AWS-Whitepaper

Erstellen von Architekturen für HIPAA-Sicherheit und -Compliance in Amazon Web Services

Erstellen von Architekturen für HIPAA-Sicherheit und -Compliance in Amazon Web Services: AWS-Whitepaper

Table of Contents

Erstellen von Architekturen für HIPAA-Sicherheit und -Compliance in Amazon Web Services

Veröffentlichungsdatum: 28. September 2022 (Dokumentversionen)

In diesem Dokument wird kurz beschrieben, wie Kunden Amazon Web Services (AWS) verwenden können, um sensible Workloads auszuführen, die nach dem U.S. Health Insurance Portability and Accountability Act (HIPAA) reguliert sind. Wir konzentrieren uns auf die HIPAA-Datenschutz- und Sicherheitsregeln zum Schutz geschützter Gesundheitsinformationen (Protected Health Information, PHI), auf die Verwendung von AWS zum Verschlüsseln von Daten während der Übertragung und im Ruhezustand und auf die Verwendung von AWS-Funktionen zum Ausführen von Workloads, die PHI enthalten.

Einführung

Der Health Insurance Portability and Accountability Act von 1996 (HIPAA) gilt für „gedeckte Unternehmen“ und „Geschäftspartner“. HIPAA wurde 2009 durch den Health Information Technology for Industry and Bol Health (HI) Act erweitert.

HIPAA und HI legen eine Reihe von Bundesstandards fest, um die Sicherheit und den Datenschutz von PHI zu schützen. HIPAA und HI legen Anforderungen im Zusammenhang mit der Verwendung und Offenlegung geschützter Gesundheitsdaten (PHI), angemessene Sicherheitsmaßnahmen zum Schutz von PHI, individuellen Rechten und administrativen Verantwortlichkeiten fest. Weitere Informationen zu HIPAA und HI finden Sie unter Home für den Datenschutz bei Gesundheitsinformationen.

abgedeckte Entitäten und ihre Geschäftspartner können die sicheren, skalierbaren und kostengünstigen IT-Komponenten von Amazon Web Services (AWS) verwenden, um Anwendungen im Einklang mit den HIPAA- und HI-Compliance-Anforderungen zu entwerfen. AWS bietet eine commercial-off-the-shelf Infrastrukturplattform mit branchenweit bekannten Zertifizierungen und Audits wie ISO 27001, FedRAMP und den Service Organization Control Reports (SOC1, SOC2 und SOC3). AWS-Services und -Rechenzentren verfügen über mehrere Ebenen betrieblicher und physischer Sicherheit, um die Integrität und Sicherheit von Kundendaten sicherzustellen. Ohne Mindestgebühren, ohne langfristige Verträge und pay-as-you-use mit Preisen ist AWS eine zuverlässige und effektive Lösung für das Wachstum von Anwendungen in der Gesundheitsbranche.

AWS ermöglicht es abgedeckten Entitäten und ihren Geschäftspartnern, die HIPAA unterliegen, PHI sicher zu verarbeiten, zu speichern und zu übertragen. Darüber hinaus bietet AWS seit Juli 2013 ein standardisiertes Business Associate Addendum (BAA) für diese Kunden. Kunden, die eine AWS BAA ausführen, können jeden AWS-Service in einem Konto verwenden, das als HIPAA-Konto festgelegt ist, aber sie können PHI nur mit den HIPAA-fähigen Services verarbeiten, speichern und übertragen, die in der AWS BAA definiert sind. Eine vollständige Liste dieser Services finden Sie auf der Seite Referenz für HIPAA-berechtigte Services.

AWS unterhält ein standardbasiertes Risikomanagementprogramm, um sicherzustellen, dass die HIPAA-fähigen Services speziell administrative, technische und physische HIPAA-Schutzmaßnahmen unterstützen. Die Verwendung dieser Services zum Speichern, Verarbeiten und Übertragen von PHI hilft unseren Kunden und AWS dabei, die HIPAA-Anforderungen zu erfüllen, die für das AWS Utility-basierte Betriebsmodell gelten.

Die BAA von AWS erfordert, dass Kunden PHI, die in HIPAA-fähigen Services gespeichert oder übertragen werden, gemäß den Anweisungen des Secretary of Health and Human Services (HHS) verschlüsseln: Anleitung zur Übermittlung ungesicherter geschützter Gesundheitsinformationen Unbrauchbar, Unlesbar oder Unentschlüsselbar für nicht autorisierte Personen („Guidance“. Bitte beziehen Sie sich auf diese Website, da sie aktualisiert werden kann und auf einer von HHS festgelegten (oder verwandten) Nachfolgerseite verfügbar gemacht werden kann.

AWS bietet eine umfassende Palette von Funktionen und Services, um die Schlüsselverwaltung und Verschlüsselung von PHI einfach zu verwalten und zu prüfen, einschließlich der AWS Key Management Service (AWS KMS). Kunden mit HIPAA-Compliance-Anforderungen haben eine große Flexibilität bei der Erfüllung der Verschlüsselungsanforderungen für PHI.

Bei der Entscheidung, wie die Verschlüsselung implementiert werden soll, können Kunden die Verschlüsselungsfunktionen auswerten und nutzen, die für die HIPAA-fähigen Services nativ sind. Oder Kunden können die Verschlüsselungsanforderungen auf andere Weise erfüllen, die den Anweisungen von HHS entspricht.

Verschlüsselung und Schutz von PHI in AWS

Die HIPAA-Sicherheitsregel enthält adressierbare Implementierungsspezifikationen für die Verschlüsselung von PHI bei der Übertragung („bei der Übertragung“) und im Speicher („beim Ruhezustand“) Obwohl es sich um eine adressierbare Implementierungsspezifikation in HIPAA handelt, verlangt AWS, dass Kunden PHI, die in HIPAA-fähigen Services gespeichert oder übertragen werden, gemäß den Anweisungen des Secretary of Health and Human Services (HHS) verschlüsseln: Anleitung zur Wiedergabe ungesicherter geschützter Gesundheitsinformationen, die für nicht autorisierte Personen unbrauchbar, unlesbar oder nicht entschlüsselbar sind („Richtlinie“). Bitte beziehen Sie sich auf diese Website, da sie aktualisiert werden kann und auf einem von HHS bestimmten Nachfolger (oder verwandten Standort) verfügbar gemacht werden kann.

AWS bietet eine umfassende Palette von Funktionen und Services, um die Schlüsselverwaltung und Verschlüsselung von PHI einfach zu verwalten und zu prüfen, einschließlich der AWS Key Management Service (AWS KMS). Kunden mit HIPAA-Compliance-Anforderungen haben eine große Flexibilität bei der Erfüllung der Verschlüsselungsanforderungen für PHI.

Bei der Entscheidung, wie die Verschlüsselung implementiert werden soll, können Kunden die für die HIPAA-fähigen Services nativen Verschlüsselungsfunktionen bewerten und nutzen oder die Verschlüsselungsanforderungen auf andere Weise erfüllen, die den Anweisungen von HHS entspricht. Die folgenden Abschnitte enthalten allgemeine Informationen zur Verwendung verfügbarer Verschlüsselungsfunktionen in jedem der HIPAA-fähigen Services und andere Muster für die Verschlüsselung von PHI und zur Verwendung von AWS KMS zum Verschlüsseln der Schlüssel, die für die Verschlüsselung von PHI in AWS verwendet werden können.

Themen

- Amazon CloudWatch -Protokolle
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB (mit MongoDB-Kompatibilität)
- Amazon DynamoDB
- Amazon Elastic Block Store
- Amazon Elastic Compute Cloud
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System (Amazon EFS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon ElastiCache für Redis
- Amazon OpenSearch Service
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- Amazon Managed Service für Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Streams
- Amazon Kinesis Video Streams
- Amazon Lex
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Amazon MQ
- Amazon Neptune

- AWS Netzwerk-Firewall
- Amazon Pinpoint
- Amazon Polly
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon QuickSight
- Amazon RDS für MariaDB
- Amazon RDS für MySQL
- Amazon RDS für Oracle
- Amazon RDS für PostgreSQL
- Amazon RDS für SQL Server
- Amazon Redshift
- Amazon Rekognition
- Amazon Route 53
- Amazon S3 Glacier
- Amazon S3 Transfer Acceleration
- Amazon SageMaker
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Email Service (Amazon SES)
- Amazon Simple Queue Service (Amazon SQS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Workflow Service
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud
- Amazon WorkDocs
- Amazon WorkSpaces
- AWS App Mesh
- AWS Application Migration Service

- AWS Auto Scaling
- AWS Backup
- AWS Batch
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodeCommit
- AWS CodePipeline
- AWS Config
- AWS Data Exchange
- AWS Database Migration Service
- AWS DataSync
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Elastic Disaster Recovery
- AWS Fargate
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS IoT Core und AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks für Chef Automate

- AWS OpsWorks für Puppet Enterprise
- AWS OpsWorks Stack
- AWS Organizations
- AWS RoboMaker
- AWS SDK-Metriken
- AWS Secrets Manager
- AWS Security Hub
- AWS Server Migration Service
- AWS Serverless Application Repository
- Servicekatalog
- AWS Shield
- AWS Snowball
- AWS Snowball Edge
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF – Firewall für Webanwendungen
- AWS X-Ray
- Elastic Load Balancing
- FreeRTOS
- Verwenden von AWS KMS für die Verschlüsselung von PHI
- VM Import/Export

Amazon API Gateway

Kunden können Amazon API Gateway verwenden, um geschützte Gesundheitsdaten (Protected Health Information, PHI) zu verarbeiten und zu übertragen. Während Amazon API Gateway automatisch HTTPS-Endpunkte für die Verschlüsselung während der Übertragung verwendet, können Kunden Nutzlasten auch clientseitig verschlüsseln. API Gateway übergibt alle nicht

zwischengespeicherten Daten über den Speicher und schreibt sie nicht auf die Festplatte. Kunden können AWS Signature Version 4 für die Autorisierung mit API Gateway verwenden. Weitere Informationen finden Sie hier:

- Häufig FAQs zu Amazon API Gateway: Sicherheit und Autorisierung
- Steuern und Verwalten des Zugriffs auf eine REST-API in API Gateway

Kunden können in jeden -Service integrieren, der mit API Gateway verbunden ist, vorausgesetzt, wenn PHI beteiligt ist, wird der Service in Übereinstimmung mit der -Anleitung und der BAA konfiguriert. Informationen zur Integration von API Gateway in Backend-Services finden Sie unter Einrichten von REST-API-Methoden in API Gateway.

Kunden können AWS CloudTrail und Amazon verwenden CloudWatch , um die Protokollierung zu aktivieren, die ihren Protokollierungsanforderungen entspricht. Stellen Sie sicher, dass alle über API Gateway gesendeten PHI (z. B. in Headern, URLs und Anfrage/Antwort) nur von HIPAA-fähigen Services erfasst werden, die so konfiguriert wurden, dass sie mit der -Anleitung übereinstimmen. Weitere Informationen zur Protokollierung mit API Gateway finden Sie unter Wie aktiviere ich CloudWatch Protokolle für die Fehlerbehebung bei meiner API-Gateway-REST-API oder WebSocket -API?

Amazon AppFlow

Amazon AppFlow ist ein vollständig verwalteter Integrationsservice, der es Kunden ermöglicht, Daten sicher zwischen S-Service (SaaS)oftware-as-a-Anwendungen wie Salesforce, Marketo, Slack und zu übertragen ServiceNow, und AWS-Services wie Amazon S3 und Amazon Redshift. AppFlow kann Datenströme mit einer vom Kunden gewählten Häufigkeit ausführen – nach einem Zeitplan, als Reaktion auf ein Geschäftsereignis oder auf Abruf. Kunden können auch Datentransformationsfunktionen wie Filterung und Validierung konfigurieren, um im Rahmen des Flows selbst ohne zusätzliche Schritte umfangreiche ready-to-use Daten zu generieren.

Amazon AppFlow kann verwendet werden, um Daten zu verarbeiten und zu übertragen, die PHI enthalten. Die Verschlüsselung von Daten während der Übertragung zwischen AppFlow und der konfigurierten Quelle/Ziel wird standardmäßig mit TLS 1.2 oder höher bereitgestellt. Daten, die im Ruhezustand in S3 gespeichert sind, werden automatisch mit einem - AWS KMS Schlüssel (früher CMK) verschlüsselt, der vom Kunden angegeben wird. Für PHI-Daten, die an Nicht-S3-Ziele übertragen werden, müssen Kunden sicherstellen, dass der Speicher im Ruhezustand für das gewählte Ziel ihren Sicherheitsanforderungen entspricht. AppFlow ermöglicht

die Anwendungsüberwachung, indem es mit integriert wird, AWS CloudTrail um API-Aufrufe zu protokollieren, und Amazon, EventBridge um Flow-Ausführungsereignisse auszugeben.

Amazon AppStream 2.0

Amazon AppStream 2.0 ist ein vollständig verwalteter Anwendungs-Streaming-Service. Kunden besitzen ihre Daten und müssen die erforderlichen Windows-Anwendungen so konfigurieren, dass sie ihren gesetzlichen Anforderungen entsprechen. Kunden können persistenten Speicher über Basisordner konfigurieren. Dateien und Ordner werden während der Übertragung über die SSL-Endpunkte von Amazon S3 verschlüsselt. Dateien und Ordner werden im Ruhezustand mit von Amazon S3-managed Verschlüsselungsschlüsseln verschlüsselt. Weitere Informationen finden Sie unter Aktivieren und Verwalten des persistenten Speichers für Ihre AppStream 2.0-Benutzer. Wenn Kunden eine Speicherlösung eines Drittanbieters verwenden, sind sie dafür verantwortlich, sicherzustellen, dass die Konfiguration dieser Lösung den Anleitungen entspricht. Die gesamte öffentliche API-Kommunikation mit Amazon AppStream 2.0 wird mit TLS verschlüsselt. Weitere Informationen finden Sie in der Amazon AppStream 2.0-Dokumentation.

Amazon AppStream 2.0 ist in integriert, einem Service AWS CloudTrail, der API-Aufrufe protokolliert, die von oder im Namen von Amazon AppStream 2.0 im AWS-Konto des Kunden getätigt wurden, und die Protokolldateien an den angegebenen Amazon S3 bucket. CloudTrail captures-API-Aufrufe übermittelt, die von der Amazon AppStream 2.0-Konsole oder von der Amazon AppStream 2.0-API aus getätigt wurden. Kunden können Amazon auch verwenden CloudWatch , um Metriken zur Ressourcennutzung zu protokollieren. Weitere Informationen finden Sie unter Überwachen von Amazon- AppStream 2.0-Ressourcen und Protokollieren von AppStream 2.0-API-Aufrufen mit AWS CloudTrail.

Amazon Athena

Amazon Athena ist ein interaktiver Abfrageservice, der die direkte Analyse von Daten in Amazon Simple Storage Service (Amazon S3) mit Standard-SQL erleichtert. Athena hilft Kunden bei der Analyse unstrukturierter, halbstrukturierter und strukturierter Daten, die in Amazon S3 gespeichert sind. Beispiele hierfür sind CSV und JSON oder spaltenbasierte Datenformate wie Apache Parquet und Apache ORC. Kunden können Athena verwenden, um Ad-hoc-Abfragen mit ANSI SQL auszuführen, ohne die Daten aggregieren oder in Athena laden zu müssen.

Amazon Athena kann jetzt verwendet werden, um Daten zu verarbeiten, die PHI enthalten. Die Verschlüsselung von Daten während der Übertragung zwischen Amazon Athena und S3 wird

standardmäßig mit SSL/TLS bereitgestellt. Die Verschlüsselung von PHI im Ruhezustand auf S3 sollte gemäß den Anleitungen im Abschnitt S3 durchgeführt werden. Die Verschlüsselung von Abfrageergebnissen von und innerhalb von Amazon Athena, einschließlich bereitgestellter Ergebnisse, sollte mit serverseitiger Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3), AWS KMS-verwalteten Schlüsseln (SSE-KMS) oder clientseitiger Verschlüsselung mit AWS KMS-verwalteten Schlüsseln (CSE-KMS) aktiviert werden. Amazon Athena verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

Amazon Aurora

Amazon Aurora ermöglicht es Kunden, Aurora-Datenbank-Cluster und Snapshots im Ruhezustand mit Schlüsseln zu verschlüsseln, die sie über verwalten AWS KMS. Auf einer Datenbank-Instance, die mit Amazon-Aurora-Verschlüsselung ausgeführt wird, werden im Ruhezustand im zugrunde liegenden Speicher gespeicherte Daten verschlüsselt, ebenso wie automatisierte Backups, Lesereplikate und Snapshots.

Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Amazon-Aurora-Verschlüsselung ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung im Ruhezustand mit Amazon Aurora finden Sie unter Schutz von Daten mithilfe der Verschlüsselung.

Verbindungen zu DB-Clustern, auf denen Aurora MySQL ausgeführt wird, müssen Transportverschlüsselung verwenden, wobei Secure Socket Layer (SSL) oder Transport Layer Security (TLS) verwendet wird. Weitere Informationen zur Implementierung von SSL/TLS finden Sie unter Verwenden von SSL/TLS mit Aurora MySQL-DB-Clustern.

Amazon Aurora PostgreSQL

Amazon Aurora ermöglicht es Kunden, Aurora-Datenbank-Cluster und Snapshots im Ruhezustand mit Schlüsseln zu verschlüsseln, die sie über verwalten AWS KMS. Auf einer Datenbank-Instance, die mit Amazon-Aurora-Verschlüsselung ausgeführt wird, werden im Ruhezustand im zugrunde liegenden Speicher gespeicherte Daten verschlüsselt, ebenso wie automatisierte Backups, Lesereplikate und Snapshots.

Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Amazon-Aurora-Verschlüsselung ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung im Ruhezustand mit Amazon Aurora finden Sie unter Schutz von Daten mithilfe der Verschlüsselung.

Verbindungen zu DB-Clustern, auf denen Aurora PostgreSQL ausgeführt wird, müssen Transportverschlüsselung verwenden, wobei Secure Socket Layer (SSL) oder Transport Layer Security (TLS) verwendet wird. Weitere Informationen zur Implementierung von SSL/TLS finden Sie unter Sichern von Aurora-PostgreSQL-Daten mit SSL.

Amazon CloudFront

Amazon CloudFront ist ein globaler Content Delivery Network (CDN)-Service, der die Bereitstellung von Kundenwebsites, APIs, Videoinhalten oder anderen Webressourcen beschleunigt. Es lässt sich in andere Amazon Web Services-Produkte integrieren, um Entwicklern und Unternehmen eine einfache Möglichkeit zu bieten, Inhalte für Endbenutzer ohne Mindestnutzungsverpflichtungen zu beschleunigen. Um die Verschlüsselung von PHI während der Übertragung mit sicherzustellen CloudFront, müssen Kunden so konfigurieren CloudFront , dass HTTPS end-to-end vom Ursprung zum Viewer verwendet wird.

Dazu gehört der Datenverkehr zwischen CloudFront und dem Viewer, die CloudFront Neuverteilung von einem benutzerdefinierten Ursprung und die CloudFront Verteilung von einem Amazon S3-Ursprung. Kunden sollten außerdem sicherstellen, dass die Daten am Ursprung verschlüsselt werden, um sicherzustellen, dass sie im Ruhezustand verschlüsselt bleiben, während sie in zwischengespeichert werden CloudFront. Wenn Amazon S3 als Ursprung verwendet wird, können Kunden serverseitige S3-Verschlüsselungsfunktionen nutzen. Wenn Kunden von einem benutzerdefinierten Ursprung verteilen, müssen sie sicherstellen, dass die Daten am Ursprung verschlüsselt werden.

Lambda@Edge

Lambda@Edge ist ein Datenverarbeitungsservice, der die Ausführung von Lambda-Funktionen an AWS-Edge-Standorten ermöglicht. Lambda@Edge kann verwendet werden, um Inhalte anzupassen, die über bereitgestellt werden CloudFront. Wenn Lambda@Edge mit PHI verwendet wird, sollten Kunden die Anleitung zur Verwendung von befolgen CloudFront. Alle Verbindungen zu und von Lambda@Edge sollten mit HTTPS oder SSL/TLS verschlüsselt werden.

Amazon CloudWatch

Amazon CloudWatch ist ein Überwachungsservice für AWS Cloud-Ressourcen und die Anwendungen, die Kunden auf AWS ausführen. Kunden können Amazon verwenden, CloudWatch um Metriken zu erfassen und zu verfolgen, Protokolldateien zu erfassen und zu überwachen und

Alarme einzurichten. Amazon CloudWatch selbst erzeugt, speichert oder überträgt PHI nicht. Kunden können CloudWatch API-Aufrufe mit überwachen AWS CloudTrail. Weitere Informationen finden Sie unter Protokollieren von Amazon CloudWatch -API-Aufrufen mit AWS CloudTrail.

Weitere Informationen zu den Konfigurationsanforderungen finden Sie im Abschnitt Amazon CloudWatch Logs.

Amazon CloudWatch -Ereignisse

Amazon CloudWatch Events liefert einen near-real-time Stream von Systemereignissen, die Änderungen an AWS-Ressourcen beschreiben. Kunden sollten sicherstellen, dass PHI nicht in CloudWatch Ereignisse fließt, und dass jede AWS-Ressource, die ein CloudWatch Ereignis ausgibt, das PHI speichert, verarbeitet oder überträgt, gemäß der -Anleitung konfiguriert ist.

Kunden können Amazon CloudWatch Events so konfigurieren, dass sie sich als AWS-API-Aufruf in registrieren CloudTrail. Weitere Informationen finden Sie unter Erstellen einer CloudWatch Ereignisregel, die bei einem AWS-API-Aufruf mit ausgelöst wird AWS CloudTrail.

Amazon CloudWatch -Protokolle

Kunden können Amazon CloudWatch Logs verwenden, um ihre Protokolldateien von Amazon Elastic Compute Cloud (Amazon EC2)-Instances, AWS CloudTrail Amazon Route 53 und anderen Quellen zu überwachen, zu speichern und darauf zuzugreifen. Anschließend können sie die zugehörigen Protokolldaten aus - CloudWatch Protokollen abrufen. Protokolldaten werden während der Übertragung und im Ruhezustand verschlüsselt. Daher ist es nicht erforderlich, PHI, die von einem anderen -Service ausgegeben und an - CloudWatch Protokolle übermittelt werden, erneut zu verschlüsseln.

Amazon Comprehend

Amazon Comprehend verwendet die natürliche Sprachverarbeitung, um Erkenntnisse in den Inhalt von Dokumenten zu gewinnen. Amazon Comprehend verarbeitet jede Textdatei im UTF-8-Format. Durch die Erkennung von Einheiten, Schlüsselphrasen, Sprache, Gefühlen und anderen gängigen Elementen eines Dokuments verschafft Amazon Comprehend Einblicke in den Inhalt von Dokumenten. Amazon Comprehend kann mit Daten verwendet werden, die PHI enthalten. Amazon Comprehend speichert oder speichert keine Daten und alle Aufrufe der API werden mit SSL/TLS verschlüsselt. Amazon Comprehend verwendet CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Identity and Access Management

Sicherheitszugriffsfunktionen wie Authentifizierung und Autorisierung sind für den Zugriff auf Amazon Comprehend erforderlich und können mit AWS Identity and Access Management (IAM) gesteuert werden. Anmeldeinformationen können für den Zugriff auf das IAM verwendet werden. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für Amazon Comprehend im Amazon Comprehend-Benutzerhandbuch.

Kontoverwaltung

Standardmäßig haben IAM-Benutzer keine Berechtigung zum Erstellen oder Ändern von Amazon Comprehend-Ressourcen oder zum Ausführen von Aufgaben mit der Amazon Comprehend-API. Damit Benutzer Ressourcen erstellen oder ändern und Aufgaben ausführen können, sind Kunden dafür verantwortlich, IAM-Richtlinien zu nutzen, die Benutzern Berechtigungen für die spezifischen Ressourcen (wie Amazon Comprehend und API-Aktionen) gewähren, die Benutzer verwenden müssen, und dann Richtlinien an die Benutzer oder Gruppen anzufügen, die bestimmte Berechtigungen benötigen.

Mit Amazon Comprehend können Sie AWS Identity and Access Management (IAM) verwenden, um einen Benutzer mit einer angehängten Richtlinie zu erstellen, um Amazon Comprehend-Berechtigungen zu aktivieren. Optional können Sie benutzerdefinierte Richtlinien erstellen, die einer Rolle zugeordnet werden sollen. Anschließend können Sie der Rolle Administratoren hinzufügen, die in der Lage sind, die APIs für die Amazon Comprehend-Verwaltung gemäß den von der Organisation definierten rollenbasierten Zugriffs- und geringsten Berechtigungsprinzipien aufzurufen.

Identität und Zugriff

Mit Amazon Comprehend können Sie verlangen, dass sich Benutzer bei AWS mithilfe der Multi-Faktor-Authentifizierung gemäß ihren organisatorischen Anforderungen für die Authentifizierung authentifizieren.

Mit der können AWS Management Console IAM-Administratoren eine vom Kunden verwaltete Richtlinie erstellen, die alle Berechtigungen verweigert, mit Ausnahme derer, die erforderlich sind, damit Benutzer ihre eigenen Anmeldeinformationen und MFA-Geräte verwalten können. Eine JSON-Richtlinienvorlage ist auf der Seite Meine Sicherheitsanmeldeinformationen in der IAM-Konsole verfügbar.

Optional können Sie kompatible MFA-Funktionen von Drittanbietern mit IAM-Partnern nutzen. Weitere Informationen finden Sie unter IAM-Partner.

Administration

Wir empfehlen, dass Sie Amazon Comprehend identitätsbasierte Richtlinien auswählen, in denen Kontoadministratoren IAM-Identitäten (Benutzern, Gruppen und Rollen) Berechtigungsrichtlinien zuweisen und somit Berechtigungen zum Ausführen von Vorgängen an Amazon Comprehend-Ressourcen erteilen können.

Eine Liste der API-Aktionen für Amazon Comprehend finden Sie im API-Referenzhandbuch für . Sie sollten auch erwägen, den Zugriff auf vordefinierte IAM-Richtlinien, Kunden-IAM-Richtlinien und API-Aktionen für Benutzer oder Rollen gemäß ihren geringsten Berechtigungen und rollenbasierten Organisationsanforderungen zu autorisieren. Weitere Informationen finden Sie unter Verwenden der Amazon Comprehend API im Entwicklerhandbuch für .

Externe Authentifizierung

Amazon Comprehend ist mit dem Identitätsverbund mithilfe von IAM-Rollen kompatibel. Auf diese Weise können sich Ihre Benutzer bei Amazon Comprehend authentifizieren, AWS indem sie eine Rolle übernehmen, die Administratoren bereitgestellt haben. Benutzer, die AWS mit Anmeldeinformationen von ihrer Organisation oder einem Drittanbieter auf zugreifen, übernehmen indirekt eine Rolle.

AWS -Unterstützung für Kerberos und Active Directory bietet die Vorteile von Single Sign-On und zentralisierter Authentifizierung von Datenbankbenutzern. - AWS Benutzer können Benutzeranmeldeinformationen entweder in AWS Directory Service für Microsoft Active Directory oder im On-Premises-Active-Directory des Kunden verwalten und speichern.

Durchsetzung des Datenflusses

AWS -Kunden und APN-Partner, die entweder als Datenverantwortliche oder als Datenverarbeiter fungieren, sind für alle personenbezogenen Daten verantwortlich, die sie in der AWS Cloud und Amazon Comprehend speichern. Sie sind dafür verantwortlich, den Fluss zu Dateneingaben und -ausgaben für Amazon Comprehend mithilfe von IAM-Richtlinien zu steuern.

Datenschutz und Verwaltung von Geheimnissen

Das - AWS Modell der geteilten Verantwortung gilt für den Datenschutz in Amazon Comprehend . Wie in diesem Modell beschrieben, AWS ist für den Schutz der globalen Infrastruktur verantwortlich, die die gesamte AWS Cloud betreibt. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Dieser Inhalt umfasst die Sicherheitskonfigurations-

und Verwaltungsaufgaben für die von Ihnen verwendeten AWS Services. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz.

Der Abschnitt Datenschutz in Amazon Comprehend im Entwicklerhandbuch für Amazon Comprehend enthält Tipps, die Sie beim Schutz von Daten wie der Verwendung von TLS für die Übertragung und der Vermeidung der Platzierung vertraulicher Informationen in Tags oder Freiformfeldern berücksichtigen sollten.

Verschlüsselung von data-at-rest

Amazon Comprehend arbeitet mit AWS Key Management Service (AWS KMS), um eine erweiterte Verschlüsselung für Ihre Daten bereitzustellen. Mit Amazon Simple Storage Service (Amazon S3) können Sie Ihre Eingabedokumente bereits verschlüsseln, wenn Sie eine Textanalyse, Themenmodellierung oder einen benutzerdefinierten Amazon Comprehend-Auftrag erstellen. Durch die Integration mit AWS KMS können Sie die Daten im Speichervolume für start*- und create*-Aufträge verschlüsseln und die Ausgabeergebnisse von start*-Aufträgen mit Ihrem eigenen AWS KMS Schlüssel verschlüsseln.

Es hat sich bewährt, dass Amazon Comprehend-Benutzer Amazon S3-Buckets, die für Eingabedokumente verwendet werden, mit verfügbaren S3-Verschlüsselungslösungen gemäß ihren Organisationsrichtlinien verschlüsseln.

Das AWS Management Console verschlüsselt benutzerdefinierte Amazon Comprehend-Modelle mit einem eigenen AWS KMS Schlüssel. Für die kann AWS CLI Amazon Comprehend benutzerdefinierte Modelle entweder mit einem eigenen AWS KMS Schlüssel oder einem bereitgestellten kundenverwalteten Schlüssel (CMK) verschlüsseln.

Wenn Sie die Verschlüsselung bei Verwendung der auswählen AWS Management Console, können Sie eine oder beide der folgenden optionalen Methoden auswählen:

- Volume-Verschlüsselung – stellt sicher, dass die Daten auf einem von Comprehend verwendeten EBS-Volume während des Trainings/der Inferenz verschlüsselt werden (Daten werden nach dem Training/der Inferenz geleert, sodass dieser Schlüssel nur relevant ist, während der Auftrag ausgeführt wird).
- Ausgabeergebnisverschlüsselung – zum Verschlüsseln der von Comprehend gespeicherten Ausgabe im Kunden-Bucket mit einem vom Kunden bereitgestellten AWS KMS Schlüssel.

Weitere Informationen zu Verschlüsselungstypen wie Volume-Verschlüsselung finden Sie unter AWS KMS Verschlüsselung in Amazon Comprehend.

Persönlich identifizierbare Informationen

Sie können die Amazon Comprehend-Konsole oder APIs verwenden, um persönlich identifizierbare Informationen (PII) in englischen Textdokumenten zu erkennen. Weitere Informationen zum Erkennen und Beschriften von PII-Entitäten und zum Betrieb verschiedener PII-Analyseaufträge finden Sie im Abschnitt Persönlich identifizierbare Informationen im Amazon Comprehend-Entwicklerhandbuch.

Löschen von Daten

Wenn Sie ein Amazon Comprehend-Kunde sind, der Amazon S3 verwendet und sich dafür entscheidet, Ihre eigenen AWS KMS Schlüssel zu verwalten, sollten Sie erwägen, AWS KMS Schlüssel zu widerrufen und die Verfahrensgrundlage dafür entsprechend ihren organisatorischen Anforderungen zu definieren. Durch den Widerruf des AWS KMS Schlüssels für Amazon S3 werden alle Daten unbrauchbar/unlesbar.

Netzwerksegmentierung und -härteung

Als verwalteter Service folgt Amazon Comprehend den AWS bewährten Methoden für Sicherheit, Identität und Compliance.

Empfohlene Sicherheitsvorkehrungen für das Netzwerk finden Sie unter Infrastruktursicherheit in Amazon Comprehend im Entwicklerhandbuch für Amazon Comprehend.

Schützen von Aufträgen mit einer Amazon Virtual Private Cloud (Amazon VPC)

Amazon Comprehend verwendet eine Vielzahl von Sicherheitsmaßnahmen, um die Sicherheit Ihrer Daten mit unseren Auftragscontainern zu gewährleisten, in denen sie gespeichert werden, während sie von Amazon Comprehend verwendet werden. Auftragscontainer greifen jedoch über das Internet auf AWS Ressourcen zu, z. B. auf die Amazon S3-Buckets, in denen Sie Daten speichern, und Modellartefakte.

Um den Zugriff auf Ihre Daten zu steuern, empfehlen wir Ihnen, eine Virtual Private Cloud (VPC) zu erstellen und sie so zu konfigurieren, dass die Daten und Container nicht über das Internet zugänglich sind. Informationen zum Erstellen und Konfigurieren einer VPC finden Sie unter Erste Schritte mit Amazon VPC im Amazon VPC Benutzerhandbuch. Die Verwendung einer VPC trägt zum Schutz Ihrer Daten bei, da Sie Ihre VPC so konfigurieren können, dass sie nicht mit dem Internet verbunden ist. Mit einer VPC können Sie auch den gesamten Netzwerkverkehr in und aus unseren Auftragscontainern mithilfe von VPC-Flow-Protokollen überwachen. Weitere Informationen finden Sie unter VPC-Flow-Protokolle im Amazon-VPC-Benutzerhandbuch.

Sie geben Ihre VPC-Konfiguration an, wenn Sie einen Auftrag erstellen, indem Sie die Subnetze und Sicherheitsgruppen angeben. Wenn Sie die Subnetze und Sicherheitsgruppen angeben, erstellt Amazon Comprehend Elastic Network-Schnittstellen (ENIs), die Ihren Sicherheitsgruppen in einem der Subnetze zugeordnet sind. ENIs ermöglichen es unseren Auftragscontainern, eine Verbindung zu Ressourcen in Ihrer VPC herzustellen. Weitere Informationen über ENIs finden Sie unter Elastic-Network-Schnittstellen im Amazon-VPC-Benutzerhandbuch.

> **Note**
>
> Bei -Aufträgen können Sie Subnetze nur mit einer Standard-Tenancy-VPC konfigurieren, in der Ihre Instance auf gemeinsam genutzter Hardware ausgeführt wird. Weitere Informationen zum Tenancy-Attribut für VPCs finden Sie unter Dedicated Instances im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Sie können eine private Verbindung zwischen Ihrer VPC und Amazon Comprehend herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt erstellen. Weitere Informationen finden Sie unter Amazon Comprehend und Schnittstellen-VPC-Endpunkte (AWS PrivateLink).

Host- und Image-Härtung

Basierend auf dem AWS Modell der geteilten Verantwortung wird die Host- und Image-Härtung der AWS Umgebung für Amazon Comprehend von AWS als bereitgestellter Service verwaltet.

Mehrmandantenfähigkeit

Um Ihre Empfehlung sicherer zu gestalten, empfehlen wir Ihnen, die folgenden Sicherheitsempfehlungen für mehrere Mandanten zu implementieren:

- Verwenden Sie nur eine verifizierte E-Mail-Adresse, um den Benutzerzugriff auf einen Mandanten basierend auf Domänenübereinstimmung zu autorisieren. Vertrauen Sie E-Mail-Adressen und Telefonnummern nur, wenn Ihre App sie überprüft oder der externe IdP Ihnen einen Nachweis über die Überprüfung erteilt. Weitere Details zum Festlegen dieser Berechtigungen finden Sie unter Attributberechtigungen und -bereiche.
- Verwenden Sie unveränderliche oder veränderliche Attribute für die Benutzerprofilattribute, die Mandanten identifizieren. Administratoren müssen diese Attribute ändern können. Ermöglichen Sie App-Clients schreibgeschützten Zugriff auf die Attribute.

- Verwenden Sie ein 1:1-Mapping zwischen dem externen IdP und dem Anwendungsclient, um einen nicht autorisierten mandantenübergreifenden Zugriff zu verhindern. Ein Benutzer, der von einem externen Identitätsanbieter authentifiziert wurde und über ein gültiges Amazon-Cognito-Sitzungscookie verfügt, kann auf andere Mandanten-Apps zugreifen, die demselben Identitätsanbieter vertrauen.
- Stellen Sie beim Implementieren von Mandantenübereinstimmungs- und Autorisierungslogik in Ihrer Anwendung sicher, dass die Kriterien, die zum Autorisieren des Benutzerzugriffs auf die Mandanten verwendet werden, nicht von den Benutzern selbst geändert werden können. Wenn ein externer IdP für den Verbund verwendet wird, beschränken Sie die Mandantenidentitätsanbieter-Administratoren, damit sie den Benutzerzugriff nicht ändern können.

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem mit mehreren Mandanten, bei dem eine Entität, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere Entität zwingen kann, die Aktion auszuführen. In kann ein AWS serviceübergreifender Identitätswechsel zu einem Confused-Deputy-Problem führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der Anruf-Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, AWS stellt Tools bereit, mit denen Sie Ihre Daten für alle Services mit Service-Prinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben. Weitere Informationen, die Schutzmaßnahmen beinhalten, die Sie bei der Behebung dieses Sicherheitsproblems berücksichtigen sollten, finden Sie unter Serviceübergreifende Prävention verwirrter Stellvertreter im Amazon Comprehend-Entwicklerhandbuch.

Amazon Comprehend Medical

Anleitungen finden Sie im vorherigen Amazon Comprehend Abschnitt.

Amazon Connect

Amazon Connect ist ein cloudbasierter Self-Service-Kontaktcenter-Service, der dynamisches, persönliches und natürliches Kundeninteragieren in jeder Größenordnung ermöglicht. Kunden sollten keine PHI in Felder aufnehmen, die mit der Verwaltung von Benutzern, Sicherheitsprofilen und Kontaktabläufen in Amazon Connect verbunden sind.

Amazon Connect Customer Profiles, eine Funktion von Amazon Connect, bietet Kundendienstmitarbeitern im Kontaktcenter eine einheitlichere Ansicht des Profils eines Kunden mit den aktuellsten Informationen, um einen personalisierteren Kundenservice zu bieten. Customer Profiles wurde entwickelt, um Kundeninformationen aus mehreren Anwendungen automatisch zu einem einheitlichen Kundenprofil zusammenzuführen und das Profil direkt an den Kundendienstmitarbeiter zu übermitteln, sobald der Support-Anruf oder die Interaktion beginnt. Kunden sollten davon abraten, Domains oder Objektschlüssel mit PHI-Daten zu benennen. Der Inhalt von Domains und Objekten ist verschlüsselt und geschützt, die Schlüsselkennungen jedoch nicht.

Amazon DocumentDB (mit MongoDB-Kompatibilität)

Amazon DocumentDB (mit MongoDB-Kompatibilität) (Amazon DocumentDB) bietet Verschlüsselung im Ruhezustand während der Clustererstellung über AWS KMS, sodass Kunden Datenbanken mit AWS- oder vom Kunden verwalteten Schlüsseln verschlüsseln können. Auf einer Datenbank-Instance, die mit aktivierter Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand gespeichert werden, gemäß der zum Zeitpunkt der Veröffentlichung dieses Whitepapers geltenden -Anleitung verschlüsselt, ebenso wie automatisierte Backups, Lesereplikate und Snapshots. Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Amazon DocumentDB-Verschlüsselung ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung von Daten im Ruhezustand mit Amazon DocumentDB finden Sie unter Verschlüsseln von Amazon DocumentDB-Daten im Ruhezustand.

Verbindungen zu Amazon DocumentDB, die PHI enthalten, müssen Endpunkte verwenden, die verschlüsselten Transport (HTTPS) akzeptieren. Standardmäßig akzeptiert ein neu erstellter Amazon DocumentDB-Cluster nur sichere Verbindungen mit Transport Layer Security (TLS). Weitere Informationen finden Sie unter Verschlüsseln von Daten während der Übertragung. Amazon DocumentDB verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren. Weitere Informationen finden Sie unter Protokollierung und Überwachung in Amazon DocumentDB.

Für bestimmte Verwaltungsfunktionen verwendet Amazon DocumentDB Betriebstechnologie, die mit Amazon RDS geteilt wird. Aufrufe über die Amazon DocumentDB-Konsole, die AWS CLI und die API werden als Aufrufe der Amazon RDS-API protokolliert.

Amazon DynamoDB

Verbindungen zu Amazon DynamoDB, die PHI enthalten, müssen Endpunkte verwenden, die verschlüsselten Transport (HTTPS) akzeptieren. Eine Liste der regionalen Endpunkte finden Sie unter AWS-Service-Endpunkte.

Amazon DynamoDB bietet DynamoDB-Verschlüsselung, mit der Kunden Datenbanken mit Schlüsseln verschlüsseln können, die Kunden über verwalten AWS KMS. Auf einer Datenbank-Instance, die mit Amazon-DynamoDB-Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand im zugrunde liegenden Speicher gespeichert sind, in Übereinstimmung mit der -Anleitung verschlüsselt, die zum Zeitpunkt der Veröffentlichung dieses Whitepapers in Kraft war, ebenso wie automatisierte Backups, Lesereplikate und Snapshots.

Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Amazon-DynamoDB-Verschlüsselung ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung im Ruhezustand mit Amazon DynamoDB finden Sie unter DynamoDB-Verschlüsselung im Ruhezustand.

Amazon Elastic Block Store

Die Amazon-EBS-Verschlüsselung im Ruhezustand entspricht der -Anleitung, die zum Zeitpunkt der Veröffentlichung dieses Whitepapers in Kraft ist. Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Amazon-EBS-Verschlüsselung ihre Compliance- und regulatorischen Anforderungen erfüllt. Mit der Amazon-EBS-Verschlüsselung wird für jedes EBS-Volume ein eindeutiger Volume-Verschlüsselungsschlüssel generiert. Kunden haben die Flexibilität zu wählen, welcher KMS-Schlüssel aus dem zur Verschlüsselung der einzelnen Volume-Schlüssel verwendet AWS Key Management Service wird. Weitere Informationen finden Sie unter Amazon-EBS-Verschlüsselung.

Amazon Elastic Compute Cloud

Amazon EC2 ist ein skalierbarer, vom Benutzer konfigurierbarer Datenverarbeitungsservice, der mehrere Methoden zur Verschlüsselung von Daten im Ruhezustand unterstützt. Kunden können sich beispielsweise dafür entscheiden, PHI auf Anwendungs- oder Feldebene zu verschlüsseln, während es innerhalb einer Anwendung oder Datenbankplattform verarbeitet wird, die in einer Amazon EC2 gehostet wird. Die Ansätze reichen von der Verschlüsselung von Daten mit Standardbibliotheken in einem Anwendungs-Framework wie Java oder .NET, der Nutzung von Transparent Data Encryption-Funktionen in Microsoft SQL oder Oracle oder durch die Integration anderer Drittanbieter- und Software-as-a-Service (SaaS)-basierter Lösungen in ihre Anwendungen.

Kunden können ihre Anwendungen, die in Amazon EC2 ausgeführt werden, in AWS KMS SDKs integrieren, wodurch der Prozess der Schlüsselverwaltung und -speicherung vereinfacht wird. Kunden können auch die Verschlüsselung von Daten im Ruhezustand mit FDE (FDE) auf Dateiebene

oder Volldatenverschlüsselung implementieren, indem sie Software von Drittanbietern von -AWS Marketplace Partnern oder native Dateisystemverschlüsselungstools (z. B. dm-crypt, LUKS usw.) verwenden.

Netzwerkverkehr, der PHI enthält, muss Daten während der Übertragung verschlüsseln. Für den Datenverkehr zwischen externen Quellen (z. B. dem Internet oder einer herkömmlichen IT-Umgebung) und Amazon EC2 sollten Kunden offene Standard-Transportverschlüsselungsmechanismen wie Transport Layer Security (TLS) oder IPsec Virtual Private Networks (VPNs) verwenden, die mit der -Anleitung übereinstimmen. Intern in einer Amazon Virtual Private Cloud (VPC) für Daten, die zwischen Amazon EC2-Instances übertragen werden, muss der Netzwerkdatenverkehr, der PHI enthält, ebenfalls verschlüsselt sein. Die meisten Anwendungen unterstützen TLS oder andere Protokolle, die während der Übertragung bereitgestellt werden und so konfiguriert werden können, dass sie mit der -Anleitung übereinstimmen. Für Anwendungen und Protokolle, die keine Verschlüsselung unterstützen, können Sitzungen, die PHI übertragen, über verschlüsselte Tunnel mit IPsec oder ähnlichen Implementierungen zwischen Instances gesendet werden.

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) ist in Amazon Elastic Container Service (Amazon ECS) integriert und ermöglicht es Kunden, Container-Images für Anwendungen, die auf Amazon ECS ausgeführt werden, einfach zu speichern, auszuführen und zu verwalten. Nachdem Kunden das Amazon-ECR-Repository in ihrer Aufgabendefinition angegeben haben, ruft Amazon ECS die entsprechenden Images für ihre Anwendungen ab.

Für die Verwendung von Amazon ECR mit Container-Images, die PHI enthalten, sind keine besonderen Schritte erforderlich. Container-Images werden während der Übertragung verschlüsselt und im Ruhezustand mit serverseitiger Amazon S3-S3-Verschlüsselung (SSE-S3) verschlüsselt gespeichert.

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer, leistungsstarker Container-Management-Service, der Docker-Container unterstützt und es Kunden ermöglicht, Anwendungen einfach auf einem verwalteten Cluster von Amazon EC2 auszuführen. Amazon ECS macht es Kunden überflüssig, ihre eigene Cluster-Verwaltungsinfrastruktur zu installieren, zu betreiben und zu skalieren.

Mit einfachen API-Aufrufen können Kunden Docker-fähige Anwendungen starten und stoppen, den vollständigen Status ihres Clusters abfragen und auf viele vertraute Funktionen wie Sicherheitsgruppen, Elastic Load Balancing, EBS-Volumes und IAM-Rollen zugreifen. Kunden können Amazon ECS verwenden, um die Platzierung von Containern in ihrem Cluster basierend auf ihren Ressourcenanforderungen und Verfügbarkeitsanforderungen zu planen.

Die Verwendung von ECS mit Workloads, die PHI verarbeiten, erfordert keine zusätzliche Konfiguration. ECS fungiert als Orchestrierungsservice, der den Start von Containern (Bilder, für die in S3 gespeichert sind) auf EC2 koordiniert und nicht mit oder auf Daten innerhalb des zu orchestrierenden Workloads arbeitet. Im Einklang mit den HIPAA-Vorschriften und dem AWS Business Associate Addendum sollte PHI während der Übertragung und im Ruhezustand verschlüsselt werden, wenn auf Container zugegriffen wird, die mit ECS gestartet wurden. Bei jeder AWS Speicheroption (z. B. S3, EBS und KMS) sind verschiedene Mechanismen für die Verschlüsselung im Ruhezustand verfügbar. Die Sicherstellung der vollständigen Verschlüsselung von PHI, die zwischen Containern gesendet werden, kann Kunden auch dazu führen, ein Overlay-Netzwerk (z. B. VNS3, Weave Net oder ähnliches) bereitzustellen, um eine redundante Verschlüsselungsebene bereitzustellen. Die vollständige Protokollierung sollte jedoch auch aktiviert sein (z. B. über CloudTrail), und alle Container-Instance-Protokolle sollten an weitergeleitet werden CloudWatch.

Die Verwendung von Firelens und AWS für Fluent Bit mit Workloads, die PHI verarbeiten, erfordert keine zusätzliche Konfiguration, es sei denn, die Protokolle enthalten PHI. Wenn Protokolle PHI enthalten, sollten sie nicht an Protokolldateien ausgegeben werden, es sei denn, die Festplattenverschlüsselung ist aktiviert. Konfigurieren Sie stattdessen Ihre Anwendung so, dass Protokolle an den Standardausgang/-fehler ausgegeben werden, der automatisch von erfasst wird FireLens. Aktivieren Sie in ähnlicher Weise keine Dateipufferung für Fluent Bit, es sei denn, die Festplattenverschlüsselung ist ebenfalls aktiviert. Schließlich muss das Protokollziel unterstützen encryption-in-transit. Alle AWS Service-Ausgabe-Plugins in AWS für Fluent Bit verwenden immer TLS-Verschlüsselung, um Protokolle zu exportieren.

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) bietet einfachen, skalierbaren elastischen Dateispeicher für die Verwendung mit AWS Cloud-Services und On-Premises-Ressourcen. Es ist einfach zu bedienen und bietet eine einfache Oberfläche, mit der Kunden Dateisysteme schnell und einfach erstellen und konfigurieren können. Amazon EFS ist so konzipiert, dass es bei Bedarf elastisch skaliert werden kann, ohne Anwendungen zu unterbrechen. Es wird automatisch erweitert und verkleinert, wenn Kunden Dateien hinzufügen und entfernen.

Um die Anforderung zu erfüllen, dass PHI im Ruhezustand verschlüsselt werden, sind zwei Pfade auf EFS verfügbar. EFS unterstützt die Verschlüsselung im Ruhezustand, wenn ein neues Dateisystem erstellt wird. Während der Erstellung sollte die Option „Verschlüsselung von Daten im Ruhezustand aktivieren“ ausgewählt werden. Die Auswahl dieser Option stellt sicher, dass alle im EFS-Dateisystem platzierten Daten mit AES-256-Verschlüsselung und von AWS KMS verwalteten Schlüsseln verschlüsselt werden. Kunden können alternativ Daten verschlüsseln, bevor sie in EFS platziert werden. Sie sind dann jedoch für die Verwaltung des Verschlüsselungsprozesses und der Schlüsselverwaltung verantwortlich.

PHI sollte nicht als ganzer oder teilweiser Dateiname oder Ordnername verwendet werden. Die Verschlüsselung von PHI während der Übertragung für Amazon EFS wird von Transport Layer Security (TLS) zwischen dem EFS-Service und der Instance bereitgestellt, die das Dateisystem mountet. EFS bietet eine Mountinghilfe, um die Verbindung mit einem Dateisystem mithilfe von TLS zu erleichtern. Standardmäßig wird TLS nicht verwendet und muss aktiviert werden, wenn das Dateisystem mit der EFS-Mountinghilfe gemountet wird. Stellen Sie sicher, dass der Mounting-Befehl die Option „-o tls“ enthält, um die TLS-Verschlüsselung zu aktivieren. Alternativ können Kunden, die die EFS-Mountinghilfe nicht verwenden möchten, die Anweisungen in der EFS-Dokumentation befolgen, um ihre NFS-Clients für die Verbindung über einen TLS-Tunnel zu konfigurieren.

Amazon Elastic Kubernetes Service (Amazon EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) ist ein verwalteter Service, der es Kunden erleichtert, Kubernetes auf AWS auszuführen, ohne ihre eigene Kubernetes-Steuerebene einrichten oder warten zu müssen. Kubernetes ist ein Open-Source-System zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von Anwendungen in Containern. Weitere Informationen zur Sicherheit und Compliance finden Sie im Whitepaper Architekturerstellung für HIPAA-Sicherheit und -Compliance in Amazon EKS.

Amazon ElastiCache für Redis

Amazon ElastiCache for Redis ist ein Redis-kompatibler In-Memory-Datenstrukturservice, der als Datenspeicher oder Cache verwendet werden kann. Um PHI speichern zu können, müssen Kunden sicherstellen, dass sie die neueste HIPAA-fähige ElastiCache für die Redis-Engine-Version und die aktuellen Knotentypen der Generation ausführen. Amazon ElastiCache for Redis unterstützt das Speichern von PHI für die folgenden Knotentypen und Redis-Engine-Versionen:

- Knotentypen: nur aktuelle Generation (z. B. zum Zeitpunkt der Veröffentlichung dieses Whitepapers, M4, M5, R4, R5, T2, T3)

- ElastiCache für Redis-Engine-Version: 3.2.6 und 4.0.10 und höher

Weitere Informationen zur Auswahl von Knoten der aktuellen Generation finden Sie unter Amazon-ElastiCache Preise. Weitere Informationen zur Auswahl einer ElastiCache für Redis-Engine finden Sie unter Was ist Amazon ElastiCache für Redis?

Kunden müssen außerdem sicherstellen, dass der Cluster und die Knoten innerhalb des Clusters so konfiguriert sind, dass Daten im Ruhezustand verschlüsselt, die Transportverschlüsselung aktiviert und die Authentifizierung von Redis-Befehlen aktiviert wird. Darüber hinaus müssen Kunden sicherstellen, dass ihre Redis-Cluster jederzeit mit den neuesten Service-Updates vom Typ „Sicherheit“ am oder vor dem „Empfohlene Anwendung nach Datum“ (dem Datum, an dem empfohlen wird, das Update anzuwenden) aktualisiert werden. Weitere Informationen dazu finden Sie in den folgenden Abschnitten.

Themen

Verschlüsselung im Ruhezustand

Amazon ElastiCache for Redis bietet Datenverschlüsselung für seinen Cluster, um die Daten im Ruhezustand zu schützen. Wenn Kunden die Verschlüsselung im Ruhezustand für einen Cluster zum Zeitpunkt der Erstellung aktivieren, verschlüsselt Amazon ElastiCache for Redis Daten auf der Festplatte und automatisierte Redis-Backups. Kundendaten auf der Festplatte werden mit hardwarebeschleunigten symmetrischen Advanced Encryption Standard (AES)-512-Schlüsseln verschlüsselt. Redis-Backups werden mit von Amazon S3-managed Verschlüsselungsschlüsseln (SSE-S3) verschlüsselt. Ein S3-Bucket mit aktivierter serverseitiger Verschlüsselung verschlüsselt die Daten mit hardwarebeschleunigten symmetrischen Advanced Encryption Standard (AES)-256-Schlüsseln, bevor sie im Bucket gespeichert werden.

Weitere Informationen zu S3-managed Verschlüsselungsschlüsseln (SSE-S3) finden Sie unter Schutz von Daten mit serverseitiger Verschlüsselung mit von Amazon S3-Managed Verschlüsselungsschlüsseln (SSE-S3). Auf einem ElastiCache Redis-Cluster (Einzel- oder Mehrfachknoten), der mit Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand

gespeichert sind, gemäß der zum Zeitpunkt der Veröffentlichung dieses Whitepapers geltenden -Anleitung verschlüsselt. Dazu gehören Daten auf der Festplatte und automatisierte Backups im S3-Bucket. Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Amazon- ElastiCache for-Redis-Verschlüsselung ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung im Ruhezustand mit Amazon ElastiCache für Redis finden Sie unter Was ist Amazon ElastiCache für Redis?

Transportverschlüsselung

Amazon ElastiCache for Redis verwendet TLS, um die Daten während der Übertragung zu verschlüsseln. Verbindungen zu ElastiCache für Redis, die PHI enthalten, müssen Transportverschlüsselung verwenden und die Konfiguration auf Konsistenz mit der -Anleitung auswerten. Weitere Informationen finden Sie unter CreateReplicationGroup. Weitere Informationen zum Aktivieren der Transportverschlüsselung finden Sie unter ElastiCache Redis-Verschlüsselung während der Übertragung (TLS).

Authentifizierung

Amazon ElastiCache -for-Redis-Cluster (Einzel-/Multiknoten), die PHI enthalten, müssen ein Redis-AUTH-Token bereitstellen, um die Authentifizierung von Redis-Befehlen zu ermöglichen. Redis AUTH ist verfügbar, wenn sowohl die Verschlüsselung im Ruhezustand als auch die Verschlüsselung während der Übertragung aktiviert sind. Kunden sollten ein starkes Token für Redis AUTH mit folgenden Einschränkungen bereitstellen:

- Darf nur druckbare ASCII-Zeichen enthalten
- Muss mindestens 16 Zeichen und nicht mehr als 128 Zeichen lang sein
- Darf keines der folgenden Zeichen enthalten: '/', '"' oder "@"

Dieses Token muss zum Zeitpunkt der Erstellung der Redis-Replikationsgruppe (einzelner/mehrere Knoten) innerhalb des Anforderungsparameters festgelegt werden und kann später mit einem neuen Wert aktualisiert werden. AWS verschlüsselt dieses Token mit AWS Key Management Service (AWS KMS). Weitere Informationen zu Redis AUTH finden Sie unter ElastiCache Redis-Verschlüsselung während der Übertragung (TLS).

Anwenden von ElastiCache Service-Updates

Amazon ElastiCache -for-Redis-Cluster (Einzel-/Multi-Knoten), die PHI enthalten, müssen am oder vor dem „Empfohlene Anwendung nach Datum“ mit den neuesten Service-Updates vom Typ

„Sicherheit“ aktualisiert werden. ElastiCache bietet dies als Self-Service-Feature, mit dem Kunden die Updates jederzeit auf Abruf und in Echtzeit anwenden können. Jedes Service-Update verfügt über „Schweregrad“ und „Empfohlene Anwendung nach Datum“ und ist nur für die entsprechenden Redis-Replikationsgruppen verfügbar.

Das Feld „SLA Met“ im Service-Update-Feature gibt an, ob das Update am oder vor dem „Empfohlene Anwendung nach Datum“ angewendet wurde. Wenn Kunden sich dafür entscheiden, die Aktualisierungen bis zum „Empfohlene Anwendung nach Datum“ nicht auf die entsprechenden Redis-Replikationsgruppen anzuwenden, ElastiCache werden sie keine Maßnahmen ergreifen, um sie anzuwenden. Kunden können das Dashboard mit dem Service-Update-Verlauf verwenden, um die Anwendung von Updates für ihre Redis-Replikationsgruppen im Laufe der Zeit zu überprüfen. Weitere Informationen zur Verwendung dieser Funktion finden Sie unter Self-Service-Updates in Amazon ElastiCache.

Amazon OpenSearch Service

Amazon OpenSearch Service ermöglicht es Kunden, einen verwalteten OpenSearch oder älteren Elasticsearch-OSS-Cluster in einer dedizierten Amazon Virtual Private Cloud (Amazon VPC) auszuführen. Bei Verwendung von OpenSearch Service mit PHI sollten Kunden OpenSearch oder Elasticsearch 6.0 oder höher verwenden. Kunden sollten sicherstellen, dass PHI im Ruhezustand und während der Übertragung innerhalb von Amazon OpenSearch Service verschlüsselt ist. Kunden können die AWS KMS Schlüsselverschlüsselung verwenden, um Daten im Ruhezustand in ihren OpenSearch Service-Domains zu verschlüsseln, die nur für OpenSearch und Elasticsearch 5.1 oder höher verfügbar sind. Weitere Informationen zum Verschlüsseln von Daten im Ruhezustand finden Sie unter Verschlüsselung von Daten im Ruhezustand für Amazon OpenSearch Service .

Jede OpenSearch Service-Domain wird in einer eigenen VPC ausgeführt. Kunden sollten die node-to-node Verschlüsselung aktivieren, die in allen OpenSearch Versionen und in Elasticsearch 6.0 oder höher verfügbar ist. Wenn Kunden Daten über HTTPS an OpenSearch Service senden, trägt die node-to-node Verschlüsselung dazu bei, dass ihre Daten verschlüsselt bleiben, während sie sie im gesamten Cluster OpenSearch verteilt (und neu verteilt). Wenn Daten unverschlüsselt über HTTP eingehen, verschlüsselt OpenSearch Service die Daten, nachdem sie den Cluster erreicht haben. Daher sollten alle PHI, die in einen Amazon- OpenSearch Service-Cluster gelangen, über HTTPS gesendet werden. Weitere Informationen finden Sie unter N-ode-to-node Verschlüsselung für Amazon OpenSearch Service .

Protokolle aus der OpenSearch Service-Konfigurations-API können in erfasst werden AWS CloudTrail. Weitere Informationen finden Sie unter Überwachen von Amazon- OpenSearch Service-API-Aufrufen mit AWS CloudTrail.

Amazon EMR

Amazon EMR stellt einen Cluster von Amazon EC2 im Konto eines Kunden bereit und verwaltet ihn. Informationen zur Verschlüsselung mit Amazon EMR finden Sie unter Verschlüsselungsoptionen.

Amazon EventBridge

Amazon EventBridge (ehemals Amazon CloudWatch Events) ist ein Serverless Event Bus, mit dem Sie skalierbare ereignisgesteuerte Anwendungen erstellen können. EventBridge stellt einen Stream von Echtzeitdaten aus Ereignisquellen wie Zendesk, Datadog oder Pager-Berechtigungen bereit und leitet diese Daten an Ziele wie weiter AWS Lambda.

Standardmäßig EventBridge verschlüsselt Daten mit dem 256-Bit Advanced Encryption Standard (AES-256) unter einem AWS-eigenen CMK, wodurch Kundendaten vor unbefugtem Zugriff geschützt werden. Kunden sollten sicherstellen, dass alle AWS-Ressourcen, die ein Ereignis ausgeben, das PHI speichert, verarbeitet oder überträgt, gemäß den bewährten Methoden konfiguriert sind.

Amazon EventBridge ist in integriert AWS CloudTrail und Kunden können die neuesten Ereignisse in der CloudTrail Konsole im Ereignisverlauf anzeigen. Weitere Informationen finden Sie unter EventBridge Informationen in CloudTrail.

Amazon Forecast

Amazon Forecast ist ein vollständig verwalteter Service, der Machine Learning verwendet, um hochpräzise Prognosen zu liefern. Basierend auf derselben Machine-Learning-Prognosetechnologie, die von Amazon.com verwendet wird. Jede Interaktion, die Kunden mit Amazon Forecast haben, ist durch Verschlüsselung geschützt. Alle von Amazon Forecast verarbeiteten Inhalte werden mit Kundenschlüsseln über Amazon Key Management Service und im Ruhezustand in der AWS-Region verschlüsselt, in der Kunden den Service nutzen.

Amazon Forecast ist in integriert, einem Service AWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Services in Amazon Forecast aufzeichnet. CloudTrail erfasst alle API-Aufrufe für Amazon Forecast als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon-Forecast-Konsole und Codeaufrufe der Amazon-Forecast-API-Operationen. Wenn Kunden

einen Trail erstellen, können sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Amazon Forecast. Weitere Informationen finden Sie unter Protokollieren von Forecast-API-Aufrufen mit AWS CloudTrail.

Standardmäßig werden die Protokolldateien, die von CloudTrail an ihren Bucket geliefert werden, durch serverseitige Amazon-Verschlüsselung mit von Amazon S3-managed Verschlüsselungsschlüsseln (SSE-S3) verschlüsselt. Um eine Sicherheitsebene bereitzustellen, die direkt verwaltet werden kann, können Kunden stattdessen die serverseitige Verschlüsselung mit AWS KMS von verwalteten Schlüsseln (SSE-KMS) für ihre CloudTrail Protokolldateien verwenden. Die Aktivierung der serverseitigen Verschlüsselung verschlüsselt die Protokolldateien mit SSE-KMS, aber nicht die Digest-Dateien. Digest-Dateien werden mit S3-verwalteten Verschlüsselungsschlüsseln (SSE-S3) von Amazon verschlüsselt.

AWS Forecast importiert und exportiert Daten in/aus S3-Buckets. Beim Importieren und Exportieren von Daten aus Amazon S3 sollten Kunden sicherstellen, dass S3-Buckets so konfiguriert sind, dass sie den Anleitungen entsprechen. Weitere Informationen finden Sie unter Erste Schritte mit .

Amazon FSx

Amazon FSx ist ein vollständig verwalteter Service, der funktionsreiche und hochperformante Dateisysteme bereitstellt. Amazon FSx for Windows File Server bietet äußerst zuverlässigen und skalierbaren Dateispeicher und ist über das Server Message Block (SMB)-Protokoll zugänglich. Amazon FSx for Lustre bietet Hochleistungsspeicher für Rechen-Workloads und wird von Lustre, dem beliebtesten Hochleistungsdateisystem der Welt, unterstützt.

Amazon FSx unterstützt zwei Formen der Verschlüsselung für Dateisysteme, die Verschlüsselung von Daten während der Übertragung und die Verschlüsselung im Ruhezustand. Amazon FSx for Windows File Server unterstützt auch die Protokollierung aller API-Aufrufe mit AWS CloudTrail.

Die Verschlüsselung von Daten während der Übertragung wird von Amazon FSx for Windows File Server auf Datenverarbeitungs-Instances unterstützt, die SMB-Protokoll 3.0 oder höher unterstützen, und von Amazon FSx for Lustre auf Amazon EC2-Instances, die die Verschlüsselung während der Übertragung unterstützen. Alternativ können Kunden Daten vor dem Speichern auf Amazon FSx verschlüsseln, sind dann aber für den Verschlüsselungsprozess und die Schlüsselverwaltung verantwortlich.

Die Verschlüsselung von Daten im Ruhezustand wird beim Erstellen eines Amazon FSx-Dateisystems mithilfe des AES-256-Verschlüsselungsalgorithmus und der von AWS KMS verwalteten Schlüssel automatisch aktiviert. Daten und Metadaten werden automatisch verschlüsselt, bevor

sie in das Dateisystem geschrieben werden, und werden automatisch entschlüsselt, bevor sie der Anwendung präsentiert werden. PHI sollte nicht in Dateien oder Ordnernamen verwendet werden.

Amazon GuardDuty

Amazon GuardDuty ist ein verwalteter Service zur Bedrohungserkennung, der kontinuierlich auf böswilliges oder unbefugtes Verhalten überwacht, um Kunden beim Schutz ihrer AWS-Konten und -Workloads zu unterstützen. Es überwacht Aktivitäten wie ungewöhnliche API-Aufrufe oder potenziell nicht autorisierte Bereitstellungen, die auf eine mögliche Kontokompromittierung hinweisen. Amazon erkennt GuardDuty auch potenziell kompromittierte Instances oder Informationen von Angreifern.

Amazon überwacht und analysiert GuardDuty kontinuierlich die folgenden Datenquellen: VPC-Flow-Protokolle, AWS CloudTrail Ereignisprotokolle und DNS-Protokolle. Es verwendet Bedrohungsinformationen wie Listen bösartiger IPs und Domains sowie Machine Learning, um unerwartete und potenziell nicht autorisierte und böswillige Aktivitäten in einer AWS-Umgebung zu identifizieren. Daher sollte Amazon GuardDuty nicht auf PHI stoßen, da diese Daten nicht in einer der oben aufgeführten AWS-basierten Datenquellen gespeichert werden sollen.

Amazon HealthLake

Amazon HealthLake ermöglicht es Kunden in der Branche Gesundheitswesen und Biowissenschaften, Gesundheitsdaten im Petabyte-Bereich zu speichern, zu transformieren, abzufragen und zu analysieren. Kunden können Amazon verwenden, HealthLake um PHI zu übertragen, zu verarbeiten und zu speichern. Amazon HealthLake verschlüsselt Daten im Ruhezustand standardmäßig in den Datenspeichern des Kunden. Alle Servicedaten und Metadaten werden mit einem serviceeigenen KMS-Schlüssel verschlüsselt. Wenn ein Kunde gemäß den Spezifikationen von Fast microSD Interoperability Resources (FHIR) die FHIR-Ressource löscht, wird sie nur beim Abruf ausgeblendet und vom Service für das Versioning beibehalten. Wenn Kunden die StartFHIRImportJob -API verwenden, HealthLake erzwingt Amazon die Anforderung, Daten in einen verschlüsselten Amazon S3-Bucket zu exportieren.

Amazon HealthLake verschlüsselt Daten sowohl während der Übertragung als auch im Ruhezustand. Für die Verschlüsselung von Daten während der Übertragung können Sie von AWS veröffentlichte API-Aufrufe verwenden, um HealthLake über das Netzwerk auf zuzugreifen. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und

höher unterstützen diese Modi. Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Kunden den AWS Security Token Service (AWS STS) verwenden, um temporäre Sicherheitsanmeldeinformationen zum Signieren von Anforderungen zu generieren. Für die Verschlüsselung von Daten im Ruhezustand HealthLake verschlüsselt Amazon Daten in den Datenspeichern des Kunden standardmäßig mit einem kundeneigenen AWS KMS-Schlüssel oder einem serviceeigenen AWS KMS-Schlüssel. Alle Servicedaten und Metadaten werden im Ruhezustand mit einem serviceeigenen AWS KMS-Schlüssel verschlüsselt.

Amazon HealthLake ist in integriert AWS CloudTrail. CloudTrail erfasst alle API-Aufrufe an Amazon HealthLake als Ereignisse, einschließlich Aufrufen, die als Ergebnis der Interaktion mit AWS Management Console, der Befehlszeilenschnittstelle (CLI) und programmgesteuert mithilfe des Software Development Kit (SDK) getätigt wurden.

Amazon Inspector

Amazon Inspector ist ein automatisierter Service zur Sicherheitsbewertung für Kunden, die ihre Sicherheit und Compliance von Anwendungen verbessern möchten, die auf AWS bereitgestellt werden. Amazon Inspector bewertet automatisch Schwachstellen in Anwendungen sowie Abweichungen von bewährten Methoden. Nach der Durchführung einer Bewertung erstellt Amazon Inspector eine detaillierte Liste der Sicherheitserkenntnisse, die nach Schweregrad priorisiert sind. Kunden können Amazon Inspector auf EC2-Instances ausführen, die PHI enthalten. Amazon Inspector verschlüsselt alle über das Netzwerk übertragenen Daten sowie alle Telemetriedaten, die im Ruhezustand gespeichert sind.

Amazon Managed Service für Apache Flink

Mit Amazon Managed Service für Apache Flink können Kunden schnell SQL-Code erstellen, der kontinuierlich Daten in nahezu Echtzeit liest, verarbeitet und speichert. Mithilfe von Standard-SQL-Abfragen für die Streaming-Daten können Kunden Anwendungen erstellen, die ihre Daten transformieren und Einblicke in sie geben. Managed Service für Apache Flink unterstützt Eingaben aus Kinesis Data Streams und Firehose-Bereitstellungsdatenströmen als Quellen für Analyseanwendungen. Wenn der Stream verschlüsselt ist, greift Managed Service für Apache Flink nahtlos auf die Daten im verschlüsselten Stream zu, ohne dass eine weitere Konfiguration erforderlich ist. Managed Service für Apache Flink speichert keine unverschlüsselten Daten, die aus Kinesis Data Streams gelesen wurden. Weitere Informationen finden Sie unter Konfigurieren der Anwendungseingabe.

Managed Service für Apache Flink lässt sich sowohl in als auch in AWS CloudTrail Amazon CloudWatch Logs für die Anwendungsüberwachung integrieren. Weitere Informationen finden Sie unter Überwachung von Tools und Arbeiten mit Amazon CloudWatch Logs.

Amazon Data Firehose

Wenn Kunden Daten von ihren Datenproduzenten an ihren Kinesis-Datenstrom senden, verschlüsselt Amazon Kinesis Data Streams Daten mit einem - AWS KMS Schlüssel, bevor sie im Ruhezustand gespeichert werden. Wenn der Firehose-Bereitstellungs-Stream Daten aus dem Kinesis-Stream liest, entschlüsselt Kinesis Data Streams zuerst die Daten und sendet sie dann an Firehose. Firehose puffert die Daten im Speicher basierend auf den vom Kunden angegebenen Pufferhinweisen.

Anschließend werden die Daten an die Ziele übermittelt, ohne die unverschlüsselten Daten im Ruhezustand zu speichern. Weitere Informationen zur Verschlüsselung mit Firehose finden Sie unter Datenschutz in Amazon Data Firehose.

AWS bietet verschiedene Tools, mit denen Kunden Amazon Data Firehose überwachen können, darunter Amazon- CloudWatch Metriken, Amazon CloudWatch Logs, Kinesis Agent sowie API-Protokollierung und -Verlauf. Weitere Informationen finden Sie unter Überwachen von Amazon Data Firehose.

Amazon Kinesis Streams

Mit Amazon Kinesis Streams können Kunden benutzerdefinierte Anwendungen erstellen, die Streaming-Daten für besondere Anforderungen verarbeiten oder analysieren. Die serverseitige Verschlüsselungsfunktion ermöglicht es Kunden, Daten im Ruhezustand zu verschlüsseln. Wenn die serverseitige Verschlüsselung aktiviert ist, verwendet Kinesis Streams einen AWS KMS - Schlüssel, um die Daten zu verschlüsseln, bevor sie auf Datenträgern gespeichert werden. Weitere Informationen finden Sie unter Datenschutz in Amazon Kinesis Data Streams. Verbindungen zu Amazon S3, die PHI enthalten, müssen Endpunkte verwenden, die verschlüsselten Transport akzeptieren (d. h. HTTPS). Eine Liste der regionalen Endpunkte finden Sie unter AWS-Service-Endpunkte.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams ist ein vollständig verwalteter AWS-Service, mit dem Kunden Live-Videos von Geräten in die AWS Cloud streamen oder Anwendungen für die Echtzeit-

Videoverarbeitung oder batchorientierte Videoanalysen erstellen können. Die serverseitige Verschlüsselung ist eine Funktion in Kinesis Video Streams, die Daten im Ruhezustand automatisch mit einem vom Kunden angegebenen - AWS KMS Schlüssel (früher CMK) verschlüsselt. Daten werden verschlüsselt, bevor sie in die Stream-Speicherschicht von Kinesis Video Streams geschrieben werden, und sie werden entschlüsselt, nachdem sie aus dem Speicher abgerufen wurden.

Das Amazon Kinesis Video Streams SDK kann verwendet werden, um Streaming-Videodaten zu übertragen, die PHI enthalten. Standardmäßig verwendet das SDK TLS, um Frames und Fragmente zu verschlüsseln, die von dem Hardwaregerät generiert werden, auf dem es installiert ist. Das SDK verwaltet oder wirkt sich nicht auf Daten aus, die im Ruhezustand gespeichert sind. Amazon Kinesis Video Streams verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

Amazon Lex

Amazon Lex ist ein AWS-Service zum Erstellen von Konversationsschnittstellen für Anwendungen, die Sprache und Text verwenden. Mit Amazon Lex ist jetzt die gleiche Konversations-Engine verfügbar, die Amazon Alexa unterstützt, sodass Kunden anspruchsvolle Chatbots in natürlicher Sprache in ihre neuen und bestehenden Anwendungen integrieren können. Amazon Lex bietet die tiefe Funktionalität und Flexibilität von NLU (Natural Language Understanding) und automatischer Spracherkennung (ASR), sodass Kunden mit lebensechten, Konversationsinteraktionen ein hochinteressantes Benutzererlebnis aufbauen und neue Produktkategorien erstellen können.

Lex verwendet das HTTPS-Protokoll, um sowohl mit Clients als auch mit anderen AWS-Services zu kommunizieren. Der Zugriff auf Lex ist API-gesteuert und es können die entsprechenden IAM-Mindestberechtigungen durchgesetzt werden. Weitere Informationen finden Sie unter Datenschutz in Amazon Lex.

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung der Amazon Lex-Chatbots der Kunden aufrechtzuerhalten. Verwenden Sie Amazon , um den Zustand von Amazon Lex-Bots zu verfolgen CloudWatch. Mit können CloudWatchKunden Metriken für einzelne Amazon Lex-Operationen oder für globale Amazon Lex-Operationen für ihr Konto abrufen. Kunden können auch CloudWatch Alarme einrichten, um benachrichtigt zu werden, wenn eine oder mehrere Metriken einen von Kunden definierten Schwellenwert überschreiten. Kunden können beispielsweise die Anzahl der Anfragen an einen Bot über einen bestimmten Zeitraum überwachen, die Latenz erfolgreicher Anfragen anzeigen oder einen Alarm auslösen, wenn Fehler einen Schwellenwert überschreiten. Lex ist auch in integriert AWS CloudTrail , um Lex-API-Aufrufe zu protokollieren. Weitere Informationen finden Sie unter Überwachung in Amazon Lex.

Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Amazon MSK bietet Verschlüsselungsfunktionen für Daten im Ruhezustand und für Daten während der Übertragung. Für die Verschlüsselung von Daten im Ruhezustand verwendet der Amazon-MSK-Cluster die serverseitige Amazon-EBS-Verschlüsselung und - AWS KMS Schlüssel, um Speicher-Volumes zu verschlüsseln. Für Daten während der Übertragung ist die Verschlüsselung über TLS für die Kommunikation zwischen Brokern aktiviert.

Die Verschlüsselungskonfigurationseinstellung wird aktiviert, wenn ein Cluster erstellt wird. Außerdem ist die Verschlüsselung während der Übertragung standardmäßig auf TLS für Cluster festgelegt, die über die CLI oder die AWS Konsole erstellt wurden. Eine zusätzliche Konfiguration ist erforderlich, damit Clients mit Clustern mithilfe der TLS-Verschlüsselung kommunizieren können. Kunden können die Standardverschlüsselungseinstellung ändern, indem sie die TLS/Klartext-Einstellungen auswählen. Weitere Informationen finden Sie unter Amazon-MSK-Verschlüsselung.

Kunden können die Leistung der Kunden-Cluster mithilfe der Amazon-MSK-Konsole, der Amazon-CloudWatch Konsole oder mithilfe von Open Monitoring mit Prometheus, einer Open-Source-Überwachungslösung, auf JMX und Host-Metriken zugreifen.

Tools, die für das Lesen aus Prometheus-Exportern entwickelt wurden, sind mit Open Monitoring kompatibel, z. B.: Datadog , Lenses , New Relic , SumSpeed oder ein Prometheus-Server. Weitere Informationen zu Open Monitoring finden Sie in der Dokumentation zu Amazon MSK Open Monitoring.

Bitte beachten Sie, dass die Standardversion von Apache Zookeeper im Paket mit Apache Kafka keine Verschlüsselung unterstützt. Beachten Sie jedoch, dass die Kommunikation zwischen Apache Zookeeper und Apache Kafka Brokern auf Broker-, Themen- und Partitionsstatusinformationen beschränkt ist. Die einzige Möglichkeit, Daten aus einem Amazon-MSK-Cluster zu erzeugen und zu verbrauchen, ist eine private Verbindung zwischen ihren Clients in ihrer VPC und dem Amazon-MSK-Cluster. Amazon MSK unterstützt keine öffentlichen Endpunkte.

Amazon MQ

Amazon MQ ist ein verwalteter Message Broker-Service für Apache ActiveMQ, der das Einrichten und Betreiben von Message Brokern in der Cloud vereinfacht. Amazon MQ funktioniert mit vorhandenen Anwendungen und Services, ohne dass ein Kunde sein eigenes Messaging-System verwalten, betreiben oder warten muss. Um die Verschlüsselung von PHI-Daten während der

Übertragung bereitzustellen, sollten die folgenden Protokolle mit aktiviertem TLS für den Zugriff auf Broker verwendet werden:

- AMQP
- MQTT
- MQTT über WebSocket
- OpenWire
- STOMP
- STOMP über WebSocket

Amazon MQ verschlüsselt Nachrichten im Ruhezustand und während der Übertragung mit Verschlüsselungsschlüsseln, die sicher verwaltet und gespeichert werden. Amazon MQ verwendet CloudTrail , um alle API-Aufrufe zu protokollieren.

Amazon Neptune

Amazon Neptune ist ein schneller, zuverlässiger, vollständig verwalteter Graph-Datenbankservice, mit dem es ganz einfach ist, Anwendungen zu erstellen und auszuführen, die mit stark verbundenen Datensätzen arbeiten. Der Kern von Amazon Neptune ist eine speziell entwickelte, leistungsstarke Graphdatenbank-Engine, die für die Speicherung von Milliarden von Beziehungen und die Abfrage des Graphen mit Latenz in Millisekunden optimiert ist. Amazon Neptune unterstützt die beliebten Graphabfragesprachen Apache TinkerPop Gremlin und W3C SPARQL.

Daten, die PHI enthalten, können jetzt in einer verschlüsselten Instance von Amazon Neptune aufbewahrt werden. Eine verschlüsselte Instance von Amazon Neptune kann nur zum Zeitpunkt der Erstellung angegeben werden, indem Sie in der Amazon Neptune-Konsole „Verschlüsselung aktivieren“ auswählen. Alle Protokolle, Backups und Snapshots werden für eine mit Amazon Neptune verschlüsselte Instance verschlüsselt. Die Schlüsselverwaltung für verschlüsselte Instances von Amazon Neptune wird über die bereitgestellt AWS KMS. Die Verschlüsselung von Daten während der Übertragung erfolgt über SSL/TLS. Amazon Neptune verwendet CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Netzwerk-Firewall

AWS Network Firewall ist ein verwalteter Firewall-Service, der die Bereitstellung wesentlicher Netzwerkschutzmaßnahmen für Ihre gesamte Amazon Virtual Private Cloud (Amazon VPC)

vereinfacht. Der Service wird automatisch mit dem Netzwerkverkehrsvolumen skaliert, um Hochverfügbarkeitsschutz bereitzustellen, ohne dass die zugrunde liegende Infrastruktur eingerichtet oder gewartet werden muss. Sowohl Kundenregeln als auch Zugriffsprotokolle können Endbenutzer-IP-Adressen enthalten, die sowohl im Ruhezustand als auch während der Übertragung innerhalb der AWS Architektur verschlüsselt sind. Darüber hinaus verschlüsselt AWS Network Firewall alle Daten im Ruhezustand und während der Übertragung zwischen AWS Komponentenservices (Amazon S3, Amazon DynamoDB, Amazon CloudWatch Logs, Amazon EBS). Der Service verschlüsselt Daten automatisch, ohne dass eine spezielle Konfiguration erforderlich ist.

Amazon Pinpoint

Amazon Pinpoint bietet Entwicklern eine einzige API-Ebene, CLI-Unterstützung und clientseitige SDK-Unterstützung, um die Anwendungskommunikationskanäle mit Benutzern zu erweitern. Zu den zulässigen Kanälen gehören: E-Mail, SMS-Textnachrichten, mobile Push-Benachrichtigungen und benutzerdefinierte Kanäle. Amazon Pinpoint bietet auch ein Analysesystem, das das Verhalten von App-Benutzern und die Benutzerinteraktion verfolgt. Mit diesem Service können Entwickler erfahren, wie jeder Benutzer bevorzugt, und die Benutzererfahrung personalisieren, um die Benutzerzufriedenheit zu erhöhen.

Amazon Pinpoint hilft Entwicklern auch dabei, mehrere Messaging-Anwendungsfälle zu lösen, z. B. direktes oder transaktionales Messaging, gezieltes Messaging oder Kampagnen-Messaging und ereignisbasiertes Messaging. Durch die Integration und Aktivierung aller Kanäle für die Endbenutzerinteraktion über Amazon Pinpoint können Entwickler eine 360-Grad-Ansicht der Benutzerinteraktion über alle Kundenkontaktpunkte hinweg erstellen. Amazon Pinpoint speichert Benutzer-, Endpunkt- und Ereignisdaten, damit Kunden Segmente erstellen, Nachrichten an Empfänger senden und Interaktionsdaten erfassen können.

Amazon Pinpoint verschlüsselt Daten sowohl im Ruhezustand als auch während der Übertragung. Weitere Informationen finden Sie unter Häufig FAQs zu Amazon Pinpoint. Während Amazon Pinpoint alle Daten im Ruhezustand und während der Übertragung verschlüsselt, wird der endgültige Kanal, z. B. SMS oder E-Mail, möglicherweise nicht verschlüsselt, und Kunden sollten jeden Kanal so konfigurieren, dass er ihren Anforderungen entspricht.

Darüber hinaus sollten Kunden, die PHI über den SMS-Kanal senden müssen, eine spezielle Kurzwahlnummer (5- und 6-stellige Ursprungstelefonnummern) verwenden, um PHI explizit zu senden. Weitere Informationen zum Anfordern einer Kurzwahlnummer finden Sie unter Anfordern dedizierter Kurzwahlnummern für SMS-Messaging mit Amazon Pinpoint. Kunden können sich

auch dafür entscheiden, PHI nicht über den endgültigen Kanal zu senden und stattdessen einen Mechanismus für den sicheren Zugriff auf PHI über HTTPS bereitzustellen.

API-Aufrufe an Amazon Pinpoint können mit erfasst werden AWS CloudTrail. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon Pinpoint-Konsole und Codeaufrufe von Amazon Pinpoint-API-Operationen. Wenn Kunden einen Trail erstellen, können sie die kontinuierliche Bereitstellung von AWS CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Amazon Pinpoint . Wenn Kunden keinen Trail konfigurieren, können sie weiterhin die neuesten Ereignisse mithilfe des Ereignisverlaufs in der AWS CloudTrail Konsole anzeigen. Anhand der von gesammelten Informationen können Kunden feststellen AWS CloudTrail, dass die Anfrage an Amazon Pinpoint gestellt wurde, die IP-Adresse der Anfrage, wer die Anfrage gestellt hat, wann die Anfrage gestellt wurde und zusätzliche Details. Weitere Informationen finden Sie unter Protokollieren von Amazon Pinpoint-API-Aufrufen mit AWS CloudTrail.

Amazon Polly

Amazon Polly ist ein Cloud-Service, der Text in naturgetreue Sprache umwandelt. Amazon Polly bietet einfache API-Operationen, die Kunden problemlos in vorhandene Anwendungen integrieren können. Amazon Polly verwendet das HTTPS-Protokoll für die Kommunikation mit Clients. Der Zugriff auf Amazon Polly ist API-gesteuert, und die entsprechenden IAM-Mindestberechtigungen können erzwungen werden. Weitere Informationen finden Sie unter Datenschutz. Einige Beispiele für Anwendungsfälle, die PHI enthalten:

- caregiver konvertiert einen Textbericht, der PHI enthält, in synthetisierte Sprache, sodass er den Bericht hören kann, während er andere Aufgaben ausführt oder ausführt.
- Visuell beeinträchtigte Patienten erhalten medizinische Beratung und verwenden die Beratung in Form von synthetisierter Sprache.

Der endgültige Übermittlungskanal von Amazon Polly könnte dazu führen, dass Audio mit PHI in einem öffentlichen Bereich wiedergegeben wird, und es sollten Vorbehalte getroffen werden, dass die Übermittlung dies berücksichtigt. Die synthetisierte Sprachausgabe kann auch asynchron an einen Amazon S3-Bucket mit aktivierter Verschlüsselung gesendet werden.

Wenn die unterstützte Ereignisaktivität in Amazon Polly auftritt, wird diese Aktivität in einem AWS CloudTrail -Ereignis zusammen mit anderen - AWS Serviceereignissen im Ereignisverlauf aufgezeichnet. Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in einem AWS Kundenkonto, einschließlich Ereignissen für Amazon Polly, einen Trail. Ein Trail ermöglicht

CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Anhand der von CloudTrailgesammelten Informationen können Kunden die an Amazon Polly gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon QLDB ist eine vollständig verwaltete Ledger-Datenbank, die ein transparentes, unveränderliches und kryptographisch überprüfbares Transaktionsprotokoll bereitstellt, das einer zentralen, vertrauenswürdigen Stelle gehört. Amazon QLDB verfolgt jede Änderung der Anwendungsdaten und führt einen vollständigen und überprüfbaren Verlauf der Änderungen im Laufe der Zeit. Daten, die PHI enthalten, können jetzt in einer QLDB-Instance aufbewahrt werden. Standardmäßig werden alle Amazon-QLDB-Daten während der Übertragung und im Ruhezustand verschlüsselt. Daten während der Übertragung werden mit TLS und Daten im Ruhezustand mit von AWS verwalteten Schlüsseln verschlüsselt. Aus Datenschutzgründen empfehlen wir Kunden, die Anmeldeinformationen für AWS -Konten zu schützen und individuelle Benutzerkonten mit AWS Identity and Access Management (IAM) einzurichten, damit jeder Benutzer nur die Berechtigungen erhält, die er für seine Aufgaben benötigt. Weitere Informationen finden Sie unter Datenschutz in Amazon QLDB.

Amazon QLDB ist in integriert, einem Service AWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines - AWS Services in QLDB protokolliert. CloudTrail erfasst alle API-Aufrufe der Steuerebene für QLDB als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der QLDB-Konsole und Codeaufrufe der QLDB-API-Operationen. Wenn Kunden einen Trail erstellen, können sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3)-Bucket, einschließlich Ereignissen für QLDB, aktivieren. Wenn Kunden keinen Trail konfigurieren, können sie weiterhin die neuesten Ereignisse in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Kunden die an QLDB gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Amazon QuickSight

Amazon QuickSight ist ein Business Analytics-Service, mit dem Kunden Visualisierungen erstellen, Ad-hoc-Analysen durchführen und schnell Geschäftseinblicke aus ihren Daten gewinnen können. Amazon QuickSight erkennt AWS Datenquellen, ermöglicht es Unternehmen, auf Hunderttausende

von Benutzern zu skalieren und bietet mithilfe einer robusten In-Memory-Engine (SPICE) reaktionsschnelle Leistung.

Kunden können die Enterprise Edition von Amazon nur verwenden QuickSight , um mit Daten zu arbeiten, die PHI enthalten, da sie Unterstützung für die Verschlüsselung von Daten bietet, die im Ruhezustand in SPICE gespeichert sind. Die Datenverschlüsselung wird mit von AWS verwalteten Schlüsseln durchgeführt.

Amazon RDS für MariaDB

Amazon RDS for MariaDB ermöglicht es Kunden, MariaDB-Datenbanken mit Schlüsseln zu verschlüsseln, die sie über verwalten AWS KMS. Auf einer Datenbank-Instance, die mit Amazon-RDS-Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand im zugrunde liegenden Speicher gespeichert sind, gemäß der zum Zeitpunkt der Veröffentlichung dieses Whitepapers geltenden -Anleitung verschlüsselt, ebenso wie automatisierte Backups, Lesereplikate und Snapshots.

Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Verschlüsselung von Amazon RDS for MariaDB ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung im Ruhezustand mit Amazon RDS finden Sie unter Verschlüsseln von Amazon-RDS-Ressourcen.

Verbindungen zu RDS für MariaDB, die PHI enthalten, müssen Transportverschlüsselung verwenden. Weitere Informationen zum Aktivieren verschlüsselter Verbindungen finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung mit einer DB-Instance.

Amazon RDS für MySQL

Amazon RDS for MySQL ermöglicht es Kunden, MySQL-Datenbanken mit Schlüsseln zu verschlüsseln, die Kunden über verwalten AWS KMS. Auf einer Datenbank-Instance, die mit Amazon-RDS-Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand im zugrunde liegenden Speicher gespeichert sind, gemäß der zum Zeitpunkt der Veröffentlichung dieses Whitepapers geltenden -Anleitung verschlüsselt, ebenso wie automatisierte Backups, Lesereplikate und Snapshots.

Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Verschlüsselung von Amazon RDS für MySQL ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung von Daten im Ruhezustand mit Amazon RDS finden Sie unter Verschlüsseln von Amazon-RDS-Ressourcen.

Verbindungen zu RDS für MySQL, die PHI enthalten, müssen Transportverschlüsselung verwenden. Weitere Informationen zum Aktivieren verschlüsselter Verbindungen finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung mit einer DB-Instance.

Amazon RDS für Oracle

Kunden haben mehrere Möglichkeiten, PHI im Ruhezustand mit Amazon RDS für Oracle zu verschlüsseln. Kunden können Oracle-Datenbanken mit Schlüsseln verschlüsseln, die sie über verwalten AWS KMS. Auf einer Datenbank-Instance, die mit Amazon-RDS-Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand im zugrunde liegenden Speicher gespeichert sind, gemäß der zum Zeitpunkt der Veröffentlichung dieses Whitepapers geltenden -Anleitung verschlüsselt, ebenso wie automatisierte Backups, Lesereplikate und Snapshots.

Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Verschlüsselung von Amazon RDS für Oracle ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung im Ruhezustand mit Amazon RDS finden Sie unter Verschlüsseln von Amazon-RDS-Ressourcen.

Kunden können auch Oracle Transparent Data Encryption (TDE) verwenden und sollten die Konfiguration auf Konsistenz mit der -Anleitung überprüfen. Oracle TDE ist eine Funktion der Oracle Advanced Security-Option, die in Oracle Enterprise Edition verfügbar ist. Mit dieser Funktion werden Daten vor dem Speichern automatisch verschlüsselt und beim Abruf aus dem Speicher automatisch entschlüsselt. Kunden können auch verwenden AWS CloudHSM , um Amazon RDS Oracle TDE-Schlüssel zu speichern. Weitere Informationen finden Sie hier:

- Amazon RDS für Oracle Transparent Data Encryption: Oracle Transparent Data Encryption .
- Verwenden von AWS CloudHSM zum Speichern von Amazon-RDS-Oracle-TDE-Schlüsseln: Was ist Amazon Relational Database Service (Amazon RDS)?

Verbindungen zu Amazon RDS für Oracle, die PHI enthalten, müssen Transportverschlüsselung verwenden und die Konfiguration auf Konsistenz mit der -Anleitung auswerten. Dies wird mit Oracle Native Network Encryption erreicht und in Optionsgruppen von Amazon RDS für Oracle aktiviert. Ausführliche Informationen finden Sie unter Oracle Native Network Encryption.

Amazon RDS für PostgreSQL

Mit Amazon RDS for PostgreSQL können Kunden PostgreSQL-Datenbanken mit Schlüsseln verschlüsseln, die Kunden über verwalten AWS KMS. Auf einer Datenbank-Instance, die mit

Amazon-RDS-Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand im zugrunde liegenden Speicher gespeichert sind, gemäß der zum Zeitpunkt der Veröffentlichung dieses Whitepapers geltenden -Anleitung verschlüsselt, ebenso wie automatisierte Backups, Lesereplikate und Snapshots.

Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Verschlüsselung von Amazon RDS für PostgreSQL ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung im Ruhezustand mit Amazon RDS finden Sie unter Verschlüsseln von Amazon-RDS-Ressourcen.

Verbindungen zu RDS für PostgreSQL, die PHI enthalten, müssen Transportverschlüsselung verwenden. Weitere Informationen zum Aktivieren verschlüsselter Verbindungen finden Sie unter Verwenden von SSL/TLS zum Verschlüsseln einer Verbindung mit einer DB-Instance.

Amazon RDS für SQL Server

RDS for SQL Server unterstützt das Speichern von PHI für die folgenden Kombinationen von Version und Edition:

- 2008 R2 – nur Enterprise Edition
- 2012, 2014 und 2016 – Web-, Standard- und Enterprise Editionen

Wichtig: Die SQL Server Express Edition wird nicht unterstützt und sollte niemals für die Speicherung von PHI verwendet werden.

Um PHI zu speichern, müssen Kunden sicherstellen, dass die Instance so konfiguriert ist, dass Daten im Ruhezustand verschlüsselt werden, und Transportverschlüsselung und -überwachung aktivieren, wie unten beschrieben.

Verschlüsselung im Ruhezustand

Kunden können SQL Server-Datenbanken mit Schlüsseln verschlüsseln, die sie über verwalten AWS KMS. Auf einer Datenbank-Instance, die mit Amazon-RDS-Verschlüsselung ausgeführt wird, werden Daten, die im Ruhezustand im zugrunde liegenden Speicher gespeichert sind, gemäß der zum Zeitpunkt der Veröffentlichung dieses Whitepapers geltenden -Anleitung verschlüsselt, ebenso wie automatisierte Backups und Snapshots. Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Verschlüsselung von Amazon RDS für

SQL Server ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen zur Verschlüsselung im Ruhezustand mit Amazon RDS finden Sie unter Verschlüsseln von Amazon-RDS-Ressourcen.

Wenn Kunden SQL Server Enterprise Edition verwenden, können sie Server Transparent Data Encryption (TDE) als Alternative verwenden. Mit dieser Funktion werden Daten vor dem Speichern automatisch verschlüsselt und beim Abruf aus dem Speicher automatisch entschlüsselt. Weitere Informationen zur transparenten Datenverschlüsselung von RDS für SQL Server finden Sie unter Unterstützung für transparente Datenverschlüsselung in SQL Server.

Transportverschlüsselung

Verbindungen zu Amazon RDS for SQL Server, die PHI enthalten, müssen Transportverschlüsselung verwenden, die von SQL Server Forced SSL bereitgestellt wird. Erzwungenes SSL ist innerhalb der Parametergruppe für Amazon RDS SQL Server aktiviert. Weitere Informationen zu RDS for SQL Server Forced SSL finden Sie unter Verwenden von SSL mit einer Microsoft SQL Server-DB-Instance.

Prüfung

Für Instances von RDS für SQL Server, die PHI enthalten, muss die Prüfung aktiviert sein. Die Prüfung ist innerhalb der Parametergruppe für Amazon RDS SQL Server aktiviert. Weitere Informationen zur Prüfung von RDS für SQL Server finden Sie unter Unterstützung des Compliance-Programms für Microsoft SQL Server-DB-Instances.

Amazon Redshift

Amazon Redshift bietet Datenbankverschlüsselung für seine Cluster, um Daten im Ruhezustand zu schützen. Wenn Kunden die Verschlüsselung für einen Cluster aktivieren, verschlüsselt Amazon Redshift alle Daten, einschließlich Sicherungen, mithilfe von hardwarebeschleunigten symmetrischen Advanced Encryption Standard (AES)-256-Schlüsseln. Amazon Redshift verwendet zur Verschlüsselung eine schlüsselbasierte Architektur mit vier Ebenen. Diese Schlüssel bestehen aus Datenverschlüsselungsschlüsseln, einem Datenbankschlüssel, einem Clusterschlüssel und einem KMS-Schlüssel.

Der Clusterschlüssel verschlüsselt den Datenbankschlüssel des Amazon Redshift-Clusters. Kunden können entweder AWS KMS oder ein AWS CloudHSM (Hardware-Sicherheitsmodul) verwenden, um den Clusterschlüssel zu verwalten. Die Amazon-Redshift-Verschlüsselung im Ruhezustand

entspricht der -Anleitung, die zum Zeitpunkt der Veröffentlichung dieses Whitepapers in Kraft ist. Da die -Anleitung möglicherweise aktualisiert wird, sollten Kunden weiterhin bewerten und feststellen, ob die Amazon-Redshift-Verschlüsselung ihre Compliance- und regulatorischen Anforderungen erfüllt. Weitere Informationen finden Sie unter Datenbankverschlüsselung in Amazon Redshift.

Verbindungen zu Amazon Redshift, die PHI enthalten, müssen Transportverschlüsselung verwenden und Kunden sollten die Konfiguration auf Konsistenz mit der -Anleitung überprüfen. Weitere Informationen finden Sie unter Konfigurieren von Sicherheitsoptionen für Verbindungen. Amazon Redshift Spectrum ermöglicht es Kunden, Amazon-Redshift-SQL-Abfragen für Exabytes von Daten in Amazon S3 auszuführen. Redshift Spectrum ist ein Feature von Amazon Redshift und fällt daher auch in den Geltungsbereich des HIPAA BAA.

Amazon Rekognition

Amazon Rekognition erleichtert das Hinzufügen von Bild- und Videoanalysen zu Kundenanwendungen. Ein Kunde muss nur ein Bild oder Video für die Amazon Rekognition-API bereitstellen, und der Service kann die Objekte, Personen, Text, Szenen und Aktivitäten identifizieren sowie unangemessene Inhalte erkennen. Amazon Rekognition bietet auch eine hochpräzise Gesichtsanalyse und Gesichtserkennung.

Amazon Rekognition ist berechtigt, mit Bildern oder Videos zu arbeiten, die PHI enthalten. Amazon Rekognition fungiert als verwalteter Service und bietet keine konfigurierbaren Optionen für die Verarbeitung von Daten. Amazon Rekognition verwendet, legt PHI nur gemäß den Bedingungen der AWS BAA offen und verwaltet sie. Alle Daten werden im Ruhezustand und während der Übertragung mit Amazon Rekognition verschlüsselt. Amazon Rekognition verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

Amazon Route 53

Amazon Route 53 ist ein verwalteter DNS-Service, der Kunden die Möglichkeit bietet, Domänennamen zu registrieren, Internetdatenverkehr an Kundendomänenressourcen weiterzuleiten und den Zustand dieser Ressourcen zu überprüfen. Während Amazon Route 53 ein HIPAA-berechtigter Service ist, sollte kein PHI in Ressourcennamen oder Tags in Amazon Route 53 gespeichert werden, da die Verschlüsselung solcher Daten nicht unterstützt wird. Stattdessen kann Amazon Route 53 verwendet werden, um Zugriff auf Kundendomänenressourcen zu gewähren, die PHI wie Webserver, die auf Amazon EC2 ausgeführt werden, oder Speicher wie Amazon S3 übertragen oder speichern.

Amazon S3 Glacier

Amazon S3 Glacier verschlüsselt Daten im Ruhezustand automatisch mit symmetrischen AES-256-Bit-Schlüsseln und unterstützt die sichere Übertragung von Kundendaten über sichere Protokolle. Verbindungen zu Amazon S3 Glacier, die PHI enthalten, müssen Endpunkte verwenden, die verschlüsselten Transport (HTTPS) akzeptieren. Eine Liste der regionalen Endpunkte finden Sie unter AWS -Service-Endpunkte.

Verwenden Sie PHI nicht in Archiv- und Tresornamen oder Metadaten, da diese Daten nicht mit serverseitiger Amazon S3-Glacier-Verschlüsselung verschlüsselt und nicht in clientseitigen Verschlüsselungsarchitekturen verschlüsselt sind.

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) ermöglicht die schnelle, einfache und sichere Übertragung von Dateien über große Entfernungen zwischen dem Client eines Kunden und einem S3-Bucket. Transfer Acceleration nutzt die global verteilten Edge- CloudFrontStandorte von Amazon . Sobald die Daten an einem Edge-Standort eingehen, werden sie über einen optimierten Netzwerkpfad an Ihren Amazon S3-Bucket weitergeleitet. Kunden sollten sicherstellen, dass alle Daten, die PHI enthalten, die mit AWS S3TA übertragen werden, während der Übertragung und im Ruhezustand verschlüsselt werden. Weitere Informationen zu den verfügbaren Verschlüsselungsoptionen finden Sie in der -Anleitung für Amazon S3.

Amazon SageMaker

Amazon SageMaker ist ein vollständig verwalteter Machine-Learning-Service. Mit Amazon können SageMakerDatenwissenschaftler und Entwickler schnell und einfach Machine-Learning-Modelle erstellen und trainieren und diese dann direkt in einer produktionsbereiten gehosteten Umgebung bereitstellen. Es bietet eine integrierte Jupyter-Authoring-Notebook-Instance für den einfachen Zugriff auf Datenquellen zur Untersuchung und Analyse. Amazon bietet SageMaker auch gängige Machine-Learning-Algorithmen, die für eine effiziente Ausführung mit extrem großen Daten in einer verteilten Umgebung optimiert sind.

Mit nativer Unterstützung für bring-your-own-algorithms und Frameworks SageMaker bietet Amazon flexible verteilte Schulungsoptionen, die sich an die spezifischen Workflows eines Kunden anpassen. Amazon SageMaker ist berechtigt, mit Daten zu arbeiten, die PHI enthalten. Die Verschlüsselung von Daten während der Übertragung wird von SSL/TLS bereitgestellt und sowohl bei der Kommunikation mit der Front-End-Schnittstelle von Amazon SageMaker (mit dem Notebook) als auch bei jeder

SageMaker Interaktion von Amazon mit anderen - AWS Services (z. B. beim Abrufen von Daten aus Amazon S3) verwendet.

Um die Anforderung zu erfüllen, dass PHI im Ruhezustand verschlüsselt werden, SageMaker wird die Verschlüsselung von Daten, die mit der Instance gespeichert werden, auf der Modelle mit Amazon ausgeführt werden, bei der Einrichtung des Endpunkts (DescribeEndpointConfig:KmsKeyID) mit AWS Key Management Service (KMS) aktiviert. Die Verschlüsselung von Modelltrainingsergebnissen (Artefakte) ist mit aktiviert AWS KMS und Schlüssel sollten mit der KmsKeyID in der OutputDataConfig Beschreibung angegeben werden. Wenn keine KMS-Schlüssel-ID angegeben wird, wird der standardmäßige Amazon S3-KMS-Schlüssel für das Konto der Rolle verwendet. Amazon SageMaker verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

Amazon Simple Notification Service (Amazon SNS)

Kunden sollten die folgenden Schlüsselverschlüsselungsanforderungen verstehen, um Amazon Simple Notification Service (SNS) mit geschützten Gesundheitsinformationen (PHI) verwenden zu können. Kunden müssen den HTTPS-API-Endpunkt verwenden, den SNS in jeder AWS Region bereitstellt. Der HTTPS-Endpunkt nutzt verschlüsselte Verbindungen und schützt den Datenschutz und die Integrität der an gesendeten Daten AWS. Eine Liste aller HTTPS-API-Endpunkte finden Sie unter AWS -Service-Endpunkte.

Darüber hinaus verwendet Amazon SNS , einen Service CloudTrail, der API-Aufrufe erfasst, die von oder im Namen von Amazon SNS im AWS Konto des Kunden getätigt wurden, und die Protokolldateien an einen Amazon S3-Bucket übermittelt, den er angibt. CloudTrail erfasst API-Aufrufe, die von der Amazon SNS-Konsole oder von der Amazon SNS-API aus getätigt wurden. Anhand der von gesammelten Informationen können Kunden bestimmen CloudTrail, welche Anfrage an Amazon SNS gestellt wurde, von welcher Quell-IP-Adresse die Anfrage gestellt wurde, wer die Anfrage gestellt hat und wann sie gestellt wurde. Weitere Informationen zum Protokollieren von SNS-Operationen finden Sie unter Protokollieren von Amazon SNS-API-Aufrufen mit CloudTrail.

Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) ist ein flexibler und hochgradig skalierbarer E-Mail-Sende- und Empfangsservice. Es unterstützt sowohl S/MIME- als auch PGP-Protokolle, um Nachrichten für vollständige end-to-end Verschlüsselung zu verschlüsseln, und die gesamte Kommunikation mit Amazon SES wird mit SSL (TLS 1.2) gesichert. Kunden haben die Möglichkeit, Nachrichten zu speichern, die im Ruhezustand verschlüsselt wurden, indem sie Amazon SES so konfigurieren, dass Nachrichten empfangen und verschlüsselt werden, bevor sie in einem Amazon

S3-Bucket gespeichert werden. Weitere Informationen finden Sie unter Wie Amazon Simple Email Service (Amazon SES) verwendet, AWS KMS um weitere Informationen zur Verschlüsselung von Nachrichten für die Speicherung zu erhalten. Nachrichten werden während der Übertragung an Amazon SES entweder über einen HTTPS-Endpunkt oder eine verschlüsselte SMTP-Verbindung gesichert.

Für Nachrichten, die von Amazon SES an einen Empfänger gesendet werden, versucht Amazon SES zunächst, eine sichere Verbindung zum empfangenden E-Mail-Server herzustellen. Wenn jedoch keine sichere Verbindung hergestellt werden kann, wird die Nachricht unverschlüsselt gesendet. Um die Verschlüsselung für die Zustellung an einen Empfänger zu verlangen, müssen Kunden einen Konfigurationssatz in Amazon SES erstellen und die verwenden, AWS CLI um die TlsPolicy Eigenschaft auf Erforderlich festzulegen. Weitere Informationen finden Sie unter Amazon SES und Sicherheitsprotokolle. Amazon SES lässt sich in integrieren AWS CloudTrail , um alle API-Aufrufe zu überwachen. Anhand der von gesammelten Informationen können Kunden feststellen AWS CloudTrail, dass die Anfrage an Amazon SES gestellt wurde, die IP-Adresse der Anfrage, wer die Anfrage gestellt hat, wann die Anfrage gestellt wurde und zusätzliche Details. Weitere Informationen finden Sie unter Protokollieren von Amazon SES-API-Aufrufen mit AWS CloudTrail. Amazon SES bietet auch Methoden zur Überwachung von Sendeaktivitäten wie Sendungen, Ablehnungen, Unzustellbarkeitsraten, Zustellungen, Öffnungen und Klicks. Weitere Informationen finden Sie unter Überwachen Ihrer Amazon SES-Sendeaktivität.

Amazon Simple Queue Service (Amazon SQS)

Kunden sollten die folgenden Schlüsselverschlüsselungsanforderungen verstehen, um Amazon SQS mit PHI verwenden zu können.

- Die Kommunikation mit der Amazon SQS-Warteschlange über die Abfrageanforderung muss mit HTTPS verschlüsselt werden. Weitere Informationen zum Senden von SQS-Anforderungen finden Sie unter Senden von Abfrage-API-Anforderungen.
- Amazon SQS unterstützt die serverseitige Verschlüsselung, die in integriert ist AWS KMS , um Data-at-Rest zu schützen. Durch die zusätzliche serverseitige Verschlüsselung können Kunden vertrauliche Daten mit der erhöhten Sicherheit der Verwendung verschlüsselter Warteschlangen übertragen und empfangen. Die serverseitige Amazon-Amazon SQS-Verschlüsselung verwendet den 256-Bit Advanced Encryption Standard (AES-256-GCM-Algorithmus), um den Text jeder Nachricht zu verschlüsseln. Die Integration mit AWS KMS ermöglicht es Kunden, die Schlüssel, die Amazon SQS-Nachrichten schützen, zusammen mit Schlüsseln, die ihre anderen AWS Ressourcen schützen, zentral zu verwalten. AWS KMS protokolliert jede Verwendung von

Verschlüsselungsschlüsseln, um regulatorische und Compliance-Anforderungen AWS CloudTrail zu erfüllen. Weitere Informationen und um die Region auf Verfügbarkeit für SSE für Amazon SQS zu überprüfen, finden Sie unter Verschlüsselung im Ruhezustand.

- Wenn keine serverseitige Verschlüsselung verwendet wird, muss die Nachrichtennutzlast selbst verschlüsselt werden, bevor sie an SQS gesendet wird. Eine Möglichkeit, die Nachrichtennutzlast zu verschlüsseln, besteht darin, den Amazon SQS Extended Client zusammen mit dem Amazon S3-Verschlüsselungsclient zu verwenden. Weitere Informationen zur Verwendung der clientseitigen Verschlüsselung finden Sie unter Verschlüsseln von Nachrichtennutzlasten mit dem Amazon SQS Extended Client und dem Amazon S3 Encryption Client.

Amazon SQS verwendet CloudTrail, einen Service, der API-Aufrufe protokolliert, die von oder im Namen von Amazon SQS im AWS Konto eines Kunden getätigt wurden, und die Protokolldateien an den angegebenen Amazon S3-Bucket. CloudTrail captures-API-Aufrufe über die Amazon SQS-Konsole oder über die Amazon SQS-API übermittelt. Kunden können anhand der von gesammelten Informationen CloudTrail bestimmen, welche Anforderungen an Amazon SQS gestellt werden, von welcher Quell-IP-Adresse die Anforderung gestellt wird, wer die Anforderung gestellt hat, wann sie gestellt wird usw. Weitere Informationen zum Protokollieren von SQS-Operationen finden Sie unter Protokollieren von Amazon SQS-API-Aufrufen mit AWS CloudTrail.

Amazon Simple Storage Service (Amazon S3)

Kunden haben bei der Verwendung von Amazon S3 mehrere Möglichkeiten, Daten im Ruhezustand zu verschlüsseln, darunter serverseitige und clientseitige Verschlüsselung sowie mehrere Methoden zur Verwaltung von Schlüsseln. Weitere Informationen finden Sie unter Schützen von Daten mithilfe von Verschlüsselung.

Verbindungen zu Amazon S3, die PHI enthalten, müssen Endpunkte verwenden, die verschlüsselten Transport (HTTPS) akzeptieren. Eine Liste der regionalen Endpunkte finden Sie unter AWS -Service-Endpunkte.

Verwenden Sie PHI nicht in Bucket-Namen, Objektnamen oder Metadaten, da diese Daten nicht mit serverseitiger S3-Verschlüsselung verschlüsselt und nicht in clientseitigen Verschlüsselungsarchitekturen verschlüsselt sind.

Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) hilft Entwicklern beim Erstellen, Ausführen und Skalieren von Hintergrundaufträgen mit parallelen oder sequenziellen Schritten. Amazon SWF kann sich als vollständig verwalteter Status-Tracker und Aufgabenkoordinator in der Cloud vorstellen.

Der Amazon Simple Workflow Service wird zur Orchestrierung von Workflows verwendet und kann keine Daten speichern oder übertragen. PHI sollten nicht in Metadaten für Amazon SWF oder in einer Aufgabenbeschreibung platziert werden. Amazon SWF verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

Amazon Textract

Amazon Textract verwendet Machine-Learning-Technologien, um automatisch Text und Daten aus gescannten Dokumenten zu extrahieren, die über die einfache OCR (Optical Character Detection) hinausgehen, um Daten aus Formularen und Tabellen zu identifizieren, zu verstehen und zu extrahieren. Kunden können Amazon Textract beispielsweise verwenden, um Daten automatisch zu extrahieren und Formulare mit geschützten Gesundheitsdaten (Protected Health Information, PHI) zu verarbeiten, ohne dass ein menschliches Eingreifen zur Erfüllung von medizinischen Ansprüchen erforderlich ist.

Amazon Textract kann auch verwendet werden, um die Compliance in Dokumentarchiven aufrechtzuerhalten. Kunden können beispielsweise Amazon Textract verwenden, um Daten aus Versicherungsansprüchen oder medizinischen Rezepten zu extrahieren und Schlüssel-Wert-Paare in diesen Dokumenten automatisch zu erkennen, sodass vertrauliche Paare redigiert werden können.

Amazon Textract unterstützt serverseitige Verschlüsselung (SSE-S3 und SSE-KMS) für Eingabedokumente und TLS-Verschlüsselung für Daten während der Übertragung zwischen dem Service und dem Agenten. Kunden können Amazon CloudWatch verwenden, um Metriken zur Ressourcennutzung AWS CloudTrail zu verfolgen und API-Aufrufe an Amazon Textract zu erfassen.

Amazon Transcribe

Amazon Transcribe verwendet fortschrittliche Machine-Learning-Technologien, um Sprache in Audiodateien zu erkennen und sie in Text zu transkribieren. Kunden können Amazon Transcribe beispielsweise verwenden, um US-Englisch und Spanisches Audio in Text umzuwandeln und Anwendungen zu erstellen, die den Inhalt von Audiodateien enthalten. Amazon Transcribe kann mit Daten verwendet werden, die PHI enthalten. Amazon Transcribe speichert oder speichert keine

Daten und alle Aufrufe der API werden mit SSL/TLS verschlüsselt. Amazon Transcribe verwendet CloudTrail , um alle API-Aufrufe zu protokollieren.

Amazon Translate

Amazon Translate verwendet fortschrittliche Machine-Learning-Technologien, um eine qualitativ hochwertige Übersetzung auf Abruf bereitzustellen. Kunden können Amazon Translate verwenden, um unstrukturierte Textdokumente zu übersetzen oder Anwendungen zu erstellen, die in mehreren Sprachen funktionieren. Dokumente, die PHI enthalten, können mit Amazon Translate verarbeitet werden. Beim Übersetzen von Dokumenten, die PHI enthalten, ist keine zusätzliche Konfiguration erforderlich. Die Verschlüsselung von Daten während der Übertragung wird durch SSL/TLS bereitgestellt und es bleiben keine Daten im Ruhezustand mit Amazon Translate . Amazon Translate verwendet CloudTrail , um alle API-Aufrufe zu protokollieren.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) bietet eine Reihe von Netzwerksicherheitsfunktionen, die gut auf die Architektur von HIPAA-konformen Workloads abgestimmt sind. Funktionen wie zustandslose Netzwerkzugriffskontrolllisten und dynamische Neuzuweisung von Instances in zustandsbehaftete Sicherheitsgruppen bieten Flexibilität beim Schutz der Instances vor unbefugtem Netzwerkzugriff.

Amazon VPC ermöglicht es Kunden auch, ihren eigenen Netzwerkadressraum in zu erweitern AWS und eine Reihe von Möglichkeiten zur Verbindung ihrer Rechenzentren mit bereitzustellen AWS. VPC-Flow-Protokolle bieten einen Audit-Trail für akzeptierte und abgelehnte Verbindungen zur Verarbeitung, Übertragung oder Speicherung von PHI.

AWS Transit Gateway fungiert als Netzwerk-Hub und vereinfacht die Konnektivität zwischen Amazon VPCs und On-Premises-Netzwerken. bietet AWS Transit Gateway auch regionsübergreifende Peering-Funktionen für andere Transit Gateways, um ein globales Netzwerk mithilfe des - AWS Backbones einzurichten. Weitere Informationen zu Amazon VPC finden Sie unter Amazon Virtual Private Cloud.

Amazon WorkDocs

Amazon WorkDocs ist ein vollständig verwalteter, sicherer Service zur Dateispeicherung und -freigabe für Unternehmen mit strengen administrativen Kontrollen und Feedback-Funktionen, die die

Produktivität der Benutzer verbessern. - Amazon WorkDocs Dateien werden im Ruhezustand mit Schlüsseln verschlüsselt, die Kunden über AWS Key Management Service (AWS KMS) verwalten. Alle Daten während der Übertragung werden mit SSL/TLS. AWS web und mobilen Anwendungen sowie Desktop-Sync-Clients verschlüsselt und übertragen Dateien direkt an Amazon WorkDocs mithilfe von SSL/TLS.

Mithilfe der - Amazon WorkDocs Managementkonsole können WorkDocs Administratoren Prüfungsprotokolle anzeigen, um Datei- und Benutzeraktivitäten nach Zeit nachzuverfolgen und zu wählen, ob Benutzern die Freigabe von Dateien für andere außerhalb ihrer Organisation erlaubt werden soll. Amazon WorkDocs ist auch in integriert CloudTrail (ein Service, der API-Aufrufe erfasst, die von oder im Namen von Amazon WorkDocs im AWS Konto des Kunden getätigt wurden), und CloudTrail Protokolldateien an einen von Kunden angegebenen Amazon S3-Bucket übermittelt.

Die Multi-Faktor-Authentifizierung (MFA) mit einem RADIUS-Server ist verfügbar und kann Kunden während des Authentifizierungsprozesses eine zusätzliche Sicherheitsebene bieten. Benutzer melden sich an, indem sie ihren Benutzernamen und ihr Passwort gefolgt von einem OTP (One-Time Passcode) eingeben, das von einem Hardware- oder Software-Token bereitgestellt wird.

Weitere Informationen finden Sie hier:

- Amazon WorkDocs Feature
- Protokollieren von Amazon WorkDocs API-Aufrufen mit AWS CloudTrail

Kunden sollten PHI nicht in Dateinamen oder Verzeichnisnamen speichern.

Amazon WorkSpaces

Amazon WorkSpaces ist eine vollständig verwaltete, sichere D-Service (DaaSesktop-as-a)-Lösung, die auf ausgeführt wird AWS. Mit Amazon können WorkSpacesKunden ihren Benutzern auf einfache Weise virtuelle, cloudbasierte Microsoft-Windows-Desktops bereitstellen und ihnen Zugriff auf die Dokumente, Anwendungen und Ressourcen gewähren, die sie benötigen, überall und jederzeit, von jedem unterstützten Gerät aus.

Amazon WorkSpaces speichert Daten in Volumes von Amazon Elastic Block Store. Kunden können die Speicher-Volumes WorkSpaces des Kunden mit Schlüsseln verschlüsseln, die Kunden über verwalten AWS Key Management Service. Wenn die Verschlüsselung auf einem aktiviert ist WorkSpace, werden sowohl die im Ruhezustand im zugrunde liegenden Speicher gespeicherten Daten als auch die automatisierten Backups (EBS-Snapshots) des Festplattenspeichers gemäß der -

Anleitung verschlüsselt. Die Kommunikation von den WorkSpace Clients zu WorkSpace wird mit SSL/TLS gesichert. Weitere Informationen zur Verschlüsselung von Daten im Ruhezustand mit Amazon WorkSpacesfinden Sie unter Verschlüsselt. WorkSpaces

AWS App Mesh

AWS App Mesh ist ein Servicegitter, das Netzwerknetzwerke auf Anwendungsebene bereitstellt, um Ihren Services die Kommunikation miteinander über mehrere Arten von Datenverarbeitungsinfrastruktur, wie Amazon-ECS-, Amazon-EKS- oder Amazon EC2Services, zu erleichtern. App Mesh konfiguriert Envoy-Proxys so, dass Beobachtbarkeitsdaten erfasst und an den von Ihnen konfigurierten Überwachungssatz übertragen werden, um Ihnen end-to-end Transparenz zu geben. Es kann Datenverkehr basierend auf Routing- und Datenverkehrsrichtlinien weiterleiten, die so konfiguriert sind, dass eine hohe Verfügbarkeit Ihrer Anwendungen gewährleistet ist. Der Datenverkehr zwischen Anwendungen kann für die Verwendung von TLS konfiguriert werden. App Mesh kann mit dem AWS SDK oder dem App-Mesh-Controller für Kubernetes verwendet werden. Während ein HIPAA-berechtigter Service AWS App Mesh ist, sollten keine PHI in Ressourcennamen/Attributen innerhalb von gespeichert werden, AWS App Mesh da der Schutz solcher Daten nicht unterstützt wird. Stattdessen AWS App Mesh kann verwendet werden, um Kundendomänenressourcen zu überwachen, zu kontrollieren und zu sichern, die PHI übertragen oder speichern.

AWS Application Migration Service

AWS Mit Application Migration Service (AWS MGN) können Sie Ihre Server und Anwendungen schnell und ohne Änderungen und mit minimaler Ausfallzeit zu migrieren. AWS MGN ist der primäre Migrationsservice AWS, der für Lift-and-Shift-Migrationen zu empfohlen wird AWS.

AWS MGN verwendet die Datenreplikation auf Blockebene, um Quelldatenträger direkt auf EBS-Volumes im Kundenkonto zu kopieren – die Daten werden niemals über eine von AWS MGN kontrollierte Cloud-Umgebung übertragen. Replizierte Daten werden standardmäßig während der Übertragung verschlüsselt. Daten auf den EBS-Volumes des Kunden werden standardmäßig mit eigenen Schlüsseln eines Kunden verschlüsselt.

AWS Auto Scaling

AWS Auto Scaling ermöglicht es Kunden, die automatische Skalierung für die AWS Ressourcen, die Teil der Anwendung eines Kunden sind, innerhalb weniger Minuten zu konfigurieren. Kunden

können AWS Auto Scaling für eine Reihe von Services verwenden, die PHI betreffen, z. B. Amazon DynamoDB , Amazon ECS, Amazon RDS Aurora-Replikate und Amazon EC2-Instances in einer Auto Scaling-Gruppe.

AWS Auto Scaling ist ein Orchestrierungsservice, der Kundeninhalte nicht direkt verarbeitet, speichert oder überträgt. Aus diesem Grund können Kunden diesen Service mit verschlüsselten Inhalten verwenden. Das - AWS Modell der geteilten Verantwortung gilt für den Datenschutz in AWS Auto Scaling : AWS ist für die AWS Netzwerksicherheitsverfahren verantwortlich, wohingegen der Kunde für die Aufrechterhaltung der Kontrolle über die Inhalte eines Kunden verantwortlich ist, die in dieser Infrastruktur gehostet werden. Dieser Inhalt umfasst die Sicherheitskonfigurations- und Verwaltungsaufgaben für die AWS Services, die Kunden verwenden. Aus Datenschutzgründen empfehlen wir Kunden, die Anmeldeinformationen für AWS -Konten zu schützen und individuelle Benutzerkonten mit AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind.

Es wird dringend empfohlen, dass Kunden niemals sensible identifizierende Informationen wie Kontonummern von Kunden in Freiformfelder wie ein Namensfeld eingeben. Dies gilt auch, wenn Kunden mit AWS Auto Scaling oder anderen - AWS Services unter Verwendung der AWS Management Console, API AWS CLI oder AWS SDKs arbeiten.

Alle Daten, die Kunden in AWS Auto Scaling oder andere Services eingeben, können in Diagnoseprotokolle aufgenommen werden. Wenn Kunden eine URL für einen externen Server bereitstellen, sollten sie keine Anmeldeinformationen in die URL aufnehmen, um ihre Anfrage an diesen Server zu validieren. AWS empfiehlt außerdem, dass Kunden ihre Daten auf folgende Weise schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit - AWS Ressourcen. Wir empfehlen TLS 1.2 oder höher
- Richten Sie die API- und Benutzeraktivitätsprotokollierung mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb AWS von -Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu sichern.

AWS Backup

AWS Backup bietet einen zentralisierten, vollständig verwalteten und richtlinienbasierten Service zum Schutz von Kundendaten und zur Sicherstellung der Compliance über - AWS Services hinweg, um die Geschäftskontinuität zu gewährleisten. Mit können AWS Backup Kunden Datenschutzrichtlinien (Backup) zentral konfigurieren und die Backup-Aktivität über AWS Kundenressourcen hinweg überwachen, einschließlich Amazon EBS-Volumes, Amazon Relational Database Service (Amazon RDS)-Datenbanken (einschließlich Aurora-Clustern), Amazon DynamoDB-Tabellen, Amazon Elastic File System (Amazon EFS), Amazon FSx-Dateisysteme, Amazon EC2-Instances und - AWS Storage Gateway Volumes.

AWS Backup verschlüsselt Kundendaten während der Übertragung und im Ruhezustand. Backups von Services mit vorhandenen Snapshot-Funktionen werden mit der Snapshot-Verschlüsselungsmethode des Quellservice verschlüsselt. Beispielsweise werden EBS-Snapshots mit dem Verschlüsselungsschlüssel des Volumes verschlüsselt, aus dem der Snapshot erstellt wurde.

Backups neuerer AWS Services, die Backup-Funktionen einführen, die auf basieren AWS Backup, wie Amazon EFS, werden unabhängig von den Quellservices während der Übertragung und im Ruhezustand verschlüsselt, wodurch Kunden-Backups eine zusätzliche Schutzebene erhalten. Die Verschlüsselung wird auf Backup-Tresor-Ebene konfiguriert. Der Standardtresor ist verschlüsselt. Wenn Kunden einen neuen Tresor erstellen, muss ein Verschlüsselungsschlüssel ausgewählt werden.

AWS Batch

AWS Batch ermöglicht es Entwicklern, Forschern und Technikern, Hunderttausende von Batch-Computing-Aufträgen einfach und effizient auf auszuführen AWS. stellt AWS Batch dynamisch die optimale Menge und Art von Rechenressourcen (z. B. CPU oder speicheroptimierte Instances) bereit, basierend auf dem Volumen und den spezifischen Ressourcenanforderungen der übermittelten Batch-Aufträge. AWS Batch plant, plant und führt Batch-Computing-Workloads für das gesamte Spektrum an AWS Rechenservices und -funktionen aus.

Ähnlich wie bei Amazon ECS sollte PHI nicht direkt in der Auftragsdefinition, der Auftragswarteschlange oder den Tags für platziert werden AWS Batch. Stattdessen AWS Batch können Aufträge, die mit geplant und ausgeführt werden, mit verschlüsselten PHI arbeiten. Alle Informationen, die von Phasen eines Auftrags an zurückgegeben werden, AWS Batch sollten auch keine PHI enthalten. Immer wenn Aufträge, die von ausgeführt werden, PHI übertragen oder

empfangen AWS Batch müssen, sollte diese Verbindung mit HTTPS oder SSL/TLS verschlüsselt werden.

AWS Certificate Manager

AWS Certificate Manager ist ein Service, mit dem Kunden auf einfache Weise öffentliche und private SSL/TLS-Zertifikate für die Verwendung mit - AWS Services und ihren internen verbundenen Ressourcen bereitstellen, verwalten und bereitstellen können. AWS Certificate Manager verwendet , CloudTrail um alle API-Aufrufe zu protokollieren.

Benutzer benötigen programmgesteuerten Zugriff, wenn sie AWS außerhalb der mit interagieren möchten AWS Management Console. Die Art und Weise, wie programmgesteuerten Zugriff gewährt wird, hängt vom Typ des Benutzers ab, der auf zugreift AWS.

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS SDKs oder AWS APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Konfigurieren der AWS CLI zur Verwendung AWS IAM Identity Center von im AWS Command Line Interface - Benutzerhandbuch. • Informationen zu AWS SDKs , Tools und AWS APIs finden Sie unter IAM-Identity-Center-Authentifizierung im AWS Referenzhandbuch für SDKs und Tools.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS SDKs oder AWS APIs zu signieren.	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit - AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmgesteuerte Anforderungen an die AWS CLI, AWS SDKs oder AWS APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zur AWS CLI finden Sie unter Authentifizierung mit IAM-Benutzeranmeldeinformationen im AWS Command Line Interface -Benutzerhandbuch. • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im AWS Referenzhandbuch für SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

AWS Cloud Map

AWS Cloud Map ist ein Service zur Erkennung von Cloud-Ressourcen. Mit AWS Cloud Map können Kunden benutzerdefinierte Namen für Anwendungsressourcen wie Amazon ECS-Aufgaben, Amazon EC2-Instances, Amazon S3-Buckets, Amazon DynamoDB-Tabellen, Amazon SQS-Warteschlangen oder andere Cloud-Ressourcen definieren. Kunden können diese benutzerdefinierten Namen dann verwenden, um den Speicherort und die Metadaten von Cloud-Ressourcen aus ihren Anwendungen mithilfe des AWS SDK und authentifizierter API-Abfragen zu ermitteln. AWS Cloud Map ist zwar ein HIPAA-berechtigter Service, es sollte jedoch kein PHI in Ressourcennamen/Attributen in AWS Cloud Map gespeichert werden, da der Schutz solcher Daten nicht unterstützt wird. Stattdessen kann AWS Cloud Map verwendet werden, um Kundendomänenressourcen zu ermitteln, die PHI übertragen oder speichern.

AWS CloudFormation

AWS CloudFormation ermöglicht es Kunden, AWS-Infrastrukturbereitstellungen vorhersehbar und wiederholt zu erstellen und bereitzustellen. Es hilft Kunden dabei, AWS-Produkte wie Amazon EC2, Amazon Elastic Block Store, Amazon SNS ,Elastic Load Balancing und Auto Scaling zu nutzen, um äußerst zuverlässige, hochgradig skalierbare und kostengünstige Anwendungen in der Cloud zu erstellen, ohne sich Gedanken über die Erstellung und Konfiguration der zugrunde liegenden AWS-Infrastruktur machen zu müssen. AWS CloudFormation ermöglicht Kunden, eine Vorlagendatei zu verwenden, um eine Sammlung von Ressourcen als eine Einheit (einen Stack) zu erstellen und zu löschen. Auto Scaling

AWS CloudFormation speichert, überträgt oder verarbeitet PHI nicht selbst. Stattdessen wird es verwendet, um Architekturen zu erstellen und bereitzustellen, die andere AWS-Services verwenden, die PHI speichern, übertragen und/oder verarbeiten können. Nur HIPAA-berechtigte Services sollten mit PHI verwendet werden. Anleitungen zur Verwendung von PHI mit diesen Services finden Sie in den Einträgen für diese Services in diesem Whitepaper. AWS CloudFormation verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS CloudHSM

AWS CloudHSM ist ein cloudbasiertes Hardware-Sicherheitsmodul (HSM), mit dem Kunden einfach ihre eigenen Verschlüsselungsschlüssel in der AWS Cloud generieren und verwenden können. Mit CloudHSM können Kunden ihre eigenen Verschlüsselungsschlüssel mithilfe von FIPS 140-2 Level 3 validierten HSMs verwalten. CloudHSM bietet Kunden die Flexibilität, mithilfe offener Standard-APIs

wie PKCS#11, Java Cryptography Extensions (JCE) und Microsoft CryptoNG (CNG)-Bibliotheken in ihre Anwendungen zu integrieren.

CloudHSM ist auch standardkonform und ermöglicht es Kunden, alle ihre Schlüssel in die meisten anderen kommerziell verfügbaren HSMs zu exportieren. Wie AWS CloudHSM ein Hardware-Appliance-Schlüsselverwaltungsservice kann er PHI nicht speichern oder übertragen. Kunden sollten PHI nicht in Tags (Metadaten) speichern. Es sind keine weiteren speziellen Anleitungen erforderlich.

AWS CloudTrail

AWS CloudTrail ist ein Service, der Governance, Compliance, Betriebsprüfung und Risikoprüfung von AWS-Konten ermöglicht. Mit können CloudTrailKunden Kontoaktivitäten im Zusammenhang mit Aktionen in ihrer gesamten AWS-Infrastruktur protokollieren, kontinuierlich überwachen und beibehalten. CloudTrail stellt den Ereignisverlauf ihrer AWS-Kontoaktivitäten bereit, einschließlich Aktionen, die über die AWS Management Console, AWS SDKs, Befehlszeilen-Tools und andere AWS-Services durchgeführt werden. Dieser Ereignisverlauf vereinfacht die Sicherheitsanalyse, die Nachverfolgung von Ressourcenänderungen und die Fehlerbehebung.

AWS CloudTrail ist für die Verwendung mit allen AWS-Konten aktiviert und kann für die Prüfungsprotokollierung verwendet werden, wie es die AWS BAA erfordert. Spezifische Trails sollten mit der CloudTrail Konsole oder der AWS Command Line Interface erstellt werden. CloudTrail verschlüsselt den gesamten Datenverkehr während der Übertragung und im Ruhezustand, wenn ein verschlüsselter Trail erstellt wird. Ein verschlüsselter Trail sollte erstellt werden, wenn das Potenzial besteht, PHI zu protokollieren.

Standardmäßig speichert ein verschlüsselter Trail Einträge in Amazon S3 mit serverseitiger Verschlüsselung mit von Amazon S3 (SSE-S3) verwalteten Schlüsseln. Wenn eine zusätzliche Verwaltung über Schlüssel gewünscht wird, kann sie auch mit von AWS KMS verwalteten Schlüsseln (SSE-KMS) konfiguriert werden. Wie das endgültige Ziel für AWS-Protokolleinträge CloudTrail ist, sollte daher eine kritische Komponente jeder Architektur, die PHI verarbeitet, die Integritätsvalidierung von CloudTrail Protokolldateien aktiviert und die zugehörigen CloudTrail Digest-Dateien regelmäßig überprüft werden. Nach der Aktivierung kann eine positive Aussage erstellt werden, dass die Protokolldateien nicht geändert wurden.

AWS CodeBuild

AWS CodeBuild ist ein vollständig verwalteter Build-Service in der Cloud. AWS CodeBuild kompiliert Quellcode, führt Einheitentests durch und erzeugt Artefakte, die bereitgestellt werden können. AWS

CodeBuild verwendet einen AWS KMS -Schlüssel, um Build-Ausgabeartefakte zu verschlüsseln. Ein KMS-Schlüssel sollte erstellt und konfiguriert werden, bevor Artefakte erstellt werden, die PHI, Secrets/Passwörter, Zertifikate usw. enthalten, die AWS CodeBuild verwendet, AWS CloudTrail um alle API-Aufrufe zu protokollieren.

AWS CodeDeploy

AWS CodeDeploy ist ein vollständig verwalteter Bereitstellungsservice, der Softwarebereitstellungen für eine Vielzahl von Datenverarbeitungsservices automatisiert AWS Fargate, darunter Amazon EC2 AWS Lambda und On-Premises-Server. Kunden verwenden AWS CodeDeploy , um schnell neue Features der containerisierten Workload zu veröffentlichen und die Komplexität der Aktualisierung von Anwendungen zu bewältigen.

AWS CodeDeploy unterstützt serverseitige Verschlüsselung (SSE-S3) für Bereitstellungsartefakte und TLS-Verschlüsselung für Daten während der Übertragung zwischen dem Service und dem Agenten. Kunden können Amazon CloudWatch Events verwenden, um Bereitstellungen AWS CloudTrail zu verfolgen und API-Aufrufe an zu erfassen AWS CodeDeploy.

AWS CodeCommit

AWS CodeCommit ist ein sicherer, hochgradig skalierbarer, verwalteter Service zur Quellcodeverwaltung, der private Git-Repositorys hostet. AWS CodeCommit macht es überflüssig, dass Kunden ihr eigenes Quellcodeverwaltungssystem verwalten oder sich Gedanken über die Skalierung ihrer Infrastruktur machen.

AWS CodeCommit verschlüsselt den gesamten Datenverkehr und die gespeicherten Informationen während der Übertragung und im Ruhezustand. Wenn ein Repository in erstellt wird AWS CodeCommit, wird standardmäßig ein von AWS verwalteter Schlüssel mit erstellt AWS KMS und nur von diesem Repository verwendet, um alle im Ruhezustand gespeicherten Daten zu verschlüsseln. AWS CodeCommit verwendet , um alle API-Aufrufe AWS CloudTrail zu protokollieren.

AWS CodePipeline

AWS CodePipeline ist ein vollständig verwalteter kontinuierlicher Bereitstellungsservice, der Kunden hilft, Kunden-Release-Pipelines für schnelle und zuverlässige Anwendungs- und Infrastrukturaktualisierungen zu automatisieren. Kunden verwenden AWS CodePipeline , um es Forschern zu ermöglichen, automatisch Patientendaten zu verarbeiten, Laborergebnisse und genomische Daten sind einige Beispiele für die Workflow-Pipeline, die von Kunden verwendet wird.

AWS CodePipeline unterstützt serverseitige Verschlüsselung (SSE-S3 und SSE-KMS) für Code-Artefakte und TLS-Verschlüsselung für Daten während der Übertragung zwischen dem Service und dem Agenten. Kunden können Amazon CloudWatch Events verwenden, um Pipeline-Änderungen AWS CloudTrail zu verfolgen und API-Aufrufe an zu erfassen AWS CodePipeline.

AWS Config

AWS Config bietet einen detaillierten Überblick über die Ressourcen, die mit dem AWS-Konto eines Kunden verknüpft sind, einschließlich der Konfiguration, der Beziehung zueinander und der Änderung der Konfigurationen und ihrer Beziehungen im Laufe der Zeit.

AWS Config kann nicht selbst zum Speichern oder Übertragen von PHI verwendet werden.

Stattdessen kann es genutzt werden, um Architekturen zu überwachen und zu bewerten, die mit anderen AWS-Services erstellt wurden, einschließlich Architekturen, die PHI verarbeiten, um festzustellen, ob sie mit ihrem beabsichtigten Designziel konform bleiben. Architekturen, die PHI verarbeiten, sollten nur mit HIPAA-fähigen Services erstellt werden. AWS Config verwendet AWS CloudTrail , um alle Ergebnisse zu protokollieren.

AWS Data Exchange

AWS Data Exchange erleichtert das Suchen, Abonnieren und Verwenden von Daten von Drittanbietern in der Cloud. Nach dem Abonnieren eines Datenprodukts können Kunden die AWS Data Exchange-API verwenden, um Daten direkt in Amazon S3 zu laden und sie dann mit einer Vielzahl von AWS-Analyse- und Machine Learning-Services zu analysieren. Für Datenanbieter macht AWS Data Exchange es einfach, die Millionen von AWS-Kunden zu erreichen, die in die Cloud migrieren, indem die Notwendigkeit entfällt, Infrastruktur für Datenspeicherung, Bereitstellung, Fakturierung und Berechtigung aufzubauen und zu verwalten.

AWS Data Exchange verschlüsselt immer alle im Service gespeicherten Datenprodukte im Ruhezustand, ohne dass eine zusätzliche Konfiguration erforderlich ist. Diese Verschlüsselung erfolgt automatisch über einen serviceverwalteten KMS-Schlüssel. AWS Data Exchange verwendet Transport Layer Security (TLS) und clientseitige Verschlüsselung für die Verschlüsselung während der Übertragung. Die Kommunikation mit AWS Data Exchange erfolgt immer über HTTPS, sodass die Daten der Kunden während der Übertragung immer verschlüsselt werden. Diese Verschlüsselung ist standardmäßig konfiguriert, wenn Kunden AWS Data Exchange verwenden. Weitere Informationen finden Sie unter Datenschutz in AWS Data Exchange.

AWS Data Exchange ist in integriert AWS CloudTrail. AWS CloudTrail erfasst alle Aufrufe an AWS Data Exchange-APIs als Ereignisse, einschließlich Aufrufen von der AWS Data Exchange-Konsole und von Codeaufrufen an die AWS Data Exchange-API-Operationen. Einige Maßnahmen, die Kunden ergreifen können, sind reine Konsolenaktionen. Es gibt keine entsprechende API im AWS SDK oder in der AWS CLI. Dies sind Aktionen, die auf - AWS Marketplace Funktionen basieren, z. B. das Veröffentlichen oder Abonnieren eines Produkts. AWS Data Exchange stellt CloudTrail Protokolle für eine Teilmenge dieser reinen Konsolenaktionen bereit. Weitere Informationen finden Sie unter Protokollieren von AWS Data Exchange-API-Aufrufen mit AWS CloudTrail.

Bitte beachten Sie, dass alle Auflistungen, die AWS Data Exchange verwenden, den Veröffentlichungsrichtlinien von AWS Data Exchange und FAQs gestellten Fragen zum AWS Data Exchange für AWS Marketplace Anbieter entsprechen müssen, die bestimmte Datenkategorien einschränken. Weitere Informationen finden Sie unter AWS Data Exchange – FAQs Fragen.

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) unterstützt Kunden bei der einfachen und sicheren Migration von Datenbanken zu AWS. Kunden können ihre Daten zu und von den gängigsten kommerziellen und Open-Source-Datenbanken wie Oracle, MySQL und PostgreSQL migrieren. Der Service unterstützt sowohl homogene Migrationen (z. B. Oracle zu Oracle) als auch heterogene Migrationen mit verschiedenen Datenbankplattformen (z. B. Oracle zu PostgreSQL oder MySQL zu Oracle).

Datenbanken, die On-Premises ausgeführt werden und mit AWS DMS in die Cloud migriert werden, können PHI-Daten enthalten. AWS DMS verschlüsselt Daten während der Übertragung und wenn Daten für die endgültige Migration in die Zieldatenbank in AWS bereitgestellt werden. AWS DMS verschlüsselt den von einer Replikations-Instance verwendeten Speicher und die Endpunktverbindungsinformationen. Um den von einer Replikations-Instance verwendeten Speicher zu verschlüsseln, verwendet AWS DMS einen - AWS KMS Schlüssel, der für das AWS-Konto eindeutig ist. Lesen Sie die -Anleitung für die entsprechende Zieldatenbank, um sicherzustellen, dass Daten nach Abschluss der Migration verschlüsselt bleiben. AWS DMS verwendet CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS DataSync

AWS DataSync ist ein Online-Übertragungsservice, der das Verschieben von Daten zwischen On-Premises-Speicher und AWS vereinfacht, automatisiert und beschleunigt. Kunden können

AWS verwenden DataSync , um ihre Datenquellen entweder mit Amazon S3 oder Amazon EFS zu verbinden. Kunden sollten sicherstellen, dass Amazon S3 und Amazon EFS auf eine Weise konfiguriert sind, die der -Anleitung entspricht. Standardmäßig werden Kundendaten während der Übertragung mit TLS 1.2 verschlüsselt. Weitere Informationen zur Verschlüsselung und zu AWS DataSyncfinden Sie unter AWS DataSync-Funktionen. Kunden können DataSync Aktivitäten mit überwachen AWS CloudTrail. Weitere Informationen zur Protokollierung mit CloudTrailfinden Sie unter Protokollieren von AWS DataSync -API-Aufrufen mit AWS CloudTrail.

AWS Directory Service

AWS Directory Service für Microsoft AD

AWS Directory Service for Microsoft Active Directory (Enterprise Edition), auch bekannt als AWS Microsoft AD, ermöglicht es verzeichnisfähigen Workloads und AWS-Ressourcen, verwaltetes Active Directory in der AWS Cloud zu verwenden. AWS Microsoft AD speichert Verzeichnisinhalte (einschließlich Inhalte, die PHI enthalten) in verschlüsselten Amazon Elastic Block Store-Volumes mithilfe von Verschlüsselungsschlüsseln, die AWS verwaltet. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung.

Daten während der Übertragung zu und von Active-Directory-Clients werden verschlüsselt, wenn sie über das Lightweight Directory Access Protocol (LDAP) über das Amazon Virtual Private Cloud (VPC)-Netzwerk des Kunden übertragen werden. Wenn sich ein Active-Directory-Client in einem On-Premises-Netzwerk befindet, wird der Datenverkehr über einen Virtual Private Network Link oder einen - AWS Direct Connect Link zur VPC des Kunden geleitet.

Amazon Cloud Directory

Amazon Cloud Directory ermöglicht es Kunden, flexible cloudnative Verzeichnisse für die Organisation von Datenhierarchien über mehrere Dimensionen hinweg zu erstellen. Kunden können auch Verzeichnisse für eine Vielzahl von Anwendungsfällen erstellen, z. B. Organigramme, Kurskataloge und Geräteregistrierungen. Kunden können beispielsweise ein Organisationsdiagramm erstellen, das durch separate Hierarchien für Berichtsstruktur, Standort und Kostenstelle navigiert werden kann. Amazon Cloud Directory verschlüsselt Daten im Ruhezustand und während der Übertragung automatisch mithilfe von 256-Bit-Verschlüsselungsschlüsseln, die von AWS Key Management Service () verwaltet werden AWS KMS.

AWS Elastic Beanstalk

Mit können Kunden Anwendungen in der AWS Cloud schnell bereitstellen und verwalten AWS Elastic Beanstalk, ohne mehr über die Infrastruktur erfahren zu müssen, die diese Anwendungen ausführt. Kunden können einfach Code hochladen und die Bereitstellung AWS Elastic Beanstalk automatisch übernehmen, von der Kapazitätsbereitstellung, dem Load Balancing, der automatischen Skalierung bis hin zur Überwachung des Anwendungsstatus. Gleichzeitig behalten Kunden die volle Kontrolle über die AWS-Ressourcen, die ihre Anwendung unterstützen, und können jederzeit auf die zugrunde liegenden Ressourcen zugreifen.

AWS Elastic Beanstalk speichert, überträgt oder verarbeitet PHI nicht selbst. Stattdessen können Kunden damit Architekturen mit anderen AWS-Services erstellen und bereitstellen, die PHI möglicherweise speichern, übertragen und/oder verarbeiten. Kunden sollten sicherstellen, dass bei der Auswahl der Services, die von bereitgestellt werden AWS Elastic Beanstalk , nur HIPAA-berechtigte Services mit PHI verwendet werden. Anleitungen zur Verwendung von PHI mit diesen Services finden Sie in den Einträgen für diese Services in diesem Whitepaper.

Kunden sollten PHI nicht in Freiformfelder in aufnehmen, z. AWS Elastic Beanstalk B. im Feld Name. AWS Elastic Beanstalk verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery (AWS DRS) minimiert Ausfallzeiten und Datenverluste durch schnelle, zuverlässige Wiederherstellung von On-Premises- und Cloud-basierten Anwendungen mit kostengünstigem Speicher, minimaler Rechenleistung und point-in-time Wiederherstellung.

Kunden können AWS Elastic Disaster Recovery auf ihren Quellservern einrichten, um eine sichere Datenreplikation zu initiieren. Ihre Daten werden in ein Staging-Bereich-Subnetz in Ihrem AWS-Konto in der ausgewählten AWS-Region repliziert. Das Staging-Bereichsdesign senkt die Kosten, indem es kostengünstigen Speicher und minimale Rechenressourcen verwendet, um die fortlaufende Replikation aufrechtzuerhalten. Von AWS Elastic Disaster Recovery replizierte Kundendaten werden während der Übertragung mit TLS 1.2 verschlüsselt und direkt von ihren Quellservern in ihre VPC übertragen. Kunden können private Konnektivität wie AWS Direct Connect oder VPN nutzen, um die Replikationsroute zu konfigurieren. Kundendaten können auch im Ruhezustand auf AWS mit Amazon EBS-Verschlüsselung verschlüsselt werden.

Kunden können unterbrechungsfreie Tests durchführen, um sicherzustellen, dass die Implementierung abgeschlossen ist. Sorgen Sie während des normalen Betriebs für die Bereitschaft,

indem Sie die Replikation überwachen und regelmäßig unterbrechungsfreie Wiederherstellungs- und Failback-Drosselungen durchführen. Wenn Kunden Anwendungen wiederherstellen müssen, können sie Wiederherstellungs-Instances auf AWS innerhalb weniger Minuten starten, wobei sie den up-to-date Serverstatus oder einen früheren Zeitpunkt verwenden. Nachdem Kundenanwendungen auf AWS ausgeführt wurden, können sie sie dort bleiben lassen oder die Datenreplikation zurück zum primären Standort initiieren, wenn das Problem behoben ist. Kunden können jederzeit wieder zu ihrem primären Standort zurückkehren.

AWS Fargate

AWS Fargate ist eine Technologie, mit der Kunden Container ausführen können, ohne Server oder Cluster verwalten zu müssen. Mit müssen AWS Fargate Kunden keine Cluster virtueller Maschinen mehr bereitstellen, konfigurieren und skalieren, um Container auszuführen. Dadurch entfällt die Notwendigkeit, Servertypen zu wählen, zu entscheiden, wann Cluster skaliert oder die Cluster-Verpackung optimiert werden sollen. AWS Fargate macht es Kunden überflüssig, mit Servern oder Clustern zu interagieren oder über diese zu denken. Mit Fargate konzentrieren sich Kunden auf das Entwerfen und Erstellen ihrer Anwendungen, anstatt die Infrastruktur zu verwalten, auf der sie ausgeführt werden.

Fargate benötigt keine zusätzliche Konfiguration, um mit Workloads zu arbeiten, die PHI verarbeiten. Kunden können Container-Workloads auf Fargate mithilfe von Container-Orchestrierungsservices wie Amazon ECS ausführen. Fargate verwaltet nur die zugrunde liegende Infrastruktur und arbeitet nicht mit oder auf Daten innerhalb des zu orchestrierenden Workloads. Im Einklang mit den HIPAA-Anforderungen sollte PHI bei jedem Transit oder im Ruhezustand verschlüsselt werden, wenn auf Container zugegriffen wird, die mit Fargate gestartet wurden. Für jede in diesem Dokument beschriebene AWS-Speicheroption sind verschiedene Mechanismen für die Verschlüsselung von Daten im Ruhezustand verfügbar. Weitere Informationen zur HIPAA-Sicherheit und -Konfiguration finden Sie im Whitepaper Architekturerstellung für HIPAA-Sicherheit und -Compliance in Amazon EKS.

AWS Firewall Manager

AWS Firewall Manager ist ein Sicherheitsverwaltungsservice, mit dem Kunden Firewall-Regeln für Kundenkonten und Anwendungen in zentral konfigurieren und verwalten können AWS Organizations. Wenn neue Anwendungen erstellt werden, erleichtert Firewall Manager die Compliance neuer Anwendungen und Ressourcen durch Durchsetzung eines gemeinsamen Satzes von Sicherheitsregeln. Jetzt verfügen Kunden über einen einzigen Service, um von einem zentralen

Administratorkonto aus Firewall-Regeln zu erstellen, Sicherheitsrichtlinien zu erstellen und diese konsistent und hierarchisch in ihrer gesamten Infrastruktur durchzusetzen.

AWS Firewall Manager ist ein Orchestrierungsservice, der Benutzerdaten nicht direkt verarbeitet, speichert oder überträgt. Der Service verschlüsselt keine Kundeninhalte, aber die zugrunde liegenden Services, die AWS Firewall Manager verwendet, wie DynamoDB, verschlüsseln Benutzerdaten.

AWS Global Accelerator

AWS Global Accelerator ist ein globaler Load-Balancing-Service, der die Verfügbarkeit und Latenz von Anwendungen mit mehreren Regionen verbessert. Um sicherzustellen, dass PHI während der Übertragung und im Ruhezustand verschlüsselt bleibt, während verwendet wird AWS Global Accelerator, sollten Architekturen, die von Global Accelerator ausgelastet werden, ein verschlüsseltes Protokoll wie HTTPS oder SSL/TLS verwenden. Lesen Sie die Anleitungen für Amazon EC2, Elastic Load Balancing und andere AWS-Services, um die verfügbaren Verschlüsselungsoptionen für Backend-Ressourcen besser zu verstehen. AWS Global Accelerator verwendet , um alle API-Aufrufe AWS CloudTrail zu protokollieren.

AWS Glue

AWS Glue ist ein vollständig verwalteter ETL-Service (Extrahieren, Transformieren und Laden), der es Kunden einfach und kostengünstig macht, ihre Daten zu kategorisieren, zu bereinigen, anzureichern und sie zuverlässig zwischen verschiedenen Datenspeichern zu verschieben. Um die Verschlüsselung von Daten sicherzustellen, die PHI während der Übertragung enthalten, sollten Sie für die Verwendung von JDBC-Verbindungen zu Datenspeichern mit SSL/TLS konfiguriert AWS Glue sein. Um die Verschlüsselung während der Übertragung aufrechtzuerhalten, sollte die Einstellung für serverseitige Verschlüsselung (SSE-S3) als Parameter an ETL-Aufträge übergeben werden, die mit ausgeführt werden AWS Glue. Alle Daten, die im Ruhezustand im Data Catalog von gespeichert werden, AWS Glue werden mit Schlüsseln verschlüsselt, die von verwaltet werden AWS KMS , wenn die Verschlüsselung bei der Erstellung eines Data-Catalog-Objekts aktiviert ist. AWS Glue verwendet CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Glue DataBrew

AWS Glue DataBrew ist ein vollständig verwalteter Service zur visuellen Datenvorbereitung, mit dem Datenanalysten und Datenwissenschaftler Daten bereinigen und normalisieren können, um sie für

Analysen und Machine Learning vorzubereiten. Um die Verschlüsselung von Daten sicherzustellen, die PHI während der Übertragung enthalten, sollten Sie für die Verwendung von JDBC-Verbindungen zu Datenspeichern mit SSL/TLS konfiguriert DataBrew werden. Wenn Sie eine Verbindung zu JDBC-Datenquellen herstellen, DataBrew verwendet die Einstellungen für Ihre AWS Glue-Verbindung, einschließlich der Option „SSL-Verbindung erforderlich“. Um die Verschlüsselung im Ruhezustand in S3-Buckets aufrechtzuerhalten, sollte außerdem die Einstellung für serverseitige Verschlüsselung (SSE-S3 oder SSE-KMS) als Parameter an - DataBrew Aufträge übergeben werden.

AWS IoT Core und AWS IoT Device Management

AWS IoT Core und AWS IoT Device Management bieten eine sichere, bidirektionale Kommunikation zwischen mit dem Internet verbundenen Geräten, wie Sensoren, Aktuatoren, eingebetteten Mikrocontrollern oder Smart-Appliances, und dem AWS Cloud. AWS IoT Core und AWS IoT Device Management können jetzt Geräte unterbringen, die Daten übertragen, die PHI enthalten. Die gesamte Kommunikation mit AWS IoT Core und AWS IoT Device Management wird mit TLS. AWS IoT Core verschlüsselt und AWS IoT Device Management verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS IoT Greengrass

AWS IoT Greengrass Mit können Kunden lokale Datenverarbeitungs-, Messaging-, Daten-Caching-, Synchronisierungs- und ML-Inferenzfunktionen für verbundene Geräte auf sichere Weise ausführen. AWS IoT Greengrass verwendet X.509-Zertifikate, verwaltete Abonnements, AWS IoT Richtlinien und IAM-Richtlinien und -Rollen, um sicherzustellen, dass die Greengrass-Anwendungen des Kunden sicher sind. AWS IoT Greengrass verwendet das AWS IoT Transportsicherheitsmodell, um die Kommunikation mit der Cloud mithilfe von TLS zu verschlüsseln. Darüber hinaus werden AWS IoT Greengrass Daten im Ruhezustand (in der Cloud) verschlüsselt. Weitere Informationen zur Greengrass-Sicherheit finden Sie unter Übersicht über die AWS IoT Greengrass Sicherheit.

Kunden können AWS IoT Greengrass API-Aktionen mit protokollieren AWS CloudTrail. Weitere Informationen finden Sie unter Protokollieren von AWS IoT Greengrass API-Aufrufen mit AWS CloudTrail.

AWS Lambda

AWS Lambda Mit können Kunden Code ausführen, ohne selbst Server bereitstellen oder verwalten zu müssen. AWS Lambda verwendet eine Datenverarbeitungsflotte von Amazon Elastic Compute

Cloud (Amazon EC2)-Instances über mehrere Availability Zones in einer Region hinweg, die die hohe Verfügbarkeit, Sicherheit, Leistung und Skalierbarkeit der AWS-Infrastruktur bietet.

Um sicherzustellen, dass PHI bei der Verwendung von verschlüsselt bleibt AWS Lambda, sollten Verbindungen zu externen Ressourcen ein verschlüsseltes Protokoll wie HTTPS oder SSL/TLS verwenden. Wenn beispielsweise von einer Lambda-Prozedur aus auf S3 zugegriffen wird, sollte es mit https://bucket.s3-aws-region.amazonaws.com. adressiert werden.

Wenn PHI in einem laufenden Verfahren im Ruhezustand platziert oder inaktiv sind, sollte sie client- oder serverseitig mit Schlüsseln verschlüsselt werden, die von AWS KMS oder bezogen wurden AWS CloudHSM. Folgen Sie den entsprechenden Anweisungen für Amazon API Gateway, wenn Sie AWS Lambda Funktionen über den Service auslösen. Wenn Ereignisse von anderen AWS-Services zum Auslösen von AWS Lambda Funktionen verwendet werden, sollten die Ereignisdaten keine (internen und eigenständigen) PHI enthalten. Wenn beispielsweise eine Lambda-Prozedur von einem S3-Ereignis ausgelöst wird, z. B. bei der Ankunft eines Objekts in S3, sollte der Objektname, der an Lambda weitergeleitet wird, keine PHI haben, obwohl das Objekt selbst solche Daten enthalten kann.

AWS Managed Services

AWS Managed Services bietet eine kontinuierliche Verwaltung der AWS-Infrastrukturen. Durch die Implementierung bewährter Methoden zur Wartung der Infrastruktur eines Kunden AWS Managed Services hilft dabei, seinen betrieblichen Aufwand und sein Risiko zu reduzieren. AWS Managed Services automatisiert allgemeine Aktivitäten wie Änderungsanforderungen, Überwachung, Patch-Management, Sicherheit und Backup-Services und bietet Services mit vollem Lebenszyklus, um Infrastrukturen bereitzustellen, auszuführen und zu unterstützen.

Kunden können verwenden, AWS Managed Services um AWS-Workloads zu verwalten, die mit Daten arbeiten, die PHI enthalten. Die Verwendung von ändert AWS Managed Services nichts an den AWS-Services, die für die Verwendung mit PHI in Frage kommen. Tools und Automatisierung von AWS Managed Services können nicht für die Speicherung oder Übertragung von PHI verwendet werden.

AWS OpsWorks für Chef Automate

AWS OpsWorks for Chef Automate ist ein vollständig verwalteter Konfigurationsverwaltungsservice, der Chef Automate hostet, eine Reihe von Automatisierungstools von Chef für Infrastruktur und Anwendungsmanagement. Der Service selbst enthält, überträgt oder verarbeitet keine PHI oder sensiblen Informationen, aber Kunden sollten sicherstellen, dass alle von OpsWorks für Chef

Automate konfigurierten Ressourcen im Einklang mit der -Anleitung konfiguriert sind. API-Aufrufe werden mit erfasst AWS CloudTrail. Weitere Informationen finden Sie unter Protokollieren von AWS OpsWorks Stacks-API-Aufrufen mit AWS CloudTrail.

AWS OpsWorks für Puppet Enterprise

AWS OpsWorks for Puppet Enterprise ist ein vollständig verwalteter Konfigurationsverwaltungsservice, der Puppet Enterprise hostet, eine Reihe von Automatisierungstools von Puppet für Infrastruktur- und Anwendungsmanagement. Der Service selbst enthält, überträgt oder verarbeitet keine PHI oder sensiblen Informationen, aber Kunden sollten sicherstellen, dass alle von OpsWorks für Puppet Enterprise konfigurierten Ressourcen im Einklang mit der -Anleitung konfiguriert sind. API-Aufrufe werden mit erfasst AWS CloudTrail. Weitere Informationen finden Sie unter Protokollieren von AWS OpsWorks Stacks-API-Aufrufen mit AWS CloudTrail.

AWS OpsWorks Stack

AWS OpsWorks Stacks bietet eine einfache und flexible Möglichkeit, Stacks und Anwendungen zu erstellen und zu verwalten. Kunden können AWS OpsWorks Stacks verwenden, um Anwendungen in ihren Stacks bereitzustellen und zu überwachen.

AWS OpsWorks Stacks verschlüsselt den gesamten Datenverkehr während der Übertragung. Verschlüsselte Datenmengen (ein Chef-Datenspeichermechanismus) sind jedoch nicht verfügbar und alle Komponenten, die sicher gespeichert werden müssen, wie PHI, Secrets/Passwörter, Zertifikate usw., sollten in einem verschlüsselten Bucket in Amazon S3 gespeichert werden. AWS OpsWorks Stack verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Organizations

AWS Organizations hilft Kunden dabei, ihre Umgebung zentral zu verwalten und zu verwalten, wenn sie ihre AWS-Ressourcen wachsen und skalieren. Mithilfe von können AWS Organizations sie programmgesteuert neue AWS-Konten erstellen und Ressourcen zuweisen, Konten gruppieren, um ihre Workflows zu organisieren, Richtlinien für die Verwaltung auf Konten oder Gruppen anwenden und die Abrechnung vereinfachen, indem sie eine einzige Zahlungsweise für alle Konten verwenden.

Darüber hinaus AWS Organizations ist in andere AWS-Services integriert, sodass Kunden zentrale Konfigurationen, Sicherheitsmechanismen, Prüfungsanforderungen und die gemeinsame Nutzung

von Ressourcen über Konten in ihrer Organisation hinweg definieren können. AWS Organizations ist für alle AWS-Kunden ohne zusätzliche Kosten verfügbar.

AWS Organizations ist ein Orchestrierungsservice, der Benutzerdaten nicht direkt verarbeitet, speichert oder überträgt. Der Service verschlüsselt keine Kundeninhalte, aber die zugrunde liegenden Services, die in gestartet werden AWS Organizations, verschlüsseln Benutzerdaten. AWS Organizations ist in integriert, einem Service AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service in durchgeführten Aktionen bietet AWS Organizations.

AWS RoboMaker

AWS RoboMaker ermöglicht es Kunden, Code in der Cloud für die Anwendungsentwicklung auszuführen, und bietet einen Robotersimulationsservice zur Beschleunigung von Anwendungstests. AWS RoboMaker bietet auch einen Roboterflottenverwaltungsservice für die Bereitstellung, Aktualisierung und Verwaltung von Remote-Anwendungen.

Netzwerkverkehr, der PHI enthält, muss Daten während der Übertragung verschlüsseln. Die gesamte Verwaltungskommunikation mit dem Simulationsserver erfolgt über TLS, und Kunden sollten offene Standard-Transportverschlüsselungsmechanismen für Verbindungen zu anderen AWS-Services verwenden. AWS lässt sich RoboMaker auch in integrieren CloudTrail , um alle API-Aufrufe in einem bestimmten Amazon S3-Bucket zu protokollieren.

AWS- RoboMaker Protokolle enthalten keine PHI und die vom Simulationsserver verwendeten EBS-Volumes werden verschlüsselt. Bei der Übertragung von Daten, die PHI enthalten können, an andere -Services wie Amazon S3 müssen Kunden die Anweisungen des empfangenden Services zum Speichern von PHI befolgen. Für Bereitstellungen an Roboter müssen Kunden sicherstellen, dass die Verschlüsselung von Daten während der Übertragung und im Ruhezustand mit ihrer Interpretation der -Anleitung übereinstimmt.

AWS SDK-Metriken

Unternehmenskunden können den AWS- CloudWatch Agenten mit AWS SDK Metrics for Enterprise Support (SDK Metrics) verwenden, um Metriken von AWS SDKs auf ihren Hosts und Clients zu sammeln. Diese Metriken werden mit AWS Enterprise Support geteilt. SDK-Metriken können Kunden dabei helfen, relevante Metriken und Diagnosedaten über die Verbindungen ihrer Anwendung zu AWS-Services zu sammeln, ohne ihrem Code eine benutzerdefinierte Instrumentierung

hinzuzufügen, und reduzieren den manuellen Aufwand, der für die Freigabe von Protokollen und Daten mit erforderlich ist AWS Support.

Bitte beachten Sie, dass SDK-Metriken nur für AWS-Kunden mit einem Enterprise Support-Abonnement verfügbar sind. Kunden können SDK Metrics mit jeder Anwendung verwenden, die AWS-Services direkt aufruft und mit einem AWS SDK erstellt wurde, das eine der in der AWS Metrics-Dokumentation aufgeführten Versionen ist.

SDK Metrics überwacht Aufrufe, die vom AWS SDK getätigt werden, und verwendet den CloudWatch Agenten, der in derselben Umgebung wie eine Clientanwendung ausgeführt wird.

Der CloudWatch Agent verschlüsselt die Daten während der Übertragung vom lokalen Computer zur Bereitstellung in der Zielprotokollgruppe. Die Protokollgruppe kann so konfiguriert werden, dass sie gemäß den Anweisungen unter Verschlüsseln von Protokolldaten in CloudWatch Protokollen mit verschlüsselt wird AWS KMS.

AWS Secrets Manager

AWS Secrets Manager ist ein AWS-Service, der es Kunden erleichtert, „Geheimnisse“ zu verwalten. Secrets können Datenbankanmeldeinformationen, Passwörter, API-Schlüssel von Drittanbietern und sogar beliebiger Text sein. AWS Secrets Manager kann verwendet werden, um PHI zu speichern, wenn solche Informationen in „Geheimnissen“ enthalten sind. Alle von AWS Secrets Manager gespeicherten Secrets werden im Ruhezustand mit dem AWS Key Management System (KMS) verschlüsselt. Benutzer können den AWS KMS Schlüssel auswählen, der beim Erstellen eines neuen Secrets verwendet wird. Wenn kein Schlüssel ausgewählt ist, wird der Standardschlüssel für das Konto verwendet. AWS Secrets Manager verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Security Hub

AWS Security Hub sammelt und konsolidiert Ergebnisse von AWS-Sicherheitsservices, die in der Umgebung eines Kunden aktiviert sind, z. B. Erkenntnisse zur Angriffserkennung von Amazon GuardDuty, Schwachstellenscans von Amazon Inspector, Erkenntnisse von Amazon S3-Bucket-Richtlinien von Amazon Macie, öffentlich zugängliche und kontoübergreifende Ressourcen von IAM Access Analyzer und Ressourcen ohne WAF-Abdeckung von AWS Firewall Manager. konsolidiert AWS Security Hub auch Ergebnisse von integrierten AWS Partner Network (APN)-Sicherheitslösungen.

AWS Security Hub lässt sich in Amazon CloudWatch Events integrieren, sodass Kunden benutzerdefinierte Reaktions- und Korrekturworkflows erstellen können. Kunden können auf einfache Weise Ergebnisse an SIEMs, Chat-Tools, Ticketing-Systeme, Tools zur Automatisierung und Reaktion auf Sicherheitsorchestrierung (Security Orchestration Automation and Response, SOAR) und Plattformen für die Verwaltung auf Abruf senden. Maßnahmen zur Reaktion und Behebung können vollständig automatisiert oder manuell in der Konsole ausgelöst werden. Kunden können auch AWS Systems Manager Automation-Dokumente und - AWS Lambda Funktionen verwenden AWS Step Functions, um automatisierte Workflows zur Behebung zu erstellen, die von initiiert werden können AWS Security Hub.

Um den Datenschutz zu gewährleisten, AWS Security Hub verschlüsselt Daten im Ruhezustand und Daten während der Übertragung zwischen Komponentenservices. Externe Prüfer bewerten die Sicherheit und Compliance von AWS Security Hub im Rahmen mehrerer AWS-Compliance-Programme. AWS Security Hub ist Teil der SOC-, ISO-, PCI- und HIPAA-Compliance-Programme von AWS.

AWS Server Migration Service

AWS Server Migration Service (AWS SMS) automatisiert die Migration von virtuellen On-Premises-Maschinen von VMware vSphere oder Microsoft Hyper-V/SCVMM in die AWS Cloud. AWS SMS repliziert Server-VMs inkrementell als in der Cloud gehostete Amazon Machine Images (AMIs), die für die Bereitstellung auf Amazon EC2 bereit sind.

Server, die On-Premises ausgeführt werden und mit (AWS SMS) in die Cloud migriert werden, können PHI-Daten enthalten. AWS SMS verschlüsselt Daten während der Übertragung und wenn Server-VM-Images für die endgültige Platzierung in EC2 bereitgestellt werden. Lesen Sie die Anleitungen für EC2 und richten Sie verschlüsselte Speicher-Volumes ein, wenn Sie eine Server-VM mit PHI mit AWS SMS migrieren. AWS SMS verwendet CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Serverless Application Repository

Das AWS Serverless Application Repository (microSD) ist ein verwaltetes Repository für Serverless-Anwendungen. Es ermöglicht Teams, Organisationen und einzelnen Entwicklern, wiederverwendbare Anwendungen zu speichern und gemeinsam zu nutzen und Serverless-Architekturen einfach und auf leistungsstarke neue Weise zusammenzustellen und bereitzustellen. Die Anwendungen sind AWS CloudFormation Vorlagen, die Definitionen der Anwendungsinfrastruktur und kompilierte Binärdateien des AWS Lambda Anwendungsfunktionscodes enthalten.

Obwohl es möglich ist, dass Anwendungen, die sich im befinden AWS Serverless Application Repository , PHI verarbeiten, tun sie dies erst nach der Bereitstellung im Konto eines Kunden und nicht als Teil des SAR selbst. Die AWS Serverless Application Repository verschlüsselt Dateien, die Kunden hochladen, einschließlich Bereitstellungspaketen und Ebenenarchiven. Bei Daten während der Übertragung AWS Serverless Application Repository verwendet TLS, um Daten zwischen dem Service und dem Agenten zu verschlüsseln. AWS Serverless Application Repository ist in integriert. Dabei handelt es sich um einen Service AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service in der durchgeführten Aktionen bereitstellt AWS Serverless Application Repository.

Servicekatalog

Service Catalog ermöglicht es IT-Administratoren, Portfolios genehmigter Produkte zu erstellen, zu verwalten und an Endbenutzer zu verteilen, die dann in einem personalisierten Portal auf die benötigten Produkte zugreifen können. Service Catalog wird verwendet, um Self-Service-Lösungen in AWS zu katalogisieren, freizugeben und bereitzustellen, und kann nicht zum Speichern, Übertragen oder Verarbeiten von PHI verwendet werden. PHI sollten nicht in Metadaten für Service-Catalog-Elemente oder in einer Elementbeschreibung platziert werden. Service Catalog verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Shield

AWS Shield ist ein verwalteter Distributed Denial of Service (DDoS)-Schutzservice, der Webanwendungen schützt, die auf AWS ausgeführt werden. AWS Shield bietet eine immer aktive Erkennung und automatische Inline-Abschwächungen, die Ausfallzeiten und Latenz von Anwendungen minimieren, sodass Sie nicht AWS Support vom DDoS-Schutz profitieren müssen.

AWS Shield kann nicht zum Speichern oder Übertragen von PHI verwendet werden, sondern zum Schutz von Webanwendungen, die mit PHI arbeiten. Daher ist keine spezielle Konfiguration erforderlich, wenn Sie mit interagieren AWS Shield.

Alle AWS-Kunden profitieren vom automatischen Schutz von AWS Shield Standard ohne zusätzliche Kosten. AWS Shield Standard schützt gegen die häufigsten, häufig auftretenden DDoS-Angriffe auf Netzwerk- und Transportebene, die auf ihre Website oder Anwendungen abzielen. Für einen höheren Schutz vor Angriffen, die auf ihre Webanwendungen abzielen CloudFront, die auf Elastic Load Balancing (ELB), Amazon und Amazon Route 53-Ressourcen ausgeführt werden, können Kunden abonnieren AWS Shield Advanced.

AWS Snowball

Mit AWS Snowball (Snowball) können Kunden Hunderte von Terabyte oder Petabyte an Daten zwischen ihren On-Premises-Rechenzentren und Amazon Simple Storage Service (Amazon S3) übertragen. In AWS Snowball gespeicherte PHI müssen im Ruhezustand gemäß der -Anleitung verschlüsselt werden. Beim Erstellen eines Importauftrags müssen Kunden den ARN für den AWS KMS Schlüssel angeben, der zum Schutz von Daten innerhalb des Snowballs verwendet werden soll. Darüber hinaus sollten Kunden während der Erstellung des Importauftrags einen Ziel-S3-Bucket auswählen, der den in der -Anleitung festgelegten Verschlüsselungsstandards entspricht.

Während Snowball derzeit keine serverseitige Verschlüsselung mit von AWS KMS verwalteten Schlüsseln (SSE-KMS) oder serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C) unterstützt, unterstützt Snowball die serverseitige Verschlüsselung mit von Amazon S3-managed Verschlüsselungsschlüsseln (SSE-S3). Weitere Informationen finden Sie unter Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).

Alternativ können Kunden die Verschlüsselungsmethode ihrer Wahl verwenden, um PHI zu verschlüsseln, bevor die Daten in gespeichert werden AWS Snowball.

Derzeit können Kunden die Standard- AWS Snowball Appliance als Teil unserer BAA verwenden.

AWS Snowball Edge

AWS Snowball Edge stellt über Standardspeicherschnittstellen eine Verbindung zu vorhandenen Kundenanwendungen und Infrastrukturen her, optimiert den Datenübertragungsprozess und minimiert die Einrichtung und Integration. Snowball Edge kann zusammen eine lokale Speicherebene bilden und Kundendaten vor Ort verarbeiten, sodass Kunden sicherstellen können, dass ihre Anwendungen weiterhin ausgeführt werden, auch wenn sie nicht auf die Cloud zugreifen können.

Um sicherzustellen, dass PHI bei der Verwendung von Snowball Edge verschlüsselt bleiben, sollten Kunden sicherstellen, dass sie ein verschlüsseltes Verbindungsprotokoll wie HTTPS oder SSL/TLS verwenden, wenn sie Verfahren verwenden AWS Lambda , die von unterstützt werden AWS IoT Greengrass , um PHI an/von Ressourcen außerhalb von Snowball Edge zu übertragen. Darüber hinaus sollte PHI verschlüsselt werden, während es auf den lokalen Volumes von Snowball Edge gespeichert wird, entweder über lokalen Zugriff oder über NFS. Die Verschlüsselung wird automatisch auf Daten angewendet, die mithilfe der Snowball-Managementkonsole und der API für den Massentransport nach S3 in Snowball Edge platziert werden. Weitere Informationen zum

Datentransport in S3 finden Sie in den zugehörigen Anleitungen für the section called “AWS Snowball”.

AWS Step Functions

AWS Step Functions erleichtert die Koordination der Komponenten verteilter Anwendungen und Microservices mithilfe visueller Workflows. kann PHI AWS Step Functions nicht speichern, übertragen oder verarbeiten. PHI sollte nicht in den Metadaten für AWS Step Functions oder innerhalb einer Aufgaben- oder Zustandsautomatendefinition platziert werden. AWS Step Functions verwendet AWS CloudTrail , um alle API-Aufrufe zu protokollieren.

AWS Storage Gateway

AWS Storage Gateway ist ein Hybrid-Speicherservice, mit dem On-Premises-Anwendungen von Kunden AWS Cloud-Speicher nahtlos verwenden können. Das Gateway verwendet offene Standardspeicherprotokolle, um vorhandene Speicheranwendungen und Workflows mit AWS Cloud-Speicherservices zu verbinden, um Unterbrechungen des Prozesses zu minimieren.

Datei-Gateway

File Gateway ist eine Art von AWS Storage Gateway , die eine Dateischnittstelle in Amazon S3 unterstützt und das aktuelle blockbasierte Volume und den VTL-Speicher erweitert. Das File Gateway verwendet HTTPS für die Kommunikation mit S3 und speichert alle Objekte standardmäßig mit S3 SSE-S3 oder clientseitiger Verschlüsselung mit Schlüsseln, die in gespeichert sind AWS KMS. Dateimetadaten wie Dateinamen bleiben unverschlüsselt und sollten keine PHI enthalten.

Volume Gateway

Volume Gateway bietet Cloud-gestützte Speicher-Volumes, die Kunden als Internet Small Computer System Interface (iSCSI)-Geräte von On-Premises-Anwendungsservern aus mounten können. Kunden sollten lokale Datenträger als Upload-Puffer und Cache an die Volume-Gateway-VM anfügen, entsprechend ihren internen Compliance- und regulatorischen Anforderungen. Es wird empfohlen, dass diese Datenträger für PHI in der Lage sein sollten, eine Verschlüsselung im Ruhezustand bereitzustellen. Die Kommunikation zwischen der Volume Gateway-VM und AWS wird mit TLS 1.2 verschlüsselt, um PHI beim Transport zu sichern.

Tape Gateway

Tape Gateway bietet eine VTL-Schnittstelle (virtuelle Bandbibliothek) für Backup-Anwendungen von Drittanbietern, die On-Premises ausgeführt werden. Kunden sollten die Verschlüsselung für PHI innerhalb der Sicherungsanwendung eines Drittanbieters aktivieren, wenn sie einen Bandsicherungsauftrag einrichten. Die Kommunikation zwischen der Tape Gateway-VM und AWS wird mit TLS 1.2 verschlüsselt, um PHI beim Transport zu sichern. Kunden, die eine der Storage Gateway-Konfigurationen mit PHI verwenden, sollten die vollständige Protokollierung aktivieren. Weitere Informationen finden Sie unter Was ist AWS Storage Gateway?.

AWS Systems Manager

AWS Systems Manager ist eine einheitliche Schnittstelle, mit der Kunden Betriebsdaten einfach zentralisieren, Aufgaben über ihre AWS-Ressourcen hinweg automatisieren und die Zeit verkürzen können, um Betriebsprobleme in ihrer Infrastruktur zu erkennen und zu beheben. Systems Manager bietet einen vollständigen Überblick über die Infrastrukturleistung und -konfiguration eines Kunden, vereinfacht das Ressourcen- und Anwendungsmanagement und erleichtert den Betrieb und die Verwaltung seiner Infrastruktur in großem Umfang.

Bei der Ausgabe von Daten, die PHI enthalten können, an andere -Services wie Amazon S3 müssen Kunden die Anweisungen des empfangenden Services zum Speichern von PHI befolgen. Kunden sollten PHI nicht in Metadaten oder Kennungen wie Dokumentnamen und Parameternamen aufnehmen.

AWS Transfer for SFTP

AWS Transfer for SFTP bietet Secure File Transfer Protocol (SFTP)-Zugriff auf die S3-Ressourcen eines Kunden. Kunden wird ein virtueller Server bereitgestellt, auf den über das Standard- SFTP-Protokoll an einem regionalen Service-Endpunkt zugegriffen wird. Aus Sicht des AWS-Kunden und des SFTP-Clients sieht das SFTP-Gateway wie ein standardmäßiger, hochverfügbarer SFTP-Server aus. Obwohl der Service selbst PHI nicht speichert, verarbeitet oder überträgt, sollten die Ressourcen, auf die der Kunde auf Amazon S3 zugreift, so konfiguriert werden, dass sie mit der -Anleitung übereinstimmen. Kunden können auch verwenden AWS CloudTrail , um API-Aufrufe an AWS Transfer for SFTP zu protokollieren.

AWS WAF – Firewall für Webanwendungen

AWS WAF ist eine Firewall für Webanwendungen, die dazu beiträgt, Webanwendungen von Kunden vor gängigen Web-Exploits zu schützen, die sich auf die Anwendungsverfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen verbrauchen könnten. Kunden können AWS WAF zwischen ihren auf AWS gehosteten Webanwendungen, die mit PHI arbeiten oder diese austauschen, und ihren Endbenutzern platzieren. Wie bei der Übertragung von PHI auf AWS müssen Daten, die PHI enthalten, während der Übertragung verschlüsselt werden. Lesen Sie die Anleitungen für Amazon EC2, um die verfügbaren Verschlüsselungsoptionen besser zu verstehen.

AWS X-Ray

AWS X-Ray ist ein Service, der Daten über Anfragen sammelt, die die Anwendung eines Kunden bedient, und Tools bereitstellt, mit denen er diese Daten anzeigen, filtern und Einblicke in sie gewinnen kann, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Für jede verfolgte Anfrage an die Anwendung eines Kunden können detaillierte Informationen nicht nur über die Anfrage und Antwort angezeigt werden, sondern auch über Aufrufe, die seine Anwendung an nachgelagerte AWS-Ressourcen, Microservices, Datenbanken und HTTP-Web-APIs vornimmt. AWS X-Ray werden nicht zum Speichern oder Verarbeiten von PHI verwendet. Informationen, die an und von übertragen AWS X-Ray werden, werden standardmäßig verschlüsselt. Wenn Sie verwenden AWS X-Ray, platzieren Sie keine PHI in Segmentanmerkungen oder Segmentmetadaten.

Elastic Load Balancing

Kunden können Elastic Load Balancing verwenden, um Sitzungen zu beenden und zu verarbeiten, die PHI enthalten. Kunden können entweder den Classic Load Balancer oder den Application Load Balancer wählen. Da der gesamte Netzwerkverkehr, der PHI enthält, während der Übertragung verschlüsselt werden muss end-to-end, haben Kunden die Flexibilität, zwei verschiedene Architekturen zu implementieren:

Kunden können HTTPS, HTTP/2 über TLS (für Anwendung) oder SSL/TLS auf Elastic Load Balancing beenden, indem sie einen Load Balancer erstellen, der ein verschlüsseltes Protokoll für Verbindungen verwendet. Diese Funktion ermöglicht die Verschlüsselung des Datenverkehrs zwischen dem Load Balancer und den Clients, die HTTPS-, HTTP/2- oder SSL/TLS-Sitzungen initiieren, sowie für Verbindungen zwischen dem Load Balancer und Kunden-Backend-Instances. Sitzungen, die PHI enthalten, müssen sowohl Frontend- als auch Backend-Listener für die

Transportverschlüsselung verschlüsseln. Kunden sollten ihre Zertifikate und Richtlinien für Sitzungsaushandlungen bewerten und sie gemäß der -Anleitung konsistent halten. Weitere Informationen finden Sie unter HTTPS-Listener für Ihren Classic Load Balancer.

Alternativ können Kunden Amazon ELB im grundlegenden TCP-Modus (für Classic) oder über WebSockets (für Anwendung) und Pass-Through-verschlüsselte Sitzungen an Backend-Instances konfigurieren, bei denen die verschlüsselte Sitzung beendet wird. In dieser Architektur verwalten Kunden ihre eigenen Zertifikate und TLS-Aushandlungsrichtlinien in Anwendungen, die in ihren eigenen Instances ausgeführt werden. Weitere Informationen finden Sie unter Listener für Ihren Classic Load Balancer. In beiden Architekturen sollten Kunden eine Protokollierungsebene implementieren, die ihrer Meinung nach den HIPAA- und HI-Anforderungen entspricht.

FreeRTOS

FreeRTOS ist ein Betriebssystem für Mikrocontroller, mit dem kleine Edge-Geräte mit geringer Leistung einfach zu programmieren, bereitzustellen, zu sichern, zu verbinden und zu verwalten sind. FreeRTOS basiert auf dem FreeRTOS-Kernel, einem beliebten Open-Source-Betriebssystem für Mikrocontroller, und erweitert ihn um Softwarebibliotheken, die es einfach machen, kleine Geräte mit geringer Leistung sicher mit AWS Cloud-Services wie AWS IoT Core oder mit leistungsfähigeren Edge-Geräten zu verbinden, auf denen ausgeführt wird AWS IoT Greengrass.

Daten, die PHI enthalten, können jetzt während der Übertragung und im Ruhezustand verschlüsselt werden, wenn ein qualifiziertes Gerät verwendet wird, auf dem FreeRTOS ausgeführt wird. FreeRTOS bietet zwei Bibliotheken zur Gewährleistung der Plattformsicherheit: TLS und PKCS#11. Die TLS-API sollte verwendet werden, um den gesamten Netzwerkverkehr zu verschlüsseln und zu authentifizieren, der PHI enthält. PKCS#11 bietet eine Standardschnittstelle für kryptografische Softwareoperationen und sollte verwendet werden, um alle PHI zu verschlüsseln, die auf einem qualifizierten Gerät mit FreeRTOS gespeichert sind.

Verwenden von AWS KMS für die Verschlüsselung von PHI

KMS-Schlüssel können verwendet werden, um Datenverschlüsselungsschlüssel zu verschlüsseln/zu entschlüsseln, die zur Verschlüsselung von PHI in den Anwendungen eines Kunden oder in AWS-Services verwendet werden AWS KMS. AWS KMS kann in Verbindung mit einem HIPAA-Konto verwendet werden, aber PHI kann nur in HIPAA-fähigen Services verarbeitet, gespeichert oder übertragen werden. AWS KMS wird normalerweise verwendet, um Schlüssel für Anwendungen zu generieren und zu verwalten, die in anderen HIPAA-fähigen Services ausgeführt werden.

Beispielsweise könnte eine Anwendung, die PHI in Amazon EC2 verarbeitet, den GenerateDataKey API-Aufruf verwenden, um Datenverschlüsselungsschlüssel für die Ver- und Entschlüsselung von PHI in der Anwendung zu generieren. Die Datenverschlüsselungsschlüssel werden durch die KMS-Schlüssel eines Kunden geschützt, die in gespeichert sind, wodurch eine hoch überprüfbare Schlüsselhierarchie erstellt wird AWS KMS, wenn API-Aufrufe an in protokolliert AWS KMS werden AWS CloudTrail. PHI sollten für Schlüssel, die in gespeichert sind, nicht in den Tags (Metadaten) gespeichert werden AWS KMS.

VM Import/Export

VM Import/Export ermöglicht es Kunden, Images virtueller Maschinen einfach aus einer vorhandenen Umgebung in Amazon EC2-Instances zu importieren und sie wieder in Ihre On-Premises-Umgebung zu exportieren. Dieses Angebot ermöglicht es Kunden, bestehende Investitionen in die virtuellen Maschinen zu nutzen, die Sie zur Erfüllung theirIT-Sicherheit, ihres Konfigurationsmanagements und ihrer Compliance-Anforderungen erstellt haben, indem diese virtuellen Maschinen als Instances in Amazon EC2 übertragen ready-to-use werden. Kunden können importierte Instances auch zurück in ihre On-Premises-Virtualisierungsinfrastruktur exportieren, sodass sie Workloads in Ihrer gesamten IT-Infrastruktur bereitstellen können.

VM Import/Export ist ohne zusätzliche Kosten verfügbar, die über die Standardnutzungsgebühren für Amazon EC2 und Amazon S3 hinausgehen.

Um Kunden-Images zu importieren, können Kunden die AWS CLI oder andere Entwicklertools verwenden, um ein Image einer virtuellen Maschine (VM) aus ihrer VMware-Umgebung zu importieren. Wenn Kunden die VMware vSphere-Virtualisierungsplattform verwenden, können sie auch das AWS Management Portal für vCenter verwenden, um ihre VM zu importieren. Im Rahmen des Importvorgangs konvertiert VM Import die Kunden-VM in ein Amazon EC2-AMI, mit dem sie Amazon EC2 ausführen können. Sobald ihre VM importiert wurde, können sie die Elastizität, Skalierbarkeit und Überwachung von Amazon über Angebote wie Auto Scaling ,Elastic Load Balancing und nutzen, CloudWatch um ihre importierten Images zu unterstützen.

Kunden können zuvor importierte Amazon EC2-Instances mithilfe der Amazon EC2-API-Tools exportieren. Geben Sie einfach die Ziel-Instance, das Dateiformat der virtuellen Maschine und einen Amazon S3-Ziel-Bucket an, und VM Import/Export exportiert die Instance automatisch zusammen mit Verschlüsselungsoptionen in den Amazon S3-Bucket, um die Übertragung und Speicherung ihrer VM-Images zu sichern. Kunden können dann die exportierte VM innerhalb ihrer On-Premises-Virtualisierungsinfrastruktur herunterladen und starten.

Kunden können Windows- und Linux-VMs importieren, die die Virtualisierungsformate VMware ESX oder Workstation, Microsoft Hyper-V und Citrix Xen verwenden. Kunden können außerdem zuvor importierte Amazon EC2-Instances in die Formate VMware ESX, Microsoft Hyper-V oder Citrix Xen exportieren. Eine vollständige Liste der unterstützten Betriebssysteme, Versionen und Formate finden Sie unter VM Import/Export-Anforderungen. AWS plant, Unterstützung für zusätzliche Betriebssysteme, Versionen und Formate in Zukunft hinzuzufügen.

Prüfung, Backups und Notfallwiederherstellung

Die Sicherheitsregel von HIPAA enthält detaillierte Anforderungen im Zusammenhang mit detaillierten Prüfungsfunktionen, Datensicherungsverfahren und Notfallwiederherstellungsmechanismen. Die Services in AWS enthalten viele Funktionen, mit denen Kunden ihre Anforderungen erfüllen können. Kunden sollten beispielsweise erwägen, Prüfungsfunktionen einzurichten, damit Sicherheitsanalysten detaillierte Aktivitätsprotokolle oder Berichte untersuchen können, um festzustellen, wer Zugriff hatte, IP-Adresseintrag, auf welche Daten zugegriffen wurde usw.

Diese Daten sollten im Falle einer Prüfung für einen längeren Zeitraum an einem zentralen Ort verfolgt, protokolliert und gespeichert werden. Mit Amazon EC2 können Kunden Aktivitätsprotokolldateien und Audits auf der Paketebene auf ihren virtuellen Servern ausführen, genau wie auf herkömmlicher Hardware. Sie können auch jeden IP-Datenverkehr verfolgen, der ihre virtuelle Server-Instance erreicht. Die Administratoren eines Kunden können die Protokolldateien in Amazon S3 für eine langfristige zuverlässige Speicherung sichern.

HIPAA hat auch detaillierte Anforderungen im Zusammenhang mit der Pflege eines Notfallplans zum Schutz von Daten im Notfall und muss exakte Kopien von elektronischen PHI erstellen und abrufbar halten. Um einen Datensicherungsplan in AWS zu implementieren, bietet Amazon EBS persistenten Speicher für virtuelle Amazon EC2-Server-Instances. Diese Volumes können als Standard-Blockgeräte bereitgestellt werden und bieten Speicher außerhalb der Instance, der unabhängig von der Lebensdauer einer Instance bestehen bleibt. Um den HIPAA-Richtlinien zu entsprechen, können Kunden Snapshots von Amazon-EBS-Volumes erstellen point-in-time, die automatisch in Amazon S3 gespeichert und über mehrere Availability Zones repliziert werden. Dabei handelt es sich um eigene Standorte, die vor Ausfällen in anderen Availability Zones geschützt sind.

Auf diese Snapshots kann jederzeit zugegriffen werden und Daten können für eine langfristige Haltbarkeit geschützt werden. Amazon S3 bietet auch eine hochverfügbare Lösung für Datenspeicherung und automatisierte Backups. Durch das einfache Laden einer Datei oder eines Images in Amazon S3 werden mehrere redundante Kopien automatisch erstellt und in separaten Rechenzentren gespeichert. Auf diese Dateien kann jederzeit von überall (basierend auf Berechtigungen) zugegriffen werden und sie werden gespeichert, bis sie absichtlich gelöscht werden.

Darüber hinaus bietet AWS von Natur aus eine Vielzahl von Mechanismen zur Notfallwiederherstellung. Notfallwiederherstellung, der Prozess des Schutzes der Daten und IT-Infrastruktur einer Organisation in Notfallsituationen, umfasst die Wartung hochverfügbarer Systeme, die Beibehaltung sowohl der Daten als auch des Systems außerhalb des Standorts und die Ermöglichung des kontinuierlichen Zugriffs auf beide.

Mit Amazon EC2 können Administratoren Server-Instances sehr schnell starten und eine Elastic IP-Adresse (eine statische IP-Adresse für die Cloud-Computing-Umgebung) für ein ordnungsgemäßes Failover von einem Computer zum anderen verwenden. Amazon EC2 bietet auch Availability Zones an. Administratoren können Amazon EC2-Instances in mehreren Availability Zones starten, um geografisch unterschiedliche, fehlertolerante Systeme zu erstellen, die bei Netzwerkausfällen, Naturkatastrophen und anderen wahrscheinlichen Ausfallzeiten äußerst ausfallsicher sind.

Mit Amazon S3 werden die Daten eines Kunden repliziert und automatisch in separaten Rechenzentren gespeichert, um eine zuverlässige Datenspeicherung zu bieten, die eine Verfügbarkeit von 99,99 % bietet.

Mit AWS Elastic Disaster Recovery (AWS DRS) können Kunden Anwendungen in AWS schnell wiederherstellen, entweder im höchsten up-to-date Zustand der Anwendungen oder ab einem früheren Zeitpunkt.

Dokumentversionen

Um über Aktualisierungen dieses Whitepapers benachrichtigt zu werden, abonnieren Sie den RSS-Feed.

Änderung	Beschreibung	Datum
Kleines Update	Kleines Update	12. Mai 2023
Kleines Update	Das -Whitepaper wurde aktualisiert, um den verfügbaren Inhalt zu -Services zu erweitern.	28. September 2022
Kleines Update	Korrigiert Nicht-inklusive-Sprache.	6. April 2022
Whitepaper aktualisiert	Informationen zum AWS Application Migration Service hinzugefügt und Informationen für Amazon ECS aktualisiert	6. Dezember 2021
Whitepaper aktualisiert	Aktualisierte Informationen in den Abschnitten Amazon Healthlake und Amazon VPC	9. November 2021
Whitepaper aktualisiert	Informationen zu AWS Network Firewall hinzugefügt	9. September 2021
Whitepaper aktualisiert	Aktualisierte Informationen zu Amazon Connect Customer Profiles	26. August 2021
Whitepaper aktualisiert	Hinzufügung der Abschnitte Amazon AppFlow und AWS Glue DataBrew	22. Juli 2021

Whitepaper aktualisiert	Die Navigation und Organisation wurden aktualisiert.	26. April 2021
Whitepaper aktualisiert	Die folgenden Abschnitte wurden hinzugefügt: AWS CodeDeploy, AWS CodePipeline,Amazon Aurora,Aurora PostgreSQL,Amazon Textract,Amazon Polly,Amazon FSx,AWS Auto Scaling, AWS Backup, AWS Elastic Beanstalk, AWS Firewall Manager, AWS Organizations AWS Security Hub,, AWS Serverless Application Repository VM Import/Export,Amazon HealthLake,Amazon EventBridge. Der Abschnitt Amazon Aurora wurde aktualisiert.	31. März 2021
Whitepaper aktualisiert	Abschnitt zu AWS App Mesh hinzugefügt und AWS System Manager-Inhalt aktualisiert	25. August 2020
Whitepaper aktualisiert	Hinzufügung der Abschnitte Amazon Appstream 2.0, AWS SDK Metrics, AWS Data Exchange, Amazon MSK, Amazon Pinpoint , Amazon Lex , Amazon SES und Amazon Forecast, Amazon Quantum Ledger Database (QLDB). AWS Cloud Map	7. Mai 2020

Whitepaper aktualisiert	Abschnitte zu Amazon CloudWatch, Amazon CloudWatch Events, Amazon Data Firehose, Amazon Managed Service für Apache Flink, Amazon OpenSearch Service, Amazon DocumentDB (mit MongoDB-Kompatibilität), AWS Mobile Hub , AWS IoT Greengrass, AWS OpsWorks für Chef Automate, AWS OpsWorks für Puppet Enterprise, AWS Transfer for SFTP, AWS DataSync, AWS Global Accelerator Amazon Comprehend Medical und AWS hinzugefügt RoboMaker.	1. Januar 2020
Whitepaper aktualisiert	Abschnitte zu Amazon Comprehend , Amazon Transcribe , Amazon Translate und AWS Certificate Manager hinzugefügt.	1. Januar 2019
Whitepaper aktualisiert	Abschnitte zu Amazon Athena , Amazon EKS, AWS IoT Core und AWS IoT Device Management, Amazon FreeRTOS , Amazon GuardDuty, Amazon Neptune , AWS Server Migration Service, AWS Database Migration Service Amazon MQ und hinzugefügt AWS Glue.	1. November 2018

Whitepaper aktualisiert	Hinzufügung von Abschnitten zu Amazon Elastic File System (EFS),Amazon Kinesis Video Streams ,Amazon Rekogniti on, Amazon SageMaker, Amazon Simple Workflow, AWS Secrets Manage, Service Catalog und AWS Step Functions.	1. Juni 2018
Whitepaper aktualisiert	Abschnitte zu AWS CloudFormation, AWS X-Ray AWS CloudTrail AWS CodeBuild AWS CodeCommi t, AWS Config und AWS OpsWorks Stack hinzugefügt.	1. April 2018
Whitepaper aktualisiert	Abschnitt zu hinzugefügt AWS Fargate.	1. Januar 2018

Aktualisierungen, die vor 2018 vorgenommen wurden:

Datum	Beschreibung
November 2017	Abschnitte zu Amazon EC2 Container Registry , Amazon Macie , Amazon QuickSigh tund hinzugefügt AWS Managed Services.
November 2017	Abschnitte zu Amazon ElastiCache für Redis und Amazon hinzugefügt CloudWatch.
. Oktober 2017	Abschnitte zu Amazon SNS , Amazon Route 53 AWS Storage Gateway und hinzugefügt AWS CloudHSM. Aktualisierter Abschnitt auf AWS Key Management Service.

Datum	Beschreibung
September 2017	Hinzufügung von Abschnitten zu Amazon Connect ,Amazon Kinesis Streams, Amazon RDS (Maria) DB, Amazon RDS SQL Server, AWS Batch, AWS Lambda, AWS Snowball Edge und der Lambda@Edge-Funktion von Amazon CloudFront.
August 2017	Abschnitte zu Amazon EC2 Systems Manager und Amazon Inspector hinzugefügt.
. Juli 2017	Abschnitte zu Amazon WorkSpaces, Amazon WorkDocs, AWS Directory Service und Amazon ECS hinzugefügt.
Juni 2017	Abschnitte zu Amazon CloudFront, AWS WAF AWS Shield und Amazon S3 Transfer Acceleration hinzugefügt.
. Mai 2017	Die Anforderung für Dedicated Instances oder Dedicated Hosts zur Verarbeitung von PHI in EC2 und EMR wurde entfernt.
März 2017	Die Liste der Services wurde aktualisiert, um auf die Seite „Betroffene AWS-Services nach Compliance-Programm“ zu verweisen . Beschreibung für Amazon API Gateway hinzugefügt.
Januar 2017	Aktualisiert auf die neueste Vorlage.
. Oktober 2016	Erstveröffentlichung

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS-Produktangebote und -praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) erstellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden unverändert ohne Garantien, Darstellungen oder Bedingungen beliebiger Art bereitgestellt, weder ausdrücklich noch implizit. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, nicht zu den Vereinbarung von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.