AWS Panduan keputusan

Memilih AWS layanan keamanan, identitas, dan tata kelola

Memilih AWS layanan keamanan, identitas, dan tata kelola: AWS Panduan keputusan

Table of Contents

Memilih AWS layanan keamanan, identitas, dan tata kelola

Mengambil langkah pertama

Waktunya membaca	27 menit	
Tujuan	Membantu Anda menentukan layanan AWS keamanan, identitas, dan tata kelola mana yang paling cocok untuk organisasi Anda.	
Terakhir diperbarui	Desember 30, 2024	
Layanan yang tercakup	• AWS Artifact • AWS Audit Manager • AWS Certificate Manager • AWS CloudHSM • AWS CloudTrail • Amazon Cognito • AWS Config • AWS Control Tower • Amazon Detective • AWS Firewall Manager • Amazon GuardDuty • AWS IAM • AWS IAM Identity Center • Amazon Inspector	• AWS KMS • Amazon Macie • AWS Network Firewall • AWS Organizations • AWS Payment Cryptography • AWS Private CA • AWS RAM • AWS Secrets Manager • AWS Security Hub CSPM • Amazon Security Lake • AWS Respon Insiden Keamanan • AWS Shield • AWS WAF

Pengantar

Keamanan, identitas, dan tata kelola di cloud adalah komponen penting bagi Anda dalam mencapai dan menjaga integritas dan keamanan data dan layanan Anda. Ini sangat relevan karena lebih banyak bisnis bermigrasi ke penyedia cloud seperti Amazon Web Services (AWS).

Panduan ini membantu Anda memilih layanan dan alat AWS keamanan, identitas, dan tata kelola yang paling sesuai dengan kebutuhan dan organisasi Anda.

Pertama, mari kita jelajahi apa yang kita maksud dengan keamanan, identitas, dan tata kelola:

- Keamanan cloud mengacu pada penggunaan tindakan dan praktik untuk melindungi aset digital dari ancaman. Ini termasuk keamanan fisik pusat data dan langkah-langkah keamanan siber untuk menjaga terhadap ancaman online. AWS memprioritaskan keamanan melalui penyimpanan data terenkripsi, keamanan jaringan, dan pemantauan berkelanjutan terhadap potensi ancaman.
- Layanan identitas membantu Anda mengelola identitas, sumber daya, dan izin dengan aman dengan cara yang dapat diskalakan. AWS menyediakan layanan identitas yang dirancang untuk tenaga kerja dan aplikasi yang dihadapi pelanggan, dan untuk mengelola akses ke beban kerja dan aplikasi Anda.
- Tata kelola cloud adalah seperangkat aturan, proses, dan laporan yang memandu organisasi Anda untuk mengikuti praktik terbaik. Anda dapat membuat tata kelola cloud di seluruh AWS sumber daya Anda, menggunakan praktik dan standar terbaik bawaan, serta mengotomatiskan proses kepatuhan dan audit. Kepatuhan di cloud mengacu pada kepatuhan terhadap hukum dan peraturan yang mengatur perlindungan data dan privasi. AWS Program Kepatuhan memberikan informasi tentang sertifikasi, peraturan, dan kerangka kerja yang AWS selaras dengannya.

Video one-and-a-half menit ini merangkum bagaimana AWS membangun keamanan yang kuat di inti kami.

Memahami AWS layanan keamanan, identitas, dan tata kelola

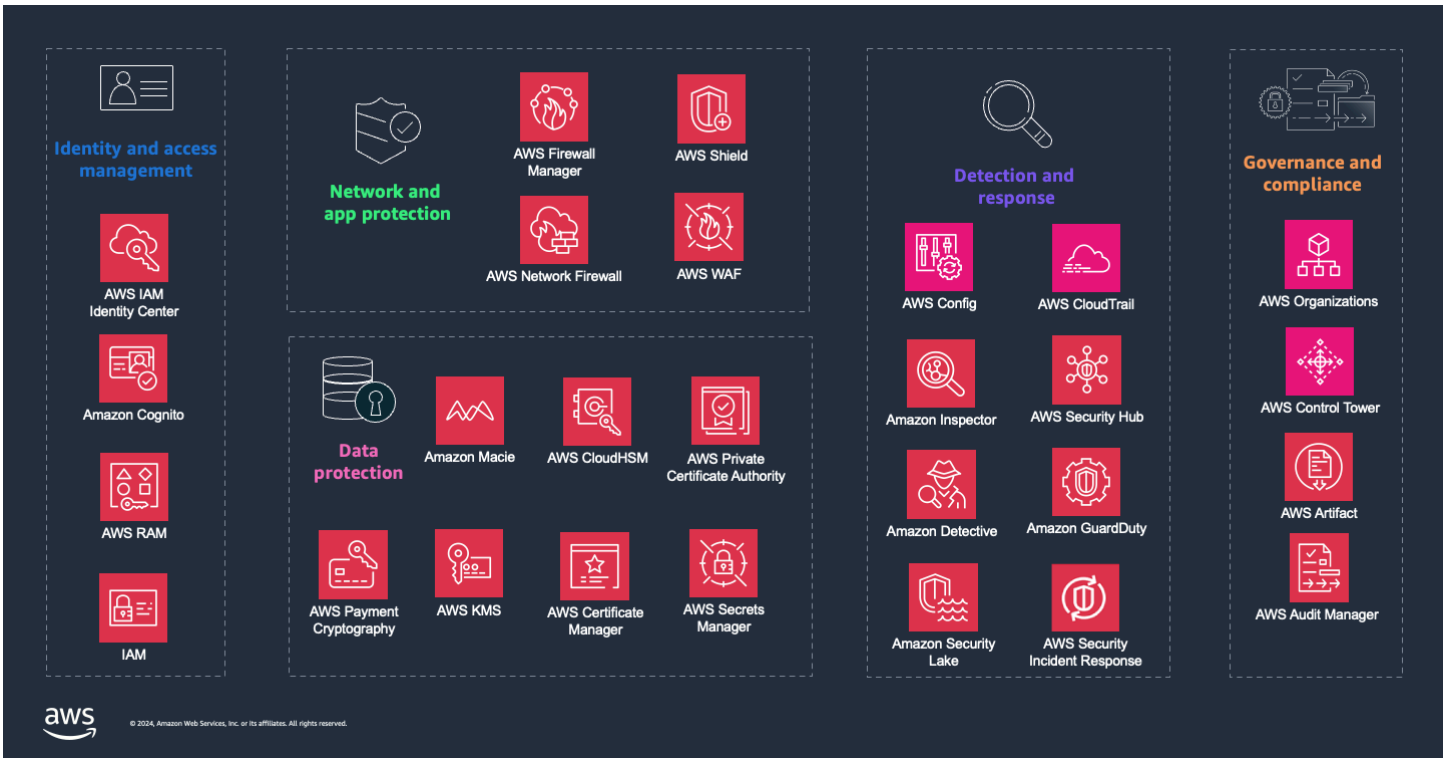
Keamanan dan kepatuhan adalah tanggung jawab bersama

Sebelum memilih layanan AWS keamanan, identitas, dan tata kelola Anda, penting bagi Anda untuk memahami bahwa keamanan dan kepatuhan adalah tanggung jawab bersama antara Anda dan AWS.

Sifat tanggung jawab bersama ini membantu meringankan beban operasional Anda, dan ini memberi Anda fleksibilitas dan kontrol atas penyebaran Anda. Diferensiasi tanggung jawab ini sering disebut sebagai keamanan “dari” cloud dan keamanan “di” cloud.

Dengan pemahaman tentang model ini, Anda dapat memahami berbagai opsi yang tersedia untuk Anda, dan bagaimana yang berlaku Layanan AWS cocok bersama.

Anda dapat menggabungkan AWS alat dan layanan untuk membantu menjaga beban kerja Anda



Seperti yang ditunjukkan pada diagram sebelumnya, AWS menawarkan alat dan layanan di lima domain untuk membantu Anda mencapai dan mempertahankan keamanan, manajemen identitas, dan tata kelola yang kuat di cloud. Anda dapat menggunakan Layanan AWS di lima domain ini untuk membantu Anda melakukan hal berikut:

- Bentuk pendekatan berlapis-lapis untuk menjaga data dan lingkungan Anda
- Bentengi infrastruktur cloud Anda dari ancaman yang terus berkembang
- Patuhi standar peraturan yang ketat

Untuk mempelajari lebih lanjut tentang AWS keamanan, termasuk dokumentasi keamanan Layanan AWS, lihat Dokumentasi AWS Keamanan.

Pada bagian berikut, kami memeriksa setiap domain lebih lanjut.

Memahami AWS identitas dan layanan manajemen akses

Di pusat AWS keamanan adalah prinsip hak istimewa paling sedikit: individu dan layanan hanya memiliki akses yang mereka butuhkan. AWS IAM Identity Centeradalah direkomendasikan Layanan

AWS untuk mengelola akses pengguna ke AWS sumber daya. Anda dapat menggunakan layanan ini untuk mengelola akses ke akun dan izin Anda dalam akun tersebut, termasuk identitas dari penyedia identitas eksternal.

Tabel berikut merangkum identitas dan penawaran manajemen akses yang dibahas dalam panduan ini:

AWS IAM Identity Center

AWS IAM Identity Centermembantu Anda menghubungkan sumber identitas Anda, atau membuat pengguna. Anda dapat mengelola akses tenaga kerja secara terpusat ke beberapa Akun AWS dan aplikasi.

Amazon Cognito

Amazon Cognito menyediakan alat identitas untuk aplikasi web dan seluler untuk mengautentikasi dan mengotorisasi pengguna dari direktori pengguna bawaan, direktori perusahaan Anda, dan penyedia identitas konsumen.

AWS RAM

AWS RAMmembantu Anda berbagi sumber daya dengan aman di seluruh Akun AWS, di dalam organisasi Anda, dan dengan peran dan pengguna IAM.

IAM

IAM memungkinkan kontrol yang aman dan halus atas akses ke sumber daya beban kerja. AWS

Memahami layanan perlindungan AWS data

Perlindungan data sangat penting di cloud, dan AWS menyediakan layanan yang membantu Anda melindungi data, akun, dan beban kerja Anda. Misalnya, mengenkripsi data Anda baik dalam perjalanan maupun saat istirahat membantu melindunginya dari paparan. Dengan AWS Key Management Service(AWS KMS) dan AWS CloudHSMAnda dapat membuat dan mengontrol kunci kriptografi yang Anda gunakan untuk melindungi data Anda.

Tabel berikut merangkum penawaran perlindungan data yang dibahas dalam panduan ini:

Amazon Macie

Amazon Macie menemukan data sensitif dengan menggunakan pembelajaran mesin dan pencocokan pola, dan memungkinkan perlindungan otomatis terhadap risiko terkait.

AWS KMS

AWS KMSmembuat dan mengontrol kunci kriptografi yang Anda gunakan untuk melindungi data Anda.

AWS CloudHSM

AWS CloudHSMmenyediakan modul keamanan perangkat keras berbasis cloud yang sangat tersedia ()HSMs.

AWS Certificate Manager

AWS Certificate Managermenangani kompleksitas pembuatan, penyimpanan, dan pembaruan sertifikat dan kunci SSL/TLS X.509 publik dan pribadi.

AWS Private CA

AWS Private CAmembantu Anda membuat hierarki otoritas sertifikat pribadi, termasuk otoritas sertifikat root dan bawahan ()CAs.

AWS Secrets Manager

AWS Secrets Managermembantu Anda mengelola, mengambil, dan memutar kredensyal basis data, kredensyal aplikasi, OAuth token, kunci API, dan rahasia lainnya.

AWS Payment Cryptography

AWS Payment Cryptographymenyediakan akses ke fungsi kriptografi dan manajemen kunci yang digunakan dalam pemrosesan pembayaran sesuai dengan standar industri kartu pembayaran (PCI).

Memahami layanan perlindungan AWS jaringan dan aplikasi

AWS menawarkan beberapa layanan untuk melindungi jaringan dan aplikasi Anda. AWS Shieldmemberi Anda perlindungan terhadap serangan Distributed Denial of Service (DDoS), dan AWS WAFmembantu Anda melindungi aplikasi web dari serangan eksploitasi web umum.

Tabel berikut merangkum penawaran perlindungan jaringan dan aplikasi yang dibahas dalam panduan ini:

AWS Firewall Manager

AWS Firewall Managermenyederhanakan tugas administrasi dan pemeliharaan Anda di beberapa akun dan sumber daya untuk perlindungan.

AWS Network Firewall

AWS Network Firewallmenyediakan firewall jaringan stateful dan terkelola serta layanan deteksi dan pencegahan intrusi dengan VPC Anda.

AWS Shield

AWS Shieldmemberikan perlindungan terhadap serangan DDo S untuk AWS sumber daya di jaringan, transportasi, dan lapisan aplikasi.

AWS WAF

AWS WAFmenyediakan firewall aplikasi web sehingga Anda dapat memantau permintaan HTTP (S) yang diteruskan ke sumber daya aplikasi web Anda yang dilindungi.

Memahami layanan AWS deteksi dan respons

AWS menyediakan alat untuk membantu Anda merampingkan operasi keamanan di seluruh AWS lingkungan Anda, termasuk lingkungan multi-akun. Misalnya, Anda dapat menggunakan Amazon GuardDuty untuk deteksi ancaman cerdas, dan Anda dapat menggunakan Amazon Detective untuk mengidentifikasi dan menganalisis temuan keamanan dengan mengumpulkan data log. AWS Security Hub CSPMmendukung beberapa standar keamanan dan memberikan gambaran umum tentang peringatan keamanan dan status kepatuhan di seluruh Akun AWS. AWS CloudTrailmelacak aktivitas pengguna dan penggunaan antarmuka pemrograman aplikasi (API), yang sangat penting untuk memahami dan menanggapi peristiwa keamanan.

Tabel berikut merangkum penawaran deteksi dan respons yang dibahas dalam panduan ini:

AWS Config

AWS Configmemberikan tampilan rinci tentang konfigurasi AWS sumber daya di Anda Akun AWS.

AWS CloudTrail

AWS CloudTrailmencatat tindakan yang diambil oleh pengguna, peran, atau Layanan AWS.

AWS Security Hub CSPM

AWS Security Hub CSPMmemberikan pandangan komprehensif tentang keadaan keamanan Anda di AWS.

Amazon GuardDuty

Amazon GuardDuty terus memantau Anda Akun AWS, beban kerja, aktivitas runtime, dan data untuk aktivitas berbahaya.

Amazon Inspector

Amazon Inspector memindai AWS beban kerja Anda untuk mencari kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan.

Amazon Security Lake

Amazon Security Lake secara otomatis memusatkan data keamanan dari AWS lingkungan, penyedia SaaS, lingkungan lokal, sumber cloud, dan sumber pihak ketiga ke dalam data lake.

Amazon Detective

Amazon Detective membantu Anda menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan atau aktivitas mencurigakan dengan cepat.

AWS Security Incident Response

AWS Respon Insiden Keamanan

Membantu Anda dengan cepat mempersiapkan, menanggapi, dan menerima panduan untuk membantu memulihkan diri dari insiden keamanan.

Memahami AWS tata kelola dan layanan kepatuhan

AWS menyediakan alat yang membantu Anda mematuhi standar keamanan, operasional, kepatuhan, dan biaya Anda. Misalnya, Anda dapat menggunakan AWS Control Toweruntuk mengatur dan mengatur lingkungan multi-akun dengan kontrol preskriptif. Dengan AWS Organizations, Anda dapat mengatur manajemen berbasis kebijakan untuk beberapa akun dalam organisasi Anda.

AWS juga memberi Anda pandangan komprehensif tentang status kepatuhan Anda dan terus memantau lingkungan Anda dengan menggunakan pemeriksaan kepatuhan otomatis berdasarkan praktik AWS terbaik dan standar industri yang diikuti organisasi Anda. Misalnya, AWS Artifactmenyediakan akses sesuai permintaan ke laporan kepatuhan, dan AWS Audit Managermengotomatiskan pengumpulan bukti sehingga Anda dapat lebih mudah menilai apakah kontrol Anda beroperasi secara efektif.

Tabel berikut merangkum penawaran tata kelola dan kepatuhan yang dibahas dalam panduan ini:

AWS Organizations

AWS Organizationsmembantu Anda mengkonsolidasikan beberapa Akun AWS ke dalam organisasi yang Anda buat dan kelola secara terpusat.

AWS Control Tower

AWS Control Towermembantu Anda mengatur dan mengatur lingkungan AWS multi-akun yang didasarkan pada praktik terbaik.

AWS Artifact

AWS Artifactmenyediakan unduhan dokumen AWS keamanan dan kepatuhan sesuai permintaan.

AWS Audit Manager

AWS Audit Manager

Membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda menilai risiko dan kepatuhan.

Pertimbangkan AWS kriteria keamanan, identitas, dan tata kelola

Memilih layanan keamanan, identitas, dan tata kelola yang tepat AWS bergantung pada persyaratan dan kasus penggunaan spesifik Anda. Memutuskan untuk mengadopsi layanan AWS keamanan menyediakan pohon keputusan untuk membantu Anda memutuskan apakah mengadopsi Layanan AWS untuk keamanan, identitas, dan tata kelola cocok untuk organisasi Anda. Selain itu, berikut adalah beberapa kriteria yang perlu dipertimbangkan saat membuat keputusan tentang layanan mana yang akan digunakan.

Security requirements and threat landscape

Lakukan penilaian komprehensif terhadap kerentanan dan ancaman spesifik organisasi Anda. Ini melibatkan identifikasi jenis data yang Anda tangani, seperti informasi pelanggan pribadi, catatan keuangan, atau data bisnis kepemilikan. Memahami potensi risiko yang terkait dengan masing-masing.

Nilai arsitektur aplikasi dan infrastruktur Anda. Tentukan apakah aplikasi Anda menghadap publik dan jenis lalu lintas web apa yang mereka tangani. Faktor ini menjadi kebutuhan Anda akan layanan seperti AWS WAF untuk melindungi terhadap eksploitasi web. Untuk aplikasi internal, pertimbangkan pentingnya deteksi ancaman internal dan pemantauan berkelanjutan dengan Amazon GuardDuty, yang dapat mengidentifikasi pola akses yang tidak biasa atau penerapan yang tidak sah.

Terakhir, pertimbangkan kecanggihan postur keamanan Anda yang ada dan keahlian tim keamanan Anda. Jika tim Anda memiliki sumber daya terbatas, memilih layanan yang

menawarkan lebih banyak otomatisasi dan integrasi dapat memberi Anda peningkatan keamanan yang efektif, tanpa membebani tim Anda. Contoh layanan termasuk AWS Shield untuk perlindungan DDo S dan AWS Security Hub CSPM untuk pemantauan keamanan terpusat.

Compliance and regulatory requirements

Identifikasi undang-undang dan standar yang relevan untuk industri atau wilayah geografis Anda, seperti Peraturan Perlindungan Data Umum (GDPR), Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan AS tahun 1996 (HIPAA), atau Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS).

AWS menawarkan layanan seperti AWS Config dan AWS Artifact untuk membantu Anda mengelola kepatuhan dengan berbagai standar. Dengan AWS Config, Anda dapat menilai, mengaudit, dan mengevaluasi konfigurasi sumber AWS daya Anda, sehingga memudahkan Anda untuk memastikan kepatuhan terhadap kebijakan internal dan persyaratan peraturan. AWS Artifact menyediakan akses sesuai permintaan ke dokumentasi AWS kepatuhan, membantu Anda dengan audit dan pelaporan kepatuhan.

Memilih layanan yang sesuai dengan kebutuhan kepatuhan spesifik Anda dapat membantu organisasi Anda memenuhi persyaratan hukum dan membangun lingkungan yang aman dan dapat dipercaya untuk data Anda. Jelajahi Program AWS Kepatuhan untuk mempelajari lebih lanjut.

Scalability and flexibility

Pertimbangkan bagaimana organisasi Anda akan tumbuh, dan seberapa cepat. Pilih Layanan AWS yang akan membantu langkah-langkah keamanan Anda tumbuh mulus dengan infrastruktur Anda dan beradaptasi dengan ancaman yang berkembang.

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

AWS Juga merancang banyak layanan untuk secara otomatis menskalakan dengan lalu lintas aplikasi dan pola penggunaan, seperti Amazon GuardDuty untuk deteksi ancaman dan AWS WAF untuk melindungi aplikasi web. Saat bisnis Anda meningkat, layanan ini berskala dengannya, tanpa memerlukan penyesuaian manual atau menyebabkan kemacetan.

Selain itu, sangat penting bagi Anda untuk dapat menyesuaikan kontrol keamanan agar sesuai dengan persyaratan bisnis dan lanskap ancaman Anda. Pertimbangkan untuk mengelola

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

Mempertimbangkan skalabilitas dan fleksibilitas membantu Anda memastikan bahwa postur keamanan Anda kuat, responsif, dan mampu mendukung lingkungan bisnis yang dinamis.

Integration with existing systems

Pertimbangkan langkah-langkah keamanan yang meningkatkan, bukan mengganggu, operasi Anda saat ini. Misalnya, pertimbangkan hal berikut:

- Rampingkan alur kerja Anda dengan menggabungkan data keamanan dan peringatan dari dan menganalisisnya bersama sistem informasi keamanan Layanan AWS dan manajemen peristiwa (SIEM) yang ada.
- Buat tampilan terpadu tentang ancaman dan kerentanan keamanan di lingkungan baik AWS maupun lokal.
- Integrasikan AWS CloudTrail dengan solusi manajemen log yang ada untuk pemantauan komprehensif aktivitas pengguna dan penggunaan API di seluruh AWS infrastruktur dan aplikasi yang ada.
- Periksa cara-cara agar Anda dapat mengoptimalkan pemanfaatan sumber daya dan menerapkan kebijakan keamanan secara konsisten di seluruh lingkungan. Ini membantu Anda mengurangi risiko kesenjangan dalam cakupan keamanan.

Cost and budget considerations

Tinjau model harga untuk setiap layanan yang Anda pertimbangkan. AWS sering mengenakan biaya berdasarkan penggunaan, seperti jumlah panggilan API, volume data yang diproses, atau jumlah data yang disimpan. Misalnya, Amazon GuardDuty mengenakan biaya berdasarkan jumlah data log yang dianalisis untuk deteksi ancaman, sementara AWS WAF tagihan didasarkan pada jumlah aturan yang diterapkan dan jumlah permintaan web yang diterima.

Perkirakan penggunaan yang Anda harapkan untuk memperkirakan biaya secara akurat. Pertimbangkan kebutuhan saat ini dan potensi pertumbuhan atau lonjakan permintaan. Misalnya, skalabilitas adalah fitur utama Layanan AWS, tetapi juga dapat menyebabkan peningkatan biaya jika tidak dikelola dengan hati-hati. Gunakan AWS Kalkulator Hargauntuk memodelkan skenario yang berbeda dan menilai dampak keuangannya.

Mengevaluasi total biaya kepemilikan (TCO), yang mencakup biaya langsung dan biaya tidak langsung, seperti waktu dan sumber daya yang dibutuhkan untuk manajemen dan pemeliharaan. Memilih layanan terkelola dapat mengurangi overhead operasional, tetapi mungkin datang pada titik harga yang lebih tinggi.

Terakhir, prioritaskan investasi keamanan Anda berdasarkan penilaian risiko. Tidak semua layanan keamanan akan sama pentingnya dengan infrastruktur Anda, jadi fokuskan anggaran Anda pada area yang akan memiliki dampak paling signifikan dalam mengurangi risiko dan memastikan kepatuhan. Menyeimbangkan efektivitas biaya dengan tingkat keamanan yang Anda butuhkan adalah kunci keberhasilan AWS strategi keamanan.

Organizational structure and access needs

Evaluasi bagaimana organisasi Anda terstruktur dan beroperasi, dan bagaimana kebutuhan akses Anda mungkin berbeda menurut tim, proyek, atau lokasi. Ini menjadi faktor dalam cara Anda mengelola dan mengautentikasi identitas pengguna, menetapkan peran, dan menerapkan kontrol akses di seluruh lingkungan Anda. AWS Menerapkan praktik terbaik, seperti menerapkan izin hak istimewa paling rendah dan memerlukan otentikasi multi-faktor (MFA).

Sebagian besar organisasi membutuhkan lingkungan multi-akun. Tinjau praktik terbaik untuk jenis lingkungan ini, dan pertimbangkan AWS Control Tower untuk menggunakan AWS Organizations dan membantu Anda menerapkannya.

Aspek lain yang harus Anda pertimbangkan adalah pengelolaan kredensyal dan kunci akses. Pertimbangkan untuk menggunakan IAM Identity Center untuk memusatkan manajemen akses di beberapa Akun AWS aplikasi bisnis, yang meningkatkan keamanan dan kenyamanan pengguna. Untuk membantu Anda mengelola akses dengan lancar di seluruh akun organisasi Anda, IAM Identity Center terintegrasi dengan. AWS Organizations

Selain itu, evaluasi bagaimana identitas dan layanan manajemen akses ini terintegrasi dengan layanan direktori yang ada. Jika Anda memiliki penyedia identitas yang sudah ada, Anda dapat mengintegrasikannya dengan IAM Identity Center dengan menggunakan SAMP 2.0 atau OpenID Connect (OIDC). IAM Identity Center juga memiliki dukungan untuk penyediaan System for Cross-domain Identity Management (SCIM) untuk membantu menjaga direktori Anda tetap disinkronkan. Ini membantu Anda memastikan pengalaman pengguna yang mulus dan aman saat mengakses sumber daya. AWS

Pilih layanan AWS keamanan, identitas, dan tata kelola

Sekarang setelah Anda mengetahui kriteria untuk mengevaluasi opsi keamanan Anda, Anda siap untuk memilih layanan AWS keamanan mana yang cocok untuk kebutuhan organisasi Anda.

Tabel berikut menyoroti layanan mana yang dioptimalkan untuk keadaan apa. Gunakan tabel untuk membantu menentukan layanan yang paling cocok untuk organisasi dan kasus penggunaan Anda.

> **Note**
>
> [1] Terintegrasi dengan AWS Security Hub CSPM (daftar lengkap)
> [2] Terintegrasi dengan Amazon GuardDuty (daftar lengkap)
> [3] Terintegrasi dengan Amazon Security Lake (daftar lengkap)

Pilih layanan manajemen AWS identitas dan akses

Berikan individu yang sesuai tingkat akses yang sesuai ke sistem, aplikasi, dan data.

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan keamanan, identitas, dan tata kelola
Gunakan layanan ini untuk membantu Anda mengelola dan mengatur akses dengan aman bagi pelanggan, tenaga kerja, dan beban kerja Anda.	Membantu Anda menghubungkan sumber identitas Anda, atau membuat pengguna. Anda dapat mengelola akses tenaga kerja secara terpusat ke beberapa AWS akun dan aplikasi.	AWS IAM Identity Center
	Dioptimalkan untuk mengautentikasi dan mengotorisasi pengguna untuk aplikasi web dan seluler.	Amazon Cognito
	Dioptimalkan untuk berbagi sumber daya dengan aman di dalamnya AWS.	AWS RAM

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan keamanan, identitas, dan tata kelola
	Memungkinkan kontrol yang aman dan halus atas akses ke AWS sumber daya beban kerja.	IAM 1

Pilih layanan perlindungan AWS data

Mengotomatiskan dan menyederhanakan tugas perlindungan dan keamanan data yang berkisar dari manajemen kunci dan penemuan data sensitif hingga manajemen kredensyal.

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan perlindungan data
Gunakan layanan ini untuk membantu Anda mencapai dan menjaga kerahasiaan, integritas, dan ketersediaan data sensitif yang disimpan dan diproses dalam lingkungan AWS .	Dioptimalkan untuk menemukan data sensitif.	Amazon Macie 1
	Dioptimalkan untuk kunci kriptografi.	AWS KMS
	Dioptimalkan untuk HSMs.	AWS CloudHSM
	Dioptimalkan untuk sertifikat dan SSL/TLS kunci X.509 pribadi.	AWS Certificate Manager
	Dioptimalkan untuk membuat hierarki otoritas sertifikat pribadi.	AWS Private CA
	Dioptimalkan untuk kredensyal database, kredensyal aplikasi, OAuth token, kunci API, dan rahasia lainnya.	AWS Secrets Manager

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan perlindungan data
	Dioptimalkan untuk menyediakan akses ke fungsi kriptografi dan manajemen kunci yang digunakan dalam pemrosesan pembayaran sesuai dengan standar PCI.	AWS Payment Cryptography

Pilih layanan perlindungan AWS jaringan dan aplikasi

Lindungi sumber daya internet Anda secara terpusat dari serangan DDo S dan aplikasi umum.

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan perlindungan jaringan dan aplikasi
Gunakan layanan ini untuk membantu Anda menegakkan kebijakan keamanan terperinci di setiap titik kontrol jaringan.	Dioptimalkan untuk mengonfigurasi dan mengelola aturan firewall secara terpusat.	AWS Firewall Manager[1]
	Dioptimalkan untuk menyediakan firewall jaringan stateful dan terkelola serta layanan deteksi dan pencegahan intrusi.	AWS Network Firewall
	Dioptimalkan untuk melindungi terhadap serangan DDo S untuk AWS sumber daya di jaringan, transportasi, dan lapisan aplikasi.	AWS Shield
	Dioptimalkan untuk menyediakan firewall aplikasi web.	AWS WAF

Pilih layanan AWS deteksi dan respons

Terus mengidentifikasi dan memprioritaskan risiko keamanan, sambil mengintegrasikan praktik terbaik keamanan sejak dini.

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan deteksi dan respons
Gunakan layanan ini untuk membantu Anda mendeteksi dan merespons risiko keamanan di seluruh akun Anda, sehingga Anda dapat melindungi beban kerja Anda dalam skala besar.	Dioptimalkan untuk mengotomatiskan pemeriksaan keamanan dan memusatkan peringatan keamanan dengan AWS dan integrasi pihak ketiga.	AWS Security Hub CSPM[2, 3]
	Dioptimalkan untuk menilai, mengaudit, dan mengevaluasi konfigurasi sumber daya Anda.	AWS Config[1]
	Dioptimalkan untuk mencatat peristiwa dari yang lain Layanan AWS sebagai jejak audit.	AWS CloudTrail
	Dioptimalkan untuk deteksi ancaman cerdas dan pelaporan terperinci.	Amazon GuardDuty [1]
	Dioptimalkan untuk manajemen kerentanan.	Amazon Inspector 1
	Dioptimalkan untuk memusatkan data keamanan.	Danau Keamanan Amazon [1]
	Dioptimalkan untuk menggabungkan dan	Detektif Amazon [1, 2, 3]

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan deteksi dan respons
	meringkas potensi masalah keamanan.	
	Dioptimalkan untuk membantu Anda melakukan triase temuan, meningkatkan peristiwa keamanan, dan mengelola kasus yang memerlukan perhatian segera Anda.	AWS Respon Insiden Keamanan

Pilih layanan AWS tata kelola dan kepatuhan

Tetapkan tata kelola cloud di seluruh sumber daya Anda, dan otomatiskan kepatuhan dan proses audit Anda.

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan tata kelola dan kepatuhan
Gunakan layanan ini untuk membantu Anda menerapkan praktik terbaik dan memenuhi standar industri saat menggunakan AWS.	Dioptimalkan untuk mengelola beberapa akun secara terpusat dan penagihan konsolidasi.	AWS Organizations
	Dioptimalkan untuk menyediakan unduhan dokumen AWS keamanan dan kepatuhan sesuai permintaan.	AWS Artifact
	Dioptimalkan untuk AWS penggunaan audit.	AWS Audit Manager[1]

Kapan sebaiknya Anda menggunakannya?	Untuk apa itu dioptimalkan?	Layanan tata kelola dan kepatuhan
	Dioptimalkan untuk menyiapkan dan mengatur lingkungan AWS multi-akun.	AWS Control Tower

Gunakan AWS layanan keamanan, identitas, dan tata kelola

Anda sekarang harus memiliki pemahaman yang jelas tentang apa yang dilakukan oleh setiap layanan AWS keamanan, identitas, dan tata kelola (dan AWS alat dan layanan pendukung), dan mana yang mungkin tepat untuk Anda.

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

Gunakan layanan manajemen AWS identitas dan akses

Tabel berikut menunjukkan beberapa identitas yang berguna dan sumber daya manajemen akses, yang diatur oleh layanan, untuk membantu Anda memulai.

AWS IAM Identity Center

- Mengaktifkan Pusat AWS Identitas IAM

  Aktifkan IAM Identity Center dan mulai menggunakannya dengan Anda AWS Organizations.

  Jelajahi panduannya
- Konfigurasikan akses pengguna dengan direktori IAM Identity Center default

  Gunakan direktori default sebagai sumber identitas Anda dan atur serta uji akses pengguna.

  Memulai dengan tutorial
- Menggunakan Active Directory sebagai sumber identitas

Selesaikan pengaturan dasar untuk menggunakan Active Directory sebagai sumber identitas IAM Identity Center.

Memulai dengan tutorial

- Konfigurasikan SAFL dan SCIM dengan Okta dan IAM Identity Center

  Siapkan koneksi SAMB dengan Okta dan IAM Identity Center.

  Memulai dengan tutorial

Amazon Cognito

- Memulai dengan Amazon Cognito

  Pelajari tentang tugas Amazon Cognito yang paling umum.

  Jelajahi panduannya
- Tutorial: Membuat kumpulan pengguna

  Buat kumpulan pengguna, yang memungkinkan pengguna Anda masuk ke web atau aplikasi seluler Anda.

  Memulai dengan tutorial
- Tutorial: Membuat kolam identitas

  Buat kumpulan identitas, yang memungkinkan pengguna Anda memperoleh AWS kredensyal sementara untuk diakses. Layanan AWS

  Memulai dengan tutorial
- Lokakarya Amazon Cognito

  Berlatih menggunakan Amazon Cognito untuk membangun solusi otentikasi untuk toko hewan peliharaan hipotetis.

  Memulai dengan tutorial

AWS RAM

- Memulai dengan AWS RAM

Pelajari tentang AWS RAM istilah dan konsep.

Jelajahi panduannya

- Bekerja dengan AWS sumber daya bersama

  Bagikan AWS sumber daya yang Anda miliki, dan akses AWS sumber daya yang dibagikan dengan Anda.

  Jelajahi panduannya

- Mengelola izin dalam RAM AWS

  Pelajari tentang dua jenis izin terkelola: izin AWS terkelola dan izin terkelola pelanggan.

  Jelajahi panduannya

- Konfigurasikan akses terperinci ke sumber daya Anda yang dibagikan menggunakan AWS RAM

  Gunakan izin yang dikelola pelanggan untuk menyesuaikan akses sumber daya Anda dan mencapai praktik terbaik dengan hak istimewa paling sedikit.

  Baca blognya

IAM

- Memulai dengan IAM

  Buat peran, pengguna, dan kebijakan IAM menggunakan. Konsol Manajemen AWS

  Memulai dengan tutorial

- Mendelegasikan akses di seluruh Akun AWS menggunakan peran

  Gunakan peran untuk mendelegasikan akses ke sumber daya yang berbeda Akun AWS yang Anda miliki disebut Produksi dan Pengembangan.

  Memulai dengan tutorial

- Buat kebijakan terkelola pelanggan

  Gunakan Konsol Manajemen AWS untuk membuat kebijakan yang dikelola pelanggan dan kemudian lampirkan kebijakan itu ke pengguna IAM di Anda Akun AWS.

Memulai dengan tutorial

- Tentukan izin untuk mengakses AWS sumber daya berdasarkan tag

  Buat dan uji kebijakan yang memungkinkan peran IAM dengan tag utama untuk mengakses sumber daya dengan tag yang cocok.

  Memulai dengan tutorial
- Praktik terbaik keamanan di IAM

  Bantu mengamankan AWS sumber daya Anda dengan menggunakan praktik terbaik IAM.

  Jelajahi panduannya

Gunakan layanan perlindungan AWS data

Bagian berikut memberi Anda tautan ke sumber daya terperinci yang menjelaskan perlindungan AWS data.

Macie

- Memulai dengan Amazon Macie

  Aktifkan Macie untuk Anda Akun AWS, nilai postur keamanan Amazon S3 Anda, dan konfigurasikan setelan kunci dan sumber daya untuk menemukan dan melaporkan data sensitif di bucket S3 Anda.

  Jelajahi panduannya
- Memantau keamanan dan privasi data dengan Amazon Macie

  Gunakan Amazon Macie untuk memantau keamanan data Amazon S3 dan menilai postur keamanan Anda.

  Jelajahi panduannya
- Menganalisis temuan Amazon Macie

  Tinjau, analisis, dan kelola temuan Amazon Macie.

  Jelajahi panduannya
- Mengambil sampel data sensitif dengan temuan Amazon Macie

Gunakan Amazon Macie untuk mengambil dan mengungkapkan sampel data sensitif yang dilaporkan oleh temuan individu.

Jelajahi panduannya

- Menemukan data sensitif dengan Amazon Macie

  Otomatiskan penemuan, pencatatan, dan pelaporan data sensitif di estat data Amazon S3 Anda.

  Jelajahi panduannya

AWS KMS

- Memulai dengan AWS KMS

  Kelola kunci KMS enkripsi simetris, dari pembuatan hingga penghapusan.

  Jelajahi panduannya
- Kunci tujuan khusus

  Pelajari tentang berbagai jenis kunci yang AWS KMS mendukung, selain kunci KMS enkripsi simetris.

  Jelajahi panduannya
- Menskalakan enkripsi Anda pada kemampuan istirahat dengan AWS KMS

  Pelajari tentang opsi enkripsi saat istirahat yang tersedia di dalamnya AWS.

  Jelajahi lokakarya

AWS CloudHSM

- Memulai dengan AWS CloudHSM

  Buat, inisialisasi, dan aktifkan AWS CloudHSM cluster.

  Jelajahi panduannya
- Mengelola AWS CloudHSM cluster

Connect ke AWS CloudHSM cluster Anda dan berbagai tugas administratif dalam mengelola klaster Anda.

Jelajahi panduannya

- Mengelola pengguna dan kunci HSM di AWS CloudHSM

  Buat pengguna dan kunci HSMs di cluster Anda.

  Jelajahi panduannya

- Otomatiskan penerapan layanan web NGINX menggunakan Amazon ECS dengan TLS offload di CloudHSM

  Gunakan AWS CloudHSM untuk menyimpan kunci pribadi Anda untuk situs web Anda yang di-host di cloud.

  Baca blognya

AWS Certificate Manager

- Meminta sertifikat publik

  Gunakan konsol AWS Certificate Manager (ACM) atau AWS CLI untuk meminta sertifikat ACM publik.

  Jelajahi panduannya

- Praktik terbaik untuk AWS Certificate Manager

  Pelajari praktik terbaik berdasarkan pengalaman dunia nyata dari pelanggan ACM saat ini.

  Jelajahi panduannya

- Cara menggunakan AWS Certificate Manager untuk menegakkan kontrol penerbitan sertifikat

  Gunakan kunci kondisi IAM untuk memastikan bahwa pengguna Anda menerbitkan atau meminta sertifikat TLS sesuai dengan pedoman organisasi Anda.

  Baca blognya

AWS Private CA

- Merencanakan AWS Private CA penyebaran Anda

  Bersiaplah AWS Private CA untuk digunakan sebelum Anda membuat otoritas sertifikat pribadi.

  Jelajahi panduannya
- AWS Private CA administrasi

  Buat hierarki otoritas sertifikat root dan bawahan yang sepenuhnya AWS dihosting untuk penggunaan internal oleh organisasi Anda.

  Jelajahi panduannya
- Administrasi sertifikat

  Lakukan tugas administrasi sertifikat dasar dengan AWS Private CA, seperti menerbitkan, mengambil, dan mencantumkan sertifikat pribadi.

  Jelajahi panduannya
- AWS Private CA lokakarya

  Kembangkan pengalaman langsung dengan berbagai kasus penggunaan otoritas sertifikat swasta.

  Jelajahi lokakarya
- Cara menyederhanakan penyediaan sertifikat di Active Directory dengan AWS Private CA

  Gunakan AWS Private CA untuk lebih mudah menyediakan sertifikat untuk pengguna dan mesin dalam lingkungan Microsoft Active Directory Anda.

  Baca blognya
- Cara menegakkan batasan nama DNS di AWS Private CA

  Terapkan batasan nama DNS ke CA bawahan dengan menggunakan layanan. AWS Private CA

  Baca blognya

AWS Secrets Manager

- AWS Secrets Manager konsep

Lakukan tugas administrasi sertifikat dasar dengan AWS Private CA, seperti menerbitkan, mengambil, dan mencantumkan sertifikat pribadi.

Jelajahi panduannya

- Siapkan rotasi pengguna bergantian untuk AWS Secrets Manager

  Siapkan rotasi pengguna bergantian untuk rahasia yang berisi kredensil basis data.

  Jelajahi panduannya

- Menggunakan AWS Secrets Manager rahasia dengan Kubernetes

  Tampilkan rahasia dari Secrets Manager sebagai file yang dipasang di pod Amazon EKS dengan menggunakan AWS Secrets and Configuration Provider (ASCP).

  Jelajahi panduannya

AWS Payment Cryptography

- Memulai dengan AWS Payment Cryptography

  Buat kunci dan gunakan dalam berbagai operasi kriptografi.

  Jelajahi panduannya

- AWS Payment Cryptography FAQs

  Memahami dasar-dasar AWS Payment Cryptography.

  Jelajahi FAQs

Gunakan layanan perlindungan AWS jaringan dan aplikasi

Tabel berikut menyediakan tautan ke sumber daya terperinci yang menggambarkan perlindungan AWS jaringan dan aplikasi.

AWS Firewall Manager

- Memulai dengan AWS Firewall Manager kebijakan

  Gunakan AWS Firewall Manager untuk mengaktifkan berbagai jenis kebijakan keamanan.

Jelajahi panduannya

- Cara terus mengaudit dan membatasi kelompok keamanan dengan AWS Firewall Manager

  Gunakan AWS Firewall Manager untuk membatasi grup keamanan, memastikan bahwa hanya port yang diperlukan yang terbuka.

  Baca blognya

- Gunakan AWS Firewall Manager untuk menerapkan perlindungan pada skala besar AWS Organizations

  Gunakan AWS Firewall Manager untuk menyebarkan dan mengelola kebijakan keamanan di seluruh Anda AWS Organizations.

  Baca blognya

AWS Network Firewall

- Memulai dengan AWS Network Firewall

  Konfigurasikan dan implementasikan AWS Network Firewall firewall untuk VPC dengan arsitektur gateway internet dasar.

  Jelajahi panduannya

- AWS Network Firewall Lokakarya

  Menyebarkan AWS Network Firewall dengan menggunakan infrastruktur sebagai kode.

  Jelajahi lokakarya

- Panduan langsung dari mesin aturan AWS Network Firewall fleksibel - Bagian 1

  Menyebarkan demonstrasi AWS Network Firewall di dalam Anda Akun AWS untuk berinteraksi dengan mesin aturannya.

  Baca blognya

- Panduan langsung dari mesin aturan AWS Network Firewall fleksibel - Bagian 2

  Buat kebijakan firewall dengan urutan aturan yang ketat dan tetapkan satu atau beberapa tindakan default.

Baca blognya

- Model penyebaran untuk AWS Network Firewall

  Pelajari model penerapan untuk kasus penggunaan umum di mana Anda dapat menambahkan AWS Network Firewall ke jalur lalu lintas.

  Baca blognya

- Model penerapan untuk peningkatan AWS Network Firewall perutean VPC

  Gunakan primitif perutean VPC yang disempurnakan untuk menyisipkan di AWS Network Firewall antara beban kerja dalam subnet yang berbeda dari VPC yang sama.

  Baca blognya

AWS Shield

- Bagaimana cara AWS Shield kerja

  Pelajari caranya AWS Shield Standard dan AWS Shield Advanced berikan perlindungan terhadap serangan DDo S untuk AWS sumber daya di jaringan dan lapisan transport (lapisan 3 dan 4) dan lapisan aplikasi (lapisan 7).

  Jelajahi panduannya

- Memulai dengan AWS Shield Advanced

  Mulai AWS Shield Advanced dengan menggunakan konsol Shield Advanced.

  Jelajahi panduannya

- AWS Shield Advanced lokakarya

  Lindungi sumber daya yang terpapar internet dari serangan DDo S, pantau serangan DDo S terhadap infrastruktur Anda, dan beri tahu tim yang sesuai.

  Jelajahi lokakarya

AWS WAF

- Memulai dengan AWS WAF

Siapkan AWS WAF, buat ACL web, dan lindungi Amazon CloudFront dengan menambahkan grup aturan dan aturan untuk memfilter permintaan web.

Memulai dengan tutorial

- Menganalisis AWS WAF Log di CloudWatch Log Amazon

  Siapkan AWS WAF pencatatan asli ke CloudWatch log Amazon dan visualisasikan serta analisis data di log.

  Baca blognya
- Visualisasikan AWS WAF log dengan dasbor Amazon CloudWatch

  Gunakan Amazon CloudWatch untuk memantau dan menganalisis AWS WAF aktivitas menggunakan CloudWatch metrik, Wawasan Kontributor, dan Wawasan Log.

  Baca blognya

Gunakan layanan AWS deteksi dan respons

Tabel berikut menyediakan tautan ke sumber daya terperinci yang menjelaskan layanan AWS deteksi dan respons.

AWS Config

- Memulai dengan AWS Config

  Mengatur AWS Config dan bekerja dengan AWS SDKs.

  Jelajahi panduannya
- Lokakarya Risiko dan Kepatuhan

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

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

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

Baca blognya

AWS CloudTrail

- Lihat riwayat acara

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

  Memulai dengan tutorial
- Buat jejak untuk mencatat peristiwa manajemen

  Buat jejak untuk mencatat peristiwa manajemen di semua Wilayah.

  Memulai dengan tutorial

AWS Security Hub CSPM

- Mengaktifkan AWS Security Hub CSPM

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

  Jelajahi panduannya
- Agregasi Lintas Wilayah

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

  Jelajahi panduannya
- AWS Security Hub CSPM lokakarya

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

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

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

Baca blognya

Amazon GuardDuty

- Memulai dengan Amazon GuardDuty

  Aktifkan Amazon GuardDuty, hasilkan temuan sampel, dan atur peringatan.

  Jelajahi tutorialnya
- Perlindungan EKS di Amazon GuardDuty

  Gunakan Amazon GuardDuty untuk memantau log audit Amazon Elastic Kubernetes Service (Amazon EKS).

  Jelajahi panduannya
- Perlindungan Lambda di Amazon GuardDuty

  Identifikasi potensi ancaman keamanan saat Anda menjalankan suatu AWS Lambda fungsi.

  Jelajahi panduannya
- GuardDuty Perlindungan Amazon RDS

  Gunakan Amazon GuardDuty untuk menganalisis dan membuat profil aktivitas login Amazon Relational Database Service (Amazon RDS) untuk potensi ancaman akses ke database Amazon Aurora Anda.

  Jelajahi panduannya
- Perlindungan Amazon S3 di Amazon GuardDuty

  Gunakan GuardDuty untuk memantau peristiwa CloudTrail data dan mengidentifikasi potensi risiko keamanan dalam bucket S3 Anda.

  Jelajahi panduannya
- Deteksi dan respons ancaman dengan Amazon GuardDuty dan Amazon Detective

  Pelajari dasar-dasar Amazon GuardDuty dan Amazon Detective.

  Jelajahi lokakarya

Amazon Inspector

- Memulai dengan Amazon Inspector

  Aktifkan pemindaian Amazon Inspector untuk memahami temuan di konsol.

  Memulai dengan tutorial
- Manajemen kerentanan dengan Amazon Inspector

  Gunakan Amazon Inspector untuk memindai instans Amazon EC2 dan gambar kontainer di Amazon Elastic Container Registry (Amazon ECR) untuk mencari kerentanan perangkat lunak.

  Jelajahi lokakarya
- Cara memindai EC2 AMIs dengan menggunakan Amazon Inspector

  Bangun solusi dengan menggunakan beberapa Layanan AWS untuk memindai kerentanan Anda AMIs yang diketahui.

  Baca blognya

Amazon Security Lake

- Memulai dengan Amazon Security Lake

  Aktifkan dan mulai menggunakan Amazon Security Lake.

  Jelajahi panduannya
- Mengelola beberapa akun dengan AWS Organizations

  Kumpulkan log keamanan dan peristiwa dari beberapa Akun AWS.

  Jelajahi panduannya
- Menelan, mengubah, dan mengirimkan acara yang diterbitkan oleh Amazon Security Lake ke Amazon Service OpenSearch

  Menyerap, mengubah, dan mengirimkan data Amazon Security Lake ke Amazon OpenSearch Service untuk digunakan oleh SecOps tim Anda.

  Baca blognya
- Cara memvisualisasikan temuan Amazon Security Lake dengan Quick

Kueri dan visualisasikan data dari Amazon Security Lake dengan menggunakan Amazon Athena dan Quick.

Baca blognya

Amazon Detective

- Istilah dan konsep Detektif Amazon

  Pelajari istilah dan konsep kunci yang penting untuk memahami Detektif Amazon dan cara kerjanya.

  Jelajahi panduannya
- Menyiapkan Detektif Amazon

  Aktifkan Amazon Detective dari konsol Amazon Detective, Amazon Detective API, atau. AWS CLI

  Jelajahi panduannya
- Deteksi dan respons ancaman dengan Amazon GuardDuty dan Amazon Detective

  Pelajari dasar-dasar Amazon GuardDuty dan Amazon Detective.

  Jelajahi lokakarya

Gunakan layanan AWS tata kelola dan kepatuhan

Tabel berikut menyediakan tautan ke sumber daya terperinci yang menjelaskan tata kelola dan kepatuhan.

AWS Organizations

- Membuat dan mengkonfigurasi organisasi

  Buat organisasi Anda dan konfigurasikan dengan dua akun AWS anggota.

  Memulai dengan tutorial
- Layanan yang bekerja dengan AWS Organizations

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

Jelajahi panduannya

- Mengatur AWS lingkungan Anda dengan menggunakan beberapa akun

  Terapkan praktik terbaik dan rekomendasi terkini untuk mengatur AWS lingkungan Anda secara keseluruhan.

  Baca whitepaper

AWS Artifact

- Memulai dengan AWS Artifact

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

  Jelajahi panduannya
- Mengelola perjanjian di AWS Artifact

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

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

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

  Baca blognya

AWS Audit Manager

- Mengaktifkan AWS Audit Manager

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

  Jelajahi panduannya

- Tutorial untuk Pemilik Audit: Membuat penilaian

  Buat penilaian dengan menggunakan Audit Manager Sample Framework.

  Jelajahi panduannya
- Tutorial untuk Delegasi: Meninjau set kontrol

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

  Jelajahi panduannya

AWS Control Tower

- Memulai dengan AWS Control Tower

  Siapkan dan luncurkan lingkungan multi-akun, yang disebut landing zone, yang mengikuti praktik terbaik preskriptif.

  Jelajahi panduannya
- Memodernisasi Manajemen Akun dengan Amazon Bedrock dan AWS Control Tower

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

  Baca blognya
- Membangun lingkungan yang dirancang dengan baik AWS GovCloud (AS) dengan AWS Control Tower

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

  Baca blognya

Jelajahi AWS layanan keamanan, identitas, dan tata kelola

Editable architecture diagrams

Diagram arsitektur referensi

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

Jelajahi arsitektur referensi keamanan, identitas, dan tata kelola

Ready-to-use code

Solusi unggulan

Wawasan Keamanan tentang AWS

Terapkan kode AWS yang dibuat untuk membantu Anda memvisualisasikan data di Amazon Security Lake untuk menyelidiki dan merespons peristiwa keamanan dengan lebih cepat.

Jelajahi solusi ini

AWS Solusi

Jelajahi solusi yang telah dikonfigurasi sebelumnya dan dapat diterapkan serta panduan implementasinya, yang dibuat oleh. AWS

Jelajahi semua AWS solusi keamanan, identitas, dan tata kelola

Documentation

Whitepaper keamanan, identitas, dan tata kelola

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

Jelajahi whitepaper keamanan, identitas, dan tata kelola

AWS Blog Keamanan

Jelajahi posting blog yang membahas kasus penggunaan keamanan tertentu.

Jelajahi blog AWS Keamanan

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Re: menciptakan pembaruan	Menambahkan informasi tentang Respons Insiden AWS Keamanan dan AWS Payment Cryptography. Informasi layanan yang diperbarui untuk AWS Identity and Access Management dan AWS IAM Identity Center.	Desember 30, 2024
Pembaruan video	Video pengantar yang diperbarui dengan pembicara an kilat baru-baru ini dari RE: Inforce 2024.	Juni 25, 2024
Menambahkan layanan tata kelola	Memperluas ruang lingkup dokumen untuk memasukka n tata kelola, termasuk menambahkan AWS CloudTrail,, dan. AWS Control Tower AWS Organizations Grafik yang diperbarui untuk mencerminkan ruang lingkup baru. Praktik terbaik yang diklarifikasi untuk identitas. Perubahan editorial di seluruh dokumen.	Juni 7, 2024
Publikasi awal	Panduan pertama kali diterbitk an.	Maret 21, 2024

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