AWS Panduan Keputusan

Memilih AWS layanan tata kelola cloud

Memilih AWS layanan tata kelola cloud: AWS Panduan Keputusan

Table of Contents

Memilih AWS layanan tata kelola cloud

Mengambil langkah pertama

Tujuan	Bantu menentukan layanan tata kelola AWS cloud mana yang paling cocok untuk organisasi Anda.
Terakhir diperbarui	Desember 23, 2024
Layanan yang tercakup	• AWS Artifact • AWS Audit Manager • CloudFormation • AWS CloudTrail • AWS Config • AWS Control Tower • AWS Organizations • AWS Security Hub • AWS Service Catalog • AWS Systems Manager • AWS Trusted Advisor

Pengantar tata kelola AWS cloud

Cloud governance adalah seperangkat aturan, proses, dan laporan yang membantu Anda menyelaraskan AWS Cloud penggunaan Anda dengan tujuan bisnis Anda.

Ini mencakup keamanan, dengan mengaktifkan strategi multi-akun, pemantauan berkelanjutan, dan kebijakan kontrol. Ini mencakup kepatuhan, dengan mengotomatiskan pemeriksaan, pelaporan, dan remediasi. Ini mencakup operasi, dengan menerapkan kontrol di seluruh perusahaan. Ini mencakup identitas dengan memusatkan identitas dan manajemen akses dalam skala besar. Ini mencakup biaya, dengan memfasilitasi laporan penggunaan dan penegakan kebijakan. Dan itu mencakup ketahanan, dengan membantu mengintegrasikan penilaian dan pengujian ke dalam CI/CD jaringan pipa untuk validasi.

Kami menawarkan berbagai layanan untuk membantu Anda mengatur, mengelola, memantau, dan mengontrol penggunaan akun, layanan, dan sumber daya di cloud, sehingga menerapkan praktik terbaik tata kelola cloud.

Panduan ini dirancang untuk membantu Anda memutuskan layanan tata kelola AWS cloud mana yang paling cocok untuk organisasi Anda, untuk memperkuat ketahanan operasional, mengoptimalkan biaya, dan membangun kontrol untuk membantu mematuhi peraturan atau standar perusahaan, sambil mempertahankan kecepatan pengembangan dan mempercepat inovasi.

Video ini adalah segmen enam menit dari presentasi yang memperkenalkan praktik terbaik untuk tata kelola cloud.

Memahami tata kelola AWS cloud

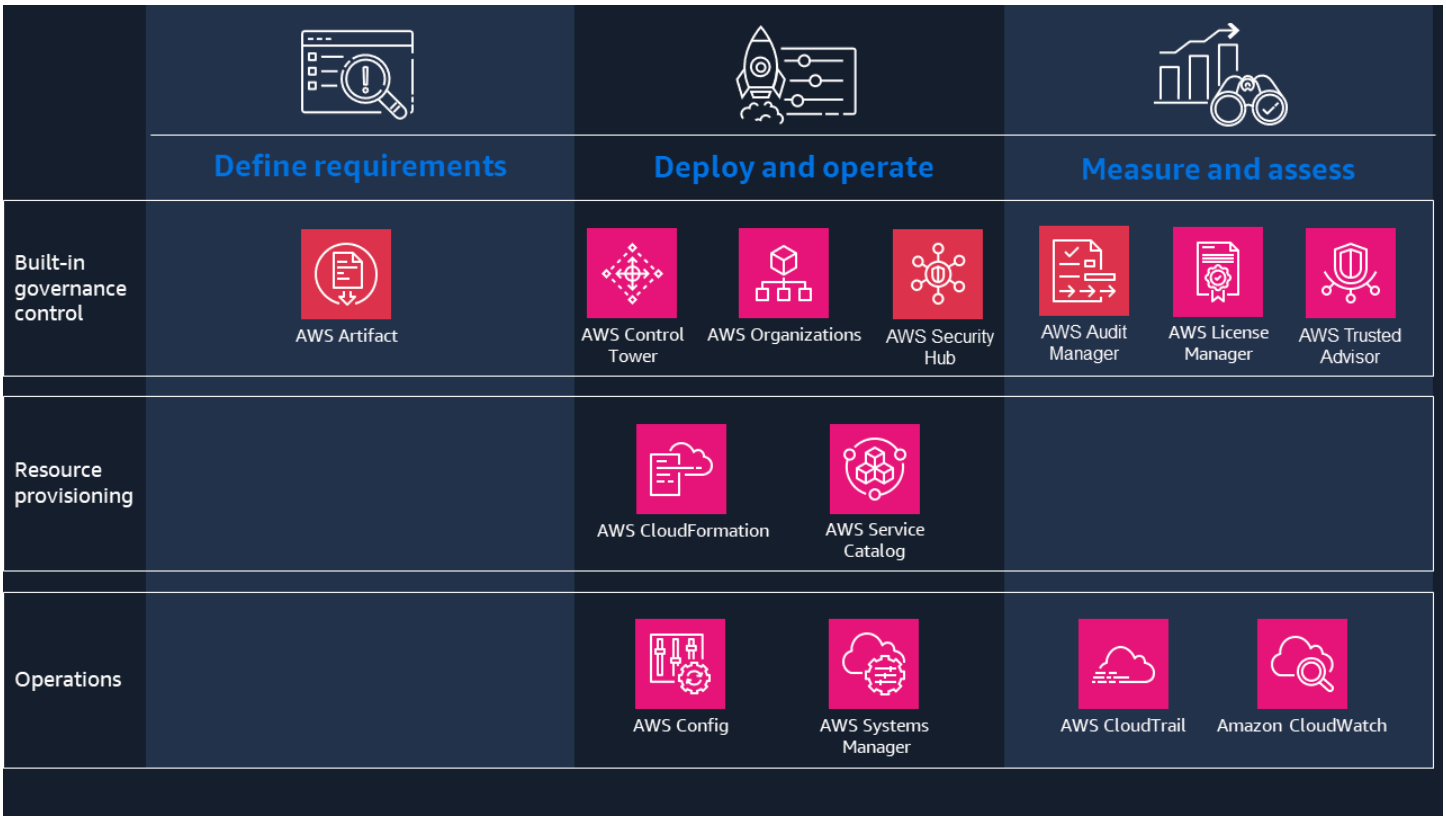

Diagram sebelumnya menunjukkan bagaimana tata kelola cloud mengacu pada beberapa Layanan AWS, yang memungkinkan Anda untuk menentukan persyaratan tata kelola Anda, menyebarkan dan mengoperasikan sistem Anda, dan mengukur dan menilai kinerjanya. Layanan ini menyediakan kontrol tata kelola bawaan, penyediaan sumber daya untuk menyelaraskan dengan kebijakan tata kelola Anda, dan alat operasi untuk membantu Anda memantau dan mengelola lingkungan Anda.

Memanfaatkan layanan tata kelola AWS cloud membantu Anda memastikan penggunaan cloud Anda mendukung tujuan bisnis Anda, Secara khusus, mereka memungkinkan Anda meningkatkan kecepatan dan kelincahan bagi pengembang, beroperasi dalam lingkungan peraturan yang dinamis, merampingkan merger dan akuisisi, dan memperkuat ketahanan operasional:

- Tingkatkan kecepatan dan kelincahan bagi pengembang — Putar lingkungan baru dengan cepat dengan APIs memastikan pengembang Anda tidak menunggu siklus penyediaan selama berminggu-minggu, dan mempercepat penyediaan pipeline. CI/CD Temukan dan cegah cacat di awal proses pengiriman perangkat lunak, menggunakan kontrol dan aturan yang dibuat sebelumnya, dan infrastructure-as-code templat untuk menyediakan sumber daya umum secara efisien.
- Beroperasi dalam lingkungan peraturan yang dinamis — Buat batasan yang selalu aktif untuk melindungi dan mengontrol akses ke data di seluruh AWS, mengkodifikasi persyaratan kepatuhan Anda, dan mengotomatiskan penilaian konfigurasi sumber daya Anda di seluruh organisasi Anda.
- Merampingkan merger dan akuisisi — Migrasikan beban kerja lebih cepat dengan membangun lingkungan multi-akun yang aman, dirancang dengan baik. Memusatkan pembuatan akun, mengalokasikan sumber daya, akun grup, dan menerapkan kebijakan dan kontrol tata kelola dengan mudah dan cepat. Mengadopsi pendekatan terprogram untuk manajemen multi-akun dalam skala besar.
- Memperkuat ketahanan operasional — Siapkan lingkungan multi-akun yang aman, terancang dengan baik, dan tangguh dengan cepat. Jalankan penilaian beban kerja Anda untuk mengungkap potensi kelemahan terkait ketahanan. Melakukan pemeriksaan otomatis terhadap lima bidang utama - pengoptimalan biaya, kinerja, keamanan, toleransi kesalahan, dan batas layanan - dan menerima rekomendasi yang memungkinkan Anda mengikuti praktik terbaik yang dikenal.
- Optimalkan biaya — Visualisasikan, pahami, dan kelola biaya dan penggunaan dari waktu ke waktu. Terus menganalisis pemanfaatan sumber daya, mengidentifikasi sumber daya yang kurang dimanfaatkan, dan menghentikan sumber daya yang menganggur.

Praktik terbaik tata kelola cloud dapat dibangun secara efektif saat Anda menyiapkan dan mengoperasikan beban kerja Anda. AWS Layanan interoperable membantu Anda mencapai tata kelola yang konsisten dan terpusat atas properti TI Anda, termasuk AWS dan produk pihak ketiga. Luas dan kedalaman kontrol di seluruh Layanan AWS membantu Anda memenuhi persyaratan peraturan yang berkembang dan meminimalkan risiko keamanan.

Pertimbangkan kriteria tata kelola AWS cloud

Bagian berikut menguraikan beberapa kriteria utama yang perlu dipertimbangkan ketika memilih strategi tata kelola cloud. Secara khusus, ini membahas berbagai jenis lingkungan cloud, rezim kontrol, dan peluang dukungan pengembang yang mungkin berlaku untuk organisasi dan tujuan bisnis Anda.

Multi-account strategy

Apa itu: Menerapkan praktik terbaik lingkungan cloud bergantung pada penerapan strategi multi-akun yang aman. Gunakan akun sebagai blok bangunan, dan kelompokkan ke dalam unit organisasi (OUs), seperti dasar OUs untuk keamanan dan infrastruktur, dan tambahan OUs untuk sandboxing dan beban kerja.

Mengapa itu penting: Strategi multi-akun memberikan batasan dan isolasi alami di lingkungan cloud Anda. Ini pada gilirannya memungkinkan Anda untuk mengelola kuota dan batas akun, mengotomatiskan penyediaan dan penyesuaian akun, dan menerapkan prinsip hak istimewa paling sedikit dengan membatasi akses ke akun manajemen Anda. Ini memungkinkan visibilitas untuk melacak aktivitas pengguna dan risiko di seluruh lingkungan Anda. Strategi multi-akun Anda bertindak sebagai fondasi di mana Anda dapat membangun proyek migrasi atau perubahan organisasi seperti merger dan akuisisi.

Gunakan AWS Organizationsuntuk mengkonsolidasikan beberapa Akun AWS ke dalam organisasi, yang dapat Anda gunakan untuk mengalokasikan sumber daya, akun grup, dan menerapkan kebijakan tata kelola.

Gunakan AWS Control Towersebagai layanan orkestrasi, berlapis di atas, untuk membantu menyusun AWS perkebunan Anda AWS Organizations, dan memperluas tata OUs kelola dan lingkungan multi-akun Anda.

Controls management best practices

Apa itu: Menerapkan praktik terbaik manajemen kontrol dapat mencakup berbagai pendekatan. Detective control menangkap sumber daya yang melanggar kebijakan keamanan yang ditetapkan. Kontrol preventif melindungi garis dasar keamanan dengan memblokir tindakan tertentu. Dan kontrol proaktif memindai sumber daya sebelum disediakan, menghentikan kode yang tidak sesuai agar tidak diterapkan, dan menginstruksikan pengembang untuk memperbaikinya. Interoperable Layanan AWS memberi Anda tata kelola terpusat dan kontrol atas seluruh IT estate Anda, termasuk AWS dan produk pihak ketiga, saat Anda tumbuh ke pasar baru.

Mengapa hal ini penting: Praktik terbaik manajemen kontrol memungkinkan Anda menerapkan kontrol secara terprogram dalam skala besar, dan secara otomatis mengonfigurasi kepatuhan atau memulihkan ketidakpatuhan. Ini sangat penting jika organisasi Anda beroperasi dalam industri yang diatur, seperti perawatan kesehatan, ilmu kehidupan, layanan keuangan, atau sektor publik, di mana kerangka peraturan khusus berlaku, atau mematuhi standar perusahaan tertentu, atau persyaratan residensi data dan kedaulatan digital.

Pertimbangkan peluang untuk mengatur beberapa Layanan AWS untuk memastikan kebutuhan keamanan dan kepatuhan organisasi Anda, menggunakan AWS Control Tower, menentukan pengaturan konfigurasi dan mendeteksi penyimpangan dari mereka, menggunakan, dan mengaudit AWS penggunaan dan kepatuhan terhadap peraturan dan standar industri AWS Config, dengan. AWS Audit Manager

Cloud governance for developers

Menerapkan praktik terbaik tata kelola cloud untuk pengembang dapat mencakup penggunaan infrastruktur sebagai kode (IAc) untuk memastikan pengulangan dan konsistensi dalam pekerjaan mereka, dan membangun proses untuk mendeteksi kerentanan keamanan.

Mengapa ini penting: Ini membantu tim bergerak cepat sambil percaya diri dalam proses tata kelola mereka. Ini memberi pengembang satu sumber kebenaran yang dapat digunakan ke seluruh tumpukan, infrastruktur yang dapat mereka replikasi, redeploy, dan digunakan kembali, kemampuan untuk mengontrol versi pada infrastruktur dan aplikasi bersama-sama, dan pilihan tindakan swalayan.

Tata kelola cloud untuk pengembang juga dapat melibatkan pendeteksian kerentanan keamanan dalam kode. Ini membantu mereka meningkatkan kualitas kode, mengidentifikasi masalah kritis, memastikan jalur rilis yang konsisten, dan meluncurkan proyek dengan cetak biru.

Pertimbangkan bagaimana Anda dapat memberikan infrastructure-as-code template yang telah disetujui sebelumnya kepada pembangun, dan kebijakan IAM terkait yang menentukan siapa, di mana, dan bagaimana mereka dapat digunakan, menggunakan Service Layanan AWS Catalog yang serupa.

Scalability and flexibility

Apa itu: Pilih Layanan AWS yang akan membantu langkah-langkah tata kelola cloud Anda tumbuh mulus dengan infrastruktur Anda dan beradaptasi dengan persyaratan yang terus berkembang. Pertimbangkan bagaimana organisasi Anda akan tumbuh, dan seberapa cepat.

Mengapa ini penting: Mempertimbangkan skalabilitas dan fleksibilitas membantu Anda memastikan bahwa pengaturan tata kelola cloud Anda kuat, responsif, dan mampu mendukung lingkungan bisnis yang dinamis.

Untuk membantu Anda menskalakan dengan cepat, AWS Control Tower mengatur kemampuan beberapa lainnya Layanan AWS, termasuk AWS Organizations dan AWS IAM Identity Center, untuk membangun landing zone dalam waktu kurang dari satu jam. Control Tower mengatur dan mengelola sumber daya atas nama Anda.

AWS Organizations memungkinkan Anda mengelola 40+ sumber daya layanan di beberapa akun. Ini memberi tim aplikasi individu fleksibilitas dan visibilitas untuk mengelola kebutuhan tata kelola cloud yang spesifik untuk beban kerja mereka, sementara juga memberi mereka visibilitas ke tim terpusat.

Pilih AWS layanan tata kelola cloud

Sekarang Anda tahu kriteria yang akan digunakan untuk mengevaluasi opsi tata kelola cloud Anda, Anda siap untuk memilih layanan tata kelola AWS cloud mana yang cocok untuk kebutuhan organisasi Anda. Tabel berikut menyoroti layanan mana yang dioptimalkan untuk keadaan apa. Gunakan untuk membantu menentukan layanan yang paling cocok untuk organisasi dan kasus penggunaan Anda.

Jenis kasus penggunaan	Kapan Anda akan menggunakannya?	Layanan yang direkomendasikan
Mendefinisikan persyaratan	Untuk menyediakan unduhan dokumen AWS keamanan dan kepatuhan sesuai permintaan.	AWS Artifact
Menyebarkan dan mengoperasikan	Untuk mempercepat penyediaan cloud dengan infrastruktur sebagai kode.	AWS CloudFormation
	Untuk mewakili pengaturan konfigurasi ideal Anda dan mendeteksi apakah AWS	AWS Config

Jenis kasus penggunaan	Kapan Anda akan menggunakannya?	Layanan yang direkomendasikan
	sumber daya melayang darinya.	
	Untuk mengatur dan mengatur beberapa Layanan AWS atas nama Anda sambil membantu Anda memenuhi kebutuhan keamanan dan kepatuhan organisasi Anda.	AWS Control Tower
	Untuk mengkonsolidasikan beberapa Akun AWS ke dalam organisasi, yang dapat Anda gunakan untuk mengalokasikan sumber daya, akun grup, menerapkan kebijakan tata kelola, dan mengelola secara terpusat dan dalam skala besar.	AWS Organizations
	Untuk menjalankan pemeriksaan otomatis dan berkelanjutan terhadap aturan dalam seperangkat standar keamanan yang didukung.	AWS Security Hub
	Untuk menyediakan infrastructure-as-code template yang disetujui sebelumnya kepada pembangun, dan kebijakan IAM yang sesuai, yang menentukan siapa, di mana, dan bagaimana mereka dapat digunakan.	Katalog Layanan

Jenis kasus penggunaan	Kapan Anda akan menggunakannya?	Layanan yang direkomendasikan
	Untuk menyediakan end-to-end pengelolaan sumber daya yang aman di dalam AWS dan di lingkungan multicloud dan hybrid.	AWS Systems Manager
Mengukur dan menilai	Untuk mengaudit AWS penggunaan dan menilai risiko dan kepatuhan terhadap peraturan dan standar industri.	AWS Audit Manager
	Untuk memungkinkan audit operasional dan risiko, tata kelola, dan kepatuhan Anda. Akun AWS	AWS CloudTrail
	Untuk memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time.	Amazon CloudWatch
	Untuk mengelola lisensi perangkat lunak dari vendor secara terpusat di seluruh AWS dan lingkungan lokal Anda.	AWS License Manager
	Untuk mengevaluasi penggunaan dan konfigurasi terhadap praktik terbaik.	AWS Trusted Advisor

Gunakan AWS layanan tata kelola cloud

Anda sekarang harus memiliki pemahaman yang jelas tentang apa yang dilakukan setiap layanan tata kelola AWS cloud, dan mana yang mungkin tepat untuk Anda.

Untuk mengeksplorasi cara menggunakan dan mempelajari lebih lanjut tentang masing-masing layanan tata kelola AWS cloud yang tersedia, kami telah menyediakan jalur untuk mengeksplorasi cara kerja masing-masing layanan tersebut. Bagian berikut menyediakan tautan ke dokumentasi mendalam, tutorial langsung, dan sumber daya lainnya untuk membantu Anda memulai.

AWS Artifact

- Memulai dengan AWS Artifact

  Unduh laporan keamanan dan kepatuhan, kelola perjanjian hukum, dan kelola pemberitahuan.

  Jelajahi panduannya”
- Mengelola perjanjian di AWS Artifact

  Gunakan Konsol Manajemen AWS untuk meninjau, menerima, dan mengelola perjanjian untuk akun atau organisasi Anda.

  Jelajahi panduannya”
- Mempersiapkan Audit di AWS Bagian 1 — AWS Audit Manager, AWS Config, dan AWS Artifact

  Gunakan Layanan AWS layanan untuk membantu Anda mengotomatiskan pengumpulan bukti yang digunakan dalam audit.

  Baca blognya”

AWS Audit Manager

- Memulai dengan AWS Audit Manager

  Aktifkan Audit Manager dengan menggunakan Konsol Manajemen AWS, Audit Manager API, atau AWS CLI.

  Jelajahi panduannya”
- Tutorial untuk Pemilik Audit: Membuat penilaian

Buat penilaian dengan menggunakan Audit Manager Sample Framework.

Memulai dengan tutorial”

- Tutorial untuk Delegasi: Meninjau set kontrol

  Tinjau set kontrol yang dibagikan dengan Anda oleh pemilik audit di Audit Manager.

  Memulai dengan tutorial”

AWS CloudTrail

- Lihat riwayat acara

  Tinjau aktivitas AWS API di layanan Akun AWS yang mendukung Anda CloudTrail.

  Memulai dengan tutorial”

- Buat jejak untuk mencatat peristiwa manajemen

  Buat jejak untuk mencatat peristiwa manajemen di semua Wilayah.

  Memulai dengan tutorial”

AWS Config

- AWS Config fitur

  Jelajahi kemampuan pelacakan sumber daya AWS Config, mulai dari riwayat konfigurasi dan snapshot hingga aturan dan paket kesesuaian yang dapat disesuaikan.

  Jelajahi bimbingan”

- Bagaimana Cara AWS Config Kerja

  Selami lebih dalam AWS Config, dan pelajari bagaimana layanan menemukan dan melacak sumber daya, dan mengirimkan item konfigurasi melalui berbagai saluran.

  Jelajahi panduannya”

- Lokakarya Risiko dan Kepatuhan

  Otomatiskan kontrol dengan menggunakan AWS Config dan Aturan Konfigurasi AWS Terkelola.

Jelajahi lokakarya”

- AWS Config Pustaka Rule Development Kit: Membangun dan mengoperasikan aturan dalam skala besar

  Gunakan Rule Development Kit (RDK) untuk membuat AWS Config aturan khusus dan menerapkannya dengan. RDKLib

  Baca blognya”

AWS Control Tower

- Memulai dengan AWS Control Tower

  Pelajari cara mengatur landing zone Anda menggunakan AWS Control Tower konsol atau APIs.

  Jelajahi panduannya”

- AWS Control Tower lokakarya manajemen kontrol

  Pelajari cara mengatur tata kelola di lingkungan multi-akun Anda agar selaras dengan praktik AWS terbaik dan kerangka kerja kepatuhan umum.

  Jelajahi lokakarya”

- Memodernisasi Manajemen Akun dengan Amazon Bedrock dan AWS Control Tower

  Menyediakan akun alat keamanan dan memanfaatkan AI generatif untuk mempercepat proses Akun AWS penyiapan dan manajemen.

  Baca blognya”

- Membangun lingkungan yang dirancang dengan baik dengan AWS GovCloud (US) AWS Control Tower

  Siapkan tata kelola Anda di AWS GovCloud (US) Wilayah, termasuk mengatur AWS beban kerja Anda dengan menggunakan Unit Organisasi () OUs dan. Akun AWS

  Baca blognya”

AWS Organizations

- Memulai dengan AWS Organizations

  Pelajari cara mulai menggunakan AWS Organizations, termasuk meninjau terminologi dan konsep, menggunakan penagihan konsolidasi, dan menerapkan kebijakan organisasi.

  Jelajahi panduannya”
- Membuat dan mengkonfigurasi organisasi

  Buat organisasi Anda dan konfigurasikan dengan dua akun AWS anggota.

  Mulai dengan tutorial”
- Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun

  Pelajari cara menggunakan beberapa Akun AWS dapat membantu mengisolasi dan mengelola aplikasi dan data bisnis Anda, serta mengoptimalkan seluruh pilar AWS Well-Architected Framework.

  Baca whitepaper”
- Layanan yang bekerja dengan AWS Organizations

  Pahami Layanan AWS layanan mana yang dapat Anda gunakan AWS Organizations dan manfaat menggunakan setiap layanan pada tingkat organisasi.

  Jelajahi panduannya”
- Praktik Terbaik untuk Unit Organisasi dengan AWS Organizations

  Selami arsitektur praktik AWS terbaik yang direkomendasikan saat membangun organisasi Anda, untuk struktur OU dan contoh implementasi spesifik.

  Baca blognya”
- Mencapai keunggulan operasional dengan pertimbangan desain untuk AWS Organizations SCPs

  Pelajari cara SCPs mengontrol akses Layanan AWS dan sumber daya yang disediakan di beberapa akun yang dibuat dalam organisasi.

  Baca blognya”

AWS Security Hub

- Mengaktifkan AWS Security Hub

  Aktifkan AWS Security Hub dengan AWS Organizations atau di akun mandiri.

  Jelajahi panduannya”
- Agregasi lintas Wilayah

  AWS Security Hub Temuan agregat dari beberapa Wilayah AWS ke satu Wilayah agregasi.

  Jelajahi panduannya”
- AWS Security Hub lokakarya

  Pelajari cara menggunakan AWS Security Hub dan mengelola serta meningkatkan postur keamanan AWS lingkungan Anda.

  Jelajahi lokakarya”
- Tiga pola penggunaan Security Hub berulang dan cara menerapkannya

  Pelajari tentang tiga pola AWS Security Hub penggunaan yang paling umum dan cara meningkatkan strategi Anda untuk mengidentifikasi dan mengelola temuan.

  Baca blognya”

Jelajahi sumber AWS daya tata kelola cloud

Diagram arsitektur

Jelajahi diagram arsitektur referensi untuk membantu Anda mengembangkan strategi keamanan, identitas, dan tata kelola Anda.

Jelajahi diagram arsitektur

Laporan Resmi

Jelajahi whitepaper untuk lebih banyak wawasan dan praktik terbaik dalam memilih, menerapkan, dan menggunakan layanan keamanan, identitas, dan tata kelola yang paling sesuai dengan organisasi Anda.

Jelajahi whitepaper

Solusi

Gunakan solusi ini untuk mengembangkan dan menyempurnakan strategi keamanan, identitas, dan tata kelola Anda.

Jelajahi solusinya

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada panduan keputusan ini. Untuk pemberitahuan tentang pembaruan panduan ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Publikasi awal	Panduan pertama kali diterbitkan.	Oktober 4, 2024

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