AWS Microsoft-Workloads-Kompetenz

Validierungscheckliste für Technologiepartner

Juni 2019

Version 1.0

aws partner network

Inhalt

Einführung

Mit dem AWS-Kompetenzprogramm sollen Partner im AWS-Partnernetzwerk ("APN-Partner") mit technischer Fachkenntnis und nachgewiesenen Kundenerfolgen in speziellen Lösungsbereichen gewürdigt werden. Die Validierungscheckliste für Kompetenzpartner ("Checklist") wurde für APN-Partner konzipiert, die Interesse an einer Teilnahme am AWS-Kompetenzprogramm haben. Diese Checklist enthält die Kriterien, die erforderlich sind, um die Bezeichnung im Rahmen des AWS-Kompetenzprogramms zu erhalten. APN-Partner absolvieren nach der Bewerbung für eine bestimmte Kompetenz ein Audit zu ihren Kompetenzen. AWS nutzt unternehmensinternes Fachwissen und zieht für die Durchführung des Audits einen externen Partner hinzu. AWS behält sich das Recht vor, jederzeit Änderungen an diesem Dokument vorzunehmen.

Erwartungen der beteiligten Parteien

Es wird erwartet, dass APN-Partner sich im Detail mit diesem Dokument vertraut machen, bevor sie sich für das AWS-Kompetenzprogramm bewerben, selbst wenn alle Voraussetzungen erfüllt sind. Sollten bestimmte Abschnitte in diesem Dokument unklar sein und weiterer Erläuterungen bedürfen, wenden Sie sich zunächst an den für Sie zuständigen AWS Partner Development Representative (PDR) oder AWS Partner Development Manager (PDM). Ihr PDR/PDM wird sich an das Programmbüro wenden, wenn weitere Unterstützung erforderlich sein sollte.

Wenn Sie als APN-Partner bereit sind, eine Programmbewerbung einzureichen, müssen Sie die Spalte "Partner Self-Assessment" in der Checkliste ausfüllen, die im weiteren Verlauf dieses Dokuments näher beschrieben wird.

So übermitteln Sie Ihre Bewerbung:

1. Melden Sie sich als Alliance Lead auf APN Partner Central (https://partnercentral.awspartner.com/) an.
2. Wählen Sie "View My APN Account" links auf der Seite aus.
3. Führen Sie einen Bildlauf zum Abschnitt "Program Details" aus.
4. Wählen Sie “Update” neben der AWS-Kompetenz aus, für die Sie sich bewerben möchten.
5. Füllen Sie die Programmbewerbung aus, und klicken Sie dann auf "Submit".
6. Senden Sie die ausgefüllte Selbsteinschätzung per E-Mail an competency-checklist@amazon.com.
    - Die Selbsteinschätzung muss Folgendes enthalten:
        - Die Kategorie der Lösung (Produktdesign, Produktionsdesign, Produktion oder Betrieb)
        - Die Art der Bereitstellung (SaaS oder durch Kunden in AWS bereitgestellt)
        - Dokumentation für die AWS-Fallstudien (siehe Definitionen unten)

Bei Fragen zu den oben genannten Anweisungen wenden Sie sich bitte an den für Sie zuständigen PDR/PDM.

AWS wird sich Ihre Fragen anschauen und ist bemüht, innerhalb von fünf Werktagen auf Ihre Fragen zu antworten, um einen Zeitplan für Ihr Audit zu erstellen oder weitere Informationen anzufordern.

APN-Partner sollten sich auf das Audit vorbereiten, indem sie die Checklist studieren, anhand der Checkliste eine Selbsteinschätzung durchführen und Nachweise erbringen, die sie dem Prüfer am Tag des Audits vorlegen.

AWS empfiehlt, dass APN-Partner Einzelpersonen benennen, die sich im Rahmen des Audits detailliert zu den Anforderungen äußern können. Es hat sich bewährt, dass APN-Partner Personen mit den folgenden Zuständigkeiten für das Audit bereitstellen: mindestens einen hochspezialisierten und von AWS zertifizierten Techniker/Architekt, einen Betriebsleiter, der für die Abläufe und die Supportelemente zuständig ist, sowie einen leitenden Mitarbeiter im Bereich Geschäftsentwicklung, der den Übersichtsvortrag durchführt. APN-Partner sollten vor der Vereinbarung eines Termins für das Audit sicherstellen, dass sie berechtigt sind, alle Informationen, die im Nachweis oder in den Präsentationen enthalten sind, gegenüber dem Prüfer (von AWS oder einem externen Partner) preisgeben dürfen.

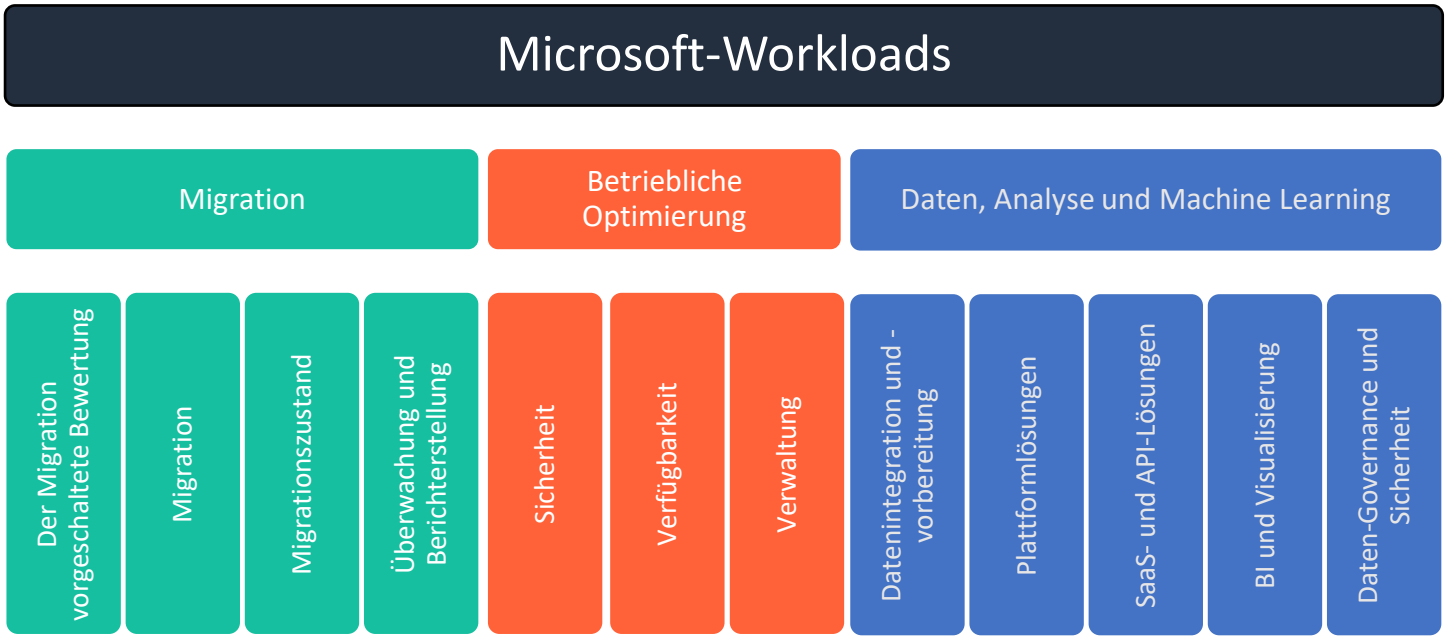
AWS Microsoft-Workloads-Kompetenzprogramm

Dieses AWS Microsoft-Workloads-Kompetenzprogramm (auch als "AWS Microsoft Workloads-Kompetenz" oder "Kompetenz" bezeichnet) identifiziert und validiert Angebote von APN-Partnern, um Kunden dabei zu unterstützen, auf Microsoft-Workloads zuzugreifen und diese nach AWS zu migrieren sowie Microsoft-Workloads auf AWS bereitzustellen, zu optimieren und zu modernisieren. Die entsprechenden Angebote sind in drei Kategorien segmentiert: Migration, Betriebliche Optimierung und Daten/Analyse/Machine Learning. Diese Kategorien sind weiter in Funktionsunterkategorien unterteilt. APN-Partner können sich über eine oder mehrere Kategorien für das AWS-Kompetenzprogramm bewerben und diesem beitreten.

Kategorien des AWS Microsoft-Workloads-Kompetenzprogramms

APN-Partner müssen die Segmentkategorie und die Unterkategorie(n) identifizieren, zu denen ihre Lösung passt:

1. **Migration von Microsoft-Workloads**: Technologien in dieser Kategorie bieten eine der Migration vorgeschaltete Bewertung und Planung oder automatisieren und verwalten die Migration von Microsoft-Workloads.
2. **Betriebliche Optimierung**: Technologien in dieser Kategorie werden dazu verwendet, Microsoft-Workloads auf AWS in den Bereichen Sicherheit, Verfügbarkeit und Verwaltbarkeit zu optimieren und zu verwalten.
3. **Daten, Analyse und Machine Learning:** Mit den Technologien in dieser Kategorie ist es möglich, Microsoft SQL Server-Daten für den Zweck der Datenanalyse und für Machine Learning auf AWS vorzubereiten, zu transformieren, zu analysieren und zu steuern.



Diese Tabelle wurde geändert

Voraussetzungen für das AWS Microsoft-Workloads-Kompetenzprogramm

Die folgenden Elemente werden durch den Manager für das AWS-Kompetenzprogramm validiert. Fehlende oder unvollständige Informationen müssen vor der Terminierung der Technologievalidierungsüberprüfung bereitgestellt werden.

1.0 APN-Programmanforderungen		**Erfüllt J/N**
1.1 Programmrichtlinien	APN-Partner müssen die Programmrichtlinien und -definitionen lesen, bevor sie sich für das Microsoft-Workloads-Kompetenzprogramm bewerben. Hier finden Sie die Programmdetails.	
1.2 APN-Technologiepartnerstufen	APN-Partner müssen sich auf der Stufe "Advanced" für APN-Technologiepartner befinden.	
1.3 Lösungskategorie	APN-Partner müssen die Segmentkategorie und die Unterkategorie(n) für ihre jeweilige Lösung identifizieren. Kategorie: ▪ **Migration von Microsoft-Workloads** ☐ Der Migration vorgeschaltete Bewertung ☐ Anwendungs- und Datenmigration ☐ Migrationszustand ☐ Überwachung und Berichterstellung ▪ **Microsoft-Workloads – Betriebliche Optimierung** ☐ Sicherheits- und Bedrohungsverwaltung ☐ Verfügbarkeit und Notfallwiederherstellung ☐ Ressourcenverwaltung, Inventar-/Zustands-/Kostenüberwachung und Berichterstellung ▪ **Daten, Analyse und Machine Learning für Microsoft-Workloads** ☐ Datenintegration und -vorbereitung ☐ Plattformlösungen ☐ SaaS- und API-Lösungen ☐ Business Intelligence und Visualisierung ☐ Daten-Governance, Compliance und Sicherheit	
2.0 Fallstudien		**Erfüllt J/N**
2.1 Microsoft Workloads-spezifische Fallstudien	APN-Partner müssen mindestens vier (4) Fallstudien nachweisen, mit denen sie die Verwendung der APN-Partnertechnologie präsentieren, die für die zu prüfende Kategorie relevant ist. Bei APN-Partnern, die bereits auf die Kompetenzen AWS Migration, DevOps oder Data & Analytics validiert wurden, wird die Anforderungen auf ein Minimum von zwei Fallstudien reduziert, davon eine öffentliche und eine private Fallstudie, mit denen die Verwendung der APN-Partnertechnologie mit Microsoft-Workloads nachgewiesen werden, die für die zu prüfende Kategorie relevant ist. Wenn mehr als eine Kategorie geprüft wird, muss mit mindestens einer Studie die Verwendung der Technologie in jeder Unterkategorie nachgewiesen werden. Für jede einzelne Fallstudie muss der APN-Partner die folgenden Informationen bereitstellen: ▪ Name des Kunden ▪ Kundenproblem ▪ Art und Weise der Bereitstellung der Lösung zur Beantwortung der Herausforderung ▪ Verwendete externe Anwendungen oder Lösungen	

	▪ Datum, am die Referenz in Produktion gegangen ist ▪ Ergebnisse ▪ Spezifische Architekturdiagramme, Bereitstellungshandbücher und weitere Materialien, in Abhängig von der Art der Lösung, gemäß Beschreibung im nächsten Abschnitt. Diese Informationen werden im Rahmen der Programmbewerbung in APN Partner Central abgefragt. Alle vier bereitgestellten Fallstudien werden im Rahmen der technischen Untersuchung bereitgestellt. Die Fallstudie wird aus der Berücksichtigung im Rahmen der AWS-Kompetenzen entfernt, wenn der APN-Partner die erforderliche Dokumentation, die für die Bewertung der Studie gegen die einzelnen Checklisten-Posten benötigt wird, nicht bereitstellen kann, oder wenn einzelne Checklisten-Posten nicht erfüllt werden können. Fallstudien müssen die Bereitstellungen beschreiben, die innerhalb der vergangenen 18 Monate ausgeführt wurden, und müssen sich auf Projekte beziehen, die bei Kunden in der Produktion sind. Nicht zulässig sind Pilotprojekte oder Projekte im Status der Machbarkeitsüberprüfung.	
2.2 Öffentliche Fallstudien	Öffentlich verfügbare Fallstudien werden von AWS nach Genehmigung der Kompetenz verwendet, um den Erfolg des APN-Partners auf Basis messbarer lösungsbezogener Leistungskennzahlen (KPIs) nachzuweisen und Kunden die Gewissheit zu geben, dass der APN-Partner über die Technologie verfügt, um Lösungen für die Kundenprobleme zu entwickeln und bereitzustellen. Zwei (2) der vier (4) Kundenbereitstellungen, die mit den Fallstudien verknüpft sind, müssen durch den APN-Partner als öffentlich verfügbare Fallstudien veröffentlicht werden. Diese öffentlich verfügbaren Fallstudien können in Form von formalen Fallstudien, Whitepapers, Videos oder Blog-Posts veröffentlicht werden.	
	Öffentlich verfügbare Fallstudien müssen auf der APN-Partnerwebsite einfach zu finden sein, so muss es beispielsweise möglich sein, über die APN-Partner-Startseite zu den öffentlich verfügbaren Fallstudien zu navigieren, und der APN-Partner muss in seinen Anwendungen Links zu diesen öffentlich verfügbaren Fallstudien implementieren.	
	Öffentlich verfügbare Fallstudien müssen die folgenden Elemente aufweisen: ▪ Kundenname, APN-Partnername und AWS ▪ Kundenproblem ▪ Art und Weise der Bereitstellung der Lösung zur Beantwortung der Herausforderung ▪ Art und Weise, wie AWS-Services als Teil der Lösung genutzt wurden ▪ Ergebnisse	
3.0 Web-Präsenz und Vordenkerposition von AWS Microsoft-Workloads		**Erfüllt J/N**
3.1 Partner AWS-Microsite	Mit der Internetpräsenz eines APN-Partners, die sich auf die AWS Microsoft-Workloads-Lösungen bezieht, gewinnen Kunden Vertrauen in die Fähigkeiten und die Erfahrung des APN-Partners. APN-Partner müssen eine AWS-Microsite-Seite einrichten, auf der sie ihre AWS Microsoft-Workloads-Lösung beschreiben, Links zu ihren öffentlich verfügbaren Fallstudien einbinden, Technologiepartnerschaften auflisten und weitere relevante Informationen bereitstellen, die die Fachkenntnis des Partners in Bezug auf Microsoft-Workloads unter Beweis stellt und die Partnerschaft mit AWS hervorhebt. Diese AWS-spezifische Microsoft-Workloads-Microsite muss über die APN-Partner-Startseite erreichbar sein. Die Startseite selbst wird nicht als eine AWS-Microsite anerkannt, es sei denn, der APN-Partner ist ein dediziertes Microsoft-Workloads-Unternehmen, und die Startseite spiegelt den Fokus des APN-Partners auf Microsoft-Workloads wieder.	
3.2 Vordenkerposition für Microsoft-Workloads	AWS Microsoft-Workloads-Kompetenzpartner werden aufgrund ihrer innovativen Lösungen, die AWS-Services nutzen oder die Verwaltung dieser unterstützen, als Experten mit umfassender Fachkompetenz im Bereich Cloud-Verwaltung anerkannt. APN-Partner müssen für die Öffentlichkeit zugänglich Materialien (z. B. Blog-Posts, Presseartikel, Videos usw.) bereitstellen, mit denen sie den Fokus und die Fachkenntnis des APN-Partners in Bezug auf Microsoft-Workloads unter Beweis stellen. Es müssen Links zu Materialbeispielen bereitgestellt werden, die in den vergangenen zwölf Monaten veröffentlicht wurden.	

4.0 Geschäftliche Anforderungen		Erfüllt J/N
4.1 Produktsupport/Helpdesk	APN-Partner bieten Kunden Support über Web-Chat, Telefon oder per E-Mail an. Der Nachweis muss in Form der Beschreibung des Supports erbracht werden, der Kunden für ihr Produkt oder ihre Lösung angeboten wird.	
4.2 Produkt ist auf AWS Marketplace gelistet	APN-Partner bietet Lösung über AWS Marketplace an. ☐ Ja ☐ Nein Falls "Ja", muss der APN-Partner einen Link zum AWS Marketplace-Listing bereitstellen. Falls "Nein", sind keine weiteren Informationen erforderlich. Beachten Sie Folgendes: AWS Marketplace ist für das Erreichen der Kompetenz keine Voraussetzung.	
4.3 Bereitstellungsmodell	Der APN-Partner identifiziert alle Modelloptionen für die Bereitstellung, aus denen Kunden auswählen können. ☐ SaaS auf AWS ☐ SaaS außerhalb von AWS (für die Migration) ☐ BYOL auf AWS ☐ BYOL am Standort (für die Migration)	
5.0 APN-Partner-Selbsteinschätzung		**Erfüllt J/N**
5.1 Selbsteinschätzung zur Validierungscheckliste des AWS-Kompetenzprogramms	APN-Partner müssen eine Selbsteinschätzung in Bezug auf die Erfüllung dieser Checkliste durchführen. ▪ APN-Partner müssen alle Abschnitte der Checkliste ausfüllen. ▪ Die ausgefüllte Selbsteinschätzung muss per E-Mail an die Adresse **competency-checklist@amazon.com** gesendet werden. Dabei gilt die folgende Konvention für die E-Mail-Betreffzeile: "[APN-Partnername], Selbsteinschätzung als Microsoft-Workloads-Kompetenztechnologiepartner abgeschlossen." ▪ Es wird empfohlen, dass der APN-Partner die ausgefüllte Selbsteinschätzung vor der Übermittlung an AWS durch den zugewiesenen Partner Solutions Architect, den PDR oder PDM überprüfen lässt. Damit soll sichergestellt werden, dass das AWS-Team beim APN-Partner einbezogen wird und daran arbeitet, vor der Überprüfung Empfehlungen bereitzustellen und eine produktive Überprüfungserfahrung zu gewährleisten.	

Validierungscheckliste für das AWS Microsoft-Workloads-Kompetenzprogramm

Die folgenden Aspekte werden durch einen AWS Partner Solutions Architect und/oder externe Prüfer und/oder AWS Partner Solutions Architects validiert. Fehlende oder unvollständige Information müssen vor der Vereinbarung eines Termins für die Technologievalidierungsprüfung bereitgestellt werden.

Technische Microsoft-Workloads-Anforderungen nach Kategorie

Die Dokumentation mit einer Beschreibung, wie die APN-Partnerlösung die Anforderungen erfüllt, muss als Teil der Selbsteinschätzung zur AWS-Kompetenz beigefügt werden.

Migration von Microsoft-Workloads

Erforderliche Funktionen der Lösung		Erfüllt J/N
Der Migration vorgeschaltete Bewertung	Die Technologielösung muss entweder eine agentengebundene oder eine Technologie ohne Agentenbindung nutzen, um nach AWS zu migrierende Daten automatisch zu identifizieren. Dies kann Folgendes umfassen: ▪ Der Migration des Microsoft-Workloads vorgeschaltete Bewertung mindestens einer der folgenden Aspekte: o Bewertung von Servern und virtuellen Maschinen, die Microsoft Windows vor Ort ausführen o Docker-Container-Bewertung (entweder wenn auf Windows Server ausgeführt oder wenn Container die .NET/.NET Core-Anwendung ausführt) o Bewertung der .NET/.NET Core-Anwendung o Bewertung der Datenmigration (SQL, Dateisystem, Blob usw.) o Bewertung der Migration von Unternehmenslösungen (Active Directory, OneDrive, Dynamics, Exchange usw.) ▪ Es sollte ein Bericht zur der Migration vorgeschalteten Bewertung generiert werden. jeder Workload in vom Kunden bestimmte AWS-Ressourcengruppe	
Migration	Die Technologielösung muss entweder eine agentengebundene oder eine Technologie ohne Agentenbindung bieten, um identifizierte Workloads oder Daten im Rahmen der Workload-Migration automatisch nach AWS zu migrieren. Dies kann Folgendes umfassen: ▪ Microsoft-Workload-Migration einer der folgenden Komponenten: o Migration virtueller Maschinen o Docker-Container-Bewertung (bei Ausführung auf Windows Server oder wenn Container die .NET/.NET Core-Anwendung ausführt) o Bewertung der .NET/.NET Core-Anwendung o Datenmigration (SQL, Dateisystem, Blob usw.) o Migration von Unternehmenslösungen (Active Directory, OneDrive, Dynamics, Exchange usw.) ▪ Fähigkeit, beim Scheitern von Migrationen Sicherungen und Rollbacks mit minimalem oder ganz ohne Datenverlust zu beliebigen Zeitpunkten durchzuführen ▪ Unterstützung von Hybrid-Cloud-Konfigurationen für Notfallwiederherstellung ▪ Differenz-Delta-Synchronisierung, um Daten nach der Migration zu synchronisieren, wenn Umstellung erreicht ist und der Quellserver bzw. die Quell-Instance heruntergefahren wurde ▪ Umstellung jedes Workloads in vom Kunden bestimmte AWS-Ressourcengruppe	

Migrationszustand	Die Technologielösung sollte während der Migration eine Bewertung zur Entscheidung der folgenden Echtzeit-Komponenten durchführen: ▪ Datenintegrität ▪ Anwendungszustand ▪ Bewertung des Zustands der allgemein verbundenen Architektur	
Überwachung und Berichterstellung	Die Technologielösung sollte die folgenden Funktionen bzw. Möglichkeiten bieten: ▪ Überwachung des Migrationsfortschritts ▪ Benachrichtigungen, Warnungen und Fehlerberichte ▪ Allgemeine Berichterstellung zur Migration	

Betriebliche Optimierung

Erforderliche Funktionen der Lösung		Erfüllt J/N
Sicherheit	Die Technologielösung sollte eine der folgenden Funktionen oder Möglichkeiten bieten: ▪ Konfiguration der Sicherheitslage (rollenbasierter Zugriff, Identitätszugriff und -verwaltung, Proxy-/Firewall-Konfiguration, Routing, Verschlüsselung usw.) ▪ Analyse für DLP (Data Loss Prevention) bereitstellen ▪ Netzwerk- und Instance-Sicherheitslage (Ports, Zertifikate, Sicherheitskonfiguration) bereitstellen ▪ Bedrohungsmodellierung für Netzwerkdatenverkehr (Vektoren für mögliche Angriffe) und Alarmierung ▪ Compliance (HIPAA, PCI, SOX usw.) ▪ Fähigkeit, Verbesserungen bei der Sicherheitslage zu empfehlen ▪ Quellcode-Prüfung auf fehlerhafte Verfahren, Speicherlücken, Datenhygiene und Sicherheitsprobleme	
Verfügbarkeit	Die Technologielösung sollte eine der folgenden Funktionen oder Möglichkeiten bieten: ▪ Laufende Prüfung auf Notfallwiederherstellung (Chaos-Engineering) o Skalierbarkeit o Verfügbarkeit o Datenintegrität und Ausfallsicherheit ▪ Ressourcenanalyse zur Bestimmung von Problemen bei der Hochverfügbarkeit. ▪ Fähigkeit zur automatischen Skalierung (hoch- und runterskalieren) bei variierenden Workloads	
Verwaltung	Die Technologielösung sollte eine der folgenden Funktionen oder Möglichkeiten bieten: ▪ Bestandsauflistung und -analyse (in Amazon EC2-Instances, Containern, Serverless) von: o Microsoft-Workload-Komponenten o Microsoft-Workload-Konfiguration o Microsoft-Infrastrukturkonfiguration ▪ Automatische Erkennung der: o Netzwerkkonfiguration o Datenverarbeitungsressourcen (Server, Cluster) o Speicherressourcen (LUNs, iSCSi-Ziele usw.) o Datenbanken (Routine, Konfiguration, Version, Kompatibilität) ▪ Verlaufsanalyse zur Bestandsänderungen (für einen ausgewählten Zeitraum) ▪ Ressourcenzuweisung, Kapazitätsnutzungsanalyse	

	▪ Laufende Kostenanalyse und Alarmierung (Ressourcennutzung und Lizenzierung) ▪ Fähigkeit, eine reduzierte Bereitstellung auf Basis von Nutzung und Workload-Mustern zu empfehlen ▪ Laufende Leistungsanalyse und Alarmierung ▪ Bekannte Microsoft-Workload-spezifische und automatisierungsbezogene Betriebsablaufaufgaben, wie z. B.: o Sicherung und Wiederherstellung o Patchen o Workload-Statusverwaltung o Konfigurationsverwaltung ▪ Benchmark für erforderliche/durchschnittliche Leistung der standortbasierten Lösungen/Anwendungen erstellen ▪ Instances, Ressourcen-Abgleich und Empfehlungen auf AWS auf Basis von Benchmarking bereitstellen ▪ POC- und Benchmark-Lösungen/Anwendungen auf AWS ▪ Geschätzte Umsatzrendite und Ressourcennutzung auf Basis von Benchmarking bereitstellen ▪ Berichterstellung: o Berichterstellung zur Leistung, Bereitstellung und Alarmierung (für Berichte) o Berichterstellung zur Infrastruktur, Bereitstellung und Alarmierung (für Berichte) o Workload-Konfiguration, Berichterstellung zum Zustand, Bereitstellung und Alarmierung (für Berichte) o Berichterstellung zum Patchen, Bereitstellung und Alarmierung (für Berichte)	

Daten, Analyse und Machine Learning

Erforderliche Funktionen der Lösung		**Erfüllt J/N**
Datenintegration und -vorbereitung	Die technische Lösung sollte die folgenden Funktionen und Möglichkeiten bieten: ▪ Workload-Daten aufnehmen und Maßnahme vorschlagen ▪ deskriptive, strukturelle, administrative, referenzielle und statistische Daten kommentieren: o Syntaktisches und Abhängigkeits-Tree-Banking, einschließlich Identifizierung von Ko-Referenzen o Semantisches Kommentieren von Text, einschließlich Identifizierung von benannten Entitäten für Such-, Stimmungsanalyse- und Data-Mining-Anwendungen o Identifizierung von Sprache, Dialekten und Sprecherdemografien o Video, Bild, Word-Datei, PDF usw. o Abteilung, Geschäftseinheit, Prozess o Sicherheitsschutzstufe (Vertraulich, Öffentlich, Privat usw.) o Objekttyp (Gebäude, Person, Tier usw.) ▪ Daten aus unterschiedlichen Quellen verschieben und konsolidieren ▪ Daten für Analysen transformieren und vorbereiten ▪ Datenqualitätsprüfung ▪ Datenreplikation ▪ Datenprofilierung	

	▪ Funktions-Engineering – Erstellen neuer Eingabefunktionen aus vorhandenen Funktionen.	
Plattformlösungen	Die technische Lösung sollte: ▪ aus eng integrierten Tools bestehen, die für die Zusammenarbeit konzipiert sind und Analyseherausforderungen innerhalb standardisierter Frameworks lösen. Zu den Komponenten zählen: o Speicher o Verarbeitung o Planung o Sicherheit o Analyseeinrichtungen ▪ Ausstattung von Datenwissenschaftlern und Machine Learning-Experten mit Tools, um Daten zu verwenden, Prognosemodelle zu trainieren und Prognosen auf Basis neuer Daten zu erstellen.	
SaaS- und API-Lösungen	Diese Kategorie umfasst Lösungen für AI-/MI-basierte Prognosefunktionen in Kundenanwendungen: ▪ Internet ▪ Client ▪ Frameworks	
Business Intelligence und Visualisierung	Technische Lösungen, die Rohdaten auf Basis analytischer Verarbeitungstechnologien in umsetzbare Geschäftsinformationen wandeln: ▪ Berichterstellung ▪ Dashboarding ▪ Datenvisualisierung	
Daten-Governance und Sicherheit	Technische Lösungen zur Ermittlung, Kategorisierung und Steuerung von Daten Darin enthalten: ▪ Definieren und Durchsetzen von Richtlinien ▪ Sicherheit und Verwaltung personenbezogener Informationen ▪ Erstellen von Datenkatalogen und Glossaren ▪ Datenverlaufskontrolle ▪ Datenmaskierung	

Technische Anforderungen für AWS

Im Folgenden werden die technischen Anforderungen für jede der vier vom APN-Partner übermittelten Fallstudien aufgeführt. Jede Kategorie muss nachweisen, dass die durch den APN-Partner bereitgestellten Lösungen die bewährten Methoden von AWS erfüllen und dem AWS Well-Architected Framework entsprechen.

	Gilt für:				
	Multi-Mandanten-SaaS	Einzel-Mandanten-SaaS	Durch Kunden am Standort bereitgestellte Lösungen	Durch Kunden in AWS bereitgestellte Lösungen	**Erfüllt J/N**
Erforderliche Dokumentation Die folgende Dokumentation muss im Rahmen der Kompetenzselbsteinschätzung übermittelt werden.					

Architekturdiagramm	Je nach Bereitstellungskategorie ist mindestens ein Architekturdiagramm erforderlich. Jedes Architekturdiagramm muss die folgenden Elemente enthalten: ▪ die wichtigsten Elemente der Architektur und wie sie sich zusammenschließen, um die APN-Partnerlösung den Kunden bereitzustellen ▪ alle verwendeten AWS Services über die entsprechenden AWS-Service-Symbole. ▪ Art und Weise der Bereitstellung der AWS-Services, darunter Amazon Virtual Private Cloud (Amazon VPC), Availability Zones, Teilbereiche und Verbindungen zu Systemen außerhalb von AWS. ▪ Enthält Elemente, die außerhalb von AWS bereitgestellt wurden, z. B. standortbasierte Komponenten oder Hardware-Geräte.	Ja – eines für die ganze Lösung und eines für die Fallstudie	Ja – eines für die ganze Lösung und eines für die Fallstudie	Ja – eines für jede einzelne Fallstudie	Ja – eines für jede einzelne Fallstudie	
Bereitstellungshandbuch	Das Bereitstellungshandbuch muss die bewährten Methoden für die Bereitstellung der APN-Partnerlösung auf AWS enthalten, sowie alle Abschnitte, die in den “Handbüchern für die Basisanforderungen für die Bereitstellung” aufgeführt sind.	Nein	Nein	Nein	Ja – eines für die Lösung.	
Ausgefüllte Validierungscheckliste	Für jede der vier Fallstudien muss der APN-Partner eine ausgefüllte Version der folgenden Checkliste bereitstellen, um zu belegen, welche Checklistenposten erfüllt sind.	Ja	Ja	Ja	Ja	
1.0 Sicherheit Die Säule zur Sicherheit setzt den Fokus auf den Schutz von Informationen und Systemen. Zu den wichtigsten Themen zählen Vertraulichkeit und Integrität von Daten, das Nutzen der Berechtigungsverwaltung, um zu identifizieren und zu verwalten, wer welche Aufgaben ausführen darf, und das Aufbauen von Kontrollen zur Erkennung von Sicherheitsereignissen.						
1.1 Stammbenutzer für AWS-Konto für Routineaktivitäten nicht verwendet	Der Stammbenutzer für das AWS-Konto darf für Routineaktivitäten nicht verwendet werden. Nach der Erstellung Ihres AWS-Kontos sollten Sie sofort AWS Identity and Access Management (IAM)-Benutzerkonten erstellen und diese IAM-Benutzerkonten für alle Routineaktivitäten verwenden. Sobald Ihre IAM-Benutzerkonten erstellt wurden, sollten Sie die Anmeldeinformationen für das AWS-Stammkonto sicher speichern und sie nur für wenige Konto- und Serviceverwaltungsaufgaben verwenden, für die ein Stammbenutzer für das AWS-Konto erforderlich ist. Weitere Informationen zur Einrichtung von IAM-Benutzerkonten und -gruppen für den alltäglichen Bedarf finden Sie unter Erstellen Ihres ersten Administratorbenutzers und Ihrer ersten Administratorgruppe in IAM.	Ja	Ja	Nein	Nein	
1.2 Multi-Factor Authentication (MFA) wurde für Stammbenutzer auf dem AWS-Konto aktiviert	Multi-Factor Authentication (MFA) muss für Ihren Stammbenutzer auf dem AWS-Konto aktiviert werden. Da Ihr Stammbenutzer auf dem AWS-Konto vertrauliche Aktivitäten in Ihrem AWS-Konto ausführen kann, kann das Hinzufügen einer zusätzlichen Authentifizierungsebene helfen, Ihr Konto besser zu schützen. Es sind mehrere MFA-Typen verfügbar, darunter virtuelle MFA und Hardware-MFA.	Ja	Ja	Nein	Nein	
1.3 Für alle Routineaktivitäten verwendete	Der Stammbenutzer für das AWS-Konto darf nur verwendet werden, wenn dies unabdingbar ist. Erstellen Sie für alle anderen Aktivitäten für jede Person, die	Ja	Ja	Nein	Nein	

IAM-Benutzerkonten	Administratorrechte benötigt, einen neuen IAM-Benutzer. Definieren Sie diese Benutzer anschließend als Administratoren, indem Sie die Benutzer in eine Administratorgruppe setzen, mit der Sie die verwaltete Richtlinie "AdministratorAccess" verknüpfen. Anschließend sollten die Benutzer in der Administratorgruppe die Gruppen, Benutzer usw. für das AWS-Konto einrichten. Alle künftigen Interaktionen sollten über die Benutzer des AWS-Kontos und ihre eigenen Schlüssel, statt über den Stammbenutzer erfolgen. Für einige Konto- und Serviceverwaltungsaufgaben müssen Sie sich jedoch mit den Anmeldeinformationen des Stammbenutzers anmelden.					
1.4 Multi-Factor Authentication (MFA) für alle interaktiven IAM-Benutzer aktiviert	Sie müssen MFA für alle interaktiven IAM-Benutzer aktivieren. Mit MFA verfügen Benutzer über ein Gerät, das einen eindeutigen Authentifizierungscode (ein Einmal-Passwort oder OTP) generiert. Benutzer müssen ihre normalen Anmeldeinformationen (Benutzername und Passwort) sowie das Einmal-Passwort eingeben. Das MFA-Gerät kann entweder ein spezielles Hardware-Teil oder ein virtuelles Gerät sein, das in einer App auf einem Smartphone ausgeführt wird.	Ja	Ja	Nein	Nein	
1.5 Regelmäßige Änderung von IAM-Anmeldeinformationen	Sie müssen Ihre Passwörter und Zugriffsschlüssel regelmäßig ändern und sicherstellen, dass alle IAM-Benutzer in Ihrem Konto Ihrem Beispiel folgen. Auf diese Weise können Sie die zulässige Nutzungsdauer für Anmeldeinformationen für den Zugriff auf Ihre Ressourcen beschränken, falls einmal ein Passwort oder ein Zugriffsschlüssel ohne Ihr Wissen kompromittiert wurde. Sie können Ihr Konto mit einer Passwort-Richtlinie belegen, die all Ihre IAM-Benutzer zum Ändern ihrer Passwörter auffordert, und Sie können wählen, wie häufig Ihre Benutzer ihre Passwörter ändern müssen. Weitere Informationen zum Ändern von Zugriffsschlüsseln für IAM-Benutzer finden Sie unter Rotieren der Zugriffsschlüssel.	Ja	Ja	Ja (für Anmeldeinformationen, die für die Integration mit AWS verwendet werden)	Ja (für Anmeldeinformationen, die für die Integration mit AWS verwendet werden)	
1.7 Richtlinie für starke Passwörter für IAM-Benutzer vorhanden	Sie müssen eine Richtlinie für starke Passwörter für Ihre IAM-Benutzer konfigurieren. Wenn Sie Benutzern genehmigen, ihre eigenen Passwörter zu ändern, müssen Sie sie zur Verwendung von starken Passwörtern und zum regelmäßigen Ändern ihrer Passwörter verpflichten. Auf der Seite "Account Settings" in der IAM-Konsole können Sie eine Passwort-Richtlinie für Ihre Konten erstellen. Sie können die Passwort-Richtlinie verwenden, um Passwort-Anforderungen zu definieren, z. B. eine Mindestlänge, ob nicht-alphanumerische Zeichen zulässig sind, wie häufig ein Passwort geändert werden muss usw. Weitere Informationen finden Sie unter Einrichten einer Kontopasswortrichtlinie für IAM-Benutzer.	Ja	Ja	Ja (für Anmeldeinformationen, die für die Integration mit AWS verwendet werden)	Ja (für Anmeldeinformationen, die für die Integration mit AWS verwendet werden)	
1.8 Keine gemeinsame Verwendung von IAM-Anmeldeinformationen durch mehrere Benutzern	Sie müssen jeweils ein individuelles IAM-Benutzerkonto für alle Benutzer erstellen, die den Zugriff auf Ihr AWS-Konto benötigen. Erstellen Sie auch einen IAM-Benutzer für Sie selbst, verknüpfen Sie diesen Benutzer mit Administratorberechtigungen, und verwenden Sie diesen IAM-Benutzer für alle Ihre Aktivitäten. Durch das Erstellen individueller IAM-Benutzer für Personen, die auf Ihr Konto zugreifen möchten, können Sie für jeden IAM-Benutzer einen einmaligen Satz mit Sicherheitsanmeldeinformationen einrichten. Sie können	Ja	Ja	Nein	Nein	

	außerdem verschiedene Berechtigungen für die einzelnen IAM-Benutzer einrichten. Bei Bedarf können Sie die Berechtigungen eines IAM-Benutzers jederzeit ändern oder widerrufen. (Wenn Sie die Anmeldeinformationen für Ihren Stammbenutzer preisgeben, kann es mitunter schwierig sein, diese Informationen zu widerrufen, und es ist nicht möglich, die jeweiligen Berechtigungen zu beschränken.)					
1.9 Herunterskalierung der IAM-Richtlinien auf die geringsten Rechte	Sie müssen der Standardsicherheitsempfehlung für das Gewähren von geringsten Rechten folgen. Dies bedeutet, dass nur die Berechtigungen gewährt werden, die für die Ausführung einer Aufgabe zwingend erforderlich sind. Bestimmen Sie, welche Aufgaben Benutzer ausführen müssen, und entwickeln Sie anschließend Richtlinien für diese Aufgaben, damit Benutzer ausschließlich zur Ausführung dieser Aufgaben berechtigt sind. Beginnen Sie mit einem Mindestberechtigungssatz, und gewähren Sie bei Bedarf weitere Berechtigungen. Dieser Ansatz ist sicherer, als mit Berechtigungen zu starten, die sich als zu milde herausstellen und daher später stark eingeschränkt werden müssen. Die Definition des richtigen Berechtigungssatzes erfordert ein gewisses Maß an Recherche. Bestimmen Sie, welche Berechtigungen für eine bestimmte Aufgabe erforderlich sind, welche Aktionen von einem bestimmten Service unterstützt werden und welche Berechtigungen erforderlich sind, um diese Aktionen auszuführen.	Ja	Ja	Ja (für Lösungen, die außerhalb von AWS ausgeführt werden und über IAM-Rollen integriert sind, sollten die geringstmöglichen Zugriffsberechtigungen angewendet werden)	Ja (für Lösungen, die außerhalb von AWS ausgeführt werden und über IAM-Rollen integriert sind, sollten die geringstmöglichen Zugriffsberechtigungen angewendet werden)	
1.10 Keine Verwendung von hartkodierten Anmeldeinformationen (z. B. Zugriffsschlüssel)	Sie müssen den bewährten Methoden für die Verwaltung von AWS-Zugriffsschlüsseln folgen und die Verwendung von hartkodierten Anmeldeinformationen vermeiden. Wenn Sie programmgesteuert auf AWS zugreifen, verwenden Sie einen Zugriffsschlüssel, um Ihre Identität und die Identität Ihrer Anwendungen zu überprüfen. Jede Person, die auf Ihren Zugriffsschlüssel zugreifen kann, besitzt dieselbe Stufe für den Zugriff auf AWS-Ressourcen wie Sie selbst. Daher hat AWS sich für erhebliche Längen zum Schutz Ihrer Zugriffsschlüssel entschieden. Und um Ihrem Anteil an unserem Modell einer gemeinsamen Verantwortung gerecht zu werden, sollten Sie diesem Beispiel folgen.	Ja	Ja	Ja (Anmeldeinformationen, die für die Integration mit AWS verwendet werden, sollten einfach zu ändern und nicht hartkodiert sein)	Ja (Anmeldeinformationen, die für die Integration mit AWS verwendet werden, sollten einfach zu ändern und nicht hartkodiert sein)	
1.11 Verschlüsselung aller Anmeldeinformationen beim Speichern	Mit dieser Anforderung soll die Verschlüsselung aller gespeicherten Anmeldeinformationen gewährleistet werden.	Ja	Ja	Ja (Anmeldeinformationen, die in einer Partnerlösung für die Integration mit AWS gespeichert werden, sollten verschlüsselt werden)	Ja (Anmeldeinformationen, die in einer Partnerlösung für die Integration mit AWS gespeichert werden, sollten verschlüsselt werden)	

1.12 Verwendung von AWS-Zugriffsschlüsseln nur von interaktiven Benutzern	Es sollten keine AWS-Zugriffsschlüssel verwendet werden, mit Ausnahme der folgenden Fälle: 1. Werden von Personen verwendet, um auf AWS-Services zuzugreifen und werden auf einem Gerät gespeichert, das von diesen Personen kontrolliert wird. 2. Wird von einem Service verwendet, um auf AWS-Services zuzugreifen, jedoch nur in Fällen, in denen: a) es nicht möglich ist, eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance-Rolle, eine Amazon ECS-Aufgabenrolle oder einen vergleichbaren Mechanismus zu verwenden, b) die AWS-Zugriffsschlüssel mindestens einmal pro Woche geändert werden und c) die IAM-Richtlinie fest umrissen und wie folgt definiert ist: i) Es wird ausschließlich Zugriff auf spezifische Methoden und Ziele gewährt, ii) und der Zugriff ist beschränkt auf Teilnetze, über die auf die Ressourcen zugegriffen wird.	Ja	Ja	Nein	Nein	
1.13 AWS CloudTrail für alle AWS-Konten in allen Regionen aktiviert	AWS CloudTrail muss auf allen AWS-Konten und in jeder Region aktiviert werden. Der Einblick in Ihre AWS-Kontoaktivität ist ein wesentlicher Aspekt für Sicherheit und bewährte Methoden in Unternehmen. Sie können AWS CloudTrail zum Anzeigen, Suchen, Herunterladen, Archivieren, Analysieren und Antworten auf Kontoaktivitäten in Ihrer gesamten AWS-Infrastruktur verwenden. Sie können identifizieren, welche Person oder welcher Vorgang welche Aktion ausgeführt hat, welche Ressourcen betroffen sind und wann das Ereignis auftrat. Außerdem können Sie weitere Details anzeigen, die Ihnen helfen, Aktivitäten in Ihrem AWS-Konto zu analysieren und auf diese zu reagieren.	Ja	Ja	Nein	Nein	
1.14 Speicherung von AWS CloudTrail-Protokollen in einem Amazon S3-Bucket, der im Besitz eines anderen AWS-Kontos ist	AWS CloudTrail-Protokolle müssen in ein Bucket im Besitz eines anderen AWS-Konto platziert werden, das für einen extrem eingeschränkten Zugriff konfiguriert ist, z. B. nur für Audits und Wiederherstellung.	Ja	Ja	Nein	Nein	
1.15 Versionierung oder MFA Delete im AWS CloudTrail Amazon S3-Protokoll-Bucket aktiviert	Die Inhalte des AWS CloudTrail-Protokoll-Buckets müssen mit Versionierung oder MFA Delete geschützt werden.	Ja	Ja	Nein	Nein	
1.16 Amazon EC2-Sicherheitsgruppen eng dimensioniert	Alle Amazon EC2-Sicherheitsgruppen sollten den Zugriff auf das erforderliche Mindestmaß beschränken. Dazu gehört als Mindestanforderung: 1. Implementieren von Sicherheitsgruppen zur Beschränkung des Datenverkehrs zwischen dem Internet und Amazon VPC 2. Implementieren von Sicherheitsgruppen zur Beschränkung des Datenverkehrs innerhalb von Amazon VPC und 3. In allen Fällen Definieren von Einstellungen mit den größtmöglichen Beschränkungen.	Ja	Ja	Nein	Ja	
1.17 Amazon S3-Buckets in Ihrem	Sie müssen sicherstellen, dass die entsprechenden Kontrollen vorhanden sind, um den Zugriff auf die	Ja	Ja	Nein	Nein (außer bei	

Konto mit entsprechenden Zugriffsebenen ausgestattet	einzelnen Amazon S3-Buckets zu steuern. Wenn Sie AWS verwenden, hat es sich bewährt, den Zugriff auf Ihre Ressourcen auf jene Personen zu beschränken, die den Zugriff unbedingt benötigen (nach dem Prinzip des geringsten Rechts).				Partnerlösungen, die auf AWS ausgeführt werden, für die der S3-Service benötigt wird)	
1.18 Keine falsche Konfiguration von Amazon S3-Buckets für den öffentlichen Zugriff	Sie müssen sicherstellen, dass diese Buckets, die den öffentlichen Zugriff nicht gewähren sollten, so konfiguriert sind, dass ein öffentlicher Zugriff verhindert wird. Standardmäßig sind alle Amazon S3-Buckets privat. Der Zugriff ist nur für Benutzer möglich, denen der Zugriff ausdrücklich gewährt wurde. In den meisten Anwendungsfällen ist ein breit angelegter öffentlicher Zugriff zum Lesen von Dateien in Ihren Amazon S3-Buckets nicht erforderlich. Eine Ausnahme ist die Verwendung von Amazon S3 zum Hosten öffentlicher Werte (z. B. zum Hosten von Bildern zur Verwendung auf einer öffentlichen Website). Es hat sich bewährt, den Zugriff für die Öffentlichkeit grundsätzlich zu verhindern.	Ja	Ja	Nein	Nein (außer bei Partnerlösungen, die auf AWS ausgeführt werden, für die der S3-Service benötigt wird)	
1.19 Entwicklung eines Überwachungsmechanismus zur Ermittlung des Zeitpunkts für die Veröffentlichung von Amazon S3-Buckets oder Objekten	Überwachung oder Alarmierung müssen aktiviert sein, um zu identifizieren, wann Amazon S3-Buckets öffentlich werden. Eine Option, die sich dafür eignet, ist die Verwendung von AWS Trusted Advisor. AWS Trusted Advisor prüft Buckets in Amazon S3 mit offenen Zugriffsberechtigungen. Bucket-Berechtigungen, die allen Benutzern Listenzugriff gewähren, können zu unerwartet umfangreicheren Änderungen führen, wenn Objekte in dem Bucket mit häufig durch unbeabsichtigte Benutzer aufgeführt werden. Bucket-Berechtigungen, die allen Benutzern den Zugriff zum Hochladen/Löschen einräumen, bergen ein hohes Potenzial für Sicherheitsrisiken, indem alle Personen Elemente in einem Bucket hinzufügen, ändern oder löschen können. Die AWS Trusted Advisor-Prüfung untersucht explizite Bucket-Berechtigungen und zugeordnete Bucket-Richtlinien, die die Bucket-Berechtigungen möglicherweise überschreiben.	Ja	Ja	Ja	Nein (außer bei Partnerlösungen, die auf AWS ausgeführt werden, für die der S3-Service benötigt wird)	
1.20 Überwachungsmechanismus für die Erkennung von Änderungen in Amazon EC2-Instances und Containern	Alle Änderungen an Ihren Amazon EC2-Instances oder Containern weisen möglicherweise auf unberechtigte Aktivitäten hin. Als Mindestanforderung müssen diese Aktivitäten in Form eines Protokolls auf einen dauerhaften Speicherort abgelegt werden, um künftige forensische Untersuchungen zu ermöglichen. Der für den Zweck verwendete Mechanismus muss die folgenden Mindestanforderungen erfüllen: 1. Ermittlung von Änderungen am BS oder den Anwendungsdateien in den Amazon EC2-Instances oder Containern, die in der Lösung verwendet werden. 2. Speichern dieser Änderungen auf einem externen Speicherplatz außerhalb von der Amazon EC2-Instance oder dem Container. Beispiele für geeignete Mechanismen: a: Bereitstellung einer Dateiintegritätsprüfung über die geplante Konfigurationsverwaltung (e.g. Chef, Puppet usw.) oder ein spezielles Tool (z, B. OSSEC, Tripwire usw.,) oder b: Ausweitung der Konfigurationsverwaltungs-Tools auf die Validierung der Amazon EC2-Host-Konfiguration und Warnungen bei Aktualisierungen an wichtigen Konfigurationsdateien oder Paketen mit so genannten	Ja	Ja	Nein	Nein	

	Canary- (logged no-op)-Ereignissen, die konfiguriert werden, um sicherzustellen, dass der Service während der Laufzeit auf allen betroffenen Hosts betriebsbereit bleibt. c: Bereitstellung eines Systems zur Angriffserkennung auf dem Host, wie z. B. eine Open-Source-Lösung wie OSSEC with ElasticSearch and Kibana oder eine Partnerlösung. Beachten Sie, dass die folgenden Mechanismen diese Anforderung nicht erfüllen: Häufig geänderte Amazon EC2-Instances oder Container					
1.21 Klassifizierung aller Daten	Alle im Workload verarbeiteten und gespeicherten Kundendaten werden berücksichtigt und klassifiziert, um deren Vertraulichkeit und die entsprechenden Methoden für die Verarbeitung zu bestimmen.	Ja	Ja	Nein	Nein	
1.22 Verschlüsselung aller vertraulichen Daten	Alle als vertraulich klassifizierten Kunden werden bei der Übertragung und der Speicherung verschlüsselt.	Ja	Ja	Nein	Nein	
1.23 Sichere Verwaltung von kryptografischen Schlüsseln	Alle kryptografischen Schlüssel werden beim Speichern und der Übertragung verschlüsselt, und der Zugriff auf die Schlüssel wird über eine AWS-Lösung, wie z. B. KMS, oder eine APN-Partnerlösung, wie z. B. HashiCorp Vault, gesteuert.	Ja	Ja	Ja	Ja	
1.24 Verschlüsselung aller Daten während der Übertragung	Alle Daten, die über eine VPC-Grenze hinweg übertragen werden, werden verschlüsselt.	Ja	Ja	Ja	Ja	
1.25 Definition und Probe der Reaktion auf Sicherheitsvorfälle	Es muss ein Reaktionsprozess auf Sicherheitsvorfälle für die Behandlung von Vorfällen definiert werden, wie z. B. AWS-Kontokompromittierungen. Dieser Prozess muss getestet werden, indem Verfahren zum Proben der Vorfallsreaktion implementiert werden, z. B. durch das Absolvieren einer Sicherheitsübung im Rahmen eines Game Days. Eine solche Probe darf höchstens zwölf Monate her sein, um Folgendes zu bestätigen: a: Die richtigen Personen haben Zugang zur Umgebung. b: Es sind die richtigen Tools verfügbar. c: Die richtigen Personen wissen, was zu tun ist, um auf diverse und in diesem Plan dargestellte Sicherheitsvorfälle zu reagieren.	Ja	Ja	Nein	Nein	
2.0 Zuverlässigkeit Die Säule für Zuverlässigkeit setzt den Fokus auf die Fähigkeit, Ausfälle zu vermeiden bzw. sich schneller von aufgetretenen Ausfällen zu erholen, um damit die Anforderungen von Unternehmen und Kunden zu erfüllen. Zu den wichtigsten Themen gehören grundlegende Elemente rund um Einrichtung, projektübergreifende Anforderungen, Wiederherstellungsplanung und Änderungsverwaltung.						
2.1 Hohe Verfügbarkeit der Netzwerkkonnektivität	Die Netzwerkkonnektivität für die Lösung muss hochverfügbar sein. Wenn Sie VPN oder AWS Direct Connect zum Verbinden mit Kundennetzwerken verwenden, muss die Lösung redundante Verbindungen unterstützen, selbst wenn die Kunden diese nicht immer implementieren.	Ja	Ja	Ja	Ja	
2.2 Infrastrukturskalierungsmechanismen folgen Geschäftsanforderungen	Infrastrukturskalierungsmechanismen müssen Geschäftsanforderungen folgen. Dazu können Sie die folgenden Aktivitäten verwenden: 1. Implementieren von Auto Scaling-Mechanismen auf den einzelnen Ebenen der Architektur 2. Bestätigen, dass für aktuelle Geschäftsanforderungen, einschließlich Kostenanforderungen und erwarteter Anstieg der	Ja	Ja	Nein	Ja	

	Benutzeranzahl, keine Auto Scaling-Mechanismen benötigt werden und manuelle Skalierungsverfahren vollständig dokumentiert und häufig getestet werden.					
2.3 Zentrale Verwaltung von AWS- und Anwendungsprotokollen	Alle Protokollinformationen aus der Anwendung und aus der AWS-Infrastruktur müssen in ein System konsolidiert werden.	Ja	Ja	Nein	Nein	
2.4 Zentrale Verwaltung von Überwachung und Alarmen für AWS und Anwendungen	Die Anwendung und die AWS-Infrastruktur müssen zentral und auf Basis von Alarmen überwacht werden, die an das zuständige Ablaufpersonal gesendet werden.	Ja	Ja	Nein	Nein	
2.5 Automatisierung der Bereitstellung und Verwaltung der Infrastruktur	Die Lösung muss ein automatisiertes Tool, wie z. B. CloudFormation oder Terraform, für die Bereitstellung und Verwaltung der AWS-Infrastruktur verwenden. Die AWS-Konsole darf nicht für Routineänderungen an der AWS-Produktionsinfrastruktur verwendet werden.	Ja	Ja	Nein	Nein	
2.6 Regelmäßige Datensicherungen	Sie müssen regelmäßige Sicherungen auf einen dauerhaften Speicherservice durchführen. Mit Sicherungen können Sie sicherstellen, dass Sie die Möglichkeit haben, administrative, logische oder physische Fehlerszenarios zu beheben. Amazon S3 und Amazon Glacier sind die bevorzugten Services für Sicherung und Archivierung. Bei beiden Lösungen handelt es sich um dauerhafte und kostengünstige Speicherplattformen. Beide Lösungen bieten außerdem unbegrenzte Kapazität, und es entfällt die Volume- oder Datenträgerverwaltung, während das zu sichernde Datenaufkommen wächst. Durch das nutzungsabhängige Gebührenmodell und die geringen Kosten pro GB pro Monat eignen sich diese Services hervorragend für Anwendungsfälle im Bereich des Datenschutzes.	Ja	Ja	Nein	Nein	
2.7 Regelmäßige Tests der Wiederherstellungsmechanismen auf Basis eines Terminplans und nach signifikanten Änderungen an der Architektur	Sie müssen Wiederherstellungsmechanismen und -verfahren regelmäßig und nach signifikanten Änderungen an Ihrer Cloud-Umgebung testen. AWS bietet substanzielle Ressourcen, um Sie bei der Sicherung und Wiederherstellung Ihrer Daten zu unterstützen.	Ja	Ja	Nein	Nein	
2.8 Lösung bietet Ausfallsicherheit bei Unterbrechungen in Availability Zones	Die Lösung muss weiter funktionieren, wenn alle Services innerhalb einer Availability Zone unterbrochen sind.	Ja	Ja	Nein	Ja	
2.9 Ausfallsicherheit der Lösung getestet	Die Ausfallsicherheit der Infrastruktur bei Unterbrechungen in einer einzelnen Availability Zone wurde innerhalb der vergangenen zwölf Monate in der Produktion getestet, z. B. im Rahmen einer Übung an einem Game Day.	Ja	Ja	Nein	Ja	
2.10 Notfallwiederherstellung (DR) definiert	Ein gut strukturierter Notfallwiederherstellungsplan enthält einen Wiederherstellungszeitpunkt (RPO) und eine Wiederherstellungsdauer (RTO). Sie müssen einen RPO und eine RTO für alle betroffenen Services definieren, und der RPO und die RTO müssen mit dem SLA übereinstimmen, den Sie Ihren Kunden anbieten.	Ja	Ja	Nein	Nein	

2.11 Wiederherstellungsdauer (RTO) weniger als 24 Stunden	Als Grundanforderung sollte die Wiederherstellungsdauer (RTO) für Kernservices weniger als 24 Stunden betragen.	Ja	Ja	Nein	Nein	
2.12 Notfallwiederherstellungsplan ausreichend getestet	Ihr Notfallwiederherstellungsplan muss regelmäßig und nach wichtigen Aktualisierungen in Bezug auf Ihren Wiederherstellungszeitpunkt (RPO) und Ihre Wiederherstellungsdauer (RTO) getestet werden. Es muss mindestens ein Test der Notfallwiederherstellung vor der Genehmigung Ihrer AWS APN-Anwendung auf der Stufe "Advanced" abgeschlossen werden.	Ja	Ja	Nein	Nein	
2.13 Notfallwiederherstellungsplan enthält Wiederherstellung auf ein anderes AWS-Konto	Ihr Notfallwiederherstellungsplan muss eine Strategie für die Wiederherstellung auf ein anderes AWS-Konto enthalten, und im Rahmen Ihrer regelmäßigen Wiederherstellungstests muss dieses Szenario getestet werden. Sie haben in den vergangenen zwölf Monaten mindestens einen vollständigen Test des Notfallwiederherstellungsplans abgeschlossen, einschließlich mindestens einer Wiederherstellung auf ein anderes AWS-Konto. Hinweis: Obwohl Prozesse zur Wiederherstellung von Daten in Testumgebungen oder das Exportieren von Daten für Benutzer sinnvolle Möglichkeiten zur Überprüfung von Sicherungen darstellen, erfüllen diese Prozesse nicht die Anforderungen zum Ausführen einer vollständigen Wiederherstellung auf ein anderes AWS-Konto.	Ja	Ja	Nein	Nein	
3.0 Optimierung der Betriebsabläufe Die Säule zur Optimierung der Betriebsabläufe setzt den Fokus auf das Ausführen und Überwachen von Systemen für die Bereitstellung von geschäftlichem Nutzen und das kontinuierliche Verbessern von Prozessen und Abläufen. Die wichtigsten Themen umfassen die Verwaltung und Automatisierung von Änderungen, die Reaktion auf Ereignisse und das Definieren von Standards für die erfolgreiche Verwaltung von Routineabläufen.						
3.1 Bereitstellung von Code-Änderungen automatisiert	Die Lösung muss eine automatisierte Methode für die Bereitstellung von Code in die AWS-Infrastruktur verwenden. Interaktive SSH- oder RDP-Sitzungen dürfen nicht für die Bereitstellung von Aktualisierungen in die AWS-Infrastruktur verwendet werden.	Ja	Ja	Nein	Nein	
3.2 Runbooks und Eskalationsprozess definiert	Runbooks müssen entwickelt werden, um die Standardverfahren für die Reaktion auf verschiedene Anwendungen und AWS-Ereignisse zu definieren. Ein Eskalationsprozess muss definiert werden, um durch das System generierte Warnungen und Alarme zu behandeln und auf von Kunden gemeldete Vorfälle zu reagieren. Der Eskalationsprozess muss, wenn zutreffend, außerdem die Eskalation auf den AWS-Support umfassen.	Ja	Ja	Nein	Nein	
3.3 AWS Business Support für das AWS-Konto aktiviert	Business Support muss aktiviert werden. Business Support (oder höher) ist eine AWS-Partnernetzwerkanforderung für Technologiepartner auf der Stufe "Advanced". Um sich für die Stufe "Advanced" zu qualifizieren, müssen Sie Business Support auf mindestens einem Ihrer AWS-Konten aktivieren.	Ja	Ja	Nein	Nein	