Laporan Resmi AWS

Menavigasi Kepatuhan GDPR di AWS

Menavigasi Kepatuhan GDPR di AWS: Laporan Resmi AWS

Table of Contents

Menavigasi Kepatuhan GDPR di AWS

Tanggal publikasi: Desember 2020 (Revisi Dokumen)

Abstrak

Dokumen ini memberikan informasi tentang layanan dan sumber daya yang ditawarkan Amazon Web Services (AWS) kepada pelanggan guna membantu mereka menyelaraskan diri dengan persyaratan General Data Protection Regulation (GDPR) yang dapat berlaku atas aktivitas mereka. Ini termasuk kepatuhan terhadap standar keamanan IT, pengesahan Katalog Kontrol Kepatuhan Komputasi AWS Cloud (C5), kepatuhan terhadap Kode Perilaku Penyedia Layanan Infrastruktur Cloud di Eropa (CISPE), kontrol akses data, alat pemantauan dan pencatatan, enkripsi, dan manajemen kunci.

Gambaran Umum General Data Protection Regulation

General Data Protection Regulation (GDPR) adalah undang-undang privasi Eropa (Peraturan 2016/679 dari Parlemen dan Dewan Eropa tanggal 27 April 2016) yang diberlakukan pada tanggal 25 Mei 2018. GDPR menggantikan Data Protection Directive UE (Directive 95/46/EC), dan ditujukan untuk menyelaraskan undang-undang perlindungan data di seluruh Uni Eropa (UE) dengan menerapkan satu undang-undang perlindungan data yang mengikat di seluruh negara anggota UE.

GDPR berlaku untuk semua pemrosesan data pribadi baik oleh organisasi yang memiliki tempat bisnis di UE, atau untuk organisasi yang memproses data pribadi penduduk UE saat menawarkan barang atau jasa kepada individu di UE atau memantau perilaku penduduk UE di Uni Eropa. Data pribadi merupakan setiap informasi yang berkaitan dengan perorangan yang sudah diidentifikasi atau dapat diidentifikasi.

Perubahan GDPR Berlaku untuk Organisasi yang Beroperasi di UE

Salah satu aspek utama GDPR adalah bahwa GDPR menciptakan konsistensi di seluruh negara anggota UE tentang cara pemrosesan, penggunaan, dan pertukaran data pribadi secara aman. Organisasi harus menunjukkan keamanan data yang mereka proses dan kepatuhannya dengan GDPR secara terus-menerus, dengan menerapkan dan secara teratur meninjau langkah-langkah teknis dan organisasional, serta kebijakan kepatuhan yang berlaku untuk pemrosesan data pribadi. Otoritas pengawas Uni Eropa dapat mengeluarkan denda hingga 20 juta EUR, atau 4% dari omset tahunan global, mana saja yang lebih tinggi, untuk pelanggaran GDPR.

Persiapan AWS untuk GDPR

Kepatuhan, perlindungan data, dan pakar keamanan AWS bekerja sama dengan pelanggan di seluruh dunia untuk menjawab pertanyaan mereka dan membantu mereka mempersiapkan diri untuk menjalankan beban kerja di cloud di bawah GDPR. Tim-tim ini juga meninjau kesiapan AWS terhadap persyaratan GDPR.

> **Note**
>
> Kami dapat memastikan bahwa semua layanan AWS dapat digunakan sesuai dengan GDPR.

Adendum Pemrosesan Data (DPA) AWS

AWS menawarkan Adendum Pemrosesan Data yang mematuhi GDPR (GDPR DPA), yang memungkinkan pelanggan mematuhi kewajiban kontrak GDPR. GDPR DPA AWS menjadi bagian dalam Syarat Layanan AWS dan berlaku secara otomatis untuk semua pelanggan secara global yang wajib mematuhi GDPR.

Pada tanggal 16 Juli 2020, Mahkamah Uni Eropa (CJEU) mengeluarkan putusan mengenai Perisai EU-US Privacy Shield dan Klausul Kontrak Standar (SCC), yang juga dikenal sebagai “klausul model”. CJEU memutuskan bahwa EU-US Privacy Shield tidak lagi berlaku untuk transfer data pribadi dari Uni Eropa (UE) ke Amerika Serikat (AS). Namun, dalam putusan yang sama, CJEU memvalidasi bahwa perusahaan dapat terus menggunakan SCC sebagai mekanisme untuk mentransfer data di luar UE.

Mengikuti putusan ini, pelanggan dan partner AWS dapat terus menggunakan AWS untuk mentransfer konten mereka dari Eropa ke AS dan negara lain, sesuai dengan undang-undang perlindungan data UE – termasuk General Data Protection Regulation (GDPR). Pelanggan AWS dapat mengandalkan SCC yang disertakan dalam Adendum Pemrosesan Data (DPA) AWS jika mereka memilih untuk mentransfer data mereka ke luar Uni Eropa sesuai dengan GDPR. Seiring lanskap peraturan dan undang-undang terus berubah, kami akan selalu berupaya untuk memastikan bahwa pelanggan kami dapat terus menikmati manfaat layanan AWS dari mana pun mereka beroperasi. Untuk informasi tambahan, lihat FAQ EU-US Privacy Shield.

Peran AWS Berdasarkan GDPR

Berdasarkan GDPR, AWS berperan sebagai pemroses data dan pengontrol data.

Berdasarkan Pasal 32, pengontrol dan pemroses data diwajibkan untuk “…menerapkan langkah-langkah teknis dan organisasional yang tepat” yang mempertimbangkan “kemutakhiran serta biaya dari implementasi dan sifat, cakupan, konteks, dan tujuan pemrosesan serta risiko dari berbagai kemungkinan dan tingkat keparahan untuk hak dan kebebasan perorangan”. GDPR memberikan saran khusus untuk jenis tindakan keamanan apa yang mungkin diperlukan, termasuk:

- Pseudonimisasi dan enkripsi data pribadi.
- Kemampuan untuk memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan yang berkelanjutan dari sistem dan layanan pemrosesan.

- Kemampuan untuk memulihkan ketersediaan dan akses ke data pribadi secara tepat waktu jika terjadi insiden fisik atau teknis.
- Sebuah proses untuk secara teratur menguji, menilai, dan mengevaluasi efektivitas langkah-langkah teknis dan organisasional untuk menjamin keamanan pemrosesan.

AWS sebagai Pemroses Data

Ketika pelanggan dan Partner AWS menggunakan layanan AWS untuk memproses data pribadi dalam konten mereka, AWS bertindak sebagai pemroses data. Pelanggan dan Partner AWS dapat menggunakan kontrol yang tersedia di layanan AWS, termasuk kontrol konfigurasi keamanan, untuk memproses data pribadi. Dalam kondisi ini, pelanggan atau Partner AWS dapat bertindak sebagai pengontrol data atau pemroses data itu sendiri, dan AWS bertindak sebagai pemroses atau sub-pemroses data Adendum Pemrosesan Data (DPA) AWS yang mematuhi GDPR mencakup komitmen AWS sebagai pemroses data.

AWS sebagai Pengontrol Data

Ketika AWS mengumpulkan data pribadi dan menentukan tujuan dan sarana dalam memproses data pribadi tersebut, AWS akan bertindak sebagai pengontrol data. Misalnya, ketika AWS memproses informasi akun untuk pendaftaran akun, administrasi, akses layanan, atau informasi kontak untuk akun AWS guna memberikan bantuan melalui aktivitas dukungan pelanggan, AWS bertindak sebagai pengontrol data.

Model Tanggung Jawab Keamanan Bersama

Keamanan dan Kepatuhan merupakan tanggung jawab bersama antara AWS dan pelanggan. Ketika pelanggan memindahkan sistem komputer dan data mereka ke cloud, tanggung jawab keamanan dibagi antara pelanggan dan penyedia layanan cloud. Ketika pelanggan beralih ke AWS Cloud, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua layanan yang ditawarkan di AWS Cloud. Untuk layanan yang diabstrak, seperti Amazon S3 dan Amazon DynamoDB, AWS juga bertanggung jawab atas keamanan sistem operasi dan platform. Pelanggan dan Partner AWS, yang bertindak baik sebagai pengontrol data atau pemroses data, bertanggung jawab atas hal apa pun yang mereka simpan atau hubungkan ke cloud. Diferensiasi tanggung jawab ini biasanya disebut sebagai keamanan dari cloud dibandingkan keamanan di cloud. Model tanggung jawab bersama ini dapat membantu mengurangi beban operasional pelanggan, dan memberi mereka fleksibilitas dan kontrol yang diperlukan untuk men-deploy infrastruktur mereka di AWS Cloud. Untuk informasi selengkapnya, lihat Model Tanggung Jawab Bersama AWS.

GDPR tidak mengubah model tanggung jawab bersama AWS, yang terus relevan bagi pelanggan dan Partner AWS yang fokus pada penggunaan layanan komputasi cloud. Model tanggung jawab bersama merupakan pendekatan bermanfaat untuk menggambarkan tanggung jawab AWS yang berbeda-beda (sebagai pemroses atau sub-pemroses data) dan pelanggan atau Partner AWS (sebagai pengontrol data atau pemroses data) berdasarkan GDPR.

Kerangka Kerja Kepatuhan dan Standar Keamanan yang Kuat

Menurut GDPR, langkah-langkah teknis dan organisasional yang tepat mungkin perlu menyertakan "…kemampuan untuk memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan yang berkelanjutan dari sistem dan layanan pemrosesan," serta proses pemulihan, pengujian, dan manajemen risiko secara keseluruhan yang dapat diandalkan.

AWS Compliance Program

AWS terus mempertahankan standar tinggi untuk keamanan dan kepatuhan di seluruh operasi global kami. Keamanan selalu menjadi prioritas tertinggi kami – benar-benar "pekerjaan nomor nol". AWS secara teratur menjalani audit pengesahan pihak ketiga independen untuk memberikan jaminan bahwa aktivitas kontrol beroperasi sebagaimana dimaksud. Lebih khusus lagi, AWS diaudit berdasarkan berbagai kerangka kerja keamanan global dan regional yang bergantung pada wilayah dan industri. Saat ini, AWS berpartisipasi dalam lebih dari 50 program audit yang berbeda.

Hasil audit ini didokumentasikan oleh badan penilaian dan tersedia untuk semua pelanggan AWS melalui AWS Artifact. AWS Artifact adalah portal layanan mandiri yang tersedia tanpa biaya untuk akses sesuai permintaan ke laporan kepatuhan AWS. Ketika laporan baru dirilis, laporan tersebut tersedia di AWS Artifact, sehingga memungkinkan pelanggan terus memantau keamanan dan kepatuhan AWS dengan akses langsung ke laporan baru.

Pelanggan dapat memanfaatkan sertifikasi dan akreditasi yang diakui secara internasional, sehingga menunjukkan kepatuhan terhadap standar internasional yang ketat, seperti ISO 27017 untuk keamanan cloud, ISO 27018 untuk privasi cloud, SOC 1, SOC 2, dan SOC 3, PCI DSS Level 1, dan lainnya. AWS juga membantu pelanggan memenuhi standar keamanan lokal seperti Common Cloud Computing Controls Catalogue (C5) dari BSI, pengesahan yang didukung oleh pemerintah Jerman.

Untuk informasi lebih mendetail tentang program sertifikasi AWS, laporan, dan pengesahan pihak ketiga, lihat AWS Compliance Programs. Untuk informasi khusus layanan, lihat Layanan AWS dalam Cakupan.

Cloud Computing Compliance Controls Catalog

Cloud Computing Compliance Controls Catalog (C5) adalah skema pengesahan yang didukung pemerintah Jerman yang diberlakukan di Jerman oleh Kantor Federal untuk Keamanan Informasi

(BSI). Ini dibuat untuk membantu organisasi menunjukkan keamanan operasional terhadap serangan siber umum dalam konteks Rekomendasi Keamanan untuk Penyedia Cloud dari pemerintah Jerman.

Langkah-langkah teknis dan organisasional perlindungan data dan langkah-langkah keamanan informasi menargetkan keamanan data untuk memastikan kerahasiaan, integritas, dan ketersediaan. C5 mendefinisikan persyaratan keamanan yang juga dapat relevan untuk perlindungan data. Pelanggan AWS dan penasihat kepatuhan mereka dapat menggunakan pengesahan C5 sebagai sumber daya untuk memahami berbagai layanan jaminan Keamanan IT yang ditawarkan AWS saat mereka memindahkan beban kerja mereka ke cloud. C5 menambahkan level Keamanan IT yang ditetapkan peraturan yang setara dengan IT-Grundschutz, dengan penambahan kontrol khusus cloud.

C5 memasukkan kontrol tambahan yang menyediakan informasi terkait dengan lokasi data, penyediaan layanan, tempat yurisdiksi, sertifikasi yang ada, kewajiban pengungkapan informasi, dan deskripsi layanan lengkap. Dengan menggunakan informasi ini, Anda dapat mengevaluasi bagaimana peraturan hukum (seperti privasi data), kebijakan Anda sendiri, atau peringatan lingkungan terkait dengan penggunaan layanan komputasi cloud Anda.

Kontrol Akses Data

Pasal 25 GDPR menyatakan bahwa pengontrol “harus menerapkan langkah-langkah teknis dan organisasional yang tepat untuk memastikan bahwa, secara default, hanya data pribadi yang diperlukan untuk setiap tujuan spesifik pemrosesan yang diproses.” Mekanisme kontrol akses AWS berikut dapat membantu pelanggan mematuhi persyaratan ini dengan hanya mengizinkan administrator, pengguna, dan aplikasi yang sah untuk mendapatkan akses ke sumber daya AWS dan data pelanggan.

AWS Identity and Access Management

Saat Anda membuat akun AWS, akun pengguna root dibuat secara otomatis untuk akun AWS Anda. Akun pengguna ini memiliki akses lengkap ke semua layanan dan sumber daya AWS Anda di akun AWS Anda. Alih-alih menggunakan akun ini untuk tugas sehari-hari, Anda seharusnya hanya menggunakannya untuk awalnya membuat peran dan akun pengguna tambahan, serta untuk aktivitas administratif yang memerlukannya. AWS merekomendasikan agar Anda menerapkan prinsip hak akses paling rendah sejak awal: tentukan akun dan peran pengguna yang berbeda untuk tugas yang berbeda, dan tentukan set izin minimum yang diperlukan untuk menyelesaikan setiap tugas. Pendekatan ini adalah mekanisme untuk menyesuaikan konsep utama yang diberlakukan di GDPR: perlindungan data secara desain. AWS Identity and Access Management(IAM) adalah layanan web yang dapat Anda gunakan untuk mengontrol akses ke sumber daya AWS Anda dengan aman.

Pengguna dan peran menentukan identitas IAM dengan izin tertentu. Pengguna yang berwenang dapat mengambil IAM role untuk melakukan tugas-tugas tertentu. Kredensial sementara dibuat ketika peran diambil. Misalnya, Anda dapat menggunakan IAM role untuk menyediakan aplikasi yang berjalan dengan aman di Amazon Elastic Compute Cloud (Amazon EC2) dengan kredensial sementara yang diperlukan untuk mengakses sumber daya AWS lainnya, seperti bucket Amazon S3, dan Amazon Relational Database Service (Amazon RDS) atau basis data Amazon DynamoDB. Demikian pula, peran eksekusi menyediakan izin yang diperlukan ke fungsi AWS Lambda untuk mengakses Layanan AWS dan sumber daya lainnya, seperti Amazon CloudWatch Logs untuk streaming log atau membaca pesan dari antrean Amazon Simple Queue Service (Amazon SQS). Saat membuat peran, Anda menambahkan kebijakan untuk menentukan otorisasi.

Untuk membantu pelanggan memantau kebijakan sumber daya dan mengidentifikasi sumber daya yang memiliki akses publik atau lintas akun yang mungkin tidak mereka inginkan, IAM Access Analyzer dapat diaktifkan untuk menghasilkan temuan komprehensif yang mengidentifikasi sumber

daya yang dapat diakses dari luar akun AWS. IAM Access Analyzer mengevaluasi kebijakan sumber daya dengan logika dan inferensi matematika untuk menentukan jalur akses yang diizinkan oleh kebijakan. IAM Access Analyzer terus memantau kebijakan baru atau yang diperbarui, dan menganalisis izin yang diberikan menggunakan kebijakan untuk IAM role—tetapi juga untuk sumber daya layanan seperti bucket Amazon S3, kunci AWS Key Management Service (AWS KMS), antrean Amazon SQS, dan fungsi Lambda.

Access Analyzer for S3 memberi tahu Anda ketika bucket dikonfigurasi untuk memungkinkan akses bagi siapa pun di internet atau akun AWS lainnya, termasuk akun AWS di luar organisasi Anda. Saat meninjau bucket berisiko di Access Analyzer untuk Amazon S3, Anda dapat memblokir semua akses publik ke bucket dengan sekali klik. AWS menyarankan agar Anda memblokir semua akses ke bucket Anda kecuali Anda memerlukan akses publik untuk mendukung kasus penggunaan tertentu. Sebelum Anda memblokir semua akses publik, pastikan bahwa aplikasi Anda akan terus bekerja dengan benar tanpa akses publik. Untuk informasi selengkapnya, lihat Menggunakan Amazon S3 untuk Memblokir Akses Publik.

IAM juga menyediakan informasi yang terakhir diakses untuk membantu Anda mengidentifikasi izin yang tidak digunakan sehingga Anda dapat menghapusnya dari entitas utama terkait. Menggunakan informasi yang terakhir diakses, Anda dapat menyempurnakan kebijakan Anda dan mengizinkan akses hanya ke layanan dan tindakan yang diperlukan. Ini membantu dalam meningkatkan kepatuhan dan menerapkan praktik terbaik hak akses paling rendah. Anda dapat melihat informasi yang terakhir diakses untuk entitas atau kebijakan yang ada di IAM, atau di seluruh lingkungan AWS Organizations.

Token Akses Sementara Melalui AWS STS

Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk membuat dan menyediakan kredensial keamanan sementara bagi pengguna tepercaya yang memberikan akses ke sumber daya AWS Anda. Kredensial keamanan sementara bekerja hampir identik dengan kredensial kunci akses jangka panjang yang dapat digunakan pengguna IAM Anda, dengan perbedaan berikut:

- Kredensial keamanan sementara ditujukan untuk penggunaan jangka pendek. Anda dapat mengonfigurasi jumlah waktu yang valid, dari 15 menit hingga maksimal 12 jam. Setelah kredensial sementara kedaluwarsa, AWS tidak mengenalinya atau mengizinkan akses apa pun dari permintaan API yang dibuat dengan kredensial ini.
- Kredensial keamanan sementara tidak disimpan dengan akun pengguna. Sebagai gantinya, kredensial ini dihasilkan secara dinamis dan diberikan kepada pengguna ketika diminta. Ketika

(atau sebelum) kredensial keamanan sementara kedaluwarsa, pengguna dapat meminta kredensial baru, jika pengguna tersebut memiliki izin untuk melakukannya.

Perbedaan ini memberikan keuntungan sebagai berikut saat Anda menggunakan kredensial sementara:

- Anda tidak perlu mendistribusikan atau menanamkan kredensial keamanan AWS jangka panjang dengan aplikasi.
- Kredensial sementara adalah dasar untuk peran dan federasi identitas. Anda dapat menyediakan akses bagi pengguna ke sumber daya AWS Anda dengan mendefinisikan identitas AWS sementara untuk mereka.
- Kredensial keamanan sementara memiliki masa aktif terbatas yang dapat disesuaikan. Karena itu, Anda tidak perlu merotasi kredensial ini atau secara eksplisit mencabutnya ketika sudah tidak lagi diperlukan. Setelah kredensial keamanan sementara berakhir, kredensial ini tidak dapat digunakan kembali. Anda dapat menentukan jumlah waktu maksimum validitas kredensial.

Autentikasi Multi-Faktor (MFA)

Untuk keamanan ekstra, Anda dapat menambahkan autentikasi dua faktor ke akun AWS Anda dan pengguna IAM. Dengan autentikasi multi-faktor (MFA) diaktifkan, ketika Anda masuk ke Konsol Manajemen AWS, Anda diminta memasukkan nama pengguna dan kata sandi Anda (faktor pertama), serta respons autentikasi dari perangkat AWS MFA Anda (faktor kedua). Anda dapat mengaktifkan MFA untuk akun AWS dan untuk pengguna IAM perorangan yang telah dibuat di akun Anda. Anda juga dapat menggunakan MFA untuk mengontrol akses ke API layanan AWS.

Misalnya, Anda dapat menentukan kebijakan yang memungkinkan akses penuh ke semua operasi API AWS di Amazon EC2, tetapi secara eksplisit menolak akses ke operasi API tertentu—seperti `StopInstances` dan `TerminateInstances`—jika pengguna tidak diautentikasi dengan MFA.

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
     {
        “Sid”: “AllowAllActionsForEC2”,
        “Effect”: “Allow”,
        “Action”: “ec2:*”,
        “Resource”: “*”
```

```
            },
            {
                "Sid": "DenyStopAndTerminateWhenMFAIsNotPResent",
                "Effect": "Deny",
                "Action": [
                    "ec2:StopInstances",
                    "ec2:TerminateInstances"
                ],
                "Resource": "*",
                "Conditions": {
                    "BoolIfExists": {"aws:MultiFactorAuthPresent":false}
                }
            }
        }
}
```

Untuk menambahkan lapisan keamanan tambahan ke bucket Amazon S3, Anda dapat mengonfigurasi MFA Delete, yang memerlukan autentikasi tambahan untuk mengubah status versioning bucket dan menghapus versi objek secara permanen. MFA Delete menyediakan keamanan tambahan jika kredensial keamanan Anda bocor.

Untuk menggunakan MFA Delete, Anda dapat menggunakan perangkat keras atau perangkat MFA virtual untuk menghasilkan kode autentikasi. Lihat halaman Autentikasi Multi-Faktor untuk daftar perangkat keras atau perangkat MFA virtual yang didukung.

Akses ke Sumber Daya AWS

Untuk menerapkan akses granular ke sumber daya AWS Anda, Anda dapat memberikan tingkat izin yang berbeda kepada orang yang berbeda untuk sumber daya yang berbeda. Misalnya, Anda dapat memberikan akses lengkap hanya untuk beberapa pengguna ke Amazon EC2, Amazon S3, DynamoDB, Amazon Redshift, dan Layanan AWS lainnya.

Untuk pengguna lain, Anda dapat memberikan akses hanya-baca hanya ke beberapa bucket Amazon S3; izin untuk mengelola hanya beberapa instans Amazon EC2, atau akses hanya ke informasi penagihan Anda.

Kebijakan berikut adalah contoh dari satu metode yang dapat Anda gunakan untuk mengizinkan semua tindakan pada bucket Amazon S3 tertentu dan secara eksplisit menolak akses ke setiap layanan AWS yang bukan Amazon S3.

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Action”: “s3:*”,
                “Resource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ],
              },
              {
                “Effect”: “Deny”,
                “NotAction”: “s3:*”,
                “NotResource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ]
               }
            ]
}
```

Anda dapat melampirkan kebijakan ke akun pengguna atau peran. Untuk contoh kebijakan IAM lainnya, lihat Contoh Kebijakan Berbasis Identitas IAM.

Mendefinisikan Batas untuk Akses Layanan Regional

Sebagai pelanggan, Anda menjaga kepemilikan konten Anda dan memilih layanan AWS mana yang dapat memproses, menyimpan, dan meng-host konten Anda. AWS tidak mengakses atau menggunakan konten Anda untuk tujuan apa pun tanpa persetujuan Anda. Berdasarkan Model Tanggung Jawab Bersama, Anda memilih Wilayah AWS tempat konten disimpan, memungkinkan Anda men-deploy layanan AWS di lokasi pilihan Anda, sesuai dengan persyaratan geografis spesifik Anda. Misalnya, jika Anda ingin memastikan konten Anda hanya berada di Eropa, Anda dapat memilih untuk men-deploy layanan AWS secara eksklusif di salah satu Wilayah AWS Eropa.

Kebijakan IAM menyediakan mekanisme sederhana untuk membatasi akses ke layanan di Wilayah tertentu. Anda dapat menambahkan syarat global (`aws:RequestedRegion`) ke kebijakan IAM yang dilampirkan pada Entitas Utama IAM Anda untuk memberlakukan syarat ini untuk semua layanan

AWS. Misalnya, kebijakan berikut menggunakan `NotAction` elemen dengan efek `Deny`, yang secara eksplisit menolak akses ke semua tindakan yang tidak tercantum dalam pernyataan jika Wilayah yang diminta bukan Eropa. Tindakan di layanan CloudFront, IAM, Amazon Route 53, dan AWS Support tidak boleh ditolak karena ini adalah layanan global AWS yang populer.

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Sid”: “DenyAllOutsideRequestedRegions”,
                “Effect”: “Deny”,
                “NotAction”: [
                     “cloudfront:*”,
                     “iam:*”,
                     ”route53:*”,
                     “support:*”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “StringNotLike”: {
                        “aws:RequestedRegion”: [
                              “eu-*”
                        ]
                    }
                 }
           }
          ]
}
```

Contoh kebijakan IAM ini juga dapat diimplementasikan sebagai Kebijakan Kontrol Layanan (SCP) di AWS Organizations, yang mendefinisikan batas izin yang diterapkan pada akun AWS atau Unit Organisasi (OU) tertentu dalam suatu organisasi. Hal ini memungkinkan Anda mengontrol akses pengguna ke layanan regional di lingkungan multi-akun yang kompleks.

Kemampuan pembatasan geografis ada untuk Wilayah yang baru diluncurkan. Wilayah yang diperkenalkan setelah 20 Maret 2019 dinonaktifkan secara default. Anda harus mengaktifkan Wilayah ini sebelum Anda dapat menggunakannya. Jika Wilayah AWS dinonaktifkan secara default, Anda dapat menggunakan Konsol Manajemen AWS untuk mengaktifkan dan menonaktifkan Wilayah. Mengaktifkan dan menonaktifkan Wilayah AWS memungkinkan Anda mengontrol apakah

pengguna di akun AWS Anda dapat mengakses sumber daya di Wilayah tersebut. Untuk informasi selengkapnya, lihat Mengelola Wilayah AWS.

Kontrol Akses ke Aplikasi Web dan Aplikasi Seluler

AWS menyediakan layanan untuk mengelola kontrol akses data dalam aplikasi pelanggan. Jika Anda perlu menambahkan fitur login dan kontrol akses pengguna ke aplikasi web dan aplikasi seluler, Anda dapat menggunakan Amazon Cognito. Pool pengguna Amazon Cognito menyediakan direktori pengguna aman yang dapat diskalakan ke ratusan juta pengguna. Untuk melindungi identitas pengguna, Anda dapat menambahkan autentikasi multi-faktor (MFA) ke pool pengguna Anda. Anda juga dapat menggunakan autentikasi adaptif, yang menggunakan model berbasis risiko untuk memprediksi kapan Anda mungkin memerlukan faktor autentikasi lain.

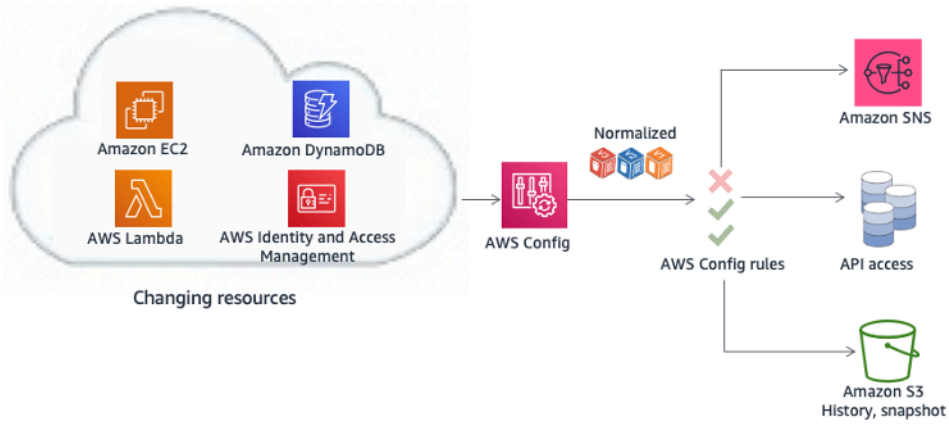
Dengan Amazon Cognito Identity Pools (Identitas Terfederasi), Anda dapat melihat siapa yang mengakses sumber daya Anda dan tempat aksesnya berasal (aplikasi seluler atau aplikasi web). Anda dapat menggunakan informasi ini untuk membuat IAM role dan kebijakan IAM yang mengizinkan atau menolak akses ke sumber daya berdasarkan jenis asal akses (aplikasi seluler atau aplikasi web) dan Penyedia Identitas.

Pemantauan dan Pencatatan Log

Pasal 30 GDPR menyatakan bahwa “... setiap pengontrol dan, jika berlaku, perwakilan pengontrol, harus menyimpan catatan aktivitas pemrosesan di bawah tanggung jawabnya”. Artikel ini juga mencakup detail tentang informasi mana yang harus dicatat saat Anda memantau pemrosesan semua data pribadi. Pengontrol dan pemroses juga diwajibkan untuk mengirim notifikasi pelanggaran pada waktu yang tepat, sehingga mendeteksi insiden dengan cepat sangatlah penting. Untuk membantu pelanggan mematuhi kewajiban ini, AWS menawarkan layanan pemantauan dan pencatatan log berikut.

Mengelola dan Mengonfigurasi Aset dengan AWS Config

AWS Config memberikan gambaran mendetail tentang konfigurasi berbagai jenis sumber daya AWS di akun AWS Anda. Ini termasuk bagaimana sumber daya terkait satu sama lain dan bagaimana sumber daya dikonfigurasikan sebelumnya sehingga Anda dapat melihat bagaimana konfigurasi dan hubungan ini berubah dari waktu ke waktu.



Gambar 1 – Memantau perubahan konfigurasi dari waktu ke waktu dengan AWS Config

Sumber daya AWS adalah entitas yang dapat Anda gunakan di AWS, seperti instans EC2, volume Amazon Elastic Block Store (Amazon EBS), grup keamanan, atau Amazon Virtual Private Cloud (Amazon VPC). Untuk daftar lengkap sumber daya AWS yang didukung oleh AWS Config, lihat Jenis Sumber Daya AWS yang Didukung.

Dengan AWS Config, Anda dapat melakukan hal berikut:

- Mengevaluasi konfigurasi sumber daya AWS Anda untuk memverifikasi bahwa pengaturan sudah benar.

- Mendapatkan snapshot konfigurasi saat ini dari sumber daya yang didukung terkait dengan Akun AWS Anda.
- Mendapatkan konfigurasi dari satu atau beberapa sumber daya yang ada di akun Anda.
- Mendapatkan konfigurasi historis dari satu atau beberapa sumber daya.
- Menerima notifikasi saat sumber daya dibuat, dimodifikasi, atau dihapus.
- Melihat hubungan di antara sumber daya. Misalnya, menemukan semua sumber daya yang menggunakan grup keamanan tertentu.

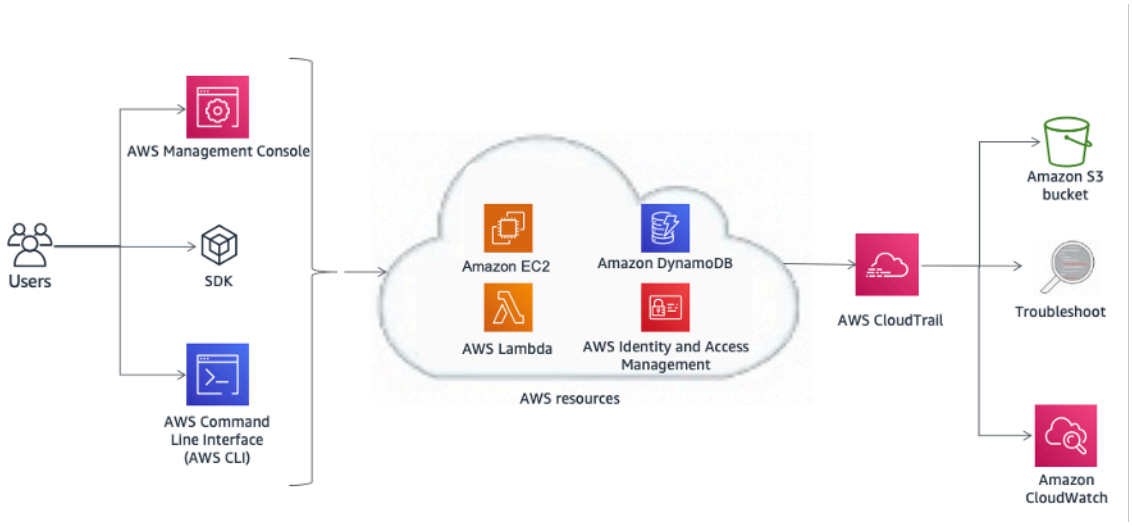
Audit Kepatuhan dan Analisis Keamanan

Dengan AWS CloudTrail, Anda dapat terus memantau aktivitas akun AWS. Riwayat panggilan API AWS untuk akun Anda akan ditangkap, termasuk panggilan API yang dilakukan melalui Konsol Manajemen AWS, SDK AWS, alat baris perintah, dan layanan AWS tingkat lebih tinggi. Anda dapat mengidentifikasi pengguna dan akun mana yang memanggil API AWS untuk layanan yang mendukung CloudTrail, alamat IP sumber yang digunakan untuk membuat panggilan, dan kapan panggilan ini terjadi. Anda dapat mengintegrasikan CloudTrail ke dalam aplikasi menggunakan API, mengotomasi pembuatan jejak untuk organisasi Anda, memeriksa status jejak Anda, dan mengontrol bagaimana administrator mengaktifkan dan menonaktifkan pencatatan log CloudTrail.

Log CloudTrail dapat digabungkan dari beberapa Wilayah dan beberapa akun AWS ke dalam satu bucket Amazon S3. AWS merekomendasikan agar Anda menulis log—terutama log AWS CloudTrail—ke bucket Amazon S3 dengan akses terbatas di akun AWS yang ditetapkan untuk pencatatan log (Log Archive). Izin pada bucket harus mencegah penghapusan log, dan izin juga harus dienkripsi secara at rest menggunakan Enkripsi Sisi Server dengan kunci enkripsi terkelola Amazon S3 (SSE-S3) atau Enkripsi Sisi Server dengan kunci terkelola AWS KMS—(SSE-KMS). Validasi integritas file log CloudTrail dapat digunakan untuk menentukan apakah file log dimodifikasi, dihapus, atau tidak berubah setelah CloudTrail mengirimkannya. Fitur ini dibangun menggunakan algoritme standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Hal ini akan membuat file log CT secara komputasional sulit untuk dimodifikasi, dihapus, atau dipalsukan; dan pasti akan memicu deteksi. Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk memvalidasi file di lokasi tempat CloudTrail mengirimkannya.

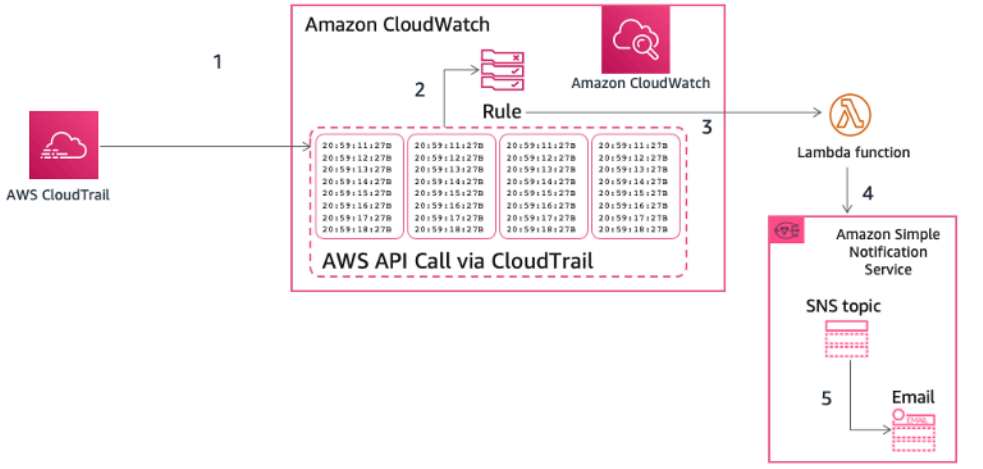
Log CloudTrail yang digabungkan dalam bucket Amazon S3 dapat dianalisis untuk tujuan audit atau untuk aktivitas pemecahan masalah. Setelah log menjadi terpusat, Anda dapat berintegrasi dengan solusi Security Information and Event Management (SIEM) atau menggunakan layanan AWS, seperti Amazon Athena atau CloudTrail Insights, untuk menganalisis dan memvisualisasikannya

menggunakan Amazon QuickSight Dasbor. Setelah log CloudTrail menjadi terpusat, Anda juga dapat menggunakan akun Log Archive yang sama untuk memusatkan log dari sumber lain, seperti CloudWatch Logs dan penyeimbang beban AWS.



Gambar 2 – Contoh arsitektur untuk audit kepatuhan dan analisis keamanan dengan AWS CloudTrail

Log AWS CloudTrail juga dapat memicu peristiwa Amazon CloudWatch yang telah dikonfigurasi sebelumnya. Anda dapat menggunakan peristiwa ini untuk memberi tahu pengguna atau sistem bahwa suatu peristiwa telah terjadi, atau untuk tindakan perbaikan. Misalnya, jika ingin memantau aktivitas di instans Amazon EC2, Anda dapat membuat aturan CloudWatch Event. Ketika aktivitas tertentu terjadi pada instans Amazon EC2 dan peristiwa ini ditangkap di log, aturan tersebut akan memicu fungsi AWS Lambda, yang mengirimkan email notifikasi tentang peristiwa tersebut ke administrator. (Lihat Gambar 3.) Email ini mencakup detail seperti kapan peristiwa terjadi, pengguna mana yang melakukan tindakan, detail Amazon EC2, dan banyak lagi. Diagram berikut menunjukkan arsitektur notifikasi peristiwa.



Gambar 3 – Contoh notifikasi peristiwa AWS CloudTrail

Mengumpulkan dan Memproses Log

CloudWatch Logs dapat digunakan untuk memantau, menyimpan, dan mengakses file log Anda dari instans Amazon EC2, AWS CloudTrail, Route 53, dan sumber lainnya. Lihat halaman dokumentasi Layanan AWS yang Memublikasikan Log ke CloudWatch Logs.

Informasi log meliputi, misalnya:

- Pencatatan log yang terperinci untuk akses ke objek Amazon S3
- Informasi mendetail tentang alur dalam jaringan melalui VPC-FlowLogs
- Verifikasi konfigurasi berbasis aturan dan tindakan dengan aturan AWS Config
- Pemfilteran dan pemantauan akses HTTP ke aplikasi dengan fungsi firewall aplikasi web (WAF) di CloudFront

Metrik dan log aplikasi kustom juga dapat dipublikasikan ke CloudWatch Logs dengan menginstal CloudWatch Agent di instans Amazon EC2 atau server on-premise.

Log dapat dianalisis secara interaktif menggunakan CloudWatch Logs Insights, dengan melakukan kueri untuk membantu Anda merespons secara lebih efisien dan efektif terhadap masalah operasional.

CloudWatch Logs dapat diproses hampir dalam waktu nyata dengan mengonfigurasi filter langganan dan dapat dikirim ke layanan lain seperti klaster Amazon OpenSearch Service (OpenSearch Service), stream Amazon Kinesis, stream Amazon Kinesis Data Firehose, atau Lambda untuk pemrosesan kustom, analisis, atau pemuatan ke sistem lain.

Filter metrik CloudWatch dapat digunakan untuk menentukan pola guna mencari data log, mengubahnya menjadi metrik CloudWatch numerik, dan mengatur alarm berdasarkan kebutuhan bisnis Anda. Misalnya, dengan mengikuti rekomendasi AWS untuk tidak menggunakan pengguna root untuk tugas sehari-hari, filter metrik CloudWatch tertentu dapat disiapkan pada log CloudTrail (dikirim ke CloudWatch Logs) untuk membuat metrik Kustom dan mengonfigurasi alarm untuk memberi tahu pemangku kepentingan yang relevan saat kredensial root digunakan untuk mengakses akun AWS Anda.

Log seperti log akses server Amazon S3, log akses Elastic Load Balancing, log stream VPC, dan log stream AWS Global Accelerator dapat dikirim langsung ke bucket Amazon S3. Misalnya, ketika Anda

mengaktifkan log akses server Amazon Simple Storage Service, Anda bisa mendapatkan informasi mendetail mengenai permintaan yang dibuat ke bucket Amazon S3 Anda. Catatan log akses berisi detail permintaan, seperti jenis permintaan, sumber daya yang ditentukan dalam permintaan, dan waktu dan tanggal permintaan diproses. Untuk informasi selengkapnya tentang konten pesan log, lihat Format Log Akses Server Amazon Simple Storage Service dalam Panduan Developer Amazon Simple Storage Service. Log akses server berguna untuk banyak aplikasi karena memberikan wawasan kepada pemilik bucket tentang sifat permintaan yang dibuat oleh klien yang tidak di bawah kontrol mereka. Secara default, Amazon S3 tidak mengumpulkan log akses layanan, tetapi ketika Anda mengaktifkan pencatatan log, Amazon S3 biasanya mengirimkan log akses ke bucket Anda dalam beberapa jam. Jika Anda memerlukan pengiriman yang lebih cepat atau perlu mengirimkan log ke beberapa tujuan, pertimbangkan untuk menggunakan log CloudTrail atau kombinasi log CloudTrail dan Amazon S3. Log dapat dienkripsi at rest dengan mengonfigurasi enkripsi objek default di bucket tujuan. Objek dienkripsi menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 (SSE-S3) atau kunci utama pelanggan (CMK) yang disimpan dalam AWS Key Management Service (AWS KMS).

Log yang disimpan dalam bucket Amazon S3 dapat dikueri dan dianalisis menggunakan Amazon Athena. Amazon Athena adalah layanan kueri interaktif yang memungkinkan Anda menganalisis data di S3 menggunakan SQL standar. Anda dapat menggunakan Athena untuk menjalankan kueri khusus menggunakan ANSI SQL, tanpa perlu menggabungkan atau memuat data ke dalam Athena. Athena dapat memproses set data yang tidak terstruktur, semi-terstruktur, dan terstruktur dan terintegrasi dengan Amazon QuickSight untuk visualisasi yang mudah.

Log juga merupakan sumber informasi yang berguna untuk deteksi ancaman otomatis. Amazon GuardDuty adalah layanan pemantauan keamanan berkelanjutan yang menganalisis dan memproses peristiwa dari beberapa sumber, seperti VPC Flow Logs, log peristiwa manajemen CloudTrail, log peristiwa data CloudTrail Amazon S3, dan log DNS. Layanan ini menggunakan umpan intelijen ancaman, seperti daftar alamat IP dan domain berbahaya, serta machine learning untuk mengidentifikasi aktivitas yang tidak terduga serta berpotensi tidak sah dan berbahaya dalam lingkungan AWS Anda. Saat Anda mengaktifkan GuardDuty di sebuah Wilayah, layanan ini akan langsung mulai menganalisis log peristiwa CloudTrail Anda. Layanan ini menyerap peristiwa manajemen CloudTrail dan peristiwa data Amazon S3 langsung dari CloudTrail melalui stream peristiwa yang independen dan duplikatif.

Menemukan dan Melindungi Data dalam Skala Besar dengan Amazon Macie

Pasal 32 GDPR menyatakan bahwa "…pengontrol dan pemroses harus menerapkan langkah-langkah teknis dan organisasional yang tepat untuk memastikan tingkat keamanan yang sesuai dengan risiko, termasuk antara lain sebagaimana diperlukan: […]

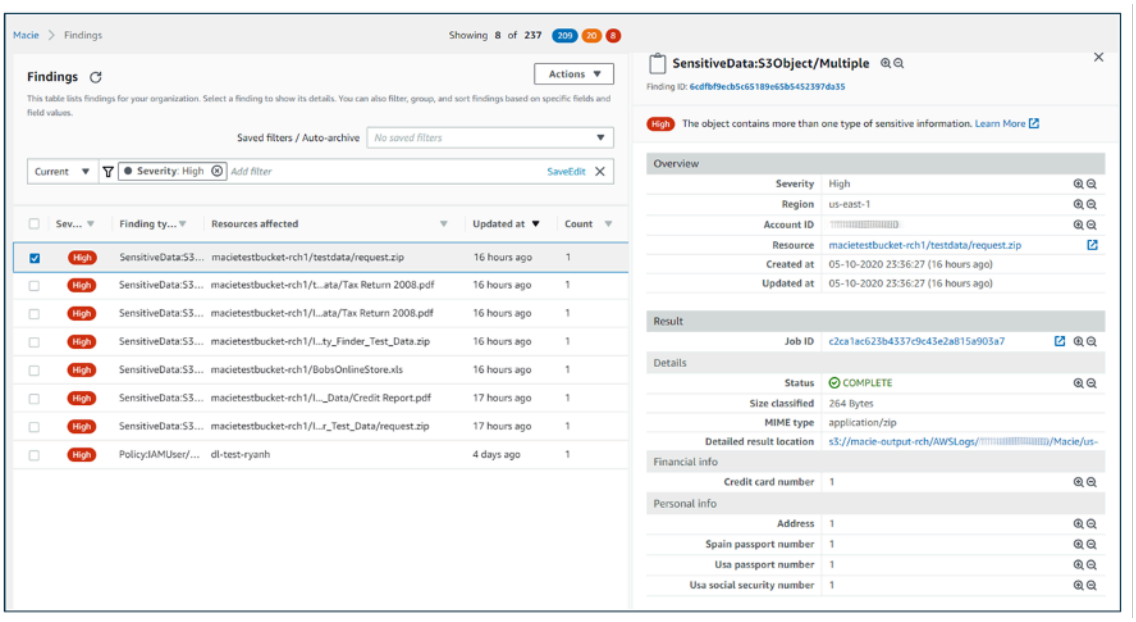
(b) kemampuan untuk memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan yang berkelanjutan dari sistem dan layanan pemrosesan;

[…]

(d) suatu proses untuk menguji, menilai, dan mengevaluasi efektivitas langkah-langkah teknis dan organisasional secara teratur untuk memastikan keamanan pemrosesan."

Memiliki proses klasifikasi data yang berkelanjutan sangat penting untuk menyesuaikan pemrosesan data keamanan dengan sifat data. Jika organisasi Anda mengelola data sensitif, pantau tempat data tersebut berada, lindungi dengan benar, dan berikan bukti bahwa Anda menerapkan keamanan dan privasi data sesuai kebutuhan untuk memenuhi persyaratan kepatuhan peraturan. Untuk membantu pelanggan mengidentifikasi dan melindungi data sensitif mereka dalam skala besar, AWS menawarkan Amazon Macie, layanan keamanan data dan privasi data terkelola penuh yang menggunakan model pencocokan pola dan machine learning untuk mendeteksi Informasi Pengenal Pribadi (PII) untuk menemukan dan melindungi data sensitif yang disimpan dalam bucket S3. Amazon Macie memindai bucket ini dan menyediakan kategorisasi data menggunakan pengidentifikasi data terkelola yang dirancang untuk mendeteksi beberapa kategori data sensitif. Macie dapat mendeteksi PII seperti nama lengkap, alamat email, tanggal lahir, nomor tanda pengenal nasional, nomor tanda pengenal atau referensi wajib pajak, dan banyak lagi. Pelanggan dapat menentukan pengidentifikasi data kustom yang mencerminkan skenario tertentu organisasi mereka (misalnya, nomor akun pelanggan atau klasifikasi data internal).

Amazon Macie terus mengevaluasi objek di dalam bucket dan secara otomatis memberikan ringkasan temuan (Gambar 4) untuk data yang tidak terenkripsi atau dapat diakses publik yang cocok dengan kategori data yang ditentukan. Data ini dapat mencakup peringatan untuk objek atau bucket yang tidak terenkripsi dan dapat diakses publik yang dibagikan ke akun AWS yang berada di luar organisasi yang telah Anda tetapkan dalam AWS Organizations. Amazon Macie terintegrasi dengan layanan AWS lainnya, seperti AWS Security Hub, untuk menghasilkan temuan keamanan yang dapat ditindaklanjuti dan memberikan tindakan otomatis dan reaktif terhadap temuan tersebut (Gambar 5).



Gambar 4 – Inspeksi data dan contoh temuan

Manajemen Keamanan yang Terpusat:

Banyak organisasi memiliki tantangan yang terkait dengan visibilitas dan manajemen terpusat untuk lingkungan mereka. Seiring pertumbuhan jejak operasional Anda, tantangan ini dapat diperparah kecuali jika Anda mempertimbangkan desain keamanan Anda dengan hati-hati. Kurangnya pengetahuan, dikombinasikan dengan pengelolaan proses tata kelola dan keamanan yang terdesentralisasi dan tidak merata, dapat membuat lingkungan Anda rentan.

AWS menyediakan alat yang membantu Anda mengatasi beberapa persyaratan yang paling menantang untuk manajemen dan tata kelola IT, serta alat untuk mendukung pendekatan perlindungan data secara desain.

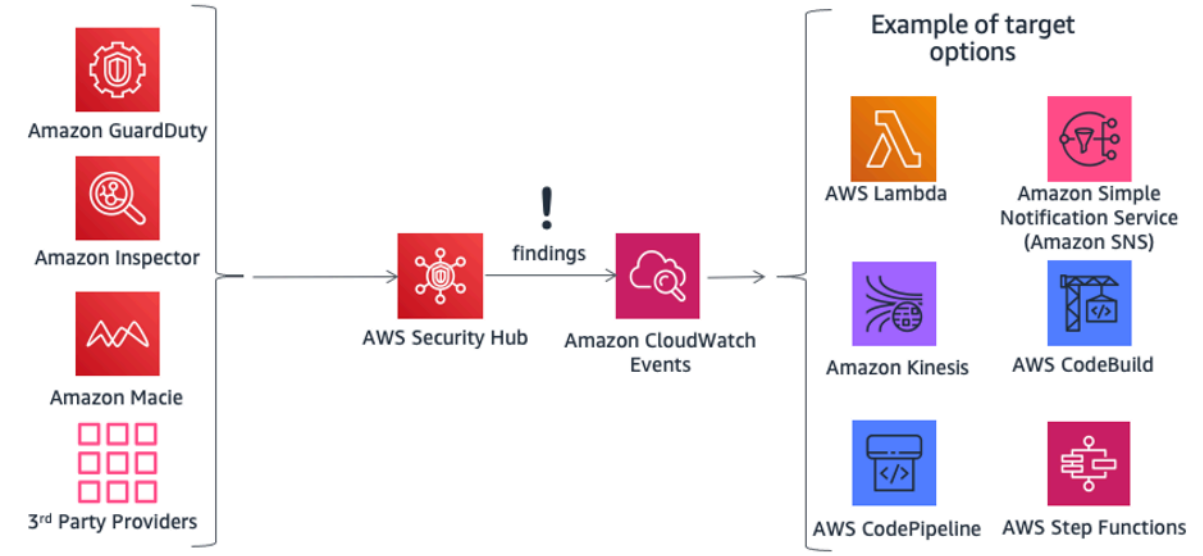
AWS Control Tower menyediakan metode untuk menyiapkan dan mengatur lingkungan AWS multi akun baru yang aman. Layanan ini mengotomatisasi pengaturan zona landasan, yang merupakan lingkungan multi-akun yang didasarkan pada cetak biru praktik terbaik, dan memungkinkan tata kelola menggunakan pagar pembatas yang dapat Anda pilih dari daftar bawaan. Guardrails menerapkan aturan tata kelola untuk keamanan, kepatuhan, dan operasi. AWS Control Tower menyediakan manajemen identitas menggunakan direktori default AWS IAM Identity Center (IAM Identity Center) dan memungkinkan audit lintas akun menggunakan IAM Identity Center dan IAM. Layanan ini juga memusatkan log yang berasal dari CloudTrail dan log AWS Config, yang disimpan di Amazon S3.

AWS Security Hub adalah layanan lain yang mendukung sentralisasi dan dapat meningkatkan visibilitas terkait organisasi. Security Hub memusatkan dan memprioritaskan temuan keamanan dan kepatuhan dari seluruh akun dan layanan AWS, seperti Amazon GuardDuty dan Amazon Inspector, dan dapat diintegrasikan dengan perangkat lunak keamanan dari partner pihak ketiga untuk membantu Anda menganalisis tren keamanan dan mengidentifikasi masalah keamanan prioritas tertinggi.

Amazon GuardDuty adalah layanan deteksi ancaman cerdas yang dapat membantu pelanggan memantau dan melindungi akun AWS, beban kerja, dan data AWS mereka yang disimpan di Amazon S3. GuardDuty menganalisis miliaran peristiwa di seluruh akun AWS Anda dari beberapa sumber, termasuk Peristiwa Manajemen AWS CloudTrail, Peristiwa Data Amazon S3 CloudTrail, Amazon Virtual Cloud Flow Logs, dan log DNS. Misalnya, layanan ini mendeteksi panggilan API yang tidak biasa, komunikasi keluar yang mencurigakan ke alamat IP berbahaya yang diketahui, atau kemungkinan pencurian data dengan menggunakan kueri DNS sebagai mekanisme pengangkutan. GuardDuty mampu memberikan temuan yang lebih akurat dengan memanfaatkan intelijen ancaman yang didukung machine learning dan partner keamanan pihak ketiga.

Amazon Inspector adalah layanan penilaian keamanan otomatis yang membantu meningkatkan keamanan dan kepatuhan aplikasi yang di-deploy di instans Amazon EC2. Amazon Inspector secara otomatis menilai aplikasi untuk paparan, kelemahan, dan penyimpangan dari praktik terbaik. Setelah melakukan penilaian, Amazon Inspector membuat daftar detail temuan keamanan yang diprioritaskan berdasarkan tingkat keparahan.

Amazon CloudWatch Events memungkinkan Anda mengatur akun AWS Anda untuk mengirim peristiwa ke akun AWS lain, atau menjadi penerima peristiwa dari akun atau organisasi lain. Mekanisme ini dapat sangat berguna untuk menerapkan skenario respons insiden lintas-akun, dengan mengambil tindakan korektif yang tepat waktu (misalnya, dengan memanggil fungsi Lambda, atau menjalankan perintah pada instans Amazon EC2) sebagaimana diperlukan setiap kali terjadi peristiwa insiden keamanan.



Gambar 5 – Mengambil tindakan dengan AWS Security Hub dan Amazon CloudWatch Events

AWS Organizations membantu Anda mengelola dan mengatur lingkungan yang kompleks secara terpusat. Layanan ini memungkinkan Anda mengontrol akses, kepatuhan, dan keamanan di lingkungan multi-akun. AWS Organizations mendukung Kebijakan Kontrol Layanan (SCP), yang menentukan tindakan layanan AWS yang tersedia untuk digunakan dengan akun atau Unit Organisasi (OU) tertentu dalam suatu organisasi.

AWS Systems Manager memberi Anda visibilitas dan kontrol terhadap infrastruktur Anda di AWS. Anda dapat melihat data operasional dari beberapa layanan AWS dari konsol terpadu dan mengotomatiskan tugas operasional di seluruh layanan tersebut. Anda dapat memiliki informasi tentang aktivitas API terbaru, perubahan konfigurasi sumber daya, pemberitahuan operasional, inventaris perangkat lunak, dan status kepatuhan patch. Melalui integrasi dengan layanan AWS lainnya, Anda juga dapat mengambil tindakan pada sumber daya tergantung pada kebutuhan operasional Anda, untuk membantu menjadikan lingkungan Anda dalam status kepatuhan.

Misalnya, dengan mengintegrasikan Amazon Inspector dengan AWS Systems Manager, penilaian keamanan disederhanakan dan otomatis, karena Anda dapat menginstal agen Amazon Inspector secara otomatis menggunakan Amazon Elastic Compute Cloud Systems Manager saat instans Amazon EC2 diluncurkan. Anda juga dapat melakukan perbaikan otomatis untuk temuan Amazon Inspector dengan menggunakan fungsi Amazon EC2 System Manager dan Lambda.

Melindungi Data Anda di AWS

Pasal 32 GDPR mewajibkan bahwa organisasi harus "…menerapkan langkah-langkah teknis dan organisasional yang tepat untuk memastikan tingkat keamanan yang sesuai dengan risiko, termasuk …pseudonimisasi dan enkripsi data pribadi[…]". Selain itu, organisasi harus memberi perlindungan terhadap pengungkapan atau akses yang tidak sah ke data pribadi."

Enkripsi mengurangi risiko yang terkait dengan penyimpanan data pribadi karena data tidak dapat dibaca tanpa kunci yang benar. Strategi enkripsi yang menyeluruh dapat membantu mengurangi dampak dari berbagai peristiwa keamanan, termasuk beberapa pelanggaran keamanan.

Enkripsi Data At Rest

Mengenkripsi data at rest sangat penting untuk kepatuhan peraturan dan perlindungan data. Ini membantu memastikan bahwa data sensitif yang disimpan pada disk tidak dapat dibaca oleh pengguna atau aplikasi tanpa kunci yang valid. AWS menyediakan beberapa opsi untuk enkripsi at rest dan manajemen kunci enkripsi. Misalnya, Anda dapat menggunakan SDK AWS Encryption dengan CMK yang dibuat dan dikelola AWS KMS untuk mengenkripsi data arbitrer.

Data terenkripsi dapat disimpan dengan aman secara at rest dan dapat didekripsi hanya oleh pihak dengan akses resmi ke CMK. Sebagai hasilnya, Anda mendapatkan data rahasia yang dienkripsi dengan envelope, mekanisme kebijakan untuk otorisasi dan enkripsi yang diautentikasi, dan pencatatan log audit melalui AWS CloudTrail. Sebagian layanan fondasi AWS memiliki fitur enkripsi at rest bawaan, sehingga memberikan opsi untuk mengenkripsi data sebelum ditulis ke penyimpanan non-volatil. Contohnya, Anda bisa mengenkripsi volume Amazon EBS dan mengonfigurasi bucket Amazon S3 untuk Enkripsi Sisi Server (SSE) menggunakan enkripsi AES-256. Amazon S3 juga mendukung enkripsi sisi klien, yang memungkinkan Anda mengenkripsi data sebelum mengirimkannya ke Amazon S3. SDK AWS mendukung enkripsi sisi klien untuk memfasilitasi operasi enkripsi dan dekripsi objek. Amazon RDS juga mendukung Enkripsi Data Transparan (TDE).

Enkripsi data dapat dilakukan di penyimpanan instans Linux Amazon EC2 dengan menggunakan pustaka Linux bawaan. Metode ini mengenkripsi file secara transparan yang melindungi data rahasia. Hasilnya, aplikasi yang memproses data tidak mengetahui enkripsi tingkat disk.

Anda dapat menggunakan dua metode untuk mengenkripsi file di penyimpanan instans:

- Enkripsi tingkat disk — Dengan metode ini, seluruh disk, atau blok dalam disk, dienkripsi menggunakan satu atau beberapa kunci enkripsi. Enkripsi disk, yang beroperasi di bawah tingkat

sistem file, bersifat agnostik sistem operasi, serta menyembunyikan informasi direktori dan file seperti nama dan ukuran. Enkripsi Sistem File, misalnya, adalah ekstensi Microsoft untuk New Technology File System (NTFS) sistem operasi Windows NT yang menyediakan enkripsi disk.

- Enkripsi tingkat sistem file — Dengan metode ini, file dan direktori dienkripsi, tetapi tidak seluruh disk atau partisi. Enkripsi tingkat sistem file beroperasi di atas sistem file dan bersifat portabel di seluruh sistem operasi.

Untuk volume penyimpanan instans SSD Non-Volatile Memory express (NVMe), enkripsi tingkat disk adalah opsi default. Data dalam penyimpanan instans NVMe dienkripsi menggunakan cipher blok XTS-AES-256 yang diimplementasikan dalam modul perangkat keras pada instans. Kunci enkripsi dihasilkan menggunakan modul perangkat keras dan bersifat unik untuk setiap perangkat penyimpanan instans NVMe. Semua kunci enkripsi dimusnahkan ketika instans dihentikan atau diakhiri, serta tidak dapat dipulihkan. Anda tidak dapat menggunakan kunci enkripsi Anda sendiri.

Enkripsi Data in Transit

AWS sangat menganjurkan untuk mengenkripsi data in transit dari satu sistem ke sistem lainnya, termasuk sumber daya di dalam dan di luar AWS.

Saat Anda membuat akun AWS, bagian yang secara logis terisolasi dari AWS Cloud—Amazon Virtual Private Cloud (Amazon VPC)—disediakan ke akun tersebut. Di sana, Anda dapat meluncurkan sumber daya AWS di jaringan virtual yang Anda tetapkan. Anda memiliki kendali penuh atas lingkungan jaringan virtual Anda, termasuk pemilihan rentang alamat IP Anda sendiri, pembuatan subnet, dan konfigurasi tabel rute dan gateway jaringan. Anda juga dapat membuat koneksi Virtual Private Network (VPN) perangkat keras antara pusat data korporasi Anda dan Amazon VPC Anda, sehingga Anda dapat memanfaatkan AWS Cloud sebagai ekstensi dari pusat data korporasi Anda.

Untuk melindungi komunikasi antara Amazon VPC dan pusat data korporasi Anda, Anda dapat memilih dari beberapa opsi konektivitas VPN, dan memilih salah satu yang paling sesuai dengan kebutuhan Anda. Anda dapat menggunakan AWS Client VPN untuk mengaktifkan akses aman ke sumber daya AWS Anda menggunakan layanan VPN berbasis klien. Anda juga dapat menggunakan peralatan VPN perangkat lunak pihak ketiga yang tersedia di AWS Marketplace, yang dapat Anda instal di instans Amazon EC2 di Amazon VPC Anda. Atau, Anda dapat membuat koneksi VPN IPsec untuk melindungi komunikasi antara VPC Anda dan jaringan jarak jauh Anda. Untuk membuat koneksi privat khusus dari jaringan jarak jauh ke Amazon VPC, Anda dapat menggunakan AWS

Direct Connect. Anda dapat menggabungkan koneksi ini dengan AWS Site-to-Site VPN untuk membuat koneksi privat yang dienkripsi IPsec.

AWS menyediakan titik akhir HTTPS menggunakan protokol TLS untuk komunikasi, yang menyediakan enkripsi in transit saat Anda menggunakan API AWS. Anda dapat menggunakan layanan AWS Certificate Manager (ACM) untuk menghasilkan, mengelola, dan men-deploy sertifikat privat dan publik yang Anda gunakan untuk membangun pengangkutan terenkripsi di antara sistem untuk beban kerja Anda. Elastic Load Balancing terintegrasi dengan ACM dan digunakan untuk mendukung protokol HTTPS. Jika konten Anda didistribusikan melalui Amazon CloudFront, konten tersebut mendukung titik akhir terenkripsi.

Alat Enkripsi

AWS menawarkan berbagai layanan, alat, dan mekanisme enkripsi data yang sangat dapat diskalakan untuk membantu melindungi data Anda yang disimpan dan diproses di AWS. Untuk informasi tentang fungsionalitas dan privasi Layanan AWS, lihat Kemampuan Layanan AWS untuk Pertimbangan Privasi.

Layanan kriptografi dari AWS menggunakan berbagai teknologi enkripsi dan penyimpanan yang dirancang untuk menjaga integritas data at rest atau in transit. AWS menawarkan empat alat utama untuk operasi kriptografi.

- AWS Key Management Service (AWS KMS) adalah layanan terkelola AWS yang menghasilkan dan mengelola kunci utama dan kunci data. AWS KMS terintegrasi dengan banyak layanan AWS untuk menyediakan enkripsi data sisi server menggunakan kunci AWS KMS dari akun pelanggan. Modul Keamanan Perangkat Keras (HSM) AWS KMS telah menerima validasi FIPS 140-2 Level 2.
- AWS CloudHSM menyediakan HSM yang telah menerima validasi FIPS 140-2 Level 3. HSM ini menyimpan dengan aman berbagai kunci kriptografi Anda yang dikelola sendiri, termasuk kunci utama dan kunci data.
- Layanan dan Alat Kriptografi AWS
  - SDK AWS Encryption menyediakan pustaka enkripsi sisi klien untuk menerapkan operasi enkripsi dan dekripsi pada semua jenis data.
  - Amazon DynamoDB Encryption Client menyediakan pustaka enkripsi sisi klien untuk mengenkripsi tabel data sebelum mengirimnya ke layanan basis data, seperti Amazon DynamoDB.

AWS Key Management Service

AWS Key Management Service adalah layanan terkelola yang memudahkan Anda untuk membuat dan mengontrol kunci enkripsi yang digunakan untuk mengenkripsi data Anda, dan menggunakan Modul Keamanan Perangkat Keras (HSM) untuk melindungi keamanan kunci Anda. AWS KMS terintegrasi dengan beberapa layanan AWS lainnya untuk membantu Anda melindungi data yang Anda simpan dengan layanan ini. AWS KMS juga terintegrasi dengan AWS CloudTrail untuk memberikan log dari semua penggunaan kunci Anda untuk kebutuhan peraturan dan kepatuhan.

Anda dapat dengan mudah membuat, mengimpor, dan merotasi kunci serta menentukan kebijakan penggunaan dan audit penggunaan dari AWS Management Console atau menggunakan SDK AWS atau AWS CLI.

CMK di AWS KMS, baik yang diimpor oleh Anda atau dibuat atas nama Anda oleh KMS, disimpan dalam penyimpanan yang sangat berdaya tahan dalam format terenkripsi untuk membantu memastikan CMK ini dapat diambil saat diperlukan. Anda dapat memilih agar KMS secara otomatis merotasi CMK yang dibuat di KMS setahun sekali tanpa perlu mengenkripsi ulang data yang sudah dienkripsi dengan kunci utama Anda. Anda tidak perlu melacak kunci utama versi lama karena KMS membuatnya tetap tersedia untuk secara otomatis mendekripsi data yang dienkripsi sebelumnya.

Untuk setiap CMK di AWS KMS, Anda dapat mengontrol siapa saja yang memiliki akses ke kunci tersebut dan di layanan mana kunci tersebut dapat digunakan melalui sejumlah kontrol akses, termasuk pemberian izin, dan syarat kebijakan kunci dalam kebijakan kunci atau kebijakan IAM. Anda juga dapat mengimpor kunci dari infrastruktur manajemen kunci Anda sendiri dan menggunakannya di KMS.

Misalnya, kebijakan berikut menggunakan syarat `kms:ViaService` untuk memungkinkan CMK yang dikelola pelanggan digunakan untuk tindakan yang ditentukan hanya jika permintaannya berasal dari Amazon EC2 atau Amazon RDS di Wilayah tertentu (us-west-2) atas nama pengguna tertentu (`ExampleUser`).

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
     {
        “Effect”: “Allow”,
        “Principal”: {
            “AWS”: “arn:aws:iam::111122223333:user/ExampleUser”
```

```
                }
               "Action": [
                    "kms:Encrypt*",
                    "kms:Decrypt",
                    "kms:ReEncrypt*",
                    "kms:GenerateDataKey*",
                    "kms:CreateGrant",
                    "kms:ListGrants",
                    "kms:DescribeKey"
                ],
                "Resource": "*",
                "Condition": {
                   "ForAnyValue:StringEquals": {
                       "kms:ViaService": [
                             "ec2.us-west-2.amazonaws.com",
                             "rds.us-west-2.amazonaws.com"
                       ]
                    }
            }
}
```

Integrasi Layanan AWS

AWS KMS telah terintegrasi dengan sejumlah layanan AWS – lihat situs web KMS untuk daftar lengkap layanan terintegrasi. Integrasi ini memungkinkan Anda dengan mudah menggunakan AWS KMS CMK untuk mengenkripsi data yang Anda simpan dengan layanan ini. Selain menggunakan CMK yang dikelola pelanggan, sejumlah layanan terintegrasi memungkinkan Anda menggunakan CMK yang dikelola AWS yang dibuat dan dikelola untuk Anda secara otomatis, tetapi hanya dapat digunakan dalam layanan tertentu yang telah membuatnya.

Kemampuan Audit

AWS CloudTrail mencatat setiap penggunaan kunci yang Anda simpan di AWS KMS dalam file log yang dikirimkan ke bucket Amazon S3 yang Anda tentukan dalam konfigurasi CloudTrail. Informasi yang dicatat mencakup detail pengguna, waktu, tanggal, operasi yang dilakukan, dan kunci yang digunakan.

Keamanan

AWS KMS dirancang untuk memastikan bahwa tidak ada yang memiliki akses ke kunci utama Anda. Layanan ini dibangun di atas sistem yang dirancang untuk menjaga kunci utama Anda dengan teknik

hardening ekstensif, misalnya tidak pernah menyimpan kunci utama teks biasa pada disk, tidak mempersistensi kunci utama dalam memori, dan membatasi sistem mana yang dapat mengakses host yang menggunakan kunci. Seluruh akses untuk memperbarui perangkat lunak pada layanan ini dikendalikan oleh kontrol akses multi-pihak yang diaudit dan ditinjau oleh kelompok independen dalam Amazon.

Untuk informasi lebih lanjut tentang AWS KMS, lihat laporan resmi AWS Key Management Service.

AWS CloudHSM

AWS CloudHSM adalah modul keamanan perangkat keras (HSM) berbasis cloud yang membantu Anda memenuhi persyaratan kepatuhan korporasi, kontrak, dan peraturan untuk keamanan data dengan memungkinkan Anda membuat dan menggunakan kunci enkripsi pada perangkat keras yang telah menerima validasi FIPS 140-2 Level 3.

Dengan AWS CloudHSM, Anda mengontrol kunci enkripsi dan operasi kriptografi yang dilakukan oleh HSM.

AWS dan partner AWS Marketplace menawarkan berbagai solusi untuk melindungi data sensitif dalam platform AWS, tetapi untuk aplikasi dan data yang tunduk pada persyaratan kontrak atau peraturan yang ketat untuk mengelola kunci kriptografi, perlindungan tambahan terkadang diperlukan. Sebelumnya, satu-satunya opsi untuk menyimpan data sensitif (atau kunci enkripsi yang melindungi data sensitif) mungkin ada di pusat data on-premise. Hal ini mungkin telah mencegah Anda memigrasikan aplikasi tersebut ke cloud, atau secara signifikan memperlambat performanya. Dengan AWS CloudHSM, Anda dapat melindungi kunci enkripsi Anda dalam HSM yang dirancang dan divalidasi dengan standar pemerintah untuk manajemen kunci yang aman. Anda dapat dengan aman membuat, menyimpan, dan mengelola kunci kriptografi yang digunakan untuk enkripsi data guna memastikan bahwa hanya Anda yang bisa mendapatkan akses ke kunci tersebut. AWS CloudHSM membantu Anda mematuhi persyaratan manajemen kunci yang ketat tanpa mengorbankan performa aplikasi.

Layanan AWS CloudHSM bekerja dengan Amazon VPC. Instans AWS CloudHSM disediakan di dalam Amazon VPC Anda dengan alamat IP yang Anda tentukan, yang menyediakan konektivitas jaringan sederhana dan privat ke instans Amazon EC2 Anda. Jika Anda menempatkan instans HSM di dekat instans Amazon EC2, Anda akan mengurangi latensi jaringan, yang dapat meningkatkan performa aplikasi. AWS menyediakan akses khusus dan eksklusif (tenant tunggal) ke instans HSM, yang terisolasi dari pelanggan AWS lainnya. Tersedia di beberapa Wilayah dan Zona Ketersediaan (AZ), AWS CloudHSM memungkinkan Anda menambahkan penyimpanan kunci yang aman dan tahan lama ke aplikasi Anda.

Integrasi dengan Layanan AWS dan Aplikasi Pihak Ketiga

Anda dapat menggunakan CloudHSM dengan Amazon Redshift, Amazon RDS for Oracle, atau aplikasi pihak ketiga seperti SafeNet Virtual KeySecure sebagai Root of Trust, Apache (penghentian SSL), atau Microsoft SQL Server (enkripsi data transparan). Anda juga dapat menggunakan AWS CloudHSM ketika menulis aplikasi Anda sendiri dan terus menggunakan pustaka kriptografi standar, termasuk PKCS #11, Java JCA/JCE, dan Microsoft CAPI dan CNG.

Aktivitas Audit

Jika Anda perlu melacak perubahan sumber daya, atau mengaudit aktivitas untuk tujuan keamanan dan kepatuhan, Anda dapat meninjau panggilan API manajemen melalui AWS CloudHSM yang dibuat dari akun Anda menggunakan AWS CloudTrail. Selain itu, Anda bisa melakukan audit operasi pada perangkat HSM menggunakan syslog atau mengirim log pesan syslog ke pengumpul log Anda sendiri.

Layanan dan Alat Kriptografi AWS

AWS menawarkan mekanisme yang sesuai dengan berbagai standar keamanan kriptografi yang dapat Anda gunakan untuk menerapkan enkripsi praktik terbaik. AWS Encryption SDK adalah pustaka enkripsi sisi klien, yang tersedia di Java, Python, C, JavaScript, dan antarmuka baris perintah yang mendukung Linux, macOS, dan Windows. Layanan ini menawarkan fitur perlindungan data canggih termasuk rangkaian algoritme kunci simetris yang aman dan terautentikasi, seperti 256-bit AES-GCM dengan derivasi dan penandatanganan kunci. Karena dirancang khusus untuk aplikasi yang menggunakan Amazon DynamoDB, DynamoDB Encryption Client memungkinkan pengguna melindungi data tabel mereka sebelum dikirim ke basis data. Layanan ini juga memverifikasi dan mendekripsi data ketika diambil. Kliennya tersedia di Java dan Python.

Infrastruktur DM-Crypt Linux

Dm-crypt adalah mekanisme enkripsi tingkat kernel Linux yang memungkinkan pengguna memasang sistem file terenkripsi. Memasang sistem file adalah proses yang menghubungkan sistem file ke direktori (titik pemasangan), yang membuatnya tersedia untuk sistem operasi. Setelah pemasangan, semua file dalam sistem file tersedia untuk aplikasi tanpa interaksi tambahan. Namun, file-file ini dienkripsi ketika disimpan pada disk.

Device mapper adalah infrastruktur di kernel Linux 2.6 dan 3.x yang menyediakan metode umum untuk membuat lapisan virtual perangkat blok. Device mapper crypt target menyediakan enkripsi transparan perangkat blok menggunakan API kernel crypto. Solusi dalam postingan ini menggunakan

dm-crypt bersama dengan sistem file yang didukung disk yang dipetakan ke volume logis oleh Logical Volume Manager (LVM). LVM menyediakan manajemen volume logis untuk kernel Linux.

Perlindungan Data Secara Desain dan Secara Default

Setiap kali pengguna atau aplikasi mencoba menggunakan AWS Management Console, API AWS, atau AWS CLI, permintaan akan dikirim ke AWS. Layanan AWS menerima permintaan dan mengeksekusi serangkaian langkah untuk menentukan apakah akan mengizinkan atau menolak permintaan ini, sesuai dengan logika evaluasi kebijakan tertentu. Kecuali untuk permintaan kredensial root, semua permintaan di AWS ditolak secara default (kebijakan penolakan default diterapkan). Ini berarti bahwa segala sesuatu yang tidak secara eksplisit diizinkan oleh kebijakan akan ditolak. Dalam definisi kebijakan dan sebagai praktik terbaik, AWS menyarankan agar Anda menerapkan prinsip hak akses paling rendah, yang berarti bahwa setiap komponen (seperti pengguna, modul, atau layanan) harus dapat mengakses hanya sumber daya yang diperlukan untuk menyelesaikan tugasnya.

Pendekatan ini selaras dengan Pasal 25 GDPR, yang menyatakan bahwa pengontrol “harus menerapkan langkah-langkah teknis dan organisasional yang tepat untuk memastikan bahwa, secara default, hanya data pribadi yang diperlukan untuk setiap tujuan spesifik pemrosesan yang diproses.”

AWS juga menyediakan alat untuk mengimplementasikan infrastruktur sebagai kode (IaC), yang merupakan mekanisme ampuh untuk menerapkan keamanan sejak awal proses desain sebuah arsitektur. AWS CloudFormation menyediakan bahasa yang sama untuk mendeskripsikan dan menyediakan semua sumber daya infrastruktur, termasuk kebijakan dan proses keamanan. Dengan alat dan praktik ini, keamanan menjadi bagian dari kode Anda dan dapat di-versioning, dipantau, dan dimodifikasi (dengan sistem versioning) sesuai dengan persyaratan organisasi Anda. Hal ini memungkinkan perlindungan data secara desain, karena proses dan kebijakan keamanan dapat disertakan dalam definisi arsitektur Anda, dan juga dapat terus dipantau oleh langkah-langkah keamanan di organisasi Anda.

Bagaimana AWS Dapat Membantu

Tabel 1 – Cara AWS dapat membantu Anda menavigasi kepatuhan GDPR

Area	Deskripsi	Layanan dan Alat AWS
Kerangka Kerja Kepatuhan yang Kuat	Langkah-langkah teknis dan organisasional yang tepat mungkin perlu menyertakan "kemampuan untuk memastikan kerahasiaan, integritas, ketersediaan, dan ketahanan yang berkelanjutan dari sistem dan layanan pemrosesan."	SOC 1 / SSAE 16 / ISAE 3402 (sebelumnya SAS 70) / SOC 2 / SOC 3 PCI DSS Level 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Common Cloud Computing Controls Catalog (C5)
Kontrol Akses Data	Pengontrol "…harus menerapkan langkah-langkah teknis dan organisasional yang tepat untuk memastikan bahwa, secara default, hanya data pribadi yang diperlukan untuk setiap	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield dan AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations AWS CloudTrail

Area	Deskripsi	Layanan dan Alat AWS
	tujuan spesifik pemrosesan yang diproses.”	
Pemantauan dan Pencatatan Log	“Setiap pengontrol dan, jika berlaku, perwakilan pengontrol, harus menyimpan catatan aktivitas pemrosesan di bawah tanggung jawabnya.” “…pengontrol dan pemroses harus menerapkan langkah-langkah teknis dan organisasional yang tepat untuk memastikan tingkat keamanan yang sesuai dengan risiko […]”	AWS Config Amazon CloudWatch AWS Control Tower Amazon GuardDuty Amazon Inspector Amazon Macie AWS Systems Manager AWS Security Hub Alat dan SDK AWS

Area	Deskripsi	Layanan dan Alat AWS
Melindungi Data Anda di AWS	Organisasi harus “menerapkan langkah-langkah teknis dan organisasional yang tepat untuk memastikan tingkat keamanan yang sesuai dengan risiko, termasuk pseudonimisasi dan enkripsi data pribadi.”	AWS Certificate Manager AWS CloudHSM AWS Key Management Service

Kontributor

Kontributor dokumen ini meliputi:

- Tim Anderson, Spesialis Industri Teknis (Technical Industry Specialist), Amazon Web Services
- Carmela Gambardella, Arsitek Solusi Sektor Publik (Public Sector Solutions Architect), Amazon Web Services
- Giuseppe Rusia, Manajer Jaminan Keamanan (Security Assurance Manager), Amazon Web Services
- Marta Taggart, Manajer Program Senior (Senior Program Manager), Amazon Web Services
- Luca Iannario, Arsitek Solusi Sektor Publik (Public Sector Solutions Architect), Amazon Web Services

Revisi Dokumen

Tanggal	Deskripsi
November 2017	Publikasi pertama
Desember 2020	Diperbarui untuk menyertakan penambahan Layanan AWS dan fungsionalitas baru.

Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya disediakan sebagai informasi, (b) berisi penawaran produk dan praktik AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak menjadi komitmen atau jaminan apa pun dari AWS dan afiliasi, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa jaminan, representasi, atau syarat 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.