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

AWS Panduan Preskriptif

AWS Panduan 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 manajer lain CxOs VPs, dan 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 menyediakan CxOs VPs, 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. AWS menawarkan berbagai layanan yang dapat Anda gunakan untuk menerapkan ZTA, seperti Akses

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 (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 IIo T) 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. Sangat 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 ()NACLs, dan AWS fitur spesifik seperti Amazon 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.

Otomasi 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.

Manajemen 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 membuat katalog 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?” 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 berkelanjutan dan manajemen patch
- Dasar 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 CCo E 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 pemantauan, respons insiden, dan kemampuan intelijen ancaman, pertimbangkan untuk menerapkan pusat operasi keamanan (SOCs) atau penyedia layanan keamanan terkelola (MSSPs). 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, tetapkan 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 (KPIs), memantau dan mengevaluasi KPIs, 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 yang relevan (KPIs) untuk mengukur keberhasilan dan kemanjuran penyebaran Zero Trust. Ini KPIs mungkin 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 ini KPIs.

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. Ini membutuhkan perubahan budaya dalam organisasi Anda. Membina pola pikir Zero Trust melibatkan penekanan aspek-aspek kunci berikut.

Pendidikan dan pelatihan Zero Trust

Mendidik karyawan tentang nilai dan keunggulan 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 up to date pada tren keamanan terbaru, teknologi, dan praktik terbaik. Memupuk budaya inovasi dan eksperimen di mana karyawan didorong untuk mengeksplorasi solusi dan pendekatan baru untuk memperkuat postur keamanan organisasi.

Metrik dan akuntabilitas

Menetapkan metrik yang jelas dan mekanisme akuntabilitas untuk mengukur efektivitas strategi Zero Trust. Tentukan indikator kinerja utama (KPIs) yang selaras dengan tujuan keamanan organisasi, dan secara teratur melacak kemajuan. 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 dasar yang kuat untuk keberhasilan adopsi dan implementasi Zero Trust. Pergeseran budaya ini sangat penting untuk membantu semua orang di organisasi untuk memahami pentingnya Zero Trust dan secara aktif berkontribusi pada keberhasilannya.

Bagian selanjutnya mengeksplorasi pendekatan adopsi bertahap, memberikan panduan tentang cara menerapkan prinsip Zero Trust secara bertahap dengan cara yang praktis dan dapat 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.

Fase 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 reguler.
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 Anda ZTAs 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, VPs, 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, VPs, 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 FIDO2 didukung perangkat keras, 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 pemberitahuan 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 Inspector AWS Security Hub CSPM, 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 CSPM
- 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 berikutnya

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?

AWS menyediakan 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 dengan AWS?

AWS menawarkan 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 Artifact menyediakan 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?

AWS menyediakan layanan seperti AWS Security Hub CSPM, 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

AWS menawarkan 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

Referensi

- Apa yang dimaksud dengan cloud center of excellence dan mengapa organisasi Anda harus membuatnya? — Posting blog ini memberikan gambaran umum tentang CCo E, praktik terbaik untuk cara membuat CCo E 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 Management Panduan Pengguna (IAM) — Panduan ini menawarkan dokumentasi komprehensif tentang pengelolaan akses pengguna dan izin di IAM, komponen penting dari arsitektur zero trust.
- AWS Security Hub CSPM— Pelajari tentang Security Hub CSPM, layanan yang memberikan pandangan komprehensif tentang peringatan keamanan dan status kepatuhan di seluruh Anda. Akun AWS
- AWS Well-Architected Framework — Jelajahi Well-Architected Framework, yang memberikan panduan untuk membangun arsitektur yang aman, berkinerja tinggi, tangguh, dan efisien. AWS
- AWS Panduan Respons Insiden Keamanan — Panduan ini menyajikan ikhtisar dasar-dasar menanggapi insiden keamanan dalam lingkungan organisasi Anda. AWS Cloud Panduan ini memberikan ikhtisar tentang keamanan cloud dan konsep respons insiden serta mengidentifikasi kemampuan, layanan, dan mekanisme cloud yang tersedia bagi pelanggan yang merespons 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 CSPM
- 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

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