Merangkul Zero Trust: Strategi untuk transformasi bisnis yang aman dan gesit

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Merangkul Zero Trust: Strategi untuk transformasi bisnis yang aman dan gesit

Table of Contents

Merangkul Zero Trust: Strategi untuk transformasi bisnis yang aman dan gesit

Greg Gooden, Amazon Web Services () AWS

Desember 2023 (riwayat dokumen)

Saat ini, lebih dari sebelumnya, organisasi berfokus pada keamanan sebagai prioritas utama. Hal ini memungkinkan berbagai manfaat, mulai dari menjaga kepercayaan pelanggan mereka, meningkatkan mobilitas tenaga kerja mereka, hingga membuka peluang bisnis digital baru. Ketika mereka melakukannya, mereka terus mengajukan pertanyaan kuno: Apa pola optimal untuk memastikan tingkat keamanan dan ketersediaan yang tepat untuk sistem dan data saya? Semakin banyak, Zero Trust telah menjadi istilah yang digunakan untuk menggambarkan jawaban modern untuk pertanyaan ini.

Zero trust architecture (ZTA) adalah model konseptual dan seperangkat mekanisme terkait yang berfokus pada penyediaan kontrol keamanan di sekitar aset digital yang tidak semata-mata atau fundamental bergantung pada kontrol jaringan tradisional atau perimeter jaringan. Sebaliknya, kontrol jaringan ditambah dengan identitas, perangkat, perilaku, dan konteks dan sinyal kaya lainnya untuk membuat keputusan akses yang lebih terperinci, cerdas, adaptif, dan berkelanjutan. Dengan menerapkan model ZTA, Anda dapat mencapai iterasi berikutnya yang bermakna dalam pematangan berkelanjutan keamanan siber dan konsep pertahanan secara mendalam khususnya.

Proses pengambilan keputusan

Menerapkan strategi ZTA membutuhkan perencanaan dan pengambilan keputusan yang cermat. Ini melibatkan evaluasi berbagai faktor dan menyelaraskannya dengan tujuan organisasi. Proses pengambilan keputusan utama untuk memulai perjalanan ZTA meliputi:

1. Keterlibatan pemangku kepentingan - Sangat penting untuk melibatkan orang lain CxOs, VP, dan manajer senior untuk memahami prioritas, kekhawatiran, dan visi mereka untuk postur keamanan organisasi Anda. Dengan melibatkan pemangku kepentingan utama sejak awal, Anda dapat menyelaraskan implementasi ZTA dengan tujuan strategis keseluruhan dan mendapatkan dukungan dan sumber daya yang diperlukan.
2. Penilaian risiko — Melakukan penilaian risiko yang komprehensif membantu mengidentifikasi masalah, luas permukaan yang berlebihan, dan aset penting, yang membantu Anda membuat

keputusan berdasarkan informasi tentang kontrol keamanan dan investasi. Mengevaluasi postur keamanan organisasi Anda yang ada, mengidentifikasi kelemahan potensial, dan memprioritaskan area perbaikan berdasarkan lanskap risiko yang spesifik untuk industri dan lingkungan operasional Anda.

3. Evaluasi teknologi — Menilai lanskap teknologi organisasi yang ada dan mengidentifikasi kesenjangan membantu dalam memilih alat dan solusi yang tepat yang selaras dengan prinsip-prinsip ZTA. Evaluasi ini harus mencakup analisis menyeluruh dari hal-hal berikut:
   - Arsitektur jaringan
   - Sistem manajemen identitas dan akses
   - Mekanisme otentikasi dan otorisasi
   - Manajemen titik akhir terpadu
   - Alat dan proses kepemilikan sumber daya
   - Teknologi enkripsi
   - Kemampuan pemantauan dan pencatatan
   - Memilih tumpukan teknologi yang tepat sangat penting untuk membangun model ZTA yang kuat.
4. Manajemen perubahan — Mengenali dampak budaya dan organisasi dari mengadopsi model ZTA sangat penting. Menerapkan praktik manajemen perubahan membantu memastikan kelancaran transisi dan penerimaan di seluruh organisasi. Ini melibatkan mendidik karyawan tentang prinsip dan manfaat ZTA, memberikan pelatihan tentang praktik keamanan baru, dan menumbuhkan budaya sadar keamanan yang mendorong akuntabilitas dan pembelajaran berkelanjutan.

Panduan preskriptif ini bertujuan untuk memberikan CxOs, VP, dan manajer senior dengan strategi komprehensif untuk menerapkan ZTA. Ini akan menyelidiki aspek-aspek kunci ZTA, termasuk yang berikut:

- Kesiapan organisasi
- Pendekatan adopsi bertahap
- Kolaborasi pemangku kepentingan
- Praktik terbaik untuk mencapai transformasi bisnis yang aman dan gesit

Dengan mengikuti panduan ini, organisasi Anda dapat menavigasi lanskap ZTA dan mencapai hasil yang sukses dalam perjalanan keamanan Anda di Amazon Web Services (AWS) Cloud. AWSmenawarkan berbagai layanan yang dapat Anda gunakan untuk menerapkan ZTA, sepertiAkses

Terverifikasi AWS, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway, dan Amazon. GuardDuty Layanan ini dapat membantu melindungi AWS sumber daya dari akses yang tidak sah.

Hasil bisnis yang ditargetkan

Bagian ini membahas hasil yang diharapkan terkait dengan mendefinisikan dan menerapkan arsitektur zero trust di seluruh organisasi Anda.

Postur keamanan yang ditingkatkan

Dengan mengadopsi prinsip Zero Trust, organisasi Anda dapat memperkuat postur keamanannya, mengurangi risiko keamanan, dan melindungi infrastruktur dan data cloud Anda. Prinsip dasar Zero Trust dalam memberikan akses atas need-to-know dasar, ditambah dengan kontrol yang ketat, secara signifikan mengurangi luas permukaan, dan membatasi dampak potensial dari peristiwa keamanan. Pendekatan proaktif ini membantu organisasi tetap berada di depan risiko keamanan yang muncul dan membantu memastikan kerahasiaan, integritas, dan ketersediaan aset.

Adopsi cloud yang mulus

Mengembangkan rencana adopsi arsitektur zero trust (ZTA) yang terdefinisi dengan baik dapat membantu memastikan transisi yang lancar dan sukses ke lingkungan cloud. Prinsip-prinsip ZTA selaras erat dengan praktik terbaik keamanan cloud dengan memberikan fondasi yang kuat bagi organisasi untuk mendapatkan manfaat komputasi awan dengan aman. Memasukkan prinsip-prinsip ZTA sejak awal membantu organisasi Anda merancang arsitektur cloud-nya dengan keamanan sebagai elemen inti.

Kepatuhan dan penyelarasan peraturan

Menerapkan praktik ZTA dapat membantu organisasi Anda memenuhi persyaratan dan standar industri dan peraturan. ZTA secara inheren mempromosikan prinsip hak istimewa paling sedikit dan menegakkan kontrol akses yang ketat. Kontrol akses sering diamanatkan oleh peraturan seperti berikut:

- Program Manajemen Risiko dan Otorisasi Federal (FedRAMP)
- Undang-Undang Akuntabilitas dan Portabilitas Asuransi Kesehatan (Health Insurance Portability and Accountability Act/HIPAA)
- Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS).

Dengan mengadopsi Zero Trust, organisasi Anda dapat membantu menunjukkan komitmennya terhadap perlindungan data, privasi, dan kepatuhan terhadap peraturan sambil meminimalkan potensi hukuman atau kerusakan reputasi.

Perlindungan data yang ditingkatkan

Organizations dapat melindungi data sensitif selama proses adopsi cloud dengan menerapkan enkripsi data, kontrol akses, dan penilaian keamanan reguler. Organisasi Anda dapat mengambil langkah-langkah spesifik berikut:

- Enkripsi data — Enkripsi data — Enkripsi data adalah proses mengenkripsi data cleartext ke dalam ciphertext dengan cara yang memerlukan kunci untuk mendekripsi data kembali ke bentuk cleartext asli. Hal ini membuat jauh lebih sulit bagi individu yang tidak berwenang untuk mengakses data sensitif, bahkan jika mereka dapat memperoleh salinan data.
- Kontrol akses — Kontrol akses membatasi siapa yang dapat mengakses data sensitif dan apa yang dapat mereka lakukan dengannya. Ini dapat dilakukan dengan menetapkan peran dan izin pengguna, dan dengan menggunakan otentikasi multi-faktor atau metode lain untuk memverifikasi identitas pengguna.
- Penilaian keamanan reguler — Penilaian keamanan reguler dapat membantu organisasi mengidentifikasi dan mengatasi masalah keamanan dan secara proaktif memperbaikinya. Penilaian ini dapat dilakukan oleh tim keamanan internal atau oleh perusahaan keamanan eksternal.

Arsitektur zero trust mengambil pendekatan komprehensif terhadap perlindungan data dengan menerapkan sejumlah langkah keamanan. Ukuran ini termasuk otentikasi yang kuat, enkripsi data, dan kontrol akses granular. Pendekatan ini meminimalkan risiko peristiwa keamanan terkait data, dan melindungi informasi sensitif dari akses yang tidak sah.

Respon insiden yang efisien

Organizations dapat mendeteksi dan merespons peristiwa keamanan dengan lebih cepat dan efektif dengan membangun kerangka kerja pemantauan dan respons insiden di lingkungan cloud. Arsitektur zero trust menekankan pemantauan berkelanjutan, integrasi intelijen ancaman, dan visibilitas real-time ke dalam aktivitas pengguna, lalu lintas jaringan, dan perilaku sistem. Tim keamanan kemudian dapat secara proaktif mengidentifikasi dan mengurangi peristiwa keamanan. Pendekatan

ini mengurangi waktu untuk mendeteksi dan menanggapi masalah potensial, dan meminimalkan dampak pada operasi bisnis. Poin-poin utama meliputi:

- Pengujian — Terlepas dari kerangka kerja atau metodologi respons insiden yang selaras dengan organisasi Anda, Anda harus menguji rencana respons insiden Anda secara teratur. Latihan meja, simulasi, dan tim merah memberikan kesempatan untuk mempraktikkan respons insiden dalam pengaturan realistis, mengungkap kesenjangan perkakas dan kemampuan, dan membangun pengalaman dan kepercayaan diri responden insiden.
- Monitoring — Terus memantau lingkungan cloud Anda untuk tanda-tanda aktivitas abnormal. Anda dapat melakukan ini dengan menggunakan berbagai alat dan teknik, seperti analisis log, pemantauan jaringan, dan pemindaian kerentanan.
- Integrasi intelijen ancaman — Integrasikan intelijen ancaman ke dalam kerangka pemantauan dan respons insiden Anda. Ini akan membantu organisasi Anda mengidentifikasi dan menanggapi ancaman dengan lebih cepat dan efektif.
- Visibilitas real-time — Untuk mengidentifikasi dan menanggapi insiden keamanan dengan cepat, organisasi Anda memerlukan visibilitas real-time ke dalam aktivitas pengguna, lalu lintas jaringan, dan perilaku sistem.
- Identifikasi dan mitigasi proaktif — Dengan secara proaktif mengidentifikasi dan mengurangi peristiwa keamanan, organisasi Anda dapat mengurangi waktu untuk mendeteksi dan menanggapi potensi ancaman, meminimalkan dampak pada operasi bisnis.

Peningkatan produktivitas tenaga kerja

Tenaga kerja modern membutuhkan fleksibilitas untuk menyelesaikan pekerjaan dari berbagai lokasi, perangkat, dan waktu yang semakin meningkat. Dengan menerapkan ZTA, Anda dapat mendukung persyaratan ini dan meningkatkan mobilitas, produktivitas, dan kepuasan tenaga kerja, sambil mempertahankan atau meningkatkan postur keamanan organisasi.

Aktifkan transformasi digital

Organizations semakin mengejar interkoneksi perangkat, mesin, fasilitas, infrastruktur, dan proses di luar perimeter jaringan tradisional sebagai bagian dari transformasi digital. Internet of things (IoT) dan teknologi operasional (OT, juga dikenal sebagai Industrial Internet of Things, atau IIoT) sering mengirimkan telemetri dan informasi pemeliharaan prediktif langsung ke cloud. Untuk melindungi

beban kerja, ini memerlukan penerapan kontrol keamanan yang melampaui pendekatan perimeter tradisional.

Ringkasan bagian

Dengan berfokus pada hasil bisnis yang ditargetkan ini, organisasi Anda dapat mewujudkan potensi penuh ZTA dan memperkuat postur keamanan Anda di cloud. Penting untuk menyelaraskan hasil ini dengan tujuan organisasi tertentu, menyesuaikannya dengan kebutuhan bisnis unik Anda, dan secara teratur menilai efektivitasnya untuk mendorong peningkatan berkelanjutan.

Memahami prinsip Zero Trust

Zero trust architecture (ZTA) didasarkan pada seperangkat prinsip inti yang membentuk fondasi model keamanannya. Memahami prinsip-prinsip ini sangat penting bagi organisasi yang ingin mengadopsi strategi ZTA secara efektif. Bagian ini mencakup prinsip-prinsip inti ZTA.

Verifikasi dan otentikasi

Prinsip verifikasi dan otentikasi menekankan pentingnya identifikasi dan otentikasi yang kuat untuk semua jenis prinsip, termasuk pengguna, mesin, dan perangkat. ZTA memerlukan verifikasi identitas dan status otentikasi berkelanjutan selama sesi, idealnya pada setiap permintaan. Itu tidak hanya bergantung pada lokasi atau kontrol jaringan tradisional. Ini termasuk menerapkan otentikasi multi-faktor kuat modern (MFA) dan mengevaluasi sinyal lingkungan dan kontekstual tambahan selama proses otentikasi. Dengan mengadopsi prinsip ini, organisasi dapat membantu memastikan bahwa keputusan otorisasi sumber daya memiliki masukan identitas terbaik.

Akses hak istimewa paling sedikit

Prinsip hak istimewa terkecil melibatkan pemberian kepala sekolah tingkat akses minimum yang diperlukan untuk melakukan tugas-tugas mereka. Dengan mengadopsi prinsip akses hak istimewa terkecil, organisasi dapat menegakkan kontrol akses granular, sehingga kepala sekolah hanya memiliki akses ke sumber daya yang diperlukan untuk memenuhi peran dan tanggung jawab mereka. Ini termasuk menerapkan penyediaan just-in-time akses, kontrol akses berbasis peran (RBAC), dan tinjauan akses reguler untuk meminimalkan luas permukaan dan risiko akses yang tidak sah.

Segmentasi mikro

Segmentasi mikro adalah strategi keamanan jaringan yang membagi jaringan menjadi segmen yang lebih kecil dan terisolasi untuk mengotorisasi arus lalu lintas tertentu. Anda dapat mencapai segmentasi mikro dengan membuat batasan beban kerja dan menegakkan kontrol akses yang ketat antara segmen yang berbeda.

Segmentasi mikro dapat diimplementasikan melalui virtualisasi jaringan, jaringan yang ditentukan perangkat lunak (SDN), firewall berbasis host, daftar kontrol akses jaringan (NACL), dan fitur spesifik seperti Amazon AWS Elastic Compute Cloud (Amazon EC2) grup keamanan atau. AWS PrivateLink

Gateway segmentasi mengontrol lalu lintas antar segmen untuk secara eksplisit mengotorisasi akses. Segmentasi mikro dan segmentasi gateway membantu organisasi membatasi jalur yang tidak perlu melalui jaringan, terutama yang mengarah pada sistem dan data kritis.

Pemantauan dan analitik berkelanjutan

Pemantauan dan analitik berkelanjutan melibatkan pengumpulan, analisis, dan korelasi peristiwa dan data terkait keamanan di seluruh lingkungan organisasi Anda. Dengan menerapkan alat pemantauan dan analitik yang kuat, organisasi Anda dapat mengevaluasi data keamanan dan telemetri secara konvergen.

Prinsip ini menekankan pentingnya visibilitas ke perilaku pengguna, lalu lintas jaringan, dan aktivitas sistem untuk mengidentifikasi anomali dan peristiwa keamanan potensial. Teknologi canggih seperti informasi keamanan dan manajemen peristiwa (SIEM), analisis perilaku pengguna dan entitas (UEBA), dan platform intelijen ancaman memainkan peran penting dalam mencapai pemantauan berkelanjutan dan deteksi ancaman proaktif.

Otomatisasi dan orkestrasi

Otomatisasi dan orkestrasi membantu organisasi untuk merampingkan proses keamanan, mengurangi intervensi manual, dan meningkatkan waktu respons. Dengan mengotomatiskan tugas keamanan rutin dan menggunakan kemampuan orkestrasi, organisasi Anda dapat menerapkan kebijakan keamanan yang konsisten dan merespons peristiwa keamanan dengan cepat. Prinsip ini juga mencakup otomatisasi penyediaan akses dan proses deprovisioning untuk membantu memastikan pengelolaan izin pengguna yang tepat waktu dan akurat. Dengan merangkul otomatisasi dan orkestrasi, organisasi Anda dapat meningkatkan efisiensi operasional, mengurangi kesalahan manusia, dan memfokuskan sumber daya pada inisiatif keamanan yang lebih strategis.

Otorisasi

Dalam ZTA, setiap permintaan untuk mengakses sumber daya harus secara eksplisit disahkan oleh titik penegakan gating. Selain identitas yang diautentikasi, kebijakan otorisasi harus mempertimbangkan konteks tambahan, seperti kesehatan dan postur perangkat, pola perilaku, klasifikasi sumber daya, dan faktor jaringan. Proses otorisasi harus mengevaluasi konteks konvergen ini terhadap kebijakan akses terkait yang relevan dengan sumber daya yang diakses. Secara optimal, model pembelajaran mesin dapat memberikan suplemen dinamis untuk kebijakan deklaratif.

Ketika digunakan, model ini harus fokus pada pembatasan tambahan saja, dan mereka tidak boleh memberikan akses yang tidak ditentukan secara eksplisit.

Ringkasan bagian

Dengan mengikuti prinsip-prinsip inti ZTA ini, organisasi dapat membangun model keamanan yang kuat yang selaras dengan keragaman lingkungan perusahaan modern. Menerapkan prinsip-prinsip ini membutuhkan pendekatan komprehensif yang menggabungkan teknologi, proses, dan orang-orang untuk mencapai pola pikir nol kepercayaan dan membangun postur keamanan yang tangguh.

Komponen kunci dari arsitektur zero trust

Untuk menerapkan strategi zero trust architecture (ZTA) secara efektif, organisasi Anda harus memahami komponen kunci yang membentuk ZTA. Komponen-komponen ini bekerja sama untuk terus meningkatkan model keamanan komprehensif yang selaras dengan prinsip Zero Trust. Bagian ini mencakup komponen-komponen kunci dari ZTA.

Pengelolaan identitas dan akses

Manajemen identitas dan akses membentuk fondasi ZTA dengan menyediakan otentikasi pengguna yang kuat dan mekanisme kontrol akses kasar. Ini mencakup teknologi seperti sistem masuk tunggal (SSO), otentikasi multi-faktor (MFA), dan tata kelola identitas dan solusi manajemen. Manajemen identitas dan akses memberikan jaminan otentikasi tingkat tinggi dan konteks penting yang merupakan bagian integral untuk membuat keputusan otorisasi tanpa kepercayaan. Pada saat yang sama, ZTA adalah model keamanan di mana akses ke aplikasi dan sumber daya diberikan berdasarkan per pengguna, per perangkat, dan per sesi. Ini membantu melindungi organisasi dari akses yang tidak sah, bahkan jika kredensil pengguna dikompromikan.

Tepi layanan akses aman

Secure Access Service Edge (SASE) adalah pendekatan baru untuk keamanan jaringan yang memvirtualisasi, menggabungkan, dan mendistribusikan fungsi jaringan dan keamanan ke dalam satu layanan berbasis cloud. SASE dapat menyediakan akses aman ke aplikasi dan sumber daya, terlepas dari lokasi pengguna.

SASE mencakup berbagai fitur keamanan, seperti gateway web aman, firewall sebagai layanan, dan akses jaringan zero trust (ZTNA). Fitur-fitur ini bekerja sama untuk melindungi organisasi dari berbagai ancaman, termasuk malware, phishing, dan ransomware.

Pencegahan kehilangan data

Teknologi pencegahan kehilangan data (DLP) dapat membantu organisasi melindungi data sensitif dari pengungkapan yang tidak sah. Solusi DLP memantau dan mengontrol data dalam gerakan dan saat istirahat. Ini membantu organisasi untuk menentukan dan menegakkan kebijakan yang mencegah peristiwa keamanan terkait data, membantu memastikan bahwa informasi sensitif tetap terlindungi di seluruh jaringan.

Informasi keamanan dan manajemen acara

Solusi manajemen informasi dan acara keamanan (SIEM) mengumpulkan, mengumpulkan, dan menganalisis log peristiwa keamanan dari berbagai sumber di seluruh infrastruktur organisasi. Anda dapat menggunakan data ini untuk mendeteksi insiden keamanan, memfasilitasi respons insiden, dan memberikan wawasan tentang potensi ancaman dan kerentanan.

Untuk ZTA secara khusus, kemampuan solusi SIEM untuk mengkorelasikan dan memahami telemetri terkait dari sistem keamanan yang berbeda sangat penting untuk meningkatkan deteksi dan respons terhadap pola abnormal.

Katalog kepemilikan sumber daya perusahaan

Untuk memberikan akses ke sumber daya perusahaan dengan benar, organisasi harus memiliki sistem yang andal yang mengkatalogkan sumber daya ini dan, yang penting, siapa yang memilikinya. Sumber kebenaran ini perlu menyediakan alur kerja yang memfasilitasi permintaan akses, keputusan persetujuan terkait, dan pengesahan reguler darinya. Pada waktunya, sumber kebenaran ini akan berisi jawaban untuk “siapa yang dapat mengakses apa?” di dalam organisasi. Anda dapat menggunakan jawaban untuk otorisasi dan audit dan kepatuhan.

Manajemen titik akhir terpadu

Selain mengautentikasi pengguna dengan kuat, ZTA juga harus mempertimbangkan kesehatan, postur, dan keadaan perangkat pengguna untuk menilai apakah data perusahaan dan akses sumber daya aman. Platform manajemen endpoint terpadu (UEM) menyediakan kemampuan berikut:

- Penyediaan perangkat
- Konfigurasi yang sedang berlangsung dan manajemen tambalan
- Baselining keamanan
- Pelaporan telemetri
- Pembersihan perangkat dan pensiun

Poin penegakan berbasis kebijakan

Dalam ZTA, akses ke setiap sumber daya harus secara eksplisit disahkan oleh titik penegakan hukum berbasis kebijakan gating. Awalnya, poin penegakan ini dapat didasarkan pada titik

penegakan yang ada di jaringan dan sistem identitas yang ada. Poin penegakan hukum dapat dibuat secara bertahap lebih mampu dengan mempertimbangkan susunan konteks dan sinyal yang lebih luas yang disediakan ZTA. Jangka panjang, organisasi Anda harus menerapkan poin penegakan khusus ZTA yang beroperasi pada konteks konvergen, secara konsisten mengintegrasikan penyedia sinyal, mempertahankan seperangkat kebijakan yang komprehensif, dan ditingkatkan dengan kecerdasan yang diperoleh dari telemetri gabungan.

Ringkasan bagian

Memahami komponen-komponen kunci ini sangat penting bagi organisasi yang berencana untuk mengadopsi ZTA. Dengan menerapkan komponen-komponen ini dan mengintegrasikannya ke dalam model keamanan yang kohesif, organisasi Anda dapat membangun postur keamanan yang kuat berdasarkan prinsip-prinsip Zero Trust. Bagian berikut mengeksplorasi kesiapan organisasi, pendekatan adopsi bertahap, dan praktik terbaik untuk membantu Anda berhasil menerapkan ZTA dalam organisasi Anda.

Menilai kesiapan organisasi untuk adopsi Zero Trust

Mengadopsi strategi arsitektur baru adalah usaha penting yang membutuhkan perencanaan yang cermat dan pertimbangan faktor organisasi. Bagian ini berfokus pada pertimbangan kesiapan organisasi utama untuk adopsi Zero Trust di seluruh perusahaan. Dengan mengatasi pertimbangan ini, organisasi Anda dapat membuka jalan bagi postur keamanan yang lebih kuat dan lebih sukses.

Penyelarasan kepemimpinan dan komunikasi

Penyelarasan kepemimpinan dan komunikasi sangat penting untuk keberhasilan implementasi Zero Trust. Kepemimpinan harus memahami manfaat Zero Trust dan sumber daya yang dibutuhkan. Pemimpin juga harus bersedia melakukan perubahan pada budaya dan proses organisasi. Komunikasi dengan karyawan diperlukan untuk membangun kepercayaan dan pembelian. Karyawan perlu memahami mengapa organisasi menerapkan Zero Trust, apa artinya bagi mereka, dan bagaimana mereka dapat membantu. Komunikasi harus terbuka, transparan, dan berkelanjutan.

Dukungan kepemimpinan dan buy-in

Untuk implementasi arsitektur zero trust (ZTA) yang sukses, sangat penting bagi Anda untuk menyelaraskan pemangku kepentingan dan eksekutif utama pada tujuan arsitektur, manfaat, dan ukuran keberhasilan. Bagikan pentingnya prinsip Zero Trust dalam meningkatkan keamanan dan memungkinkan kelincahan bisnis dengan beralih dari keamanan berbasis perimeter tradisional ke pendekatan yang lebih terperinci dan berpusat pada pengguna. Dengan beralih ke pendekatan ini, organisasi Anda dapat beradaptasi dengan perubahan dan ancaman lebih cepat. Penyelarasan eksekutif menetapkan nada untuk organisasi dan membantu mengatasi potensi resistensi terhadap perubahan.

Komunikasi transparan

Menjaga komunikasi yang terbuka dan transparan dengan karyawan selama proses implementasi Zero Trust. Jelaskan alasan, manfaat, dan hasil yang diharapkan dari adopsi, dan atasi masalah dengan segera. Berikan pembaruan rutin tentang kemajuan implementasi. Ini akan meningkatkan buy-in, mengurangi resistensi, dan membangun kepercayaan.

Pengembangan keterampilan dan pelatihan

Setelah kepemimpinan selaras dan komunikasi terbuka, penting untuk mengembangkan keterampilan dan pengetahuan karyawan yang akan menerapkan Zero Trust. Ini termasuk

memahami prinsip-prinsip Zero Trust, bagaimana menerapkannya dalam pekerjaan mereka, dan bagaimana menanggapi peristiwa keamanan. Memberikan kesempatan pelatihan dan pengembangan untuk membantu karyawan memperoleh keterampilan ini.

Pengetahuan dan keterampilan cloud

Menilai kesenjangan keterampilan dan pengetahuan organisasi dalam teknologi cloud dan prinsip Zero Trust. Menyediakan program pelatihan dan pengembangan untuk meningkatkan keterampilan karyawan dan membekali mereka dengan keahlian yang diperlukan untuk bekerja secara efektif di lingkungan cloud-centric dan Zero Trust. Untuk mengimbangi perkembangan teknologi dan praktik keamanan, kembangkan budaya pembelajaran berkelanjutan.

Budaya dan kesadaran keamanan

Menilai budaya keamanan organisasi. Mengevaluasi tingkat kesadaran keamanan di antara karyawan, pemahaman mereka tentang praktik terbaik keamanan, dan kepatuhan mereka terhadap kebijakan dan prosedur. Identifikasi kesenjangan dalam pengetahuan keamanan. Pertimbangkan untuk melakukan program pelatihan kesadaran keamanan untuk mendidik karyawan tentang pentingnya Zero Trust dan peran mereka dalam menjaga lingkungan yang aman.

Struktur dan peran organisasi

Untuk berhasil menerapkan Zero Trust, buatlah struktur dan peran organisasi yang efektif. Ini termasuk membuat Cloud Center of Excellence (CCoE), meninjau dan memodifikasi operasi keamanan, dan menetapkan peran dan tanggung jawab untuk manajemen kerentanan, respons insiden, dan pemantauan keamanan.

Pusat Keunggulan Cloud

Menetapkan CCoE untuk memberikan panduan, praktik terbaik, dan pengawasan untuk operasi cloud. CCoE adalah tim atau sekelompok individu yang bertanggung jawab untuk membuat dan menerapkan praktik terbaik, pedoman, dan kebijakan tata kelola terkait cloud. CCoE harus mencakup perwakilan dari berbagai unit bisnis dan tim TI untuk membantu memastikan kolaborasi dan keselarasan. CCoE memainkan peran penting dalam mendorong penerapan prinsip Zero Trust ke dalam beban kerja yang dihosting cloud. CCoE juga memfasilitasi berbagi pengetahuan di seluruh organisasi.

Operasi keamanan

Untuk memenuhi kebutuhan lingkungan Zero Trust, tinjau dan modifikasi organisasi operasi keamanan saat ini. Untuk meningkatkan kemampuan pemantauan, respons insiden, dan intelijen ancaman, pertimbangkan untuk menerapkan pusat operasi keamanan (SoC) atau penyedia layanan keamanan terkelola (MSSP). Menetapkan peran dan tanggung jawab untuk manajemen kerentanan, respons insiden, dan pemantauan keamanan. Proses respons insiden yang berfungsi dengan baik sangat penting untuk memastikan bahwa peristiwa keamanan kecil dapat dideteksi dan diperbaiki dengan cepat untuk mengganggu urutan peristiwa. Ini membantu mencegah peristiwa kecil berkembang menjadi peristiwa yang lebih berdampak.

Infrastruktur dan arsitektur TI

Periksa arsitektur TI dan infrastruktur perusahaan Anda untuk menemukan kendala atau dependensi yang mungkin memengaruhi penerapan pendekatan Zero Trust. Tentukan apakah aplikasi dan sistem saat ini kompatibel dengan komponen arsitektur zero trust yang diperlukan. Analisis apakah ada perbaikan atau penyesuaian infrastruktur yang diperlukan untuk mendukung keberhasilan penerapan prinsip Zero Trust. Untuk setiap aplikasi atau sistem, pertimbangkan apakah Zero Trust paling baik diterapkan di tempat atau melalui upaya modernisasi yang lebih besar.

Manajemen risiko, tata kelola, dan pengendalian perubahan

Untuk berhasil menerapkan Zero Trust, Menetapkan manajemen risiko, tata kelola, dan proses pengendalian perubahan yang efektif. Ini termasuk menyelaraskan manajemen risiko dengan prinsip Zero Trust, mengembangkan rencana respons insiden, bekerja dengan departemen hukum dan kepatuhan, dan menetapkan proses pengendalian perubahan.

Manajemen risiko

Periksa strategi manajemen risiko yang ada di perusahaan Anda dan tentukan seberapa baik strategi tersebut mematuhi prinsip-prinsip Zero Trust. Menganalisis efisiensi sistem respons insiden saat ini, langkah-langkah keamanan, dan prosedur penilaian risiko. Tentukan area mana yang perlu ditingkatkan agar sesuai dengan strategi Zero Trust. Mulailah mengembangkan sistem respons insiden otomatis atau kerangka pemantauan dan analitik berkelanjutan untuk meningkatkan kecepatan resolusi.

Ubah proses kontrol

Untuk membantu memastikan bahwa semua modifikasi terkait cloud mematuhi persyaratan keamanan dan kepatuhan, buat metode kontrol perubahan yang efektif. Menetapkan prosedur

manajemen perubahan sistematis yang mencakup analisis konfigurasi keamanan, evaluasi risiko, persetujuan, dan dokumentasi. Tinjau dan audit pembaruan sesering mungkin untuk menjaga integritas arsitektur zero trust.

Pemantauan dan evaluasi

Agar berhasil menerapkan Zero Trust, organisasi Anda harus terus memantau dan mengevaluasi postur keamanannya. Ini termasuk menetapkan indikator kinerja utama (KPI), memantau dan mengevaluasi KPI, dan menumbuhkan budaya perbaikan berkelanjutan. Dengan mengikuti langkah-langkah ini, organisasi dapat memastikan bahwa implementasi Zero Trust mereka berhasil dan bahwa mereka selalu bekerja untuk meningkatkan keamanan mereka.

Indikator kinerja utama

Menetapkan indikator kinerja kunci terkait (KPI) untuk mengukur keberhasilan dan kemanjuran penyebaran Zero Trust. KPI ini dapat mengukur kepuasan pengguna, kemajuan peralatan dan peluncuran, pengurangan biaya, kepatuhan kepatuhan, dan jumlah kejadian keamanan. Untuk melacak perkembangan secara keseluruhan dan menemukan peluang untuk perbaikan, secara teratur memantau dan mengevaluasi KPI ini.

Perbaikan berkelanjutan

Membangun sistem untuk memperoleh pendapat dan wawasan dari para pemangku kepentingan akan membantu menumbuhkan budaya perbaikan berkelanjutan. Dorong anggota staf untuk menawarkan pemikiran dan proposal untuk meningkatkan keamanan, efektivitas, dan pengalaman pengguna lingkungan cloud. Gunakan masukan ini untuk merampingkan prosedur, meningkatkan langkah-langkah keamanan, dan memacu inovasi.

Ringkasan bagian

Dengan menangani pertimbangan organisasi dan budaya ini, organisasi Anda dapat menumbuhkan lingkungan yang mendukung untuk adopsi cloud dari model keamanan Zero Trust. Bagian selanjutnya mengeksplorasi pendekatan adopsi bertahap, memberikan panduan tentang cara menerapkan prinsip Zero Trust secara bertahap dengan cara yang praktis dan dapat dikelola.

Menumbuhkan pola pikir Zero Trust

Menerapkan Zero Trust melampaui implementasi teknis. Hal ini membutuhkan pergeseran budaya dalam organisasi Anda. Membina pola pikir Zero Trust melibatkan penekanan aspek-aspek kunci berikut.

Pendidikan dan pelatihan Zero Trust

Mendidik karyawan tentang nilai-nilai dan keuntungan dari arsitektur zero trust (ZTA). Memberikan penjelasan teknis dan non-teknis tentang konsep dan pendekatan ZTA melalui sesi pelatihan, lokakarya, dan sumber daya lainnya. Dorong anggota staf untuk menyadari tanggung jawab mereka dalam membangun dan menegakkan paradigma keamanan Zero Trust.

Kolaborasi dan komunikasi

Menumbuhkan kolaborasi dan transparansi di semua tim dan departemen yang terlibat dalam implementasi ZTA. Untuk memastikan setiap orang memiliki pemahaman menyeluruh tentang rencana tersebut, mempromosikan komunikasi lintas fungsi, berbagi pengetahuan, dan pertukaran informasi. Ciptakan budaya tanggung jawab bersama di mana setiap orang menyadari pentingnya kontribusi mereka terhadap keamanan bisnis secara keseluruhan.

Pembelajaran dan peningkatan berkelanjutan

Prioritaskan pembelajaran berkelanjutan dan peningkatan dalam konteks Zero Trust. Dorong karyawan untuk tetap mengikuti perkembangan tren keamanan, teknologi, dan praktik terbaik terkini. Memupuk budaya inovasi dan eksperimen di mana karyawan didorong untuk mengeksplorasi solusi dan pendekatan baru untuk memperkuat postur keamanan organisasi.

Metrik dan akuntabilitas

Tetapkan metrik dan mekanisme akuntabilitas yang jelas untuk mengukur efektivitas strategi Zero Trust. Tentukan indikator kinerja utama (KPI) yang selaras dengan tujuan keamanan organisasi, dan melacak kemajuan secara teratur. Meminta pertanggungjawaban individu dan tim atas kontribusi mereka terhadap implementasi dan pemeliharaan prinsip-prinsip Zero Trust.

Ringkasan bagian

Dengan mengatasi aspek-aspek ini dan menumbuhkan pola pikir Zero Trust, organisasi dapat menciptakan fondasi yang kuat untuk keberhasilan adopsi dan implementasi Zero Trust. Pergeseran budaya ini sangat penting untuk membantu semua orang dalam organisasi memahami pentingnya Zero Trust dan secara aktif berkontribusi pada keberhasilannya.

Bagian selanjutnya mengeksplorasi pendekatan adopsi bertahap, memberikan panduan tentang cara menerapkan prinsip-prinsip Zero Trust secara bertahap secara praktis dan mudah dikelola.

Pendekatan bertahap ke Zero Trust

Adopsi arsitektur zero trust (ZTA) membutuhkan perencanaan dan implementasi yang cermat. Kami merekomendasikan pendekatan adopsi bertahap untuk kelancaran transisi dan meminimalkan gangguan pada operasi bisnis. Bagian ini memberikan panduan tentang fase-fase kunci yang terlibat dalam mengadopsi ZTA.

Tahap 1: Penilaian dan Perencanaan

Tahap pertama implementasi Zero Trust adalah penilaian dan perencanaan. Fase ini sangat penting untuk keberhasilan implementasi secara keseluruhan, karena melibatkan identifikasi dan penanganan kesenjangan dalam postur keamanan organisasi Anda saat ini. Dengan meluangkan waktu untuk menilai keadaan Anda saat ini dan menentukan tujuan keamanan Anda, Anda dapat meletakkan dasar untuk implementasi Zero Trust yang sukses.

Pada saat yang sama, penilaian yang sempurna dan akurat mungkin tidak selalu realistis. Untuk menghindari kelumpuhan analisis yang mencegah Anda beralih ke fase lebih lanjut, bersiaplah untuk mengelompokkan atau menerima beberapa tingkat ketidaksempurnaan.

1. Menilai keadaan saat ini — Lakukan penilaian terhadap infrastruktur, kebijakan, dan kontrol keamanan yang ada. Identifikasi potensi kerentanan, kesenjangan dalam keamanan, dan area di mana penerapan prinsip Zero Trust dapat memberikan perbaikan.
2. Tentukan tujuan keamanan — Berdasarkan temuan penilaian negara saat ini, tentukan tujuan keamanan yang selaras dengan prinsip-prinsip Zero Trust. Tujuan keamanan ini juga harus selaras dengan strategi keamanan organisasi Anda secara keseluruhan dan mengatasi kerentanan dan kesenjangan yang teridentifikasi.
3. Rancang arsitektur — Kembangkan ZTA yang mendukung tujuan keamanan organisasi Anda. Arsitektur ini harus mencakup komponen yang diperlukan, seperti solusi manajemen identitas dan akses, mekanisme segmentasi jaringan, dan sistem pemantauan berkelanjutan. Arsitektur juga harus terukur, mudah beradaptasi, dan mampu mengakomodasi pertumbuhan masa depan dan kemajuan teknologi. Idealnya, arsitektur ini harus direpresentasikan dalam format yang mudah dikonsumsi oleh tim yang bertanggung jawab untuk mengimplementasikannya, seperti AWS CloudFormation templat, bukan hanya sebagai dokumen atau diagram.
4. Libatkan pemangku kepentingan — Libatkan semua pemangku kepentingan, termasuk unit bisnis, tim TI, dan tim keamanan, untuk mendapatkan wawasan dan menyelaraskan tujuan mereka

dengan rencana implementasi ZTA. Mendorong kolaborasi dan komunikasi untuk membangun pemahaman bersama tentang manfaat dan persyaratan pendekatan Zero Trust.

Tahap 2: Piloting dan implementasi

Tahap kedua implementasi Zero Trust adalah piloting dan implementasi. Fase ini melibatkan pengujian ZTA dalam skala kecil, lingkungan terkontrol, dan kemudian secara berulang menerapkannya di seluruh organisasi Anda. Penting untuk mendidik karyawan tentang langkah-langkah keamanan baru dan peran mereka dalam menjaga lingkungan Zero Trust.

1. Pilot penyebaran - Uji ZTA dalam skala kecil, lingkungan yang terkendali. Menerapkan komponen yang diperlukan dan kontrol keamanan yang didefinisikan dalam fase desain arsitektur. Pantau penyebaran pilot dengan cermat, kumpulkan umpan balik, dan buat penyesuaian yang diperlukan. Bersiaplah untuk fleksibel di awal proses, ketika Zero Trust beralih dari latihan hipotetis ke latihan yang Anda bangun dengan pengalaman nyata.
2. Terapkan secara iteratif — Berdasarkan pelajaran yang dipetik dari penerapan pilot, mulailah penyebaran berulang Zero Trust di seluruh organisasi. Bangun momentum melalui efek flywheel yang tidak memerlukan kampanye ekstensif untuk mencapai massa penyebaran kritis. Cadangan mandat kepemimpinan atau eskalasi untuk ekor peluncuran yang lebih panjang di mana mereka mungkin diperlukan.
3. Memberikan pelatihan pengguna dan meningkatkan kesadaran — Mendidik karyawan tentang langkah-langkah keamanan baru dan peran mereka dalam menjaga lingkungan Zero Trust. Tekankan pentingnya praktik aman, seperti kata sandi yang kuat, otentikasi multi-faktor, dan pembaruan keamanan rutin.
4. Kelola perubahan — Buat rencana manajemen perubahan yang komprehensif untuk mengatasi perubahan organisasi dan budaya yang terkait dengan adopsi Zero Trust. Komunikasikan manfaat dan alasan di balik adopsi kepada karyawan, dan atasi masalah atau penolakan apa pun. Memberikan dukungan dan bimbingan berkelanjutan untuk memfasilitasi transisi yang mulus.

Tahap 3: Pemantauan dan perbaikan berkelanjutan

Tahap ketiga dan terakhir dari implementasi Zero Trust adalah pemantauan dan perbaikan berkelanjutan. Fase ini melibatkan pembentukan program pemantauan dan analitik yang komprehensif, membuat rencana respons insiden yang komprehensif, dan secara teratur meminta umpan balik dari pemangku kepentingan dan pengguna.

1. Pantau terus menerus — Buat program pemantauan dan analitik yang komprehensif untuk menilai postur keamanan secara terus menerus dan mendeteksi potensi anomali. Gunakan alat dan teknologi keamanan canggih untuk memantau perilaku pengguna, lalu lintas jaringan, dan aktivitas sistem.
2. Rencanakan respons insiden dan remediasi — Buat rencana respons insiden komprehensif yang selaras dengan prinsip Zero Trust. Tetapkan jalur eskalasi yang jelas, tentukan peran dan tanggung jawab, dan terapkan mekanisme respons insiden otomatis jika memungkinkan. Uji dan perbarui rencana respons insiden secara teratur.
3. Dapatkan umpan balik dan evaluasi — Secara teratur meminta umpan balik dari pemangku kepentingan dan pengguna untuk mengumpulkan wawasan tentang efektivitas arsitektur zero trust (ZTA). Melakukan evaluasi dan penilaian berkala untuk mengukur dampak pada postur keamanan, efisiensi operasional, dan pengalaman pengguna. Gunakan umpan balik dan hasil evaluasi untuk mengidentifikasi area untuk perbaikan. Harapkan bahwa ZTA Anda akan berubah seiring waktu, dan pertimbangkan bagaimana tim pengembangan akan menerapkan pembaruan ini dengan sedikit usaha atau gangguan.

Ringkasan bagian

Dengan mengikuti pendekatan adopsi bertahap ini, organisasi dapat secara efektif beralih ke ZTA sambil meminimalkan risiko dan gangguan. Bagian selanjutnya membahas praktik terbaik untuk mencapai kesuksesan dengan implementasi Zero Trust, yang mencakup pertimbangan dan rekomendasi utama untuk CxOs, VP, dan manajer senior.

Praktik terbaik untuk mencapai kesuksesan dengan Zero Trust

Keberhasilan adopsi arsitektur zero trust (ZTA) membutuhkan pendekatan strategis dan kepatuhan terhadap praktik terbaik. Bagian ini menyajikan serangkaian praktik terbaik untuk memandu CxOs, VP, dan manajer senior dalam mencapai kesuksesan dengan adopsi Zero Trust mereka. Dengan mengikuti rekomendasi ini, organisasi Anda dapat membangun fondasi keamanan yang kuat dan menyadari manfaat dari pendekatan Zero Trust:

- Tentukan tujuan dan hasil bisnis yang jelas — Tentukan dengan jelas tujuan dan hasil bisnis yang diinginkan dari operasi cloud. Selaraskan tujuan ini dengan prinsip-prinsip Zero Trust untuk membangun fondasi keamanan yang kuat sekaligus memungkinkan pertumbuhan bisnis dan inovasi.
- Melakukan penilaian komprehensif — Lakukan evaluasi komprehensif terhadap infrastruktur, aplikasi, dan aset data TI saat ini. Identifikasi dependensi, utang teknis, dan potensi masalah kompatibilitas. Evaluasi ini akan menginformasikan rencana adopsi dan membantu memprioritaskan beban kerja berdasarkan kekritisan, kompleksitas, dan dampak bisnis.
- Kembangkan rencana adopsi — Gabungkan rencana adopsi terperinci yang menguraikan step-by-step pendekatan untuk memindahkan beban kerja, aplikasi, dan data ke cloud. Tentukan fase adopsi, garis waktu, dan dependensi. Libatkan pemangku kepentingan utama dan alokasikan sumber daya yang sesuai.
- Mulai membangun lebih awal — Kemampuan Anda untuk secara otentik mewakili seperti apa Zero Trust dalam organisasi Anda akan meningkat secara substansif setelah Anda mulai membangun dan menerapkannya (daripada menganalisis dan membicarakannya).
- Dapatkan sponsor eksekutif — Sponsor eksekutif yang aman dan dukungan untuk implementasi Zero Trust. Libatkan eksekutif tingkat C lainnya untuk memperjuangkan inisiatif dan mengalokasikan sumber daya yang diperlukan. Komitmen kepemimpinan sangat penting untuk mendorong perubahan budaya dan organisasi yang diperlukan untuk implementasi yang sukses.
- Menerapkan kerangka tata kelola — Buat kerangka kerja tata kelola yang mendefinisikan peran, tanggung jawab, dan proses pengambilan keputusan untuk implementasi Zero Trust. Mendefinisikan dengan jelas akuntabilitas dan kepemilikan kontrol keamanan, manajemen risiko, dan kepatuhan. Secara teratur meninjau dan memperbarui kerangka tata kelola untuk beradaptasi dengan persyaratan keamanan yang berkembang.

- Support kolaborasi lintas fungsi — Mendorong kolaborasi dan komunikasi antara berbagai unit bisnis, tim TI, dan tim keamanan. Ciptakan budaya tanggung jawab bersama untuk mendorong keselarasan dan koordinasi di seluruh implementasi Zero Trust. Dorong interaksi yang sering, berbagi pengetahuan, dan pemecahan masalah bersama.
- Amankan data dan aplikasi Anda — Zero Trust tidak hanya tentang pengguna akhir yang mengakses sumber daya dan aplikasi. Prinsip Zero Trust juga harus diterapkan di dalam dan di antara beban kerja. Terapkan prinsip teknis yang sama — identitas yang kuat, segmentasi mikro, dan otorisasi — dengan menggunakan semua konteks yang tersedia di dalam pusat data juga.
- Memberikan pertahanan secara mendalam — Menerapkan defense-in-depth strategi dengan menggunakan beberapa lapisan kontrol keamanan. Menggabungkan berbagai teknologi keamanan, seperti otentikasi multi-faktor (MFA), segmentasi jaringan, enkripsi, dan deteksi anomali, untuk memberikan perlindungan komprehensif. Pastikan bahwa setiap lapisan melengkapi yang lain untuk menciptakan sistem pertahanan yang kuat.
- Memerlukan otentikasi yang kuat - Menerapkan mekanisme otentikasi yang kuat, seperti MFA, untuk semua pengguna yang mengakses semua sumber daya. Idealnya, pertimbangkan MFA modern, seperti kunci keamanan yang didukung perangkat keras FIDO2, yang memberikan jaminan otentikasi tingkat tinggi untuk Zero Trust dan membawa manfaat keamanan yang luas (misalnya, perlindungan terhadap phishing).
- Memusatkan dan meningkatkan otorisasi — Secara khusus mengotorisasi setiap upaya akses. Bergantung pada spesifikasi protokol, ini harus dilakukan berdasarkan per-koneksi atau per-permintaan. Per-permintaan sangat ideal. Gunakan semua konteks yang tersedia, termasuk identitas, perangkat, perilaku, dan informasi jaringan untuk membuat keputusan otorisasi yang lebih terperinci, adaptif, dan canggih.
- Gunakan prinsip hak istimewa terkecil — Menerapkan prinsip hak istimewa terkecil untuk memberikan pengguna hak akses minimum yang diperlukan untuk melakukan tugas pekerjaan mereka. Secara teratur meninjau dan memperbarui izin akses berdasarkan peran pekerjaan, tanggung jawab, dan kebutuhan bisnis. Menerapkan penyediaan just-in-time akses.
- Gunakan manajemen akses istimewa - Menerapkan solusi manajemen akses istimewa (PAM) untuk mengamankan akun istimewa dan mengurangi risiko akses tidak sah ke sistem kritis. Solusi PAM dapat memberikan kontrol akses istimewa, perekaman sesi, dan kemampuan audit untuk membantu organisasi Anda melindungi data dan sistemnya yang paling sensitif.
- Gunakan segmentasi mikro — Bagilah jaringan Anda menjadi segmen yang lebih kecil dan lebih terisolasi. Gunakan segmentasi mikro untuk menegakkan kontrol akses yang ketat antar segmen berdasarkan peran pengguna, aplikasi, atau sensitivitas data. Berusaha keras untuk menghilangkan semua jalur jaringan yang tidak perlu, terutama yang mengarah ke data.

- Pantau dan tanggapi peringatan keamanan — Menerapkan program pemantauan keamanan dan respons insiden yang komprehensif di lingkungan cloud. Gunakan alat dan layanan keamanan cloud-native untuk mendeteksi ancaman secara real time, menganalisis log, dan mengotomatiskan respons insiden. Menetapkan prosedur respons insiden yang jelas, melakukan penilaian keamanan secara teratur, dan terus memantau anomali atau aktivitas yang mencurigakan.
- Gunakan pemantauan berkelanjutan — Untuk mendeteksi dan menanggapi insiden keamanan dengan cepat dan efektif, terapkan pemantauan berkelanjutan. Gunakan alat analisis keamanan canggih untuk memantau perilaku pengguna, lalu lintas jaringan, dan aktivitas sistem. Otomatiskan peringatan dan notifikasi untuk memastikan bahwa insiden ditanggapi tepat waktu.
- Mempromosikan budaya keamanan dan kepatuhan — Mempromosikan budaya keamanan dan kepatuhan di seluruh organisasi. Mendidik karyawan tentang praktik terbaik keamanan, pentingnya mematuhi prinsip Zero Trust, dan peran karyawan dalam menjaga lingkungan cloud yang aman. Melakukan pelatihan kesadaran keamanan secara teratur untuk membantu memastikan bahwa karyawan waspada terhadap rekayasa sosial dan bahwa mereka memahami tanggung jawab mereka mengenai perlindungan data dan privasi.
- Gunakan simulasi rekayasa sosial - Lakukan simulasi rekayasa sosial untuk menilai kerentanan pengguna terhadap serangan rekayasa sosial. Gunakan hasil simulasi untuk menyesuaikan program pelatihan untuk meningkatkan kesadaran pengguna dan respons terhadap potensi ancaman.
- Mempromosikan pendidikan berkelanjutan - Membangun budaya pendidikan dan pembelajaran berkelanjutan dengan memberikan pelatihan dan sumber daya keamanan yang berkelanjutan. Beri tahu pengguna tentang praktik terbaik keamanan yang berkembang. Dorong pengguna untuk tetap waspada dan melaporkan aktivitas mencurigakan dengan segera.
- Terus menilai dan mengoptimalkan — Secara teratur menilai lingkungan cloud untuk area perbaikan. Gunakan alat cloud-native untuk memantau penggunaan dan kinerja sumber daya, serta melakukan penilaian kerentanan dan pengujian penetrasi untuk mengidentifikasi dan mengatasi kelemahan apa pun.
- Menetapkan kerangka kerja tata kelola dan kepatuhan — Kembangkan kerangka kerja tata kelola dan kepatuhan untuk membantu memastikan bahwa organisasi Anda selaras dengan standar industri dan persyaratan peraturan. Dalam kerangka kerja, tentukan kebijakan, prosedur, dan kontrol untuk melindungi data dan sistem dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah. Menerapkan mekanisme untuk melacak dan melaporkan metrik kepatuhan, melakukan audit rutin, dan menangani masalah ketidakpatuhan dengan segera.

- Mendorong kolaborasi dan berbagi pengetahuan — Mendorong kolaborasi dan berbagi pengetahuan di antara tim yang terlibat dalam adopsi ZTA. Anda dapat melakukan ini dengan mendorong komunikasi lintas fungsi dan kolaborasi antara TI, keamanan, dan unit bisnis. Organisasi Anda juga dapat membuat forum, lokakarya, dan sesi berbagi pengetahuan untuk mempromosikan pemahaman, mengatasi tantangan, dan berbagi pelajaran selama proses adopsi.

Takeaways kunci

Panduan ini telah mengeksplorasi aspek-aspek penting dari pengembangan strategi arsitektur zero trust (ZTA) yang sukses. Bagian ini merangkum takeaways utama dari panduan preskriptif yang disajikan:

- Memahami prinsip Zero Trust — Zero Trust adalah model konseptual dan serangkaian mekanisme terkait yang berfokus pada penyediaan kontrol keamanan di sekitar aset digital yang tidak semata-mata atau secara fundamental bergantung pada kontrol jaringan tradisional atau perimeter jaringan. Sebaliknya, kontrol jaringan ditambah dengan identitas, perangkat, perilaku, dan konteks dan sinyal kaya lainnya untuk membuat keputusan akses yang lebih terperinci, cerdas, adaptif, dan berkelanjutan. Biasakan diri Anda dengan prinsip-prinsip inti Zero Trust, seperti hak istimewa terkecil, segmentasi mikro, otentikasi berkelanjutan, dan otorisasi adaptif.
- Tentukan tujuan yang jelas — Tentukan dengan jelas tujuan dan hasil bisnis yang diinginkan dari adopsi ZTA. Selaraskan tujuan ini dengan prinsip-prinsip Zero Trust untuk membantu memastikan fondasi keamanan yang kuat sekaligus memungkinkan pertumbuhan dan inovasi bisnis.
- Lakukan penilaian komprehensif — Lakukan penilaian menyeluruh terhadap infrastruktur, aplikasi, dan aset data TI Anda yang ada. Identifikasi ketergantungan, utang teknis, dan masalah kompatibilitas untuk menginformasikan strategi adopsi Anda.
- Kembangkan rencana adopsi ZTA — Buat rencana terperinci yang menguraikan step-by-step pendekatan untuk memindahkan beban kerja, aplikasi, dan data ke cloud. Pertimbangkan faktor-faktor seperti persyaratan kepatuhan dan modernisasi aplikasi.
- Menerapkan ZTA yang kuat - Merancang dan menerapkan ZTA yang memberlakukan kontrol akses granular, mekanisme otentikasi yang kuat, dan pemantauan berkelanjutan. Untuk adopsi ZTA yang lebih efisien, gunakan layanan Zero Trust cloud-native, seperti dan Akses Terverifikasi AWS Amazon VPC Lattice.
- Prioritaskan keamanan data dan aplikasi — Terapkan prinsip Zero Trust — identitas yang kuat, segmentasi mikro, dan otorisasi — untuk menyediakan semua konteks yang tersedia. Gunakan konteks ini untuk pengguna yang mengakses sistem dan sumber daya dan untuk aliran komunikasi dan data di dalam dan di antara komponen backend.
- Menetapkan kerangka kerja pemantauan dan respons insiden — Menerapkan pemantauan keamanan yang kuat dan kemampuan respons insiden di lingkungan cloud. Gunakan alat keamanan cloud-native untuk deteksi ancaman real-time, analisis log, dan otomatisasi respons insiden, seperti Amazon InspectorAWS Security Hub, dan Amazon. GuardDuty

- Menumbuhkan budaya keamanan dan kepatuhan - Mempromosikan budaya kesadaran keamanan dan kepatuhan di seluruh organisasi. Mendidik karyawan tentang praktik terbaik keamanan dan peran mereka dalam menjaga lingkungan cloud yang aman.
- Terus menilai dan mengoptimalkan — Secara teratur menilai lingkungan cloud, kontrol keamanan, dan proses operasional. Untuk mengumpulkan wawasan dan mengoptimalkan pemanfaatan sumber daya, manajemen biaya, dan kinerja, gunakan alat analisis dan pemantauan cloud-native seperti Amazon dan. CloudWatch AWS Security Hub
- Menetapkan kerangka kerja tata kelola dan kepatuhan — Mengembangkan kerangka kerja tata kelola dan kepatuhan yang selaras dengan standar industri dan persyaratan peraturan. Tetapkan kebijakan, prosedur, dan kontrol untuk membantu memastikan kepatuhan terhadap standar keamanan, privasi, dan kepatuhan.

Langkah selanjutnya

Mengadopsi arsitektur zero trust (ZTA) adalah salah satu cara paling aman untuk meningkatkan postur organisasi Anda dan mengurangi risiko. Panduan preskriptif ini telah memberi Anda peta jalan komprehensif untuk menerapkan Zero Trust, mulai dari memahami prinsip-prinsip hingga menilai kesiapan Anda, hingga menerapkan komponen yang diperlukan.

Langkah selanjutnya dalam alur kerja atau domain ini melibatkan hal-hal berikut:

- Menerapkan rencana adopsi
- Menerapkan ZTA
- Melakukan penilaian keamanan secara teratur
- Terus mengoptimalkan lingkungan cloud dan kontrol keamanan

ZTA adalah proses berkelanjutan yang membutuhkan pemantauan, evaluasi, dan adaptasi yang konstan untuk memastikan fondasi keamanan yang kuat. Dengan mengikuti praktik terbaik yang diuraikan dalam panduan ini, organisasi Anda dapat meningkatkan postur keamanannya, memastikan kepatuhan terhadap peraturan, dan melindungi data sensitif.

Pertanyaan yang Sering Diajukan

Bagian ini memberikan jawaban atas pertanyaan umum tentang merancang dan menerapkan arsitektur zero trust (ZTA).

Apa itu Zero Trust?

Zero trust adalah model konseptual dan serangkaian mekanisme terkait yang berfokus pada penyediaan kontrol keamanan di sekitar aset digital yang tidak semata-mata atau secara fundamental bergantung pada kontrol jaringan tradisional atau perimeter jaringan. Sebaliknya, kontrol jaringan ditambah dengan identitas, perangkat, perilaku, dan konteks dan sinyal kaya lainnya untuk membuat keputusan akses yang lebih terperinci, cerdas, adaptif, dan berkelanjutan.

Apa yang Layanan AWS dapat membantu saya menerapkan arsitektur zero trust?

AWSmenyediakan beberapa layanan yang dapat membantu dalam menerapkan Zero Trust, seperti, AWS Identity and Access Management (IAM)Akses Terverifikasi AWS, Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway, dan Amazon. GuardDuty

Bagaimana saya bisa memastikan keamanan data denganAWS?

AWSmenawarkan layanan seperti AWS Key Management Service (AWS KMS) untuk enkripsi data saat istirahat dan dalam perjalanan, Amazon Virtual Private Cloud (Amazon VPC) untuk isolasi jaringan, dan AWS Secrets Manager untuk penyimpanan dan pengambilan kredensional yang aman.

Dapatkah AWS membantu dengan persyaratan kepatuhan di lingkungan Zero Trust?

Ya, AWS memiliki program dan layanan kepatuhan untuk membantu memenuhi berbagai persyaratan peraturan. AWS Artifactmenyediakan akses ke laporan AWS kepatuhan, dan AWS Config mendukung pemantauan dan penilaian kepatuhan yang berkelanjutan.

Apakah ada AWS alat atau layanan untuk mengotomatiskan keamanan di lingkungan Zero Trust?

AWSmenyediakan layanan sepertiAWS Security Hub, yang memusatkan dan mengotomatiskan temuan keamanan, dan AWS Config aturan untuk mendefinisikan dan menegakkan kebijakan keamanan.

Bagaimana saya bisa memastikan pemantauan berkelanjutan dan respons insiden di lingkungan cloud Zero Trust dengan AWS

AWSmenawarkan layanan seperti Amazon CloudWatch untuk pemantauan waktu nyata dan AWS CloudTrail untuk pencatatan dan analisis. Untuk praktik terbaik respons insiden, Anda dapat menggunakan Panduan Respons Insiden AWS Keamanan.

Sumber daya

References

- Apa yang dimaksud dengan cloud center of excellence dan mengapa organisasi Anda harus membuatnya? — Posting blog ini memberikan gambaran umum tentang CCoE, praktik terbaik untuk cara membuat CCoE yang efektif, dan banyak lagi.
- Zero Trust on AWS — Halaman ini memberikan gambaran umum tentang prinsip keamanan Zero Trust dan praktik terbaik di AWS lingkungan.
- Arsitektur Zero Trust: Sebuah AWS perspektif — Posting blog ini berbagi definisi dan prinsip panduan tentang cara Zero Trust diimplementasikan. AWS
- AWS Identity and Access ManagementPanduan Pengguna (IAM) — Panduan ini menawarkan dokumentasi komprehensif tentang pengelolaan akses pengguna dan izin di IAM, komponen penting dari arsitektur zero trust.
- AWS Security Hub— Pelajari tentang Security Hub, layanan yang memberikan pandangan komprehensif tentang peringatan keamanan dan status kepatuhan di seluruh AndaAkun AWS.
- AWSWell-Architected Framework — Jelajahi Well-Architected Framework, yang memberikan panduan untuk membangun arsitektur yang aman, berkinerja tinggi, tangguh, dan efisien. AWS
- AWSPanduan Respons Insiden Keamanan — Panduan ini menyajikan ikhtisar dasar-dasar menanggapi insiden keamanan dalam lingkungan organisasi Anda. AWS Cloud Ini memberikan gambaran umum tentang keamanan cloud dan konsep respons insiden dan mengidentifikasi kemampuan cloud, layanan, dan mekanisme yang tersedia bagi pelanggan yang menanggapi masalah keamanan.

Alat

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty

- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- Akses Terverifikasi AWS

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Menambahkan pembaruan	Menambahkan informasi ke Komponen kunci dari bagian arsitektur nol kepercayaan, membuat perubahan di bagian Menilai kesiapan organisasi untuk adopsi Zero Trust, menambahkan informasi ke bagian Praktik Terbaik, dan membuat perubahan pada FAQ.	Desember 4, 2023
Publikasi awal	—	19 Juni 2023

AWS Glosarium Panduan Preskriptif

Berikut ini adalah istilah yang umum digunakan dalam strategi, panduan, dan pola yang disediakan oleh Panduan AWS Preskriptif. Untuk menyarankan entri, silakan gunakan tautan Berikan umpan balik di akhir glosarium.

Nomor

7 Rs

Tujuh strategi migrasi umum untuk memindahkan aplikasi ke cloud. Strategi ini dibangun di atas 5 Rs yang diidentifikasi Gartner pada tahun 2011 dan terdiri dari yang berikut:

- Refactor/Re-Architect — Memindahkan aplikasi dan memodifikasi arsitekturnya dengan memanfaatkan sepenuhnya fitur cloud-native untuk meningkatkan kelincahan, kinerja, dan skalabilitas. Ini biasanya melibatkan porting sistem operasi dan database. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Aurora Postgre -Compatible Edition. SQL
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: Memigrasikan database Oracle lokal Anda ke Amazon Relational Database Service (RDSAmazon) untuk Oracle di. AWS Cloud
- Pembelian kembali (drop and shop) - Beralih ke produk yang berbeda, biasanya dengan beralih dari lisensi tradisional ke model SaaS. Contoh: Migrasikan sistem manajemen hubungan pelanggan (CRM) Anda ke Salesforce.com.
- Rehost (lift dan shift) — Pindahkan aplikasi ke cloud tanpa membuat perubahan apa pun untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Oracle pada instance EC2 di. AWS Cloud
- Relokasi (hypervisor-level lift and shift) — Pindahkan infrastruktur ke cloud tanpa membeli perangkat keras baru, menulis ulang aplikasi, atau memodifikasi operasi yang ada. Anda memigrasikan server dari platform lokal ke layanan cloud untuk platform yang sama. Contoh: Migrasi a Microsoft Hyper-V aplikasi untuk AWS.
- Pertahankan (kunjungi kembali) - Simpan aplikasi di lingkungan sumber Anda. Ini mungkin termasuk aplikasi yang memerlukan refactoring besar, dan Anda ingin menunda pekerjaan itu sampai nanti, dan aplikasi lama yang ingin Anda pertahankan, karena tidak ada pembenaran bisnis untuk memigrasikannya.

- Pensiun — Menonaktifkan atau menghapus aplikasi yang tidak lagi diperlukan di lingkungan sumber Anda.

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ACID

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

Metode migrasi database di mana database sumber dan target tetap sinkron (dengan menggunakan alat replikasi dua arah atau operasi penulisan ganda), dan kedua database menangani transaksi dari menghubungkan aplikasi selama migrasi. Metode ini mendukung migrasi dalam batch kecil yang terkontrol alih-alih memerlukan pemotongan satu kali. Ini lebih fleksibel tetapi membutuhkan lebih banyak pekerjaan daripada migrasi aktif-pasif.

migrasi aktif-pasif

Metode migrasi database di mana database sumber dan target disimpan dalam sinkron, tetapi hanya database sumber yang menangani transaksi dari menghubungkan aplikasi sementara data direplikasi ke database target. Basis data target tidak menerima transaksi apa pun selama migrasi.

fungsi agregat

SQLFungsi yang beroperasi pada sekelompok baris dan menghitung nilai pengembalian tunggal untuk grup. Contoh fungsi agregat meliputi `SUM` dan`MAX`.

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

Proses menghapus informasi pribadi secara permanen dalam kumpulan data. Anonimisasi dapat membantu melindungi privasi pribadi. Data anonim tidak lagi dianggap sebagai data pribadi.

anti-pola

Solusi yang sering digunakan untuk masalah berulang di mana solusinya kontra-produktif, tidak efektif, atau kurang efektif daripada alternatif.

kontrol aplikasi

Pendekatan keamanan yang memungkinkan penggunaan hanya aplikasi yang disetujui untuk membantu melindungi sistem dari malware.

portofolio aplikasi

Kumpulan informasi rinci tentang setiap aplikasi yang digunakan oleh organisasi, termasuk biaya untuk membangun dan memelihara aplikasi, dan nilai bisnisnya. Informasi ini adalah kunci untuk penemuan portofolio dan proses analisis dan membantu mengidentifikasi dan memprioritaskan aplikasi yang akan dimigrasi, dimodernisasi, dan dioptimalkan.

kecerdasan buatan (AI)

Bidang ilmu komputer yang didedikasikan untuk menggunakan teknologi komputasi untuk melakukan fungsi kognitif yang biasanya terkait dengan manusia, seperti belajar, memecahkan masalah, dan mengenali pola. Untuk informasi lebih lanjut, lihat Apa itu Kecerdasan Buatan?

operasi kecerdasan buatan (AIOps)

Proses menggunakan teknik pembelajaran mesin untuk memecahkan masalah operasional, mengurangi insiden operasional dan intervensi manusia, dan meningkatkan kualitas layanan. Untuk informasi selengkapnya tentang cara AIOps digunakan dalam strategi AWS migrasi, lihat panduan integrasi operasi.

enkripsi asimetris

Algoritma enkripsi yang menggunakan sepasang kunci, kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi. Anda dapat berbagi kunci publik karena tidak digunakan untuk dekripsi, tetapi akses ke kunci pribadi harus sangat dibatasi.

atomisitas, konsistensi, isolasi, daya tahan () ACID

Satu set properti perangkat lunak yang menjamin validitas data dan keandalan operasional database, bahkan dalam kasus kesalahan, kegagalan daya, atau masalah lainnya.

kontrol akses berbasis atribut () ABAC

Praktik membuat izin berbutir halus berdasarkan atribut pengguna, seperti departemen, peran pekerjaan, dan nama tim. Untuk informasi selengkapnya, lihat ABAC AWS di dokumentasi AWS Identity and Access Management (IAM).

sumber data otoritatif

Lokasi di mana Anda menyimpan versi utama data, yang dianggap sebagai sumber informasi yang paling dapat diandalkan. Anda dapat menyalin data dari sumber data otoritatif ke lokasi lain untuk tujuan pemrosesan atau modifikasi data, seperti menganonimkan, menyunting, atau membuat nama samaran.

Zona Ketersediaan

Lokasi berbeda di dalam Wilayah AWS yang terisolasi dari kegagalan di Availability Zone lainnya dan menyediakan konektivitas jaringan latensi rendah yang murah ke Availability Zone lainnya di Wilayah yang sama.

AWS Kerangka Adopsi Cloud (AWS CAF)

Kerangka pedoman dan praktik terbaik AWS untuk membantu organisasi mengembangkan rencana yang efisien dan efektif untuk bergerak dengan sukses ke cloud. AWS CAFMengatur panduan ke dalam enam bidang fokus yang disebut perspektif: bisnis, orang, tata kelola, platform, keamanan, dan operasi. Perspektif bisnis, orang, dan tata kelola fokus pada keterampilan dan proses bisnis; perspektif platform, keamanan, dan operasi fokus pada keterampilan dan proses teknis. Misalnya, perspektif masyarakat menargetkan pemangku kepentingan yang menangani sumber daya manusia (SDM), fungsi kepegawaian, dan manajemen orang. Untuk perspektif ini, AWS CAF berikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs AWS CAFweb dan AWS CAFwhitepaper.

AWS Kerangka Kualifikasi Beban Kerja ()AWS WQF

Alat yang mengevaluasi beban kerja migrasi database, merekomendasikan strategi migrasi, dan memberikan perkiraan kerja. AWS WQFdisertakan dengan AWS Schema Conversion Tool (AWS SCT). Ini menganalisis skema database dan objek kode, kode aplikasi, dependensi, dan karakteristik kinerja, dan memberikan laporan penilaian.

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau menyebabkan kerugian bagi individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

Pandangan interaktif yang terpadu tentang perilaku dan interaksi sumber daya dari waktu ke waktu. Anda dapat menggunakan grafik perilaku dengan Amazon Detective untuk memeriksa upaya logon yang gagal, API panggilan mencurigakan, dan tindakan serupa. Untuk informasi selengkapnya, lihat Data dalam grafik perilaku di dokumentasi Detektif.

sistem big-endian

Sistem yang menyimpan byte paling signifikan terlebih dahulu. Lihat juga endianness.

klasifikasi biner

Sebuah proses yang memprediksi hasil biner (salah satu dari dua kelas yang mungkin). Misalnya, model ML Anda mungkin perlu memprediksi masalah seperti “Apakah email ini spam atau bukan spam?” atau “Apakah produk ini buku atau mobil?”

filter mekar

Struktur data probabilistik dan efisien memori yang digunakan untuk menguji apakah suatu elemen adalah anggota dari suatu himpunan.

deployment biru/hijau

Strategi penyebaran tempat Anda membuat dua lingkungan yang terpisah namun identik. Anda menjalankan versi aplikasi saat ini di satu lingkungan (biru) dan versi aplikasi baru di lingkungan lain (hijau). Strategi ini membantu Anda dengan cepat memutar kembali dengan dampak minimal.

bot

Aplikasi perangkat lunak yang menjalankan tugas otomatis melalui internet dan mensimulasikan aktivitas atau interaksi manusia. Beberapa bot berguna atau bermanfaat, seperti perayap web yang mengindeks informasi di internet. Beberapa bot lain, yang dikenal sebagai bot buruk, dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

botnet

Jaringan bot yang terinfeksi oleh malware dan berada di bawah kendali satu pihak, yang dikenal sebagai bot herder atau operator bot. Botnet adalah mekanisme paling terkenal untuk skala bot dan dampaknya.

cabang

Area berisi repositori kode. Cabang pertama yang dibuat dalam repositori adalah cabang utama. Anda dapat membuat cabang baru dari cabang yang ada, dan Anda kemudian dapat mengembangkan fitur atau memperbaiki bug di cabang baru. Cabang yang Anda buat untuk membangun fitur biasanya disebut sebagai cabang fitur. Saat fitur siap dirilis, Anda menggabungkan cabang fitur kembali ke cabang utama. Untuk informasi selengkapnya, lihat Tentang cabang (GitHub dokumentasi).

akses break-glass

Dalam keadaan luar biasa dan melalui proses yang disetujui, cara cepat bagi pengguna untuk mendapatkan akses ke Akun AWS yang biasanya tidak memiliki izin untuk mengaksesnya. Untuk informasi lebih lanjut, lihat indikator Implementasikan prosedur break-glass dalam panduan Well-Architected AWS .

strategi brownfield

Infrastruktur yang ada di lingkungan Anda. Saat mengadopsi strategi brownfield untuk arsitektur sistem, Anda merancang arsitektur di sekitar kendala sistem dan infrastruktur saat ini. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

Apa yang dilakukan bisnis untuk menghasilkan nilai (misalnya, penjualan, layanan pelanggan, atau pemasaran). Arsitektur layanan mikro dan keputusan pengembangan dapat didorong oleh kemampuan bisnis. Untuk informasi selengkapnya, lihat bagian Terorganisir di sekitar kemampuan bisnis dari Menjalankan layanan mikro kontainer di whitepaper. AWS

perencanaan kelangsungan bisnis () BCP

Rencana yang membahas dampak potensial dari peristiwa yang mengganggu, seperti migrasi skala besar, pada operasi dan memungkinkan bisnis untuk melanjutkan operasi dengan cepat.

C

CAF

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

Rilis versi yang lambat dan bertahap untuk pengguna akhir. Ketika Anda yakin, Anda menyebarkan versi baru dan mengganti versi saat ini secara keseluruhan.

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

Proses melacak perubahan ke sumber data, seperti tabel database, dan merekam metadata tentang perubahan tersebut. Anda dapat menggunakan CDC untuk berbagai tujuan, seperti mengaudit atau mereplikasi perubahan dalam sistem target untuk mempertahankan sinkronisasi.

rekayasa kekacauan

Sengaja memperkenalkan kegagalan atau peristiwa yang mengganggu untuk menguji ketahanan sistem. Anda dapat menggunakan AWS Fault Injection Service (AWS FIS) untuk melakukan eksperimen yang menekankan AWS beban kerja Anda dan mengevaluasi responsnya.

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

Proses kategorisasi yang membantu menghasilkan prediksi. Model ML untuk masalah klasifikasi memprediksi nilai diskrit. Nilai diskrit selalu berbeda satu sama lain. Misalnya, model mungkin perlu mengevaluasi apakah ada mobil dalam gambar atau tidak.

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat CCoEposting di Blog Strategi AWS Cloud Perusahaan.

komputasi cloud

Teknologi cloud yang biasanya digunakan untuk penyimpanan data jarak jauh dan manajemen perangkat IoT. Cloud computing umumnya terhubung ke teknologi edge computing.

model operasi cloud

Dalam organisasi TI, model operasi yang digunakan untuk membangun, mematangkan, dan mengoptimalkan satu atau lebih lingkungan cloud. Untuk informasi selengkapnya, lihat Membangun Model Operasi Cloud Anda.

tahap adopsi cloud

Empat fase yang biasanya dilalui organisasi ketika mereka bermigrasi ke AWS Cloud:

- Proyek — Menjalankan beberapa proyek terkait cloud untuk bukti konsep dan tujuan pembelajaran
- Foundation — Melakukan investasi dasar untuk meningkatkan adopsi cloud Anda (misalnya, membuat landing zone, mendefinisikanCCoE, membuat model operasi)
- Migrasi — Migrasi aplikasi individual
- Re-invention — Mengoptimalkan produk dan layanan, dan berinovasi di cloud

Tahapan ini didefinisikan oleh Stephen Orban dalam posting blog The Journey Toward Cloud-First & the Stages of Adoption di blog Strategi Perusahaan. AWS Cloud Untuk informasi tentang bagaimana kaitannya dengan strategi AWS migrasi, lihat panduan kesiapan migrasi.

CMDB

Lihat database manajemen konfigurasi.

repositori kode

Lokasi di mana kode sumber dan aset lainnya, seperti dokumentasi, sampel, dan skrip, disimpan dan diperbarui melalui proses kontrol versi. Repositori cloud umum termasuk GitHub atau Bitbucket Cloud. Setiap versi kode disebut cabang. Dalam struktur layanan mikro, setiap repositori

dikhususkan untuk satu bagian fungsionalitas. Pipa CI/CD tunggal dapat menggunakan beberapa repositori.

cache dingin

Cache buffer yang kosong, tidak terisi dengan baik, atau berisi data basi atau tidak relevan. Ini mempengaruhi kinerja karena instance database harus membaca dari memori utama atau disk, yang lebih lambat daripada membaca dari cache buffer.

data dingin

Data yang jarang diakses dan biasanya historis. Saat menanyakan jenis data ini, kueri lambat biasanya dapat diterima. Memindahkan data ini ke tingkat penyimpanan atau kelas yang berkinerja lebih rendah dan lebih murah dapat mengurangi biaya.

visi komputer (CV)

Bidang AI yang menggunakan pembelajaran mesin untuk menganalisis dan mengekstrak informasi dari format visual seperti gambar dan video digital. Misalnya, AWS Panorama menawarkan perangkat yang menambahkan CV ke jaringan kamera lokal, dan Amazon SageMaker menyediakan algoritme pemrosesan gambar untuk CV.

konfigurasi drift

Untuk beban kerja, konfigurasi berubah dari status yang diharapkan. Ini dapat menyebabkan beban kerja menjadi tidak patuh, dan biasanya bertahap dan tidak disengaja.

database manajemen konfigurasi (CMDB)

Repositori yang menyimpan dan mengelola informasi tentang database dan lingkungan TI, termasuk komponen perangkat keras dan perangkat lunak dan konfigurasinya. Anda biasanya menggunakan data dari CMDB dalam penemuan portofolio dan tahap analisis migrasi.

paket kesesuaian

Kumpulan AWS Config aturan dan tindakan remediasi yang dapat Anda kumpulkan untuk menyesuaikan kepatuhan dan pemeriksaan keamanan Anda. Anda dapat menerapkan paket kesesuaian sebagai entitas tunggal di Akun AWS dan Wilayah, atau di seluruh organisasi, dengan menggunakan templat. YAML Untuk informasi selengkapnya, lihat Paket kesesuaian dalam dokumentasi. AWS Config

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

Proses mengotomatiskan sumber, membangun, menguji, pementasan, dan tahap produksi dari proses rilis perangkat lunak. CI/CD is commonly described as a pipeline. CI/CDdapat membantu

Anda mengotomatiskan proses, meningkatkan produktivitas, meningkatkan kualitas kode, dan memberikan lebih cepat. Untuk informasi lebih lanjut, lihat Manfaat pengiriman berkelanjutan. CD juga dapat berarti penerapan berkelanjutan. Untuk informasi selengkapnya, lihat Continuous Delivery vs Continuous Deployment.

CV

Lihat visi komputer.

D

data saat istirahat

Data yang stasioner di jaringan Anda, seperti data yang ada di penyimpanan.

klasifikasi data

Proses untuk mengidentifikasi dan mengkategorikan data dalam jaringan Anda berdasarkan kekritisan dan sensitivitasnya. Ini adalah komponen penting dari setiap strategi manajemen risiko keamanan siber karena membantu Anda menentukan perlindungan dan kontrol retensi yang tepat untuk data. Klasifikasi data adalah komponen pilar keamanan dalam AWS Well-Architected Framework. Untuk informasi selengkapnya, lihat Klasifikasi data.

penyimpangan data

Variasi yang berarti antara data produksi dan data yang digunakan untuk melatih model ML, atau perubahan yang berarti dalam data input dari waktu ke waktu. Penyimpangan data dapat mengurangi kualitas, akurasi, dan keadilan keseluruhan dalam prediksi model ML.

data dalam transit

Data yang aktif bergerak melalui jaringan Anda, seperti antara sumber daya jaringan.

jala data

Kerangka arsitektur yang menyediakan kepemilikan data terdistribusi dan terdesentralisasi dengan manajemen dan tata kelola terpusat.

minimalisasi data

Prinsip pengumpulan dan pemrosesan hanya data yang sangat diperlukan. Mempraktikkan minimalisasi data di dalamnya AWS Cloud dapat mengurangi risiko privasi, biaya, dan jejak karbon analitik Anda.

perimeter data

Satu set pagar pembatas pencegahan di AWS lingkungan Anda yang membantu memastikan bahwa hanya identitas tepercaya yang mengakses sumber daya tepercaya dari jaringan yang diharapkan. Untuk informasi selengkapnya, lihat Membangun perimeter data pada AWS.

prapemrosesan data

Untuk mengubah data mentah menjadi format yang mudah diuraikan oleh model ML Anda. Preprocessing data dapat berarti menghapus kolom atau baris tertentu dan menangani nilai yang hilang, tidak konsisten, atau duplikat.

asal data

Proses melacak asal dan riwayat data sepanjang siklus hidupnya, seperti bagaimana data dihasilkan, ditransmisikan, dan disimpan.

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

Sistem manajemen data yang mendukung intelijen bisnis, seperti analitik. Gudang data biasanya berisi sejumlah besar data historis, dan biasanya digunakan untuk kueri dan analisis.

bahasa definisi database (DDL)

Pernyataan atau perintah untuk membuat atau memodifikasi struktur tabel dan objek dalam database.

bahasa manipulasi database (DML)

Pernyataan atau perintah untuk memodifikasi (memasukkan, memperbarui, dan menghapus) informasi dalam database.

DDL

Lihat bahasa definisi database.

ansambel yang dalam

Untuk menggabungkan beberapa model pembelajaran mendalam untuk prediksi. Anda dapat menggunakan ansambel dalam untuk mendapatkan prediksi yang lebih akurat atau untuk memperkirakan ketidakpastian dalam prediksi.

pembelajaran mendalam

Subbidang ML yang menggunakan beberapa lapisan jaringan saraf tiruan untuk mengidentifikasi pemetaan antara data input dan variabel target yang diinginkan.

defense-in-depth

Pendekatan keamanan informasi di mana serangkaian mekanisme dan kontrol keamanan dilapisi dengan cermat di seluruh jaringan komputer untuk melindungi kerahasiaan, integritas, dan ketersediaan jaringan dan data di dalamnya. Saat Anda mengadopsi strategi ini AWS, Anda menambahkan beberapa kontrol pada lapisan AWS Organizations struktur yang berbeda untuk membantu mengamankan sumber daya. Misalnya, defense-in-depth pendekatan mungkin menggabungkan otentikasi multi-faktor, segmentasi jaringan, dan enkripsi.

administrator yang didelegasikan

Di AWS Organizations, layanan yang kompatibel dapat mendaftarkan akun AWS anggota untuk mengelola akun organisasi dan mengelola izin untuk layanan tersebut. Akun ini disebut administrator yang didelegasikan untuk layanan itu. Untuk informasi selengkapnya dan daftar layanan yang kompatibel, lihat Layanan yang berfungsi dengan AWS Organizations AWS Organizations dokumentasi.

deployment

Proses pembuatan aplikasi, fitur baru, atau perbaikan kode tersedia di lingkungan target. Deployment melibatkan penerapan perubahan dalam basis kode dan kemudian membangun dan menjalankan basis kode itu di lingkungan aplikasi.

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

Kontrol keamanan yang dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan kedua, memperingatkan Anda tentang peristiwa keamanan yang melewati kontrol pencegahan yang ada. Untuk informasi selengkapnya, lihat Kontrol Detektif dalam Menerapkan kontrol keamanan pada. AWS

pemetaan aliran nilai pengembangan () DVSM

Sebuah proses yang digunakan untuk mengidentifikasi dan memprioritaskan kendala yang mempengaruhi kecepatan dan kualitas dalam siklus hidup pengembangan perangkat lunak. DVSMmemperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik manufaktur

lean. Ini berfokus pada langkah-langkah dan tim yang diperlukan untuk menciptakan dan memindahkan nilai melalui proses pengembangan perangkat lunak.

kembar digital

Representasi virtual dari sistem dunia nyata, seperti bangunan, pabrik, peralatan industri, atau jalur produksi. Kembar digital mendukung pemeliharaan prediktif, pemantauan jarak jauh, dan optimalisasi produksi.

tabel dimensi

Dalam skema bintang, tabel yang lebih kecil yang berisi atribut data tentang data kuantitatif dalam tabel fakta. Atribut tabel dimensi biasanya bidang teks atau angka diskrit yang berperilaku seperti teks. Atribut ini biasanya digunakan untuk pembatasan kueri, pemfilteran, dan pelabelan set hasil.

musibah

Peristiwa yang mencegah beban kerja atau sistem memenuhi tujuan bisnisnya di lokasi utama yang digunakan. Peristiwa ini dapat berupa bencana alam, kegagalan teknis, atau akibat dari tindakan manusia, seperti kesalahan konfigurasi yang tidak disengaja atau serangan malware.

pemulihan bencana (DR)

Strategi dan proses yang Anda gunakan untuk meminimalkan downtime dan kehilangan data yang disebabkan oleh bencana. Untuk informasi selengkapnya, lihat Disaster Recovery of Workloads on AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Lihat bahasa manipulasi basis data.

desain berbasis domain

Pendekatan untuk mengembangkan sistem perangkat lunak yang kompleks dengan menghubungkan komponennya ke domain yang berkembang, atau tujuan bisnis inti, yang dilayani oleh setiap komponen. Konsep ini diperkenalkan oleh Eric Evans dalam bukunya, Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Untuk informasi tentang bagaimana Anda dapat menggunakan desain berbasis domain dengan pola ara pencekik, lihat Memodernisasi Microsoft lama. ASP NET(ASMX) layanan web secara bertahap dengan menggunakan kontainer dan Amazon API Gateway.

DR

Lihat pemulihan bencana.

deteksi drift

Melacak penyimpangan dari konfigurasi dasar. Misalnya, Anda dapat menggunakan AWS CloudFormation untuk mendeteksi penyimpangan dalam sumber daya sistem, atau Anda dapat menggunakannya AWS Control Tower untuk mendeteksi perubahan di landing zone yang mungkin memengaruhi kepatuhan terhadap persyaratan tata kelola.

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

Teknologi yang meningkatkan daya komputasi untuk perangkat pintar di tepi jaringan IoT. Jika dibandingkan dengan komputasi awan, komputasi tepi dapat mengurangi latensi komunikasi dan meningkatkan waktu respons.

pertukaran data elektronik () EDI

Pertukaran otomatis dokumen bisnis antar organisasi. Untuk informasi selengkapnya, lihat Apa itu Pertukaran Data Elektronik.

enkripsi

Proses komputasi yang mengubah data plaintext, yang dapat dibaca manusia, menjadi ciphertext.

kunci enkripsi

String kriptografi dari bit acak yang dihasilkan oleh algoritma enkripsi. Panjang kunci dapat bervariasi, dan setiap kunci dirancang agar tidak dapat diprediksi dan unik.

endianness

Urutan byte disimpan dalam memori komputer. Sistem big-endian menyimpan byte paling signifikan terlebih dahulu. Sistem little-endian menyimpan byte paling tidak signifikan terlebih dahulu.

titik akhir

Lihat titik akhir layanan.

layanan endpoint

Layanan yang dapat Anda host di cloud pribadi virtual (VPC) untuk dibagikan dengan pengguna lain. Anda dapat membuat layanan endpoint dengan AWS PrivateLink dan memberikan izin kepada prinsipal lain Akun AWS atau to AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir antarmuka. VPC Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (AmazonVPC).

perencanaan sumber daya perusahaan (ERP)

Sistem yang mengotomatiskan dan mengelola proses bisnis utama (seperti akuntansi, MES, dan manajemen proyek) untuk suatu perusahaan.

enkripsi amplop

Proses mengenkripsi kunci enkripsi dengan kunci enkripsi lain. Untuk informasi selengkapnya, lihat Enkripsi amplop dalam dokumentasi AWS Key Management Service (AWS KMS).

lingkungan

Sebuah contoh dari aplikasi yang sedang berjalan. Berikut ini adalah jenis lingkungan yang umum dalam komputasi awan:

- Development Environment — Sebuah contoh dari aplikasi yang berjalan yang hanya tersedia untuk tim inti yang bertanggung jawab untuk memelihara aplikasi. Lingkungan pengembangan digunakan untuk menguji perubahan sebelum mempromosikannya ke lingkungan atas. Jenis lingkungan ini kadang-kadang disebut sebagai lingkungan pengujian.
- lingkungan yang lebih rendah — Semua lingkungan pengembangan untuk aplikasi, seperti yang digunakan untuk build awal dan pengujian.
- lingkungan produksi — Sebuah contoh dari aplikasi yang berjalan yang pengguna akhir dapat mengakses. Dalam pipa CI/CD, lingkungan produksi adalah lingkungan penyebaran terakhir.

- lingkungan atas — Semua lingkungan yang dapat diakses oleh pengguna selain tim pengembangan inti. Ini dapat mencakup lingkungan produksi, lingkungan praproduksi, dan lingkungan untuk pengujian penerimaan pengguna.

epik

Dalam metodologi tangkas, kategori fungsional yang membantu mengatur dan memprioritaskan pekerjaan Anda. Epik memberikan deskripsi tingkat tinggi tentang persyaratan dan tugas implementasi. Misalnya, epos AWS CAF keamanan termasuk manajemen identitas dan akses, kontrol detektif, keamanan infrastruktur, perlindungan data, dan respons insiden. Untuk informasi selengkapnya tentang epos dalam strategi AWS migrasi, lihat panduan implementasi program.

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi () EDA

Proses menganalisis dataset untuk memahami karakteristik utamanya. Anda mengumpulkan atau mengumpulkan data dan kemudian melakukan penyelidikan awal untuk menemukan pola, mendeteksi anomali, dan memeriksa asumsi. EDAdilakukan dengan menghitung statistik ringkasan dan membuat visualisasi data.

F

tabel fakta

Tabel tengah dalam skema bintang. Ini menyimpan data kuantitatif tentang operasi bisnis. Biasanya, tabel fakta berisi dua jenis kolom: kolom yang berisi ukuran dan yang berisi kunci asing ke tabel dimensi.

gagal cepat

Filosofi yang menggunakan pengujian yang sering dan bertahap untuk mengurangi siklus hidup pengembangan. Ini adalah bagian penting dari pendekatan tangkas.

batas isolasi kesalahan

Dalam AWS Cloud, batas seperti Availability Zone, Wilayah AWS, control plane, atau data plane yang membatasi efek kegagalan dan membantu meningkatkan ketahanan beban kerja. Untuk informasi selengkapnya, lihat Batas Isolasi AWS Kesalahan.

cabang fitur

Lihat cabang.

fitur

Data input yang Anda gunakan untuk membuat prediksi. Misalnya, dalam konteks manufaktur, fitur bisa berupa gambar yang diambil secara berkala dari lini manufaktur.

pentingnya fitur

Seberapa signifikan fitur untuk prediksi model. Ini biasanya dinyatakan sebagai skor numerik yang dapat dihitung melalui berbagai teknik, seperti Shapley Additive Explanations (SHAP) dan gradien terintegrasi. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan:.AWS

transformasi fitur

Untuk mengoptimalkan data untuk proses ML, termasuk memperkaya data dengan sumber tambahan, menskalakan nilai, atau mengekstrak beberapa set informasi dari satu bidang data. Hal ini memungkinkan model ML untuk mendapatkan keuntungan dari data. Misalnya, jika Anda memecah tanggal “2021-05-27 00:15:37" menjadi “2021", “Mei”, “Kamis”, dan “15", Anda dapat membantu algoritme pembelajaran mempelajari pola bernuansa yang terkait dengan komponen data yang berbeda.

beberapa tembakan mendorong

Memberikan sejumlah kecil contoh yang menunjukkan tugas dan output yang diinginkan sebelum memintanya untuk melakukan tugas serupa. LLM Teknik ini adalah aplikasi pembelajaran dalam konteks, di mana model belajar dari contoh (bidikan) yang tertanam dalam petunjuk. Beberapa bidikan dapat efektif untuk tugas-tugas yang memerlukan pemformatan, penalaran, atau pengetahuan domain tertentu. Lihat juga bidikan nol.

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus () FGAC

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

Metode migrasi database yang menggunakan replikasi data berkelanjutan melalui pengambilan data perubahan untuk memigrasikan data dalam waktu sesingkat mungkin, alih-alih

menggunakan pendekatan bertahap. Tujuannya adalah untuk menjaga downtime seminimal mungkin.

FM

Lihat model pondasi.

model pondasi (FM)

Jaringan saraf pembelajaran mendalam yang besar yang telah melatih kumpulan data besar-besaran data umum dan tidak berlabel. FMsmampu melakukan berbagai tugas umum, seperti memahami bahasa, menghasilkan teks dan gambar, dan berbicara dalam bahasa alami. Untuk informasi selengkapnya, lihat Apa itu Model Foundation.

G

AI generatif

Subset model AI yang telah dilatih pada sejumlah besar data dan yang dapat menggunakan prompt teks sederhana untuk membuat konten dan artefak baru, seperti gambar, video, teks, dan audio. Untuk informasi lebih lanjut, lihat Apa itu AI Generatif.

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

Di Amazon CloudFront, opsi untuk mencegah pengguna di negara tertentu mengakses distribusi konten. Anda dapat menggunakan daftar izinkan atau daftar blokir untuk menentukan negara yang disetujui dan dilarang. Untuk informasi selengkapnya, lihat Membatasi distribusi geografis konten Anda dalam dokumentasi. CloudFront

Alur kerja Gitflow

Pendekatan di mana lingkungan bawah dan atas menggunakan cabang yang berbeda dalam repositori kode sumber. Alur kerja Gitflow dianggap warisan, dan alur kerja berbasis batang adalah pendekatan modern yang lebih disukai.

gambar emas

Sebuah snapshot dari sistem atau perangkat lunak yang digunakan sebagai template untuk menyebarkan instance baru dari sistem atau perangkat lunak itu. Misalnya, di bidang manufaktur,

gambar emas dapat digunakan untuk menyediakan perangkat lunak pada beberapa perangkat dan membantu meningkatkan kecepatan, skalabilitas, dan produktivitas dalam operasi manufaktur perangkat.

strategi greenfield

Tidak adanya infrastruktur yang ada di lingkungan baru. Saat mengadopsi strategi greenfield untuk arsitektur sistem, Anda dapat memilih semua teknologi baru tanpa batasan kompatibilitas dengan infrastruktur yang ada, juga dikenal sebagai brownfield. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

pagar pembatas

Aturan tingkat tinggi yang membantu mengatur sumber daya, kebijakan, dan kepatuhan di seluruh unit organisasi ()OUs. Pagar pembatas preventif menegakkan kebijakan untuk memastikan keselarasan dengan standar kepatuhan. Mereka diimplementasikan dengan menggunakan kebijakan kontrol layanan dan batas IAM izin. Detective guardrails mendeteksi pelanggaran kebijakan dan masalah kepatuhan, dan menghasilkan peringatan untuk remediasi. Mereka diimplementasikan dengan menggunakan AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector, dan pemeriksaan khusus AWS Lambda .

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

Memigrasi database sumber Anda ke database target yang menggunakan mesin database yang berbeda (misalnya, Oracle ke Amazon Aurora). Migrasi heterogen biasanya merupakan bagian dari upaya arsitektur ulang, dan mengubah skema dapat menjadi tugas yang kompleks. AWS menyediakan AWS SCT yang membantu dengan konversi skema.

ketersediaan tinggi (HA)

Kemampuan beban kerja untuk beroperasi terus menerus, tanpa intervensi, jika terjadi tantangan atau bencana. Sistem HA dirancang untuk gagal secara otomatis, secara konsisten memberikan kinerja berkualitas tinggi, dan menangani beban dan kegagalan yang berbeda dengan dampak kinerja minimal.

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

data penahanan

Sebagian dari data historis berlabel yang ditahan dari kumpulan data yang digunakan untuk melatih model pembelajaran mesin. Anda dapat menggunakan data penahanan untuk mengevaluasi kinerja model dengan membandingkan prediksi model dengan data penahanan.

migrasi database homogen

Memigrasi database sumber Anda ke database target yang berbagi mesin database yang sama (misalnya, Microsoft SQL Server ke Amazon RDS untuk SQL Server). Migrasi homogen biasanya merupakan bagian dari upaya rehosting atau replatforming. Anda dapat menggunakan utilitas database asli untuk memigrasi skema.

data panas

Data yang sering diakses, seperti data real-time atau data translasi terbaru. Data ini biasanya memerlukan tingkat atau kelas penyimpanan berkinerja tinggi untuk memberikan respons kueri yang cepat.

perbaikan terbaru

Perbaikan mendesak untuk masalah kritis dalam lingkungan produksi. Karena urgensinya, perbaikan terbaru biasanya dibuat di luar alur kerja DevOps rilis biasa.

periode hypercare

Segera setelah cutover, periode waktu ketika tim migrasi mengelola dan memantau aplikasi yang dimigrasi di cloud untuk mengatasi masalah apa pun. Biasanya, periode ini panjangnya 1-4 hari. Pada akhir periode hypercare, tim migrasi biasanya mentransfer tanggung jawab untuk aplikasi ke tim operasi cloud.

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

Kebijakan yang dilampirkan pada satu atau beberapa IAM prinsip yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki rata-rata CPU dan penggunaan memori antara 5 dan 20 persen selama periode 90 hari. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini atau mempertahankannya di tempat.

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

Model yang menyebarkan infrastruktur baru untuk beban kerja produksi alih-alih memperbarui, menambal, atau memodifikasi infrastruktur yang ada. Infrastruktur yang tidak dapat diubah secara inheren lebih konsisten, andal, dan dapat diprediksi daripada infrastruktur yang dapat berubah. Untuk informasi selengkapnya, lihat praktik terbaik Deploy using immutable infrastructure di AWS Well-Architected Framework.

masuk (masuknya) VPC

Dalam arsitektur AWS multi-akun, a VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

migrasi inkremental

Strategi cutover di mana Anda memigrasikan aplikasi Anda dalam bagian-bagian kecil alih-alih melakukan satu cutover penuh. Misalnya, Anda mungkin hanya memindahkan beberapa layanan mikro atau pengguna ke sistem baru pada awalnya. Setelah Anda memverifikasi bahwa semuanya berfungsi dengan baik, Anda dapat secara bertahap memindahkan layanan mikro atau pengguna tambahan hingga Anda dapat menonaktifkan sistem lama Anda. Strategi ini mengurangi risiko yang terkait dengan migrasi besar.

Industri 4.0

Sebuah istilah yang diperkenalkan oleh Klaus Schwab pada tahun 2016 untuk merujuk pada modernisasi proses manufaktur melalui kemajuan dalam konektivitas, data real-time, otomatisasi, analitik, dan AI/ML.

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

Proses penyediaan dan pengelolaan infrastruktur aplikasi melalui satu set file konfigurasi. IAc dirancang untuk membantu Anda memusatkan manajemen infrastruktur, menstandarisasi sumber daya, dan menskalakan dengan cepat sehingga lingkungan baru dapat diulang, andal, dan konsisten.

Internet of Things industri (IIoT)

Penggunaan sensor dan perangkat yang terhubung ke internet di sektor industri, seperti manufaktur, energi, otomotif, perawatan kesehatan, ilmu kehidupan, dan pertanian. Untuk informasi selengkapnya, lihat Membangun strategi transformasi digital Internet of Things (IIoT) industri.

inspeksi VPC

Dalam arsitektur AWS multi-akun, terpusat VPC yang mengelola inspeksi lalu lintas jaringan antara VPCs (dalam hal yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

Internet of Things (IoT)

Jaringan objek fisik yang terhubung dengan sensor atau prosesor tertanam yang berkomunikasi dengan perangkat dan sistem lain melalui internet atau melalui jaringan komunikasi lokal. Untuk informasi selengkapnya, lihat Apa itu IoT?

interpretabilitas

Karakteristik model pembelajaran mesin yang menggambarkan sejauh mana manusia dapat memahami bagaimana prediksi model bergantung pada inputnya. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

Serangkaian praktik terbaik untuk memberikan layanan TI dan menyelaraskan layanan ini dengan persyaratan bisnis. ITILmenyediakan fondasi untukITSM.

Manajemen layanan TI (ITSM)

Kegiatan yang terkait dengan merancang, menerapkan, mengelola, dan mendukung layanan TI untuk suatu organisasi. Untuk informasi tentang mengintegrasikan operasi cloud dengan ITSM alat, lihat panduan integrasi operasi.

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label () LBAC

Implementasi kontrol akses wajib (MAC) di mana pengguna dan data itu sendiri masing-masing secara eksplisit diberi nilai label keamanan. Persimpangan antara label keamanan pengguna dan label keamanan data menentukan baris dan kolom mana yang dapat dilihat oleh pengguna.

landing zone

Landing zone adalah AWS lingkungan multi-akun yang dirancang dengan baik yang dapat diskalakan dan aman. Ini adalah titik awal dari mana organisasi Anda dapat dengan cepat meluncurkan dan menyebarkan beban kerja dan aplikasi dengan percaya diri dalam lingkungan keamanan dan infrastruktur mereka. Untuk informasi selengkapnya tentang zona pendaratan, lihat Menyiapkan lingkungan multi-akun AWS yang aman dan dapat diskalakan.

model bahasa besar (LLM)

Model AI pembelajaran mendalam yang dilatih sebelumnya pada sejumlah besar data. An LLM dapat melakukan banyak tugas, seperti menjawab pertanyaan, meringkas dokumen, menerjemahkan teks ke dalam bahasa lain, dan menyelesaikan kalimat. Untuk informasi lebih lanjut, lihat Apa itu LLMs.

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

Praktik keamanan terbaik untuk memberikan izin minimum yang diperlukan untuk melakukan tugas. Untuk informasi selengkapnya, lihat Menerapkan izin hak istimewa terkecil dalam dokumentasi. IAM

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

Sebuah sistem yang menyimpan byte paling tidak signifikan terlebih dahulu. Lihat juga endianness.

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan pola dan pembelajaran. ML menganalisis dan belajar dari data yang direkam, seperti data Internet of Things (IoT), untuk menghasilkan model statistik berdasarkan pola. Untuk informasi selengkapnya, lihat Machine Learning.

cabang utama

Lihat cabang.

malware

Perangkat lunak yang dirancang untuk membahayakan keamanan atau privasi komputer. Malware dapat mengganggu sistem komputer, membocorkan informasi sensitif, atau mendapatkan akses yang tidak sah. Contoh malware termasuk virus, worm, ransomware, Trojan horse, spyware, dan keyloggers.

layanan terkelola

Layanan AWS yang AWS mengoperasikan lapisan infrastruktur, sistem operasi, dan platform, dan Anda mengakses titik akhir untuk menyimpan dan mengambil data. Amazon Simple Storage Service (Amazon S3) dan Amazon DynamoDB adalah contoh layanan terkelola. Ini juga dikenal sebagai layanan abstrak.

sistem eksekusi manufaktur (MES)

Sistem perangkat lunak untuk melacak, memantau, mendokumentasikan, dan mengendalikan proses produksi yang mengubah bahan baku menjadi produk jadi di lantai toko.

MAP

Lihat Program Percepatan Migrasi.

mekanisme

Proses lengkap di mana Anda membuat alat, mendorong adopsi alat, dan kemudian memeriksa hasilnya untuk melakukan penyesuaian. Mekanisme adalah siklus yang memperkuat dan meningkatkan dirinya sendiri saat beroperasi. Untuk informasi lebih lanjut, lihat Membangun mekanisme di AWS Well-Architected Framework.

akun anggota

Semua Akun AWS selain akun manajemen yang merupakan bagian dari organisasi di AWS Organizations. Akun dapat menjadi anggota dari hanya satu organisasi pada suatu waktu.

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan () MQTT

Protokol komunikasi ringan machine-to-machine (M2M), berdasarkan pola terbitkan/berlangganan, untuk perangkat IoT yang dibatasi sumber daya.

layanan mikro

Layanan kecil dan independen yang berkomunikasi melalui definisi yang jelas APIs dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali, dan ketahanan. Untuk informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

Pendekatan untuk membangun aplikasi dengan komponen independen yang menjalankan setiap proses aplikasi sebagai layanan mikro. Layanan mikro ini berkomunikasi melalui antarmuka yang terdefinisi dengan baik dengan menggunakan ringan. APIs Setiap layanan mikro dalam arsitektur ini dapat diperbarui, digunakan, dan diskalakan untuk memenuhi permintaan fungsi tertentu dari suatu aplikasi. Untuk informasi selengkapnya, lihat Menerapkan layanan mikro di AWS.

Program Percepatan Migrasi (MAP)

AWS Program yang menyediakan dukungan konsultasi, pelatihan, dan layanan untuk membantu organisasi membangun fondasi operasional yang kuat untuk pindah ke cloud, dan untuk membantu mengimbangi biaya awal migrasi. MAPmencakup metodologi migrasi untuk mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatiskan dan mempercepat skenario migrasi umum.

migrasi dalam skala

Proses memindahkan sebagian besar portofolio aplikasi ke cloud dalam gelombang, dengan lebih banyak aplikasi bergerak pada tingkat yang lebih cepat di setiap gelombang. Fase ini menggunakan praktik terbaik dan pelajaran yang dipetik dari fase sebelumnya untuk mengimplementasikan pabrik migrasi tim, alat, dan proses untuk merampingkan migrasi beban kerja melalui otomatisasi dan pengiriman tangkas. Ini adalah fase ketiga dari strategi AWS migrasi.

pabrik migrasi

Tim lintas fungsi yang merampingkan migrasi beban kerja melalui pendekatan otomatis dan gesit. Tim pabrik migrasi biasanya mencakup operasi, analis dan pemilik bisnis, insinyur migrasi, pengembang, dan DevOps profesional yang bekerja di sprint. Antara 20 dan 50 persen portofolio aplikasi perusahaan terdiri dari pola berulang yang dapat dioptimalkan dengan pendekatan pabrik.

Untuk informasi selengkapnya, lihat diskusi tentang pabrik migrasi dan panduan Pabrik Migrasi Cloud di kumpulan konten ini.

metadata migrasi

Informasi tentang aplikasi dan server yang diperlukan untuk menyelesaikan migrasi. Setiap pola migrasi memerlukan satu set metadata migrasi yang berbeda. Contoh metadata migrasi termasuk subnet target, grup keamanan, dan akun. AWS

pola migrasi

Tugas migrasi berulang yang merinci strategi migrasi, tujuan migrasi, dan aplikasi atau layanan migrasi yang digunakan. Contoh: Rehost migrasi ke Amazon EC2 dengan Layanan Migrasi AWS Aplikasi.

Penilaian Portofolio Migrasi (MPA)

Alat online yang menyediakan informasi untuk memvalidasi kasus bisnis untuk bermigrasi ke. AWS Cloud MPAmemberikan penilaian portofolio terperinci (ukuran kanan server, harga, TCO perbandingan, analisis biaya migrasi) serta perencanaan migrasi (analisis data aplikasi dan pengumpulan data, pengelompokan aplikasi, prioritas migrasi, dan perencanaan gelombang). MPAAlat ini (memerlukan login) tersedia gratis untuk semua AWS konsultan dan konsultan APN Mitra.

Penilaian Kesiapan Migrasi () MRA

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana aksi untuk menutup kesenjangan yang teridentifikasi, menggunakan. AWS CAF Untuk informasi selengkapnya, lihat panduan kesiapan migrasi. MRAIni adalah tahap pertama dari strategi AWS migrasi.

strategi migrasi

Pendekatan yang digunakan untuk memigrasikan beban kerja ke file. AWS Cloud Untuk informasi lebih lanjut, lihat entri 7 Rs di glosarium ini dan lihat Memobilisasi organisasi Anda untuk mempercepat migrasi skala besar.

ML

Lihat pembelajaran mesin.

modernisasi

Mengubah aplikasi usang (warisan atau monolitik) dan infrastrukturnya menjadi sistem yang gesit, elastis, dan sangat tersedia di cloud untuk mengurangi biaya, mendapatkan efisiensi, dan

memanfaatkan inovasi. Untuk informasi selengkapnya, lihat Strategi untuk memodernisasi aplikasi di. AWS Cloud

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi lebih lanjut, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di. AWS Cloud

aplikasi monolitik (monolit)

Aplikasi yang berjalan sebagai layanan tunggal dengan proses yang digabungkan secara ketat. Aplikasi monolitik memiliki beberapa kelemahan. Jika satu fitur aplikasi mengalami lonjakan permintaan, seluruh arsitektur harus diskalakan. Menambahkan atau meningkatkan fitur aplikasi monolitik juga menjadi lebih kompleks ketika basis kode tumbuh. Untuk mengatasi masalah ini, Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat Mengurai monolit menjadi layanan mikro.

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

Sebuah proses yang membantu menghasilkan prediksi untuk beberapa kelas (memprediksi satu dari lebih dari dua hasil). Misalnya, model ML mungkin bertanya “Apakah produk ini buku, mobil, atau telepon?” atau “Kategori produk mana yang paling menarik bagi pelanggan ini?”

infrastruktur yang bisa berubah

Model yang memperbarui dan memodifikasi infrastruktur yang ada untuk beban kerja produksi. Untuk meningkatkan konsistensi, keandalan, dan prediktabilitas, AWS Well-Architected Framework merekomendasikan penggunaan infrastruktur yang tidak dapat diubah sebagai praktik terbaik.

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

Metode migrasi di mana beban kerja sumber diturunkan selama proses migrasi. Metode ini melibatkan waktu henti yang diperpanjang dan biasanya digunakan untuk beban kerja kecil dan tidak kritis.

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

Metode migrasi di mana beban kerja sumber disalin ke sistem target tanpa diambil offline. Aplikasi yang terhubung ke beban kerja dapat terus berfungsi selama migrasi. Metode ini melibatkan waktu henti nol hingga minimal dan biasanya digunakan untuk beban kerja produksi yang kritis.

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

Protokol komunikasi machine-to-machine (M2M) untuk otomasi industri. OPC-UA menyediakan standar interoperabilitas dengan enkripsi data, otentikasi, dan skema otorisasi.

perjanjian tingkat operasional () OLA

Perjanjian yang menjelaskan apa yang dijanjikan oleh kelompok TI fungsional untuk diberikan satu sama lain, untuk mendukung perjanjian tingkat layanan (). SLA

tinjauan kesiapan operasional () ORR

Daftar pertanyaan dan praktik terbaik terkait yang membantu Anda memahami, mengevaluasi, mencegah, atau mengurangi ruang lingkup insiden dan kemungkinan kegagalan. Untuk informasi lebih lanjut, lihat Ulasan Kesiapan Operasional (ORR) dalam Kerangka Kerja AWS Well-Architected.

teknologi operasional (OT)

Sistem perangkat keras dan perangkat lunak yang bekerja dengan lingkungan fisik untuk mengendalikan operasi industri, peralatan, dan infrastruktur. Di bidang manufaktur, integrasi sistem OT dan teknologi informasi (TI) adalah fokus utama untuk transformasi Industri 4.0.

integrasi operasi (OI)

Proses modernisasi operasi di cloud, yang melibatkan perencanaan kesiapan, otomatisasi, dan integrasi. Untuk informasi selengkapnya, lihat panduan integrasi operasi.

jejak organisasi

Jejak yang dibuat oleh AWS CloudTrail itu mencatat semua peristiwa untuk semua Akun AWS dalam organisasi di AWS Organizations. Jejak ini dibuat di setiap Akun AWS bagian organisasi dan melacak aktivitas di setiap akun. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dalam CloudTrail dokumentasi.

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. OCMmembantu organisasi mempersiapkan, dan transisi ke, sistem dan strategi baru dengan mempercepat adopsi perubahan, mengatasi masalah transisi, dan mendorong perubahan budaya dan organisasi. Dalam strategi AWS migrasi, kerangka kerja ini disebut percepatan orang, karena kecepatan perubahan yang diperlukan dalam proyek adopsi cloud. Untuk informasi lebih lanjut, lihat OCMpanduannya.

kontrol akses asal (OAC)

Di CloudFront, opsi yang disempurnakan untuk membatasi akses untuk mengamankan konten Amazon Simple Storage Service (Amazon S3) Anda. OACmendukung semua bucket S3 di semua Wilayah AWS, enkripsi sisi server dengan AWS KMS (SSE-KMS), dan dinamis `PUT` dan `DELETE` permintaan ke bucket S3.

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakanOAI, CloudFront buat prinsipal yang dapat diautentikasi oleh Amazon S3. Prinsipal yang diautentikasi dapat mengakses konten dalam bucket S3 hanya melalui distribusi tertentu. CloudFront Lihat juga OAC, yang menyediakan kontrol akses yang lebih terperinci dan ditingkatkan.

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

Dalam arsitektur AWS multi-akun, a VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

Kebijakan IAM manajemen yang dilampirkan pada IAM prinsipal untuk menetapkan izin maksimum yang dapat dimiliki pengguna atau peran. Untuk informasi selengkapnya, lihat Batas izin dalam IAM dokumentasi.

Informasi Identifikasi Pribadi () PII

Informasi yang, jika dilihat secara langsung atau dipasangkan dengan data terkait lainnya, dapat digunakan untuk menyimpulkan identitas individu secara wajar. Contohnya PII termasuk nama, alamat, dan informasi kontak.

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

Serangkaian langkah yang telah ditentukan sebelumnya yang menangkap pekerjaan yang terkait dengan migrasi, seperti mengirimkan fungsi operasi inti di cloud. Buku pedoman dapat berupa skrip, runbook otomatis, atau ringkasan proses atau langkah-langkah yang diperlukan untuk mengoperasikan lingkungan modern Anda.

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

Objek yang dapat menentukan izin (lihat kebijakan berbasis identitas), menentukan kondisi akses (lihat kebijakanberbasis sumber daya), atau menentukan izin maksimum untuk semua akun dalam organisasi di (lihat kebijakan kontrol layanan). AWS Organizations

ketekunan poliglot

Secara independen memilih teknologi penyimpanan data microservice berdasarkan pola akses data dan persyaratan lainnya. Jika layanan mikro Anda memiliki teknologi penyimpanan data yang sama, mereka dapat menghadapi tantangan implementasi atau mengalami kinerja yang buruk. Layanan mikro lebih mudah diimplementasikan dan mencapai kinerja dan skalabilitas yang lebih baik jika mereka menggunakan penyimpanan data yang paling sesuai dengan kebutuhan mereka. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi data di layanan mikro.

penilaian portofolio

Proses menemukan, menganalisis, dan memprioritaskan portofolio aplikasi untuk merencanakan migrasi. Untuk informasi selengkapnya, lihat Mengevaluasi kesiapan migrasi.

predikat

Kondisi kueri yang mengembalikan `true` atau`false`, biasanya terletak di `WHERE` klausa.

predikat pushdown

Teknik pengoptimalan kueri database yang menyaring data dalam kueri sebelum transfer. Ini mengurangi jumlah data yang harus diambil dan diproses dari database relasional, dan meningkatkan kinerja kueri.

kontrol preventif

Kontrol keamanan yang dirancang untuk mencegah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan pertama untuk membantu mencegah akses tidak sah atau perubahan yang tidak diinginkan ke jaringan Anda. Untuk informasi selengkapnya, lihat Kontrol pencegahan dalam Menerapkan kontrol keamanan pada. AWS

principal

Entitas AWS yang dapat melakukan tindakan dan mengakses sumber daya. Entitas ini biasanya merupakan pengguna root untuk Akun AWS, IAM peran, atau pengguna. Untuk informasi selengkapnya, lihat Prinsip dalam istilah dan konsep Peran dalam IAM dokumentasi.

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona yang dihosting pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons DNS kueri untuk domain dan subdomainnya dalam satu atau lebih. VPCs Untuk informasi selengkapnya, lihat Bekerja dengan zona yang dihosting pribadi di dokumentasi Route 53.

kontrol proaktif

Kontrol keamanan yang dirancang untuk mencegah penyebaran sumber daya yang tidak sesuai. Kontrol ini memindai sumber daya sebelum disediakan. Jika sumber daya tidak sesuai dengan kontrol, maka itu tidak disediakan. Untuk informasi selengkapnya, lihat panduan referensi Kontrol dalam AWS Control Tower dokumentasi dan lihat Kontrol proaktif dalam Menerapkan kontrol keamanan pada AWS.

manajemen siklus hidup produk () PLM

Manajemen data dan proses untuk suatu produk di seluruh siklus hidupnya, mulai dari desain, pengembangan, dan peluncuran, melalui pertumbuhan dan kematangan, hingga penurunan dan penghapusan.

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram () PLC

Di bidang manufaktur, komputer yang sangat andal dan mudah beradaptasi yang memantau mesin dan mengotomatiskan proses manufaktur.

rantai cepat

Menggunakan output dari satu LLMprompt sebagai input untuk prompt berikutnya untuk menghasilkan respons yang lebih baik. Teknik ini digunakan untuk memecah tugas yang kompleks menjadi subtugas, atau untuk secara iteratif memperbaiki atau memperluas respons awal. Ini membantu meningkatkan akurasi dan relevansi respons model dan memungkinkan hasil yang lebih terperinci dan dipersonalisasi.

pseudonimisasi

Proses penggantian pengenal pribadi dalam kumpulan data dengan nilai placeholder. Pseudonimisasi dapat membantu melindungi privasi pribadi. Data pseudonim masih dianggap sebagai data pribadi.

publish/subscribe (pub/sub)

Pola yang memungkinkan komunikasi asinkron antara layanan mikro untuk meningkatkan skalabilitas dan daya tanggap. Misalnya, dalam layanan mikro berbasis MES, layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan oleh layanan mikro lainnya. Sistem dapat menambahkan layanan mikro baru tanpa mengubah layanan penerbitan.

Q

rencana kueri

Serangkaian langkah, seperti instruksi, yang digunakan untuk mengakses data dalam sistem database SQL relasional.

regresi rencana kueri

Ketika pengoptimal layanan database memilih rencana yang kurang optimal daripada sebelum perubahan yang diberikan ke lingkungan database. Hal ini dapat disebabkan oleh perubahan statistik, kendala, pengaturan lingkungan, pengikatan parameter kueri, dan pembaruan ke mesin database.

R

RACImatriks

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan () RACI.

RAG

Lihat Retrieval Augmented Generation.

ransomware

Perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data sampai pembayaran dilakukan.

RASCImatriks

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan () RACI.

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

Salinan database yang digunakan untuk tujuan read-only. Anda dapat merutekan kueri ke replika baca untuk mengurangi beban pada database utama Anda.

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

Jumlah waktu maksimum yang dapat diterima sejak titik pemulihan data terakhir. Ini menentukan apa yang dianggap sebagai kehilangan data yang dapat diterima antara titik pemulihan terakhir dan gangguan layanan.

tujuan waktu pemulihan (RTO)

Penundaan maksimum yang dapat diterima antara gangguan layanan dan pemulihan layanan.

refactor

Lihat 7 Rs.

Wilayah

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing Wilayah AWS terisolasi dan independen dari yang lain untuk memberikan toleransi kesalahan, stabilitas, dan ketahanan. Untuk informasi selengkapnya, lihat Menentukan Wilayah AWS akun yang dapat digunakan.

regresi

Teknik ML yang memprediksi nilai numerik. Misalnya, untuk memecahkan masalah "Berapa harga rumah ini akan dijual?" Model ML dapat menggunakan model regresi linier untuk memprediksi harga jual rumah berdasarkan fakta yang diketahui tentang rumah (misalnya, luas persegi).

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

Kemampuan aplikasi untuk melawan atau pulih dari gangguan. Ketersediaan tinggi dan pemulihan bencana adalah pertimbangan umum ketika merencanakan ketahanan di. AWS Cloud Untuk informasi lebih lanjut, lihat AWS Cloud Ketahanan.

kebijakan berbasis sumber daya

Kebijakan yang dilampirkan ke sumber daya, seperti bucket Amazon S3, titik akhir, atau kunci enkripsi. Jenis kebijakan ini menentukan prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

matriks yang bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan () RACI

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang

didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Jenis dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut RASCImatriks, dan jika Anda mengecualikannya, itu disebut RACImatriks.

kontrol responsif

Kontrol keamanan yang dirancang untuk mendorong remediasi efek samping atau penyimpangan dari garis dasar keamanan Anda. Untuk informasi selengkapnya, lihat Kontrol responsif dalam Menerapkan kontrol keamanan pada AWS.

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Pengambilan Generasi Augmented () RAG

Teknologi AI generatif di mana LLMreferensi sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, RAG model mungkin melakukan pencarian semantik dari basis pengetahuan organisasi atau data kustom. Untuk informasi lebih lanjut, lihat Apa itu RAG.

rotasi

Proses memperbarui rahasia secara berkala untuk membuatnya lebih sulit bagi penyerang untuk mengakses kredensil.

kontrol akses baris dan kolom (RCAC)

Penggunaan SQL ekspresi dasar dan fleksibel yang telah menetapkan aturan akses. RCACterdiri dari izin baris dan topeng kolom.

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

Satu set prosedur manual atau otomatis yang diperlukan untuk melakukan tugas tertentu. Ini biasanya dibangun untuk merampingkan operasi berulang atau prosedur dengan tingkat kesalahan yang tinggi.

D

SAML 2.0

Standar terbuka yang digunakan oleh banyak penyedia identitas (IdPs). Fitur ini memungkinkan sistem masuk tunggal (SSO) gabungan, sehingga pengguna dapat masuk ke AWS Management Console atau memanggil AWS API operasi tanpa Anda harus membuat pengguna untuk semua orang di IAM organisasi Anda. Untuk informasi lebih lanjut tentang federasi SAML berbasis 2.0, lihat Tentang federasi SAML berbasis 2.0 dalam dokumentasi. IAM

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

Dalam AWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensil pengguna, yang Anda simpan dalam bentuk terenkripsi. Ini terdiri dari nilai rahasia dan metadata-nya. Nilai rahasia dapat berupa biner, string tunggal, atau beberapa string. Untuk informasi selengkapnya, lihat Apa yang ada di rahasia Secrets Manager? dalam dokumentasi Secrets Manager.

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

Pagar pembatas teknis atau administratif yang mencegah, mendeteksi, atau mengurangi kemampuan pelaku ancaman untuk mengeksploitasi kerentanan keamanan. Ada empat jenis kontrol keamanan utama: preventif, detektif, responsif, dan proaktif.

pengerasan keamanan

Proses mengurangi permukaan serangan untuk membuatnya lebih tahan terhadap serangan. Ini dapat mencakup tindakan seperti menghapus sumber daya yang tidak lagi diperlukan, menerapkan praktik keamanan terbaik untuk memberikan hak istimewa paling sedikit, atau menonaktifkan fitur yang tidak perlu dalam file konfigurasi.

informasi keamanan dan manajemen acara (SIEM) sistem

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen peristiwa keamanan (SEM). Sebuah SIEM sistem mengumpulkan, memantau, dan menganalisis data dari server, jaringan, perangkat, dan sumber lain untuk mendeteksi ancaman dan pelanggaran keamanan, dan untuk menghasilkan peringatan.

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup VPC keamanan, menambal EC2 instans Amazon, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCPsmenentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCPs daftar izin atau daftar penolakan, untuk menentukan layanan atau tindakan mana yang diizinkan atau dilarang. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam AWS Organizations dokumentasi.

titik akhir layanan

Titik masuk untuk sebuah Layanan AWS. URL Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat Layanan AWS titik akhir di Referensi Umum AWS.

perjanjian tingkat layanan () SLA

Perjanjian yang menjelaskan apa yang dijanjikan tim TI untuk diberikan kepada pelanggan mereka, seperti waktu kerja dan kinerja layanan.

indikator tingkat layanan () SLI

Pengukuran aspek kinerja layanan, seperti tingkat kesalahan, ketersediaan, atau throughputnya.

tujuan tingkat layanan () SLO

Metrik target yang mewakili kesehatan layanan, yang diukur dengan indikator tingkat layanan.

model tanggung jawab bersama

Model yang menjelaskan tanggung jawab yang Anda bagikan AWS untuk keamanan dan kepatuhan cloud. AWS bertanggung jawab atas keamanan cloud, sedangkan Anda bertanggung jawab atas keamanan di cloud. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

satu titik kegagalan (SPOF)

Kegagalan dalam satu komponen penting dari aplikasi yang dapat mengganggu sistem.

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan

mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

Struktur organisasi database yang menggunakan satu tabel fakta besar untuk menyimpan data transaksional atau terukur dan menggunakan satu atau lebih tabel dimensi yang lebih kecil untuk menyimpan atribut data. Struktur ini dirancang untuk digunakan dalam gudang data atau untuk tujuan intelijen bisnis.

pola ara pencekik

Pendekatan untuk memodernisasi sistem monolitik dengan menulis ulang secara bertahap dan mengganti fungsionalitas sistem sampai sistem warisan dapat dinonaktifkan. Pola ini menggunakan analogi pohon ara yang tumbuh menjadi pohon yang sudah mapan dan akhirnya mengatasi dan menggantikan inangnya. Pola ini diperkenalkan oleh Martin Fowler sebagai cara untuk mengelola risiko saat menulis ulang sistem monolitik. Untuk contoh cara menerapkan pola ini, lihat Memodernisasi Microsoft lama. ASP NET(ASMX) layanan web secara bertahap dengan menggunakan kontainer dan Amazon API Gateway.

subnet

Berbagai alamat IP di AndaVPC. Subnet harus berada di Availability Zone tunggal.

kontrol pengawasan dan akuisisi data () SCADA

Di bidang manufaktur, sistem yang menggunakan perangkat keras dan perangkat lunak untuk memantau aset fisik dan operasi produksi.

enkripsi simetris

Algoritma enkripsi yang menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.

pengujian sintetis

Menguji sistem dengan cara yang mensimulasikan interaksi pengguna untuk mendeteksi potensi masalah atau untuk memantau kinerja. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat tes ini.

sistem prompt

Teknik untuk memberikan konteks, instruksi, atau pedoman LLMuntuk mengarahkan perilakunya. Permintaan sistem membantu mengatur konteks dan menetapkan aturan untuk interaksi dengan pengguna.

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Tanda dapat membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda.

variabel target

Nilai yang Anda coba prediksi dalam ML yang diawasi. Ini juga disebut sebagai variabel hasil. Misalnya, dalam pengaturan manufaktur, variabel target bisa menjadi cacat produk.

daftar tugas

Alat yang digunakan untuk melacak kemajuan melalui runbook. Daftar tugas berisi ikhtisar runbook dan daftar tugas umum yang harus diselesaikan. Untuk setiap tugas umum, itu termasuk perkiraan jumlah waktu yang dibutuhkan, pemilik, dan kemajuan.

lingkungan uji

Lihat lingkungan.

pelatihan

Untuk menyediakan data bagi model ML Anda untuk dipelajari. Data pelatihan harus berisi jawaban yang benar. Algoritma pembelajaran menemukan pola dalam data pelatihan yang memetakan atribut data input ke target (jawaban yang ingin Anda prediksi). Ini menghasilkan model ML yang menangkap pola-pola ini. Anda kemudian dapat menggunakan model ML untuk membuat prediksi pada data baru yang Anda tidak tahu targetnya.

gerbang transit

Hub transit jaringan yang dapat Anda gunakan untuk menghubungkan jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

Pendekatan di mana pengembang membangun dan menguji fitur secara lokal di cabang fitur dan kemudian menggabungkan perubahan tersebut ke cabang utama. Cabang utama kemudian dibangun untuk pengembangan, praproduksi, dan lingkungan produksi, secara berurutan.

akses tepercaya

Memberikan izin ke layanan yang Anda tentukan untuk melakukan tugas di organisasi Anda di dalam AWS Organizations dan di akunnya atas nama Anda. Layanan tepercaya menciptakan peran terkait layanan di setiap akun, ketika peran itu diperlukan, untuk melakukan tugas manajemen untuk Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan AWS layanan lain dalam AWS Organizations dokumentasi.

penyetelan

Untuk mengubah aspek proses pelatihan Anda untuk meningkatkan akurasi model ML. Misalnya, Anda dapat melatih model ML dengan membuat set pelabelan, menambahkan label, dan kemudian mengulangi langkah-langkah ini beberapa kali di bawah pengaturan yang berbeda untuk mengoptimalkan model.

tim dua pizza

Sebuah DevOps tim kecil yang bisa Anda beri makan dengan dua pizza. Ukuran tim dua pizza memastikan peluang terbaik untuk berkolaborasi dalam pengembangan perangkat lunak.

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian: ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data. Untuk informasi lebih lanjut, lihat panduan Mengukur ketidakpastian dalam sistem pembelajaran mendalam.

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau

memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

Operasi pemeliharaan database yang melibatkan pembersihan setelah pembaruan tambahan untuk merebut kembali penyimpanan dan meningkatkan kinerja.

kendali versi

Proses dan alat yang melacak perubahan, seperti perubahan kode sumber dalam repositori.

VPCmengintip

Koneksi antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas dengan menggunakan alamat IP pribadi. Untuk informasi selengkapnya, lihat Apa yang VPC mengintip di VPC dokumentasi Amazon.

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data terkini dan relevan yang sering diakses. Instance database dapat membaca dari cache buffer, yang lebih cepat daripada membaca dari memori utama atau disk.

data hangat

Data yang jarang diakses. Saat menanyakan jenis data ini, kueri yang cukup lambat biasanya dapat diterima.

fungsi jendela

SQLFungsi yang melakukan perhitungan pada sekelompok baris yang berhubungan dengan catatan saat ini. Fungsi jendela berguna untuk memproses tugas, seperti menghitung rata-rata bergerak atau mengakses nilai baris berdasarkan posisi relatif dari baris saat ini.

beban kerja

Kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti aplikasi yang dihadapi pelanggan atau proses backend.

aliran kerja

Grup fungsional dalam proyek migrasi yang bertanggung jawab atas serangkaian tugas tertentu. Setiap alur kerja independen tetapi mendukung alur kerja lain dalam proyek. Misalnya, alur kerja portofolio bertanggung jawab untuk memprioritaskan aplikasi, perencanaan gelombang, dan mengumpulkan metadata migrasi. Alur kerja portofolio mengirimkan aset ini ke alur kerja migrasi, yang kemudian memigrasikan server dan aplikasi.

WORM

Lihat menulis sekali, baca banyak.

WQF

Lihat AWSKerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

Model penyimpanan yang menulis data satu kali dan mencegah data dihapus atau dimodifikasi. Pengguna yang berwenang dapat membaca data sebanyak yang diperlukan, tetapi mereka tidak dapat mengubahnya. Infrastruktur penyimpanan data ini dianggap tidak dapat diubah.

Z

eksploitasi zero-day

Serangan, biasanya malware, yang memanfaatkan kerentanan zero-day.

kerentanan zero-day

Cacat atau kerentanan yang tak tanggung-tanggung dalam sistem produksi. Aktor ancaman dapat menggunakan jenis kerentanan ini untuk menyerang sistem. Pengembang sering menyadari kerentanan sebagai akibat dari serangan tersebut.

bisikan zero-shot

LLMMemberikan instruksi untuk melakukan tugas tetapi tidak ada contoh (bidikan) yang dapat membantu membimbingnya. LLMHarus menggunakan pengetahuan pra-terlatih untuk menangani tugas. Efektivitas bidikan nol tergantung pada kompleksitas tugas dan kualitas prompt. Lihat juga beberapa bidikan yang diminta.

aplikasi zombie

Aplikasi yang memiliki rata-rata CPU dan penggunaan memori di bawah 5 persen. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini.

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