Laporan Resmi AWS

Pendahuluan tentang Keamanan AWS

Pendahuluan tentang Keamanan AWS: Laporan Resmi AWS

Table of Contents

Pendahuluan tentang Keamanan AWS

Tanggal publikasi: 11 November 2021 (Revisi Dokumen)

Abstrak

Amazon Web Services (AWS) memberikan platform komputasi cloud yang dapat diskalakan dan dirancang untuk ketersediaan serta keandalan tinggi, yang menyediakan alat untuk memungkinkan Anda menjalankan berbagai aplikasi. Membantu melindungi kerahasiaan, integritas, dan ketersediaan sistem serta data Anda adalah hal yang paling penting bagi AWS, begitu juga dengan menjaga kepercayaan dan keyakinan Anda. Dokumen ini dimaksudkan untuk memberikan pengantar terkait pendekatan AWS terhadap keamanan, termasuk kontrol di lingkungan AWS serta sejumlah produk dan fitur yang disediakan AWS bagi pelanggan untuk memenuhi tujuan keamanan.

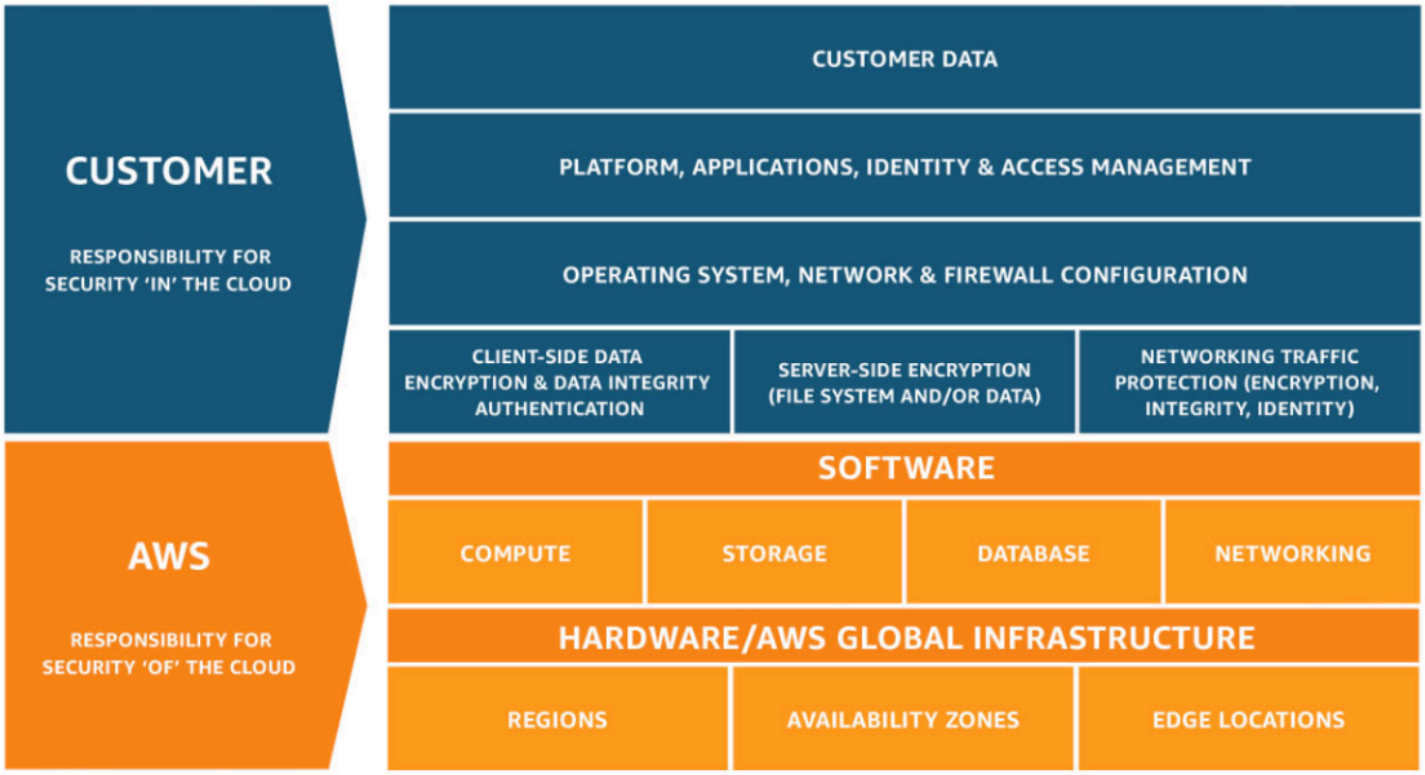
Keamanan Infrastruktur AWS

Infrastruktur AWS telah dirancang untuk menjadi salah satu lingkungan komputasi cloud paling fleksibel dan aman yang tersedia saat ini. Infrastruktur AWS dirancang untuk menyediakan platform yang sangat mudah diskalakan dan begitu andal sehingga memungkinkan pelanggan untuk men-deploy aplikasi dan data dengan cepat dan aman.

Infrastruktur ini dibangun dan dikelola sesuai standar dan praktik terbaik keamanan, serta mempertimbangkan kebutuhan yang berbeda-beda akan cloud. AWS menggunakan kontrol redundan dan berlapis, validasi serta pengujian berkelanjutan, dan sejumlah besar otomatisasi untuk memastikan bahwa infrastruktur yang mendasarinya terus terpantau dan terlindungi sepanjang waktu. AWS memastikan bahwa semua pusat data atau layanan baru menerapkan kontrol yang sama.

Semua pelanggan AWS diuntungkan dengan pusat data dan arsitektur jaringan yang dibangun untuk memenuhi kebutuhan pelanggan kami yang sangat memperhatikan keamanan. Artinya, Anda mendapatkan infrastruktur yang tangguh, dirancang untuk keamanan tinggi, tanpa mengeluarkan modal dan pengeluaran operasional (overhead) seperti pada pusat data tradisional.

AWS beroperasi di bawah model tanggung jawab keamanan bersama, tempat AWS bertanggung jawab atas keamanan infrastruktur cloud yang mendasarinya dan Anda bertanggung jawab mengamankan beban kerja yang Anda deploy di AWS (Gambar 1). Model ini memberi fleksibilitas dan ketangkasan yang Anda butuhkan untuk menerapkan kontrol keamanan yang paling sesuai untuk fungsi bisnis Anda di lingkungan AWS. Anda dapat membatasi akses dengan ketat ke lingkungan yang memproses data sensitif, atau men-deploy kontrol yang tidak terlalu ketat untuk informasi yang ingin Anda publikasikan.



Gambar 1 - Model Tanggung Jawab Bersama AWS

Produk dan Fitur Keamanan

AWS dan partnernya menawarkan berbagai alat dan fitur untuk membantu Anda memenuhi tujuan keamanan. Alat-alat ini serupa dengan kontrol yang biasa Anda deploy dalam lingkungan on-premise Anda. AWS menyediakan alat dan fitur khusus keamanan di seluruh elemen keamanan jaringan, manajemen konfigurasi, kontrol akses, dan keamanan data. Selain itu, AWS juga menyediakan alat pemantauan dan pembuatan log agar Anda bisa mendapatkan visibilitas penuh tentang apa yang terjadi di lingkungan Anda.

Topik

Keamanan Infrastruktur

AWS menyediakan beberapa kemampuan dan layanan keamanan untuk meningkatkan privasi dan mengontrol akses jaringan. Antara lain:

- Firewall jaringan yang tertanam di Amazon VPC memungkinkan Anda menciptakan jaringan pribadi dan mengontrol akses ke instans atau aplikasi Anda. Pelanggan dapat mengontrol enkripsi saat berjalan dengan TLS di seluruh layanan AWS.
- Opsi konektivitas yang memungkinkan koneksi pribadi, atau khusus, dari kantor atau lingkungan on-premise Anda.
- Teknologi mitigasi DDoS yang diterapkan pada lapisan 3 atau 4 serta lapisan 7. Teknologi ini dapat diterapkan sebagai bagian dari aplikasi dan strategi pengiriman konten.
- Enkripsi otomatis semua lalu lintas di jaringan global dan regional AWS antar-fasilitas aman AWS.

Manajemen Konfigurasi dan Inventaris

AWS menawarkan berbagai alat untuk mendukung Anda bergerak cepat, sambil tetap memastikan bahwa sumber daya cloud Anda mematuhi standar organisasi dan praktik terbaik. Antara lain:

- Alat deployment untuk mengelola pembuatan dan penonaktifan sumber daya AWS sesuai dengan standar organisasi.
- Alat manajemen inventaris dan konfigurasi untuk mengidentifikasi sumber daya AWS dan kemudian melacak dan mengelola perubahan pada sumber daya tersebut seiring waktu.
- Definisi templat dan alat manajemen untuk menciptakan mesin virtual standar yang diperkuat dan sudah dikonfigurasi untuk instans EC2.

Enkripsi Data

AWS menawarkan kemampuan untuk menambahkan lapisan keamanan ke data nonaktif (data at rest) Anda di cloud, yang menyediakan fitur enkripsi yang efisien dan dapat diskalakan. Antara lain:

- Kemampuan enkripsi data at rest tersedia di sebagian besar layanan AWS, seperti Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda, dan Amazon SageMaker
- Opsi manajemen kunci yang fleksibel, termasuk AWS Key Management Service, yang memungkinkan Anda memilih apakah AWS akan mengelola kunci enkripsi atau memungkinkan Anda untuk tetap memegang kendali penuh atas kunci Anda sendiri
- Penyimpanan kunci kriptografi khusus berbasis perangkat keras menggunakan AWS CloudHSM, memungkinkan Anda memenuhi persyaratan kepatuhan
- Antrean pesan terenkripsi untuk transmisi data sensitif menggunakan enkripsi di sisi server (SSE) untuk Amazon SQS

Selain itu, AWS juga menyediakan API bagi Anda untuk mengintegrasikan enkripsi dan perlindungan data dengan layanan apa pun yang Anda kembangkan atau deploy di lingkungan AWS.

Kontrol Akses dan Identitas

AWS menawarkan kemampuan kepada Anda untuk menentukan, menegakkan, dan mengelola kebijakan akses pengguna di seluruh layanan AWS. Antara lain:

- AWS Identity and Access Management (IAM) memungkinkan Anda menentukan akun pengguna individu dengan izin AWS Multi-Factor Authentication di seluruh sumber daya AWS untuk akun yang memiliki hak istimewa, termasuk opsi untuk pengautentikasi berbasis perangkat lunak dan perangkat keras. IAM dapat digunakan untuk memberi akses federasi ke Konsol Manajemen AWS dan API layanan AWS, menggunakan sistem identitas Anda saat ini, seperti Microsoft Active Directory atau penawaran dari partner lain.
- AWS Directory Service memungkinkan Anda untuk berintegrasi dan berfederasi dengan direktori korporasi guna mengurangi biaya administrasi dan meningkatkan pengalaman pengguna akhir.
- AWS Single Sign-On (AWS SSO) memungkinkan Anda mengelola akses SSO dan izin pengguna ke semua akun Anda di AWS Organizations, secara terpusat.

AWS menyediakan integrasi manajemen identitas dan akses native di banyak layanannya, ditambah integrasi API dengan aplikasi atau layanan Anda sendiri.

Pemantauan dan Pembuatan Log

AWS menyediakan alat dan fitur yang memungkinkan Anda melihat apa yang terjadi di lingkungan AWS Anda. Antara lain:

- Dengan AWS CloudTrail, Anda dapat memantau deployment AWS Anda di cloud dengan mendapatkan riwayat permintaan API AWS untuk akun Anda, termasuk panggilan API yang dibuat melalui Konsol Manajemen AWS, SDK AWS, alat baris perintah, dan layanan AWS tingkat lebih tinggi. Anda juga dapat mengidentifikasi pengguna dan akun yang meminta API AWS untuk layanan yang mendukung CloudTrail, sumber alamat IP asal permintaan, dan kapan permintaan terjadi.
- Amazon CloudWatch menyediakan solusi pemantauan yang andal, dapat diskalakan, dan fleksibel yang dapat mulai Anda gunakan dalam hitungan menit. Anda tidak perlu lagi mengonfigurasi, mengelola, dan menskalakan sistem serta infrastruktur pemantauan Anda sendiri.
- Amazon GuardDuty adalah layanan deteksi ancaman yang terus memantau aktivitas berbahaya dan perilaku tidak terotorisasi untuk melindungi akun dan beban kerja AWS Anda. Amazon GuardDuty memaparkan pemberitahuan melalui Amazon CloudWatch sehingga Anda dapat memicu respons otomatis atau memberi tahu manusia.

Berbagai alat dan fitur ini menawarkan visibilitas yang Anda butuhkan untuk menemukan masalah sebelum berdampak pada bisnis, yang memungkinkan Anda untuk meningkatkan postur keamanan, dan mengurangi profil risiko, lingkungan Anda.

Produk Keamanan di AWS Marketplace

Memindahkan beban kerja produksi ke AWS dapat memungkinkan organisasi meningkatkan ketangkasan, skalabilitas, inovasi, dan penghematan biaya — sambil mempertahankan lingkungan yang aman. AWS Marketplace menawarkan produk terdepan di industri keamanan yang setara, identik dengan, atau terintegrasi dengan kontrol yang ada di lingkungan on-premise Anda. Produk ini melengkapi layanan AWS yang ada untuk memungkinkan pelanggan men-deploy arsitektur keamanan yang komprehensif dan pengalaman yang lebih lancar di seluruh lingkungan cloud dan on-premise Anda.

Panduan Keamanan

AWS memberi panduan dan keahlian kepada pelanggan melalui alat online, sumber daya, dukungan, dan layanan profesional yang disediakan oleh AWS dan partnernya.

AWS Trusted Advisor adalah alat online yang bertindak seperti ahli cloud khusus, yang membantu Anda mengonfigurasi sumber daya untuk mengikuti praktik terbaik. Trusted Advisor memeriksa lingkungan AWS Anda untuk membantu menutup celah keamanan, dan menemukan peluang untuk menghemat biaya, menyempurnakan kinerja sistem, dan meningkatkan keandalan.

Tim Akun AWS adalah titik kontak pertama Anda, yang memandu Anda dalam proses deployment dan implementasi, serta mengarahkan Anda ke sumber daya yang tepat untuk menyelesaikan masalah keamanan yang mungkin Anda hadapi.

AWS Enterprise Support dapat merespons dalam waktu 15 menit dan dapat dihubungi setiap saat melalui telepon, obrolan, atau email; seorang Manajer Akun Teknis khusus juga siap siaga. Layanan concierge ini memastikan bahwa masalah pelanggan ditangani secepat mungkin.

AWS Partner Network menawarkan ratusan produk terkemuka di industri yang setara, identik, atau terintegrasi dengan kontrol yang ada di lingkungan on-premise Anda. Produk-produk ini melengkapi layanan AWS yang ada untuk memungkinkan Anda men-deploy arsitektur keamanan yang komprehensif dan pengalaman yang lebih lancar di cloud dan di lingkungan on-premise Anda, serta ratusan Partner Konsultasi AWS bersertifikat di seluruh dunia yang akan membantu kebutuhan Anda dalam hal keamanan dan kepatuhan.

Layanan Profesional AWS menyediakan praktik khusus Keamanan, Risiko, dan Kepatuhan untuk membantu Anda mengembangkan kepercayaan diri dan kemampuan teknis saat memigrasi beban kerja yang paling sensitif ke AWS Cloud. Layanan Profesional AWS membantu pelanggan mengembangkan kebijakan dan praktik keamanan berdasarkan desain yang telah terbukti, dan membantu memastikan bahwa desain keamanan pelanggan memenuhi persyaratan kepatuhan internal dan eksternal.

AWS Marketplace adalah katalog digital dengan ribuan daftar vendor perangkat lunak independen yang memudahkan Anda menemukan, menguji, membeli, dan men-deploy perangkat lunak yang berjalan di AWS. Produk keamanan AWS Marketplace melengkapi layanan AWS yang ada untuk memungkinkan Anda men-deploy arsitektur keamanan yang komprehensif dan pengalaman yang lebih lancar di seluruh lingkungan cloud dan on-premise Anda.

Buletin Keamanan AWS menyediakan buletin keamanan seputar kerentanan dan ancaman saat ini, dan memungkinkan pelanggan untuk bekerja dengan ahli keamanan AWS untuk mengatasi masalah seperti pelaporan penyalahgunaan, kerentanan, dan uji penetrasi. Kami juga memiliki sumber daya online untuk pelaporan kerentanan.

Dokumentasi Keamanan AWS menunjukkan cara mengonfigurasi layanan AWS untuk memenuhi tujuan keamanan dan kepatuhan Anda. Pelanggan AWS mendapatkan keuntungan dari pusat data dan arsitektur jaringan yang dibuat untuk memenuhi persyaratan dari organisasi yang sangat memperhatikan keamanan.

AWS Well-Architected Framework membantu arsitek cloud membangun infrastruktur yang paling aman, berkinerja tinggi, tangguh, dan efisien untuk aplikasi mereka. AWS Well-Architected Framework berisi pilar keamanan yang berfokus pada perlindungan informasi dan sistem. Topik utama mencakup kerahasiaan dan integritas data, mengidentifikasi dan mengelola siapa yang dapat melakukan apa dengan manajemen hak istimewa, melindungi sistem, dan menetapkan kontrol untuk mendeteksi peristiwa keamanan. Pelanggan dapat menggunakan AWS Well-Architected Tool dari Konsol Manajemen AWS atau terlibat layanan dari salah satu mitra APN untuk membantu mereka.

AWS Well-Architected Tool membantu Anda meninjau status beban kerja Anda dan membandingkannya dengan praktik terbaik arsitektur terbaru di AWS. Alat gratis ini tersedia di Konsol Manajemen AWS, dan setelah menjawab serangkaian pertanyaan tentang keunggulan operasional, keamanan, keandalan, efisiensi performa, dan pengoptimalan biaya. AWS Well-Architected Tool kemudian menyediakan rencana tentang cara merancang cloud menggunakan praktik terbaik yang ada.

Kepatuhan

Kepatuhan AWS memberdayakan pelanggan untuk memahami kontrol andal yang diterapkan di AWS untuk menjaga keamanan dan perlindungan data di AWS Cloud. Saat sistem dibangun di AWS Cloud, AWS dan pelanggan memiliki tanggung jawab kepatuhan bersama. Lingkungan komputasi AWS terus diaudit, dengan sertifikasi dari badan akreditasi di seluruh wilayah dan vertikal, termasuk SOC 1/SSAE 16/ISAE 3402 (sebelumnya SAS 70), SOC 2, SOC 3, ISO 9001/ISO 27001, FedRAMP, DoD SRG, dan PCI DSS Level 1.i. Selain itu, AWS juga memiliki program jaminan yang menyediakan templat dan pemetaan kontrol untuk membantu pelanggan menetapkan kepatuhan lingkungan mereka yang berjalan di AWS, untuk daftar lengkap program, lihat Program Kepatuhan AWS.

Kami dapat memastikan bahwa semua layanan AWS dapat digunakan sesuai dengan GDPR. Artinya, selain mendapatkan keuntungan dari semua tindakan yang telah AWS lakukan untuk menjaga keamanan layanan, pelanggan dapat men-deploy layanan AWS sebagai bagian dari rencana kepatuhan GDPR mereka. AWS menawarkan Perjanjian Pemrosesan Data (Data Processing Addendum) yang mematuhi GDPR (GDPR DPA), yang memungkinkan Anda untuk mematuhi kewajiban kontrak GDPR. GDPR DPA AWS menjadi bagian dalam Ketentuan Layanan AWS dan berlaku secara otomatis untuk semua pelanggan secara global yang wajib mematuhi GDPR. Amazon.com, Inc. disertifikasi berdasarkan Perlindungan Privasi UE-AS (EU-US Privacy Shield) dan AWS tercakup dalam sertifikasi ini. Hal ini membantu pelanggan yang memilih untuk mentransfer data pribadi ke AS untuk memenuhi kewajiban perlindungan data mereka. Sertifikasi Amazon.com Inc. dapat dilihat di situs web Perlindungan Privasi UE-AS: https://www.privacyshield.gov/list

Dengan beroperasi di lingkungan yang terakreditasi, pelanggan dapat mengurangi cakupan dan biaya audit yang perlu mereka keluarkan. AWS terus-menerus melakukan penilaian atas infrastruktur dasarnya—termasuk keamanan fisik dan lingkungan dari perangkat keras dan pusat datanya—sehingga pelanggan dapat memanfaatkan sertifikasi tersebut dan mewarisi kontrol tersebut.

Di pusat data tradisional, aktivitas kepatuhan umum sering kali merupakan aktivitas manual dan berkala. Aktivitas ini termasuk memverifikasi konfigurasi aset dan melaporkan kegiatan administratif. Jadi, laporan yang dihasilkan bisa saja sudah tidak relevan bahkan sebelum dipublikasikan. Beroperasi di lingkungan AWS memungkinkan pelanggan memanfaatkan alat otomatis yang disematkan, seperti AWS Security Hub CSPM, AWS Config dan AWS CloudTrail untuk memvalidasi kepatuhan. Alat ini mengurangi upaya yang diperlukan untuk melakukan audit, karena tugas ini menjadi rutin, berkelanjutan, dan otomatis. Karena waktu yang diperlukan untuk aktivitas manual menjadi lebih sedikit, Anda dapat membantu mengembangkan peran kepatuhan di perusahaan Anda,

dari beban pekerjaan administratif menjadi peran untuk mengelola risiko dan menyempurnakan struktur keamanan Anda.

Bacaan Lebih Lanjut

Untuk informasi tambahan, baca sumber daya berikut ini:

Untuk informasi tentang …	Lihat
Topik utama, area penelitian, dan peluang pelatihan untuk keamanan cloud di AWS	Pembelajaran Keamanan AWS Cloud
AWS Cloud Adoption Framework yang menyusun panduan ke dalam enam area fokus: Bisnis, Personel, Tata Kelola, Platform, Keamanan, dan Operasi	AWS Cloud Adoption Framework
Kontrol spesifik diterapkan di AWS; cara mengintegrasikan AWS ke dalam kerangka kerja yang Anda miliki	Amazon Web Services: Risiko dan Kepatuhan
Praktik terbaik untuk Keamanan, Identitas & Kepatuhan	Praktik terbaik untuk Keamanan, Identitas & Kepatuhan
Pilar Keamanan - AWS Well-Architected Framework	Pilar Keamanan - AWS Well-Architected Framework

Revisi Dokumen

Untuk menerima pemberitahuan tentang pembaruan laporan resmi ini, berlangganan umpan RSS.

pembaruan-riwayat-perubahan	pembaruan-riwayat-deskripsi	pembaruan-riwayat-tanggal
Laporan resmi diperbarui	Diperbarui untuk tautan untuk Bacaan Lebih Lanjut.	11 November 2021
Laporan resmi diperbarui	Diperbarui untuk layanan, sumber daya, dan teknologi terbaru.	22 Januari 2020
Publikasi awal	Pengantar Keamanan AWS diterbitkan.	1 Juli 2015

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 ketentuan 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.