Memutuskan untuk mengadopsi layanan AWS keamanan

AWS Panduan Preskriptif

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Panduan Preskriptif: Memutuskan untuk mengadopsi layanan AWS keamanan

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Pengantar 1
Audiens yang dituju 1
Tujuan 1
Pohon keputusan 3
Konteks perusahaan 5
1.1 Apakah mandat kepatuhan, keamanan, atau privasi tidak dihadiri? 5
1.2 Apakah Anda memiliki risiko tinggi yang tidak ditangani? 5
1.3 Apakah Anda memiliki solusi manual atau rawan kesalahan? 5
1.4 Apakah Anda menghadapi masalah manajemen, kelincahan, atau skalabilitas? 5
1.5 Apakah Anda memiliki total biaya kepemilikan yang tinggi? 6
AWS evaluasi layanan 6
2.1 Apakah AWS Layanan keamanan menangani kepatuhan, keamanan, atau mandat privasi Anda? 6
2.2 Apakah AWS layanan keamanan membantu mengurangi risiko? 7
2.3 Apakah POT menunjukkan efektivitas layanan keamanan? 7
2.4 Apakah TCO lebih rendah dari kontrol atau solusi saat ini? 7
2.5 Trade-off keputusan 8
AWS Kerangka Well-Architected 9
Keunggulan operasional 9
Keamanan 9
Keandalan 9
Efisiensi kinerja 9
Optimalisasi biaya 10
Keberlanjutan 10
Sumber daya 11
AWS dokumentasi 11
AWS Sumber daya lainnya 11
Riwayat dokumen 12
..... xiii

Memutuskan untuk mengadopsi layanan AWS keamanan

Diogo Guedes, Amazon Web Services

Februari 2025 (riwayat dokumen)

Banyak organisasi tidak yakin tentang mengadopsi layanan AWS keamanan. Terkadang, sudah ada solusi yang ada, dan organisasi perlu menentukan apakah memperdagangkan solusi mereka saat ini untuk layanan yang berbeda bermanfaat.

Misalnya, organisasi Anda mungkin mempertimbangkan adopsi Amazon Security Lake untuk memusatkan data terkait keamanan Anda. Atau Anda mungkin ingin menjelajahi menggunakan Amazon Macie untuk menemukan dan membantu melindungi data sensitif di bucket Amazon Simple Storage Service (Amazon S3). Bahkan jika organisasi Anda sudah memiliki solusi lain, Anda dapat mengevaluasi apakah Layanan AWS dapat mengurangi biaya atau meningkatkan efektivitas atau skalabilitas.

Pertanyaan apa yang perlu Anda jawab untuk menentukan apakah layanan AWS keamanan cocok untuk organisasi Anda? Panduan ini menyediakan pohon keputusan yang membantu Anda mengevaluasi potensi adopsi layanan dan membuat pilihan berbasis data yang selaras dengan Kerangka Kerja AWS Well-Architected.

Audiens yang dituju

Panduan ini ditujukan bagi mereka yang memiliki peran teknologi, seperti kepala perusahaan teknologi (CTOs), arsitek, pengembang, dan anggota tim operasi, yang perlu memilih layanan keamanan dan solusi untuk organisasi mereka. Untuk menggunakan panduan ini, Anda harus terbiasa dengan konsep bisnis dan manajemen teknis, seperti total biaya kepemilikan (TCO) dan bukti teknologi (POT).

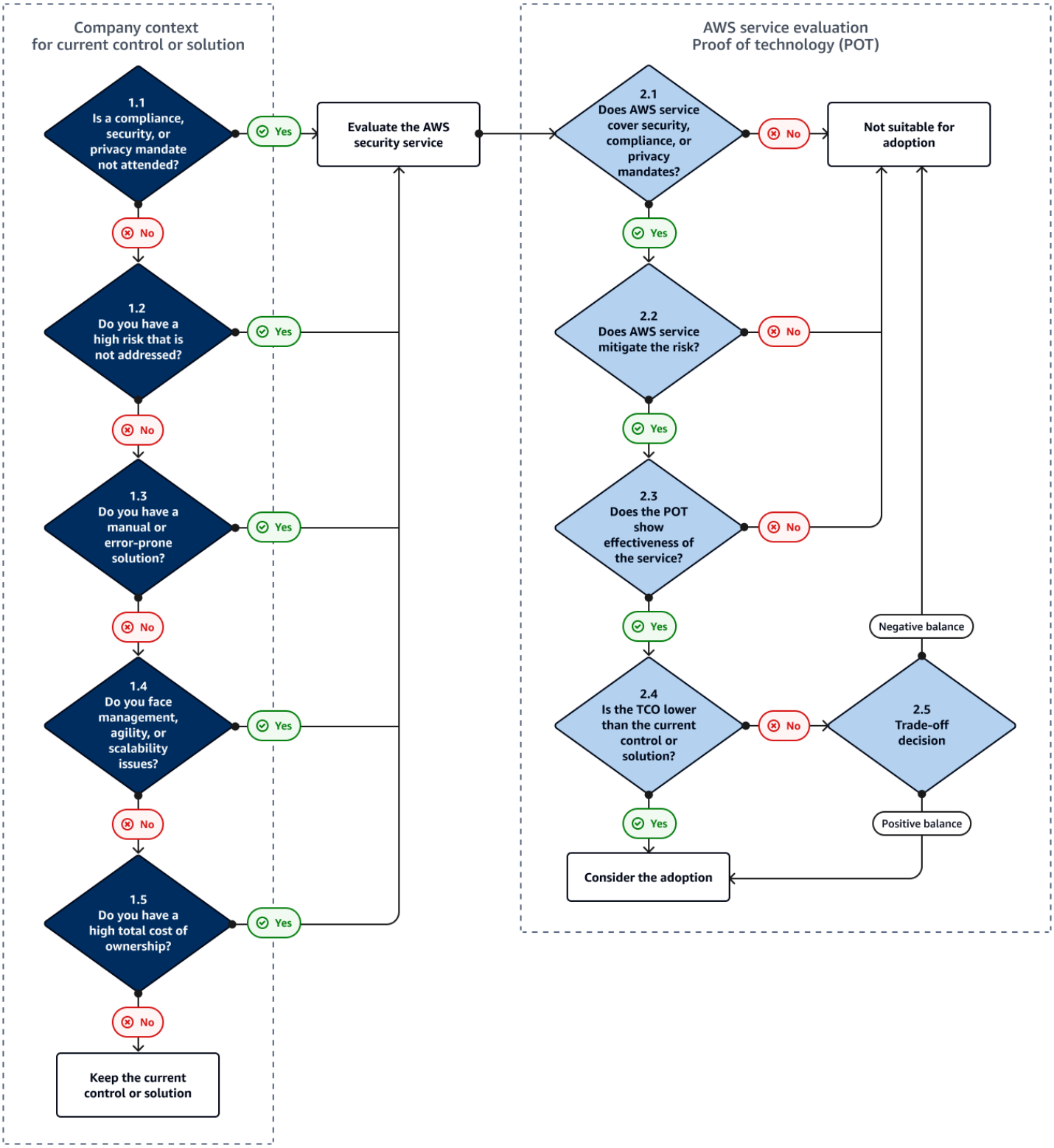
Tujuan

Dengan menggunakan pohon keputusan dalam panduan ini, Anda dapat secara efektif mengevaluasi apakah organisasi Anda harus mengadopsi layanan AWS keamanan. Mengevaluasi persyaratan bisnis dan teknis dengan tepat dapat memberikan peluang organisasi, seperti penghematan biaya, peningkatan mitigasi risiko, otomatisasi, kelincahan, skalabilitas, dan efektivitas.

Keputusan berbasis data mendukung adopsi dan meningkatkan postur keamanan perusahaan Anda, mempertahankan pertumbuhan dan membantu Anda mencapai tujuan bisnis.

Pohon keputusan untuk mengadopsi AWS layanan keamanan

Gambar berikut menunjukkan pohon keputusan yang dapat Anda gunakan untuk mengevaluasi apakah organisasi Anda harus mengadopsi layanan AWS keamanan. Pohon keputusan dibagi menjadi dua bagian: Konteks perusahaan dan evaluasi layanan AWS keamanan. Bagian pertama, konteks Perusahaan, dirancang untuk mengevaluasi kontrol atau solusi Anda saat ini, jika ada. Anda melanjutkan ke bagian kedua, evaluasi layanan AWS keamanan, jika Anda tidak memiliki solusi saat ini atau jika kontrol atau solusi Anda saat ini tidak memenuhi persyaratan bisnis atau teknis Anda. Di bagian evaluasi layanan AWS keamanan, Anda menentukan apakah Layanan AWS memenuhi persyaratan tersebut.


Company context
for current control or solution
1.1
Is a compliance, security, or privacy mandate not attended?
Yes
No
1.2
Do you have a high risk that is not addressed?
Yes
No
1.3
Do you have a manual or error-prone solution?
Yes
No
1.4
Do you face management, agility, or scalability issues?
Yes
No
1.5
Do you have a high total cost of ownership?
Yes
No
Keep the current control or solution
Evaluate the AWS security service
AWS service evaluation
Proof of technology (POT)
2.1
Does AWS service cover security, compliance, or privacy mandates?
No
Not suitable for adoption
Yes
2.2
Does AWS service mitigate the risk?
No
Yes
2.3
Does the POT show effectiveness of the service?
No
Yes
2.4
Is the TCO lower than the current control or solution?
No
Yes
2.5
Trade-off decision
Negative balance
Positive balance
Consider the adoption

Konteks perusahaan untuk mengevaluasi kontrol atau solusi keamanan saat ini

Di bagian ini, Anda mengevaluasi kontrol atau solusi Anda saat ini untuk memastikan bahwa itu memenuhi persyaratan bisnis dan teknis organisasi Anda. Jika Anda tidak memiliki kontrol atau solusi, Anda harus mengevaluasi layanan AWS keamanan dan langsung masuk ke bagian evaluasi layanan keamanan AWS.

1.1 Apakah mandat kepatuhan, keamanan, atau privasi tidak dihadiri?

Organizations berada di bawah lingkup undang-undang dan peraturan mengenai keamanan dan privasi data. Setiap pelanggaran mandat ini dapat mengakibatkan konsekuensi yang parah. Jika perusahaan Anda tidak dapat memenuhi persyaratan kepatuhan, keamanan, atau privasi, Anda harus mengevaluasi layanan AWS keamanan.

1.2 Apakah Anda memiliki risiko tinggi yang tidak ditangani?

Organizations perlu mengidentifikasi dan mengelola risiko keamanan yang signifikan di lingkungan mereka. Risiko tinggi dapat melibatkan potensi pelanggaran data, kerentanan sistem, gangguan operasional, atau masalah keamanan kritis lainnya. Jika solusi Anda saat ini (atau tidak adanya) tidak cukup mengurangi risiko tinggi ini, lanjutkan dengan mengevaluasi layanan keamanan. AWS

1.3 Apakah Anda memiliki solusi manual atau rawan kesalahan?

Solusi yang membutuhkan langkah manual atau interaksi manusia lebih rawan kesalahan. Ketidakkonsistenan, keandalan data yang rendah, aset yang tidak patuh, dan kurangnya skalabilitas sering terjadi dalam skenario ini. Kontrol otomatis pada dasarnya penting untuk sistem TI dan beban kerja. Jika solusi Anda saat ini tidak mendukung otomatisasi penuh, pertimbangkan untuk mengevaluasi layanan AWS keamanan.

1.4 Apakah Anda menghadapi masalah manajemen, kelincahan, atau skalabilitas?

Penting untuk memetakan masalah apa pun yang terkait dengan manajemen. Berikut ini adalah beberapa contoh: Kurangnya kompatibilitas mengelola aset yang berbeda, solusinya tidak mencakup semua perangkat, kesalahan dan gangguan selama pembaruan, dan dampak kinerja negatif dalam produksi. Solusinya harus menawarkan kelincahan sehingga tim dapat berinovasi dari postur

keamanan yang kuat. Anda harus mendukung skalabilitas untuk mencapai pertumbuhan bisnis eksponensial. Jika Anda memiliki masalah manajemen, ketersediaan, atau penskalaan, Anda harus mengevaluasi layanan AWS keamanan.

1.5 Apakah Anda memiliki total biaya kepemilikan yang tinggi?

Evaluasi total biaya kepemilikan (TCO) untuk solusi keamanan Anda saat ini dengan membandingkan biaya terhadap tolok ukur industri dan metrik internal. Umumnya, organisasi menginvestasikan 6-14% dari anggaran TI mereka dalam keamanan siber, dan 10% adalah rata-rata. Pertimbangkan faktor-faktor seperti perizinan, implementasi, pemeliharaan, dukungan, dan biaya operasional untuk melindungi aset Anda. Anda dapat menyertakan alat internal Anda yang mencakup jumlah aset yang sama untuk dilindungi. Anggaran keamanan yang tidak seimbang untuk alat juga dapat menunjukkan TCO yang tinggi, seperti jika 60% dari anggaran diarahkan ke satu alat. Jika TCO Anda lebih tinggi dari tolok ukur ini, lanjutkan dengan mengevaluasi layanan keamanan. AWS

AWS evaluasi layanan keamanan

Bukti teknologi (POT) mirip dengan bukti konsep. Tujuan dari POT adalah untuk menentukan apakah solusi potensial untuk masalah teknis layak. Misalnya, Anda mungkin menggunakan POT untuk membuktikan bahwa konfigurasi tertentu dapat mencapai hasil tertentu. Di bagian ini, Anda menggunakan POT untuk mengevaluasi dan menunjukkan apakah layanan AWS keamanan tertentu memenuhi persyaratan bisnis dan teknis Anda.

AWS Security Reference Architecture (AWS SRA) memberikan panduan preskriptif untuk menyebarkan layanan AWS keamanan lengkap di lingkungan multi-akun. Arsitektur ini dapat membantu Anda merencanakan dan melaksanakan evaluasi POT Anda.

Panduan keputusan ini berlaku untuk semua layanan AWS keamanan, termasuk penawaran terbaru. Untuk daftar layanan terbaru dan praktik terbaik saat ini, lihat AWS Cloud Keamanan.

2.1 Apakah AWS Layanan keamanan menangani kepatuhan, keamanan, atau mandat privasi Anda?

Layanan AWS keamanan harus menangani mandat kepatuhan, keamanan, dan privasi apa pun yang tidak ditangani oleh solusi saat ini. Anda dapat menemukan AWS sertifikasi dan laporan untuk keamanan dan kepatuhan di AWS Artifact. Selain itu, Anda dapat menggunakan Layanan AWS dokumentasi untuk validasi cakupan.

2.2 Apakah AWS layanan keamanan membantu mengurangi risiko?

Manajemen risiko adalah faktor kunci untuk membantu melindungi perusahaan dari banyak ancaman. Keputusan untuk mengadopsi layanan mungkin terkait langsung dengan mengurangi satu atau lebih risiko tinggi di organisasi Anda. Layanan AWS keamanan harus mengurangi risiko ke tingkat yang dapat diterima, berdasarkan selera risiko dan konteks bisnis Anda.

2.3 Apakah POT menunjukkan efektivitas layanan keamanan?

Efektivitas layanan AWS keamanan harus ditunjukkan melalui POT, sesuai dengan metrik yang berbeda dari setiap layanan keamanan. Misalnya, POT mungkin memvalidasi bahwa layanan dapat mendeteksi dan merespons ancaman keamanan dengan cepat melalui algoritma intelijen ancaman. Anda dapat mengevaluasi keberhasilan dengan mengonfirmasi bahwa ancaman yang terdeteksi dalam hitungan menit dan pemberitahuan dan remediasi otomatis berjalan dengan sukses. Untuk layanan manajemen kerentanan, Anda dapat mengevaluasi efektivitas berdasarkan hal berikut:

- Berapa banyak kerentanan yang terdeteksi?
- Berapa tingkat keberhasilan menerapkan tambalan dan pembaruan?
- Untuk perlindungan web, apakah cross-site scripting (XSS) dan SQL-injection serangan yang dilakukan oleh tim keamanan ofensif (juga dikenal sebagai tim merah) segera diblokir?

AWS Layanan dan AWS Mitra Profesional dapat mendukung Anda dalam evaluasi POT ini.

2.4 Apakah TCO lebih rendah dari kontrol atau solusi saat ini?

TCO yang lebih rendah dapat membantu Anda mengoptimalkan biaya di organisasi Anda. Beberapa metrik umum yang digunakan dalam perbandingan ini adalah: biaya akuisisi dan implementasi, biaya tetap dan variabel, biaya operasi, biaya pemeliharaan dan dukungan, biaya ekspansi dan keandalan, dan biaya pelatihan. Ada pengukuran dan perbandingan biaya lain yang dapat Anda lakukan berdasarkan kasus penggunaan spesifik Anda. Ini AWS Kalkulator Hargadapat membantu Anda memperkirakan biaya untuk Layanan AWS. Selain itu, Anda dapat menggunakan produk di jalur bebas AWS Tingkat Gratis dan gratis untuk mengevaluasi banyak Layanan AWS. Untuk informasi selengkapnya, lihat Uji Coba AWS Cloud Keamanan Gratis.

2.5 Trade-off keputusan

Keputusan trade-off membutuhkan penyeimbangan beberapa faktor, terutama efektivitas layanan dan pertimbangan TCO. Ketika perhitungan yang tepat atau penentuan yang jelas tidak memungkinkan, evaluasi keseimbangan manfaat dan batasan secara keseluruhan.

Keseimbangan positif mungkin muncul bahkan ketika faktor-faktor tampaknya bertentangan. Misalnya, layanan dapat meningkatkan biaya tetapi memberikan peningkatan skalabilitas. Ini merupakan keseimbangan positif di mana peningkatan efektivitas membenarkan biaya tambahan. Sebaliknya, penurunan kemampuan mungkin tidak dapat diterima bahkan jika layanan menawarkan penghematan biaya yang signifikan.

Anda harus menyeimbangkan semua informasi yang tersedia untuk menentukan hasil positif atau negatif secara keseluruhan. Berdasarkan analisis ini, Anda dapat membuat keputusan trade-off Anda.

Penyelarasan dengan Kerangka AWS Well-Architected

Kerangka AWS Well-Architected menjelaskan konsep-konsep kunci, prinsip desain, dan praktik terbaik arsitektur untuk merancang dan menjalankan beban kerja di. AWS Cloud Bagian ini menjelaskan bagaimana pohon keputusan dalam panduan ini mendukung manfaat keseluruhan dari Kerangka AWS Well-Architected dan enam pilarnya.

Keunggulan operasional

Pohon keputusan membantu organisasi mengevaluasi solusi keamanan mereka saat ini dan menilai keunggulan operasional dari kontrol tersebut. Faktor-faktor seperti proses manual atau rawan kesalahan, masalah manajemen dan skalabilitas, dan TCO tinggi menunjukkan area di mana layanan AWS keamanan dapat meningkatkan efisiensi operasional, memberikan wawasan, dan mendorong peningkatan berkelanjutan. Dengan mengadopsi layanan AWS keamanan yang efektif, organisasi dapat lebih mendukung pengembangan dan pengoperasian beban kerja mereka.

Keamanan

Mengevaluasi apakah layanan AWS keamanan dapat menangani mandat kepatuhan, mengurangi risiko tinggi, dan menunjukkan hasil keamanan yang efektif secara langsung mendukung pilar keamanan. Kerangka keputusan membantu organisasi menilai secara menyeluruh Layanan AWS untuk memverifikasi bahwa ia dapat melindungi data, sistem, dan aset mereka secara memadai, bila digunakan sesuai dengan praktik terbaik AWS keamanan.

Keandalan

Kekhawatiran seputar manajemen, kelincahan, dan skalabilitas solusi keamanan saat ini menunjukkan masalah keandalan yang mungkin diselesaikan oleh layanan AWS keamanan. Dengan memvalidasi keandalan dan kinerja yang konsisten dari Layanan AWS melalui proses POT, organisasi dapat memastikan bahwa beban kerja mereka memiliki ketahanan yang diperlukan untuk berfungsi dengan benar dari waktu ke waktu.

Efisiensi kinerja

AWS Layanan keamanan dapat meningkatkan efisiensi kinerja dengan secara otomatis menskalakan sumber daya untuk memenuhi permintaan yang berubah dan meminimalkan overhead operasional

melalui layanan terkelola. Kemampuan penskalaan dinamis memastikan bahwa sumber daya komputasi digunakan secara efisien, dan layanan terkelola membantu tim fokus pada peningkatan kinerja khusus beban kerja. Layanan yang tepat dan sumber daya komputasi dirancang untuk memberikan perlindungan dan efisiensi kinerja dan untuk mempertahankan efisiensi seiring dengan perubahan permintaan dan kemajuan teknologi.

Optimalisasi biaya

Bagian penting dari kerangka keputusan adalah menentukan apakah layanan AWS keamanan dapat memberikan TCO yang lebih rendah dibandingkan dengan solusi saat ini. Ini secara langsung sejalan dengan pilar pengoptimalan biaya, yang membantu organisasi menjalankan sistem keamanan mereka dengan biaya optimal untuk memberikan nilai bisnis.

Keberlanjutan

Mengadopsi layanan AWS keamanan yang lebih efisien, otomatis, dan hemat biaya secara tidak langsung dapat berkontribusi pada peningkatan keberlanjutan. Dengan meminimalkan sumber daya yang dibutuhkan untuk keamanan yang efektif, organisasi dapat meningkatkan keberlanjutan keseluruhan portofolio teknologi mereka.

Sumber daya

AWS dokumentasi

- Pilar Keandalan (Kerangka AWS Well-Architected)
- Pilar Keamanan (KerangkaAWS Well-Architected)

AWS Sumber daya lainnya

- AWS Artifact
- AWS Kalkulator Harga
- Uji Coba AWS Cloud Keamanan Gratis
- Keamanan, Identitas, dan Kepatuhan pada AWS

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Perbarui	Memperbarui pohon keputusan dan menambahkan Alignment dengan halaman AWS Well-Architected Framework.	Februari 27, 2025
Publikasi awal	—	April 11, 2024

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