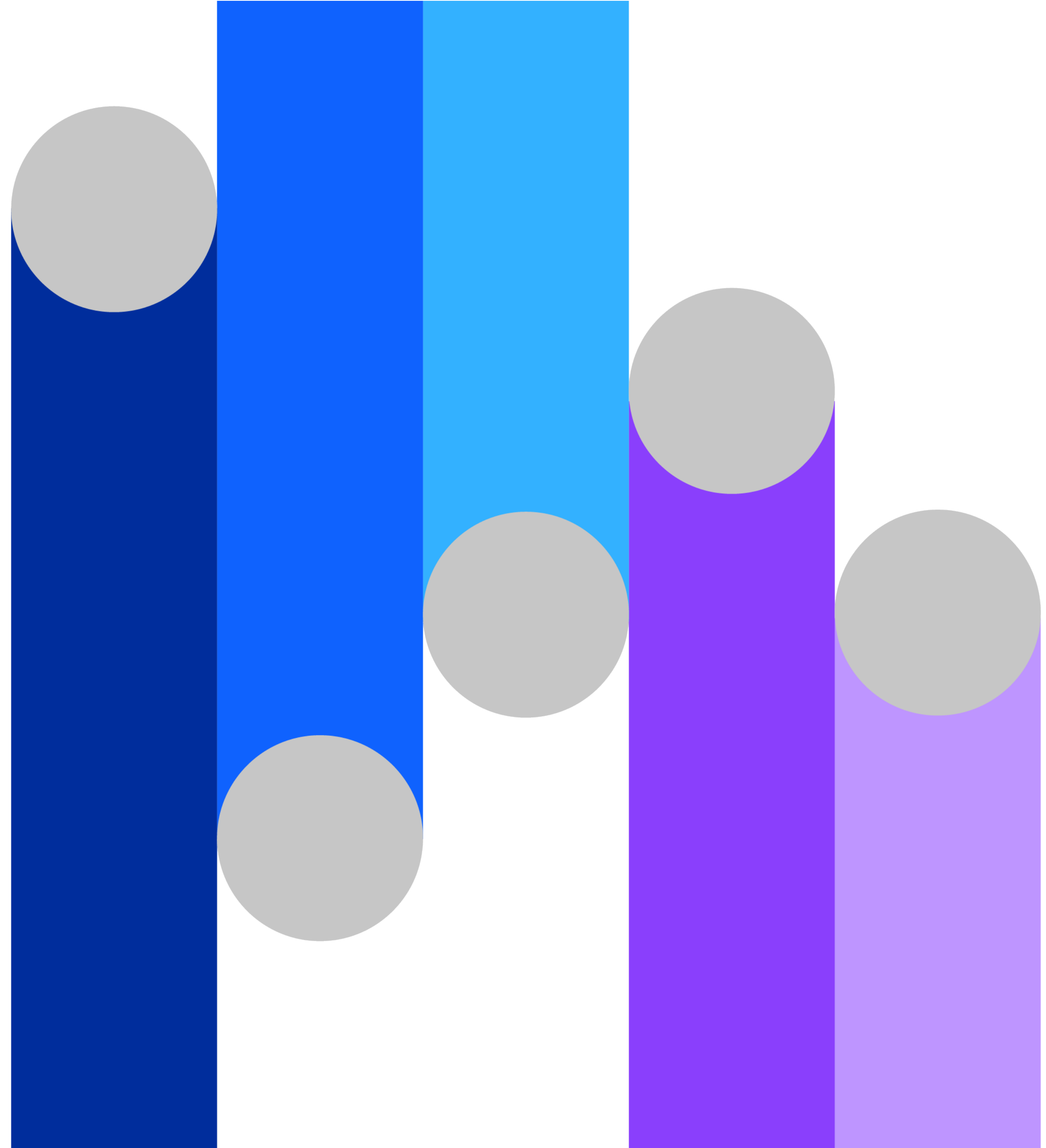


Lima masalah keamanan data yang umum untuk dihindari

Pelajari cara meningkatkan keamanan data dan sikap kepatuhan Anda



Daftar Isi

[00 →](#)

Pendahuluan

[01 →](#)

Masalah 1:

Kegagalan untuk
melampaui kepatuhan

[02 →](#)

Masalah 2: Kegagalan untuk
menyadari perlunya keamanan
data terpusat

[03 →](#)

Masalah 3: Kegagalan untuk
menentukan siapa yang
bertanggung jawab atas data

[04 →](#)

Masalah 4: Kegagalan untuk
menangani kerentanan yang
diketahui

[05 →](#)

Masalah 5: Kegagalan
memprioritaskan dan
menggunakan pemantauan
aktivitas data modern

[06 →](#)

Apa berikutnya?

[07 →](#)

Mengapa IBM Security?

Pendahuluan

Keamanan data harus menjadi prioritas utama bagi perusahaan, dan hal itu beralasan

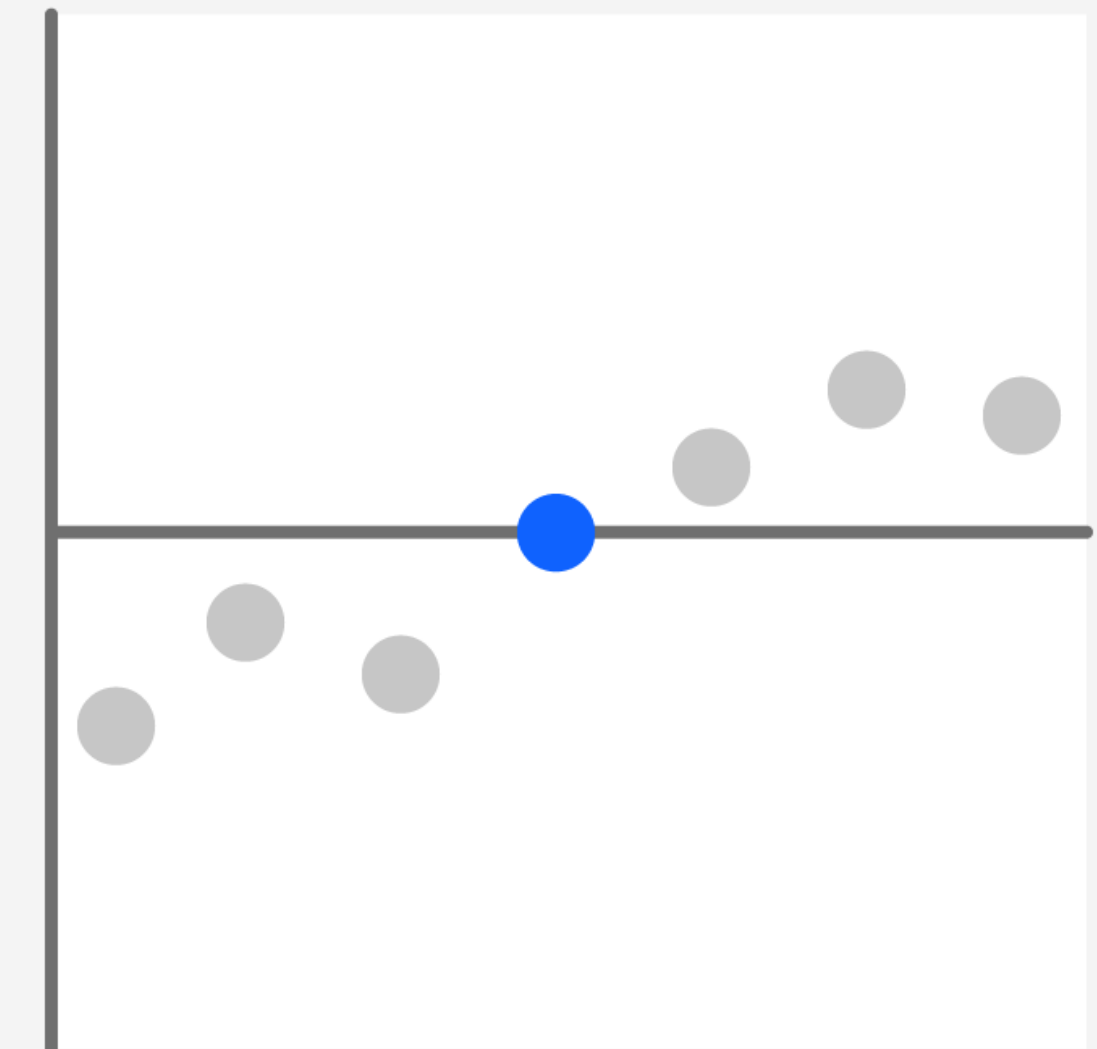
Bahkan ketika lanskap TI menjadi semakin terdesentralisasi dan kompleks, penting untuk dipahami bahwa banyak pelanggaran data dapat dicegah. Meskipun tantangan dan tujuan keamanan siber individu mungkin berbeda dari satu perusahaan ke perusahaan lainnya, sering kali organisasi juga melakukan kesalahan sama yang tersebar luas ketika mereka mulai menangani keamanan data. Terlebih lagi, banyak pimpinan perusahaan sering menerima kesalahan ini sebagai praktik bisnis yang normal.

Ada beberapa faktor internal dan eksternal yang dapat menyebabkan serangan siber berhasil, antara lain:

- Erosi perimeter jaringan
- Peningkatan permukaan serangan yang ditawarkan oleh lingkungan TI yang lebih kompleks
- Meningkatnya tuntutan layanan cloud yang menampung praktik-praktik keamanan siber
- Semakin canggihnya jenis kejahatan siber
- Kekurangan keterampilan akan keamanan siber yang terjadi terus-menerus
- Kurangnya kesadaran karyawan seputar risiko keamanan data

USD 4,45 JUTA

Rata-rata kerugian global akibat pelanggaran data meningkat pada 2023, naik 15% dalam kurun waktu 3 tahun.¹



Masalah 1: Kegagalan untuk melampaui kepatuhan

Kepatuhan tidak selalu sama dengan keamanan data. Organisasi yang memfokuskan sumber daya keamanan data mereka yang terbatas hanya untuk mematuhi audit atau sertifikasi dapat menjadi berpuas diri. Banyak pelanggaran data besar terjadi di organisasi yang sangat patuh pada peraturan di atas kertas. Contoh berikut menunjukkan bagaimana fokus hanya pada kepatuhan dapat mengurangi keamanan yang efektif.

Cakupan tidak lengkap

Perusahaan sering kali berjuang untuk menangani ketidaksesuaian basis data alamat dan kebijakan akses yang ketinggalan zaman sebelum audit tahunan. Penilaian kerentanan dan risiko semestinya menjadi aktivitas yang terus berlangsung.

Upaya minimal

Banyak bisnis mengadopsi solusi keamanan data hanya untuk memenuhi persyaratan hukum atau mitra bisnis. Pola pikir "mari terapkan standar minimum dan kembali berbisnis" dapat bertentangan dengan praktik keamanan siber yang baik. Keamanan data yang efektif adalah lari maraton dan bukan lari sprint.

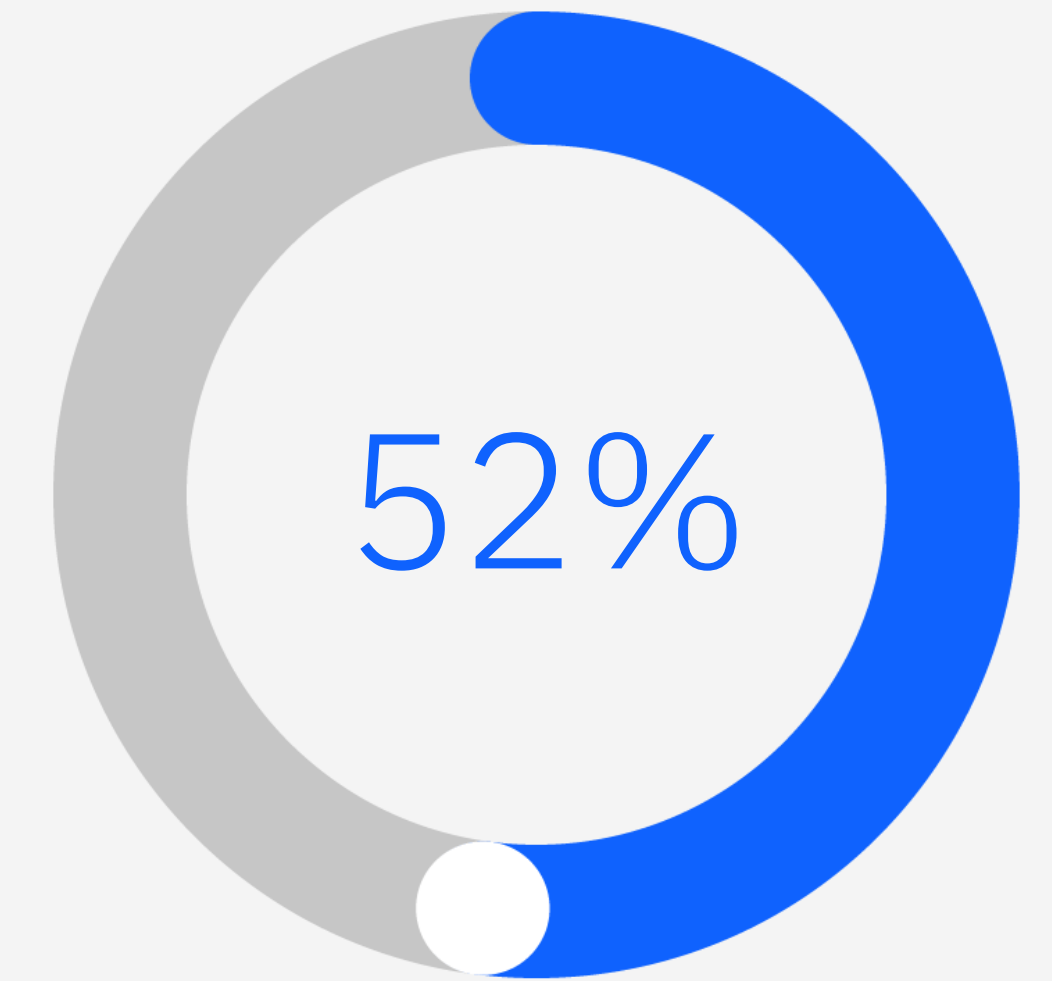
Memudarnya urgensi

Dunia usaha dapat berpuas diri dalam mengelola kontrol ketika peraturan sempurna, seperti Sarbanes-Oxley Act (SOX), General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS) dan California Privacy Rights Act (CPRA), sebelumnya dikenal sebagai CCPA.

Sementara itu, seiring berjalannya waktu, pimpinan dapat menjadi kurang perhatian pada privasi, keamanan, dan perlindungan data yang diregulasi, risiko dan biaya terkait ketidakpatuhan tidak hilang.

Penghilangan data yang tidak diregulasi

Aset, seperti kekayaan intelektual, dapat membahayakan organisasi Anda jika hilang atau dibagikan kepada personel yang tidak berwenang. Berfokus hanya pada kepatuhan dapat mengakibatkan organisasi keamanan data mengabaikan dan kurang melindungi data berharga.



52% organisasi mengatakan kompleksitas yang disebabkan karena pengalihan beban kerja ke cloud publik juga telah mengakibatkan pemenuhan kewajiban kepatuhan menjadi lebih sulit.²

Pandang kepatuhan sebagai peluang untuk berinovasi dan meningkatkan standar keamanan untuk mendukung bisnis Anda.

Solusi: Sadari dan terima bahwa kepatuhan adalah titik awal

Organisasi keamanan data harus membentuk program strategis yang secara konsisten melindungi data penting bisnis mereka, dan sebaliknya bukan sekadar merespons persyaratan kepatuhan.

Program keamanan data dan kepatuhan harus mencakup praktik inti berikut:

- Menemukan dan mengklasifikasikan data sensitif Anda di seluruh on premises, penyimpanan data cloud, dan aplikasi perangkat lunak sebagai layanan (SaaS).
- Menilai risiko dengan insight dan analisis kontekstual.

- Melindungi data sensitif melalui enkripsi dan kebijakan akses fleksibel.
- Memantau akses data dan pola pemakaian untuk mengungkap aktivitas mencurigakan dengan cepat.
- Menanggapi ancaman secara real time.
- Memudahkan kepatuhan dan pelaporannya.

Elemen terakhir dapat mencakup pertanggungjawaban hukum yang terkait dengan kepatuhan regulasi, kemungkinan kerugian yang dapat diderita oleh suatu bisnis, dan potensi biaya yang diakibatkannya selain denda ketidakpatuhan.

Pada akhirnya, Anda harus berpikir secara holistik tentang risiko dan nilai data yang ingin Anda amankan.

Masalah 2: Kegagalan untuk menyadari perlunya keamanan data terpusat

Masalah 2: Kegagalan untuk menyadari perlunya keamanan data terpusat

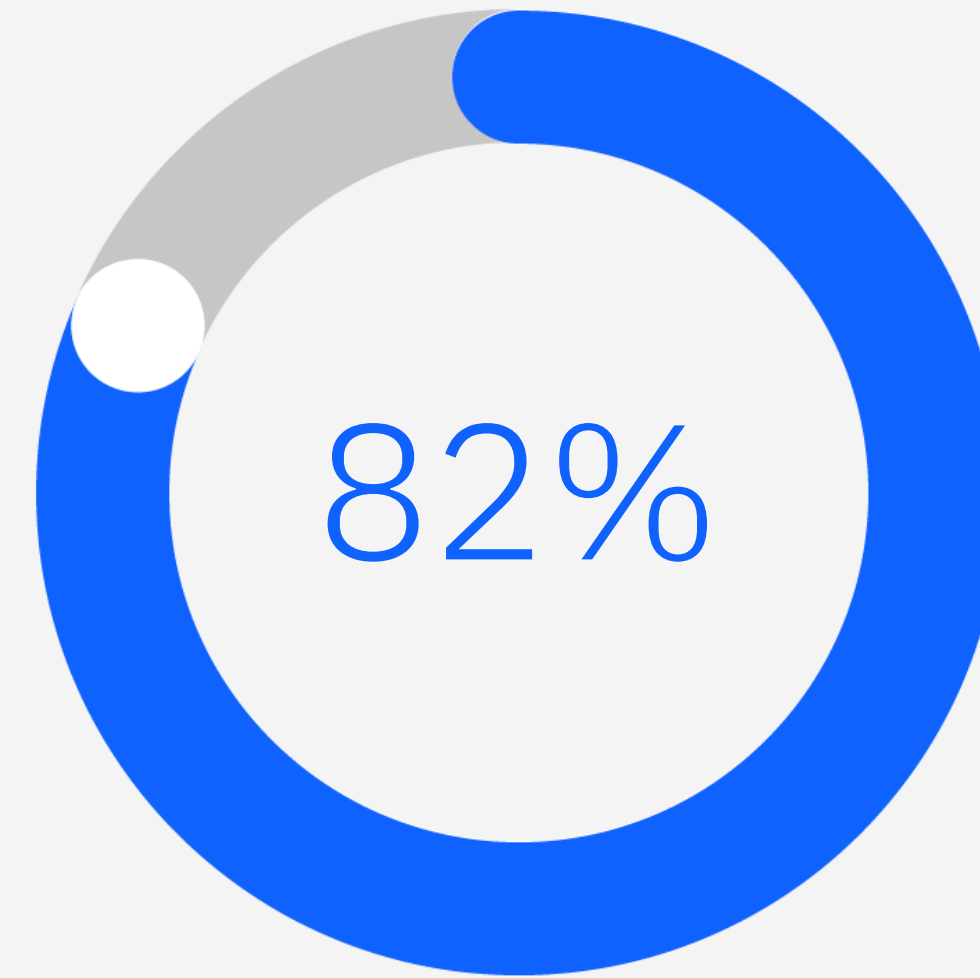
Tanpa mandat kepatuhan yang lebih luas yang mencakup privasi data dan keamanan, pimpinan organisasi dapat kehilangan pandangan tentang perlunya keamanan data yang konsisten di seluruh perusahaan.

Untuk perusahaan dengan lingkungan multicloud hybrid, yang terus berubah dan berkembang, jenis sumber data baru dapat muncul setiap minggu atau setiap hari dan menyebarkan data sensitif dengan luas.

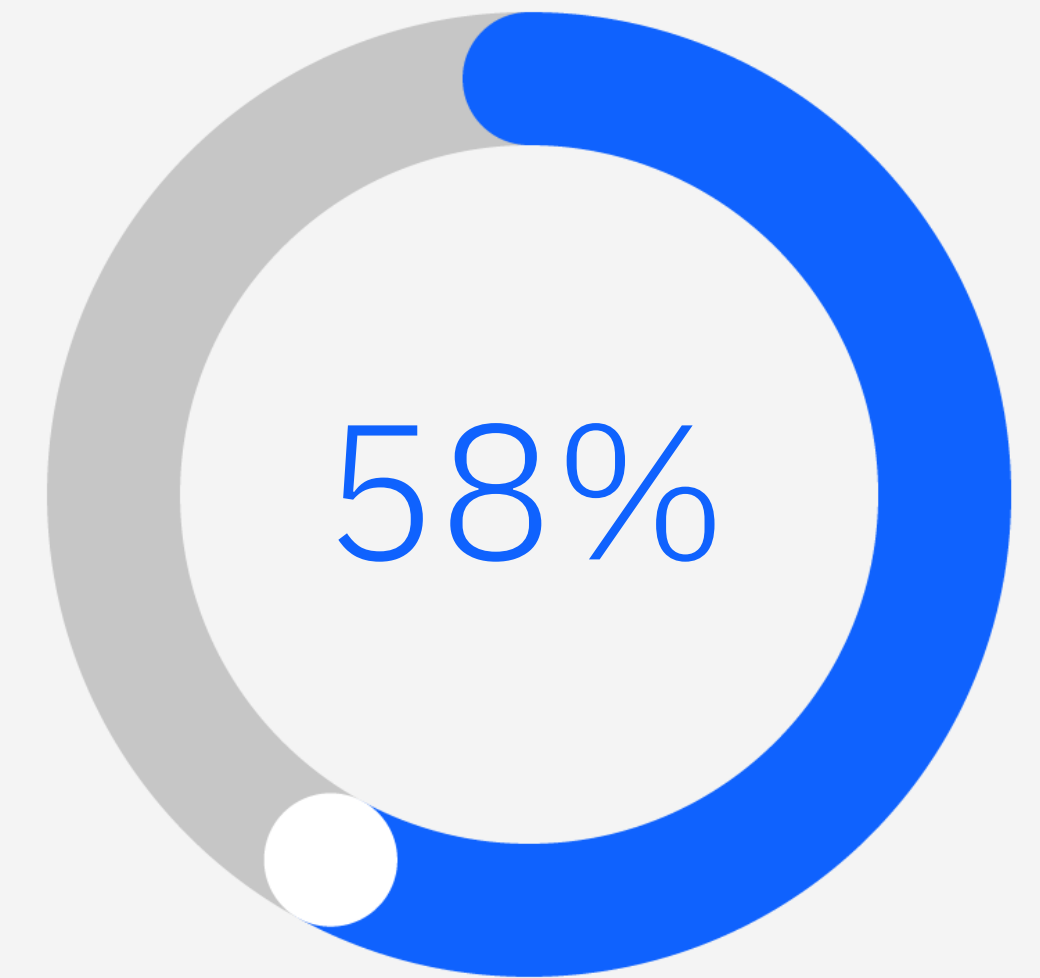
Pimpinan dari perusahaan yang sedang mengembangkan dan memperluas infrastruktur TI mereka mungkin tidak sadar akan risiko yang timbul akibat perubahan permukaan serangan mereka. Mereka bisa kekurangan visibilitas dan kontrol yang memadai seraya data sensitif mereka berkeliling di lingkungan TI yang

semakin kompleks dan berbeda. Kegagalan untuk mengadopsi kendali data privasi, keamanan, dan perlindungan yang lengkap—terutama dalam lingkungan yang kompleks—dapat menjadi pengawasan yang sangat mahal.

Mengoperasikan solusi keamanan siber secara terpisah-pisah dapat menimbulkan masalah tambahan. Misalnya, organisasi yang memiliki pusat operasi keamanan (SOC) dan solusi informasi keamanan dan manajemen peristiwa (SIEM) dapat mengabaikan untuk mengumpan sistem tersebut dengan wawasan yang dikumpulkan bertahap dari solusi keamanan data mereka. Demikian pula, kurangnya interoperabilitas antara tim, proses, dan alat keamanan dapat menghambat keberhasilan program keamanan siber apa pun.



82% pelanggaran melibatkan data yang disimpan di cloud.¹



58% organisasi mengatakan mereka memiliki sekitar 21% hingga 50% data sensitif yang ditempatkan di cloud tanpa pengamanan yang memadai.²

Mengamankan data sensitif harus dilakukan bersamaan dengan upaya keamanan siber Anda yang lebih luas.

■
Solusi: Ketahui di mana data sensitif Anda berada, termasuk on premises, repositori yang ditempatkan di cloud, dan aplikasi SaaS

Mengamankan data sensitif harus dilakukan bersamaan dengan upaya keamanan siber Anda yang lebih luas. Selain memahami di mana data sensitif Anda disimpan, Anda juga perlu mengetahui kapan dan bagaimana data tersebut diakses— meskipun informasi ini berubah dengan cepat. Selain itu, Anda harus berupaya mengintegrasikan keamanan data serta wawasan dan kebijakan perlindungan dengan keseluruhan program keamanan siber Anda untuk memungkinkan komunikasi yang sangat bersesuaian antar-teknologi. Solusi keamanan data yang beroperasi di berbagai lingkungan dan platform berbeda dapat membantu proses ini.

Kapan waktu yang tepat untuk mengintegrasikan keamanan data dengan kontrol keamanan siber lainnya sebagai bagian dari praktik keamanan siber yang lebih holistik? Berikut adalah beberapa tanda yang menunjukkan bahwa organisasi Anda siap mengambil langkah selanjutnya.

Risiko kehilangan data berharga

Nilai data pribadi, sensitif, dan hak milik organisasi Anda begitu signifikan sehingga kehilangan data tersebut akan menyebabkan kerugian yang sangat besar terhadap kelangsungan bisnis Anda.

Masalah 2: Kegagalan untuk menyadari perlunya keamanan data terpusat

Implikasi regulasi

Organisasi Anda mengumpulkan dan menyimpan data yang memiliki persyaratan hukum, seperti nomor kartu kredit, informasi pembayaran lainnya, atau data pribadi.

Kurangnya pengawasan keamanan siber

Organisasi Anda telah berkembang ke titik ketika sulit untuk melacak dan mengamankan semua titik akhir jaringan, termasuk contoh cloud. Misalnya, apakah Anda memiliki gagasan yang jelas tentang di mana, kapan, dan bagaimana data disimpan, dibagikan, dan diakses di seluruh on premises, penyimpanan data cloud, dan aplikasi SaaS Anda?

Penilaian yang tidak memadai

Organisasi Anda telah mengadopsi pendekatan terbagi-bagi di mana tidak ada pemahaman yang jelas tentang apa yang sebenarnya dibelanjakan di seluruh aktivitas keamanan siber Anda. Misalnya, apakah ada proses yang berlaku untuk mengukur keuntungan atas investasi (ROI) Anda secara akurat dalam kaitannya dengan alokasi sumber daya untuk mengurangi risiko keamanan data?

Jika salah satu situasi ini terjadi pada organisasi Anda, maka Anda semestinya mempertimbangkan untuk memperoleh keterampilan dan solusi keamanan siber yang diperlukan untuk mengintegrasikan keamanan data ke dalam praktik keamanan Anda yang lebih luas saat ini.



Masalah 3: Kegagalan untuk menentukan siapa yang bertanggung jawab atas data

Masalah 3: Kegagalan untuk menentukan siapa yang bertanggung jawab atas data

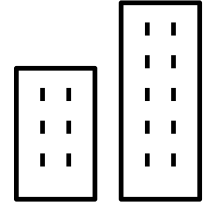
Bahkan ketika menyadari perlunya keamanan data, banyak perusahaan tidak memiliki seseorang yang khusus untuk menangani perlindungan data sensitif. Situasi ini sering terlihat pada waktu insiden keamanan data atau audit ketika organisasi berada di bawah tekanan untuk mencari tahu siapa yang bertanggung jawab.

Para eksekutif puncak mungkin akan menuding Chief Information Officer (CIO) yang mungkin bilang, "Tugas kami adalah menjaga sistem utama tetap berjalan. Silakan bicara dengan salah seorang di staf TI saya." Karyawan IT tersebut mungkin bertanggung jawab atas beberapa database yang menyimpan data sensitif, namun anggaran keamanan siber tidak mencukupi.

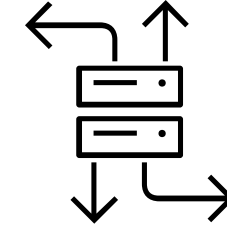
Biasanya, anggota Chief Information Security Officer (CISO) dari suatu organisasi tidak bertanggung jawab langsung atas data yang mengalir melalui bisnis secara keseluruhan. Mereka mungkin memberikan saran kepada manajer lini bisnis (LOB) yang lain dalam suatu perusahaan, namun di banyak perusahaan, tidak ada seorang pun yang secara gamblang bertanggung jawab atas data itu sendiri. Bagi organisasi, data adalah salah satu aset paling berharga. Namun, tanpa tanggung jawab kepemilikan, mengamankan data sensitif dengan sepatutnya akan menjadi tantangan.



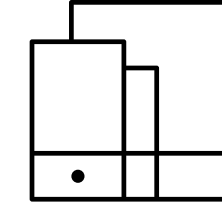
Dalam lingkungan TI yang kompleks,
penting untuk memperhitungkan data
di lokasi berikut:



Yang dibagikan di
seluruh unit bisnis



Yang ditempatkan di
infrastruktur multicloud
hybrid



Yang disimpan di
di perangkat seluler

Solusi: Pekerjakan CDO atau DPO yang dikhususkan untuk keberadaan dan keamanan aset data yang sensitif dan penting

Chief Data Officer (CDO) atau Data Protection Officer (DPO) dapat menangani tugas-tugas ini. Faktanya, perusahaan yang berbasis di Eropa atau melakukan bisnis dengan subjek data Uni Eropa menghadapi mandat GDPR yang mengharuskan mereka memiliki DPO. Prasyarat ini mengakui bahwa data sensitif—dalam hal ini informasi pribadi—memiliki nilai yang melampaui LOB yang menggunakan data tersebut. Selain itu, persyaratan ini menekankan bahwa perusahaan memiliki peran pekerjaan yang dirancang khusus untuk bertanggung jawab atas aset-aset data.

Pertimbangkan tujuan dan tanggung jawab berikut untuk memilih CDO atau DPO:

Pengetahuan teknis dan indra bisnis

Menilai risiko dan membuat contoh bisnis praktis yang dapat dipahami oleh para pemimpin bisnis non-teknis mengenai investasi keamanan data yang tepat.

Implementasi strategis

Mengarahkan rencana pada tingkat teknis yang menggunakan deteksi, respons, dan kontrol keamanan data untuk memberikan perlindungan.

Kepemimpinan kepatuhan

Memahami persyaratan kepatuhan dan Mengetahui cara memetakan persyaratan tersebut pada kontrol keamanan data sehingga bisnis Anda mematuhi.

Masalah 3: Kegagalan untuk menentukan siapa yang bertanggung jawab atas data

Pemantauan dan penilaian

Memantau lingkup ancaman dan mengukur efektivitas program keamanan data Anda.

Fleksibilitas dan penskalaan

Mengetahui kapan dan bagaimana menyesuaikan strategi keamanan data, seperti memperluas akses data dan kebijakan pemakaian di lingkungan baru dengan mengintegrasikan alat yang lebih canggih.

Pembagian tenaga kerja

Menetapkan ekspektasi dengan penyedia layanan cloud mengenai perjanjian tingkat layanan (SLA) dan tanggung jawab yang terkait dengan risiko keamanan data dan remediasi.

Rencana respons pelanggaran data

Terakhir, bersiaplah untuk memainkan peran kunci dalam memikirkan rencana mitigasi dan respons pelanggaran yang strategis.

Pada akhirnya, CDO atau DPO harus memimpin dalam mendorong kolaborasi keamanan data di seluruh tim dan keseluruhan perusahaan Anda, karena semua orang perlu bekerja sama untuk melindungi data perusahaan secara efektif. Kolaborasi ini dapat membantu CDO atau DPO mengawasi program dan perlindungan yang dibutuhkan organisasi Anda untuk membantu mengamankan data sensitifnya.



Masalah 4: Kegagalan untuk menanggapi kerentanan yang sudah diketahui

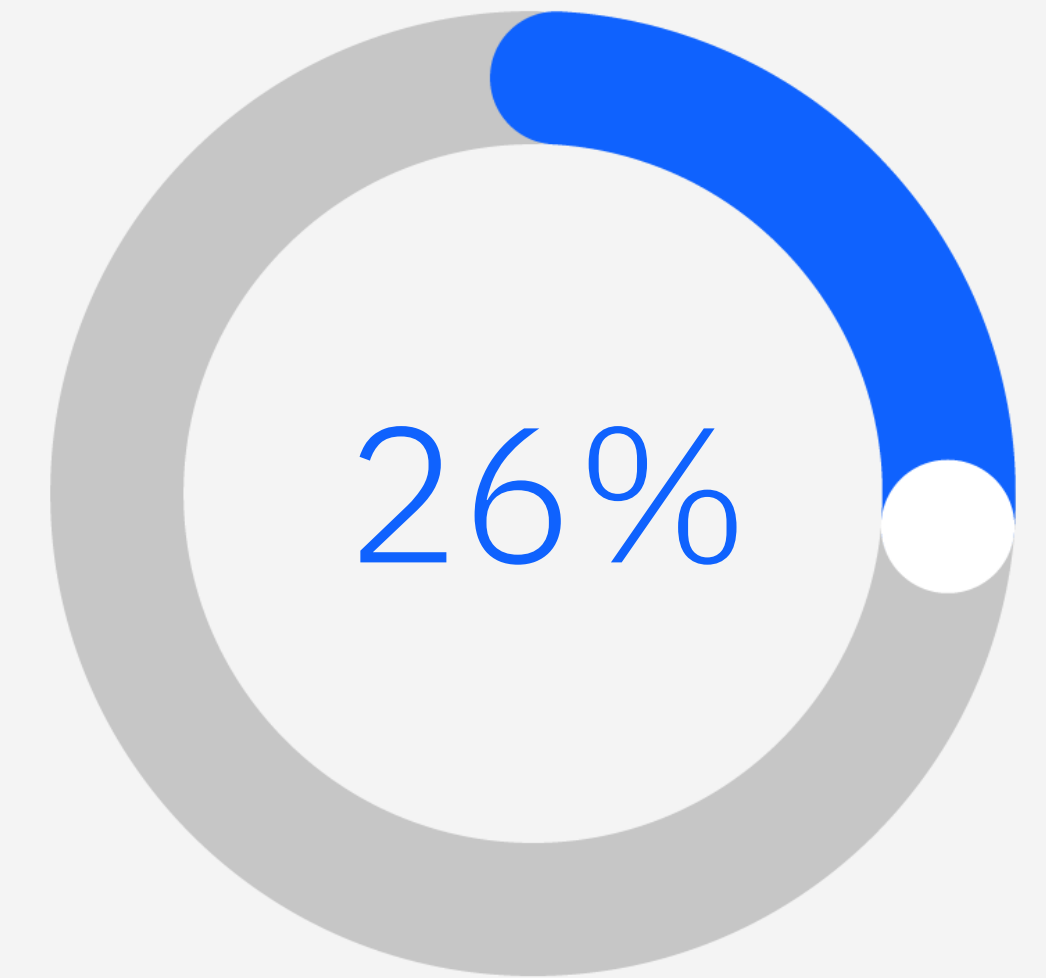
Masalah 4: Kegagalan untuk menangani kerentanan yang sudah diketahui

Pelanggaran tingkat tinggi di perusahaan sering kali disebabkan oleh kerentanan yang sudah diketahui dan tidak ditambal bahkan setelah tambalan dirilis. Kegagalan untuk segera menambal kerentanan yang sudah diketahui akan membahayakan data organisasi Anda karena penjahat siber secara aktif mencari titik-titik masuk yang mudah ini.

Namun, banyak bisnis merasa kesulitan untuk melakukan penambalan dengan cepat karena diperlukannya tingkat koordinasi antar kelompok TI, keamanan, dan operasional.

Selain itu, penambalan sering kali memerlukan pengujian untuk mengetahui apakah tambalan tersebut tidak mengganggu proses atau menimbulkan kerentanan baru.

Di lingkungan cloud, terkadang sulit untuk mengetahui apakah suatu layanan kontrak atau komponen aplikasi harus ditambal. Sekalipun ditemukan kerentanan dalam suatu layanan, penggunaannya sering kali tidak memiliki kendali atas proses remediasi penyedia layanan tersebut.



26% kerentanan baru yang telah diketahui dieksploitasi.³

Ambil sikap proaktif dengan melakukan penilaian kerentanan atas penyimpanan data Anda untuk membantu memitigasi risiko.

■
Solusi: Bentuk program manajemen kerentanan yang efektif dengan teknologi yang tepat untuk mendukung pertumbuhannya

Manajemen kerentanan biasanya melibatkan beberapa tingkat aktivitas berikut:

- Mempertahankan inventaris yang akurat dan kondisi dasar untuk aset data Anda.
- Sering melakukan pemindaian dan penilaian kerentanan di seluruh infrastruktur Anda, termasuk aset cloud.
- Memprioritaskan remediasi kerentanan yang mempertimbangkan kemungkinan kerentanan tersebut dieksploitasi dan dampak akibat peristiwa tersebut pada bisnis Anda.
- Memasukkan manajemen kerentanan dan daya tanggap sebagai bagian dari SLA dengan penyedia layanan pihak ketiga.
- Mengaburkan data sensitif atau pribadi bila memungkinkan. Enkripsi, tokenisasi, dan redaksi adalah tiga opsi untuk mencapai tujuan ini.

- Menggunakan manajemen kunci enkripsi yang tepat dan memastikan kunci enkripsi disimpan dengan aman dan disirkulasikan dengan sepatutnya untuk menjaga keamanan data terenkripsi Anda.

Bahkan dalam program manajemen kerentanan yang sempurna, tidak ada sistem yang dapat diamankan sepenuhnya. Dengan asumsi intrusi dapat terjadi bahkan di lingkungan dengan perlindungan terbaik, maka data Anda memerlukan tingkat perlindungan lain. Rangkaian teknik dan kemampuan enkripsi data yang tepat dapat membantu melindungi data Anda terhadap ancaman baru dan yang sedang berkembang.

Masalah 5: Kegagalan untuk memprioritaskan dan menggunakan pemantauan aktivitas data modern

Masalah 5: Kegagalan untuk memprioritaskan dan menggunakan pemantauan aktivitas data modern

Memantau akses dan penggunaan data adalah bagian penting dari setiap strategi keamanan data. Pimpinan organisasi perlu tahu siapa, bagaimana, dan kapan orang mengakses data. Pemantauan ini harus mencakup apakah orang-orang tersebut harus memiliki akses, apakah tingkat akses itu benar, dan apakah hal tersebut menunjukkan peningkatan risiko bagi perusahaan.

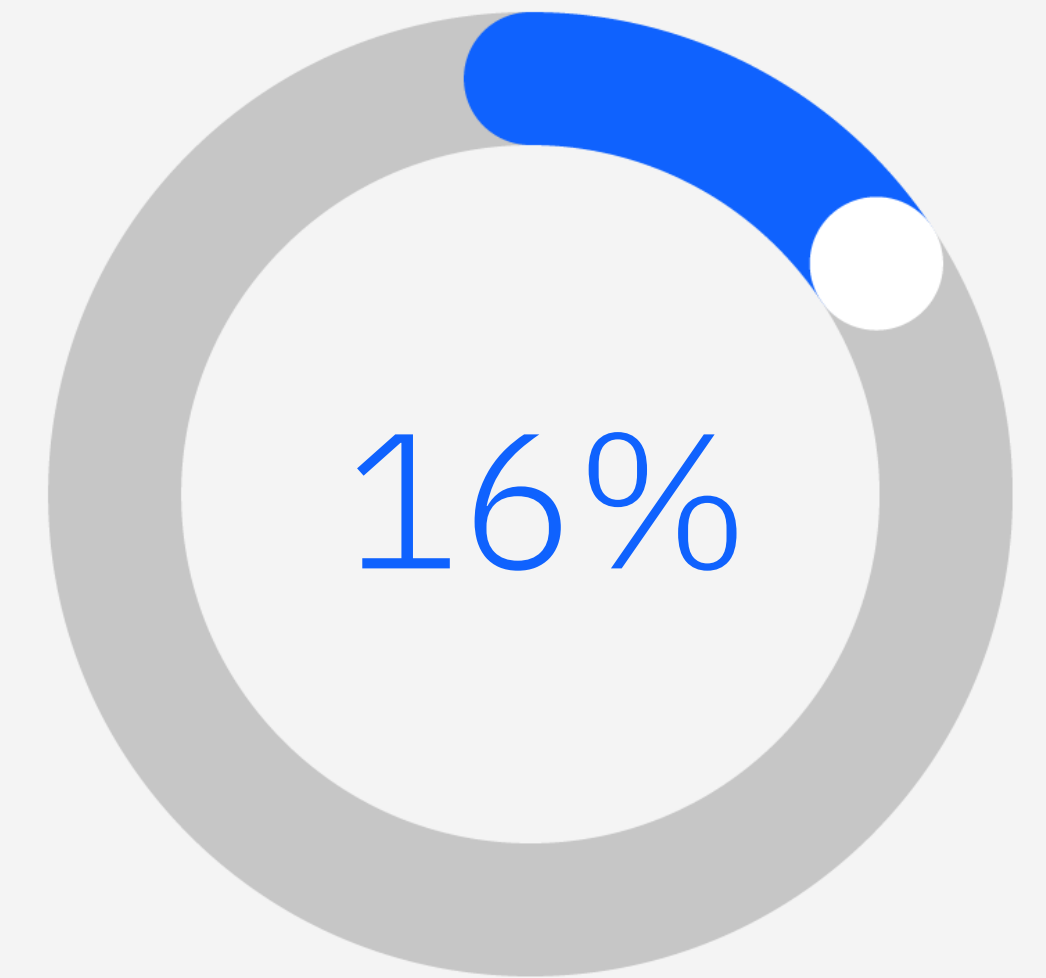
Pengguna yang memiliki hak istimewa adalah pelanggar yang umum terkait ancaman orang dalam. Rencana perlindungan data harus mencakup pemantauan real-time untuk mendeteksi akun pengguna dengan hak istimewa yang digunakan untuk aktivitas

mencurigakan atau tidak sah. Untuk mencegah kemungkinan terjadinya aktivitas berbahaya, solusi harus melakukan tugas berikut:

- Memblokir dan mengarantina aktivitas mencurigakan berdasarkan pelanggaran kebijakan.
- Menangguhkan atau menonaktifkan sesi berdasarkan perilaku yang tidak wajar.
- Menggunakan alur kerja dengan regulasi khusus yang telah ditentukan sebelumnya di seluruh lingkungan data.
- Mengirimkan peringatan yang dapat ditindaklanjuti ke keamanan TI dan sistem operasi.

Memperhitungkan keamanan data dan informasi terkait kepatuhan serta mengetahui kapan dan bagaimana merespons potensi

ancaman bisa jadi sulit. Dengan pengguna resmi yang mengakses berbagai sumber data, termasuk basis data, sistem file, lingkungan mainframe, lingkungan cloud, dan aplikasi SaaS, menyimpan data dari semua interaksi ini bisa terlihat merepotkan. Tantangannya terletak pada bagaimana secara efektif memantau, menangkap, memfilter, memproses, dan merespons volume aktivitas data yang sangat besar. Tanpa rencana yang tepat, organisasi Anda dapat memiliki lebih banyak informasi aktivitas daripada yang dapat diprosesnya secara wajar dan, pada gilirannya, mengurangi nilai pemantauan aktivitas data.



16% insiden yang teramati mengalami penyalahgunaan akun yang valid di mana musuh memperoleh dan menyalahgunakan kredensial akun yang ada sebagai sarana untuk mendapatkan akses.³

Menggunakan solusi pemantauan aktivitas data dapat membantu analis keamanan data menghemat waktu yang berharga.

Solusi: Kembangkan strategi keamanan data dan kepatuhan yang komprehensif

Untuk mencapai tujuan ini, saat memulai perjalanan keamanan data, Anda perlu mengukur dan menskala upaya pemantauan Anda agar dapat menangani persyaratan dan risiko dengan sepatutnya. Aktivitas ini sering kali melibatkan pengadopsian pendekatan bertahap yang memungkinkan pengembangan dan peningkatan praktik-praktik terbaik di seluruh perusahaan Anda. Selain itu, penting untuk melakukan diskusi dengan pemangku kepentingan bisnis utama dan TI di awal proses untuk memahami tujuan bisnis jangka pendek dan jangka panjang.

Percakapan ini juga harus menangkap teknologi yang diperlukan untuk mendukung inisiatif utama mereka. Misalnya, jika bisnis Anda berencana untuk mendirikan sejumlah kantor di wilayah baru menggunakan perpaduan antara repositori data berbasis on premises, ditempatkan di cloud, dan aplikasi SaaS, maka strategi keamanan data Anda harus menilai bagaimana rencana tersebut akan berdampak pada keamanan data dan sikap kepatuhan organisasi. Dalam hal ini, data yang dimiliki

perusahaan kini akan tunduk pada keamanan data dan persyaratan kepatuhan yang baru, seperti GDPR, CPRA, Brazil's Lei Geral de Proteção de Dados (LGPD), dan seterusnya.

Anda juga harus memprioritaskan dan fokus pada satu atau dua sumber yang kemungkinan memiliki data paling sensitif. Pastikan kebijakan keamanan data Anda jelas dan terperinci untuk sumber-sumber ini sebelum memperluas praktik-praktik ini ke seluruh infrastruktur Anda.

Anda harus mencari solusi pemantauan aktivitas data atau file otomatis dengan analitik kaya yang dapat fokus pada risiko utama dan perilaku tidak wajar oleh pengguna dengan hak istimewa. Meskipun penting untuk menerima peringatan otomatis ketika solusi pemantauan aktivitas data atau file mendeteksi perilaku abnormal, Anda juga harus dapat mengambil tindakan cepat ketika anomali atau penyimpangan dari kebijakan akses data Anda ditemukan. Tindakan perlindungan harus mencakup penyembunyian atau pemblokiran data dinamis.

Masalah 5: Kegagalan untuk memprioritaskan dan menggunakan pemantauan aktivitas data modern

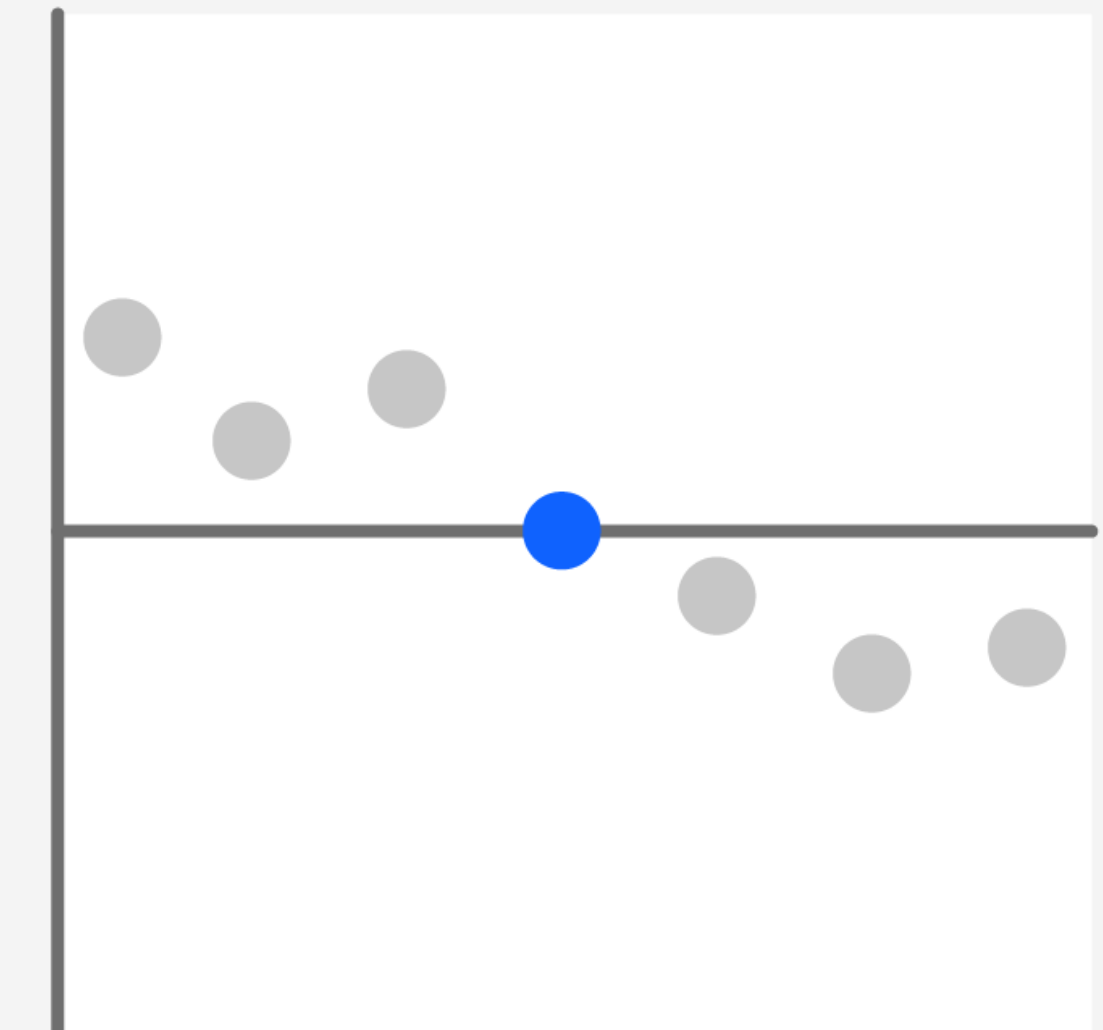
Seraya Anda mengembangkan rencana pemantauan dan perlindungan aktivitas data, sering kali berguna untuk mempertimbangkan pertanyaan-pertanyaan berikut:

- Apa dua sumber data saya yang paling sensitif?
- Lima hingga sepuluh sumber data manakah yang harus saya prioritaskan selanjutnya, berdasarkan volume data sensitifnya?
- Apakah titik akhir atau aset cloud tertentu berkaitan dengan data berisiko tinggi?
- Apakah data sensitif berpindah bolak balik dengan bebas di lingkungan on premises, hybrid, dan cloud?
- Pengguna mana yang harus diberi akses ke sumber data dan dengan persyaratan apa?
- Pengguna berisiko tinggi atau akun dengan hak istimewa seperti apa yang perlu dimatikan atau memerlukan pengawasan lebih dekat?
- Apakah solusi keamanan data saya mendukung pemantauan aktivitas real-time dan kemampuan perlindungan data otomatis?
- Apakah pemantauan real-time tersedia untuk melacak data dalam file yang berada di penyimpanan data, seperti Basis Data Structured Query Language (SQL), Distribusi Hadoop, platform Not only SQL (NoSQL), dan sebagainya?
- Apakah solusi pemantauan saya memperhitungkan penyimpanan data yang mencakup lingkungan multicloud hybrid dan memungkinkan saya membuat laporan khusus yang ditujukan kepada orang yang tepat pada waktu yang tepat?
- Apakah saya memiliki analitik risiko dan kemampuan pemantauan terfilter yang diperlukan untuk memprioritaskan risiko, kerentanan, dan upaya remediasi secara efektif?

Semakin spesifik Anda mengenai prioritas pemantauan dan persyaratan perlindungan, maka akan semakin efektif solusinya bagi Anda untuk menggunakan sumber daya deteksi dan responsnya yang tersedia.

USD 1,76 JUTA

Penghematan rata-rata untuk organisasi yang menggunakan AI keamanan dan otomatisasi secara ekstensif adalah USD 1,76 juta dibandingkan dengan organisasi yang tidak menggunakannya.¹



Bagaimana selanjutnya?

Bagaimana Anda dapat menghindari masalah keamanan data yang umum ini, khususnya karena semakin banyak perusahaan yang menguber lingkungan multicloud hybrid?

Pertama-tama pahami duduk permasalahannya dan persiapkan organisasi Anda untuk mengambil pendekatan proaktif dan holistik untuk mengamankan data, di mana pun data tersebut berada.

Jika bisnis Anda memiliki lingkungan TI yang kompleks dan hybrid, Anda tidak boleh menghasilkan pendekatan yang terpisah-pisah untuk keamanan data. Anda perlu menambahkan strategi keamanan data dan kepatuhan yang mencakup seluruh infrastruktur data dan mendukung semua jenis data Anda.

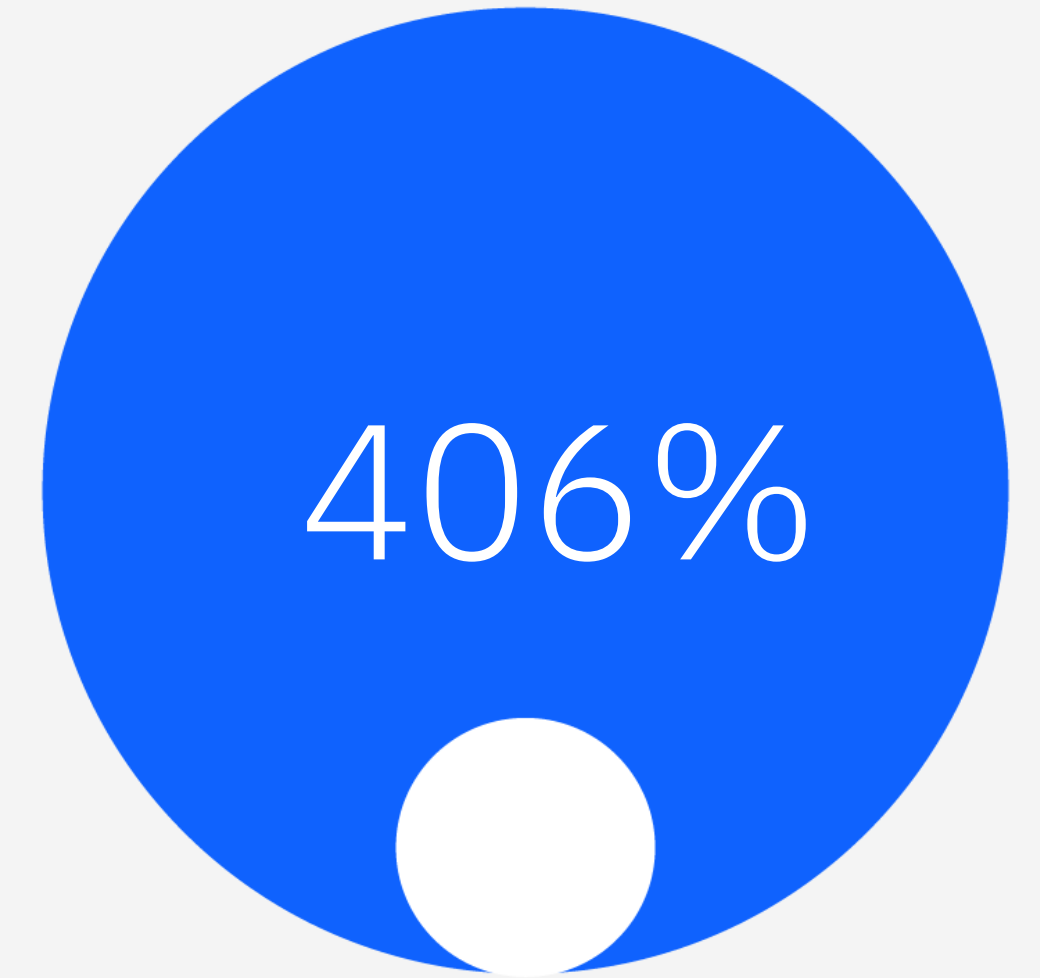
Langkah segera selanjutnya yang dapat Anda lakukan untuk melindungi data berharga organisasi Anda meliputi:

- Membangun rencana keamanan data dan kepatuhan yang mendukung tujuan bisnis dan teknologi jangka pendek dan jangka panjang organisasi Anda
- Menerapkan rencana tersebut dengan orang, proses, dan alat yang tepat
- Merencanakan sumber daya Anda untuk memastikan program keamanan data dan kepatuhan Anda dapat meningkat secara efektif seiring organisasi Anda merangkul teknologi modern

Platform IBM Security® Guardium® adalah solusi keamanan data dan kepatuhan yang dirancang untuk membantu organisasi mengambil pendekatan yang lebih cerdas dan adaptif untuk melindungi data penting dan sensitif di mana pun data tersebut berada. Lihat mengapa ini cocok untuk organisasi Anda.

[Ketahuilah lebih lanjut](#) →

[Hubungi kami](#) →



Penelitian tentang solusi Guardium menemukan ROI 406% dengan manfaat sebesar USD 5,86 juta selama tiga tahun.⁴

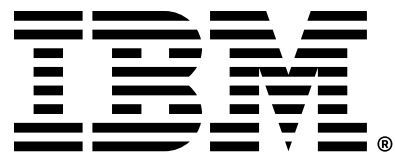
Mengapa IBM Security?

IBM Security membantu mengamankan perusahaan dan pemerintah terbesar di dunia dengan portofolio produk dan layanan keamanan terintegrasi yang ditanamkan dengan kemampuan AI dan otomatisasi keamanan yang dinamis. Portofolio ini, yang didukung oleh penelitian IBM® X-Force® yang terkemuka di dunia, memungkinkan organisasi untuk memprediksi ancaman, melindungi data saat data berpindah, dan merespons dengan kecepatan dan ketepatan tanpa menghambat inovasi bisnis. IBM dipercaya oleh ribuan

organisasi sebagai mitra mereka untuk menilai, menyusun strategi, menerapkan, dan mengelola transformasi keamanan.

IBM mengoperasikan salah satu organisasi penelitian, pengembangan, dan penyediaan keamanan yang paling luas di dunia; memantau lebih dari 150 miliar peristiwa keamanan setiap hari di lebih dari 130 negara; dan telah mendapatkan lebih dari 10.000 paten keamanan di seluruh dunia.





1. Laporan Biaya Pelanggaran Data 2023, IBM, Juli 2023.
2. The Need for Data Compliance in Today's Cloud Era, Enterprise Strategy Group oleh TechTarget, April 2023.
3. X-Force Threat Intelligence Index 2023, IBM Security, Februari 2023.
4. Total Economic Impact™ (TEI) dari IBM Security Guardium Data Protection, sebuah studi Forrester Consulting yang ditugaskan oleh IBM, Juni 2023.

© Hak Cipta IBM Corporation 2023

IBM Corporation
New Orchard Road
Armonk, NY 10504

Diproduksi di Amerika Serikat
September 2023

IBM, logo IBM, Guardium, IBM Security, dan X-Force adalah merek dagang atau merek dagang terdaftar dari International Business Machines Corporation, di Amerika Serikat dan/atau negara lain. Nama produk dan layanan lainnya mungkin merupakan merek dagang dari IBM atau perusahaan lain. Daftar terkini merek dagang IBM tersedia di ibm.com/id-id/legal/copyright-trademark.

Dokumen ini adalah yang terbaru pada tanggal awal publikasi dan dapat diubah oleh IBM kapan saja. Tidak semua penawaran tersedia di setiap negara tempat IBM beroperasi.

INFORMASI DALAM DOKUMEN INI DIBERIKAN "SEBAGAIMANA ADANYA" TANPA JAMINAN APA PUN, TERSURAT MAUPUN TERSIRAT, TERMASUK TANPA JAMINAN KELAYAKAN UNTUK DIPERDAGANGKAN, KESESUAIAN UNTUK TUJUAN TERTENTU, DAN JAMINAN ATAU KETENTUAN NON-PELANGGARAN. Produk IBM dijamin sesuai dengan syarat dan ketentuan perjanjian yang mengatur penyediaan produk tersebut.

Pernyataan Praktik Keamanan yang Baik: Tidak ada sistem atau produk IT yang dapat dianggap sepenuhnya aman, dan tidak ada satu pun produk, layanan, atau tindakan keamanan yang dapat sepenuhnya efektif untuk mencegah penggunaan atau akses yang tidak semestinya. IBM tidak menjamin bahwa sistem, produk, atau layanan apa pun kebal dari, atau akan membuat perusahaan Anda kebal terhadap, tindakan jahat atau ilegal dari pihak mana pun.

Klien bertanggung jawab untuk memastikan kepatuhan terhadap semua hukum dan peraturan yang berlaku. IBM tidak memberikan nasihat hukum atau menyatakan atau menjamin bahwa layanan atau produknya akan memastikan bahwa klien mematuhi hukum atau peraturan apa pun.