

Assured Controls





- 01 Pengantar
- 02 Meningkatnya tuntutan regulasi
- 03 Industri yang merasakan tekanan
- 04 Rencana lima langkah
- 05 Kesimpulan



01

Pengantar



Kolaborasi mendorong bisnis modern. Berbagi data di seluruh tim, wilayah, dan organisasi mendorong inovasi, meningkatkan produktivitas tim, dan mempercepat pertumbuhan bisnis. Namun, keterbukaan ini sering kali bertentangan dengan tuntutan keamanan dan kepatuhan data, sehingga menciptakan tantangan kompleks bagi bisnis untuk mengatasinya.

Taruhannya tinggi. Pada tahun 2024 saja, pelanggaran terhadap General Data Protection Regulation (GDPR) di Uni Eropa mengakibatkan dijatuhkannya 277 denda, dengan total €1,19 miliar¹. Kasus berprofil tinggi seperti denda terhadap Meta sebesar €1,2 miliar² karena mentransfer data pengguna Uni Eropa ke AS tanpa pengamanan yang memadai menggarisbawahi risiko finansial dan reputasi akibat ketidakpatuhan.

Inti dari tantangan ini adalah kedaulatan data, yaitu kemampuan untuk mengontrol lokasi penyimpanan data, cara mengaksesnya, dan siapa yang berwenang menanganinya. Dengan berkembangnya peraturan di berbagai wilayah, seperti Uni Eropa, Amerika Serikat, dan lainnya di seluruh dunia, menjaga kedaulatan data menjadi semakin penting. Organisasi harus melindungi data mereka dari akses tidak sah sekaligus mematuhi berbagai undang-undang regional yang terus berkembang. Hal ini merupakan tantangan signifikan bagi CIO, CISO, dan Compliance Officer, yang sering kali menghadapi resistensi internal terhadap inisiatif perlindungan data.

Sumber: 1. <https://www.enforcementtracker.com/?insights> 2. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Assured Controls di Google Workspace memberi organisasi opsi untuk memisahkan data mereka ke dalam region-region data, sehingga organisasi dapat memilih lokasi tempat data mereka diproses dan disimpan—seperti Uni Eropa atau AS—untuk memenuhi peraturan yang ketat. Dengan kontrol administratif yang terperinci, layanan ini membantu memastikan data Anda tetap terlindungi dari akses tidak sah sekaligus mendukung kolaborasi yang aman dan lancar.

Panduan ini menawarkan roadmap praktis untuk mengamankan data Anda dan menghadapi tantangan kepatuhan secara langsung. Mulai dari menilai lingkungan Anda saat ini hingga menerapkan kontrol lanjutan, Anda akan mendapatkan insight dan alat yang diperlukan untuk mengatasi kompleksitas kedaulatan data.



Untuk mewujudkan kedaulatan data di dunia yang kolaboratif, organisasi harus:

01

Mengontrol tempat penyimpanan dan pemrosesan data mereka.

02

Memastikan hanya pihak yang diotorisasi yang dapat mengaksesnya.



02

Meningkatnya tuntutan regulasi



Pemerintah di seluruh dunia memperkenalkan hukum perlindungan data yang lebih ketat untuk melindungi informasi pribadi dan memastikan kontrol lokal atas data sensitif. Kerangka kerja ini mengubah cara bisnis mengelola informasi mereka, menciptakan peluang baru untuk kepatuhan dan inovasi sekaligus meningkatkan risiko ketidakpatuhan.





Uni Eropa: GDPR dan EU AI Act

General Data Protection Regulation (GDPR) menetapkan tolok ukur global untuk privasi data. GDPR mewajibkan kontrol ketat terhadap cara penyimpanan, pemrosesan, dan transfer data pribadi, terutama di luar Wilayah Ekonomi Eropa (EEA). Organisasi harus menerapkan pengamanan yang memadai, seperti klausul kontrak standar atau perlindungan yang setara, untuk memastikan kepatuhan. GDPR berlaku untuk bisnis yang menawarkan barang atau jasa kepada warga negara Uni Eropa atau memantau perilaku mereka, terlepas dari lokasi bisnis tersebut.



European Union Artificial Intelligence Act (EU AI Act) adalah kerangka hukum pertama di dunia untuk AI, yang mengatur risiko dan mendorong penggunaan AI yang tepercaya di Eropa. Peraturan ini berlaku untuk bisnis apa pun yang mengembangkan atau men-deploy AI di pasar EU, terlepas dari lokasi bisnis tersebut. Sistem AI dikategorikan ke dalam empat tingkat risiko:

Risiko yang tidak dapat diterima

Melarang aplikasi AI yang mengancam keselamatan dan hak (misalnya, penilaian sosial, pengawasan biometrik).

Risiko tinggi

AI di sektor penting (misalnya, layanan kesehatan, penegakan hukum) harus mematuhi peraturan ketat, termasuk penilaian risiko dan pengawasan manusia.

Risiko transparansi

Sistem AI, seperti chatbot dan AI generatif, harus mengungkapkan konten buatan AI dengan jelas.

Risiko minimal atau tidak ada risiko

AI berisiko rendah (misalnya, filter spam, game berteknologi AI) tidak dikenai pembatasan.



Amerika Serikat: HIPAA, CCPA, dan CDPA

Meskipun Amerika Serikat tidak memiliki hukum privasi data federal yang terpadu, peraturan sektoral dan tingkat negara bagian memberlakukan kewajiban yang signifikan:

HIPAA

Berlaku untuk penyedia layanan kesehatan, perusahaan asuransi, dan rekan bisnis mereka, yang melindungi informasi pasien melalui tindakan privasi dan keamanan yang ketat.

CCPA (California)

Memberikan hak kepada konsumen atas data pribadi mereka, termasuk kemampuan untuk mengakses, menghapus, atau memilih tidak ikut dalam penjualan data tersebut. Hal ini berlaku untuk bisnis yang memenuhi batas pendapatan atau data tertentu.

CDPA (Virginia)

Mirip dengan CCPA, undang-undang ini menargetkan privasi konsumen dengan penekanan pada minimalisasi dan transparansi data.

Asia Pasifik: APPI dan PIPA

- 01 Act on the Protection of Personal Information (APPI) Jepang: Berfokus pada transfer data lintas batas, yang memerlukan izin atau perlindungan yang setara saat menangani data warga negara Jepang.
- 02 Personal Information Protection Act (PIPA) Korea Selatan: Menegakkan persyaratan ketat, termasuk batasan transfer lintas batas dan hukuman berat untuk pelanggaran.

Amerika Selatan: LGPD Brasil

Lei Geral de Proteção de Dados (LGPD) Brasil mirip dengan GDPR, yang menuntut izin ketat untuk pemrosesan data dan hukuman berat untuk pelanggaran. Hukum ini berlaku untuk bisnis yang menangani data terkait warga negara Brasil.



Kompleksitas lintas batas

Mentransfer data secara internasional memerlukan kepatuhan terhadap berbagai framework.

Persyaratan yang terus berkembang

Seiring terus berkembangnya hukum, seperti GDPR dan LGPD, organisasi harus beradaptasi agar tetap mematuhi hukum.

Nuansa sektoral

Peraturan sering kali tumpang tindih, tetapi penerapannya bervariasi bergantung pada risiko dan kebutuhan khusus industri.

Tantangan umum di seluruh framework

Terlepas dari perbedaan regional, bisnis menghadapi tantangan universal.

Framework ini membentuk tulang punggung kedaulatan data secara hukum, tetapi implikasinya paling terasa dalam industri yang menangani data sensitif. Baca terus untuk mempelajari bagaimana berbagai sektor, seperti keuangan, layanan kesehatan, dan teknologi, mengatasi tantangan unik ini.



03

Industri yang merasakan tekanan

Tantangan kedaulatan data tidak memengaruhi semua industri dengan cara yang sama. Tantangan ini lebih membebani industri tertentu karena data sensitif yang mereka tangani dan peraturan ketat yang menentukan setiap langkah mereka.

Bagi sektor seperti keuangan, layanan kesehatan, pemerintah, dan teknologi, mewujudkan kedaulatan data bukan hanya sekadar memenuhi persyaratan kepatuhan. Hal ini terkait dengan perlindungan aset penting, membangun kepercayaan dengan pemangku kepentingan, dan memastikan operasi tetap lancar dan aman dalam lanskap yang semakin kompleks.



 Bagikan ▼



Keuangan: Menjaga kepercayaan dalam lanskap yang kompetitif

Lembaga keuangan terus diawasi karena sifat sensitif data pelanggan dan peran mereka dalam perekonomian global. Peraturan seperti GDPR menuntut kontrol yang tepat atas penyimpanan dan akses data, sementara inisiatif Open Banking mengharuskan berbagi data pelanggan secara aman dengan penyedia pihak ketiga guna mendorong inovasi.



Shirley Franklin

Pertimbangan utama:

Tantangan lintas batas

Mengelola data keuangan di berbagai wilayah hukum menimbulkan risiko, terutama saat data mengalir di antara region dengan persyaratan peraturan yang berbeda.

Sistem lama

Banyak bank mengandalkan infrastruktur usang yang mempersulit penerapan langkah-langkah kepatuhan modern, seperti enkripsi tingkat lanjut atau akses berbasis peran.

Taruhan reputasi

Dalam industri yang mengutamakan kepercayaan, satu saja pelanggaran atau kegagalan kepatuhan dapat menyebabkan kerugian finansial dan reputasi yang signifikan.

Dengan menerapkan solusi seperti kontrol akses terperinci dan pemrosesan data yang dilokalkan, organisasi keuangan dapat memenuhi standar kepatuhan dengan percaya diri sekaligus melindungi kepercayaan pelanggan.



Layanan kesehatan: Menyeimbangkan privasi dengan kemajuan

Dalam layanan kesehatan, privasi pasien adalah kewajiban hukum dan komitmen etis. Industri kesehatan berjalan dalam lingkup keseimbangan yang rumit, karena wajib melindungi catatan medis yang sensitif dengan tetap mendorong kolaborasi riset yang dapat menyelamatkan kehidupan.

Pertimbangan utama:

Tumpang tindih peraturan

Penyedia layanan kesehatan harus mematuhi berbagai peraturan yang kompleks, mulai dari HIPAA di AS hingga GDPR di Uni Eropa, yang masing-masing memiliki standar sendiri untuk penyimpanan, enkripsi, dan akses data.

Kolaborasi lintas batas

Lembaga riset sering kali memerlukan aktivitas berbagi data lintas negara, yang semakin memperumit aspek kepatuhan. Misalnya, berbagi data pasien yang dianonimkan untuk uji klinis global harus selaras dengan hukum kedaulatan data lokal.

Gangguan operasional

Sistem yang usang dan data yang terisolasi sering menyebabkan inefisiensi dan peningkatan risiko dalam audit kepatuhan.

Langkah-langkah perlindungan data yang kuat, seperti enkripsi end-to-end dan alat pengawasan real-time, memastikan organisasi layanan kesehatan dapat memenuhi kepatuhan sekaligus mendorong inovasi dan kolaborasi.

Pemerintahan: Mengamankan kepercayaan warga dan menjaga keamanan nasional

Badan pemerintah mengelola data warga negara yang sensitif dalam jumlah besar, mulai dari catatan pajak hingga informasi keamanan nasional. Taruhannya tinggi; perlindungan terhadap data ini tidak hanya mandat kepatuhan, tetapi juga masalah kepercayaan publik dan keamanan nasional.



Pertimbangan utama:

Risiko geopolitik

Lembaga pemerintah menghadapi tantangan unik, termasuk ancaman siber dan tekanan dari pihak-pihak asing, sehingga residensi dan kedaulatan data menjadi penting.

Transparansi vs. keamanan

Menyeimbangkan keterbukaan dengan kebutuhan akan kontrol data yang ketat sangat penting untuk menjaga kepercayaan publik.

Hukum regional

Lembaga pemerintah harus mematuhi peraturan yang tumpang tindih seperti GDPR di Eropa atau regulasi lokal yang mewajibkan pelokalan data.

Dengan alat kedaulatan data seperti enkripsi end-to-end dan kontrol akses yang ketat, organisasi sektor publik dapat mengamankan data tanpa mengorbankan transparansi atau efisiensi operasional mereka.



Teknologi: Berinovasi di bawah pengawasan

Perusahaan teknologi berada di persimpangan antara skalabilitas global dan kepatuhan regional, dengan memproses sejumlah besar data pengguna di berbagai negara. Bagi organisasi semacam ini, residensi data tidak hanya masalah kepatuhan, tetapi juga penting untuk melindungi kekayaan intelektual dan menjaga kepercayaan pelanggan.



“Ketika data tidak teregionalisasi atau ditangani oleh penyedia teknologi lain, akan muncul risiko bagi Eropa, bagi negara terkait, dan bagi Airbus. Ini adalah risiko yang tidak dapat kami tanggung.”

Sebastien Aubineau, Airbus

Pertimbangan utama:

Jangkauan global, aturan lokal

Perusahaan seperti Airbus menekankan pentingnya pemrosesan data yang teregionalisasi untuk melindungi informasi sensitif dan mematuhi peraturan kedaulatan.

Solusi yang skalabel

Organisasi teknologi harus menerapkan sistem yang memungkinkan mereka berkembang secara global tanpa mengorbankan kepatuhan.

Risiko yang muncul

Inovasi cepat sering kali menyebabkan kerentanan yang tidak terduga, mulai dari integrasi aplikasi pihak ketiga hingga akses yang tidak terkontrol dengan baik.

Kontrol administratif yang terperinci dan langkah-langkah keamanan tingkat lanjut memungkinkan perusahaan teknologi mengatasi tantangan ini tanpa menghambat inovasi atau pertumbuhan.



04

Rencana lima langkah



Untuk menempuh jalan menuju kedaulatan data, diperlukan pendekatan terstruktur yang disesuaikan dengan kebutuhan, industri, dan lokasi unik Anda. Panduan ini menguraikan lima langkah yang dapat ditindaklanjuti untuk membantu Anda mengontrol lingkungan data, mematuhi peraturan, dan membangun kepercayaan terhadap strategi kepatuhan organisasi Anda.

01

Menilai lingkungan Anda

Pahami tempat penyimpanan data Anda, siapa yang memiliki akses, dan peraturan mana yang berlaku. Hal ini merupakan titik awal Anda untuk mengidentifikasi kesenjangan.

02

Memilih region data

Lokalkan penyimpanan dan pemrosesan data Anda agar selaras dengan persyaratan peraturan sekaligus menjaga fleksibilitas operasional.

03

Memperbaiki kontrol akses

Sesuaikan izin untuk memastikan hanya orang yang tepat memiliki akses ke data yang tepat, sehingga meminimalkan eksposur.

04

Memperkuat perlindungan data

Tetap waspada terhadap ancaman siber yang terus berkembang dengan meningkatkan tindakan keamanan dan melindungi data sensitif.

05

Pelaporan dan pengawasan

Gunakan pemantauan dan pelaporan berkelanjutan agar tetap patuh dan proaktif dalam lingkungan peraturan yang terus berubah.



01

Menilai lingkungan Anda

Setiap perjalanan dimulai dengan memahami posisi Anda saat ini dan tujuan yang ingin Anda capai.

Untuk mewujudkan kedaulatan data, mulailah dengan memahami peraturan eksternal yang mengatur industri Anda dan realitas internal lanskap data Anda. Hal ini terkait dengan menyelaraskan tempat penyimpanan data Anda, cara mengaksesnya, dan hal yang diperlukan untuk memenuhi kepatuhan—sekaligus mengidentifikasi celah dalam konfigurasi Anda saat ini.



Memahami peraturannya

Framework global seperti **GDPR**, **ISO**, dan **SOC** menetapkan standar kepatuhan. Namun, berbagai framework itu memiliki implikasi; peraturan tersebut menuntut keselarasan dengan operasi spesifik organisasi Anda:

GDPR (Eropa)

Memerlukan residensi data yang ketat di dalam Wilayah Ekonomi Eropa (EEA), kecuali jika langkah pengamanan yang memadai, seperti klausul kontrak standar, telah diterapkan. Bagi organisasi yang memiliki pelanggan Eropa, memahami dengan tepat lokasi penyimpanan dan transfer data pribadi sangatlah penting.

EU AI Act (Uni Eropa)

EU Artificial Intelligence Act adalah peraturan Uni Eropa yang bertujuan untuk menetapkan kerangka kerja peraturan bersama bagi AI di wilayah EU. Peraturan ini mengklasifikasikan sistem dan model AI ke dalam beberapa kategori serta menetapkan persyaratan yang berbeda untuk setiap kategori. Pada 2 Agustus 2024, EU AI Act tersebut resmi diberlakukan secara hukum.

DORA (Uni Eropa)

Digital Operational Resilience Act menetapkan standar teknis untuk memperkuat keamanan IT lembaga keuangan. Disusun oleh European Supervisory Authorities (ESA) dan diberlakukan oleh Komisi Eropa, peraturan ini menyatukan aturan tentang ketahanan operasional untuk sektor keuangan dan penyedia pihak ketiga ICT.

Kepatuhan terhadap SOC (Amerika Serikat)

Laporan Kontrol Organisasi Layanan (SOC) berfokus pada prinsip kepercayaan, seperti keamanan, ketersediaan, dan kerahasiaan. Pemenuhan standar yang ditetapkan oleh AICPA ini mewajibkan audit internal yang ketat dan transparansi operasional, terutama bagi organisasi yang berlokasi di AS atau berurusan dengan entitas dari AS.

Standar ISO (Global)

Diatur oleh International Organization for Standardization, standar ini menyediakan framework yang diakui secara global untuk mengelola keamanan informasi. Standar ini penting bagi organisasi multinasional yang beroperasi di wilayah seperti Uni Eropa, Amerika Serikat, dan Asia-Pasifik untuk menetapkan kebijakan keamanan yang konsisten.

Mengaudit Data Anda

Langkah selanjutnya bersifat internal yaitu memetakan lingkungan data Anda. Di mana data Anda berada? Siapa yang memiliki akses? Apa saja kekurangan yang ada di sistem Anda saat ini? Menjawab pertanyaan ini adalah dasar dari strategi kepatuhan Anda.

Misalnya:

- Penyedia layanan kesehatan mungkin mendapati bahwa data sensitif pasien disimpan di berbagai layanan cloud, dengan tingkat enkripsi yang berbeda-beda. Berbagi data lintas negara untuk penelitian semakin mempersulit kepatuhan terhadap GDPR (Eropa) dan HIPAA (Amerika Serikat).
- Dalam kasus ini, audit data dapat mengungkapkan risiko, seperti data yang tidak terenkripsi atau izin akses yang tidak jelas, yang harus ditangani untuk memenuhi persyaratan peraturan.

Dengan menyelaraskan insight ini dengan peraturan eksternal, organisasi dapat menjembatani kesenjangan antara mandat kepatuhan dan realitas operasional.





Membentuk tim Anda

Kedaulatan data bukan hanya merupakan tantangan dari sisi teknis, tetapi juga dari segi kolaboratif. Membangun tim lintas fungsi yang tepat sangat penting:

- **Pemimpin IT** dapat memetakan infrastruktur teknis Anda dan mengatasi enkripsi atau kesenjangan penyimpanan.
- **Tim hukum** dapat menafsirkan persyaratan peraturan regional dan memastikan kontrak mencerminkan kebutuhan kepatuhan.
- **Unit bisnis** dapat membantu mengidentifikasi dampak praktis pada operasi sehari-hari, seperti izin akses dan gangguan alur kerja.

Tim ini harus bekerja sama untuk menyelaraskan proses internal Anda dengan tuntutan dari berbagai framework, seperti GDPR, SOC, atau ISO, di wilayah masing-masing.

Perencanaan Proaktif

Peraturan terus berkembang, begitu juga kebutuhan bisnis. Dengan mengambil langkah-langkah ini sekarang, organisasi dapat melampaui kepatuhan yang dicapai secara reaktif dan membangun framework yang mendukung pertumbuhan di masa depan.

Sebagai contoh, mengadopsi solusi seperti **Assured Controls di Google Workspace** dapat memberikan dasar untuk memenuhi persyaratan residensi dan akses data, sehingga dapat menjamin kepatuhan sekaligus menjaga fleksibilitas.



Residensi data dan kontrol akses

02

Residensi data tidak hanya menyangkut lokasi data Anda, tetapi juga tentang memastikan Anda memiliki kontrol atas cara data disimpan, diakses, dan diproses, dengan tetap menjaga keseimbangan antara performa, skalabilitas, dan kepatuhan.

Bagi organisasi yang menangani data sensitif dalam jumlah besar, alat seperti Assured Controls di Google Workspace menyederhanakan kepatuhan tanpa mengganggu operasi.

“Kami melakukan analisis ekstensif terhadap pemrosesan data di region, dan prosesnya berjalan lancar, sehingga mengurangi kebutuhan integrasi pihak ketiga yang mahal dan kompleks. Selain itu, kami tidak mengalami kasus malfungsi atau kelambatan. Semua berjalan lancar.”

Roman Spantgar, Product Owner Global Collaboration di Randstad

Residensi data lokal vs. fleksibilitas

Bagi banyak organisasi, tantangan yang dihadapi adalah menemukan keseimbangan yang tepat antara memenuhi persyaratan residensi yang ketat dan menjaga agar mereka tetap gesit dalam menjalankan kegiatan operasional. Misalnya, organisasi yang berekspansi secara global sering kali perlu mengakomodasi peraturan regional dan juga tuntutan kinerja.

Hal ini menimbulkan dilema umum: bagaimana organisasi dapat mematuhi peraturan tanpa membangun sistem terpisah yang mengganggu kolaborasi? Assured Controls di Google Workspace menjawab masalah ini dengan menawarkan fleksibilitas terperinci yaitu Anda dapat menentukan tempat penyimpanan dan pemrosesan data sekaligus mempertahankan skalabilitas cloud. Bagi bisnis multinasional, hal ini berarti kemampuan menetapkan kebijakan residensi data untuk masing-masing tim, departemen, atau wilayah tanpa mengorbankan performa.

Pemrosesan data: bukan sekadar penyimpanan

Banyak organisasi sangat berfokus pada lokasi penyimpanan data mereka, tetapi mengabaikan tempat pemrosesannya. Padahal, hal tersebut merupakan faktor kepatuhan penting dalam framework seperti GDPR. Pemrosesan data mengacu pada cara data Anda digunakan, dianalisis, atau dibagikan, dan sering kali memerlukan pengawasan lebih ketat dibanding hanya penyimpanan. Assured Controls tidak hanya mencakup penyimpanan. Dengan melokalkan penyimpanan dan pemrosesan, kedaulatan data menyeluruh bagi organisasi dapat dipastikan terpenuhi.



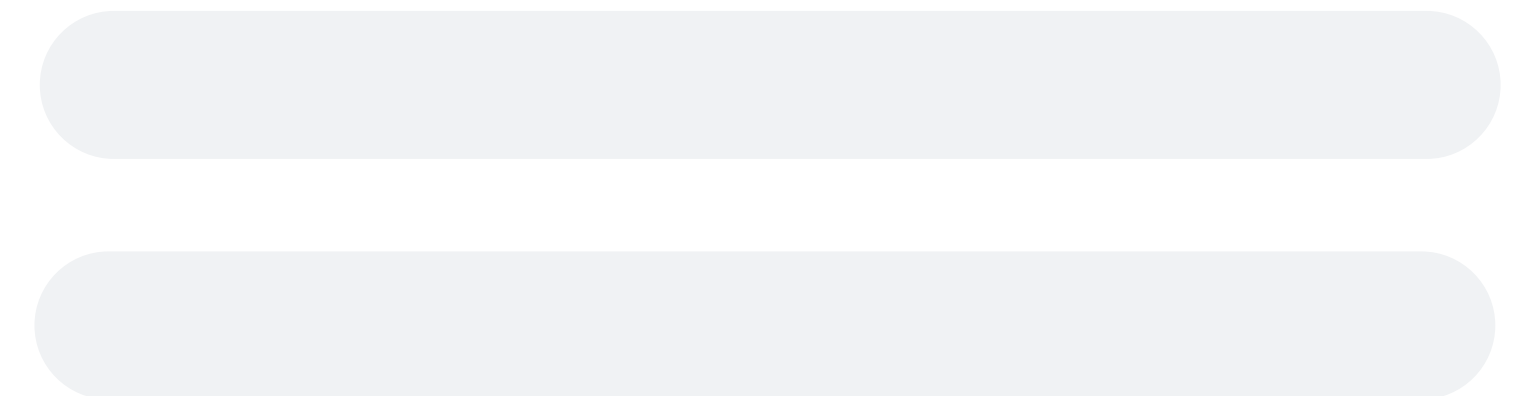


Memenuhi kepatuhan bidang perawatan kesehatan di AS

Hukum federal seperti HIPAA telah menetapkan standar nasional untuk perlindungan data pasien, tetapi hukum negara bagian memberikan kompleksitas tambahan. Peraturan seperti CCPA California dan CDPA Virginia menetapkan persyaratan yang lebih ketat terkait privasi data, hak konsumen, dan periode retensi. Pemrosesan data yang dilokalkan membantu penyedia layanan kesehatan melaksanakan amanat peraturan yang tumpang tindih tersebut dengan percaya diri.

Mempersiapkan diri menghadapi perubahan peraturan di masa mendatang

Kedaulatan data adalah target yang terus berubah. Pemerintah terus menyempurnakan peraturan yang ada dan memperkenalkan peraturan baru, sehingga menimbulkan ketidakpastian bagi bisnis. Sistem yang kaku dan dirancang untuk memenuhi aturan saat ini mungkin akan kesulitan beradaptasi di masa mendatang. Assured Controls di Google Workspace menawarkan fleksibilitas untuk menyesuaikan kebijakan residensi data seiring berkembangnya peraturan. Apakah itu berarti memigrasikan data antar-region ataupun menyempurnakan kontrol akses, tujuannya adalah memastikan agar postur kedaulatan data Anda tetap sejalan dengan perubahan.





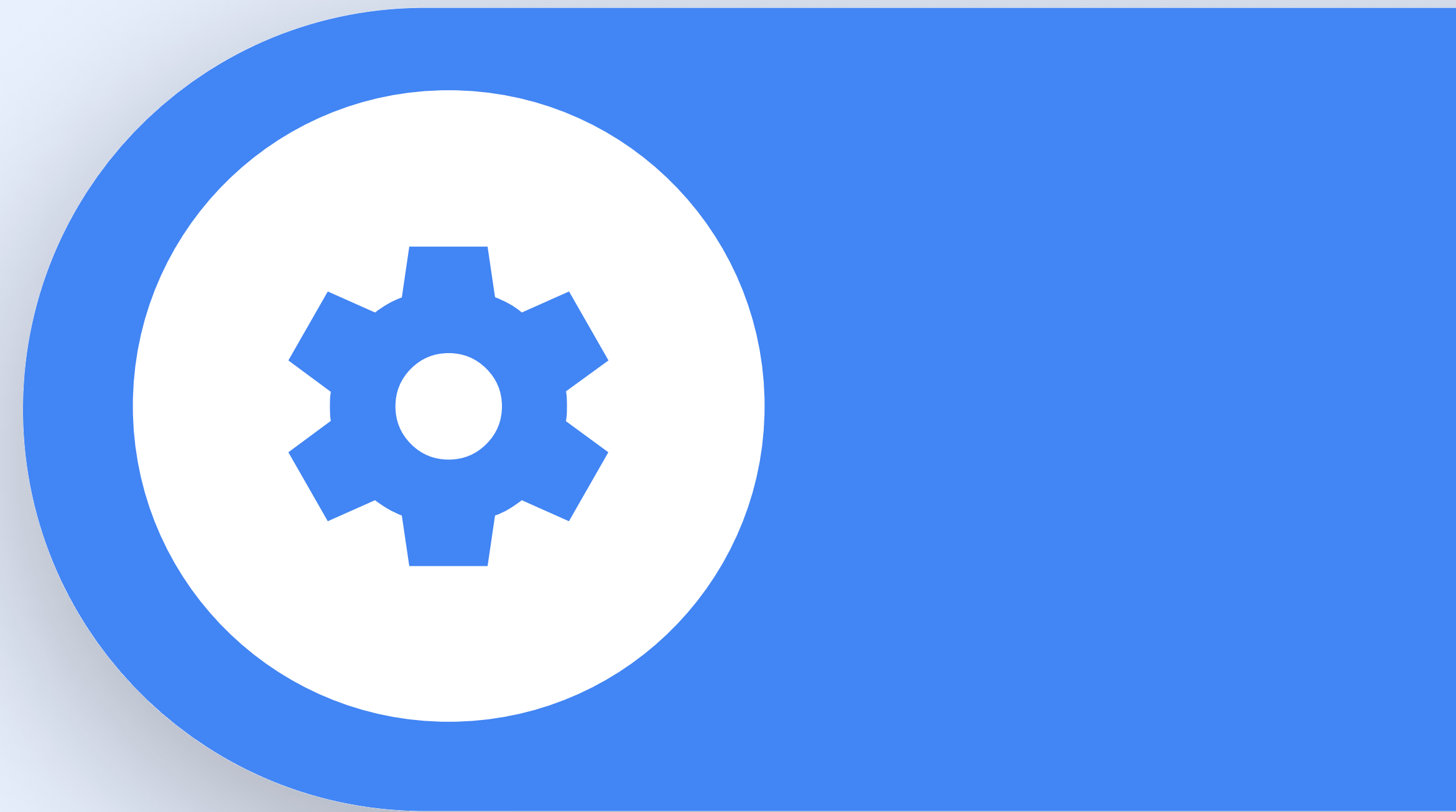
03

Memperbaiki kontrol akses

Setelah data Anda disimpan dengan aman, langkah berikutnya adalah memastikan bahwa aksesnya juga dilindungi. Dengan menerapkan prinsip hak istimewa terendah, organisasi dapat menjamin bahwa informasi sensitif hanya dapat diakses oleh pihak yang benar-benar memerlukannya. Dengan memperketat siapa yang dapat melihat apa, organisasi dapat mengurangi risiko kebocoran yang tidak disengaja, penyalahgunaan internal, dan kerentanan pihak ketiga.

Mengapa kontrol akses itu penting

Akses data yang tidak dibatasi merupakan risiko yang terus meningkat dalam kondisi saat ini. Pemberian izin berlebihan secara internal meningkatkan eksposur terhadap kebocoran dan error; akses pihak ketiga dapat mempersulit kepatuhan; dan berbagai peraturan, seperti GDPR, HIPAA, serta framework lainnya, menuntut pengawasan yang lebih ketat terhadap pihak yang dapat mengakses informasi sensitif.



Cara menyempurnakan akses

Alat yang tepat membantu organisasi menerapkan kebijakan akses yang lebih cerdas dan aman:



Framework zero-trust

Prinsip “Jangan percaya siapa pun, verifikasi semuanya” memastikan setiap pengguna, perangkat, dan koneksi diautentikasi dan diotorisasi—bahkan pengguna internal.

Role-based access control (RBAC)

Menyelaraskan izin dengan peran tertentu meminimalkan eksposur yang tidak perlu. Misalnya:

- Tim keuangan mengakses sistem pembayaran, tetapi tidak mengakses data HR.
- Penyedia layanan kesehatan melihat data perawatan pasien, tetapi tidak melihat file administratif.
- Tim dukungan hanya dapat mengakses data setelah mendapatkan persetujuan eksplisit dan untuk durasi terbatas.

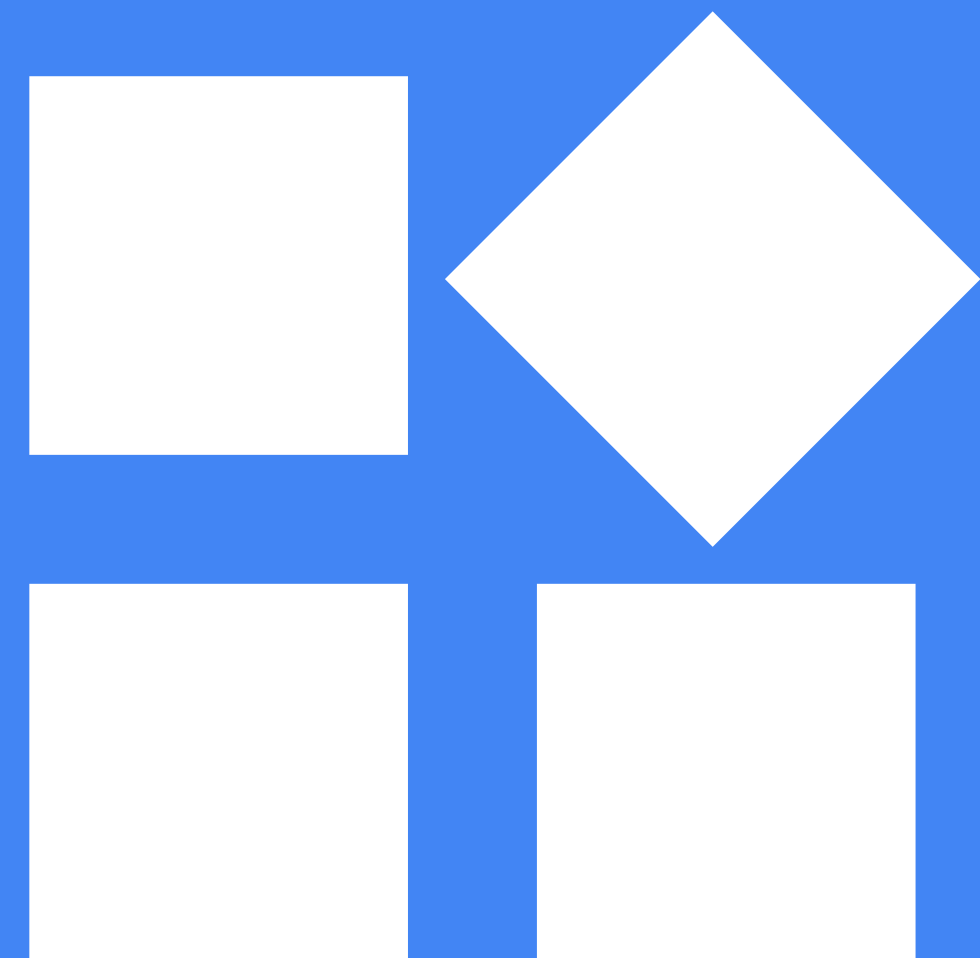
Transparansi dan persetujuan akses

Terapkan alur kerja yang memerlukan otorisasi eksplisit untuk akses pihak ketiga. Alat seperti Persetujuan Akses di Google Workspace memastikan tim dukungan hanya mengakses data jika benar-benar diperlukan—dengan visibilitas dan kontrol penuh.

Enkripsi sisi klien

Penambahan lapisan keamanan lain memastikan bisnis mengelola kunci enkripsi mereka sendiri, sehingga mencegah penyedia cloud mengakses data sensitif.

Dengan menerapkan kontrol akses yang lebih baik, organisasi dapat menyeimbangkan keamanan dan kepatuhan dengan tuntutan tempat kerja modern yang kolaboratif. Pada langkah berikutnya, kita akan mempelajari cara memperkuat langkah-langkah keamanan Anda untuk mengurangi risiko lebih lanjut dan memastikan organisasi Anda tetap terdepan dalam menghadapi ancaman siber yang terus berkembang.

**Bagikan**

Pembatasan akses tidak hanya soal keamanan, tetapi juga menyangkut operasi yang lebih cerdas.

Performa

Menyimpan data dekat dengan pengguna akhir akan mengurangi latensi, meningkatkan produktivitas, dan memastikan tim Anda dapat bekerja dengan lancar, di mana pun mereka berada.

Kepatuhan

Menyimpan data di wilayah yang sama menghindari risiko hukum dan memastikan kepatuhan terhadap berbagai framework, seperti GDPR, HIPAA, dan peraturan lain yang terus berkembang.

Keamanan dan Pencegahan Kebocoran Data (DLP)

04

Setelah data disimpan dengan aman dan kontrol akses disempurnakan, langkah penting berikutnya adalah melindungi organisasi Anda dari ancaman yang terus berkembang. Assured Controls di Google Workspace menyediakan enkripsi sisi klien tingkat lanjut, kontrol akses terperinci, dan alat DLP (Pencegahan Kebocoran Data) yang tangguh untuk memastikan data Anda tetap aman di setiap tahap—baik saat disimpan, dalam pengiriman, atau sedang digunakan secara aktif.





Mengapa hal ini penting

Organisasi modern menghadapi tantangan keamanan yang semakin kompleks:

- **Ancaman eksternal:** Serangan phishing, malware, dan upaya akses tidak sah menjadi semakin canggih. Organisasi memerlukan langkah proaktif untuk melindungi informasi sensitif dari pelaku kejahatan.
- **Risiko internal:** Pemberian izin yang berlebihan, berbagi data secara tidak sengaja, dan kesalahan manusia tetap menjadi sebagian penyebab utama pelanggaran data. Memperketat akses dan menyematkan pengamanan teknis membantu memitigasi kerentanan ini.

Alat yang digunakan karyawan setiap hari, seperti ekstensi browser, aplikasi produktivitas, atau integrasi pihak ketiga, dapat menimbulkan kerentanan yang tidak disengaja. Entah berupa aplikasi yang tidak diperiksa yang membagikan data sensitif, izin berlebihan, ataupun eksposur ke software berbahaya, risiko ini menambah lapisan kompleksitas yang tidak terlihat pada postur keamanan Anda.

Jadi, bagaimana cara melindungi data penting sekaligus memastikan karyawan dapat bekerja dengan lancar menggunakan alat yang mereka butuhkan?

Dengan Assured Controls di Google Workspace, organisasi mendapatkan keseimbangan antara fleksibilitas dan keamanan:

- **Izin terperinci:** Membatasi akses alat pihak ketiga, sehingga dapat memastikan data sensitif tetap aman dan mengurangi eksposur yang tidak perlu.
- **Enkripsi sisi klien:** Melindungi data secara menyeluruh, bahkan saat karyawan berkolaborasi di berbagai layanan cloud. Enkripsi memastikan aplikasi atau layanan tidak sah tidak dapat membaca informasi sensitif.
- **Visibilitas dan persetujuan:** Menjaga pengawasan terhadap alat yang digunakan, mengidentifikasi potensi risiko sejak dini, dan menyetujui akses eksternal hanya jika benar-benar diperlukan.

Dengan kontrol tersemat ini, Assured Controls memberdayakan organisasi agar memberi karyawan kebebasan berinovasi dengan tetap menjaga keamanan sebagai prioritas utama. Alat tetap dapat bermanfaat, dan bukannya berbahaya.

Menambahkan lapisan pertahanan

Assured Controls juga terintegrasi secara lancar dengan framework Zero Trust, melalui penerapan filosofi “jangan percaya siapa pun, verifikasi semuanya” yang mengharuskan setiap pengguna, perangkat, dan koneksi membuktikan kredensialnya sebelum mengakses data sensitif.

Entah itu mengenkripsi file sebelum file dibagikan atau mewajibkan beberapa lapis persetujuan untuk mengizinkan akses pihak ketiga, kontrol teknis ini memastikan bahwa keamanan selalu bersifat proaktif.





Mengapa DLP itu penting

Kebijakan Pencegahan Kebocoran Data (DLP) memainkan peran penting dalam memperkuat postur keamanan Anda. Dengan alat ini, Anda dapat:

- **Memantau pergerakan data:** Melacak data sensitif saat berpindah melalui sistem Anda, mengidentifikasi dan mengatasi kebocoran atau pembagian data yang tidak sah.
- **Menetapkan kebijakan kustom:** Menentukan aturan untuk otomatis memblokir, memberi tahu, atau menandai aktivitas berbagi data yang melanggar mandat kepatuhan.
- **Melindungi kategori sensitif:** Mengidentifikasi dan mengamankan jenis data tertentu, seperti informasi identitas pribadi (PII), data keuangan, atau kekayaan intelektual.



Keamanan sering kali dianggap sebagai penghalang dan hambatan lain dalam berkolaborasi. Namun, aspek ini sebenarnya membantu bisnis beroperasi dengan percaya diri. Dengan enkripsi lanjutan, kebijakan DLP proaktif, dan proses persetujuan Assured Controls, organisasi dapat mencapai keseimbangan yang tepat antara melindungi data sensitif dan mendorong kolaborasi.

Di bagian berikutnya, kita akan melihat bagaimana pelaporan dan pengawasan dapat membantu Anda tetap proaktif dan patuh dalam lanskap peraturan yang terus berubah.



Pelaporan dan pengawasan: keyakinan melalui visibilitas

05

Kedaulatan data tidak berhenti setelah kontrol diterapkan. Hal itu juga berkaitan dengan membuktikan bahwa kontrol tersebut berfungsi. Pelaporan dan pengawasan memberi organisasi kemampuan untuk memantau, mengaudit, dan menyesuaikan strategi data mereka. Dengan visibilitas berkelanjutan di seluruh enkripsi, akses, dan penyimpanan, Anda dapat memastikan kepatuhan tidak hanya tercapai, tetapi juga terjaga. Bagi organisasi seperti Randstad, alat pelaporan real-time menyederhanakan audit dan memastikan kepatuhan yang lancar.

“Penerapan Region Data telah menjadi langkah transformatif dalam mengembangkan strategi kami untuk pemrosesan data pribadi di EU. Prosesnya lancar, dan kami tidak mengalami kendala operasional apa pun.”

Roman Spantgar, Product Owner Global Collaboration di Randstad



Anggaplah pelaporan sebagai piramida kontrol—sistem berlapis yang membangun kepercayaan di setiap tingkat:

Enkripsi sisi klien:

Enkripsi adalah dasar keamanan Anda. Namun, enkripsi hanya efektif jika diterapkan secara konsisten. Alat pelaporan mengonfirmasi bahwa data sensitif tetap terenkripsi end-to-end, mulai dari pembuatan hingga penyimpanan, sementara audit trail memvalidasi bahwa kunci enkripsi tetap berada dalam kendali Anda.

Akses kontekstual:

Akses data tidak hanya harus dikontrol, tetapi juga harus dipantau. Pelaporan real-time dapat memunculkan anomali, seperti lokasi akses yang tidak biasa, upaya login yang gagal, atau aktivitas di luar jam kerja. Visibilitas ini memungkinkan Anda mengatasi risiko sebelum terjadi insiden.

Kontrol akses terperinci:

Alat pengawasan membantu Anda melihat siapa yang memiliki akses ke apa, kapan, dan mengapa. Dengan membuat log dan laporan akses yang jelas, Anda dapat mengidentifikasi peran yang memiliki izin berlebihan, memantau akses sementara (misalnya, untuk tim dukungan), dan tetap mematuhi framework-framework, seperti GDPR dan HIPAA.

Penyimpanan data lokal:

Bagi industri yang memiliki persyaratan residensi yang ketat, transparansi adalah segalanya. Alat pelaporan memverifikasi bahwa data tetap tersimpan di tempat seharusnya—baik di negara bagian maupun wilayah tertentu—sehingga memberikan bukti yang dibutuhkan oleh tim IT dan badan pengatur terkait.

Region data:

Ingin berekspansi ke pasar baru? Dasbor pelaporan memberikan kejelasan tentang tempat data disimpan, diproses, dan diakses, sehingga bisnis dapat menyesuaikan kebijakan seiring berkembangnya peraturan atau skala operasi secara global.

Arsitektur zero-trust:

Zero-trust berarti tidak pernah berasumsi—selalu memverifikasi. Alat pelaporan mencatat setiap permintaan akses, perangkat, dan tindakan pengguna, sehingga memastikan kebijakan data ditegakkan sekaligus memudahkan pemantauan aktivitas dan deteksi pola mencurigakan.



Mengapa visibilitas itu penting

Tanpa pelaporan yang kuat, kepatuhan bisa terasa seperti bermain tebak-tebakan. Organisasi perlu membuktikan bahwa mereka dapat memenuhi persyaratan peraturan sekaligus tetap cukup tangkas untuk merespons ancaman yang muncul. Assured Controls di Google Workspace menyediakan alat pengawasan yang Anda perlukan untuk memantau, memverifikasi, dan menyesuaikan strategi data dengan percaya diri.

- **Menyederhanakan audit:** Membuat laporan siap kepatuhan yang selaras dengan beragam framework, seperti GDPR, HIPAA, dan SOC 2. Assured Controls menyederhanakan pelaporan untuk tim IT dan kepatuhan, dengan memberikan log terperinci dan dapat diaudit dari semua aktivitas data dengan hanya sekali klik.
- **Tetap memegang kendali:** Dasbor real-time menunjukkan adanya risiko sejak dini, sementara log aktivitas transparan melacak setiap tindakan, persetujuan, atau perubahan. Tim mendapatkan visibilitas yang diperlukan untuk mengatasi risiko, menguji tata kelola, dan menjaga kepercayaan.

Dengan insight real-time, pelaporan siap audit, dan log aktivitas transparan, Assured Controls tidak hanya membantu Anda memenuhi kepatuhan, tetapi juga membantu Anda tetap mematuhi. Dengan menyediakan alat untuk memantau, memverifikasi, dan beradaptasi, organisasi dapat dengan percaya diri menunjukkan kontrol atas data mereka sekaligus mengurangi risiko terjadinya hal yang tidak diantisipasi atau ancaman yang terus berkembang.

Pelaporan yang kuat mengubah kepatuhan dari sekadar formalitas menjadi keunggulan strategis. Dengan alat untuk memantau aktivitas, memverifikasi kontrol, dan merespons secara proaktif, organisasi dapat percaya diri dalam beradaptasi dengan risiko dan peraturan yang terus berkembang dengan tetap memupuk kepercayaan.





05

Kesimpulan



Assured Controls di Google Workspace



dapat membantu mendorong organisasi mewujudkan kedaulatan data dengan upaya minimal melalui perpaduan alat kepatuhan yang canggih dengan fleksibilitas dan skalabilitas cloud. Add-on ini memberikan kontrol terperinci atas penyimpanan, pemrosesan, dan akses data sekaligus membekali bisnis dalam beradaptasi dengan peraturan yang terus berkembang. Baik untuk melindungi kekayaan intelektual di bidang kedirgantaraan maupun mengelola data pelanggan sensitif di bidang keuangan, Assured Controls memberdayakan organisasi untuk berfokus pada kolaborasi, pertumbuhan, dan inovasi.

[Pelajari lebih lanjut](#) →