Pemisahan Logikal di AWS

Laporan Resmi AWS

Pemisahan Logikal di AWS: Laporan Resmi AWS

Daftar Isi

Pemisahan Logikal di AWS

Tanggal publikasi: **28 Juli 2020** (*Revisi Dokumen* (hal. 19))

Abstrak

Laporan ini membahas topik pemisahan logikal untuk pelanggan yang menggunakan Amazon Web Services (AWS). Laporan ini membahas penggunaan pendekatan multicabang — misalnya, memanfaatkan virtualisasi, enkripsi, dan kebijakan program — untuk membangun mekanisme keamanan logikal yang memenuhi dan sering melebihi hasil keamanan dari pemisahan fisik dan pendekatan keamanan di lokasi lainnya. Sektor publik dan organisasi komersial di seluruh dunia dapat memanfaatkan mekanisme ini agar lebih percaya diri dalam memigrasi beban kerja sensitif ke cloud tanpa memerlukan infrastruktur khusus secara fisik.

Pendahuluan

Teknologi cloud memanfaatkan teknik transformatif dalam teknologi informasi (TI). Salah satu teknik fundamental adalah menawarkan layanan multipenyewa yang menempatkan banyak aplikasi dan data pelanggan pada infrastruktur fisik yang sama. Arsitektur ini memungkinkan penyedia layanan cloud (CSP), seperti AWS, untuk memaksimalkan penggunaan sumber daya fisik sehingga mereka dapat menawarkan nilai sumber daya tersebut dengan biaya lebih rendah kepada pelanggan. Hal ini juga memungkinkan pelanggan untuk dengan mudah memperbarui dan memigrasi beban kerja mereka dengan gangguan minimal ke teknologi terbaru karena terus masuk ke infrastruktur CSP. Pilihan arsitektur ini dimungkinkan oleh pengembangan kontrol keamanan logikal yang kuat dan fleksibel yang menciptakan batas isolasi yang kuat di antara pelanggan. Sejak meluncurkan layanan cloud pertamanya pada tahun 2006, AWS terus meningkatkan fitur dan kontrolnya sehingga pelanggan dapat mencapai kondisi keamanan yang diperlukan untuk memenuhi persyaratan klasifikasi data mereka. Pelanggan sering kali menemukan bahwa CSP, seperti AWS, memungkinkan mereka untuk mengoptimalkan konfigurasi keamanan di cloud secara efektif dibandingkan dengan solusi lokal mereka.

Pelanggan yang menggunakan AWS dapat memperoleh manfaat dari pusat data, jaringan, dan arsitektur perangkat lunak yang dibangun untuk memenuhi persyaratan dari organisasi yang paling sensitif terhadap keamanan di dunia. AWS menyediakan layanan yang sangat tersedia dan mendukung kombinasi mekanisme keamanan tradisional dan baru yang melekat pada desain dan operasi layanannya.

AWS memberi pelanggan beragam kontrol atas konten mereka dan menyediakan alat untuk menentukan lokasi konten mereka dan cara perlindungannya. Fitur-fitur AWS memberi pelanggan kemampuan untuk mengamankan konten mereka saat transit dan saat diam, untuk mengontrol akses secara ketat ke layanan dan sumber daya AWS bagi pengguna mereka, dan untuk memantau akses serta perkembangan sistem mereka. Pelanggan AWS menjaga kontrol penuh atas akses ke konten mereka, yang memungkinkan arsitektur untuk mencegah akses data pelanggan oleh pengguna yang tidak sah. Semua ini terjadi dalam kerangka kerja layanan multipenyewa dengan isolasi logika yang ketat. Isolasi logikal antara lingkungan pelanggan yang disediakan oleh AWS bisa lebih efektif dan andal daripada keamanan yang terlihat pada infrastruktur fisik khusus.

Pendorong Persyaratan Pemisahan Fisik

Persyaratan untuk lingkungan khusus secara fisik terutama didorong oleh kekhawatiran seputar akses pihak ketiga atau tidak sah ke sistem, aplikasi, atau data. Ada kesalahpahaman umum bahwa lingkungan yang terpisah secara fisik akan memberikan perlindungan yang lebih baik terhadap informasi yang tidak diinginkan atau pengungkapan sistem, gangguan, dan akses tidak sah dibandingkan dengan lingkungan cloud multipenyewa yang dipisahkan secara logikal. Namun, saat memeriksa vektor serangan yang paling umum terhadap akses tidak sah — seperti eksploitasi jarak jauh, kesalahan manusia, dan ancaman orang dalam — lingkungan yang terpisah secara fisik tidak mengurangi profil risiko. Faktanya, untuk sistem apa pun yang dapat diakses melalui jaringan atau Internet, pemisahan fisik — seperti menempatkannya dalam sangkar terkunci atau fasilitas pusat data terpisah — tidak secara inheren memberikan keamanan atau kontrol tambahan atas bentuk akses yang paling penting.

Selain itu, lingkungan lebih kecil yang terpisah secara fisik tidak memiliki kesamaan dengan lingkungan cloud yang tersedia secara umum; karenanya, persyaratan pemisahan fisik apa pun dapat membatasi atau menunda kemampuan pelanggan untuk memanfaatkan investasi inovatif (termasuk inovasi fitur keamanan) yang dilakukan atas nama semua pelanggan yang menggunakan layanan AWS. Kerugiannya mungkin termasuk struktur biaya yang lebih tinggi, garis waktu kepatuhan yang meluas, serta opsi dan fitur redundansi yang terbatas dibandingkan dengan keragaman geografis wilayah pusat data komersial.

AWS mengatasi masalah yang mendorong persyaratan pemisahan fisik melalui kemampuan keamanan logikal yang kami berikan kepada pelanggan dan kontrol keamanan yang kami miliki untuk membantu melindungi data pelanggan. Kekuatan isolasi tersebut dipadukan dengan otomatisasi dan fleksibilitas yang diberikan setara atau lebih baik daripada kontrol keamanan yang terlihat di lingkungan tradisional yang terpisah secara fisik.

Pemisahan Logikal Dibandingkan dengan Pemisahan Fisik

Pelanggan dapat memanfaatkan beberapa atau semua aspek kemampuan AWS di bawah ini untuk memenuhi atau melampaui keamanan dari persyaratan pemisahan fisik di lokasi mereka.

- **Autentikasi dan otorisasi terpadu** – Model autentikasi dan otorisasi yang kuat dan terperinci yang umum di semua layanan AWS yang terintegrasi dengan sistem pengelolaanidentitas pengguna di lokasi.
- **Pemantauan dan pembuatan log yang ditingkatkan** – Layanan pembuatan log yang mendalam dan mendetail untuk visibilitas semua panggilan API dan status sumber daya di seluruh layanan AWS. Peristiwa aplikasi dan konfigurasi saat ini dibuat log secara terpusat untuk memahami dengan cepat postur keamanan saat ini serta rekaman status konfigurasi sebelumnya.
- **Virtual private cloud (VPC) dan fitur yang menyertainya** — VPC adalah jaringan yang ditentukan perangkat lunak yang memungkinkan pelanggan membuat domain jaringan tersegmentasi atau tersegmentasi mikro untuk mengisolasi arus lalu lintas antara lingkungan komputasi yang berbeda dan layanan AWS serta menggabungkan segmen saat diperlukan dengan cara yang aman dan terbatas.
- **Mengenkripsi data saat tidak digunakan dan saat transit** — Opsi enkripsi untuk semua layanan penyimpanan AWS, pembuatan sertifikat yang andal, dan pengelolaan siklus hidup untuk mengenkripsi data saat transit. Pengelolaan kunci melalui AWS Key Management Service (AWS KMS) atau secara optional menggunakan AWS CloudHSM untuk pembuatan dan penyimpanan kunci.
- **Isolasi instans dan host** — Opsi untuk menyediakan arsitektur khusus yang menggunakan hypervisor atau bare-metal untuk mengamankan data pelanggan di host komputasi fisik tidak dibagikan dengan orang lain.
- **Arsitektur kontainer dan tanpa server** — Lingkungan eksekusi yang terisolasi menawarkan lingkungan waktu operasi singkat yang lebih singkat untuk menyederhanakan kontrol keamanan.

Topik

Mekanisme Autentikasi dan Otorisasi Terpadu

Mekanisme keamanan yang mendefinisikan dan mengelola identitas dan pengelolaan akses termasuk salah satu bagian paling penting dari program keamanan informasi. Mekanisme itu berfungsi untuk memastikan bahwa hanya pelaku yang diautentikasi (pengguna, peran, grup, aplikasi, dan identitas lain) yang diberi wewenang untuk mengakses sumber daya yang ditargetkan dengan cara yang dimaksudkan dan dengan hak istimewa paling kecil. Fitur utama yang diupayakan oleh banyak organisasi adalah autentikasi terpadu di seluruh layanan perusahaan. Fitur ini memungkinkan untuk validasi identitas yang berlaku untuk seluruh portofolio layanan. Menjalankan fungsi ini sulit terutama jika berurusan dengan beragam sistem yang memerlukan format kredensial khusus atau memiliki model otorisasi yang tidak kompatibel.

Dengan AWS, pelanggan mendapatkan kemampuan untuk melakukan autentikasi dan otorisasi terpadu di semua layanan AWS guna menerapkan hak istimewa yang paling rendah. AWS Identity and Access Management (IAM) memungkinkan pelanggan untuk mengautentikasi ke layanan AWS apa pun menggunakan format kredensial yang sama. IAM mendukung berbagai cara autentikasi termasuk kunci akses API, kata sandi pengguna berbasis konsol, dan federasi menggunakan penyedia identitas eksternal. Pelanggan dapat mengonfigurasi mode autentikasi di IAM untuk meminta multifaktor. AWS memungkinkan pelanggan mengontrol akses ke sumber dayanya di layanan AWS menggunakan mekanisme autentikasi berbasis kebijakan. Setiap kebijakan diisi baik oleh pelanggan atau AWS, jika menggunakan kebijakan yang dikelola AWS, dengan elemen yang dapat ditentukan yang bekerja bersama untuk membuat tindakan "izinkan" atau "tolak" secara terperinci dan bersyarat pada sumber daya tertentu. Pelanggan dapat membagikan atau menggunakan kembali kebijakan lintas identitas keduanya di dalam dan antarakun, terlepas dari bagaimana identitas tersebut diautentikasi. Ketangguhan kemampuan ini memungkinkan pelanggan merancang berbagai mekanisme isolasi serta penggunaan sumber daya cloud dan elemen tingkat aplikasi. Ini dapat dilakukan dengan menggunakan metode kontrol akses berbasis peran (RBAC) atau metode kontrol akses berbasis atribut (ABAC) maupun keduanya.

Pelanggan dapat menggunakan kebijakan dalam berbagai cara termasuk 1) mengontrol sumber daya yang dapat diakses oleh sekelompok pengguna, 2) mengontrol pengguna yang dapat mengakses sumber daya tertentu, 3) mengontrol layanan AWS yang dapat digunakan, dan 4) mengontrol pengguna yang diizinkan untuk memodifikasi kebijakan. Semua kebijakan memungkinkan penggunaan kondisi untuk cakupan akses lebih lanjut. Misalnya, pelanggan dapat memberlakukan kebijakan yang hanya mengizinkan akses ke konten di dalam bucket Amazon Simple Storage Service (Amazon S3) jika pengguna memiliki akses ke kunci dekripsi terkelola dalam AWS Key Management Service dan permintaan itu dibuat melalui VPC tertentu. Kemampuan apa pun untuk mengubah kebijakan seperti itu dapat dicakup ke dalam kumpulan modifikasi terbatas yang hanya dapat dilakukan oleh kumpulan administrator yang memiliki hak istimewa, yang semuanya harus mengautentikasi menggunakan beberapa faktor. Kebijakan dapat ditegakkan pada seluruh akun menggunakan AWS Organizations.

Tingkat kontrol, integrasi mendalam, dan interoperabilitas yang luas ini akan sangat sulit untuk diterapkan dan dikelola dalam lingkungan perusahaan on-premise tradisional dengan sistem yang terpisah dan terpisah secara fisik. Sebagian besar organisasi menggunakan kombinasi akses dan solusi pengelolaan identitas yang bervariasi di seluruh unit bisnis dan aplikasi, tetapi juga di berbagai lapisan "tumpukan" infrastruktur — perangkat jaringan, virtualisasi, sistem operasi, dan aplikasi. Ini mengarah pada serangkaian besar layanan identitas yang perlu diikat dan dikelola secara terpadu. Dengan menambah kompleksitas pengelolaan, integrasi sistem ini biasanya memerlukan pekerjaan manual yang signifikan ditambah dengan perawatan dan perhatian yang terus-menerus saat bagian lain dari portofolio layanan dimasukkan ke dalam paket. Selain itu, kebijakan akses seragam masih harus dibuat untuk memastikan penerapan dilaksanakan pada tingkat sistem dan data di seluruh perusahaan.

Dengan AWS, pengelolaan keamanan berbasis kebijakan memberi beberapa keuntungan berbeda kepada pelanggan. Kebijakan keamanan dapat dibuat agar dapat dipahami oleh manusia dan mesin. Ini berarti bahwa, selain memperlakukan kebijakan sebagai kode, juga dapat menjadi artefak yang representatif untuk upaya tata kelola, risiko, dan kepatuhan. Ini sangat meningkatkan kejelasan, keakuratan, dan transparansi dengan membiarkan para pemangku kepentingan melihat tindakan yang bisa dan tidak bisa dilakukan saat dapat menjalankan kebijakan tersebut secara langsung dalam layanan. Kebijakan dapat dibuat dan dikelola secara terprogram dalam saluran sebagai kode. Hal ini memungkinkan kontrol pengelolaan konfigurasi yang sama atas kebijakan yang dimiliki organisasi dengan kode aplikasinya. Manfaat lain yang berbeda adalah kemampuan untuk memanfaatkan otomatisasi pengujian dalam saluran proses, seperti yang Anda lakukan pada pengembangan perangkat lunak, untuk memverifikasi dan memvalidasi bahwa kebijakan berfungsi seperti yang diharapkan. Contohnya adalah IAM Access Analyzer yang dapat diaktifkan pelanggan untuk terus mengevaluasi izin yang diberikan dalam kebijakan guna mengidentifikasi sumber daya yang dapat diakses dari luar akun AWS pelanggan. IAM Access Analyzer menggunakan penalaran otomatis, yang menerapkan logikal dan inferensi matematika untuk mengevaluasi ratusan atau bahkan ribuan kebijakan di lingkungan pelanggan dalam hitungan detik.

Pemantauan dan Pembuatan Log yang Ditingkatkan

Landasan untuk mendeteksi dan melindungi lingkungan dan data seseorang adalah kemampuan untuk memantau konfigurasi secara terperinci di seluruh perusahaan dan pembuatan log yang kuat dari aktivitas yang terjadi dalam infrastruktur TI. Visibilitas dan keterbacaan dalam lingkungan TI seringkali sulit dicapai untuk operasi on-premise besar yang berfokus pada kontrol keamanan berbasis pemisahan fisik. Rancangan ini dapat mengakibatkan fragmentasi pandangan operasional karena kurangnya integrasi antarlayanan. Situasi ini membuat deteksi ancaman dan analisis akar masalah menjadi tantangan. AWS membangun layanan keamanan inti yang sangat terintegrasi di seluruh layanan AWS, termasuk pemantauan dan pembuatan log. AWS CloudTrail, Amazon CloudWatch,

VPC Flow Logs, dan AWS Config diintegrasikan di seluruh penawaran layanan AWS, menyediakan rekaman aktivitas dan perubahan konfigurasi yang jelas. Informasi yang diberikan oleh layanan ini menggambarkan pandangan multidimensi status operasional sistem dan data dari perspektif fungsional, performa, dan keamanan. Visibilitas komprehensif ini juga dapat dicapai dengan biaya lebih rendah dibandingkan dengan sistem perusahaan on-premise.

AWS CloudTrail menyediakan opsi pembuatan log permintaan AWS API bagi pelanggan, terlepas apakah permintaan tersebut dibuat melalui AWS Management Console, AWS SDKs, alat baris perintah, atau melalui layanan AWS lainnya atas nama pelanggan. Setiap peristiwa log mengidentifikasi identitas pemanggil dan memanggil AWS API, alamat IP sumber panggilan, saat panggilan terjadi, dan parameter lain yang khusus untuk API. Log dapat diserap ke dalam sistem informasi keamanan lokal dan pengelolaan peristiwa (SIEM) pelanggan untuk analisis atau dikirim ke layanan analitik AWS lainnya seperti CloudWatch Logs Insights. Log AWS CloudTrail ditandatangani secara digital guna mencegah gangguan sebelum disimpan di Amazon S3 untuk diakses pelanggan. Log juga dapat disimpan menggunakan S3 Object Lock untuk membuat kebijakan kuat yang membuat semua pengguna, bahkan pengguna root, tidak dapat menghapus objek. Log dienkripsi dalam penyimpanan, secara opsional di bawah kunci kontrol pelanggan di AWS KMS.

Amazon CloudWatch digunakan untuk memantau sumber daya AWS dan aplikasi yang mendekati waktu nyata. Dapat mengumpulkan, melacak, dan memperingatkan berdasarkan metrik yang dapat diakses melalui dasbor atau API yang dapat disesuaikan. Data CloudWatch dienkripsi saat transit dan saat tidak digunakan. Selain itu, Amazon EventBridge memberikan aliran peristiwa sistem yang mendekati waktu nyata yang menjelaskan perubahan pada sumber daya AWS kepada pelanggan, yang dapat mengatur alarm dan memberitahukan akses yang berpotensi tidak sah. Aturan dapat diterapkan untuk mencocokkan peristiwa dan diarahkan ke satu atau beberapa fungsi atau aliran target untuk pemantauan lebih lanjut atau bahkan pelaksanaan tindakan korektif. Misalnya, aturan dapat memeriksa peristiwa masuk, mengurai nilai yang masuk, dan merutekan peristiwa dengan benar ke sejumlah target, seperti email atau perangkat seluler, antrean tiket, dan sistem pengelolaan masalah.

Pengelolaan konfigurasi adalah inti dari kontrol perubahan lingkungan. Konfigurasi yang menyimpang dari keadaan yang diinginkan menimbulkan risiko pada postur keamanan sistem. Mengelola dan menegakkan status konfigurasi di lingkungan on-premise biasanya sulit karena sarana untuk mengukur keadaan sistem saat ini sering kali kekurangan titik integrasi yang cukup untuk memberikan pandangan holistik perusahaan. Di AWS, pelanggan dapat mengatasi pengelolaan konfigurasi dalam beberapa cara. Salah satu opsi terbaik adalah beralih ke model infrastruktur sebagai kode (IaC) untuk lingkungan Anda. IaC memungkinkan Anda untuk menyediakan, membatalkan penyediaan, dan memelihara status konfigurasi infrastruktur secara konsisten, berulang, dan otomatis menggunakan kode. Termasuk kemampuan untuk menggunakan praktik pengelolaan kode yang aman dan otomatisasi pengujian langsung pada komponen infrastruktur. Salah satu cara untuk mencapainya dengan AWS yaitu menggunakan AWS CloudFormation.

Templat AWS CloudFormation dapat membuat, mengonfigurasi, dan mengelola sumber daya melalui penggunaan JavaScript Object Notation (JSON) atau YAML. Anda mengelola sumber daya ini dicantumkan pada templat dalam unit yang disebut Tumpukan AWS CloudFormation. Tumpukan dapat disusun sebagai StackSets untuk mengelola sumber daya di seluruh wilayah dan akun dari satu templat atau kumpulan templat. Dari sudut pandang pemantauan, CloudFormation terintegrasi dengan CloudTrail untuk merekam tindakan yang dilakukan oleh layanan. Selain itu, CloudFormation dapat mendeteksi penyimpangan konfigurasi antara konfigurasi sumber daya saat ini dari StackSets dengan konfigurasi yang diharapkan yang dicantumkan di StackSets. Tingkat pengelolaan konfigurasi ini dapat mendeteksi perubahan yang tidak dikelola dan memungkinkan pengguna untuk menerapkan kembali templat guna mengembalikan sumber daya ke keadaan yang dicantumkan.

Sering kali kemampuan pengelolaan konfigurasi yang lebih dalam dan lebih luas dibutuhkan oleh pelanggan untuk menangani banyak cara sumber daya AWS dapat disediakan, diubah, dan dikelola. AWS Config memenuhi kebutuhan ini dengan memberikan tampilan konfigurasi yang terperinci dan berkelanjutan dari sumber daya AWS di akun AWS pelanggan. Termasuk bagaimana sumber daya terkait satu sama lain dan dikonfigurasi di masa lalu sehingga pelanggan dapat melihat perubahan konfigurasi dan hubungan seiring waktu. AWS Config menyediakan inventaris sumber daya AWS, riwayat konfigurasi, dan pemberitahuan perubahan konfigurasi di seluruh wilayah dan akun. Kemampuan ini, bersama dengan kueri lanjutan dan aturan yang dapat disesuaikan, memungkinkan wawasan keamanan dan tata kelola serta otomatisasi alur kerja untuk sumber daya AWS.

Kunci utama lainnya untuk pemantauan dan pembuatan log mendalam adalah visibilitas arus lalu lintas. VPC Flow Logs adalah fitur di mana pelanggan dapat menangkap informasi tentang lalu lintas IP yang pergi ke dan dari antarmuka jaringan di VPC mereka. Data log aliran dapat diterbitkan sebagai rekaman ke Amazon CloudWatch Logs dan Amazon S3 untuk analisis lebih lanjut. Log aliran dapat dibuat untuk seluruh VPC, subnet, atau satu antarmuka

jaringan. Selain Flow Logs, VPC juga memungkinkan pengambilan paket lengkap jika berguna atau perlu menggunakan fitur Traffic Mirroring. Kedua fitur ini bekerja sama dengan baik, VPC Flow Logs untuk pencatatan log jaringan rutin, dan mengaktifkan Traffic Mirroring secara sementara saat keadaan memerlukannya.

Berurusan dengan volume data log bisa jadi merepotkan bagi beberapa pelanggan sehingga banyak yang memilih untuk memudahkan pemantauan dan analisis log menggunakan Amazon GuardDuty, AWS yang dikelola untuk penawaran deteksi ancaman. GuardDuty adalah layanan yang menyediakan deteksi ancaman dan pemantauan keamanan jaringan berkelanjutan dengan mengonsumsi dan menganalisis banyak sumber data yang disebutkan di sini seperti Flow Logs dan log CloudTrail, ditambah log DNS AWS internal dan umpan intelijen ancaman. GuardDuty menerapkan pembelajaran mesin, analisis anomali perilaku, dan teknik deteksi lainnya untuk mengidentifikasi ancaman di seluruh aktivitas jaringan.

VPC dan Fitur yang Menyertai

Amazon Virtual Private Cloud (Amazon VPC) memungkinkan pembuatan daerah jaringan yang terpisah secara logis di dalam jaringan Amazon Elastic Cloud Compute (Amazon EC2) yang dapat menampung sumber daya komputasi dan penyimpanan. Lingkungan ini dapat dihubungkan ke infrastruktur pelanggan yang ada melalui berbagai cara termasuk koneksi jaringan pribadi virtual (VPN) melalui Internet, atau melalui AWS Direct Connect, suatu layanan yang menyediakan konektivitas pribadi ke AWS Cloud. Penggunaan VPC memberi organisasi fleksibilitas, keamanan, dan kontrol penuh atas kehadiran jaringan mereka di cloud. Pelanggan mengontrol lingkungan pribadi termasuk alamat IP, subnet, daftar kontrol akses jaringan, grup keamanan, firewall sistem operasi, tabel rute, VPN, dan gateway internet. Amazon VPC menyediakan isolasi logikal yang kuat dari semua sumber daya pelanggan, termasuk jalur akses mereka satu sama lain dan dengan layanan AWS.

Setiap aliran paket di jaringan secara individual diotorisasi terhadap aturan untuk memvalidasi sumber dan tujuan yang benar sebelum ditransmisi dan dikirim. Sangat tidak mungkin informasi secara sewenang-wenang melewati antara entitas tanpa secara khusus diizinkan oleh entitas pengirim dan penerima. Jika sebuah paket dirutekan ke tujuan tanpa aturan yang cocok, paket tersebut akan dibuang. Alamat balasan harus valid atau paket dibuang. Selain itu, meskipun paket protokol resolusi alamat (ARP) memicu pencarian database yang diautentikasi, paket ARP tidak pernah mencapai jaringan karena tidak diperlukan untuk menemukan topologi jaringan virtual. Artinya, pemalsuan ARP sangat tidak mungkin di jaringan AWS. Selain itu, mode campur-aduk tidak menampilkan lalu lintas apa pun selain lalu lintas yang terikat ke dan dari sistem operasi pelanggan. Pelanggan dapat menetapkan aturan yang tepat untuk masuk dan keluar lalu lintas yang memungkinkan peningkatan fleksibilitas konektivitas, dan memungkinkan kontrol pelanggan yang lebih besar atas segmentasi dan perutean lalu lintas.

Opsi konektivitas VPC mencakup berbagai kemampuan bagi pelanggan untuk:

- Terhubung ke Internet menggunakan Penerjemahan Alamat Jaringan (subnet pribadi) — Subnet pribadi yang dapat digunakan untuk instans yang seharusnya tidak memiliki akses langsung ke atau dari Internet. Instans di dalam suatu subnet pribadi dapat mengakses Internet tanpa mengekspos alamat IP pribadi mereka dengan merutekan lalu lintas mereka melalui gateway Penerjemahan Alamat Jaringan (NAT) di subnet publik.
- Terhubung dengan aman ke pusat data perusahaan — Semua lalu lintas ke dan dari instans di VPC dapat dirutekan ke pusat data perusahaan pelanggan melalui koneksi VPN perangkat keras IPsec terenkripsi yang sesuai standar industri.
- Terhubung secara pribadi ke VPC lain — Peer VPC bersama-sama berbagi sumber daya di beberapa jaringan virtual di beberapa akun AWS.
- Menghubungkan layanan internal secara pribadi di berbagai akun dan VPC dalam AWS Organization, yang secara signifikan menyederhanakan arsitektur jaringan internal.
- Menggunakan AWS Transit Gateway sebagai gerbang pusat tunggal dan terpadu tempat koneksi dapat dibuat ke banyak VPC dan sistem di lokasi sekaligus dapat mengelola autentikasi dan akses ke layanan dengan AWS IAM.
- Menggunakan fitur-fitur VPC seperti AWS PrivateLink untuk membuat koneksi pribadi ke sumber daya di luar VPC pelanggan. Koneksi pribadi ini tidak melintasi Internet publik dan dapat menyediakan konektivitas yang aman antara VPC, layanan AWS, dan aplikasi on-premise.

Selain itu, semua lalu lintas dalam sebuah VPC dan peer antarwilayah dienkripsi secara transparan saat menggunakan jenis instans yang didukung. Dari sudut pandang infrastruktur, enkripsi jaringan fisik digunakan oleh AWS untuk mengenkripsi lalu lintas jaringan pada tautan apa pun di luar kontrol fisik AWS seperti di antara beberapa pusat data.

Mengenkripsi Data yang Disimpan dan saat Transit

AWS merekomendasikan enkripsi sebagai kontrol akses tambahan untuk melengkapi identitas, sumber daya, dan kontrol akses berorientasi jaringan yang telah dijelaskan. AWS menyediakan sejumlah fitur yang memungkinkan pelanggan dengan mudah mengenkripsi data dan mengelola kunci. Semua layanan AWS menawarkan kemampuan untuk mengenkripsi data saat transit dan tidak digunakan. AWS KMS terintegrasi dengan sebagian besar layanan agar pelanggan dapat mengontrol siklus hidup dan izin pada kunci yang digunakan untuk mengenkripsi data atas nama pelanggan. Pelanggan dapat menerapkan dan mengelola enkripsi di seluruh layanan yang terintegrasi dengan AWS KMS melalui penggunaan alat konfigurasi dan kebijakan. Penggunaan enkripsi sisi server layanan AWS adalah cara termudah bagi pelanggan untuk memastikan enkripsi diterapkan dengan benar dan diterapkan secara konsisten. Pelanggan dapat mengontrol kapan data didekripsi, oleh siapa, dan dalam kondisi apa saat diteruskan ke dan dari aplikasi dan layanan AWS. Karena akses untuk mengenkripsi atau mendekripsi data dalam layanan dikontrol secara independen oleh kebijakan AWS KMS di bawah kontrol pelanggan, pelanggan dapat mengisolasi kontrol atas akses ke data, dari akses ke kunci. Model isolasi ini adalah kontrol pemisahan logikal tambahan yang kuat yang dapat diterapkan di seluruh lingkungan AWS pelanggan.

Selain mengontrol bagaimana enkripsi sisi server terjadi dalam layanan AWS, pelanggan dapat memilih untuk mengenkripsi data dalam lingkungan aplikasi mereka menggunakan AWS KMS dengan enkripsi sisi klien, sehingga mengeluarkan layanan AWS dari batas kepercayaan mereka. Enkripsi sisi klien tingkat aplikasi dapat digunakan untuk memastikan postur keamanan yang konsisten saat data melintas di dalam arsitektur layanan pelanggan, baik di AWS, on-premise, atau dalam model hibrida. Penggunaan AWS KMS untuk mengelola siklus hidup dan izin pada kunci menyediakan mekanisme kontrol akses yang konsisten bagi semua kunci enkripsi, di mana pun kunci tersebut digunakan.

Untuk mencegah penggunaan yang tidak sah atas kunci enkripsi di luar batas AWS KMS, layanan menggunakan modul keamanan perangkat keras (HSM) untuk melindungi materi kunci pelanggan saat digunakan. HSM ini divalidasi berdasarkan Standar Pemrosesan Informasi Federal (FIPS) 140-2 dengan kontrol respons kerusakan fisik. HSM dirancang sehingga kunci teks biasa tidak dapat digunakan di luar HSM oleh siapa pun, termasuk karyawan AWS. Satu-satunya cara kunci dapat digunakan adalah ketika permintaan pelanggan yang diautentikasi dan diotorisasi sudah diterima oleh layanan. Menanggapi permintaan tersebut, AWS KMS memungkinkan kunci pelanggan digunakan dalam HSM untuk operasi enkripsi atau dekripsi. Kunci pelanggan hanya dapat digunakan di dalam wilayah AWS tempatnya dibuat. HSM di AWS KMS dirancang sebagai multipenyewa yang berarti bahwa setiap kunci pelanggan dapat digunakan di HSM mana pun di wilayah tersebut. Seperti layanan AWS lainnya yang menggunakan multipenyewa, AWS KMS dirancang untuk mengisolasi penggunaan kunci hanya untuk pelanggan yang memiliki kunci. Tidak ada mekanisme bagi pengguna yang tidak sah untuk menyebabkan kunci pelanggan digunakan. AWS KMS secara transparan mengelola ketahanan dan ketersediaan kunci pelanggan dan dapat diskalakan guna mendukung sejumlah kunci dengan kecepatan yang dibutuhkan aplikasi pelanggan untuk menggunakannya. Pelanggan cukup mengelola siklus hidup dan izin kunci menggunakan kontrol autentikasi dan otorisasi yang sama tersedia untuk setiap layanan AWS lainnya.
Setiap permintaan yang dibuat dari AWS KMS dicatat ke AWS CloudTrail untuk memberikan audit kapan kunci digunakan dan dalam keadaan apa. AWS KMS berada dalam cakupan semua program akreditasi yang didukung oleh AWS yang terkait dengan perlindungan data.

Bagi pelanggan dengan persyaratan agar secara langsung mengelola perangkat HSM yang menghasilkan, menyimpan, dan menggunakan kunci enkripsi mereka, AWS CloudHSM tersedia sebagai opsi. AWS CloudHSM menawarkan FIPS 140-2 Level 3 khusus yang divalidasi dan meningkatkan fleksibilitas integrasi dengan aplikasi pelanggan menggunakan API standar industri seperti PKCS#11, Java Cryptography Extensions (JCE), dan pustaka Microsoft CryptoNG (CNG). Ini memungkinkan organisasi mengekspor kunci ke sebagian besar HSM lain yang tersedia secara komersial untuk digunakan dalam arsitektur hibrida. AWS mengotomatiskan tugas administratif yang memakan waktu seputar HSM ini, seperti penyediaan perangkat keras, penambalan perangkat lunak, perutean jaringan, dan pembuatan cadangan terenkripsi dari penyimpanan kunci. Pelanggan bertanggung jawab untuk menskalakan lingkungan CloudHSM dan mengelola akun pengguna kripto dan kredensial dalam HSM. Seperti AWS KSM, CloudHSM dirancang sehingga kunci teks biasa tidak dapat digunakan di luar HSM oleh siapa pun, termasuk karyawan AWS.

Pelanggan dapat memadukan kemudahan penggunaan dan integrasi dengan layanan AWS yang ditawarkan oleh AWS KMS dengan AWS CloudHSM menggunakan opsi penyimpanan kunci kustom AWS KMS. Pelanggan secara logis menempelkan kluster AWS CloudHSM ke pengenal kunci AWS KMS sehingga permintaan yang dibuat pada kunci akan diotorisasi oleh AWS KMS, tetapi dieksekusi pada CloudHSM pelanggan yang ditentukan.

Untuk melindungi data saat transit, AWS mendorong pelanggan untuk memanfaatkan pendekatan multitingkat. Semua lalu lintas jaringan antarpusat data AWS dienkripsi secara transparan di lapisan fisik. Semua lalu lintas dalam sebuah VPC dan di antara VPC yang dilakukan peer di seluruh wilayah akan dienkripsi secara transparan di lapisan jaringan saat menggunakan jenis instans Amazon EC2 yang didukung. Pada lapisan aplikasi, pelanggan memiliki pilihan tentang apakah dan bagaimana menggunakan enkripsi menggunakan protokol seperti Transport Layer Security (TLS). Semua titik akhir layanan AWS mendukung TLS guna membuat koneksi HTTPS yang aman untuk membuat permintaan API.

> AWS memperbarui semua titik akhir AWS FIPS ke versi minimum Transport Layer Security (TLS) 1.2 di semua Wilayah AWS, dengan target tanggal penyelesaian 31 Maret 2021. Setelah selesai, pembaruan ini akan mencabut kemampuan untuk menggunakan TLS 1.0 dan TLS 1.1 di semua titik akhir FIPS. Tidak ada titik akhir AWS lain yang akan terpengaruh oleh perubahan ini.

Untuk infrastruktur yang dikelola pelanggan dalam AWS yang perlu menghentikan TLS, AWS menawarkan beberapa opsi termasuk layanan load balancing (misalnya, Elastic Load Balancing, Network Load Balancer, dan Application Load Balancer), Amazon CloudFront (jaringan pengiriman konten), dan Amazon API Gateway. Untuk menerapkan koneksi TLS, masing-masing layanan titik akhir ini memungkinkan pelanggan mengunggah sertifikat digital mereka untuk mengikat identitas kriptografi ke titik akhir. Sertifikat digital terkenal sulit untuk dikelola dalam skala besar karena sudah habis masa berlakunya dan perlu dirotasi. AWS menyederhanakan proses pembuatan, pendistribusian, dan perputaran sertifikat digital menggunakan AWS Certificate Manager (ACM). ACM menawarkan sertifikat tepercaya publik tanpa biaya yang dapat digunakan dalam layanan AWS yang mengharuskan mereka untuk menghentikan koneksi TLS ke Internet. ACM juga menawarkan kemampuan untuk membuat otoritas sertifikat swasta agar secara otomatis menghasilkan, mendistribusikan dan merotasi sertifikat untuk mengamankan komunikasi internal di antara infrastruktur yang dikelola pelanggan.

Dengan menggunakan layanan seperti AWS KMS, AWS CloudHSM, dan AWS ACM, pelanggan dapat menerapkan strategi enkripsi data saat disimpan dan pada saat sedang transit yang komprehensif di seluruh ekosistem AWS untuk memastikan semua data dari klasifikasi yang diberikan memiliki postur keamanan yang sama.

Fitur Instans dan Host

AWS terus mengembangkan kemampuan keamanannya di tingkat operasi host dan instans. Fitur-fitur ini menyediakan isolasi dan pemisahan operasi untuk perangkat keras host dan instans yang berjalan pada host tersebut. Dengan pengantar tentang AWS Nitro System, AWS menyediakan mekanisme keamanan yang mendefinisikan industri untuk operasi firmware dan hypervisor. AWS Nitro System terdiri dari rangkaian kartu Peripheral component Interconnect Express (PCIe) dengan custom integrated circuit (ASIC) yang mengontrol fungsi berbeda seperti akses ke penyimpanan, jaringan virtual, dan Cip Kemanan Nitro yang terus memantau dan melindungi sumber daya perangkat keras dan memverifikasi firmware secara independen setiap kali sistem melakukan boot. Bersama dengan Nitro hypervisor, hypervisor berbasis mesin virtual kernel (KVM) ringan ini, menyediakan tulang punggung bagi banyak keluarga instans AWS. Ini memungkinkan AWS membatasi interaksi operator-host ke sekumpulan kecil fungsi yang hanya dapat dipanggil melalui API. Tidak ada akses shell interaktif. Instans virtual yang beroperasi pada host ini juga memiliki banyak mekanisme keamanan tambahan yang diberlakukan, seperti isolasi memori dan CPU.

Selain menyediakan layanan komputasi multipenyewa yang sangat aman dan terisolasi secara logis, AWS juga menyediakan sarana untuk menyebarkan komputasi ke perangkat keras khusus menggunakan Instans Khusus, Host Khusus, dan Bare Metal. Opsi penerapan ini dapat digunakan untuk meluncurkan instans Amazon EC2 ke server fisik yang dibuat khusus untuk penggunaan pelanggan. Instans Khusus adalah instans Amazon EC2 hypervised yang berjalan di sebuah VPC pada perangkat keras yang digunakan khusus untuk satu pelanggan. Instans Khusus secara fisik diisolasi di tingkat perangkat keras host dari instans milik akun AWS lain. Instans Khusus dapat berbagi perangkat keras dengan instans lain dari akun AWS yang sama yang bukan Instans Khusus. Host Khusus juga merupakan server fisik yang digunakan khusus untuk pelanggan. Dengan Host Khusus, pelanggan memiliki visibilitas dan kontrol atas bagaimana instans hypervised ditempatkan di server. Instans Bare Metal adalah perangkat keras host non-hypervised. Dengan menggunakan teknologi AWS Nitro untuk jaringan dan penyimpanan, serta Cip Keamanan Nitro untuk mengatasi risiko yang terkait dengan penyewa tunggal serial di Bare Metal, pelanggan memiliki akses langsung ke perangkat keras Amazon EC2. Instans Bare Metal ini adalah anggota penuh dari layanan Amazon EC2 dan memiliki akses ke layanan seperti Amazon VPC dan Amazon Elastic Block Store (Amazon EBS).

Ada sedikit atau tidak ada perbedaan kinerja, keamanan, atau fisik antara Instans Khusus dan instans yang diterapkan pada Host Khusus. Namun, Host Khusus memberi pelanggan kontrol tambahan atas cara penempatan instans di server fisik dan cara penggunaan server itu. Saat pelanggan menggunakan Host Khusus, mereka memiliki kontrol atas penempatan instans di host menggunakan pengaturan Host Affinity dan Instance Auto-placement. Jika pelanggan ingin menggunakan AWS, dan memiliki lisensi perangkat lunak yang ada yang mengharuskan perangkat lunak dijalankan pada perangkat keras tertentu selama suatu waktu minimum, Host Khusus memungkinkan visibilitas ke perangkat keras host, yang memungkinkan pelanggan untuk memenuhi persyaratan lisensi.

Kontainer dan Tanpa Server

Kemampuan untuk menggabungkan teknologi tanpa server, teknologi kontainer, dan desain layanan mikro secara lancar di AWS memungkinkan pelanggan membangun beberapa tingkat isolasi untuk beban kerja. Layanan AWS menggunakan keamanan berlapis untuk mencapai operasi yang terisolasi. Banyak fitur layanan keamanan seperti AWS Lambda dan AWS Fargate, saat beroperasi di belakang layar, didasarkan pada fungsionalitas yang disediakan oleh kapabilitas fitur dan layanan AWS yang telah dibahas dalam laporan resmi ini. Misalnya, kumpulan layanan dan kemampuan keamanan yang disertakan dengan arsitektur Nitro EC2, jaringan VPC, dan IAM, (misalnya, ACL, Grup Keamanan, dan Kebijakan IAM) juga berlaku di sini.

AWS melakukan pendekatan isolasi logikal dengan layanan tanpa servernya, AWS Lambda, dan layanan kontainer terkelola, AWS Fargate, secara berlapis-lapis. Lapisan ini dimulai dengan contoh bare matel, lapisan sama yang dapat disediakan oleh pelanggan mana pun, menggunakan arsitektur Nitro yang mendasari dan manfaat keamanan yang telah dibahas sebelumnya. Kemudian, pada lapisan berikutnya, ada monitor mesin virtual ringan yang dibuat khusus dan disebut Firecracker yang dibuat oleh AWS untuk mengelola kontainer dan fungsi tanpa server dengan aman. Firecracker berfungsi sebagai lingkungan terisolasi yang menyediakan eksekusi waktu operasi aman untuk kontainer dan fungsi tanpa server. Lambda beroperasi di EC2 sebagai mesin virtual mikro (VM mikro) dan menawarkan perlindungan serupa untuk isolasi logikal seperti instans EC2 lainnya. Setiap fungsi dijalankan di lingkungan pengujian yang terdapat di mikro-VM. Lingkungan pengujian menawarkan isolasi kernel Linux yang aman menggunakan cgroups, namespaces, seccomp, dan fitur lainnya. Selain itu, teknik-teknik seperti pemenjaraan proses dan tautan statis digunakan untuk mengisolasi waktu operasi dengan aman. Firecracker menyajikan beberapa fitur keamanan seperti model tamu sederhana — dengan kata lain, model perangkat virtual yang menyajikan area permukaan minimal yang memungkinkan fitur yang mencukupi untuk pengoperasian. Tingkat perlindungan konsentris ini memungkinkan pemanggilan cepat, sepersekian detik sembari mengisolasi mikro-VM dengan aman ke akun pelanggan. Kode sumber untuk Firecracker telah disediakan sebagai sumber terbuka bagi masyarakat luas untuk mendukung transparansi penuh dengan konfigurasi dan kemampuan operasionalnya.

Pelanggan dapat membangun praktik isolasi dan pemisahan logis yang disesuaikan dengan organisasi mereka menggunakan kemampuan seperti sumber daya tanpa server. Misalnya, pelanggan dapat membangun arsitektur yang didorong oleh peristiwa yang memiliki beberapa kasus penggunaan yang berfokus pada otomasi mulai dari respons insiden hingga pengelolaan jaringan. Lambda yang dipadukan dengan layanan AWS lainnya, seperti Amazon CloudWatch Events atau Amazon EventBridge, AWS Step Functions, Amazon GuardDuty, dan lain-lain untuk menciptakan kemampuan keamanan yang baru. Dengan layanan ini, operasi dapat dirancang untuk memulihkan masalah keamanan secara otomatis tanpa perlu campur tangan manusia. Misalnya, temuan di Amazon GuardDuty dapat dikirim ke CloudWatch Events yang kemudian dapat memicu fungsi Lambda untuk memulai aktivitas remediasi, seperti memperbarui grup keamanan, firewall aplikasi web, atau mengubah kebijakan IAM. AWS Step Functions dan fungsi Lambda lainnya dapat ditambahkan ke aliran kerja untuk logikal yang lebih kompleks, seperti AWS Systems Manager, guna mengeksekusi perintah di instans EC2 untuk menangkap atau memodifikasi konfigurasi. Konsep ini dapat digunakan untuk membangun praktik isolasi serupa yang menjauhkan akses langsung manusia dari beban kerja penting — sesuatu yang akan sangat sulit dalam lingkungan lokal tradisional. Untuk informasi lebih lanjut, lihat Panduan Respons Insiden Keamanan AWS.

Layanan perencanaan kontainer AWS, Amazon Elastic Container Service (Amazon ECS), menyediakan pemisahan keamanan dan properti isolasi sendiri apakah Anda menggunakannya untuk mengelola layanan kontainer seperti AWS Fargate atau di dalam lingkungan terkelola mandiri di EC2. Amazon ECS Task Definitions memungkinkan pelanggan untuk mendefinisikan fungsionalitas keamanan dan parameter isolasi menggunakan fitur keamanan VPC milik mereka. Satu atau beberapa kontainer dapat beroperasi dalam batasan yang ditentukan menggunakan Amazon ECS Task Definition. Pelanggan dapat menentukan aturan komunikasi kontainer secara mendetail karena setiap definisi tugas dapat menerima antarmuka jaringan elastis di VPC pelanggan. Ini memberi penampung fitur keamanan jaringan VPC yang sama seperti yang terlihat di instans EC2. Pelanggan dapat menerapkan kebijakan

IAM untuk setiap tugas yang melanjutkan akses dan batasan operasional pada setiap penampung atau kumpulan penampung. Mekanisme isolasi dan keamanan yang terkait dengan fungsi hulu seperti registri kontainer ditangani dengan Amazon Elastic Container Registry (Amazon ECR). Saat sebuah kontainer dibuat atau ditarik, perlindungan di sekitar gambar sumber tersebut sangat penting, baik saat ditempatkan maupun ditransmisikan. Amazon ECR secara otomatis mengenkripsi gambar kontainer saat tidak digunakan dan sedang transit. Dengan menggunakan kebijakan IAM, akses ke gambar di Amazon ECR dapat dibatasi hanya untuk pelaku yang memiliki kebutuhan akan akses tersebut. Saat digunakan bersama, rangkaian layanan kontainer AWS menciptakan lingkungan yang terisolasi dan aman dari ujung ke ujung untuk sejumlah kontainer atau layanan mikro.

Layanan cloud AWS menawarkan pelanggan dengan daftar kemampuan yang terus bertambah untuk membuat keamanan "di dalam cloud" kuat dan mudah diterapkan sembari mempertahankan standar keamanan yang tinggi. Layanan dan fitur keamanan yang terus berkembang meminimalkan proses yang rumit, meningkatkan kerahasiaan, dan memperluas aksesibilitas untuk mendemokratisasi keamanan serta manfaat teknik dan inovasi modern. Menerapkan praktik keamanan dasar, seperti enkripsi, dengan penerapan pelanggan yang tepat dapat secara efektif mengatasi risiko keamanan yang terkait dengan permintaan pemisahan fisik.

Memitigasi Akses Data yang Tidak Sah

Mencegah akses tidak sah membutuhkan praktik kebersihan keamanan yang tepat serta menerapkan kemampuan pencegahan dan deteksi yang kuat. Misalnya, sistem harus dirancang untuk membatasi "cakupan dampak" peristiwa keamanan sehingga node dengan akses yang tidak diotorisasi itu memiliki dampak minimal pada node lain di perusahaan. CSP berskala hiper, seperti AWS, menyediakan lingkungan dengan sarana keamanan lengkap agar pelanggan dapat mempertahankan komunikasi terenkripsi dan menerapkan perlindungan gangguan guna mengurangi risiko akses yang tidak sah. AWS tidak memiliki visibilitas ke, atau pengetahuan tentang, konten atau data di dalam akun pelanggan, termasuk apakah konten tersebut menyertakan informasi pribadi atau tidak. Pelanggan AWS diberdayakan untuk menggunakan berbagai teknik seperti enkripsi, tokenisasi, dekomposisi data, dan penipuan cyber untuk membuat konten tidak dapat dipahami oleh AWS atau pihak lain yang mengupayakan akses ke kontennya.

- **Enkripsi** — Mengenkripsi data secara benar dapat membuat data tidak dapat dibaca. Artinya, menyimpan data terenkripsi di cloud, terlepas dari lokasinya, dapat memberikan perlindungan yang memadai terhadap sebagian besar upaya eksfiltrasi. Kunci enkripsi data harus dikelola dengan hati-hati untuk memastikan tetap ada perlindungan yang kuat terhadap pihak yang menyadap. AWS menyediakan layanan yang dapat memberikan kemampuan ini di tingkat perusahaan dengan AWS CloudHSM atau AWS KMS. [8] Jumlah kontrol yang ingin dimiliki pelanggan atas metode enkripsi, penyimpanan kunci kriptografi, dan pengelolaan kunci kriptografi yang digunakan dengan data mereka ditentukan sesuai keinginan pelanggan.
- **Tokenisasi** – Tokenisasi adalah sebuah proses yang memungkinkan Anda menentukan sebuah urutan data untuk mewakili bagian informasi sensitif (misalnya, sebuah token untuk mewakili nomor kartu kredit pelanggan). Token tidak ada artinya jika digunakan sendirian dan tidak dapat dipetakan kembali ke data yang diwakilinya tanpa menggunakan sistem tokenisasi. Penyimpanan token dapat dibangun di VPC untuk menyimpan informasi sensitif dalam bentuk terenkripsi sembari membagikan token ke layanan yang disetujui untuk mengirimkan data yang dikaburkan. Selain itu, AWS memiliki sejumlah mitra yang berspesialisasi dalam menyediakan layanan tokenisasi yang terintegrasi dengan database populer dan layanan penyimpanan lainnya.
- **Dekomposisi Data** – Ini adalah sebuah proses yang mengurangi kumpulan data menjadi elemen yang tidak dapat dikenali yang tidak memiliki signifikansi sendiri.[10] Elemen atau fragmen ini kemudian disimpan dalam mode terdistribusi sehingga setiap akses yang tidak sah ke satu node hanya akan menghasilkan fragmen data yang tidak penting. Keuntungan khusus dari teknik ini adalah mengharuskan pengguna yang tidak diotorisasi untuk mengganggu semua node, mendapatkan semua fragmen, dan mengetahui algoritme (atau skema fragmentasi) guna mengumpulkan data dengan cara yang koheren.
- **Pertahanan terhadap Penipuan Cyber** – Arsitektur dan solusi penipuan cyber dapat menjadi komponen kunci untuk memitigasi peristiwa keamanan yang canggih. Solusi penipuan dapat menggunakan jebakan dan umpan yang sangat mutakhir untuk membuat pihak yang tidak diotorisasi mengira bahwa mereka telah menyusup ke sistem, padahal sesungguhnya, ia dialihkan ke sebuah lingkungan yang sangat terkontrol. Informasi tentang pihak yang tidak diotorisasi dikumpulkan untuk mengurangi ancaman di masa depan dan serangan itu dinetralkan.

AWS juga memantau pengelolaan jarak jauh yang tidak sah dan dengan cepat memutuskan atau menonaktifkan akses jarak jauh yang tidak sah setelah terdeteksi. Semua upaya akses administratif jarak jauh dicatat, dan log ditinjau, tidak hanya oleh manusia untuk aktivitas yang mencurigakan, tetapi juga oleh sistem pembelajaran mesin otomatis yang dibuat oleh tim Keamanan AWS untuk mendeteksi pola akses tidak biasa yang mungkin menunjukkan upaya tidak sah untuk mengakses data. Jika aktivitas mencurigakan terdeteksi, prosedur respons insiden dimulai. Selanjutnya, AWS telah menetapkan kebijakan dan prosedur formal untuk menggambarkan standar akses logis ke host dan infrastruktur AWS. Kebijakan juga mengidentifikasi tanggung jawab fungsional untuk administrasi keamanan dan akses logis. Kecuali dilarang oleh hukum, AWS mengharuskan semua karyawan menjalani penyelidikan latar belakang yang sesuai dengan posisi dan tingkat akses mereka. Terakhir, instans virtual pelanggan hanya dikontrol oleh pelanggan yang memiliki akses root penuh atau kontrol administratif atas akun, layanan, dan aplikasi. Personel AWS tidak memiliki kemampuan untuk masuk ke instans EC2 atau kontainer ECS/EKS pelanggan.

Tugas dan bidang tanggung jawab (misalnya, permintaan dan persetujuan akses, permintaan dan persetujuan pengelolaan perubahan) harus dipisahkan di antara berbagai individu untuk mengurangi peluang modifikasi yang tidak sah atau tidak disengaja maupun penyalahgunaan sistem AWS. Personel AWS dengan kebutuhan bisnis untuk mengakses bidang pengelolaan diharuskan agar terlebih dahulu menggunakan autentikasi multifaktor, yang berbeda dari kredensial Amazon perusahaan normal, untuk mendapatkan akses ke host administratif yang dibuat khusus.

Host administratif ini adalah sistem yang dirancang, dibangun, dikonfigurasi, dan diperkuat secara khusus untuk melindungi bidang pengelolaan. Semua akses tersebut dicatat dan diaudit. Ketika seorang karyawan tidak lagi memiliki kebutuhan bisnis untuk mengakses bidang pengelolaan, hak istimewa dan akses ke host ini dan sistem yang relevan akan dicabut. AWS telah menerapkan kebijakan penguncian sesi yang diberlakukan secara sistematis. Kunci sesi disimpan hingga prosedur identifikasi dan autentikasi yang ditetapkan telah dilakukan.

AWS memungkinkan organisasi untuk menyimpan rekaman audit yang mendukung investigasi peristiwa keamanan setelah kejadian dan kemampuan untuk memenuhi persyaratan penyimpanan informasi organisasi dan peraturan. Pelanggan dapat mengambil log dan laporan audit cloud dengan memanfaatkan CloudTrail dan CloudWatch Logs, yang kemudian dapat mereka berikan kepada otoritas yang sesuai. Solusi ini memungkinkan pelanggan AWS untuk menanggapi secara langsung permintaan penegakan hukum terhadap informasi, memungkinkan pejabat pemerintah mendapatkan informasi yang mereka butuhkan tanpa mengakses konten pelanggan yang mendasarinya. Untuk informasi tambahan tentang “pengungkapan paksa” atau penegakan hukum terhadap akses data, lihat Laporan Resmi Residensi Data AWS.

Studi Kasus

Departemen Pertahanan AS menerima pendekatan pemisahan penyimpanan logikal untuk beban kerja sensitif yang tidak diklasifikasikan

Pada bulan Desember 2011, Federal Chief Information Officer (Kepala Informasi Federal) AS membuat kebijakan pemerintah yang mengamanatkan lembaga federal menggunakan Federal Risk and Authorization Management Program (FedRAMP) — suatu program berstandar federal untuk otorisasi keamanan layanan cloud. FedRAMP menetapkan tiga dasar keamanan standar — Dampak Rendah, Sedang, dan Tinggi — berdasarkan kategorisasi Publikasi Standar Pemrosesan Informasi Federal (FIPS) 199. Dasar ini dikembangkan melalui kolaborasi para ahli keamanan cyber di seluruh industri swasta dan Pemerintah AS (termasuk Departemen Pertahanan (DoD)). Meskipun DoD menetapkan timbal balik dengan FedRAMP dasar Menengah, belum ditetapkan timbal balik dengan FedRAMP dasar Tinggi. Sebaliknya, DoD mengembangkan dan menerapkan apa yang secara efektif merupakan serangkaian persyaratan dan kontrol keamanan "FedRAMP plus" melalui Panduan Persyaratan Keamanan (SRG) Komputasi Cloud DoD.

Khususnya, DoD melalui SRG mensyaratkan pemisahan antara penyewa/misi DoD dan pemerintah Federal baik melalui cara fisik atau logikal. Lebih khusus lagi, SRG menyatakan bahwa "CSP harus memberikan bukti kontrol dan pemantauan pemisahan virtual yang kuat, dan kemampuan untuk memenuhi permintaan 'penelusuran dan penyitaan' tanpa merilis informasi dan data DoD". Lebih lanjut lagi, sistem Tingkat Dampak 5 (IL5), DoD memerlukan "pemisahan fisik (mis. infrastruktur khusus) dari penyewa non-DoD/non-Pemerintah Federal." Persyaratan DoD ini dimaksudkan untuk mengatasi masalah DoD mengenai penggabungan data DoD dengan data penyewa lain dari pengungkapan data yang tidak diinginkan dan akses tidak sah atau perusakan data DoD oleh penyewa non-DoD.

Untuk menerapkan praktik terbaik yang berfokus pada hasil, SRG mengakui penggunaan pemisahan logis sebagai pendekatan yang layak untuk memenuhi persyaratan pemisahan DoD IL5:

"CSP mungkin menawarkan solusi alternatif yang menyediakan keamanan yang setara dengan persyaratan yang disebutkan. Persetujuan akan dinilai berdasarkan kasus per kasus selama proses penilaian PA [otorisasi sementara]".

> Melalui proses penilaian dan otorisasi SRG komputasi cloud DoD (yaitu, akreditasi), AWS menunjukkan kelayakan pemisahan logikal yang *dikombinasikan dengan penyewaan khusus* untuk memenuhi maksud di balik persyaratan infrastruktur khusus yang terisolasi secara fisik untuk beban kerja yang paling sensitif dan tidak diklasifikasikan oleh DoD. (Lihat bagian sebelumnya tentang "Fitur Instans dan Host".) Pendekatan yang kami terima menegaskan bahwa lingkungan yang dipisahkan secara logikal oleh multipenyewa yang memenuhi kontrol keamanan yang kuat dapat memberikan tingkat keamanan yang lebih unggul daripada penerapan cloud pribadi khusus, sekaligus memberikan keuntungan yang signifikan dalam ketersediaan, skalabilitas, dan biaya yang lebih rendah. Teknologi cloud modern dari penyedia mapan dapat menawarkan solusi baru yang dapat memenuhi tujuan keamanan teknologi tradisional selama pendekatan akreditasi cukup fleksibel untuk mengakomodasi penerapan alternatif.

5.2.2.2 Tingkat Dampak 5, Persyaratan Pemisahan dan Lokasi

Informasi yang harus diproses dan disimpan di Tingkat Dampak 5 hanya dapat diproses di infrastruktur khusus, di lokasi atau di luar lokasi dalam model penerapan cloud apa pun yang membatasi lokasi fisik informasi seperti yang dijelaskan pada bagian 5.2.1, "Wilayah Hukum/Persyaratan Lokasi." Ini meliputi penawaran layanan publik.

Berlaku hal-hal berikut:

- Hanya cloud komunitas Pemerintah Federal, komunitas DoD, dan DoD privat yang memenuhi syarat untuk Tingkat Dampak 5.
- Setiap model penerapan dapat mendukung banyak misi atau penyewa/misi dari setiap organisasi pelanggan.

- Pemisahan virtual/logikal antara penyewa/misi DoD dan Pemerintah Federal diizinkan.
- Pemisahan virtual/logikal antara sistem penyewa/misi diwajibkan secara minimal.
- Pemisahan fisik (mis. Infrastruktur Khusus) dari penyewa non-DoD/non-Pemerintah Federal diwajibkan.

https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf

Catatan
CSP mungkin menawarkan solusi alternatif yang menyediakan keamanan yang setara dengan persyaratan yang disebutkan. Persetujuan akan dinilai berdasarkan kasus per kasus selama proses penilaian PA.

Kesimpulan

Pendekatan AWS menunjukkan bahwa lingkungan dikonfigurasi dengan benar, multipenyewa, dan dipisahkan secara logikal dapat memberikan suatu tingkat keamanan yang lebih unggul daripada penerapan cloud pribadi khusus, sekaligus memberikan keuntungan yang signifikan dalam hal ketersediaan, skalabilitas, dan biaya yang lebih rendah. Teknologi cloud modern dari penyedia mapan menawarkan solusi baru yang dapat memenuhi tujuan keamanan teknologi tradisional asalkan pendekatan akreditasi cukup fleksibel untuk mengakomodasi penerapan alternatif.

Meskipun meninjau kontrol keamanan dapat bermanfaat untuk menunjukkan kepatuhan, pengalaman telah menunjukkan bahwa organisasi yang berfokus terutama (dan dalam beberapa kasus secara eksklusif) pada penerapan kontrol tradisional dapat secara tidak sengaja membatasi akses mereka ke solusi keamanan terbaik di kelasnya. Ketika organisasi sektor publik dan swasta mengevaluasi apakah CSP memenuhi persyaratan berdasarkan konsep warisan dan arsitektur lokal, mereka harus mundur dan mengartikulasikan hasil keamanan yang diinginkan dengan jelas terlebih dahulu. Pemetaan hasil tersebut pada kemampuan CSP dan pemahaman cara menangani kebutuhan tersebut dengan tepat mengarah pada pemahaman yang lebih dalam tentang cara merancang solusi secara paling efisien serta menjelaskan risiko yang perlu diterima saat beroperasi di cloud.

Seiring program jaminan keamanan yang matang dan berskala untuk mengimbangi kecepatan cepat fitur cloud dan inovasi keamanan, detail implementasi kontrol tradisional akan menjadi semakin tidak relevan dibandingkan dengan kemampuan yang dimiliki CSP saat ini dan kemungkinan akan meningkat dengan sangat cepat. Kondisi akhir yang diinginkan – keamanan cloud yang kuat, berdasarkan kerangka kerja yang ditentukan oleh hasil keamanan pelanggan dan kemampuan keamanan yang ditentukan CSP untuk memenuhi hasil tersebut – hanya dapat muncul sebagai hasil dari dialog berkelanjutan di seluruh komunitas pemangku kepentingan jaminan cloud. AWS yakin bahwa pendekatan ini akan terus memberikan peningkatan yang signifikan dalam menjaga jaminan postur keamanan CSP.

Kontributor

Kontributor dokumen ini meliputi:

- Tim Anderson, Penasihat Senior Keamanan, Strategi Pertumbuhan, Keamanan
- Ken Beer, Manajer Umum, Kriptografi
- Min Hyun, Pimpinan Global, Strategi Pertumbuhan, Keamanan
- Mark Ryland, Direktur, Departemen CISO, Keamanan

Bacaan Lebih Lanjut

Untuk informasi tambahan, lihat:

- Laman Laporan Resmi AWS
- Laporan Resmi Residensi Data AWS
- Panduan Respons Insiden Keamanan AWS

Revisi Dokumen

Untuk mendapatkan pemberitahuan tentang pembaruan laporan resmi ini, silakan berlangganan RSS feed.

perubahan-riwayat-pembaruan	deskripsi-riwayat-pembaruan	tanggal-riwayat-pembaruan
Publikasi awal (hal. 19)	Terbitan pertama.	28 Juli 2020

Pemberitahuan

Pelanggan bertanggung jawab untuk melakukan penilaian independen mereka terhadap informasi dalam dokumen ini. Dokumen ini: (a) adalah untuk tujuan informasi saja, (b) merupakan praktik dan penawaran produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak memberikan komitmen atau jaminan apa pun dari AWS dan afiliasi, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa garansi, representasi, atau kondisi apa pun, baik secara tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggan dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.