egress, Menschen – über fünf Jahre gerechnet, nicht über drei Monate.
- **Exit:** Wie kommen wir wieder heraus – technisch, vertraglich, operativ?
- **Betriebsfähigkeit:** Hat die eigene Organisation die Kompetenzen, um diesen Betrieb langfristig zu leisten?

Wer diese Fragen beantworten kann, ist vorbereitet. Wer stockt, hat seinen Handlungsbedarf gefunden.

Für die Workload-Platzierung arbeiten wir mit drei Bezugsformen – keine alternative NIST-Taxonomie, sondern eine praxisorientierte Einordnung:

PRIVATE CLOUD	TRUSTED CLOUD	PUBLIC CLOUD
Maximale Kontrolle und Integration.	Cloud-Eigenschaften plus nachvollziehbarer Rechtsraum und Managed Service.	Breite Plattformservices und globale Skalierung.
Eng gekoppelte, stabile oder regulierte Workloads.	Wenn Souveränität und Betriebsentlastung zusammenkommen sollen.	Cloud-native Anwendungen, Analytics und variable Last.
Betrieb bleibt anspruchsvoll: Automation, Security und Lifecycle-Management nötig.	Vertrauen entsteht aus Rechtsraum, Verantwortung, Transparenz, Security und Exit – nicht nur aus dem Serverstandort.	Governance, FinOps und Provider-Abhängigkeit müssen aktiv gesteuert werden.

Hinweis: Broadcom, Hyperscaler-Kosten und Cloud Act sind Kontextfaktoren, keine Cloud-Strategie. Hersteller können wechseln. Die Frage nach dem richtigen Betriebsmodell bleibt.



Technik allein reicht nicht.

Hybrid Cloud braucht passende Prozesse, Kompetenzen und Verantwortlichkeiten.

Hybrid Cloud verändert nicht nur die Infrastruktur. Sie verändert die Art, wie IT organisiert ist, wie Prozesse ablaufen und welche Kompetenzen gefragt sind. Klassische IT-Abteilungen sind entlang von Technologien aufgebaut: Server-Team, Storage-Team, Netzwerk-Team. Eine Plattformorganisation braucht etwas anderes: Plattformverantwortung über Domäne-Grenzen hinweg, direkte Verbindung zum Business, Automatisierungsexpertise.

Wenn Automation an Prozessgrenzen endet

Ein typisches Muster aus der Praxis: Die Plattform kann in fünf Minuten eine VM bereitstellen. Aber der Change-Prozess braucht fünf Tage. Das Ergebnis: Die Automation existiert – und läuft gegen eine manuelle Wand. ITIL-Prozesse bleiben wichtig, müssen jedoch zu einer hochautomatisierten Plattform passen. Wer Change-Management, Incident-Management und Configuration-Management nicht mitverändert, bremst die Plattform aus, bevor sie wirken kann. Gleichzeitig gewinnt Business Relationship Management an Bedeutung. IT-Plattformteams müssen verstehen, welche Services das Business tatsächlich braucht, wie sie genutzt werden – und wo verbessert werden muss. Sonst optimiert die IT ihre Technologie, aber nicht den Wert für den Kunden. Swiss IT Magazine beschreibt Cloud-Transformation 2026 ausdrücklich als strategische, organisatorische,

MAKE OR BUY? DIE RICHTIGE FRAGE ZUERST.

Welche Fähigkeiten differenzieren Ihr Geschäft und müssen intern bleiben? Welche Leistungen sind standardisierbar und damit auslagerfähig? Und welche Plattform kann ein Partner zuverlässiger, skalierbarer oder wirtschaftlicher betreiben – weil er ausschliesslich das macht?

personelle und betriebliche Aufgabe – nicht nur als technische.

Fachkräftemangel trifft auf steigende Komplexität

Erfahrene Spezialisten scheiden aus – die Baby-Boomer-Generation verlässt den Markt. Gleichzeitig werden neue Kompetenzen in Automation, Kubernetes, Security-Engineering, FinOps und AI Operations gebraucht. Beides trifft gleichzeitig ein. Wer glaubt, dieses Problem mit Stellenausschreibungen zu lösen, unterschlägt, wie lange der Aufbau dieser Kompetenzen dauert. Managed Services sind kein Notbehelf. Sie sind eine bewusste Betriebsentscheidung. Die beste Hybrid-Cloud-Architektur bringt wenig, wenn das Betriebsmodell nicht zur Organisation passt. Architektur und Betriebsmodell müssen zusammen gedacht werden, nicht nacheinander.

Erst verstehen. Dann entscheiden.

Sonio schafft Transparenz über Workloads, Kosten, Risiken und Betriebsmodelle – bevor Architekturentscheide fallen.

Wer mit einem Produkt beginnt, hat die wichtigste Entscheidung bereits übersprungen. Eine belastbare Hybrid-Cloud-Strategie beginnt mit Transparenz: über Business-Services, Applikationen, Daten, Kosten, Risiken und – ehrlich bewertet – die eigene Betriebsfähigkeit.

Das Sonio Hybrid Cloud Assessment ist kein Vertriebs-Tool. Es ist eine strukturierte Analyse, deren Ergebnis keine Produktliste ist, sondern eine Workload Map, ein Zielbild für das Betriebs- und Security-Modell und eine Roadmap, die umsetzbar ist.

Wie Sonio begleitet: Drei Betriebsmodelle

- **Managed On Premises:** Sonio betreibt Plattformen beim Kunden – Monitoring, Security,

Lifecycle-Management, Patching.

- **Managed Sonio Cloud (Trusted Cloud):** Schweizer Cloud, betrieben durch Sonio – Datensouveränität, Compliance und Managed Service aus einer Hand.
- **Managed Hyperscaler:** Governance, FinOps, Security und Betrieb auf Microsoft Azure – mit klarer Verantwortung und Transparenz.

Die Architektur bleibt damit offen. Ein Workload kann dort laufen, wo er fachlich am besten aufgehoben ist – und nicht dort, wo der nächste Vertrag bereits unterschrieben ist.

WAS DAS HYBRID CLOUD ASSESSMENT LIEFERT

Workload Map: Welche Applikationen existieren? Welche Abhängigkeiten, welche Compliance-Anforderungen, welche Cloud-Fähigkeit?

Vollkosten-Transparenz: Betriebskosten, Lizenzrisiken, Egress-Kosten und Make-or-Buy-Entscheide auf dem Tisch.

Workload-Platzierung: Private Cloud, Trusted Cloud oder Public Cloud – begründet, nicht verkauft. Betriebsmodell-Empfehlung: Was betreibt die eigene IT? Was übernimmt ein Managed Service? Bewusst entschieden.

Einfachheit ist kein Zufall.

Hybrid Cloud funktioniert nur, wenn Komplexität bewusst standardisiert, automatisiert und betrieben wird.

Hybrid Cloud macht das Leben für den Consumer einfacher. Aber nur dann, wenn jemand die Komplexität dahinter bewusst standardisiert, automatisiert und betreibt. Das passiert nicht von selbst.

Die entscheidende Managementfrage lautet deshalb nicht «Cloud oder Rechenzentrum?». Sie lautet: Welche Plattform passt zu welchem Workload? Welche Fähigkeiten will die eigene Organisation besitzen? Und welche Komplexität will sie dauerhaft selbst betreiben?

„ Einfach für den
Nutzer heisst: konsequent
engineered im Hintergrund.

Sonio AG, Hybrid Cloud Praxis

Die sieben zentralen Erkenntnisse:

- **Cloud ist ein Betriebsmodell, kein Produkt.**
Wer Ressourcen noch manuell bereitstellt, betreibt Virtualisierung – keine Cloud.
- **Hybrid Cloud verschiebt Komplexität.**
Der Consumer profitiert. Der Betreiber trägt mehr Verantwortung – und braucht Plattform, Automation und Governance, die das tragen.
- **Multi Cloud entsteht oft ungeplant.** Mehrere Provider zu nutzen ist kein Betriebsmodell.

Governance, Integration und gemeinsame Standards sind es.

- **Security ist Plattformarchitektur.** Instant Patching, Policy-as-Code, getestete Recovery – keine Zusatzmodule, sondern Kernfähigkeiten.
- **AI und Kubernetes sind Teil der Gleichung.**
Wer AI als neues Silo aufbaut, wiederholt den alten Fehler. Neue Workloads, gleiche Fragen.
- **Workload first, nicht Cloud first.** Die Plattform folgt dem Workload – nicht dem Hersteller und nicht dem Trend.
- **Die Organisation entscheidet über Erfolg oder Misserfolg.** Technik ist selten das grösste Problem. Skills, Prozesse und Make-or-Buy-Entscheide sind es.

DIE ENTSCHEIDUNG.

Wenn morgen ein neuer Business-Service, ein AI-Workload oder eine regulatorische Anforderung dazukommt: Kann Ihre IT ihn kontrolliert bereitstellen, ohne ein neues Silo zu bauen? Wenn nicht, beginnt genau dort die Arbeit.

Jetzt ins Handeln kommen.

Mit klaren Checks, einer belastbaren Workload-Sicht und einem passenden Betriebsmodell wird aus Hybrid Cloud eine umsetzbare Roadmap.

Drei Zeithorizonte – konkrete Massnahmen für KMU, Mid-Market und Enterprise gleichermassen.

Menschen, Lifecycle – über fünf Jahre, nicht über drei Monate.

Sofortmassnahmen – diese Woche

1. Cloud-Realitätscheck: Wie lange dauert die Bereitstellung einer neuen VM? Ist das Self-Service oder ein Ticket-Prozess? Die Antwort zeigt, wo Sie wirklich stehen.

2. Broadcom-Check: Welche VMware-Versionen laufen? Wann läuft der Vertrag aus? Supportende Oktober 2027 – wer jetzt nicht plant, plant unter Druck.

3. Souveränitäts-Check: Welche Daten und Applikationen laufen bei US-Anbietern? Welche Compliance-Konsequenzen hat das konkret?

Mittelfristig – in den nächsten 90 Tagen

1. Applikations- und Abhängigkeitsinventar: Was läuft? Was hängt woran? Was ist tatsächlich Cloud-fähig – und was nicht?

2. Vollkosten-Analyse: Betrieb, Lizenzen, Egress,

3. Hybrid Cloud Assessment starten: Mit einem Partner, der eine Workload Map liefert – keine Produktliste.

Strategisch: Ihre Cloud-Roadmap

1. Betriebsmodell entscheiden: Was betreibt die eigene IT? Was wird als Managed Service bezogen? Bewusst – nicht historisch gewachsen.

2. Security als Plattformarchitektur: Instant Patching, Policy-as-Code, zentrale Telemetrie, getestete Recovery – Plattformfähigkeiten, keine Sonderprojekte.

3. AI- und Kubernetes-Readiness mitplanen: Wer heute die Plattform plant, entscheidet mit – ob in zwei Jahren AI-Workloads und Container-Services sinnvoll integrierbar sind.

3. FinOps etablieren: Kosten und Wert für alle Plattformen gemeinsam sichtbar machen – Private Cloud, Trusted Cloud, Public Cloud.

BEREIT FÜR DEN NÄCHSTEN SCHRITT?

Sonio begleitet Sie vom Assessment über die Workload-Platzierung bis zum laufenden Managed Service – auf allen drei Betriebsmodellen. Unabhängig davon, welche Cloud am Ende die richtige für Sie ist.

Vereinbaren Sie jetzt ein persönliches Beratungsgespräch:

www.sonio.com/hybrid-cloud

Primärquelle: Diskussionsrunde Hybrid Cloud White Paper mit Markus Fischer, Dirk Weis und Ralph Budil, Sonio AG, 3. August 2026.

Externe Quellen: NIST SP 800-145. Flexera State of the Cloud 2026 (73% Hybrid Cloud, 88% Multi Cloud). FinOps Foundation State of FinOps 2026.

CNCF Annual Cloud Native Survey 2025 (82% Kubernetes produktiv, 66% für GenAI Inference). BACS Halbjahresbericht 2025/2 (über 29'000 Meldungen). privatim Resolution zu internationalen Cloud-Lösungen, November 2025. Swiss IT Magazine Cloud-Transformation 2026/06 und CIO Interview

Rapp Gruppe 2026/06. OWASP GenAI Exploit Round-up Q1 2026. NIST Security Considerations for AI Agents, Mai 2026. Sonio Managed Services:

sonio.com/services/managed-services.

The background of the entire page is a photograph of a car's interior, specifically the dashboard and steering wheel area. The image is heavily blurred, showing out-of-focus lights and shapes. A large, solid blue semi-circular shape is overlaid on the bottom left portion of the image, partially obscuring the car's interior. The word "sonio." is written in white, lowercase letters in the top left corner.

sonio.

Kontaktieren
Sie uns für ein
unverbindliches
Gespräch:

info@sonio.com

www.sonio.com