AWS Whitepaper

Merancang untuk Keamanan dan Kepatuhan HIPAA pada Amazon Web Services

Merancang untuk Keamanan dan Kepatuhan HIPAA pada Amazon Web Services: AWS Whitepaper

Table of Contents

Merancang untuk Keamanan dan Kepatuhan HIPAA pada Amazon Web Services

Tanggal publikasi: 28 September 2022 (Revisi dokumen)

Paper ini secara singkat menguraikan bagaimana pelanggan dapat menggunakan Amazon Web Services (AWS) untuk menjalankan beban kerja sensitif yang diatur berdasarkan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan AS (HIPAA). Kami akan fokus pada Aturan Privasi dan Keamanan HIPAA untuk melindungi Informasi Kesehatan yang Dilindungi (PHI), cara menggunakan AWS untuk mengenkripsi data saat transit dan saat istirahat, dan bagaimana fitur AWS dapat digunakan untuk menjalankan beban kerja yang mengandung PHI.

Pengantar

Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan tahun 1996 (HIPAA) berlaku untuk “entitas yang dilindungi” dan “rekan bisnis.” HIPAA diperluas pada tahun 2009 oleh Health Information Technology for Economic and Clinical Health (HITECH) Act.

HIPAA dan HITECH menetapkan seperangkat standar federal yang dimaksudkan untuk melindungi keamanan dan privasi PHI. HIPAA dan HITECH memberlakukan persyaratan terkait penggunaan dan pengungkapan informasi kesehatan yang dilindungi (PHI), perlindungan yang tepat untuk melindungi PHI, hak individu, dan tanggung jawab administratif. Untuk informasi lebih lanjut tentang HIPAA dan HITECH, kunjungi Rumah Privasi Informasi Kesehatan.

Entitas yang tercakup dan rekan bisnisnya dapat menggunakan komponen TI yang aman, dapat diskalakan, dan berbiaya rendah yang disediakan oleh Amazon Web Services (AWS) untuk merancang aplikasi yang selaras dengan persyaratan kepatuhan HIPAA dan HITECH. AWS menawarkan platform commercial-off-the-shelf infrastruktur dengan sertifikasi dan audit yang diakui industri seperti ISO 27001, FedRAMP, dan Laporan Kontrol Organisasi Layanan (SOC1, SOC2, dan SOC3). Layanan dan pusat data AWS memiliki beberapa lapisan keamanan operasional dan fisik untuk membantu memastikan integritas dan keamanan data pelanggan. Tanpa biaya minimum, tidak diperlukan kontrak berbasis jangka waktu, dan pay-as-you-use harga, AWS adalah solusi yang andal dan efektif untuk mengembangkan aplikasi industri perawatan kesehatan.

AWS memungkinkan entitas yang dilindungi dan rekan bisnisnya yang tunduk pada HIPAA untuk memproses, menyimpan, dan mengirimkan PHI dengan aman. Selain itu, pada Juli 2013, AWS menawarkan Business Associate Addendum (BAA) standar untuk pelanggan tersebut. Pelanggan yang menjalankan AWS BAA dapat menggunakan layanan AWS apa pun di akun yang ditetapkan sebagai Akun HIPAA, tetapi mereka hanya dapat memproses, menyimpan, dan mengirimkan PHI menggunakan layanan yang memenuhi syarat HIPAA yang ditentukan dalam AWS BAA. Untuk daftar lengkap layanan ini, lihat halaman Referensi Layanan yang Memenuhi Syarat HIPAA.

AWS mempertahankan program manajemen risiko berbasis standar untuk memastikan bahwa layanan yang memenuhi syarat HIPAA secara khusus mendukung perlindungan administratif, teknis, dan fisik HIPAA. Menggunakan layanan ini untuk menyimpan, memproses, dan mengirimkan PHI membantu pelanggan dan AWS kami untuk memenuhi persyaratan HIPAA yang berlaku untuk model operasi berbasis utilitas AWS.

BAA AWS mewajibkan pelanggan untuk mengenkripsi PHI yang disimpan atau ditransmisikan menggunakan layanan yang memenuhi syarat HIPAA sesuai dengan panduan dari Sekretaris

Kesehatan dan Layanan Kemanusiaan (HHS): Panduan untuk Membuat Informasi Kesehatan yang Dilindungi Tanpa Aman Tidak Dapat Digunakan, Tidak Dapat Dibaca, atau Tidak Dapat Diuraikan kepada Individu yang Tidak Sah ("Panduan"). Silakan merujuk ke situs ini karena dapat diperbarui, dan mungkin tersedia di situs penerus (atau terkait) yang ditunjuk oleh HHS.

AWS menawarkan serangkaian fitur dan layanan yang komprehensif untuk membuat manajemen kunci dan enkripsi PHI mudah dikelola dan lebih mudah untuk diaudit, termasuk AWS Key Management Service (AWS KMS). Pelanggan dengan persyaratan kepatuhan HIPAA memiliki banyak fleksibilitas dalam cara mereka memenuhi persyaratan enkripsi untuk PHI.

Saat menentukan cara menerapkan enkripsi, pelanggan dapat mengevaluasi dan memanfaatkan fitur enkripsi asli layanan yang memenuhi syarat HIPAA. Atau pelanggan dapat memenuhi persyaratan enkripsi melalui cara lain yang konsisten dengan panduan dari HHS.

Enkripsi dan perlindungan PHI di AWS

Aturan Keamanan HIPAA mencakup spesifikasi implementasi yang dapat dialamatkan untuk enkripsi PHI dalam transmisi (“dalam perjalanan”) dan dalam penyimpanan (“saat istirahat”). Meskipun ini adalah spesifikasi implementasi yang dapat dialamatkan di HIPAA, AWS mewajibkan pelanggan untuk mengenkripsi PHI yang disimpan atau ditransmisikan menggunakan layanan yang memenuhi syarat HIPAA sesuai dengan panduan dari Sekretaris Kesehatan dan Layanan Kemanusiaan (HHS): Panduan untuk Membuat Informasi Kesehatan yang Dilindungi Tanpa Aman Tidak Dapat Digunakan, Tidak Dapat Dibaca, atau Tidak Dapat Diuraikan oleh Individu yang Tidak Sah (“Panduan”). Silakan merujuk ke situs ini karena dapat diperbarui, dan mungkin tersedia di penerus (atau situs terkait) yang ditunjuk oleh HHS.

AWS menawarkan serangkaian fitur dan layanan yang komprehensif untuk membuat manajemen kunci dan enkripsi PHI mudah dikelola dan lebih mudah untuk diaudit, termasuk AWS Key Management Service (AWS KMS). Pelanggan dengan persyaratan kepatuhan HIPAA memiliki banyak fleksibilitas dalam cara mereka memenuhi persyaratan enkripsi untuk PHI.

Saat menentukan cara menerapkan enkripsi, pelanggan dapat mengevaluasi dan memanfaatkan fitur enkripsi asli layanan yang memenuhi syarat HIPAA, atau mereka dapat memenuhi persyaratan enkripsi melalui cara lain yang konsisten dengan panduan dari HHS. Bagian berikut memberikan detail tingkat tinggi tentang penggunaan fitur enkripsi yang tersedia di setiap layanan yang memenuhi syarat HIPAA dan pola lain untuk mengenkripsi PHI, dan bagaimana AWS KMS dapat digunakan untuk mengenkripsi kunci yang digunakan untuk enkripsi PHI di AWS.

Topik

- Amazon API Gateway
- Amazon AppFlow
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Aurora
- Amazon Aurora PostgreSQL
- Amazon CloudFront
- Amazon CloudWatch
- CloudWatch Acara Amazon

- CloudWatch Log Amazon
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon DocumentDB (dengan kompatibilitas MongoDB)
- 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 untuk Redis
- OpenSearch Layanan Amazon
- Amazon EMR
- Amazon EventBridge
- Amazon Forecast
- Amazon FSx
- Amazon GuardDuty
- Amazon HealthLake
- Amazon Inspector
- Layanan Terkelola Amazon untuk 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 Network Firewall
- Amazon Pinpoint
- Amazon Polly
- Amazon Quantum Ledger Database (Amazon QLDB)
- Amazon QuickSight
- Amazon RDS for MariaDB
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for 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)
- Layanan Alur Kerja Sederhana Amazon
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud
- Amazon WorkDocs
- Amazon WorkSpaces
- AWS App Mesh
- AWS Layanan Migrasi Aplikasi

- 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 Inti dan AWS IoT Device Management
- AWS IoT Greengrass
- AWS Lambda
- AWS Managed Services
- AWS OpsWorks untuk Chef Automate

- AWS OpsWorks untuk Puppet Enterprise
- AWS OpsWorks Tumpukan
- AWS Organizations
- AWS RoboMaker
- Metrik AWS SDK
- AWS Secrets Manager
- AWS Security Hub
- Layanan Migrasi Server AWS
- AWS Serverless Application Repository
- Service Catalog
- AWS Shield
- AWS Snowball
- AWS Snowball Tepi
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer for SFTP
- AWS WAF — Firewall Aplikasi Web
- AWS X-Ray
- Penyeimbang Beban Elastis
- FreeRTOS
- Menggunakan AWS KMS untuk Enkripsi PHI
- VM Import/Export

Amazon API Gateway

Pelanggan dapat menggunakan Amazon API Gateway untuk memproses dan mengirimkan informasi kesehatan yang dilindungi (PHI). Meskipun Amazon API Gateway secara otomatis menggunakan titik akhir HTTPS untuk enkripsi dalam penerbangan, pelanggan juga dapat memilih untuk mengenkripsi muatan sisi klien. API Gateway meneruskan semua data yang tidak di-cache melalui memori dan

tidak menuliskannya ke disk. Pelanggan dapat menggunakan AWS Signature Version 4 untuk otorisasi dengan API Gateway. Untuk informasi selengkapnya, lihat hal berikut:

- FAQ Amazon API Gateway: Keamanan dan Otorisasi
- Mengontrol dan mengelola akses ke REST API di API Gateway

Pelanggan dapat berintegrasi dengan layanan apa pun yang terhubung ke API Gateway, asalkan ketika PHI terlibat, layanan dikonfigurasi konsisten dengan Guidance dan BAA. Untuk informasi tentang mengintegrasikan API Gateway dengan layanan backend, lihat Menyiapkan metode REST API di API Gateway.

Pelanggan dapat menggunakan AWS CloudTrail dan Amazon CloudWatch untuk mengaktifkan logging yang konsisten dengan persyaratan logging mereka. Pastikan bahwa setiap PHI yang dikirim melalui API Gateway (seperti di header, URL, dan permintaan/respons) hanya ditangkap oleh layanan yang memenuhi syarat HIPAA yang telah dikonfigurasi agar konsisten dengan Panduan. Untuk informasi selengkapnya tentang logging dengan API Gateway, lihat Bagaimana cara mengaktifkan CloudWatch Log untuk memecahkan masalah API atau WebSocket API REST API Gateway API saya?

Amazon AppFlow

Amazon AppFlow adalah layanan integrasi yang dikelola sepenuhnya yang memungkinkan pelanggan mentransfer data dengan aman antara aplikasi oftware-as-a S-Service (SaaS) seperti Salesforce, Marketo, Slack, dan, dan layanan ServiceNow AWS seperti Amazon S3 dan Amazon Redshift. AppFlow dapat menjalankan aliran data pada frekuensi yang dipilih pelanggan - sesuai jadwal, dalam menanggapi acara bisnis, atau sesuai permintaan. Pelanggan juga dapat mengonfigurasi kemampuan transformasi data seperti pemfilteran dan validasi untuk menghasilkan ready-to-use data yang kaya sebagai bagian dari aliran itu sendiri, tanpa langkah tambahan.

Amazon AppFlow dapat digunakan untuk memproses dan mentransfer data yang mengandung PHI. Enkripsi data saat transit antara AppFlow dan sumber/tujuan yang dikonfigurasi disediakan secara default menggunakan TLS 1.2 atau yang lebih baru. Data yang disimpan saat istirahat di S3 secara otomatis dienkripsi menggunakan AWS KMS kunci (sebelumnya CMK) yang ditentukan oleh pelanggan. Untuk data PHI yang ditransfer ke tujuan non S3, pelanggan harus memastikan penyimpanan saat istirahat untuk tujuan yang dipilih memenuhi kebutuhan keamanan mereka. AppFlow memungkinkan pemantauan aplikasi dengan mengintegrasikan dengan AWS CloudTrail log panggilan API dan Amazon EventBridge untuk memancarkan peristiwa eksekusi aliran.

Amazon AppStream 2.0

Amazon AppStream 2.0 adalah layanan streaming aplikasi yang dikelola sepenuhnya. Pelanggan memiliki data mereka dan harus mengkonfigurasi aplikasi Windows yang diperlukan dengan cara yang memenuhi persyaratan peraturan mereka. Pelanggan dapat mengonfigurasi penyimpanan persisten melalui Folder Rumah. File dan folder dienkripsi saat transit menggunakan titik akhir SSL Amazon S3. File dan folder dienkripsi saat istirahat menggunakan kunci enkripsi yang dikelola Amazon S3. Untuk informasi selengkapnya, lihat Mengaktifkan dan Mengelola Penyimpanan Persisten untuk Pengguna AppStream 2.0 Anda Jika pelanggan memilih untuk menggunakan solusi penyimpanan pihak ketiga, mereka bertanggung jawab untuk memastikan konfigurasi solusi tersebut konsisten dengan panduan. Semua komunikasi API publik dengan Amazon AppStream 2.0 dienkripsi menggunakan TLS. Untuk informasi lebih lanjut, silakan lihat Dokumentasi Amazon AppStream 2.0.

Amazon AppStream 2.0 terintegrasi dengan AWS CloudTrail, layanan yang mencatat panggilan API yang dilakukan oleh atau atas nama Amazon AppStream 2.0 di akun AWS pelanggan dan mengirimkan file log ke bucket Amazon S3 yang ditentukan. CloudTrail menangkap panggilan API yang dilakukan dari konsol Amazon AppStream 2.0 atau dari Amazon AppStream 2.0 API. Pelanggan juga dapat menggunakan Amazon CloudWatch untuk mencatat metrik penggunaan sumber daya. Untuk informasi selengkapnya, lihat Memantau Sumber Daya Amazon AppStream 2.0 dan Mencatat Panggilan API AppStream 2.0 dengan AWS CloudTrail.

Amazon Athena

Amazon Athena adalah layanan kueri interaktif yang memudahkan untuk menganalisis data di Amazon Simple Storage Service (Amazon S3) menggunakan SQL standar. Athena membantu pelanggan menganalisis data tidak terstruktur, semi-terstruktur, dan terstruktur yang disimpan di Amazon S3. Contohnya termasuk format data CSV, JSON, atau kolumnar seperti Apache Parquet dan Apache ORC. Pelanggan dapat menggunakan Athena untuk menjalankan kueri ad hoc menggunakan ANSI SQL, tanpa perlu mengumpulkan atau memuat data ke Athena.

Amazon Athena sekarang dapat digunakan untuk memproses data yang mengandung PHI. Enkripsi data saat transit antara Amazon Athena dan S3 disediakan secara default menggunakan SSL/TLS. Enkripsi PHI saat beristirahat di S3 harus dilakukan sesuai dengan panduan yang disediakan di bagian S3. Enkripsi hasil kueri dari dan dalam Amazon Athena, termasuk hasil bertahap, harus diaktifkan menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3), kunci yang dikelola (SSE-KMS) atau enkripsi sisi klien dengan kunci yang dikelola (CSE-KMS) AWS KMS. AWS KMS Amazon Athena menggunakan AWS CloudTrail untuk mencatat semua panggilan API.

Amazon Aurora

Amazon Aurora memungkinkan pelanggan untuk mengenkripsi cluster database Aurora dan snapshot saat istirahat menggunakan kunci yang mereka kelola. AWS KMS Pada instance database yang berjalan dengan enkripsi Amazon Aurora, data yang disimpan saat istirahat di penyimpanan dasar dienkripsi, seperti pencadangan otomatis, replika baca, dan snapshot.

Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon Aurora memenuhi persyaratan kepatuhan dan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon Aurora, lihat Melindungi data menggunakan enkripsi.

Koneksi ke cluster DB yang menjalankan Aurora MySQL harus menggunakan enkripsi transport, menggunakan Secure Socket Layer (SSL) atau Transport Layer Security (TLS). Untuk informasi selengkapnya tentang penerapan SSL/TLS, lihat Menggunakan SSL/TLS dengan cluster DB MySQL Aurora.

Amazon Aurora PostgreSQL

Amazon Aurora memungkinkan pelanggan untuk mengenkripsi cluster database Aurora dan snapshot saat istirahat menggunakan kunci yang mereka kelola. AWS KMS Pada instance database yang berjalan dengan enkripsi Amazon Aurora, data yang disimpan saat istirahat di penyimpanan dasar dienkripsi, seperti pencadangan otomatis, replika baca, dan snapshot.

Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon Aurora memenuhi persyaratan kepatuhan dan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon Aurora, lihat Melindungi data menggunakan enkripsi.

Koneksi ke cluster DB yang menjalankan Aurora PostgreSQL harus menggunakan enkripsi transport, menggunakan Secure Socket Layer (SSL) atau Transport Layer Security (TLS). Untuk informasi selengkapnya tentang penerapan SSL/TLS, lihat Mengamankan data Aurora PostgreSQL dengan SSL.

Amazon CloudFront

Amazon CloudFront adalah layanan jaringan pengiriman konten global (CDN) yang mempercepat pengiriman situs web pelanggan, API, konten video, atau aset web lainnya. Ini terintegrasi dengan

produk Amazon Web Services lainnya untuk memberi pengembang dan bisnis cara mudah untuk mempercepat konten ke pengguna akhir tanpa komitmen penggunaan minimum. Untuk memastikan enkripsi PHI saat transit CloudFront, pelanggan harus mengonfigurasi CloudFront untuk menggunakan HTTPS end-to-end dari asal ke penampil.

Ini termasuk lalu lintas antara CloudFront dan penampil, CloudFront mendistribusikan ulang dari asal kustom, dan CloudFront mendistribusikan dari asal Amazon S3. Pelanggan juga harus memastikan bahwa data dienkripsi di tempat asal untuk memastikannya tetap terenkripsi saat istirahat saat di-cache. CloudFront Jika menggunakan Amazon S3 sebagai asal, pelanggan dapat menggunakan fitur enkripsi sisi server S3. Jika pelanggan mendistribusikan dari asal kustom, mereka harus memastikan bahwa data dienkripsi di asal.

Lambda@Edge

Lambda @Edge adalah layanan komputasi yang memungkinkan eksekusi fungsi Lambda di lokasi edge AWS. Lambda @Edge dapat digunakan untuk menyesuaikan konten yang dikirimkan. CloudFront Saat menggunakan Lambda @Edge dengan PHI, pelanggan harus mengikuti Panduan untuk penggunaan. CloudFront Semua koneksi masuk dan keluar dari Lambda @Edge harus dienkripsi menggunakan HTTPS atau SSL/TLS.

Amazon CloudWatch

Amazon CloudWatch adalah layanan pemantauan untuk sumber daya AWS Cloud dan aplikasi yang dijalankan pelanggan di AWS. Pelanggan dapat menggunakan Amazon CloudWatch untuk mengumpulkan dan melacak metrik, mengumpulkan dan memantau file log, dan mengatur alarm. Amazon CloudWatch sendiri tidak memproduksi, menyimpan, atau mengirimkan PHI. Pelanggan dapat memantau panggilan CloudWatch API dengan AWS CloudTrail. Untuk informasi selengkapnya, lihat Mencatat Panggilan CloudWatch API Amazon dengan AWS CloudTrail.

Untuk detail selengkapnya tentang persyaratan konfigurasi, lihat bagian CloudWatch Log Amazon.

CloudWatch Acara Amazon

Amazon CloudWatch Events menghadirkan near-real-time aliran peristiwa sistem yang menjelaskan perubahan dalam sumber daya AWS. Pelanggan harus memastikan bahwa PHI tidak mengalir ke CloudWatch Acara, dan sumber daya AWS apa pun yang memancarkan CloudWatch peristiwa yang menyimpan, memproses, atau mentransmisikan PHI dikonfigurasi sesuai dengan Panduan.

Pelanggan dapat mengonfigurasi CloudWatch Acara Amazon untuk mendaftar sebagai panggilan AWS API CloudTrail. Untuk informasi selengkapnya, lihat Membuat Aturan CloudWatch Peristiwa yang Memicu Penggunaan AWS CloudTrail Panggilan AWS API.

CloudWatch Log Amazon

Pelanggan dapat menggunakan Amazon CloudWatch Logs untuk memantau, menyimpan, dan mengakses file log mereka dari instans Amazon Elastic Compute Cloud (Amazon EC2), Amazon Route 53 AWS CloudTrail, dan sumber lainnya. Mereka kemudian dapat mengambil data log terkait dari CloudWatch Log. Data log dienkripsi saat dalam perjalanan dan saat sedang istirahat. Akibatnya, tidak perlu mengenkripsi ulang PHI yang dipancarkan oleh layanan lain dan dikirim ke Log. CloudWatch

Amazon Comprehend

Amazon Comprehend menggunakan pemrosesan bahasa alami untuk mengekstrak wawasan tentang konten dokumen. Amazon Comprehend memproses file teks apa pun dalam format UTF-8. Hal ini mengembangkan wawasan dengan mengakui entitas, frase kunci, bahasa, sentimen, dan elemen umum lainnya dalam dokumen. Amazon Comprehend dapat digunakan dengan data yang mengandung PHI. Amazon Comprehend tidak menyimpan atau menyimpan data apa pun dan semua panggilan ke API dienkripsi dengan SSL/TLS. Amazon CloudTrail Comprehend menggunakan untuk mencatat semua panggilan API.

AWS Identity and Access Management

Fungsi akses keamanan seperti otentikasi dan otorisasi diperlukan untuk mengakses Amazon Comprehend dan dapat dikontrol dengan AWS Identity and Access Management(IAM), dan kredensyal dapat digunakan untuk mengakses IAM. Untuk informasi selengkapnya, lihat Otentikasi dan Kontrol Akses untuk Amazon Comprehend di Panduan Pengguna Amazon Comprehend.

Pengelolaan akun

Secara default, pengguna IAM tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon Comprehend, atau melakukan tugas menggunakan Amazon Comprehend API. Untuk memungkinkan pengguna membuat atau memodifikasi sumber daya dan melakukan tugas, pelanggan bertanggung jawab untuk memanfaatkan kebijakan IAM yang memberikan izin kepada pengguna untuk sumber daya tertentu (seperti Amazon Comprehend dan tindakan API) yang perlu

digunakan pengguna, lalu melampirkan kebijakan ke pengguna atau grup yang memerlukan izin tertentu.

Dengan Amazon Comprehend, Anda AWS Identity and Access Management dapat menggunakan (IAM) untuk membuat pengguna dengan kebijakan terlampir untuk mengaktifkan izin Amazon Comprehend. Secara opsional, Anda dapat memilih untuk membuat kebijakan khusus untuk dilampirkan ke peran. Kemudian, Anda dapat menambahkan administrator ke peran dengan kemampuan untuk memanggil API untuk administrasi Amazon Comprehend sesuai dengan akses berbasis peran yang ditentukan organisasi dan prinsip hak istimewa yang paling tidak.

Identitas dan akses

Dengan Amazon Comprehend Anda dapat meminta pengguna untuk mengautentikasi menggunakan AWS otentikasi multi-faktor sesuai dengan persyaratan organisasi mereka untuk otentikasi.

Dengan menggunakan AWS Management Console, administrator IAM dapat membuat kebijakan yang dikelola pelanggan yang menolak semua izin kecuali yang diperlukan bagi pengguna untuk mengelola kredensyal dan perangkat MFA mereka sendiri. Template kebijakan JSON tersedia di halaman My Security Credential di konsol IAM.

Secara opsional, Anda dapat memanfaatkan kemampuan MFA pihak ketiga yang kompatibel dengan mitra IAM. Untuk informasi tambahan, lihat Mitra IAM.

Administrasi

Kami menyarankan Anda Amazon Comprehend memilih kebijakan berbasis identitas di mana administrator akun dapat melampirkan kebijakan izin ke identitas IAM (pengguna, grup, dan peran) dan dengan demikian memberikan izin untuk melakukan operasi di sumber daya Amazon Comprehend.

Daftar tindakan API untuk Amazon Comprehend dapat ditemukan di panduan Referensi API. Anda juga harus mempertimbangkan otorisasi akses ke kebijakan IAM yang telah ditentukan sebelumnya, kebijakan IAM pelanggan, dan tindakan API kepada pengguna atau peran sesuai dengan hak istimewa dan persyaratan organisasi berbasis peran mereka yang paling rendah. Untuk informasi selengkapnya, lihat Menggunakan Amazon Comprehend API di Panduan Pengembang.

Otentikasi eksternal

Amazon Comprehend kompatibel dengan federasi identitas menggunakan peran IAM. Hal ini memungkinkan Amazon Comprehend pengguna Anda untuk AWS mengautentikasi dengan

mengasumsikan peran yang telah disediakan administrator. Pengguna yang mengakses AWS menggunakan kredensyal dari organisasi mereka atau pihak ketiga mengambil peran secara tidak langsung.

AWS dukungan untuk Kerberos dan Active Directory memberikan manfaat sistem masuk tunggal dan otentikasi terpusat dari pengguna database. AWS pengguna dapat memilih untuk mengelola dan menyimpan kredensyal pengguna baik untuk AWS Directory Service Microsoft Active Directory atau di Active Directory pelanggan lokal.

Penegakan aliran data

AWS pelanggan dan mitra APN, yang bertindak baik sebagai pengontrol data atau pengolah data, bertanggung jawab atas data pribadi apa pun yang mereka masukkan ke dalam AWS Cloud dan Amazon Comprehend. Anda bertanggung jawab untuk mengontrol aliran ke input dan output data untuk Amazon Comprehend menggunakan kebijakan IAM.

Perlindungan data dan manajemen rahasia

Model tanggung jawab AWS bersama berlaku untuk perlindungan data di Amazon Comprehend. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk memelihara kendali atas isi yang dihost pada infrastruktur ini. Konten ini mencakup konfigurasi keamanan dan tugas manajemen untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, silakan lihat Pertanyaan Umum Privasi Data.

Bagian Perlindungan Data di Amazon Comprehend di Panduan Pengembang Amazon Comprehend memberikan tips yang harus Anda pertimbangkan dalam melindungi data seperti menggunakan TLS untuk transmisi dan menghindari penempatan informasi sensitif ke dalam tag atau bidang bentuk bebas.

Enkripsi data-at-rest

Amazon Comprehend AWS Key Management Servicebekerja AWS KMS dengan () untuk menyediakan enkripsi yang disempurnakan untuk data Anda. Amazon Simple Storage Service (Amazon S3) sudah memungkinkan Anda mengenkripsi dokumen masukan saat membuat analisis teks, pemodelan topik, atau pekerjaan Amazon Comprehend khusus. Integrasi dengan AWS KMS memungkinkan Anda mengenkripsi data dalam volume penyimpanan untuk memulai* dan membuat* pekerjaan, dan mengenkripsi hasil output dari pekerjaan mulai* menggunakan kunci Anda sendiri. AWS KMS

Ini adalah praktik terbaik bagi pengguna Amazon Comprehend untuk mengenkripsi bucket Amazon S3 yang digunakan untuk memasukkan dokumen menggunakan solusi enkripsi S3 yang tersedia sesuai dengan kebijakan organisasi mereka.

The AWS Management Console, mengenkripsi Amazon Comprehend model kustom dengan kuncinya sendiri. AWS KMS Untuk itu AWS CLI, Amazon Comprehend dapat mengenkripsi model kustom menggunakan AWS KMS kuncinya sendiri atau kunci terkelola pelanggan (CMK) yang disediakan.

Jika memilih enkripsi saat menggunakan AWS Management Console, Anda dapat memilih salah satu atau kedua metode opsional berikut:

- Enkripsi volume - memastikan bahwa data pada Volume EBS yang digunakan oleh Comprehend dienkripsi selama pelatihan/inferensi (data dibilas setelah pelatihan/inferensi, jadi kunci ini hanya relevan saat pekerjaan sedang berlangsung).
- Enkripsi hasil keluaran - untuk mengenkripsi output yang disimpan dengan memahami di bucket pelanggan menggunakan kunci yang disediakan pelanggan. AWS KMS

Untuk informasi selengkapnya tentang jenis enkripsi seperti enkripsi volume, lihat AWS KMS Enkripsi di Amazon Comprehend.

Informasi pengenal pribadi

Anda dapat menggunakan konsol Amazon Comprehend atau API untuk mendeteksi informasi identitas pribadi (PII) dalam dokumen teks bahasa Inggris. Untuk informasi selengkapnya tentang mendeteksi dan memberi label pada entitas PII dan mengoperasikan berbagai pekerjaan analisis PII, lihat bagian Informasi yang dapat diidentifikasi secara pribadi di Panduan Pengembang Amazon Comprehend.

Penghapusan data

Jika Anda adalah pelanggan Amazon Comprehend yang menggunakan Amazon S3 dan memilih untuk AWS KMS mengelola kunci Anda sendiri, Anda AWS KMS harus mempertimbangkan untuk mencabut kunci dan mendefinisikan pembenaran prosedural untuk melakukannya sesuai dengan persyaratan organisasi mereka. Pencabutan AWS KMS kunci untuk Amazon S3 membuat data apa pun tidak dapat digunakan/tidak dapat dibaca.

Segmentasi dan pengerasan jaringan

Sebagai layanan terkelola, Amazon Comprehend mematuhi Praktik Terbaik AWS untuk Keamanan, Identitas, dan Kepatuhan.

Untuk perlindungan keamanan jaringan yang direkomendasikan, lihat Keamanan Infrastruktur di Amazon Comprehend di Panduan Pengembang Amazon Comprehend.

Lindungi pekerjaan menggunakan Amazon Virtual Private Cloud (Amazon VPC)

Amazon Comprehend menggunakan berbagai langkah keamanan untuk memastikan keamanan data Anda dengan wadah kerja kami di mana disimpan saat digunakan oleh Amazon Comprehend. Namun, wadah pekerjaan mengakses AWS sumber daya—seperti bucket Amazon S3 tempat Anda menyimpan data dan artefak model—melalui internet.

Untuk mengontrol akses ke data Anda, kami sarankan Anda membuat virtual private cloud (VPC) dan mengonfigurasinya sehingga data dan kontainer tidak dapat diakses melalui internet. Untuk informasi tentang membuat dan mengonfigurasi VPC, lihat Memulai Dengan Amazon VPC di Panduan Pengguna Amazon VPC. Menggunakan VPC membantu melindungi data Anda karena Anda dapat mengonfigurasi VPC Anda sehingga tidak terhubung ke internet. Menggunakan VPC juga memungkinkan Anda untuk memantau semua lalu lintas jaringan masuk dan keluar dari wadah pekerjaan kami dengan menggunakan log aliran VPC. Untuk informasi selengkapnya, lihat Log Alur VPC di Panduan Pengguna Amazon VPC.

Anda menentukan konfigurasi VPC Anda ketika Anda membuat pekerjaan, dengan menentukan subnet dan grup keamanan. Saat Anda menentukan subnet dan grup keamanan, Amazon Comprehend membuat antarmuka jaringan elastis (ENI) yang terkait dengan grup keamanan Anda di salah satu subnet. ENI memungkinkan wadah pekerjaan kami terhubung ke sumber daya di VPC Anda. Untuk informasi tentang ENI, lihat Antarmuka Jaringan Elastis di Panduan Pengguna Amazon VPC.

> **Note**
>
> Untuk pekerjaan, Anda hanya dapat mengonfigurasi subnet dengan VPC penyewaan default di mana instans Anda berjalan pada perangkat keras bersama. Untuk informasi selengkapnya tentang atribut tenancy untuk VPC, lihat Instans Khusus di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Anda dapat membuat koneksi pribadi antara VPC Anda dan Amazon Comprehend dengan membuat antarmuka VPC endpoint. Untuk informasi selengkapnya, lihat Amazon Comprehend dan Interface VPC Endpoints ().AWS PrivateLink

Host dan pengerasan gambar

Berdasarkan model tanggung jawab AWS bersama, host dan pengerasan citra AWS lingkungan untuk Amazon Comprehend dikelola oleh sebagai layanan yang disediakan AWS .

Multi-penghunian

Untuk membantu membuat rekomendasi Anda lebih aman, kami sarankan Anda menerapkan rekomendasi keamanan multi-tenancy berikut:

- Gunakan hanya alamat email terverifikasi untuk mengotorisasi akses pengguna ke penyewa berdasarkan kecocokan domain. Jangan percaya alamat email dan nomor telepon kecuali aplikasi Anda memverifikasinya, atau iDP eksternal memberikan bukti verifikasi. Untuk detail lebih lanjut tentang pengaturan izin ini, lihat Izin dan Cakupan Atribut.
- Gunakan atribut yang tidak dapat diubah atau dapat diubah untuk atribut profil pengguna yang mengidentifikasi penyewa. Administrator harus dapat mengubah atribut ini. Selain itu, berikan akses hanya-baca kepada klien aplikasi ke atribut.
- Gunakan pemetaan 1:1 antara IDP eksternal dan klien aplikasi untuk mencegah akses lintas penyewa yang tidak sah. Pengguna yang telah diautentikasi oleh iDP eksternal, dan yang memiliki cookie sesi Amazon Cognito yang valid, dapat mengakses aplikasi penyewa lain yang mempercayai IDP yang sama.
- Saat Anda menerapkan logika pencocokan penyewa dan otorisasi dalam aplikasi Anda, batasi pengguna sehingga mereka tidak dapat mengubah kriteria yang mengotorisasi akses pengguna ke penyewa. Juga, jika iDP eksternal digunakan untuk federasi, batasi administrator penyedia identitas penyewa sehingga mereka tidak dapat mengubah akses pengguna.

Pencegahan confused deputy lintas layanan

Masalah deputi yang membingungkan adalah masalah keamanan multi-tenancy di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan pemanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggil dapat

dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS sediakan alat yang dapat membantu Anda melindungi data Anda untuk semua layanan dengan prinsip layanan yang telah diberikan akses ke sumber daya di akun Anda. Untuk informasi selengkapnya yang mencakup pengamanan yang harus Anda pertimbangkan untuk mengatasi masalah keamanan ini, lihat Pencegahan Deputi Bingung Lintas Layanan di Panduan Pengembang Amazon Comprehend.

Amazon Comprehend Medical

Untuk panduan, lihat Amazon Comprehend bagian sebelumnya.

Amazon Connect

Amazon Connect adalah layanan pusat kontak mandiri berbasis cloud yang memungkinkan keterlibatan pelanggan yang dinamis, pribadi, dan alami dalam skala apa pun. Pelanggan tidak boleh menyertakan PHI apa pun di bidang apa pun yang terkait dengan pengelolaan pengguna, profil keamanan, dan alur kontak dalam Amazon Connect.

Profil Pelanggan Amazon Connect, fitur Amazon Connect, melengkapi agen pusat kontak dengan tampilan profil pelanggan yang lebih terpadu dengan informasi terbaru, untuk menyediakan layanan pelanggan yang lebih personal. Profil Pelanggan dirancang untuk secara otomatis menyatukan informasi pelanggan dari beberapa aplikasi ke dalam profil pelanggan terpadu, mengirimkan profil langsung ke agen segera setelah panggilan dukungan atau interaksi dimulai. Pelanggan harus menahan diri dari penamaan domain atau kunci objek dengan data PHI. Isi Domain dan Objek dienkripsi dan dilindungi, tetapi pengidentifikasi kunci tidak.

Amazon DocumentDB (dengan kompatibilitas MongoDB)

Amazon DocumentDB (dengan kompatibilitas MongoDB) (Amazon DocumentDB) menawarkan enkripsi saat istirahat selama AWS KMS pembuatan cluster via, yang memungkinkan pelanggan mengenkripsi database menggunakan AWS atau kunci yang dikelola pelanggan. Pada instance database yang berjalan dengan enkripsi diaktifkan, data yang disimpan saat istirahat dienkripsi konsisten dengan Panduan yang berlaku pada saat publikasi whitepaper ini, seperti halnya backup otomatis, replika baca, dan snapshot. Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon DocumentDB memenuhi persyaratan

kepatuhan dan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon DocumentDB, lihat Mengenkripsi Data Amazon DocumentDB saat Istirahat.

Koneksi ke Amazon DocumentDB yang berisi PHI harus menggunakan endpoint yang menerima transport terenkripsi (HTTPS). Secara default, cluster Amazon DocumentDB yang baru dibuat hanya menerima koneksi aman menggunakan Transport Layer Security (TLS). Untuk informasi selengkapnya, lihat Mengenkripsi Data dalam Transit. Amazon DocumentDB AWS CloudTrail menggunakan untuk mencatat semua panggilan API. Untuk informasi selengkapnya, lihat Logging dan Monitoring di Amazon DocumentDB.

Untuk fitur manajemen tertentu, Amazon DocumentDB menggunakan teknologi operasional yang dibagi dengan Amazon RDS. Konsol Amazon DocumentDB, AWS CLI, dan panggilan API dicatat sebagai panggilan yang dilakukan ke Amazon RDS API.

Amazon DynamoDB

Koneksi ke Amazon DynamoDB yang berisi PHI harus menggunakan endpoint yang menerima transport terenkripsi (HTTPS). Untuk daftar titik akhir regional, lihat titik akhir layanan AWS.

Amazon DynamoDB menawarkan enkripsi DynamoDB, yang memungkinkan pelanggan mengenkripsi database menggunakan kunci yang dikelola pelanggan. AWS KMS Pada instance database yang berjalan dengan enkripsi Amazon DynamoDB, data yang disimpan saat istirahat di penyimpanan dasar dienkripsi konsisten dengan Panduan yang berlaku pada saat publikasi whitepaper ini, seperti halnya backup otomatis, replika baca, dan snapshot.

Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon DynamoDB memenuhi kepatuhan dan persyaratan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon DynamoDB, lihat Enkripsi DynamoDB saat Istirahat.

Amazon Elastic Block Store

Enkripsi Amazon EBS saat istirahat konsisten dengan Panduan yang berlaku pada saat publikasi whitepaper ini. Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon EBS memenuhi persyaratan kepatuhan dan peraturan mereka. Dengan enkripsi Amazon EBS, kunci enkripsi volume unik dihasilkan untuk setiap volume EBS. Pelanggan memiliki fleksibilitas untuk memilih kunci KMS mana dari yang AWS Key Management Service digunakan untuk mengenkripsi setiap tombol volume. Untuk informasi selengkapnya, lihat Enkripsi Amazon EBS.

Amazon Elastic Compute Cloud

Amazon EC2 adalah layanan komputasi yang dapat diskalakan dan dapat dikonfigurasi pengguna yang mendukung beberapa metode untuk mengenkripsi data saat istirahat. Misalnya, pelanggan mungkin memilih untuk melakukan enkripsi PHI tingkat aplikasi atau lapangan karena diproses dalam aplikasi atau platform basis data yang dihosting di instans Amazon EC2. Pendekatan berkisar dari mengenkripsi data menggunakan pustaka standar dalam kerangka aplikasi seperti Java atau .NET; memanfaatkan fitur Enkripsi Data Transparan di Microsoft SQL atau Oracle; atau dengan mengintegrasikan solusi berbasis pihak ketiga dan perangkat lunak lainnya sebagai layanan (SaaS) ke dalam aplikasi mereka.

Pelanggan dapat memilih untuk mengintegrasikan aplikasi mereka yang berjalan di Amazon EC2 dengan AWS KMS SDK, menyederhanakan proses manajemen dan penyimpanan kunci. Pelanggan juga dapat menerapkan enkripsi data saat istirahat menggunakan enkripsi tingkat file atau full disk (FDE) dengan menggunakan perangkat lunak pihak ketiga dari AWS Marketplace Mitra atau alat enkripsi sistem file asli (seperti dm-crypt, LUKS, dll.).

Lalu lintas jaringan yang berisi PHI harus mengenkripsi data dalam perjalanan. Untuk lalu lintas antara sumber eksternal (seperti internet atau lingkungan TI tradisional) dan Amazon EC2, pelanggan harus menggunakan mekanisme enkripsi transportasi standar terbuka seperti Transport Layer Security (TLS) atau jaringan pribadi virtual IPsec (VPN), konsisten dengan Panduan. Internal ke Amazon Virtual Private Cloud (VPC) untuk perjalanan data antara instans Amazon EC2, lalu lintas jaringan yang berisi PHI juga harus dienkripsi; sebagian besar aplikasi mendukung TLS atau protokol lain yang menyediakan enkripsi transit yang dapat dikonfigurasi agar konsisten dengan Panduan. Untuk aplikasi dan protokol yang tidak mendukung enkripsi, sesi transmisi PHI dapat dikirim melalui terowongan terenkripsi menggunakan IPsec atau implementasi serupa antar instance.

Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) terintegrasi dengan Amazon Elastic Container Service (Amazon ECS) dan memungkinkan pelanggan untuk dengan mudah menyimpan, menjalankan, dan mengelola gambar kontainer untuk aplikasi yang berjalan di Amazon ECS. Setelah pelanggan menentukan repositori Amazon ECR dalam Definisi Tugas mereka, Amazon ECS akan mengambil gambar yang sesuai untuk aplikasi mereka.

Tidak ada langkah khusus yang diperlukan untuk menggunakan Amazon ECR dengan gambar kontainer yang berisi PHI. Gambar kontainer dienkripsi saat dalam perjalanan dan disimpan dienkripsi saat diam menggunakan enkripsi sisi server Amazon S3 (SSE-S3).

Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) adalah layanan manajemen kontainer yang sangat skalabel dan berkinerja tinggi yang mendukung kontainer Docker dan memungkinkan pelanggan menjalankan aplikasi dengan mudah pada cluster instans Amazon EC2 yang dikelola. Amazon ECS menghilangkan kebutuhan pelanggan untuk menginstal, mengoperasikan, dan menskalakan infrastruktur manajemen klaster mereka sendiri.

Dengan panggilan API sederhana, pelanggan dapat meluncurkan dan menghentikan aplikasi yang mendukung Docker, menanyakan status lengkap klaster mereka, dan mengakses banyak fitur yang sudah dikenal seperti grup keamanan, Elastic Load Balancing, volume EBS, dan peran IAM. Pelanggan dapat menggunakan Amazon ECS untuk menjadwalkan penempatan kontainer di seluruh klaster mereka berdasarkan kebutuhan sumber daya dan persyaratan ketersediaan.

Menggunakan ECS dengan beban kerja yang memproses PHI tidak memerlukan konfigurasi tambahan. ECS bertindak sebagai layanan orkestrasi yang mengoordinasikan peluncuran kontainer (gambar yang disimpan dalam S3) pada EC2, dan tidak beroperasi dengan atau pada data dalam beban kerja yang diatur. Konsisten dengan peraturan HIPAA dan Adendum Asosiasi AWS Bisnis, PHI harus dienkripsi saat transit dan istirahat saat diakses oleh kontainer yang diluncurkan dengan ECS. Berbagai mekanisme untuk mengenkripsi saat istirahat tersedia dengan setiap opsi AWS penyimpanan (misalnya, S3, EBS, dan KMS). Memastikan enkripsi lengkap PHI yang dikirim antar kontainer juga dapat mengarahkan pelanggan untuk menyebarkan jaringan overlay (seperti VNS3, Weave Net atau sejenisnya), untuk menyediakan lapisan enkripsi yang berlebihan. Namun demikian, logging lengkap juga harus diaktifkan (misalnya, melalui CloudTrail), dan semua log instance container harus diarahkan ke CloudWatch.

Menggunakan Firelens dan AWS untuk Fluent Bit dengan beban kerja yang memproses PHI tidak memerlukan konfigurasi tambahan, kecuali log berisi PHI. Jika log berisi PHI, maka log tersebut tidak boleh dipancarkan ke file log, kecuali enkripsi disk diaktifkan. Sebagai gantinya, konfigurasikan aplikasi Anda untuk memancarkan log ke out/error standar yang akan dikumpulkan secara otomatis oleh. FireLens Demikian pula, jangan aktifkan buffering file untuk Fluent Bit, kecuali enkripsi disk juga diaktifkan. Terakhir, tujuan log harus mendukung encryption-in-transit; semua plugin keluaran AWS Layanan di AWS untuk Bit Lancar akan selalu menggunakan enkripsi TLS untuk mengekspor log.

Amazon Elastic File System (Amazon EFS)

Amazon Elastic File System (Amazon EFS) menyediakan penyimpanan file yang sederhana, dapat diskalakan, dan elastis untuk digunakan dengan layanan AWS Cloud dan sumber daya lokal. Mudah

digunakan dan menawarkan antarmuka sederhana yang memungkinkan pelanggan membuat dan mengkonfigurasi sistem file dengan cepat dan mudah. Amazon EFS dibangun untuk meningkatkan skala permintaan secara elastis tanpa mengganggu aplikasi, tumbuh dan menyusut secara otomatis saat pelanggan menambah dan menghapus file.

Untuk memenuhi persyaratan bahwa PHI dienkripsi saat istirahat, dua jalur tersedia di EFS. EFS mendukung enkripsi saat istirahat saat sistem file baru dibuat. Selama pembuatan, opsi untuk "Aktifkan enkripsi data saat istirahat" harus dipilih. Memilih opsi ini memastikan bahwa semua data yang ditempatkan pada sistem file EFS akan dienkripsi menggunakan enkripsi AES-256 dan kunci -managed. AWS KMS Pelanggan dapat memilih untuk mengenkripsi data sebelum ditempatkan di EFS, tetapi mereka kemudian bertanggung jawab untuk mengelola proses enkripsi dan manajemen kunci.

PHI tidak boleh digunakan sebagai semua atau bagian dari nama file atau nama folder apa pun. Enkripsi PHI saat transit untuk Amazon EFS disediakan oleh Transport Layer Security (TLS) antara layanan EFS dan instans yang memasang sistem file. EFS menawarkan mount helper untuk memfasilitasi koneksi ke sistem file menggunakan TLS. Secara default, TLS tidak digunakan dan harus diaktifkan saat memasang sistem file menggunakan EFS mount helper. Pastikan bahwa perintah mount berisi opsi "-o tls" untuk mengaktifkan enkripsi TLS. Atau, pelanggan yang memilih untuk tidak menggunakan EFS mount helper dapat mengikuti instruksi dalam dokumentasi EFS untuk mengonfigurasi klien NFS mereka agar terhubung melalui terowongan TLS.

Amazon Elastic Kubernetes Service (Amazon EKS)

Amazon Elastic Kubernetes Service (Amazon EKS) adalah layanan terkelola yang memudahkan pelanggan menjalankan Kubernetes di AWS tanpa perlu berdiri atau memelihara pesawat kontrol Kubernetes mereka sendiri. Kubernetes adalah sebuah sistem sumber terbuka untuk melakukan otomatisasi terhadap deployment, penskalaan, dan pengelolaan aplikasi terkontainer. Untuk informasi Keamanan dan Kepatuhan tambahan, lihat whitepaper Architecting for HIPAA Security and Compliance on Amazon EKS.

Amazon ElastiCache untuk Redis

Amazon ElastiCache for Redis adalah layanan struktur data dalam memori yang kompatibel dengan Redis yang dapat digunakan sebagai penyimpanan data atau cache. Untuk menyimpan PHI, pelanggan harus memastikan bahwa mereka menjalankan HIPAA terbaru yang memenuhi syarat ElastiCache untuk versi mesin Redis dan tipe node generasi saat ini. Amazon ElastiCache untuk Redis mendukung penyimpanan PHI untuk jenis node berikut dan versi mesin Redis:

- Jenis Node: generasi saat ini saja (misalnya, pada saat publikasi whitepaper ini, M4, M5, R4, R5, T2, T3)
- ElastiCache untuk versi mesin Redis: 3.2.6 dan 4.0.10 dan seterusnya

Untuk informasi selengkapnya tentang memilih node generasi saat ini, lihat ElastiCache harga Amazon. Untuk informasi selengkapnya tentang memilih mesin Redis ElastiCache untuk Redis, lihat Apa itu Amazon ElastiCache untuk Redis?

Pelanggan juga harus memastikan bahwa cluster dan node dalam cluster dikonfigurasi untuk mengenkripsi data saat istirahat, mengaktifkan enkripsi transport dan mengaktifkan otentikasi perintah Redis. Selain itu, pelanggan juga harus memastikan bahwa kluster Redis mereka diperbarui dengan pembaruan layanan jenis 'Keamanan' terbaru pada atau sebelum 'Direkomendasikan Terapkan berdasarkan Tanggal' (tanggal yang direkomendasikan pembaruan diterapkan) setiap saat. Untuk informasi selengkapnya, lihat bagian di bawah ini.

Topik

- Enkripsi saat Data Tidak Berpindah
- Enkripsi Transportasi
- Autentikasi
- Menerapkan Pembaruan ElastiCache Layanan

Enkripsi saat Data Tidak Berpindah

Amazon ElastiCache untuk Redis menyediakan enkripsi data untuk klasternya untuk membantu melindungi data saat istirahat. Ketika pelanggan mengaktifkan enkripsi saat istirahat untuk cluster pada saat pembuatan, Amazon ElastiCache untuk Redis mengenkripsi data pada disk dan backup Redis otomatis. Data pelanggan pada disk dienkripsi menggunakan kunci simetris Advanced Encryption Standard (AES) -512 yang dipercepat perangkat keras. Cadangan Redis dienkripsi melalui kunci enkripsi yang dikelola Amazon S3 (SSE-S3). Bucket S3 dengan enkripsi sisi server diaktifkan akan mengenkripsi data menggunakan kunci simetris Advanced Encryption Standard (AES) -256 yang dipercepat perangkat keras sebelum menyimpannya di bucket.

Untuk detail selengkapnya tentang kunci enkripsi terkelola Amazon S3 (SSE-S3), lihat Melindungi Data Menggunakan Enkripsi Sisi Server dengan Kunci Enkripsi Terkelola Amazon S3 (SSE-S3). Pada kluster ElastiCache Redis (tunggal atau multi-node) yang berjalan dengan enkripsi, data yang disimpan saat istirahat dienkripsi konsisten dengan Panduan yang berlaku pada saat publikasi

whitepaper ini. Ini termasuk data pada disk dan backup otomatis di bucket S3. Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon ElastiCache for Redis memenuhi persyaratan kepatuhan dan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon ElastiCache untuk Redis, lihat Apa itu Amazon ElastiCache untuk Redis?

Enkripsi Transportasi

Amazon ElastiCache untuk Redis menggunakan TLS untuk mengenkripsi data dalam perjalanan. Koneksi ke ElastiCache untuk Redis yang mengandung PHI harus menggunakan enkripsi transport dan mengevaluasi konfigurasi untuk konsistensi dengan Panduan. Untuk informasi lebih lanjut, lihat CreateReplicationGroup. Untuk informasi selengkapnya tentang mengaktifkan enkripsi transport, lihat ElastiCache untuk Redis In-Transit Encryption (TLS).

Autentikasi

Amazon ElastiCache untuk kluster Redis (node tunggal/multi) yang berisi PHI harus menyediakan token Redis AUTH untuk mengaktifkan otentikasi perintah Redis. Redis AUTH tersedia saat enkripsi saat istirahat dan enkripsi dalam transit diaktifkan. Pelanggan harus memberikan token yang kuat untuk Redis AUTH dengan batasan berikut:

- Harus hanya karakter ASCII yang dapat dicetak
- Harus minimal 16 karakter dan panjangnya tidak lebih dari 128 karakter
- Tidak dapat berisi salah satu karakter berikut: '/', '"', atau “@”

Token ini harus diatur dari dalam Parameter Permintaan pada saat pembuatan grup replikasi Redis (single/multi node) dan dapat diperbarui nanti dengan nilai baru. AWS mengenkripsi token ini menggunakan AWS Key Management Service ()AWS KMS. Untuk informasi selengkapnya tentang Redis AUTH, lihat ElastiCache Redis In-Transit Encryption (TLS).

Menerapkan Pembaruan ElastiCache Layanan

Amazon ElastiCache for Redis cluster (single/multi node) yang berisi PHI harus diperbarui dengan pembaruan layanan jenis 'Keamanan' terbaru pada atau sebelum 'Direkomendasikan Terapkan berdasarkan Tanggal. ' ElastiCache menawarkan ini sebagai fitur swalayan yang dapat digunakan pelanggan untuk menerapkan pembaruan kapan saja sesuai permintaan dan secara real time. Setiap pembaruan layanan dilengkapi dengan 'Keparahan' dan 'Direkomendasikan Terapkan berdasarkan Tanggal' dan hanya tersedia untuk grup replikasi Redis yang berlaku.

Bidang 'SLA Met' di fitur pembaruan layanan akan menyatakan apakah pembaruan diterapkan pada atau sebelum 'Direkomendasikan Terapkan berdasarkan Tanggal'. Jika pelanggan memilih untuk tidak menerapkan pembaruan ke grup replikasi Redis yang berlaku dengan 'Direkomendasikan Terapkan berdasarkan Tanggal, 'tidak ElastiCache akan mengambil tindakan apa pun untuk menerapkannya. Pelanggan dapat menggunakan dasbor riwayat pembaruan layanan untuk meninjau aplikasi pembaruan ke grup replikasi Redis mereka dari waktu ke waktu. Untuk informasi selengkapnya tentang cara menggunakan fitur ini, lihat Pembaruan Layanan Mandiri di Amazon ElastiCache.

OpenSearch Layanan Amazon

Amazon OpenSearch Service memungkinkan pelanggan menjalankan cluster OSS Elasticsearch yang dikelola OpenSearch atau lama di Amazon Virtual Private Cloud (Amazon VPC) khusus. Saat menggunakan OpenSearch Layanan dengan PHI, pelanggan harus menggunakan OpenSearch atau Elasticsearch 6.0 atau yang lebih baru. Pelanggan harus memastikan PHI dienkripsi saat istirahat dan dalam perjalanan dalam Layanan Amazon. OpenSearch Pelanggan dapat menggunakan enkripsi AWS KMS kunci untuk mengenkripsi data saat istirahat di domain OpenSearch Layanan mereka, yang hanya tersedia untuk OpenSearch dan Elasticsearch 5.1 atau yang lebih baru. Untuk informasi selengkapnya tentang cara mengenkripsi data saat istirahat, lihat Enkripsi data saat istirahat untuk OpenSearch Layanan Amazon.

Setiap domain OpenSearch Layanan berjalan di VPC-nya sendiri. Pelanggan harus mengaktifkan node-to-node enkripsi, yang tersedia di semua OpenSearch versi, dan di Elasticsearch 6.0 atau yang lebih baru. Jika pelanggan mengirim data ke OpenSearch Layanan melalui HTTPS, node-to-node enkripsi membantu memastikan bahwa data mereka tetap dienkripsi sebagai OpenSearch mendistribusikan (dan mendistribusikan ulang) ke seluruh cluster. Jika data tiba tanpa dienkripsi melalui HTTP, OpenSearch Layanan mengenkripsi data setelah mencapai cluster. Oleh karena itu, PHI apa pun yang memasuki kluster OpenSearch Layanan Amazon harus dikirim melalui HTTPS. Untuk informasi selengkapnya, lihat ode-to-node enkripsi N untuk OpenSearch Layanan Amazon.

Log dari API konfigurasi OpenSearch Layanan dapat ditangkap AWS CloudTrail. Untuk informasi selengkapnya, lihat Memantau panggilan API OpenSearch Layanan Amazon dengan AWS CloudTrail.

Amazon EMR

Amazon EMR menyebarkan dan mengelola sekelompok instans Amazon EC2 ke akun pelanggan. Untuk informasi tentang enkripsi dengan Amazon EMR, lihat Opsi Enkripsi.

Amazon EventBridge

Amazon EventBridge (sebelumnya Amazon CloudWatch Events) adalah bus acara tanpa server yang memungkinkan Anda membuat aplikasi berbasis peristiwa yang dapat diskalakan. EventBridge mengirimkan aliran data waktu nyata dari sumber peristiwa, seperti Zendesk, Datadog, atau Pagerduty, dan merutekan data tersebut ke target seperti. AWS Lambda

Secara default, mengenkripsi data menggunakan Standar EventBridge Enkripsi Lanjutan (AES-256) 256-bit di bawah CMK milik AWS, yang membantu mengamankan data pelanggan dari akses yang tidak sah. Pelanggan harus memastikan bahwa sumber daya AWS apa pun yang memancarkan peristiwa yang menyimpan, memproses, atau mentransmisikan PHI dikonfigurasi sesuai dengan praktik terbaik.

Amazon EventBridge terintegrasi dengan AWS CloudTrail dan pelanggan dapat melihat peristiwa terbaru di CloudTrail konsol dalam riwayat Acara. Untuk informasi lebih lanjut, lihat EventBridge Informasi di CloudTrail.

Amazon Forecast

Amazon Forecast adalah layanan yang dikelola sepenuhnya yang menggunakan pembelajaran mesin untuk memberikan perkiraan yang sangat akurat. Berdasarkan teknologi peramalan pembelajaran mesin yang sama yang digunakan oleh Amazon.com. Setiap interaksi yang dilakukan pelanggan dengan Amazon Forecast dilindungi oleh enkripsi. Konten apa pun yang diproses oleh Amazon Forecast dienkripsi dengan kunci pelanggan melalui Amazon Key Management Service, dan dienkripsi saat istirahat di Wilayah AWS tempat pelanggan menggunakan layanan ini.

Amazon Forecast terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau layanan AWS di Amazon Forecast. CloudTrail menangkap semua panggilan API untuk Amazon Forecast sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Amazon Forecast dan panggilan kode ke operasi Amazon Forecast API. Jika pelanggan membuat jejak, pelanggan dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Amazon Forecast. Untuk informasi selengkapnya, lihat Logging Forecast API Calls with AWS CloudTrail.

Secara default, file log yang dikirimkan CloudTrail ke bucket mereka dienkripsi oleh enkripsi sisi server Amazon dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3). Untuk menyediakan lapisan keamanan yang dapat dikelola secara langsung, pelanggan dapat menggunakan enkripsi sisi server dengan AWS KMS—managed keys (SSE-KMS) untuk file log mereka. CloudTrail

Mengaktifkan enkripsi sisi server mengenkripsi file log tetapi bukan file intisari dengan SSE-KMS. File Digest dienkripsi dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3).

AWS Forecast mengimpor dan mengekspor data ke/dari bucket S3. Saat mengimpor dan mengekspor data dari Amazon S3, pelanggan harus memastikan bucket S3 dikonfigurasi dengan cara yang konsisten dengan panduan. Untuk informasi selengkapnya, lihat Memulai.

Amazon FSx

Amazon FSx adalah layanan yang dikelola sepenuhnya yang menyediakan sistem file yang kaya fitur dan berkinerja tinggi. Amazon FSx untuk Windows File Server menyediakan penyimpanan file yang sangat andal dan terukur dan dapat diakses melalui protokol Server Message Block (SMB). Amazon FSx for Lustre menyediakan penyimpanan berkinerja tinggi untuk beban kerja komputasi dan didukung oleh Lustre, sistem file berkinerja tinggi paling populer di dunia.

Amazon FSx mendukung dua bentuk enkripsi untuk sistem file, enkripsi data dalam perjalanan dan enkripsi saat istirahat. Amazon FSx for Windows File Server juga mendukung pencatatan semua panggilan AWS CloudTrail API menggunakan.

Enkripsi data dalam perjalanan didukung oleh Amazon FSx for Windows File Server pada instans komputasi yang mendukung protokol SMB 3.0 atau yang lebih baru, dan oleh Amazon FSx for Lustre di instans Amazon EC2 yang mendukung enkripsi saat transit. Atau, pelanggan dapat mengenkripsi data sebelum menyimpan di Amazon FSx tetapi kemudian bertanggung jawab atas proses enkripsi dan manajemen kunci.

Enkripsi data saat istirahat diaktifkan secara otomatis saat membuat sistem file Amazon FSx, menggunakan algoritma enkripsi AES-256 dan kunci -managed. AWS KMS Data dan metadata secara otomatis dienkripsi sebelum ditulis ke sistem file, dan secara otomatis didekripsi sebelum disajikan ke aplikasi. PHI tidak boleh digunakan dalam nama file atau folder apa pun.

Amazon GuardDuty

Amazon GuardDuty adalah layanan deteksi ancaman terkelola yang terus memantau perilaku berbahaya atau tidak sah untuk membantu pelanggan melindungi akun dan beban kerja AWS mereka. Ini memantau aktivitas seperti panggilan API yang tidak biasa atau penerapan yang berpotensi tidak sah yang menunjukkan kemungkinan kompromi akun. Amazon GuardDuty juga mendeteksi kejadian yang berpotensi dikompromikan atau pengintaian oleh penyerang.

Amazon GuardDuty terus memantau dan menganalisis sumber data berikut: Log Aliran VPC AWS CloudTrail , log peristiwa, dan log DNS. Ini menggunakan umpan intelijen ancaman, seperti daftar IP dan domain berbahaya, dan pembelajaran mesin untuk mengidentifikasi aktivitas yang tidak terduga dan berpotensi tidak sah dan berbahaya dalam lingkungan AWS. Dengan demikian, Amazon tidak GuardDuty boleh menemukan PHI apa pun karena data ini tidak boleh disimpan di salah satu sumber data berbasis AWS yang tercantum di atas.

Amazon HealthLake

Amazon HealthLake memungkinkan pelanggan di industri perawatan kesehatan dan ilmu hayati untuk menyimpan, mengubah, menanyakan, dan menganalisis data kesehatan pada skala petabyte. Pelanggan dapat menggunakan Amazon HealthLake untuk mengirimkan, memproses, dan menyimpan PHI. Amazon HealthLake mengenkripsi data saat istirahat di penyimpanan data pelanggan secara default. Semua data layanan dan metadata dienkripsi dengan kunci KMS milik layanan. Sesuai spesifikasi Fast Healthcare Interoperability Resources (FHIR), jika pelanggan menghapus sumber daya FHIR, itu hanya akan disembunyikan dari pengambilan, dan akan disimpan oleh layanan untuk pembuatan versi. Saat pelanggan menggunakan StartFhir APIImportJob , Amazon HealthLake akan memberlakukan persyaratan untuk mengekspor data ke bucket Amazon S3 terenkripsi.

Amazon HealthLake mengenkripsi data baik dalam perjalanan maupun saat istirahat. Untuk enkripsi data dalam perjalanan, Anda dapat menggunakan panggilan API AWS yang diterbitkan untuk mengakses HealthLake melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.0 atau versi yang lebih baru. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3. Klien juga harus mendukung cipher suite dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini. Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Sebagai alternatif, pelanggan dapat menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensyal keamanan sementara guna menandatangani permintaan. Untuk enkripsi data saat istirahat, Amazon HealthLake mengenkripsi data di penyimpanan data pelanggan dengan kunci AWS KMS milik pelanggan atau dengan kunci AWS KMS milik layanan secara default. Semua data layanan dan metadata dienkripsi saat istirahat dengan kunci AWS KMS milik layanan.

Amazon HealthLake terintegrasi dengan AWS CloudTrail. CloudTrail menangkap semua panggilan API ke Amazon HealthLake sebagai peristiwa, termasuk panggilan yang dilakukan sebagai hasil

interaksi dengan AWS Management Console, antarmuka baris perintah (CLI), dan secara terprogram menggunakan perangkat pengembangan perangkat lunak (SDK).

Amazon Inspector

Amazon Inspector adalah layanan penilaian keamanan otomatis bagi pelanggan yang ingin meningkatkan keamanan dan kepatuhan mereka terhadap aplikasi yang digunakan di AWS. Amazon Inspector secara otomatis menilai kerentanan atau penyimpangan dari praktik terbaik pada aplikasi. Setelah melakukan penilaian, Amazon Inspector menghasilkan daftar detail temuan keamanan yang diprioritaskan berdasarkan tingkat keparahan. Pelanggan dapat menjalankan Amazon Inspector pada instans EC2 yang berisi PHI. Amazon Inspector mengenkripsi semua data yang dikirimkan melalui jaringan serta semua data telemetri yang disimpan saat istirahat.

Layanan Terkelola Amazon untuk Apache Flink

Amazon Managed Service untuk Apache Flink memungkinkan pelanggan untuk dengan cepat membuat kode SQL yang terus membaca, memproses, dan menyimpan data dalam waktu dekat. Menggunakan kueri SQL standar pada data streaming, pelanggan dapat membangun aplikasi yang mengubah dan memberikan wawasan ke dalam data mereka. Layanan Terkelola untuk Apache Flink mendukung input dari Kinesis Data Streams dan aliran pengiriman Firehose sebagai sumber untuk aplikasi analitik. Jika aliran dienkripsi, Managed Service for Apache Flink mengakses data dalam aliran terenkripsi dengan mulus tanpa perlu konfigurasi lebih lanjut. Layanan Terkelola untuk Apache Flink tidak menyimpan data yang tidak terenkripsi yang dibaca dari Kinesis Data Streams. Untuk informasi lebih lanjut, lihat Pengonfigurasian Input Aplikasi.

Layanan Terkelola untuk Apache Flink terintegrasi dengan keduanya dan AWS CloudTrail Amazon CloudWatch Logs untuk pemantauan aplikasi. Untuk informasi selengkapnya, lihat Alat Pemantauan dan Bekerja dengan CloudWatch Log Amazon.

Amazon Data Firehose

Ketika pelanggan mengirim data dari produsen data mereka ke aliran data Kinesis mereka, Amazon Kinesis Data Streams mengenkripsi data menggunakan kunci sebelum menyimpannya saat istirahat. AWS KMS Ketika aliran pengiriman Firehose membaca data dari aliran Kinesis, Kinesis Data Streams pertama-tama mendekripsi data dan kemudian mengirimkannya ke Firehose. Firehose menyangga data dalam memori berdasarkan petunjuk buffering yang ditentukan oleh pelanggan.

Kemudian mengirimkan data ke tujuan tanpa menyimpan data yang tidak terenkripsi saat istirahat. Untuk informasi selengkapnya tentang enkripsi dengan Firehose, lihat Perlindungan Data di Amazon Data Firehose.

AWS menyediakan berbagai alat yang dapat digunakan pelanggan untuk memantau Amazon Data Firehose, termasuk CloudWatch metrik Amazon, Log Amazon, Agen Kinesis CloudWatch , serta pencatatan dan riwayat API. Untuk informasi selengkapnya, lihat Memantau Amazon Data Firehose.

Amazon Kinesis Streams

Amazon Kinesis Streams memungkinkan pelanggan membuat aplikasi khusus yang memproses atau menganalisis data streaming untuk kebutuhan khusus. Fitur enkripsi sisi server memungkinkan pelanggan untuk mengenkripsi data saat istirahat. Ketika enkripsi sisi server diaktifkan, Kinesis Streams akan menggunakan AWS KMS kunci untuk mengenkripsi data sebelum menyimpannya di disk. Untuk informasi selengkapnya, lihat Perlindungan Data di Amazon Kinesis Data Streams. Koneksi ke Amazon S3 yang berisi PHI harus menggunakan titik akhir yang menerima transportasi terenkripsi (yaitu, HTTPS). Untuk daftar titik akhir regional, lihat titik akhir layanan AWS.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams adalah layanan AWS yang dikelola sepenuhnya yang dapat digunakan pelanggan untuk melakukan streaming video langsung dari perangkat ke AWS Cloud, atau membuat aplikasi untuk pemrosesan video real-time atau analitik video berorientasi batch. Enkripsi sisi server adalah fitur dalam Kinesis Video Streams yang secara otomatis mengenkripsi data saat istirahat dengan menggunakan kunci (sebelumnya CMK) AWS KMS yang ditentukan oleh pelanggan. Data dienkripsi sebelum ditulis ke lapisan penyimpanan aliran Kinesis Video Streams, dan didekripsi setelah diambil dari penyimpanan.

Amazon Kinesis Video Streams SDK dapat digunakan untuk mengirimkan data video streaming yang berisi PHI. Secara default, SDK menggunakan TLS untuk mengenkripsi bingkai dan fragmen yang dihasilkan oleh perangkat keras tempat ia diinstal. SDK tidak mengelola atau memengaruhi data yang disimpan saat istirahat. Amazon Kinesis Video AWS CloudTrail Streams digunakan untuk mencatat semua panggilan API.

Amazon Lex

Amazon Lex adalah layanan AWS untuk membangun antarmuka percakapan untuk aplikasi yang menggunakan suara dan teks. Dengan Amazon Lex, mesin percakapan yang sama yang mendukung

Amazon Alexa sekarang tersedia untuk pengembang mana pun, memungkinkan pelanggan untuk membangun chatbots bahasa alami yang canggih ke dalam aplikasi baru dan yang sudah ada. Amazon Lex menyediakan fungsionalitas mendalam dan fleksibilitas pemahaman bahasa alami (NLU) dan pengenalan suara otomatis (ASR) sehingga pelanggan dapat membangun pengalaman pengguna yang sangat menarik dengan interaksi percakapan yang hidup, dan membuat kategori produk baru.

Lex menggunakan protokol HTTPS untuk berkomunikasi baik dengan klien maupun layanan AWS lainnya. Akses ke Lex didorong oleh API, dan hak istimewa IAM yang paling tidak sesuai dapat ditegakkan. Untuk informasi selengkapnya, lihat Perlindungan Data di Amazon Lex.

Pemantauan penting untuk menjaga keandalan, ketersediaan, dan kinerja chatbot Amazon Lex pelanggan. Untuk melacak kesehatan bot Amazon Lex, gunakan Amazon CloudWatch. Dengan CloudWatch, pelanggan bisa mendapatkan metrik untuk operasi Amazon Lex individual atau untuk operasi Amazon Lex global untuk akun mereka. Pelanggan juga dapat mengatur CloudWatch alarm untuk diberi tahu ketika satu atau beberapa metrik melebihi ambang batas yang ditentukan pelanggan. Misalnya, pelanggan dapat memantau jumlah permintaan yang dibuat ke bot selama periode waktu tertentu, melihat latensi permintaan yang berhasil, atau menaikkan alarm ketika kesalahan melebihi ambang batas. Lex juga terintegrasi dengan AWS CloudTrail log panggilan Lex API. Untuk informasi selengkapnya, lihat Pemantauan di Amazon Lex.

Amazon Managed Streaming for Apache Kafka (Amazon MSK)

Amazon MSK menyediakan fitur enkripsi untuk data saat istirahat dan untuk data dalam perjalanan. Untuk enkripsi data saat istirahat, Amazon MSK cluster menggunakan enkripsi sisi server Amazon EBS dan AWS KMS kunci untuk mengenkripsi volume penyimpanan. Untuk data dalam transit, kluster MSK Amazon memiliki enkripsi yang diaktifkan melalui TLS untuk komunikasi antar broker.

Pengaturan konfigurasi enkripsi diaktifkan saat cluster dibuat. Selain itu, secara default, enkripsi dalam transit diatur ke TLS untuk cluster yang dibuat dari CLI atau Konsol. AWS Konfigurasi tambahan diperlukan bagi klien untuk berkomunikasi dengan cluster menggunakan enkripsi TLS. Pelanggan dapat mengubah pengaturan enkripsi default dengan memilih pengaturan TLS/PlainText. Untuk informasi selengkapnya, lihat Enkripsi MSK Amazon.

Pelanggan dapat memantau kinerja cluster pelanggan menggunakan konsol MSK Amazon, CloudWatch konsol Amazon, atau pelanggan dapat mengakses metrik JMX dan host menggunakan Open Monitoring dengan Prometheus, solusi pemantauan open source.

Alat yang dirancang untuk dibaca dari eksportir Prometheus kompatibel dengan Pemantauan Terbuka, seperti: Datadog, Lensa, Relik Baru, Sumologic, atau server Prometheus. Untuk detail tentang Pemantauan Terbuka, lihat dokumentasi Pemantauan Terbuka MSK Amazon.

Harap dicatat bahwa versi default Apache Zookeeper yang dibundel dengan Apache Kafka tidak mendukung enkripsi. Namun, penting untuk dicatat bahwa komunikasi antara Apache Zookeeper dan Apache Kafka broker terbatas pada broker, topik, dan informasi status partisi. Satu-satunya cara data dapat diproduksi dan dikonsumsi dari kluster MSK Amazon adalah melalui koneksi pribadi antara klien mereka di VPC mereka dan kluster MSK Amazon. Amazon MSK tidak mendukung titik akhir publik.

Amazon MQ

Amazon MQ adalah layanan broker pesan terkelola untuk Apache ActiveMQ yang memudahkan untuk mengatur dan mengoperasikan broker pesan di cloud. Amazon MQ bekerja dengan aplikasi dan layanan yang ada tanpa perlu pelanggan untuk mengelola, mengoperasikan, atau memelihara sistem pesan mereka sendiri. Untuk menyediakan enkripsi data PHI saat transit, protokol berikut dengan TLS diaktifkan harus digunakan untuk mengakses broker:

- AMQP
- MQTT
- MQTT lebih WebSocket
- OpenWire
- STOMP
- STOMP berakhir WebSocket

Amazon MQ mengenkripsi pesan saat istirahat dan dalam perjalanan menggunakan kunci enkripsi yang dikelola dan disimpan dengan aman. Amazon MQ menggunakan CloudTrail untuk mencatat semua panggilan API.

Amazon Neptune

Amazon Neptune adalah layanan basis data grafik yang cepat, andal, terkelola penuh yang memudahkan membangun dan menjalankan aplikasi yang bekerja dengan set data yang sangat terhubung. Inti dari Amazon Neptunus adalah mesin database grafik berkinerja tinggi yang dibuat khusus yang dioptimalkan untuk menyimpan miliaran hubungan dan menanyakan grafik dengan

latensi milidetik. Amazon Neptunus mendukung bahasa kueri grafik populer TinkerPop Apache Gremlin dan SPARQL W3C.

Data yang berisi PHI sekarang dapat disimpan dalam contoh terenkripsi Amazon Neptunus. Instance terenkripsi Amazon Neptunus hanya dapat ditentukan pada saat pembuatan dengan memilih 'Aktifkan Enkripsi' dari konsol Amazon Neptunus. Semua log, cadangan, dan snapshot dienkripsi untuk instance terenkripsi Amazon Neptunus. Manajemen kunci untuk instance terenkripsi Amazon Neptunus disediakan melalui file. AWS KMS Enkripsi data dalam perjalanan disediakan melalui SSL/TLS. Amazon Neptunus CloudTrail menggunakan untuk mencatat semua panggilan API.

AWS Network Firewall

AWS Network Firewall adalah layanan firewall terkelola yang memudahkan penerapan perlindungan jaringan penting untuk semua Amazon Virtual Private Cloud (Amazon VPC) Anda. Layanan ini secara otomatis menskalakan volume lalu lintas jaringan untuk memberikan perlindungan ketersediaan tinggi tanpa perlu mengatur atau memelihara infrastruktur yang mendasarinya. Aturan pelanggan dan log akses mungkin berisi alamat IP pengguna akhir, yang dienkripsi baik saat istirahat maupun dalam perjalanan dalam arsitektur. AWS Selanjutnya, AWS Network Firewall mengenkripsi semua data saat istirahat dan dalam perjalanan antara AWS layanan komponen (Amazon S3, Amazon DynamoDB, Amazon Logs, CloudWatch Amazon EBS). Layanan ini secara otomatis mengenkripsi data tanpa memerlukan konfigurasi khusus.

Amazon Pinpoint

Amazon Pinpoint menawarkan pengembang satu lapisan API, dukungan CLI, dan dukungan SDK sisi klien untuk memperluas saluran komunikasi aplikasi dengan pengguna. Saluran yang memenuhi syarat meliputi: email, pesan teks SMS, pemberitahuan push seluler, dan saluran khusus. Amazon Pinpoint juga menyediakan sistem analitik yang melacak perilaku pengguna aplikasi dan keterlibatan pengguna. Dengan layanan ini, pengembang dapat mempelajari bagaimana setiap pengguna lebih suka terlibat dan dapat mempersonalisasi pengalaman pengguna untuk meningkatkan kepuasan pengguna.

Amazon Pinpoint juga membantu pengembang mengatasi beberapa kasus penggunaan pesan, seperti pesan langsung atau transaksional, pesan bertarget atau kampanye, dan pesan berbasis acara. Dengan mengintegrasikan dan mengaktifkan semua saluran keterlibatan pengguna akhir melalui Amazon Pinpoint, pengembang dapat membuat tampilan 360 derajat keterlibatan pengguna di semua titik sentuh pelanggan. Amazon Pinpoint menyimpan data pengguna, titik akhir,

dan peristiwa sehingga pelanggan dapat membuat segmen, mengirim pesan ke penerima, dan menangkap data keterlibatan.

Amazon Pinpoint mengenkripsi data baik saat istirahat maupun dalam perjalanan. Untuk informasi selengkapnya, lihat FAQ Amazon Pinpoint. Meskipun Amazon Pinpoint mengenkripsi semua data saat istirahat dan dalam perjalanan, saluran akhir, seperti SMS atau email, mungkin tidak dienkripsi, dan pelanggan harus mengonfigurasi saluran apa pun dengan cara yang sesuai dengan persyaratan mereka.

Selain itu, pelanggan yang perlu mengirim PHI melalui saluran SMS harus menggunakan kode pendek khusus (nomor telepon originasi 5-, 6 digit) untuk tujuan eksplisit pengiriman PHI. Untuk informasi selengkapnya tentang cara meminta kode singkat, lihat Meminta Kode Pendek Khusus untuk Pesan SMS dengan Amazon Pinpoint. Pelanggan juga dapat memilih untuk tidak mengirim PHI melalui saluran akhir dan sebagai gantinya menyediakan mekanisme untuk mengakses PHI dengan aman melalui HTTPS.

Panggilan API ke Amazon Pinpoint dapat ditangkap menggunakan. AWS CloudTrail Panggilan yang diambil termasuk panggilan dari konsol Amazon Pinpoint dan panggilan kode ke operasi Amazon Pinpoint API. Jika pelanggan membuat jejak, pelanggan dapat mengaktifkan pengiriman AWS CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Amazon Pinpoint. Jika pelanggan tidak mengonfigurasi jejak, mereka masih dapat melihat peristiwa terbaru dengan menggunakan riwayat Acara di AWS CloudTrail konsol. Dengan menggunakan informasi yang dikumpulkan oleh AWS CloudTrail, pelanggan dapat menentukan bahwa permintaan dibuat ke Amazon Pinpoint, alamat IP permintaan, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Mencatat Panggilan API Amazon Pinpoint dengan. AWS CloudTrail

Amazon Polly

Amazon Polly adalah layanan cloud yang mengubah teks menjadi ucapan yang hidup. Amazon Polly menyediakan operasi API sederhana yang dapat dengan mudah diintegrasikan oleh pelanggan dengan aplikasi yang ada. Amazon Polly menggunakan protokol HTTPS untuk berkomunikasi dengan klien. Akses ke Amazon Polly digerakkan oleh API, dan hak istimewa IAM yang paling tidak sesuai dapat ditegakkan. Untuk informasi selengkapnya, lihat Perlindungan Data. Beberapa contoh kasus penggunaan yang mencakup PHI:

- Pengasuh mengubah laporan teks yang berisi PHI menjadi pidato yang disintesis sehingga mereka dapat mendengarkan laporan sambil berjalan atau melakukan tugas lain.

- Pasien tunanetra diberikan bimbingan medis dan mengkonsumsi bimbingan dalam bentuk ucapan yang disintesis.

Saluran pengiriman akhir dari Amazon Polly dapat mengakibatkan pemutaran audio dengan PHI di ruang publik dan tindakan pencegahan harus diambil agar pengiriman mempertimbangkan hal ini. Output ucapan yang disintesis juga dapat dikirim secara asinkron ke bucket Amazon S3 dengan enkripsi diaktifkan.

Ketika aktivitas acara yang didukung terjadi di Amazon Polly, aktivitas tersebut direkam dalam suatu AWS CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam Riwayat Peristiwa. Untuk catatan peristiwa yang sedang berlangsung di AWS akun pelanggan, termasuk acara untuk Amazon Polly, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim file log ke bucket Amazon S3. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, pelanggan dapat menentukan permintaan yang dibuat ke Amazon Polly, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon QLDB adalah basis data buku besar terkelola penuh yang menyediakan log transaksi transparan, berubah-ubah, dan secara kriptografi terverifikasi yang dimiliki oleh otoritas tepercaya pusat. Amazon QLDB melacak setiap perubahan data aplikasi dan mempertahankan riwayat perubahan yang lengkap dan dapat diverifikasi dari waktu ke waktu. Data yang berisi PHI sekarang dapat disimpan dalam contoh QLDB. Secara default, semua data QLDB Amazon dalam perjalanan dan saat istirahat dienkripsi. Data dalam perjalanan dienkripsi menggunakan TLS dan data saat istirahat dienkripsi menggunakan kunci terkelola. AWS Untuk tujuan perlindungan data, kami menyarankan agar pelanggan melindungi kredensyal AWS akun dan mengatur akun pengguna individu dengan AWS Identity and Access Management (IAM), sehingga setiap pengguna hanya diberikan izin yang diperlukan untuk memenuhi tugas pekerjaan mereka. Untuk informasi selengkapnya, lihat Perlindungan Data di Amazon QLDB.

Amazon QLDB terintegrasi AWS CloudTrail dengan, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di QLDB. CloudTrail menangkap semua panggilan API bidang kontrol untuk QLDB sebagai peristiwa. Panggilan yang ditangkap termasuk panggilan dari konsol QLDB dan panggilan kode ke operasi QLDB API. Jika pelanggan membuat jejak, pelanggan dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon Simple Storage Service (Amazon S3), termasuk peristiwa untuk QLDB. Jika pelanggan tidak mengonfigurasi jejak, pelanggan masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam

riwayat Acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, pelanggan dapat menentukan permintaan yang dibuat ke QLDB, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Amazon QuickSight

Amazon QuickSight adalah layanan analisis bisnis yang dapat digunakan pelanggan untuk membangun visualisasi, melakukan analisis ad hoc, dan dengan cepat mendapatkan wawasan bisnis dari data mereka. Amazon QuickSight menemukan sumber AWS data, memungkinkan organisasi untuk menskalakan hingga ratusan ribu pengguna, dan memberikan kinerja responsif dengan menggunakan mesin dalam memori (SPICE) yang kuat.

Pelanggan hanya dapat menggunakan Amazon edisi Enterprise QuickSight untuk bekerja dengan data yang mengandung PHI karena menyediakan dukungan untuk enkripsi data yang disimpan saat istirahat di SPICE. Enkripsi data dilakukan dengan menggunakan kunci AWS terkelola.

Amazon RDS for MariaDB

Amazon RDS for MariaDB memungkinkan pelanggan mengenkripsi database MariaDB menggunakan kunci yang mereka kelola. AWS KMS Pada instance database yang berjalan dengan enkripsi Amazon RDS, data yang disimpan saat istirahat di penyimpanan dasar dienkripsi sesuai dengan Panduan yang berlaku pada saat publikasi whitepaper ini, seperti halnya backup otomatis, replika baca, dan snapshot.

Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon RDS for MariaDB memenuhi kepatuhan dan persyaratan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon RDS, lihat Mengenkripsi Sumber Daya Amazon RDS.

Koneksi ke RDS untuk MariaDB yang mengandung PHI harus menggunakan enkripsi transport. Untuk informasi selengkapnya tentang mengaktifkan koneksi terenkripsi, lihat Menggunakan SSL/TLS untuk Mengenkripsi Koneksi ke Instans DB.

Amazon RDS for MySQL

Amazon RDS for MySQL memungkinkan pelanggan mengenkripsi database MySQL menggunakan kunci yang dikelola pelanggan. AWS KMS Pada instance database yang berjalan dengan enkripsi Amazon RDS, data yang disimpan saat istirahat di penyimpanan dasar dienkripsi sesuai dengan

Panduan yang berlaku pada saat publikasi whitepaper ini, seperti halnya backup otomatis, replika baca, dan snapshot.

Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon RDS for MySQL memenuhi persyaratan kepatuhan dan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon RDS, lihat Mengenkripsi Sumber Daya Amazon RDS.

Koneksi ke RDS untuk MySQL yang berisi PHI harus menggunakan enkripsi transport. Untuk informasi selengkapnya tentang mengaktifkan koneksi terenkripsi, lihat Menggunakan SSL/TLS untuk Mengenkripsi Koneksi ke Instans DB.

Amazon RDS for Oracle

Pelanggan memiliki beberapa opsi untuk mengenkripsi PHI saat istirahat menggunakan Amazon RDS for Oracle. Pelanggan dapat mengenkripsi database Oracle menggunakan kunci yang mereka kelola. AWS KMS Pada instance database yang berjalan dengan enkripsi Amazon RDS, data yang disimpan saat istirahat di penyimpanan dasar dienkripsi sesuai dengan Panduan yang berlaku pada saat publikasi whitepaper ini, seperti halnya backup otomatis, replika baca, dan snapshot.

Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon RDS for Oracle memenuhi kepatuhan dan persyaratan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon RDS, lihat Mengenkripsi Sumber Daya Amazon RDS.

Pelanggan juga dapat menggunakan Oracle Transparent Data Encryption (TDE), dan mereka harus mengevaluasi konfigurasi untuk konsistensi dengan Guidance. Oracle TDE adalah fitur dari opsi Oracle Advanced Security yang tersedia di Oracle Enterprise Edition. Fitur ini secara otomatis mengenkripsi data sebelum ditulis ke penyimpanan dan secara otomatis mendekripsi data saat data dibaca dari penyimpanan. Pelanggan juga dapat menggunakan AWS CloudHSM untuk menyimpan kunci Amazon RDS Oracle TDE. Untuk informasi selengkapnya, lihat hal berikut:

- Amazon RDS for Oracle Enkripsi Data Transparan: Enkripsi Data Transparan Oracle.
- Menggunakan AWS CloudHSM untuk menyimpan kunci Amazon RDS Oracle TDE: Apa itu Amazon Relational Database Service (Amazon RDS)?

Koneksi ke Amazon RDS for Oracle yang berisi PHI harus menggunakan enkripsi transport dan mengevaluasi konfigurasi untuk konsistensi dengan Guidance. Ini dilakukan dengan menggunakan

Enkripsi Jaringan Asli Oracle dan diaktifkan di grup opsi Amazon RDS for Oracle. Untuk informasi lebih lanjut, lihat Enkripsi Jaringan Asli Oracle.

Amazon RDS for PostgreSQL

Amazon RDS for PostgreSQL memungkinkan pelanggan mengenkripsi database PostgreSQL menggunakan kunci yang dikelola pelanggan. AWS KMS Pada instance database yang berjalan dengan enkripsi Amazon RDS, data yang disimpan saat istirahat di penyimpanan dasar dienkripsi sesuai dengan Panduan yang berlaku pada saat publikasi whitepaper ini, seperti halnya backup otomatis, replika baca, dan snapshot.

Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon RDS for PostgreSQL memenuhi kepatuhan dan persyaratan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon RDS, lihat Mengenkripsi Sumber Daya Amazon RDS.

Koneksi ke RDS untuk PostgreSQL yang berisi PHI harus menggunakan enkripsi transport. Untuk informasi selengkapnya tentang mengaktifkan koneksi terenkripsi, lihat Menggunakan SSL/TLS untuk Mengenkripsi Koneksi ke Instans DB.

Amazon RDS for SQL Server

RDS untuk SQL Server mendukung penyimpanan PHI untuk kombinasi versi dan edisi berikut:

- 2008 R2 - Edisi Perusahaan saja
- 2012, 2014 dan 2016 - Edisi Web, Standar dan Perusahaan

Penting: edisi SQL Server Express tidak didukung dan tidak boleh digunakan untuk penyimpanan PHI.

Untuk menyimpan PHI, pelanggan harus memastikan bahwa instans dikonfigurasi untuk mengenkripsi data saat istirahat, dan mengaktifkan enkripsi dan audit transportasi, seperti yang dijelaskan di bawah ini.

Enkripsi saat Data Tidak Berpindah

Pelanggan dapat mengenkripsi database SQL Server menggunakan kunci yang mereka kelola. AWS KMS Pada instance database yang berjalan dengan enkripsi Amazon RDS, data yang disimpan

saat istirahat di penyimpanan dasar dienkripsi sesuai dengan Panduan yang berlaku pada saat publikasi whitepaper ini, seperti halnya pencadangan otomatis, dan snapshot. Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon RDS for SQL Server memenuhi kepatuhan dan persyaratan peraturan mereka. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon RDS, lihat Mengenkripsi Sumber Daya Amazon RDS.

Jika pelanggan menggunakan SQL Server Enterprise Edition, mereka dapat menggunakan Server Transparent Data Encryption (TDE) sebagai alternatif. Fitur ini secara otomatis mengenkripsi data sebelum ditulis ke penyimpanan dan secara otomatis mendekripsi data saat data dibaca dari penyimpanan. Untuk informasi selengkapnya tentang RDS for SQL Server Transparent Data Encryption, lihat Support for Transparent Data Encryption di SQL Server.

Enkripsi Transportasi

Koneksi ke Amazon RDS for SQL Server yang berisi PHI harus menggunakan enkripsi transport yang disediakan oleh SQL Server Forced SSL. SSL paksa diaktifkan dari dalam grup parameter untuk Amazon RDS SQL Server. Untuk informasi selengkapnya tentang RDS untuk SQL Server Forced SSL, lihat Menggunakan SSL dengan Instans Microsoft SQL Server DB.

Audit

RDS untuk instance SQL Server yang berisi PHI harus mengaktifkan audit. Audit diaktifkan dari dalam grup parameter untuk Amazon RDS SQL Server. Untuk informasi selengkapnya tentang audit RDS untuk SQL Server, lihat Dukungan Program Kepatuhan untuk Instans DB Microsoft SQL Server.

Amazon Redshift

Amazon Redshift menyediakan enkripsi database untuk klaster untuk membantu melindungi data saat istirahat. Saat pelanggan mengaktifkan enkripsi untuk klaster, Amazon Redshift mengenkripsi semua data, termasuk cadangan, dengan menggunakan kunci simetris Advanced Encryption Standard (AES) -256 yang dipercepat perangkat keras. Amazon Redshift menggunakan arsitektur berbasis kunci empat tingkat untuk enkripsi. Kunci ini terdiri dari kunci enkripsi data, kunci database, kunci cluster, dan kunci KMS.

Kunci klaster mengenkripsi kunci database untuk klaster Amazon Redshift. Pelanggan dapat menggunakan salah satu AWS KMS atau AWS CloudHSM (Modul Keamanan Perangkat Keras)

untuk mengelola kunci cluster. Enkripsi Amazon Redshift saat istirahat konsisten dengan Panduan yang berlaku pada saat publikasi whitepaper ini. Karena Panduan dapat diperbarui, pelanggan harus terus mengevaluasi dan menentukan apakah enkripsi Amazon Redshift memenuhi persyaratan kepatuhan dan peraturan mereka. Untuk informasi selengkapnya, lihat enkripsi basis data Amazon Redshift.

Koneksi ke Amazon Redshift yang berisi PHI harus menggunakan enkripsi transport dan pelanggan harus mengevaluasi konfigurasi untuk konsistensi dengan Panduan. Untuk informasi selengkapnya, lihat Mengonfigurasi opsi keamanan untuk koneksi. Amazon Redshift Spectrum memungkinkan pelanggan menjalankan kueri Amazon Redshift SQL terhadap exabyte data di Amazon S3. Redshift Spectrum adalah fitur Amazon Redshift, dan dengan demikian juga dalam cakupan HIPAA BAA.

Amazon Rekognition

Amazon Rekognition memudahkan untuk menambahkan analisis gambar dan video ke aplikasi pelanggan. Pelanggan hanya perlu menyediakan gambar atau video ke Amazon Rekognition API, dan layanan dapat mengidentifikasi objek, orang, teks, adegan, dan aktivitas, serta mendeteksi konten yang tidak pantas. Amazon Rekognition juga menyediakan analisis wajah dan pengenalan wajah yang sangat akurat.

Amazon Rekognition memenuhi syarat untuk beroperasi dengan gambar atau video yang berisi PHI. Amazon Rekognition beroperasi sebagai layanan terkelola dan tidak menyajikan opsi yang dapat dikonfigurasi untuk penanganan data. Amazon Rekognition hanya menggunakan, mengungkapkan, dan memelihara PHI sebagaimana diizinkan oleh ketentuan BAA. AWS Semua data dienkripsi saat istirahat dan dalam perjalanan dengan Amazon Rekognition. Amazon Rekognition AWS CloudTrail digunakan untuk mencatat semua panggilan API.

Amazon Route 53

Amazon Route 53 adalah layanan DNS terkelola yang memberi pelanggan kemampuan untuk mendaftarkan nama domain, merutekan sumber daya domain pelanggan lalu lintas internet, dan memeriksa kesehatan sumber daya tersebut. Meskipun Amazon Route 53 adalah Layanan yang Memenuhi Syarat HIPAA, tidak ada PHI yang harus disimpan dalam nama atau tag sumber daya apa pun dalam Amazon Route 53 karena tidak ada dukungan untuk mengenkripsi data tersebut. Sebagai gantinya, Amazon Route 53 dapat digunakan untuk menyediakan akses ke sumber daya domain pelanggan yang mengirimkan atau menyimpan PHI seperti server web yang berjalan di Amazon EC2 atau penyimpanan seperti Amazon S3.

Amazon S3 Glacier

Amazon S3 Glacier secara otomatis mengenkripsi data saat istirahat menggunakan kunci simetris AES 256-bit dan mendukung transfer data pelanggan yang aman melalui protokol aman. Koneksi ke Amazon S3 Glacier yang berisi PHI harus menggunakan titik akhir yang menerima transportasi terenkripsi (HTTPS). Untuk daftar titik akhir regional, lihat titik akhir AWS layanan.

Jangan gunakan PHI dalam nama arsip dan vault atau metadata karena data ini tidak dienkripsi menggunakan enkripsi sisi server Amazon S3 Glacier dan umumnya tidak dienkripsi dalam arsitektur enkripsi sisi klien.

Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration (S3TA) memungkinkan transfer file yang cepat, mudah, dan aman dalam jarak jauh antara klien pelanggan dan bucket S3. Transfer Acceleration memanfaatkan lokasi edge CloudFront Amazon yang didistribusikan secara global. Saat datanya tiba di lokasi edge, data diarahkan ke Amazon S3 melalui jalur jaringan yang dioptimalkan. Pelanggan harus memastikan bahwa data apa pun yang mengandung PHI yang ditransfer menggunakan AWS S3TA dienkripsi saat transit dan saat istirahat. Lihat Panduan untuk Amazon S3 untuk memahami opsi enkripsi yang tersedia.

Amazon SageMaker

Amazon SageMaker adalah layanan pembelajaran mesin yang dikelola sepenuhnya. Dengan Amazon SageMaker, ilmuwan dan pengembang data dapat dengan cepat dan mudah membangun dan melatih model pembelajaran mesin, dan kemudian langsung menerapkannya ke lingkungan host yang siap produksi. Ini menyediakan instance notebook penulisan Jupyter terintegrasi untuk akses mudah ke sumber data untuk eksplorasi dan analisis. Amazon SageMaker juga menyediakan algoritma pembelajaran mesin umum yang dioptimalkan untuk berjalan secara efisien terhadap data yang sangat besar dalam lingkungan terdistribusi.

Dengan dukungan bring-your-own-algorithms dan kerangka kerja asli, Amazon SageMaker menawarkan opsi pelatihan terdistribusi fleksibel yang menyesuaikan dengan alur kerja spesifik pelanggan. Amazon SageMaker memenuhi syarat untuk beroperasi dengan data yang berisi PHI. Enkripsi data dalam perjalanan disediakan oleh SSL/TLS dan digunakan saat berkomunikasi baik dengan antarmuka front-end Amazon (ke Notebook) dan setiap kali Amazon SageMaker berinteraksi dengan AWS layanan lain SageMaker (misalnya, menarik data dari Amazon S3).

Untuk memenuhi persyaratan bahwa PHI dienkripsi saat istirahat, enkripsi data yang disimpan dengan model yang menjalankan instance dengan Amazon SageMaker diaktifkan menggunakan AWS Key Management Service (KMS) saat menyiapkan titik akhir (: ID). DescribeEndpointConfig KmsKey Enkripsi hasil pelatihan model (artefak) diaktifkan menggunakan AWS KMS dan kunci harus ditentukan menggunakan KmsKey ID dalam OutputDataConfig deskripsi. Jika ID Kunci KMS tidak disediakan, Kunci Amazon S3 KMS default untuk akun peran akan digunakan. Amazon SageMaker menggunakan AWS CloudTrail untuk mencatat semua panggilan API.

Amazon Simple Notification Service (Amazon SNS)

Pelanggan harus memahami persyaratan enkripsi utama berikut untuk menggunakan Amazon Simple Notification Service (SNS) dengan Protected Health Information (PHI). Pelanggan harus menggunakan titik akhir HTTPS API yang disediakan SNS di setiap AWS Wilayah. Titik akhir HTTPS memanfaatkan koneksi terenkripsi, dan melindungi privasi dan integritas data yang dikirim. AWS Untuk daftar semua titik akhir HTTPS API, lihat titik akhir AWS layanan.

Selain itu, Amazon SNS menggunakan CloudTrail, layanan yang menangkap panggilan API yang dilakukan oleh atau atas nama Amazon SNS di AWS akun pelanggan dan mengirimkan file log ke bucket Amazon S3 yang mereka tentukan. CloudTrail menangkap panggilan API yang dilakukan dari konsol Amazon SNS atau dari Amazon SNS API. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, pelanggan dapat menentukan permintaan apa yang dibuat untuk Amazon SNS, alamat IP sumber dari mana permintaan itu dibuat, siapa yang membuat permintaan, dan kapan dibuat. Untuk informasi selengkapnya tentang pencatatan operasi SNS, lihat Mencatat panggilan API Amazon SNS menggunakan. CloudTrail

Amazon Simple Email Service (Amazon SES)

Amazon Simple Email Service (Amazon SES) adalah layanan pengiriman dan penerimaan email yang fleksibel dan sangat skalabel. Ini mendukung protokol S/MIME dan PGP untuk mengenkripsi pesan untuk end-to-end enkripsi penuh, dan semua komunikasi dengan Amazon SES diamankan menggunakan SSL (TLS 1.2). Pelanggan memiliki opsi untuk menyimpan pesan yang dienkripsi saat istirahat dengan mengonfigurasi Amazon SES untuk menerima dan mengenkripsi pesan sebelum menyimpannya di bucket Amazon S3. Untuk informasi selengkapnya, lihat Cara Amazon Simple Email Service (Amazon AWS KMS SES) digunakan untuk mengetahui informasi selengkapnya tentang mengenkripsi pesan untuk penyimpanan. Pesan diamankan saat transit ke Amazon SES baik melalui titik akhir HTTPS atau koneksi SMTP terenkripsi.

Untuk pesan yang dikirim dari Amazon SES ke penerima, Amazon SES pertama-tama akan mencoba membuat koneksi aman ke server email penerima, tetapi jika koneksi aman tidak dapat dibuat, itu akan mengirim pesan yang tidak terenkripsi. Untuk memerlukan enkripsi untuk pengiriman ke penerima, pelanggan harus membuat konfigurasi yang disetel di Amazon SES dan menggunakan AWS CLI untuk menyetel TlsPolicy properti ke Memerlukan. Untuk informasi selengkapnya, lihat Amazon SES dan Protokol Keamanan. Amazon SES terintegrasi dengan AWS CloudTrail untuk memantau semua panggilan API. Dengan menggunakan informasi yang dikumpulkan oleh AWS CloudTrail, pelanggan dapat menentukan bahwa permintaan dibuat ke Amazon SES, alamat IP permintaan, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Mencatat Panggilan API Amazon SES dengan AWS CloudTrail. Amazon SES juga menyediakan metode untuk memantau aktivitas pengiriman seperti mengirim, menolak, rasio pentalan, pengiriman, pembukaan, dan klik. Untuk informasi selengkapnya, lihat Memantau Aktivitas Pengiriman Amazon SES Anda.

Amazon Simple Queue Service (Amazon SQS)

Pelanggan harus memahami persyaratan enkripsi utama berikut untuk menggunakan Amazon SQS dengan PHI.

- Komunikasi dengan Antrian Amazon SQS melalui Permintaan Kueri harus dienkripsi dengan HTTPS. Untuk informasi selengkapnya tentang membuat permintaan SQS, lihat Membuat permintaan API Kueri.
- Amazon SQS mendukung enkripsi sisi server yang terintegrasi dengan AWS KMS untuk melindungi data saat istirahat. Penambahan enkripsi sisi server memungkinkan pelanggan untuk mengirimkan dan menerima data sensitif dengan peningkatan keamanan menggunakan antrian terenkripsi. Enkripsi sisi server Amazon SQS menggunakan Standar Enkripsi Lanjutan 256-bit (algoritma AES-256 GCM) untuk mengenkripsi isi setiap pesan. Integrasi dengan AWS KMS memungkinkan pelanggan untuk mengelola kunci secara terpusat yang melindungi pesan Amazon SQS bersama dengan kunci yang melindungi sumber daya mereka AWS yang lain. AWS KMS mencatat setiap penggunaan kunci enkripsi AWS CloudTrail untuk membantu memenuhi kebutuhan peraturan dan kepatuhan. Untuk informasi selengkapnya, dan untuk memeriksa ketersediaan SSE untuk Amazon SQS Wilayah, lihat Enkripsi saat Istirahat.
- Jika enkripsi sisi server tidak digunakan, muatan pesan itu sendiri harus dienkripsi sebelum dikirim ke SQS. Salah satu cara untuk mengenkripsi payload pesan adalah dengan menggunakan Amazon SQS Extended Client bersama dengan klien enkripsi Amazon S3. Untuk informasi selengkapnya tentang penggunaan enkripsi sisi klien, lihat Mengenkripsi Muatan Pesan Menggunakan Klien Diperpanjang Amazon SQS dan Klien Enkripsi Amazon S3.

Amazon SQS menggunakan CloudTrail, layanan yang mencatat panggilan API yang dilakukan oleh atau atas nama Amazon SQS di akun pelanggan AWS dan mengirimkan file log ke bucket Amazon S3 yang ditentukan. CloudTrail menangkap panggilan API yang dibuat dari konsol Amazon SQS atau dari Amazon SQS API. Pelanggan dapat menggunakan informasi yang dikumpulkan oleh CloudTrail untuk menentukan permintaan mana yang dibuat ke Amazon SQS, alamat IP sumber dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan sebagainya. Untuk informasi selengkapnya tentang pencatatan operasi SQS, lihat Mencatat panggilan Amazon SQS API menggunakan. AWS CloudTrail

Amazon Simple Storage Service (Amazon S3)

Pelanggan memiliki beberapa opsi untuk enkripsi data saat istirahat saat menggunakan Amazon S3, termasuk enkripsi sisi server dan sisi klien, dan beberapa metode pengelolaan kunci. Untuk informasi selengkapnya, lihat Melindungi data menggunakan enkripsi.

Koneksi ke Amazon S3 yang berisi PHI harus menggunakan titik akhir yang menerima transportasi terenkripsi (HTTPS). Untuk daftar titik akhir regional, lihat titik akhir AWS layanan.

Jangan gunakan PHI dalam nama bucket, nama objek, atau metadata karena data ini tidak dienkripsi menggunakan enkripsi sisi server S3 dan umumnya tidak dienkripsi dalam arsitektur enkripsi sisi klien.

Layanan Alur Kerja Sederhana Amazon

Amazon Simple Workflow Service (Amazon Simple Workflow Service) membantu developer membangun, menjalankan, dan menskalakan pekerjaan latar belakang yang memiliki langkah paralel atau berurutan. Amazon SWF dapat dianggap sebagai pelacak status dan koordinator tugas yang dikelola sepenuhnya di Cloud.

Amazon Simple Workflow Service digunakan untuk mengatur alur kerja dan tidak dapat menyimpan atau mengirimkan data. PHI tidak boleh ditempatkan dalam metadata untuk Amazon SWF atau dalam deskripsi tugas apa pun. Amazon SWF menggunakan AWS CloudTrail untuk mencatat semua panggilan API.

Amazon Textract

Amazon Textract menggunakan teknologi pembelajaran mesin untuk secara otomatis mengekstrak teks dan data dari dokumen yang dipindai yang melampaui pengenalan karakter optik sederhana

(OCR) untuk mengidentifikasi, memahami, dan mengekstrak data dari formulir dan tabel. Misalnya, pelanggan dapat menggunakan Amazon Ttract untuk secara otomatis mengekstrak data dan memproses formulir dengan informasi kesehatan yang dilindungi (PHI) tanpa campur tangan manusia untuk memenuhi klaim medis.

Amazon Textract juga dapat digunakan untuk menjaga kepatuhan dalam arsip dokumen. Misalnya, pelanggan dapat menggunakan Amazon Ttract untuk mengekstrak data dari klaim asuransi atau resep medis, dan secara otomatis mengenali pasangan nilai kunci dalam dokumen tersebut sehingga yang sensitif dapat disunting.

Amazon Textract mendukung enkripsi sisi server (SSE-S3 dan SSE-KMS) untuk masukan dokumen dan enkripsi TLS untuk data dalam perjalanan antara layanan dan agen. Pelanggan dapat menggunakan Amazon CloudWatch untuk melacak metrik penggunaan sumber daya dan AWS CloudTrail menangkap panggilan API ke Amazon Textract.

Amazon Transcribe

Amazon Transcribe menggunakan teknologi pembelajaran mesin canggih untuk mengenali ucapan dalam file audio dan menyalinnya ke dalam teks. Misalnya, pelanggan dapat menggunakan Amazon Transcribe untuk mengonversi audio bahasa Inggris AS dan Spanyol Meksiko menjadi teks dan untuk membuat aplikasi yang menggabungkan konten file audio. Amazon Transcribe dapat digunakan dengan data yang mengandung PHI. Amazon Transcribe tidak menyimpan atau menyimpan data apa pun dan semua panggilan ke API dienkripsi dengan SSL/TLS. Amazon Transcribe menggunakan CloudTrail untuk mencatat semua panggilan API.

Amazon Translate

Amazon Translate menggunakan teknologi pembelajaran mesin canggih untuk menyediakan terjemahan berkualitas tinggi sesuai permintaan. Pelanggan dapat menggunakan Amazon Translate untuk menerjemahkan dokumen teks yang tidak terstruktur atau untuk membangun aplikasi yang berfungsi dalam berbagai bahasa. Dokumen yang berisi PHI dapat diproses dengan Amazon Translate. Tidak diperlukan konfigurasi tambahan saat menerjemahkan dokumen yang berisi PHI. Enkripsi data saat transit disediakan oleh SSL/TLS dan tidak ada data yang tersisa dengan Amazon Translate. Amazon Translate menggunakan CloudTrail untuk mencatat semua panggilan API.

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) menawarkan serangkaian fitur keamanan jaringan yang selaras dengan arsitektur untuk beban kerja yang diatur HIPAA. Fitur seperti daftar kontrol akses jaringan stateless dan penugasan ulang instans dinamis ke dalam kelompok keamanan stateful memberikan fleksibilitas dalam melindungi instance dari akses jaringan yang tidak sah.

Amazon VPC juga memungkinkan pelanggan untuk memperluas ruang alamat jaringan mereka sendiri AWS, serta menyediakan sejumlah cara untuk menghubungkan pusat data mereka. AWS VPC Flow Logs menyediakan jejak audit koneksi yang diterima dan ditolak ke instans yang memproses, mentransmisikan, atau menyimpan PHI.

AWS Transit Gateway bertindak sebagai hub jaringan dan menyederhanakan konektivitas antara VPC Amazon serta jaringan lokal. AWS Transit Gateway juga menyediakan kemampuan mengintip antar wilayah ke Transit Gateway lainnya untuk membangun jaringan global menggunakan tulang punggung. AWS Untuk informasi selengkapnya tentang Amazon VPC, lihat Amazon Virtual Private Cloud.

Amazon WorkDocs

Amazon WorkDocs adalah layanan penyimpanan dan berbagi file perusahaan yang dikelola sepenuhnya dan aman dengan kontrol administratif yang kuat dan kemampuan umpan balik yang meningkatkan produktivitas pengguna. Amazon WorkDocs file dienkripsi saat istirahat menggunakan kunci yang dikelola pelanggan melalui AWS Key Management Service ().AWS KMS Semua data dalam perjalanan dienkripsi menggunakan SSL/TLS. AWS aplikasi web dan seluler, dan klien sinkronisasi desktop, mengirimkan file langsung ke Amazon WorkDocs menggunakan SSL/TLS.

Menggunakan Amazon WorkDocs Management Console, WorkDocs administrator dapat melihat log audit untuk melacak file dan aktivitas pengguna berdasarkan waktu, dan memilih apakah akan mengizinkan pengguna berbagi file dengan orang lain di luar organisasi mereka. Amazon WorkDocs juga terintegrasi dengan CloudTrail (layanan yang menangkap panggilan API yang dilakukan oleh atau atas nama Amazon WorkDocs di AWS akun pelanggan), dan mengirimkan file CloudTrail log ke bucket Amazon S3 yang ditentukan pelanggan.

Otentikasi multi-faktor (MFA) menggunakan server RADIUS tersedia dan dapat memberi pelanggan lapisan keamanan tambahan selama proses otentikasi. Pengguna masuk dengan memasukkan nama pengguna dan kata sandi mereka diikuti oleh OTP (One-Time Passcode) yang disediakan oleh perangkat keras atau token perangkat lunak.

Lihat informasi yang lebih lengkap di:

- Amazon WorkDocs fitur
- Pencatatan panggilan Amazon WorkDocs API menggunakan AWS CloudTrail

Pelanggan tidak boleh menyimpan PHI dalam nama file atau nama direktori.

Amazon WorkSpaces

Amazon WorkSpaces adalah solusi esktop-as-a D-Service (DaaS) yang dikelola sepenuhnya dan aman yang berjalan. AWS Dengan Amazon WorkSpaces, pelanggan dapat dengan mudah menyediakan desktop Microsoft Windows virtual berbasis cloud untuk penggunanya, memberi mereka akses ke dokumen, aplikasi, dan sumber daya yang mereka butuhkan, di mana saja, kapan saja, dari perangkat apa pun yang didukung.

Amazon WorkSpaces menyimpan data dalam volume Amazon Elastic Block Store. Pelanggan dapat mengenkripsi volume WorkSpaces penyimpanan pelanggan menggunakan kunci yang dikelola pelanggan. AWS Key Management Service Saat enkripsi diaktifkan pada a WorkSpace, baik data yang disimpan saat istirahat di penyimpanan yang mendasarinya dan pencadangan otomatis (EBS Snapshots) dari penyimpanan disk dienkripsi sesuai dengan Panduan. Komunikasi dari WorkSpace klien ke WorkSpace diamankan menggunakan SSL/TLS. Untuk informasi selengkapnya tentang enkripsi saat istirahat menggunakan Amazon WorkSpaces, lihat Terenkripsi WorkSpaces.

AWS App Mesh

AWS App Mesh adalah mesh layanan yang menyediakan jaringan tingkat aplikasi untuk memudahkan layanan Anda berkomunikasi satu sama lain di berbagai jenis infrastruktur komputasi, seperti Amazon ECS, Amazon EKS, atau layanan Amazon EC2. App Mesh mengonfigurasi proxy Envoy untuk mengumpulkan dan mengirimkan data observabilitas ke perangkat pemantauan yang Anda konfigurasikan, untuk memberi Anda visibilitas. end-to-end Ini dapat merutekan lalu lintas berdasarkan kebijakan perutean dan lalu lintas yang dikonfigurasi untuk memastikan ketersediaan aplikasi Anda yang tinggi. Lalu lintas antar aplikasi dapat dikonfigurasi untuk menggunakan TLS. App Mesh dapat digunakan menggunakan AWS SDK atau pengontrol App Mesh untuk Kubernetes. Meskipun AWS App Mesh merupakan Layanan yang Memenuhi Syarat HIPAA, tidak ada PHI yang harus disimpan dalam nama/atribut sumber daya apa pun di dalamnya AWS App Mesh karena tidak ada dukungan untuk melindungi data tersebut. Sebagai gantinya, AWS App Mesh dapat

digunakan untuk memantau, mengontrol, dan mengamankan sumber daya domain pelanggan yang mengirimkan atau menyimpan PHI.

AWS Layanan Migrasi Aplikasi

AWS Layanan Migrasi Aplikasi (AWS MGN) memungkinkan Anda untuk dengan cepat memigrasikan server dan aplikasi Anda ke AWS, tanpa perubahan dan dengan waktu henti minimal. AWS MGN adalah layanan migrasi utama yang direkomendasikan untuk migrasi lift dan shift ke. AWS

AWS MGN menggunakan replikasi data tingkat blok untuk menyalin disk sumber langsung ke volume EBS di akun pelanggan - data tidak pernah ditransmisikan melalui lingkungan cloud yang dikendalikan AWS MGN. Data yang direplikasi dienkripsi dalam perjalanan secara default. Data dalam volume EBS pelanggan dienkripsi secara default menggunakan kunci pelanggan sendiri.

AWS Auto Scaling

AWS Auto Scaling memungkinkan pelanggan mengonfigurasi penskalaan otomatis untuk AWS sumber daya yang merupakan bagian dari aplikasi pelanggan dalam hitungan menit. Pelanggan dapat menggunakan AWS Auto Scaling untuk sejumlah layanan yang melibatkan PHI, seperti Amazon DynamoDB, Amazon ECS, replika Amazon RDS Aurora, dan instans Amazon EC2 di Grup Auto Scaling.

AWS Auto Scaling adalah layanan orkestrasi yang tidak secara langsung memproses, menyimpan, atau mengirimkan konten pelanggan; untuk alasan itu, pelanggan dapat menggunakan layanan ini dengan konten terenkripsi. Model tanggung jawab AWS bersama berlaku untuk perlindungan data dalam AWS Auto Scaling: AWS bertanggung jawab atas prosedur keamanan AWS jaringan, sedangkan pelanggan bertanggung jawab untuk menjaga kontrol atas konten pelanggan yang di-host di infrastruktur ini. Konten ini mencakup konfigurasi keamanan dan tugas manajemen untuk AWS layanan yang digunakan pelanggan. Untuk tujuan perlindungan data, kami menyarankan agar pelanggan melindungi kredensyal AWS akun dan menyiapkan akun pengguna individu dengan AWS Identity and Access Management (IAM). Dengan cara ini, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka.

Kami sangat menyarankan agar pelanggan tidak pernah memasukkan informasi identifikasi sensitif, seperti nomor akun pelanggan, ke dalam bidang bentuk bebas seperti bidang Nama. Ini termasuk saat pelanggan bekerja dengan AWS Auto Scaling atau AWS layanan lain menggunakan AWS Management Console, API AWS CLI, atau AWS SDK.

Data apa pun yang dimasukkan pelanggan ke AWS Auto Scaling atau layanan lain mungkin diambil untuk dimasukkan dalam log diagnostik. Ketika pelanggan memberikan URL ke server eksternal, mereka tidak boleh menyertakan informasi kredensyal dalam URL untuk memvalidasi permintaan mereka ke server tersebut. AWS juga merekomendasikan agar pelanggan mengamankan data mereka dengan cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami merekomendasikan TLS 1.2 atau yang lebih baru
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default dalam AWS layanan.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data pribadi yang disimpan di Amazon S3.

AWS Backup

AWS Backup menawarkan layanan terpusat, dikelola sepenuhnya, dan berbasis kebijakan untuk melindungi data pelanggan dan memastikan kepatuhan di seluruh AWS layanan untuk tujuan kelangsungan bisnis. Dengan AWS Backup, pelanggan dapat mengonfigurasi kebijakan perlindungan data (pencadangan) secara terpusat dan memantau aktivitas pencadangan di seluruh AWS sumber daya pelanggan, termasuk volume Amazon EBS, database Amazon Relational Database Service (Amazon RDS) (termasuk cluster Aurora), tabel Amazon DynamoDB, Amazon Elastic File System (Amazon EFS), sistem file Amazon FSx, Amazon EC2 Contoh EC2, dan volume. AWS Storage Gateway

AWS Backup mengenkripsi data pelanggan dalam perjalanan dan saat istirahat. Cadangan dari layanan dengan kemampuan snapshot yang ada dienkripsi menggunakan metodologi enkripsi snapshot layanan sumber. Misalnya, snapshot EBS dienkripsi menggunakan kunci enkripsi volume tempat snapshot dibuat.

Pencadangan dari AWS layanan baru yang memperkenalkan fungsionalitas cadangan bawaan AWS Backup, seperti Amazon EFS, dienkripsi dalam perjalanan dan istirahat secara independen dari layanan sumber, memberikan cadangan pelanggan lapisan perlindungan tambahan. Enkripsi dikonfigurasi pada tingkat Backup Vault. Default Default dienkripsi. Saat pelanggan membuat brankas baru, Kunci Enkripsi harus dipilih.

AWS Batch

AWS Batch memungkinkan pengembang, ilmuwan, dan insinyur untuk dengan mudah dan efisien menjalankan ratusan ribu pekerjaan komputasi batch AWS. AWS Batch secara dinamis menyediakan kuantitas dan jenis sumber daya komputasi yang optimal (seperti CPU atau instance yang dioptimalkan memori) berdasarkan volume dan persyaratan sumber daya spesifik dari pekerjaan batch yang dikirimkan. AWS Batch merencanakan, menjadwalkan, dan mengeksekusi beban kerja komputasi batch di berbagai layanan dan fitur AWS komputasi.

Mirip dengan panduan untuk Amazon ECS, PHI tidak boleh ditempatkan langsung ke definisi pekerjaan, antrian pekerjaan atau tag untuk. AWS Batch Sebaliknya, pekerjaan yang dijadwalkan dan dilaksanakan dengan AWS Batch dapat beroperasi pada PHI terenkripsi. Setiap informasi yang dikembalikan oleh tahapan pekerjaan juga tidak AWS Batch boleh mengandung PHI apa pun. Setiap kali pekerjaan yang dijalankan oleh AWS Batch harus mengirimkan atau menerima PHI, koneksi itu harus dienkripsi menggunakan HTTPS atau SSL/TLS.

AWS Certificate Manager

AWS Certificate Manager adalah layanan yang memungkinkan pelanggan dengan mudah menyediakan, mengelola, dan menyebarkan sertifikat SSL/TLS publik dan pribadi untuk digunakan dengan AWS layanan dan sumber daya internal mereka yang terhubung. AWS Certificate Manager digunakan CloudTrail untuk mencatat semua panggilan API.

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses terprogram, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensyal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan.

Pengguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
		• Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat autentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.
IAM	Gunakan kredensyal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensyal sementara dengan AWS sumber daya di Panduan Pengguna IAM.

Pengguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
IAM	(Tidak direkomendasikan) Gunakan kredensyal jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensyal pengguna IAM di Panduan Pengguna.AWS Command Line Interface • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensyal jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

AWS Cloud Map

AWS Cloud Map adalah layanan penemuan sumber daya cloud. Dengan AWS Cloud Map, pelanggan dapat menentukan nama khusus untuk sumber daya aplikasi, seperti tugas Amazon ECS, instans Amazon EC2, bucket Amazon S3, tabel Amazon DynamoDB, antrian Amazon SQS, atau sumber daya cloud lainnya. Pelanggan kemudian dapat menggunakan nama kustom ini untuk menemukan lokasi dan metadata sumber daya cloud dari aplikasi mereka menggunakan AWS SDK dan kueri API yang diautentikasi. Meskipun AWS Cloud Map adalah Layanan yang Memenuhi Syarat HIPAA, tidak ada PHI yang harus disimpan dalam nama/atribut sumber daya apa pun dalam AWS Cloud Map karena tidak ada dukungan untuk melindungi data tersebut. Sebagai gantinya, AWS

Cloud Map dapat digunakan untuk menemukan sumber daya domain pelanggan yang mengirimkan atau menyimpan PHI.

AWS CloudFormation

AWS CloudFormation memungkinkan pelanggan untuk membuat dan menyediakan penerapan infrastruktur AWS secara dapat diprediksi dan berulang kali. Ini membantu pelanggan memanfaatkan produk AWS seperti Amazon EC2, Amazon Elastic Block Store, Amazon SNS, Elastic Load Balancing, dan Auto Scaling untuk membangun aplikasi yang sangat andal, sangat skalabel, dan hemat biaya di cloud tanpa khawatir tentang membuat dan mengonfigurasi infrastruktur AWS yang mendasarinya. AWS CloudFormation memungkinkan pelanggan untuk menggunakan file template untuk membuat dan menghapus kumpulan sumber daya bersama-sama sebagai satu unit (tumpukan).

AWS CloudFormation tidak dengan sendirinya menyimpan, mengirimkan, atau memproses PHI. Sebagai gantinya, ini digunakan untuk membangun dan menerapkan arsitektur yang menggunakan layanan AWS lain yang mungkin menyimpan, mengirimkan, dan/atau memproses PHI. Hanya Layanan yang Memenuhi Syarat HIPAA yang harus digunakan dengan PHI. Silakan merujuk ke entri untuk layanan tersebut di Whitepaper ini untuk panduan penggunaan PHI dengan layanan tersebut. AWS CloudFormation digunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS CloudHSM

AWS CloudHSM adalah modul keamanan perangkat keras berbasis cloud (HSM) yang memungkinkan pelanggan untuk dengan mudah membuat dan menggunakan kunci enkripsi mereka sendiri di AWS Cloud. Dengan CloudHSM, pelanggan dapat mengelola kunci enkripsi mereka sendiri menggunakan HSM yang divalidasi FIPS 140-2 Level 3. CloudHSM menawarkan pelanggan fleksibilitas untuk berintegrasi dengan aplikasi mereka menggunakan API standar terbuka, seperti PKCS #11, Java Cryptography Extensions (JCE), dan Microsoft Cryptong (CNG) library.

CloudHSM juga memenuhi standar dan memungkinkan pelanggan untuk mengekspor semua kunci mereka ke sebagian besar HSM lain yang tersedia secara komersial. Seperti AWS CloudHSM layanan manajemen kunci alat perangkat keras, ia tidak dapat menyimpan atau mengirimkan PHI. Pelanggan tidak boleh menyimpan PHI di Tag (metadata). Tidak diperlukan panduan khusus lainnya.

AWS CloudTrail

AWS CloudTrail adalah layanan yang memungkinkan tata kelola, kepatuhan, audit operasional, dan audit risiko akun AWS. Dengan CloudTrail, pelanggan dapat mencatat, terus memantau, dan mempertahankan aktivitas akun yang terkait dengan tindakan di seluruh infrastruktur AWS mereka. CloudTrail menyediakan riwayat peristiwa aktivitas akun AWS mereka, termasuk tindakan yang dilakukan melalui AWS SDK, alat baris perintah, dan layanan AWS lainnya. AWS Management Console Riwayat peristiwa ini menyederhanakan analisis keamanan, pelacakan perubahan sumber daya, dan pemecahan masalah.

AWS CloudTrail diaktifkan untuk digunakan dengan semua akun AWS dan dapat digunakan untuk pencatatan audit, seperti yang dipersyaratkan oleh AWS BAA. Jalur Khusus harus dibuat menggunakan CloudTrail konsol atau AWS Command Line Interface. CloudTrail mengenkripsi semua lalu lintas saat transit dan istirahat saat Trail terenkripsi dibuat. Jejak terenkripsi harus dibuat ketika ada potensi untuk mencatat PHI.

Secara default, Trail terenkripsi menyimpan entri di Amazon S3 menggunakan Enkripsi Sisi Server dengan kunci terkelola Amazon S3 (SSE-S3). Jika manajemen tambahan atas kunci diinginkan, itu juga dapat dikonfigurasi dengan kunci AWS KMS-managed (SSE-KMS). Seperti CloudTrail tujuan akhir untuk entri log AWS, dan dengan demikian, komponen penting dari arsitektur apa pun yang menangani PHI, validasi integritas file CloudTrail log harus diaktifkan dan file CloudTrail intisari terkait harus ditinjau secara berkala. Setelah diaktifkan, pernyataan positif bahwa file log belum diubah atau diubah dapat dibuat.

AWS CodeBuild

AWS CodeBuild adalah layanan build yang dikelola sepenuhnya di cloud. AWS CodeBuild mengkompilasi kode sumber, menjalankan pengujian unit, dan menghasilkan artefak yang siap digunakan. AWS CodeBuild menggunakan AWS KMS kunci untuk mengenkripsi artefak keluaran build. Kunci KMS harus dibuat dan dikonfigurasi sebelum membuat artefak yang berisi PHI, rahasia/ kata sandi, sertifikat, dll. AWS CodeBuild Digunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS CodeDeploy

AWS CodeDeploy adalah layanan penyebaran terkelola penuh yang mengotomatiskan penerapan perangkat lunak ke berbagai layanan komputasi termasuk Amazon EC2,,, dan server lokal. AWS

Fargate AWS Lambda Pelanggan menggunakannya AWS CodeDeploy untuk dengan cepat merilis fitur baru dari beban kerja kontainer dan menangani kompleksitas memperbarui aplikasi.

AWS CodeDeploy mendukung enkripsi sisi server (SSE-S3) untuk artefak penyebaran dan enkripsi TLS untuk data dalam perjalanan antara layanan dan agen. Pelanggan dapat menggunakan Amazon CloudWatch Events untuk melacak penerapan dan AWS CloudTrail untuk menangkap panggilan API. AWS CodeDeploy

AWS CodeCommit

AWS CodeCommit adalah layanan kontrol sumber terkelola yang aman, sangat skalabel, dan terkelola yang menampung repositori Git pribadi. AWS CodeCommit menghilangkan kebutuhan pelanggan untuk mengelola sistem kontrol sumber mereka sendiri atau khawatir tentang penskalaan infrastrukturnya.

AWS CodeCommit mengenkripsi semua lalu lintas dan informasi yang disimpan saat transit dan istirahat. Secara default, ketika repositori dibuat di dalam AWS CodeCommit, kunci yang dikelola AWS dibuat dengan AWS KMS dan hanya digunakan oleh repositori itu untuk mengenkripsi semua data yang disimpan saat istirahat. AWS CodeCommit digunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS CodePipeline

AWS CodePipeline adalah layanan pengiriman berkelanjutan yang dikelola sepenuhnya yang membantu pelanggan mengotomatiskan saluran rilis pelanggan untuk pembaruan aplikasi dan infrastruktur yang cepat dan andal. Pelanggan gunakan AWS CodePipeline untuk memungkinkan peneliti memproses data uji klinis secara otomatis, hasil lab, dan data genom adalah beberapa contoh alur kerja yang digunakan oleh pelanggan.

AWS CodePipeline mendukung enkripsi sisi server (SSE-S3 dan SSE-KMS) untuk artefak Kode dan enkripsi TLS untuk data dalam perjalanan antara layanan dan agen. Pelanggan dapat menggunakan Amazon CloudWatch Events untuk melacak perubahan pipeline dan AWS CloudTrail untuk menangkap panggilan API AWS CodePipeline.

AWS Config

AWS Config memberikan tampilan terperinci tentang sumber daya yang terkait dengan akun AWS pelanggan, termasuk bagaimana mereka dikonfigurasi, bagaimana mereka terkait satu sama lain, dan bagaimana konfigurasi dan hubungan mereka telah berubah dari waktu ke waktu.

AWS Config sendiri tidak dapat digunakan untuk menyimpan atau mengirimkan PHI.

Sebaliknya, ini dapat dimanfaatkan untuk memantau dan mengevaluasi arsitektur yang dibangun dengan layanan AWS lainnya, termasuk arsitektur yang menangani PHI, untuk membantu menentukan apakah mereka tetap sesuai dengan tujuan desain yang dimaksudkan. Arsitektur yang menangani PHI hanya boleh dibangun dengan Layanan yang Memenuhi Syarat HIPAA. AWS Config digunakan AWS CloudTrail untuk mencatat semua hasil.

AWS Data Exchange

AWS Data Exchange memudahkan Anda menemukan, berlangganan, dan menggunakan data pihak ketiga di cloud. Setelah berlangganan produk data, pelanggan dapat menggunakan AWS Data Exchange API untuk memuat data langsung ke Amazon S3 dan kemudian menganalisisnya dengan berbagai macam analitik AWS dan layanan pembelajaran mesin. Untuk penyedia data, AWS Data Exchange memudahkan untuk menjangkau jutaan pelanggan AWS yang bermigrasi ke cloud dengan menghilangkan kebutuhan untuk membangun dan memelihara infrastruktur untuk penyimpanan data, pengiriman, penagihan, dan pemberian hak.

AWS Data Exchange selalu mengenkripsi semua produk data yang disimpan dalam layanan saat istirahat tanpa memerlukan konfigurasi tambahan apa pun. Enkripsi ini secara otomatis dilakukan melalui kunci KMS yang dikelola layanan. AWS Data Exchange menggunakan Transport Layer Security (TLS) dan enkripsi sisi klien untuk enkripsi saat transit. Komunikasi dengan AWS Data Exchange selalu dilakukan melalui HTTPS sehingga data pelanggan selalu dienkripsi saat transit. Enkripsi ini dikonfigurasi secara default saat pelanggan menggunakan AWS Data Exchange. Untuk informasi selengkapnya, lihat Perlindungan Data di AWS Data Exchange.

AWS Data Exchange terintegrasi dengan AWS CloudTrail. AWS CloudTrail menangkap semua panggilan ke AWS Data Exchange API sebagai peristiwa, termasuk panggilan dari konsol AWS Data Exchange dan dari panggilan kode ke operasi AWS Data Exchange API. Beberapa tindakan yang dapat dilakukan pelanggan adalah tindakan khusus konsol. Tidak ada API yang sesuai di AWS SDK atau AWS CLI. Ini adalah tindakan yang mengandalkan AWS Marketplace fungsionalitas, seperti

menerbitkan atau berlangganan produk. AWS Data Exchange menyediakan CloudTrail log untuk subset tindakan khusus konsol ini. Untuk informasi selengkapnya, lihat Mencatat Panggilan API AWS Data Exchange dengan AWS CloudTrail.

Harap dicatat bahwa semua cantuman yang menggunakan AWS Data Exchange harus mematuhi Panduan Penerbitan AWS Data Exchange dan FAQ AWS Data Exchange untuk AWS Marketplace Penyedia, yang membatasi kategori data tertentu. Untuk informasi selengkapnya, lihat FAQ AWS Data Exchange.

AWS Database Migration Service

AWS Database Migration Service (AWS DMS) membantu pelanggan memigrasikan database ke AWS dengan mudah dan aman. Pelanggan dapat memigrasikan data mereka ke dan dari basis data komersial dan open-source yang paling banyak digunakan, seperti Oracle, MySQL, dan PostgreSQL. Layanan ini mendukung migrasi homogen seperti Oracle ke Oracle, dan juga migrasi heterogen antara platform database yang berbeda, seperti Oracle ke PostgreSQL atau MySQL ke Oracle.

Database yang berjalan di tempat dan dimigrasikan ke cloud dengan AWS DMS dapat berisi data PHI. AWS DMS mengenkripsi data saat transit dan saat data dipentaskan untuk migrasi akhir ke database target di AWS. AWS DMS mengenkripsi penyimpanan yang digunakan oleh instance replikasi dan informasi koneksi titik akhir. Untuk mengenkripsi penyimpanan yang digunakan oleh instance replikasi, AWS DMS menggunakan AWS KMS kunci yang unik untuk akun AWS. Lihat Panduan untuk database target yang sesuai untuk memastikan bahwa data tetap terenkripsi setelah migrasi selesai. AWS DMS digunakan CloudTrail untuk mencatat semua panggilan API.

AWS DataSync

AWS DataSync adalah layanan transfer online yang menyederhanakan, mengotomatiskan, dan mempercepat pemindahan data antara penyimpanan lokal dan AWS. Pelanggan dapat menggunakan AWS DataSync untuk menghubungkan sumber data mereka ke Amazon S3 atau Amazon EFS. Pelanggan harus memastikan bahwa Amazon S3 dan Amazon EFS dikonfigurasi dengan cara yang konsisten dengan Panduan. Secara default, data pelanggan dienkripsi dalam perjalanan menggunakan TLS 1.2. Untuk informasi selengkapnya tentang enkripsi dan AWS DataSync, lihat DataSyncfitur AWS. Pelanggan dapat memantau DataSync aktivitas menggunakan AWS CloudTrail. Untuk informasi selengkapnya tentang login dengan CloudTrail, lihat Logging AWS DataSync API Calls with AWS CloudTrail.

AWS Directory Service

AWS Directory Service untuk Microsoft AD

AWS Directory Service untuk Microsoft Active Directory (Enterprise Edition), juga dikenal sebagai AWS Microsoft AD, memungkinkan beban kerja sadar direktori dan sumber daya AWS untuk menggunakan Active Directory yang dikelola di AWS Cloud. AWS Microsoft AD menyimpan konten direktori (termasuk konten yang berisi PHI) dalam volume Amazon Elastic Block Store terenkripsi menggunakan kunci enkripsi yang dikelola AWS. Untuk informasi lebih lanjut, lihat Enkripsi Amazon EBS.

Data dalam perjalanan ke dan dari klien Active Directory dienkripsi saat melakukan perjalanan melalui Lightweight Directory Access Protocol (LDAP) melalui jaringan Amazon Virtual Private Cloud (VPC) pelanggan. Jika klien Active Directory berada di jaringan lokal, lalu lintas akan berpindah ke VPC pelanggan melalui tautan jaringan pribadi virtual atau tautan. AWS Direct Connect

Direktori Cloud Amazon

Amazon Cloud Directory memungkinkan pelanggan membangun direktori cloud-native yang fleksibel untuk mengatur hierarki data di berbagai dimensi. Pelanggan juga dapat membuat direktori untuk berbagai kasus penggunaan, seperti bagan organisasi, katalog kursus, dan pendaftar perangkat. Misalnya, pelanggan dapat membuat bagan organisasi yang dapat dinavigasi melalui hierarki terpisah untuk struktur pelaporan, lokasi, dan pusat biaya. Amazon Cloud Directory secara otomatis mengenkripsi data saat istirahat dan dalam perjalanan dengan menggunakan kunci enkripsi 256-bit yang dikelola oleh (). AWS Key Management Service AWS KMS

AWS Elastic Beanstalk

Dengan AWS Elastic Beanstalk, pelanggan dapat dengan cepat menyebarkan dan mengelola aplikasi di AWS Cloud tanpa harus mempelajari infrastruktur yang menjalankan aplikasi tersebut. Pelanggan cukup mengunggah kode dan AWS Elastic Beanstalk secara otomatis menangani penyebaran, mulai dari penyediaan kapasitas, penyeimbangan beban, penskalaan otomatis hingga pemantauan kesehatan aplikasi. Pada saat yang sama, pelanggan mempertahankan kendali penuh atas sumber daya AWS yang mendukung aplikasi mereka dan dapat mengakses sumber daya yang mendasarinya kapan saja.

AWS Elastic Beanstalk tidak dengan sendirinya menyimpan, mengirimkan, atau memproses PHI. Sebagai gantinya, pelanggan dapat menggunakannya untuk membangun dan menerapkan arsitektur

dengan layanan AWS lain yang mungkin menyimpan, mengirimkan, dan/atau memproses PHI. Pelanggan harus memastikan bahwa ketika memilih layanan yang digunakan oleh AWS Elastic Beanstalk untuk hanya menggunakan Layanan yang Memenuhi Syarat HIPAA dengan PHI. Lihat entri untuk layanan tersebut di whitepaper ini untuk panduan penggunaan PHI dengan layanan tersebut.

Pelanggan tidak boleh menyertakan PHI dalam bidang bentuk bebas apa pun AWS Elastic Beanstalk seperti bidang Nama. AWS Elastic Beanstalk digunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery (AWS DRS) meminimalkan waktu henti dan kehilangan data dengan pemulihan aplikasi berbasis cloud dan lokal yang cepat dan andal menggunakan penyimpanan yang terjangkau, komputasi minimal, dan pemulihan. point-in-time

Pelanggan dapat menyiapkan AWS Elastic Disaster Recovery di server sumber mereka untuk memulai replikasi data yang aman. Data mereka direplikasi ke subnet area pementasan di akun AWS Anda, di Wilayah AWS yang mereka pilih. Desain area pementasan mengurangi biaya dengan menggunakan penyimpanan yang terjangkau dan sumber daya komputasi minimal untuk mempertahankan replikasi yang berkelanjutan. Data pelanggan yang direplikasi oleh AWS Elastic Disaster Recovery dienkripsi dalam perjalanan menggunakan TLS 1.2, dan ditransfer langsung dari server sumber mereka ke VPC mereka. Pelanggan dapat memanfaatkan konektivitas pribadi seperti AWS Direct Connect atau VPN untuk mengonfigurasi rute replikasi. Data pelanggan juga dapat dienkripsi saat istirahat di AWS menggunakan enkripsi Amazon EBS.

Pelanggan dapat melakukan tes non-disruptif untuk mengonfirmasi bahwa implementasi telah selesai. Selama operasi normal, pertahankan kesiapan dengan memantau replikasi dan secara berkala melakukan latihan pemulihan dan kegagalan yang tidak mengganggu. Jika pelanggan perlu memulihkan aplikasi, mereka dapat meluncurkan instans pemulihan di AWS dalam beberapa menit, menggunakan status up-to-date server terbanyak atau titik waktu sebelumnya. Setelah aplikasi pelanggan berjalan di AWS, mereka dapat memilih untuk menyimpannya di sana, atau mereka dapat memulai replikasi data kembali ke situs utama mereka saat masalah teratasi. Pelanggan dapat gagal kembali ke situs utama mereka kapan pun mereka siap.

AWS Fargate

AWS Fargate adalah teknologi yang memungkinkan pelanggan untuk menjalankan kontainer tanpa harus mengelola server atau cluster. Dengan AWS Fargate, pelanggan tidak lagi harus menyediakan, mengkonfigurasi, dan menskalakan cluster mesin virtual untuk menjalankan kontainer. Ini menghilangkan kebutuhan untuk memilih jenis server, memutuskan kapan harus menskalakan cluster, atau mengoptimalkan pengemasan cluster. AWS Fargate menghilangkan kebutuhan pelanggan untuk berinteraksi dengan atau berpikir tentang server atau cluster. Dengan Fargate, pelanggan fokus pada merancang dan membangun aplikasi mereka daripada mengelola infrastruktur yang menjalankannya.

Fargate tidak memerlukan konfigurasi tambahan untuk bekerja dengan beban kerja yang memproses PHI. Pelanggan dapat menjalankan beban kerja kontainer di Fargate menggunakan layanan orkestrasi kontainer seperti Amazon ECS. Fargate hanya mengelola infrastruktur yang mendasarinya dan tidak beroperasi dengan atau pada data dalam beban kerja yang diatur. Sesuai dengan persyaratan untuk HIPAA, PHI harus tetap dienkripsi setiap kali dalam perjalanan atau saat istirahat ketika diakses oleh kontainer yang diluncurkan dengan Fargate. Berbagai mekanisme untuk mengenkripsi saat istirahat tersedia dengan setiap opsi penyimpanan AWS yang dijelaskan dalam paper ini. Untuk informasi keamanan dan konfigurasi HIPAA tambahan, lihat whitepaper Architecting for HIPAA Security and Compliance on Amazon EKS.

AWS Firewall Manager

AWS Firewall Manager adalah layanan manajemen keamanan yang memungkinkan pelanggan untuk secara terpusat mengkonfigurasi dan mengelola aturan firewall di seluruh akun pelanggan dan aplikasi di AWS Organizations. Ketika aplikasi baru dibuat, Firewall Manager memudahkan untuk membawa aplikasi dan sumber daya baru ke dalam kepatuhan dengan menegakkan seperangkat aturan keamanan umum. Sekarang pelanggan memiliki satu layanan untuk membangun aturan firewall, membuat kebijakan keamanan, dan menegakkannya secara konsisten, hierarkis di seluruh infrastruktur mereka, dari akun administrator pusat.

AWS Firewall Manager adalah layanan orkestrasi yang tidak secara langsung memproses, menyimpan, atau mengirimkan data pengguna. Layanan tidak mengenkripsi konten pelanggan, tetapi layanan dasar yang AWS Firewall Manager menggunakan, seperti DynamoDB, mengenkripsi data pengguna.

AWS Global Accelerator

AWS Global Accelerator adalah layanan penyeimbangan beban global yang meningkatkan ketersediaan dan latensi aplikasi multi-wilayah. Untuk memastikan bahwa PHI tetap terenkripsi dalam perjalanan dan saat istirahat saat menggunakan AWS Global Accelerator, arsitektur yang diseimbangkan beban oleh Global Accelerator harus menggunakan protokol terenkripsi, seperti HTTPS atau SSL/TLS. Lihat panduan untuk Amazon EC2, Elastic Load Balancing, dan layanan AWS lainnya untuk lebih memahami opsi enkripsi yang tersedia untuk sumber daya backend. AWS Global Accelerator digunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS Glue

AWS Glue adalah layanan ETL (ekstrak, transformasi, dan muat) yang dikelola sepenuhnya yang membuatnya sederhana dan hemat biaya bagi pelanggan untuk mengkategorikan data mereka, membersihkannya, memperkayanya, dan memindahkannya dengan andal di antara berbagai penyimpanan data. Untuk memastikan enkripsi data yang mengandung PHI saat transit, AWS Glue harus dikonfigurasi untuk menggunakan koneksi JDBC ke penyimpanan data dengan SSL/TLS. Selain itu, untuk mempertahankan enkripsi saat dalam perjalanan, pengaturan untuk enkripsi sisi server (SSE-S3) harus diteruskan sebagai parameter ke pekerjaan ETL yang dijalankan. AWS Glue Semua data yang disimpan saat istirahat dalam Katalog Data AWS Glue dienkripsi menggunakan kunci yang dikelola oleh AWS KMS saat enkripsi diaktifkan saat pembuatan objek Katalog Data. AWS Glue digunakan CloudTrail untuk mencatat semua panggilan API.

AWS Glue DataBrew

AWS Glue DataBrew adalah layanan persiapan data visual yang dikelola sepenuhnya yang memudahkan analis data dan ilmuwan data untuk membersihkan dan menormalkan data guna mempersiapkannya untuk analitik dan pembelajaran mesin. Untuk memastikan enkripsi data yang mengandung PHI saat transit, DataBrew harus dikonfigurasi untuk menggunakan koneksi JDBC ke penyimpanan data dengan SSL/TLS. Saat menyambungkan ke sumber data JDBC, DataBrew gunakan pengaturan pada koneksi AWS Glue Anda, termasuk opsi “Memerlukan koneksi SSL”. Selain itu, untuk mempertahankan enkripsi saat diam di bucket S3, pengaturan untuk enkripsi sisi server (SSE-S3 atau SSE-KMS) harus diteruskan sebagai parameter ke pekerjaan. DataBrew

AWS IoT Inti dan AWS IoT Device Management

AWS IoT Inti dan AWS IoT Device Management menyediakan komunikasi dua arah yang aman antara perangkat yang terhubung ke internet, seperti sensor, aktuator, pengontrol mikro tertanam, atau peralatan pintar, dan AWS Cloud. AWS IoT Core dan sekarang AWS IoT Device Management dapat mengakomodasi perangkat yang mengirimkan data yang mengandung PHI. Semua komunikasi dengan AWS IoT Core dan AWS IoT Device Management dienkripsi menggunakan TLS. AWS IoT Inti dan AWS IoT Device Management gunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS IoT Greengrass

AWS IoT Greengrass memungkinkan pelanggan menjalankan komputasi lokal, perpesanan, caching data, sinkronisasi, dan kemampuan inferensi ML untuk perangkat yang terhubung dengan cara yang aman. AWS IoT Greengrass menggunakan sertifikat X.509, langganan terkelola, AWS IoT kebijakan, dan kebijakan dan peran IAM untuk memastikan bahwa aplikasi Greengrass pelanggan aman. AWS IoT Greengrass menggunakan model keamanan AWS IoT transportasi untuk mengenkripsi komunikasi dengan cloud menggunakan TLS. Selain itu, AWS IoT Greengrass data dienkripsi saat istirahat (di cloud). Untuk informasi lebih lanjut tentang keamanan Greengrass, lihat Ikhtisar Keamanan. AWS IoT Greengrass

Pelanggan dapat mencatat tindakan AWS IoT Greengrass API menggunakan AWS CloudTrail. Untuk informasi selengkapnya, lihat Mencatat Panggilan AWS IoT Greengrass API dengan AWS CloudTrail.

AWS Lambda

AWS Lambda memungkinkan pelanggan menjalankan kode tanpa menyediakan atau mengelola server sendiri. AWS Lambda menggunakan armada komputasi instans Amazon Elastic Compute Cloud (Amazon EC2) di beberapa Availability Zone di suatu Wilayah, yang menyediakan ketersediaan, keamanan, kinerja, dan skalabilitas infrastruktur AWS yang tinggi.

Untuk memastikan bahwa PHI tetap terenkripsi saat menggunakan AWS Lambda, koneksi ke sumber daya eksternal harus menggunakan protokol terenkripsi seperti HTTPS atau SSL/TLS. Misalnya, ketika S3 diakses dari prosedur Lambda, itu harus ditangani dengan https://bucket.s3-aws-region.amazonaws.com.

Jika ada PHI yang ditempatkan saat istirahat atau idled dalam prosedur yang sedang berjalan, itu harus dienkripsi sisi klien atau sisi server dengan kunci yang diperoleh dari atau. AWS KMS AWS

CloudHSM Ikuti panduan terkait untuk Amazon API Gateway saat memicu AWS Lambda fungsi melalui layanan. Saat menggunakan peristiwa dari layanan AWS lain untuk memicu AWS Lambda fungsi, data peristiwa tidak boleh berisi (dalam dan dari dirinya sendiri) PHI. Misalnya, ketika prosedur Lambda dipicu dari peristiwa S3, seperti kedatangan objek di S3, nama objek yang diteruskan ke Lambda seharusnya tidak memiliki PHI, meskipun objek itu sendiri dapat berisi data tersebut.

AWS Managed Services

AWS Managed Services menyediakan pengelolaan infrastruktur AWS yang berkelanjutan. Dengan menerapkan praktik terbaik untuk memelihara infrastruktur pelanggan, AWS Managed Services membantu mengurangi overhead dan risiko operasional mereka. AWS Managed Services mengotomatiskan aktivitas umum seperti permintaan perubahan, pemantauan, manajemen patch, keamanan, dan layanan pencadangan, dan menyediakan layanan siklus hidup penuh untuk menyediakan, menjalankan, dan mendukung infrastruktur.

Pelanggan dapat menggunakannya AWS Managed Services untuk mengelola beban kerja AWS yang beroperasi dengan data yang berisi PHI. Penggunaan AWS Managed Services tidak mengubah Layanan AWS yang memenuhi syarat untuk digunakan dengan PHI. Perkakas dan otomatisasi yang disediakan oleh AWS Managed Services tidak dapat digunakan untuk penyimpanan atau transmisi PHI.

AWS OpsWorks untuk Chef Automate

AWS OpsWorks untuk Chef Automate adalah layanan manajemen konfigurasi yang dikelola sepenuhnya yang menampung Chef Automate, seperangkat alat otomatisasi dari Chef untuk infrastruktur dan manajemen aplikasi. Layanan itu sendiri tidak berisi, mengirimkan, atau menangani PHI atau informasi sensitif apa pun, tetapi pelanggan harus memastikan bahwa sumber daya apa pun yang dikonfigurasi oleh OpsWorks for Chef Automate dikonfigurasi sesuai dengan Panduan. Panggilan API ditangkap dengan AWS CloudTrail. Untuk informasi selengkapnya, lihat Mencatat Panggilan API AWS OpsWorks Tumpukan dengan AWS CloudTrail.

AWS OpsWorks untuk Puppet Enterprise

AWS OpsWorks for Puppet Enterprise adalah layanan manajemen konfigurasi yang dikelola sepenuhnya yang menjadi tuan rumah Puppet Enterprise, seperangkat alat otomatisasi dari Puppet untuk infrastruktur dan manajemen aplikasi. Layanan itu sendiri tidak berisi, mengirimkan, atau

menangani PHI atau informasi sensitif apa pun, tetapi pelanggan harus memastikan bahwa sumber daya apa pun yang dikonfigurasi oleh OpsWorks Perusahaan Boneka dikonfigurasi sesuai dengan Panduan. Panggilan API ditangkap dengan AWS CloudTrail. Untuk informasi selengkapnya, lihat Mencatat Panggilan API AWS OpsWorks Tumpukan dengan AWS CloudTrail.

AWS OpsWorks Tumpukan

AWS OpsWorks Stacks menyediakan cara sederhana dan fleksibel untuk membuat dan mengelola tumpukan dan aplikasi. Pelanggan dapat menggunakan AWS OpsWorks Stacks untuk menyebarkan dan memantau aplikasi di tumpukan mereka.

AWS OpsWorks Stacks mengenkripsi semua lalu lintas saat dalam perjalanan. Namun, kantong data terenkripsi (mekanisme penyimpanan data Chef) tidak tersedia dan aset apa pun yang harus disimpan dengan aman, seperti PHI, rahasia/kata sandi, sertifikat, dll., harus disimpan dalam ember terenkripsi di Amazon S3. AWS OpsWorks Stack menggunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS Organizations

AWS Organizations membantu pelanggan mengelola dan mengatur lingkungan mereka secara terpusat saat mereka menumbuhkan dan menskalakan sumber daya AWS mereka. Dengan menggunakan AWS Organizations, mereka dapat secara terprogram membuat akun AWS baru dan mengalokasikan sumber daya, mengelompokkan akun untuk mengatur alur kerja mereka, menerapkan kebijakan ke akun atau grup untuk tata kelola, dan menyederhanakan penagihan dengan menggunakan metode pembayaran tunggal untuk semua akun mereka.

Selain AWS Organizations itu, terintegrasi dengan layanan AWS lainnya sehingga pelanggan dapat menentukan konfigurasi pusat, mekanisme keamanan, persyaratan audit, dan berbagi sumber daya di seluruh akun di organisasi mereka. AWS Organizations tersedia untuk semua pelanggan AWS tanpa biaya tambahan.

AWS Organizations adalah layanan orkestrasi yang tidak secara langsung memproses, menyimpan, atau mengirimkan data pengguna. Layanan ini tidak mengenkripsi konten pelanggan, tetapi layanan yang mendasari yang diluncurkan di dalamnya AWS Organizations, mengenkripsi data pengguna. AWS Organizations terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau layanan AWS di AWS Organizations.

AWS RoboMaker

AWS RoboMaker memungkinkan pelanggan mengeksekusi kode di cloud untuk pengembangan aplikasi dan menyediakan layanan simulasi robotika untuk mempercepat pengujian aplikasi. AWS RoboMaker juga menyediakan layanan manajemen armada robotika untuk penyebaran, pembaruan, dan manajemen aplikasi jarak jauh.

Lalu lintas jaringan yang berisi PHI harus mengenkripsi data dalam perjalanan. Semua komunikasi manajemen dengan server simulasi melalui TLS, dan pelanggan harus menggunakan mekanisme enkripsi transport standar terbuka untuk koneksi ke layanan AWS lainnya. AWS RoboMaker juga terintegrasi dengan CloudTrail untuk mencatat semua panggilan API ke bucket Amazon S3 tertentu.

RoboMaker Log AWS tidak mengandung PHI, dan volume EBS yang digunakan oleh server simulasi dienkripsi. Saat mentransfer data yang mungkin berisi PHI ke layanan lain, seperti Amazon S3, pelanggan harus mengikuti panduan layanan penerima untuk menyimpan PHI. Untuk penyebaran ke robot, pelanggan harus memastikan bahwa enkripsi data dalam perjalanan dan saat istirahat konsisten dengan interpretasi mereka terhadap Panduan.

Metrik AWS SDK

Pelanggan perusahaan dapat menggunakan CloudWatch agen AWS dengan AWS SDK Metrics for Enterprise Support (SDK Metrics) untuk mengumpulkan metrik dari AWS SDK di host dan klien mereka. Metrik ini dibagikan dengan Dukungan Perusahaan AWS. SDK Metrics dapat membantu pelanggan mengumpulkan metrik dan data diagnostik yang relevan tentang koneksi aplikasi mereka ke layanan AWS tanpa menambahkan instrumentasi khusus ke kode mereka, dan mengurangi pekerjaan manual yang diperlukan untuk berbagi log dan data. AWS Support

Harap dicatat bahwa Metrik SDK hanya tersedia untuk pelanggan AWS dengan langganan Enterprise Support. Pelanggan dapat menggunakan SDK Metrics dengan aplikasi apa pun yang secara langsung memanggil layanan AWS dan yang dibuat menggunakan AWS SDK yang merupakan salah satu versi yang tercantum dalam dokumentasi AWS Metrics.

SDK Metrics memantau panggilan yang dibuat oleh AWS SDK dan menggunakan CloudWatch agen yang berjalan di lingkungan yang sama dengan aplikasi klien.

CloudWatch Agen mengenkripsi data dalam perjalanan dari mesin lokal ke pengiriman di grup log tujuan. Grup log dapat dikonfigurasi untuk dienkripsi mengikuti petunjuk di Encrypt Log Data in CloudWatch Logs Using. AWS KMS

AWS Secrets Manager

AWS Secrets Manager adalah layanan AWS yang memudahkan pelanggan untuk mengelola “rahasia”. Rahasia dapat berupa kredensyal basis data, kata sandi, kunci API pihak ketiga, dan bahkan teks arbitrer. AWS Secrets Manager dapat digunakan untuk menyimpan PHI jika informasi tersebut terkandung dalam “rahasia”. Semua rahasia yang disimpan oleh AWS Secrets Manager dienkripsi saat istirahat menggunakan AWS Key Management System (KMS). Pengguna dapat memilih AWS KMS kunci yang digunakan saat membuat rahasia baru. Jika tidak ada kunci yang dipilih, kunci default untuk akun akan digunakan. AWS Secrets Manager menggunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS Security Hub

AWS Security Hub mengumpulkan dan mengkonsolidasikan temuan dari layanan keamanan AWS yang diaktifkan di lingkungan pelanggan, seperti temuan deteksi intrusi dari Amazon, pemindaian kerentanan dari Amazon Inspector GuardDuty, temuan kebijakan bucket Amazon S3 dari Amazon Macie, sumber daya yang dapat diakses publik dan lintas akun dari IAM Access Analyzer, dan sumber daya yang tidak memiliki cakupan WAF. AWS Firewall Manager AWS Security Hub juga mengkonsolidasikan temuan dari solusi keamanan AWS Partner Network (APN) terintegrasi.

AWS Security Hub terintegrasi dengan Amazon CloudWatch Events, memungkinkan pelanggan untuk membuat respons kustom dan alur kerja remediasi. Pelanggan dapat dengan mudah mengirim temuan ke SIEM, alat obrolan, sistem tiket, alat Otomatisasi dan Respons Orkestrasi Keamanan (SOAR), dan platform manajemen panggilan. Tindakan respons dan remediasi dapat sepenuhnya otomatis atau dapat dipicu secara manual di konsol. Pelanggan juga dapat menggunakan dokumen AWS Systems Manager Otomasi AWS Step Functions,, dan AWS Lambda fungsi untuk membangun alur kerja remediasi otomatis yang dapat dimulai. AWS Security Hub

Untuk memastikan perlindungan data, AWS Security Hub mengenkripsi data saat istirahat dan data dalam perjalanan antar layanan komponen. Auditor pihak ketiga menilai keamanan dan kepatuhan AWS Security Hub sebagai bagian dari beberapa program kepatuhan AWS. AWS Security Hub adalah bagian dari program kepatuhan SOC, ISO, PCI, dan HIPAA AWS.

Layanan Migrasi Server AWS

AWS Server Migration Service (AWS SMS) mengotomatiskan migrasi mesin virtual VMware vSphere atau Microsoft Hyper-V/SCVMM lokal ke AWS Cloud. AWS SMS secara bertahap mereplikasi VM

server sebagai Amazon Machine Images (AMI) yang dihosting cloud yang siap digunakan di Amazon EC2.

Server yang berjalan di tempat dan dimigrasikan ke cloud dengan (AWS SMS) dapat berisi data PHI. AWS SMS mengenkripsi data saat transit dan ketika image VM server sedang dipentaskan untuk penempatan akhir ke EC2. Lihat panduan untuk EC2 dan menyiapkan volume penyimpanan terenkripsi saat memigrasikan VM server yang berisi PHI dengan AWS SMS. AWS SMS digunakan CloudTrail untuk mencatat semua panggilan API.

AWS Serverless Application Repository

The AWS Serverless Application Repository (SAR) adalah repositori terkelola untuk aplikasi tanpa server. Ini memungkinkan tim, organisasi, dan pengembang individu untuk menyimpan dan berbagi aplikasi yang dapat digunakan kembali, dan dengan mudah merakit dan menerapkan arsitektur tanpa server dengan cara baru yang kuat. Aplikasi adalah AWS CloudFormation template, yang berisi definisi infrastruktur aplikasi dan binari yang dikompilasi dari kode AWS Lambda fungsi aplikasi.

Meskipun dimungkinkan untuk aplikasi yang sedang memproses PHI, mereka hanya akan melakukan ini setelah dikerahkan ke akun pelanggan dan bukan sebagai bagian dari SAR itu sendiri. AWS Serverless Application Repository AWS Serverless Application Repository Enkripsi file yang diunggah pelanggan, termasuk paket penyebaran dan arsip lapisan. Untuk data dalam perjalanan, AWS Serverless Application Repository menggunakan TLS untuk mengenkripsi data antara layanan dan agen. AWS Serverless Application Repository terintegrasi dengan AWS CloudTrail, yang merupakan layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau layanan AWS di AWS Serverless Application Repository.

Service Catalog

Service Catalog memungkinkan administrator TI untuk membuat, mengelola, dan mendistribusikan portofolio produk yang disetujui kepada pengguna akhir, yang kemudian dapat mengakses produk yang mereka butuhkan di portal yang dipersonalisasi. Service Catalog digunakan untuk membuat katalog, berbagi, dan menyebarkan solusi swalayan di AWS dan tidak dapat digunakan untuk menyimpan, mengirimkan, atau memproses PHI. PHI tidak boleh ditempatkan dalam metadata apa pun untuk item Service Catalog atau dalam deskripsi item apa pun. Service Catalog digunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS Shield

AWS Shield adalah layanan perlindungan Distributed Denial of Service (DDoS) terkelola yang melindungi aplikasi web yang berjalan di AWS. AWS Shield menyediakan deteksi selalu aktif dan mitigasi inline otomatis yang meminimalkan waktu henti dan latensi aplikasi, sehingga tidak perlu terlibat untuk mendapatkan manfaat dari perlindungan DDoS. AWS Support

AWS Shield tidak dapat digunakan untuk menyimpan atau mengirimkan PHI, tetapi sebaliknya dapat digunakan untuk melindungi aplikasi web yang beroperasi dengan PHI. Dengan demikian, tidak diperlukan konfigurasi khusus saat terlibat AWS Shield.

Semua pelanggan AWS mendapat manfaat dari perlindungan otomatis AWS Shield Standard, tanpa biaya tambahan. AWS Shield Standard bertahan terhadap serangan DDoS lapisan jaringan dan transport yang paling umum dan sering terjadi yang menargetkan situs web atau aplikasi mereka. Untuk tingkat perlindungan yang lebih tinggi terhadap serangan yang menargetkan aplikasi web mereka yang berjalan pada sumber daya Elastic Load Balancing (ELB), Amazon CloudFront, dan Amazon Route 53, pelanggan dapat berlangganan. AWS Shield Advanced

AWS Snowball

Dengan AWS Snowball (Snowball), pelanggan dapat mentransfer ratusan terabyte atau petabyte data antara pusat data lokal mereka dan Amazon Simple Storage Service (Amazon S3). PHI yang disimpan AWS Snowball harus dienkripsi saat istirahat sesuai dengan Panduan. Saat membuat pekerjaan impor, pelanggan harus menentukan ARN untuk AWS KMS kunci yang akan digunakan untuk melindungi data dalam Snowball. Selain itu, selama pembuatan pekerjaan impor, pelanggan harus memilih bucket S3 tujuan yang memenuhi standar enkripsi yang ditetapkan oleh Guidance.

Meskipun Snowball saat ini tidak mendukung enkripsi sisi server dengan kunci yang AWS KMS dikelola (SSE-KMS) atau enkripsi sisi server dengan kunci yang disediakan pelanggan (SSE-C), Snowball mendukung enkripsi sisi server dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3). Untuk informasi selengkapnya, lihat Melindungi Data Menggunakan Enkripsi Sisi Server dengan Kunci Enkripsi Terkelola Amazon S3 (SSE-S3).

Atau, pelanggan dapat menggunakan metodologi enkripsi pilihan mereka untuk mengenkripsi PHI sebelum menyimpan data. AWS Snowball

Saat ini, pelanggan dapat menggunakan AWS Snowball alat standar sebagai bagian dari BAA kami.

AWS Snowball Tepi

AWS Snowball Edge terhubung ke aplikasi dan infrastruktur pelanggan yang ada menggunakan antarmuka penyimpanan standar, merampingkan proses transfer data dan meminimalkan pengaturan dan integrasi. Snowball Edge dapat mengelompokkan bersama untuk membentuk tingkat penyimpanan lokal dan memproses data pelanggan di tempat, membantu pelanggan memastikan bahwa aplikasi mereka terus berjalan bahkan ketika mereka tidak dapat mengakses cloud.

Untuk memastikan bahwa PHI tetap terenkripsi saat menggunakan Snowball Edge, pelanggan harus memastikan untuk menggunakan protokol koneksi terenkripsi seperti HTTPS atau SSL/TLS saat menggunakan prosedur yang AWS Lambda didukung oleh untuk mengirimkan PHI ke/dari sumber daya eksternal ke Snowball Edge. AWS IoT Greengrass Selain itu, PHI harus dienkripsi saat disimpan di volume lokal Snowball Edge, baik melalui akses lokal atau melalui NFS. Enkripsi secara otomatis diterapkan ke data yang ditempatkan ke Snowball Edge menggunakan Snowball Management Console dan API untuk transportasi massal ke S3. Untuk informasi lebih lanjut tentang transportasi data ke S3, lihat panduan terkait untukthe section called “AWS Snowball”.

AWS Step Functions

AWS Step Functions memudahkan untuk mengoordinasikan komponen aplikasi terdistribusi dan layanan mikro menggunakan alur kerja visual. AWS Step Functions tidak dapat menyimpan, mengirimkan, atau memproses PHI. PHI tidak boleh ditempatkan dalam metadata untuk AWS Step Functions atau dalam tugas atau definisi mesin negara apa pun. AWS Step Functions digunakan AWS CloudTrail untuk mencatat semua panggilan API.

AWS Storage Gateway

AWS Storage Gateway adalah layanan penyimpanan hybrid yang memungkinkan aplikasi lokal pelanggan untuk menggunakan penyimpanan AWS Cloud dengan mulus. Gateway menggunakan protokol penyimpanan standar terbuka untuk menghubungkan aplikasi penyimpanan dan alur kerja yang ada ke layanan penyimpanan AWS Cloud untuk gangguan proses minimal.

Gerbang Berkas

File gateway adalah jenis AWS Storage Gateway yang mendukung antarmuka file ke Amazon S3 dan yang menambah volume berbasis blok saat ini dan penyimpanan VTL. File gateway menggunakan

HTTPS untuk berkomunikasi dengan S3 dan menyimpan semua objek yang dienkripsi saat berada di S3 menggunakan SSE-S3, secara default, atau menggunakan enkripsi sisi klien dengan kunci yang disimpan. AWS KMS Metadata file, seperti nama file, tetap tidak terenkripsi dan tidak boleh mengandung PHI apa pun.

Gerbang Volume

Volume gateway menyediakan volume penyimpanan yang didukung cloud yang dapat dipasang pelanggan sebagai perangkat Antarmuka Sistem Komputer Kecil (iSCSI) internet dari server aplikasi lokal. Pelanggan harus melampirkan disk lokal sebagai buffer Upload dan Cache ke Volume Gateway VM sesuai dengan kepatuhan internal dan persyaratan peraturan mereka. Disarankan bahwa, untuk PHI, disk ini harus mampu menyediakan enkripsi saat istirahat. Komunikasi antara Volume Gateway VM dan AWS dienkripsi menggunakan TLS 1.2 untuk mengamankan PHI dalam transportasi.

Gerbang Pita

Tape gateway menyediakan antarmuka VTL (pustaka pita virtual) ke aplikasi cadangan pihak ketiga yang berjalan di tempat. Pelanggan harus mengaktifkan enkripsi untuk PHI dalam aplikasi cadangan pihak ketiga saat menyiapkan pekerjaan pencadangan rekaman. Komunikasi antara Tape Gateway VM dan AWS dienkripsi menggunakan TLS 1.2 untuk mengamankan PHI dalam transportasi. Pelanggan yang menggunakan salah satu konfigurasi Storage Gateway dengan PHI harus mengaktifkan pencatatan penuh. Untuk informasi lebih lanjut, lihat Apa Itu AWS Storage Gateway?

AWS Systems Manager

AWS Systems Manager adalah antarmuka terpadu yang memungkinkan pelanggan untuk dengan mudah memusatkan data operasional, mengotomatiskan tugas di seluruh sumber daya AWS mereka, dan mempersingkat waktu untuk mendeteksi dan menyelesaikan masalah operasional di infrastruktur mereka. Systems Manager memberikan pandangan lengkap tentang kinerja dan konfigurasi infrastruktur pelanggan, menyederhanakan manajemen sumber daya dan aplikasi, dan membuatnya mudah untuk mengoperasikan dan mengelola infrastruktur mereka dalam skala besar.

Saat mengeluarkan data yang mungkin berisi PHI ke layanan lain, seperti Amazon S3, pelanggan harus mengikuti panduan layanan penerima untuk menyimpan PHI. Pelanggan tidak boleh menyertakan PHI dalam metadata atau pengidentifikasi, seperti nama dokumen dan nama parameter.

AWS Transfer for SFTP

AWS Transfer for SFTP menyediakan akses Secure File Transfer Protocol (SFTP) ke sumber daya S3 pelanggan. Pelanggan disajikan dengan server virtual, yang diakses menggunakan protokol SFTP standar di titik akhir layanan regional. Dari sudut pandang pelanggan AWS dan klien SFTP, gateway SFTP terlihat seperti server SFTP standar yang sangat tersedia. Meskipun layanan itu sendiri tidak menyimpan, memproses, atau mengirimkan PHI, sumber daya yang diakses pelanggan di Amazon S3 harus dikonfigurasi dengan cara yang konsisten dengan Panduan. Pelanggan juga dapat menggunakan AWS CloudTrail untuk mencatat panggilan API yang dilakukan ke AWS Transfer for SFTP.

AWS WAF — Firewall Aplikasi Web

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web pelanggan dari eksploitasi web umum yang dapat memengaruhi ketersediaan aplikasi, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. Pelanggan dapat menempatkan AWS WAF di antara aplikasi web mereka yang dihosting di AWS yang beroperasi dengan atau bertukar PHI, dan pengguna akhir mereka. Seperti halnya transmisi PHI apa pun saat menggunakan AWS, data yang berisi PHI harus dienkripsi saat dalam perjalanan. Lihat panduan Amazon EC2 untuk lebih memahami opsi enkripsi yang tersedia.

AWS X-Ray

AWS X-Ray adalah layanan yang mengumpulkan data tentang permintaan yang dilayani aplikasi pelanggan, dan menyediakan alat yang dapat mereka gunakan untuk melihat, memfilter, dan mendapatkan wawasan tentang data tersebut untuk mengidentifikasi masalah dan peluang untuk pengoptimalan. Untuk setiap permintaan yang dilacak ke aplikasi pelanggan, mereka dapat melihat informasi terperinci tidak hanya tentang permintaan dan respons, tetapi juga tentang panggilan yang dilakukan aplikasi mereka ke hilir sumber daya AWS, layanan mikro, database, dan API web HTTP. AWS X-Ray tidak boleh digunakan untuk menyimpan atau memproses PHI. Informasi yang dikirimkan ke dan dari AWS X-Ray dienkripsi secara default. Saat menggunakan AWS X-Ray, jangan letakkan PHI apa pun dalam anotasi segmen atau metadata segmen.

Penyeimbang Beban Elastis

Pelanggan dapat menggunakan Elastic Load Balancing untuk mengakhiri dan memproses sesi yang berisi PHI. Pelanggan dapat memilih Classic Load Balancer atau Application Load Balancer. Karena

semua lalu lintas jaringan yang mengandung PHI harus dienkripsi dalam perjalanan end-to-end, pelanggan memiliki fleksibilitas untuk menerapkan dua arsitektur yang berbeda:

Pelanggan dapat menghentikan HTTPS, HTTP/2 melalui TLS (untuk Aplikasi), atau SSL/TLS pada Elastic Load Balancing dengan membuat penyeimbang beban yang menggunakan protokol terenkripsi untuk koneksi. Fitur ini memungkinkan enkripsi lalu lintas antara penyeimbang beban dan klien yang memulai HTTPS, HTTP/2 melalui sesi TLS, atau SSL/TLS, dan untuk koneksi antara penyeimbang beban dan instance backend pelanggan. Sesi yang berisi PHI harus mengenkripsi pendengar front-end dan backend untuk enkripsi transport. Pelanggan harus mengevaluasi sertifikat dan kebijakan negosiasi sesi mereka dan menjaganya agar tetap konsisten dengan Panduan. Untuk informasi selengkapnya, lihat HTTPS Listener untuk Classic Load Balancer Anda.

Atau, pelanggan dapat mengonfigurasi Amazon ELB dalam mode TCP dasar (untuk Klasik) atau lebih WebSockets (untuk Aplikasi) dan sesi terenkripsi pass-through ke instance backend di mana sesi terenkripsi dihentikan. Dalam arsitektur ini, pelanggan mengelola sertifikat mereka sendiri dan kebijakan negosiasi TLS dalam aplikasi yang berjalan dalam instans mereka sendiri. Untuk informasi selengkapnya, lihat Pendengar untuk Classic Load Balancer Anda. Dalam kedua arsitektur, pelanggan harus menerapkan tingkat logging yang mereka tentukan konsisten dengan persyaratan HIPAA dan HITECH.

FreeRTOS

FreeRTOS adalah sistem operasi untuk mikrokontroler yang membuat perangkat edge kecil berdaya rendah mudah diprogram, digunakan, aman, terhubung, dan dikelola. FreeRTOS didasarkan pada kernel FreeRTOS, sistem operasi open source yang populer untuk mikrokontroler, dan memperluasnya dengan pustaka perangkat lunak yang memudahkan untuk menghubungkan perangkat kecil berdaya rendah dengan aman ke layanan AWS Cloud seperti Core atau ke perangkat edge yang lebih kuat yang berjalan. AWS IoT AWS IoT Greengrass

Data yang berisi PHI sekarang dapat dienkripsi dalam perjalanan dan saat istirahat saat menggunakan perangkat yang memenuhi syarat yang menjalankan FreeRTOS. FreeRTOS menyediakan dua pustaka untuk menyediakan keamanan platform: TLS dan PKCS #11. API TLS harus digunakan untuk mengenkripsi dan mengotentikasi semua lalu lintas jaringan yang berisi PHI. PKCS #11 menyediakan antarmuka standar untuk operasi kriptografi perangkat lunak dan harus digunakan untuk mengenkripsi PHI apa pun yang disimpan pada perangkat yang memenuhi syarat yang menjalankan FreeRTOS.

Menggunakan AWS KMS untuk Enkripsi PHI

Kunci KMS dapat digunakan untuk mengenkripsi/mendekripsi kunci enkripsi data yang digunakan untuk mengenkripsi PHI dalam aplikasi pelanggan atau dalam layanan AWS yang digunakan. AWS KMS AWS KMS dapat digunakan bersama dengan akun HIPAA, tetapi PHI hanya dapat diproses, disimpan, atau ditransmisikan dalam Layanan yang Memenuhi Syarat HIPAA. AWS KMS biasanya digunakan untuk menghasilkan dan mengelola kunci untuk aplikasi yang berjalan di Layanan Layak HIPAA lainnya.

Misalnya, aplikasi yang memproses PHI di Amazon EC2 dapat menggunakan GenerateDataKey panggilan API untuk menghasilkan kunci enkripsi data untuk mengenkripsi dan mendekripsi PHI dalam aplikasi. Kunci enkripsi data akan dilindungi oleh kunci KMS pelanggan yang disimpan AWS KMS, menciptakan hierarki kunci yang sangat dapat diaudit saat panggilan API masuk AWS KMS . AWS CloudTrail PHI tidak boleh disimpan dalam Tag (metadata) untuk kunci apa pun yang disimpan di. AWS KMS

VM Import/Export

VM Impor/Ekspor memungkinkan pelanggan untuk dengan mudah mengimpor gambar mesin virtual dari lingkungan yang ada ke instans Amazon EC2 dan mengekspornya kembali ke lingkungan lokal Anda. Penawaran ini memungkinkan pelanggan untuk memanfaatkan investasi yang ada di mesin virtual yang telah Anda buat untuk memenuhi keamanan IRIT mereka, manajemen konfigurasi mereka, dan persyaratan kepatuhan mereka dengan membawa mesin virtual tersebut ke Amazon ready-to-use EC2 sebagai instance. Pelanggan juga dapat mengekspor instans yang diimpor kembali ke infrastruktur virtualisasi lokal mereka, memungkinkan mereka untuk menyebarkan beban kerja di seluruh infrastruktur TI Anda.

Impor/Ekspor VM tersedia tanpa biaya tambahan di luar biaya penggunaan standar untuk Amazon EC2 dan Amazon S3.

Untuk mengimpor gambar pelanggan, pelanggan dapat menggunakan AWS CLI atau alat pengembang lainnya untuk mengimpor gambar mesin virtual (VM) dari lingkungan VMware mereka. Jika pelanggan menggunakan platform virtualisasi VMware vSphere, mereka juga dapat menggunakan AWS Management Portal for vCenter untuk mengimpor VM mereka. Sebagai bagian dari proses impor, VM Import akan mengubah VM pelanggan menjadi Amazon EC2 AMI, yang dapat mereka gunakan untuk menjalankan instans Amazon EC2. Setelah VM mereka diimpor, mereka dapat memanfaatkan elastisitas, skalabilitas, dan pemantauan Amazon melalui penawaran seperti Auto Scaling, Elastic Load Balancing dan untuk mendukung gambar impor mereka. CloudWatch

Pelanggan dapat mengekspor instans Amazon EC2 yang diimpor sebelumnya menggunakan alat API Amazon EC2. Cukup tentukan instance target, format file mesin virtual, dan bucket Amazon S3 tujuan, dan Impor/Ekspor VM akan secara otomatis mengekspor instance ke bucket Amazon S3 bersama dengan opsi enkripsi untuk mengamankan transmisi dan penyimpanan gambar VM mereka. Pelanggan kemudian dapat mengunduh dan meluncurkan VM yang diekspor dalam infrastruktur virtualisasi lokal mereka.

Pelanggan dapat mengimpor VM Windows dan Linux yang menggunakan format virtualisasi VMware ESX atau Workstation, Microsoft Hyper-V, dan Citrix Xen. Dan pelanggan dapat mengekspor instans Amazon EC2 yang diimpor sebelumnya ke format VMware ESX, Microsoft Hyper-V atau Citrix Xen. Untuk daftar lengkap sistem operasi, versi, dan format yang didukung, lihat Persyaratan Impor/Ekspor VM. AWS berencana untuk menambahkan dukungan untuk sistem operasi, versi, dan format tambahan di masa mendatang.

Audit, backup, dan pemulihan bencana

Aturan Keamanan HIPAA memiliki persyaratan terperinci terkait dengan kemampuan audit mendalam, prosedur cadangan data, dan mekanisme pemulihan bencana. Layanan di AWS berisi banyak fitur yang membantu pelanggan memenuhi persyaratan mereka. Misalnya, pelanggan harus mempertimbangkan untuk membangun kemampuan audit untuk memungkinkan analis keamanan memeriksa log aktivitas terperinci atau laporan untuk melihat siapa yang memiliki akses, entri alamat IP, data apa yang diakses, dll.

Data ini harus dilacak, dicatat, dan disimpan di lokasi pusat untuk jangka waktu yang lama, jika terjadi audit. Menggunakan Amazon EC2, pelanggan dapat menjalankan file log aktivitas dan mengaudit ke lapisan paket di server virtual mereka, seperti yang mereka lakukan pada perangkat keras tradisional. Mereka juga dapat melacak lalu lintas IP apa pun yang mencapai instance server virtual mereka. Administrator pelanggan dapat mencadangkan file log ke Amazon S3 untuk penyimpanan jangka panjang yang andal.

HIPAA juga memiliki persyaratan terperinci terkait dengan pemeliharaan rencana darurat untuk melindungi data jika terjadi keadaan darurat dan harus membuat dan memelihara salinan PHI elektronik yang dapat diambil. Untuk mengimplementasikan paket cadangan data di AWS, Amazon EBS menawarkan penyimpanan persisten untuk instans server virtual Amazon EC2. Volume ini dapat diekspos sebagai perangkat blok standar, dan mereka menawarkan penyimpanan off-instance yang bertahan secara independen dari masa pakai instans. Agar selaras dengan pedoman HIPAA, pelanggan dapat membuat point-in-time snapshot volume Amazon EBS yang disimpan secara otomatis di Amazon S3 dan direplikasi di beberapa Availability Zone, yang merupakan lokasi berbeda yang dirancang untuk diisolasi dari kegagalan di Availability Zone lainnya.

Snapshot ini dapat diakses kapan saja dan dapat melindungi data untuk daya tahan jangka panjang. Amazon S3 juga menyediakan solusi yang sangat tersedia untuk penyimpanan data dan pencadangan otomatis. Dengan hanya memuat file atau gambar ke Amazon S3, beberapa salinan redundan secara otomatis dibuat dan disimpan di pusat data terpisah. File-file ini dapat diakses kapan saja, dari mana saja (berdasarkan izin), dan disimpan hingga sengaja dihapus.

Selain itu, AWS secara inheren menawarkan berbagai mekanisme pemulihan bencana. Pemulihan bencana, proses melindungi data organisasi dan infrastruktur TI pada saat bencana, melibatkan pemeliharaan sistem yang sangat tersedia, menjaga data dan sistem direplikasi di luar lokasi, dan memungkinkan akses berkelanjutan ke keduanya.

Dengan Amazon EC2, administrator dapat memulai instans server dengan sangat cepat dan dapat menggunakan alamat IP Elastis (alamat IP statis untuk lingkungan komputasi awan) untuk failover yang anggun dari satu mesin ke mesin lainnya. Amazon EC2 juga menawarkan Availability Zone. Administrator dapat meluncurkan instans Amazon EC2 di beberapa Availability Zone untuk menciptakan sistem toleran kesalahan yang beragam secara geografis yang sangat tangguh jika terjadi kegagalan jaringan, bencana alam, dan sebagian besar kemungkinan sumber downtime lainnya.

Menggunakan Amazon S3, data pelanggan direplikasi dan disimpan secara otomatis di pusat data terpisah untuk menyediakan penyimpanan data yang andal yang dirancang untuk menyediakan ketersediaan 99,99%.

Menggunakan AWS Elastic Disaster Recovery (AWS DRS), pelanggan dapat dengan cepat memulihkan aplikasi di AWS, baik di sebagian besar up-to-date keadaan aplikasi, atau dari titik waktu sebelumnya.

Revisi dokumen

Untuk mengetahui jika ada perubahan pada laporan resmi ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Pembaruan kecil	Pembaruan kecil	12 Mei 2023
Pembaruan kecil	Whitepaper yang diperbaru i untuk memperluas konten yang tersedia pada layanan.	September 28, 2022
Pembaruan kecil	Perbaiki bahasa non-inklusif.	April 6, 2022
Laporan resmi diperbarui	Menambahkan informasi tentang Layanan Migrasi AWS Aplikasi, dan informasi terbaru untuk Amazon ECS	Desember 6, 2021
Laporan resmi diperbarui	Informasi yang diperbarui di bagian Amazon Healthlake dan Amazon VPC	November 9, 2021
Laporan resmi diperbarui	Menambahkan informasi tentang AWS Network Firewall	9 September 2021
Laporan resmi diperbarui	Informasi terbaru tentang Profil Pelanggan Amazon Connect	26 Agustus 2021
Laporan resmi diperbarui	Menambahkan bagian Amazon AppFlow dan AWS Glue DataBrew	22 Juli 2021
Laporan resmi diperbarui	Navigasi dan organisasi yang diperbarui.	26 April 2021
Laporan resmi diperbarui	Menambahkan bagian berikut: AWS CodeDeploy,, Amazon	31 Maret 2021

	Aurora AWS CodePipeline, Aurora PostgreSQL, Amazon Textract, Amazon Polly, Amazon FSx, AWS Auto AWS Backup Scaling,,,,,,, VM Impor/ Ekspor, Amazon, Amazon. AWS Elastic Beanstalk AWS Firewall Manager AWS Organizations AWS Security Hub AWS Serverless Applicati on Repository HealthLake EventBridge Bagian Amazon Aurora yang diperbarui.	
Laporan resmi diperbarui	Menambahkan bagian pada AWS App Mesh, dan konten AWS System Manager yang diperbarui	25 Agustus 2020
Laporan resmi diperbarui	Menambahkan bagian Amazon Appstream 2.0, AWS SDK Metrics, AWS Data Exchange, Amazon MSK, Amazon Pinpoint, Amazon Lex, Amazon SES, dan Amazon Forecast, Amazon Quantum Ledger Database (QLDB),. AWS Cloud Map	7 Mei 2020

Laporan resmi diperbarui	Menambahkan bagian di Amazon CloudWatch, CloudWatch Acara Amazon, Firehose Data Amazon, Layanan Terkelola Amazon untuk Apache Flink, Layanan Amazon, OpenSearch Amazon DocumentDB (dengan kompatibilitas MongoDB), AWS Mobile Hub,, untuk Chef Automate, untuk Puppet Enterprise, AWS Transfer AWS OpsWorks for DataSync SFTP, AWS AWS IoT Greengrass, AWS, AWS,, Amazon Comprehend Medical Prehend Medical, dan AWS. AWS OpsWorks AWS Global Accelerator RoboMaker	Januari 1, 2020
Laporan resmi diperbarui	Menambahkan bagian di Amazon Comprehend, Amazon Transcribe, Amazon Translate, dan AWS Certificate Manager.	Januari 1, 2019
Laporan resmi diperbarui	Menambahkan bagian di Amazon Athena, Amazon EKS, AWS IoT Core dan, Amazon FreerTOS AWS IoT Device Management, Amazon, Amazon GuardDuty Neptunus, Layanan Migrasi AWS Server, Amazon MQ, dan. AWS Database Migration Service AWS Glue	1 November 2018

Laporan resmi diperbarui	Menambahkan bagian di Amazon Elastic File System (EFS), Amazon Kinesis Video Streams, Amazon Rekogniti on SageMaker, Amazon, Amazon Simple Workflow, AWS Secrets Manage, Service Catalog, dan. AWS Step Functions	1 Juni 2018
Laporan resmi diperbarui	Ditambahkan bagian pada AWS CloudFormation, AWS X-Ray, AWS CloudTrail, AWS CodeBuild, AWS CodeCommi t, AWS Config, dan AWS OpsWorks Stack.	April 1, 2018
Laporan resmi diperbarui	Ditambahkan bagian pada AWS Fargate.	Januari 1, 2018

Pembaruan yang dilakukan sebelum 2018:

Tanggal	Deskripsi
November 2017	Menambahkan bagian di Amazon EC2 Container Registry, Amazon Macie, QuickSight Amazon, dan. AWS Managed Services
November 2017	Menambahkan bagian di Amazon ElastiCache untuk Redis dan Amazon CloudWatch.
Oktober 2017	Menambahkan bagian di Amazon SNS, Amazon Route 53, AWS Storage Gateway, dan. AWS CloudHSM Bagian yang diperbarui pada AWS Key Management Service.

Tanggal	Deskripsi
September 2017	Menambahkan bagian di Amazon Connect, Amazon Kinesis Streams, Amazon RDS (Maria) DB, Amazon RDS SQL AWS Batch Server,,, Edge AWS Lambda AWS Snowball , dan fitur Lambda @Edge dari Amazon. CloudFront
Agustus 2017	Menambahkan bagian di Amazon EC2 Systems Manager dan Amazon Inspector.
Juli 2017	Menambahkan bagian di Amazon WorkSpace s, Amazon WorkDocs, AWS Directory Service, dan Amazon ECS.
Juni 2017	Menambahkan bagian di Amazon CloudFron t, AWS WAF AWS Shield, dan Amazon S3 Transfer Acceleration.
Mei 2017	Persyaratan dihapus untuk Instans Khusus atau Host Khusus untuk memproses PHI di EC2 dan EMR.
Maret 2017	Daftar layanan yang diperbarui untuk mengarah ke halaman AWS Services in Ccope by Compliance Program. Menambahkan deskripsi untuk Amazon API Gateway.
Januari 2017	Diperbarui ke template terbaru.
Oktober 2016	Publikasi pertama

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa jaminan, pernyataan, atau ketentuan dalam bentuk apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.