IBM Security

IBM

Menghadapi tantangan melindungi data yang ada di sini, dan di segala tempat

Menjaga keamanan data sensitif di era komputasi Cloud

Klik lingkaran untuk melompat ke bab

1

Menerapkan lingkungan cloud

Organisasi berpindah dengan cepat ke cloud, memanfaatkan infrastruktur sebagai layanan (IaaS), perangkat lunak sebagai layanan (SaaS), dan platform sebagai layanan (PaaS) sebagai cara baru untuk mengoptimalkan bisnis mereka, walaupun lingkungan tersebut memberikan risiko baru pada data sensitif.

2

Tantangan keamanan cloud

Penerapan cloud sering kali berarti data sensitif disimpan di lokasi yang tidak bisa Anda kendalikan dan dikelola oleh pihak ketiga yang mungkin memiliki akses tanpa batasan.

3

Tantangan organisasional

Tantangan ketika melindungi data di cloud termasuk memastikan kepatuhan, mengawasi akses kendali, memastikan privasi, meningkatkan produktivitas, dan menunjukkan kerapuhan-sementara memanfaatkan data lokal dan data berbasis cloud Anda bersamaan untuk mendorong maju bisnis Anda.

4

Pendekatan perlindungan data

Keamanan data dan teknologi perlindungan harus beroperasi dalam beberapa lingkungan (fisik, cloud, dan hibrida) di saat yang sama. Solusi keamanan data Anda harus otomatis, dinamis, dan adaptif, serta memberikan kemampuan enkripsi yang konsisten dan fleksibel.

5

Kesimpulan

Seiring komputasi cloud semakin meluas, dasar keamanan tetap sama: mengamankan dan melindungi data serta mendukung kepatuhan.

1.1 Menerapkan lingkungan cloud

Beberapa tahun lalu, banyak organisasi beralih ke lingkungan cloud privat untuk membantu meningkatkan fleksibilitas dan biaya kendali--sebagian besar karena ketidakmatangan dan kurangnya kendali dalam lingkungan cloud publik yang saat itu tersedia. Di masa kini, keputusan untuk "berpindah ke cloud" bukan karena biner, dan lebih kepada spektrum pilihan, menyajikan berbagai model penerapan (publik, privat, dan hibrida) serta jenis layanan, termasuk IaaS, PaaS, dan SaaS.

Dengan lebih banyak pilihan granular, penerapan cloud telah menjadi terfragmentasi menurut jenis usaha, dan bukan hanya menjadi keputusan TI yang distandarkan. Sementara daftar pilihan cloud baru jumlahnya beragam, sebagian besar perusahaan akan menerapkan lingkungan campuran, hibrida, untuk meningkatkan investasi yang sudah ada dalam bingkai utama, database lokal, distribusi big data, sistem file, dan banyak lagi.[1]

Cloud privat adalah infrastruktur TI yang beroperasi hanya untuk satu organisasi, baik dikelola secara internal maupun pihak ketiga. Dengan cloud privat, organisasi dapat mengendalikan keseluruhan perangkat lunak, dan juga platform dasar, dari infrastruktur perangkat keras hingga alat pengukur. Layanan cloud privat ditujukan bagi penggunaan unit bisnis perusahaan tunggal (atau hanya dibagikan dengan mitranya).[1] Walaupun demikian, ketika beban kerja berpindah ke cloud privat, mengamankan data dalam lingkungan virtual menjadi jauh lebih penting, terutama karena beban kerja dengan berbagai tingkat kepercayaan digabungkan untuk dijalankan di perangkat keras fisik yang sama. Riset Gartner menunjukkan bahwa akan ada keberlanjutan penggunaan penting dan investasi dalam komputasi cloud privat. Hampir semua perusahaan yang disurvei Gartner ingin memanfaatkan model cloud hibrida--dengan elemen cloud privat dan publik. Perusahaan memanfaatkan opsi komputasi cloud publik turnkey untuk mengaktifkan layanan yang lebih cepat dan bebas gesekan dan untuk meningkatkan ketangkasan bisnis dan mendorong inovasi. Komputasi cloud publik mengisi peran penting untuk inovasi dan, sebagai hasilnya, diramalkan akan tumbuh 15,2 persen setiap tahunnya di tahun 2019.[1]

Dalam lingkungan cloud, baik dalam cloud publik atau lingkungan yang di-host secara privat, keamanan data dan kendali perlindungan harus melindungi data sensitif--serta mendukung pemerintah yang terus berkembang dan persyaratan kepatuhan industri.

1.2 Menerapkan lingkungan cloud

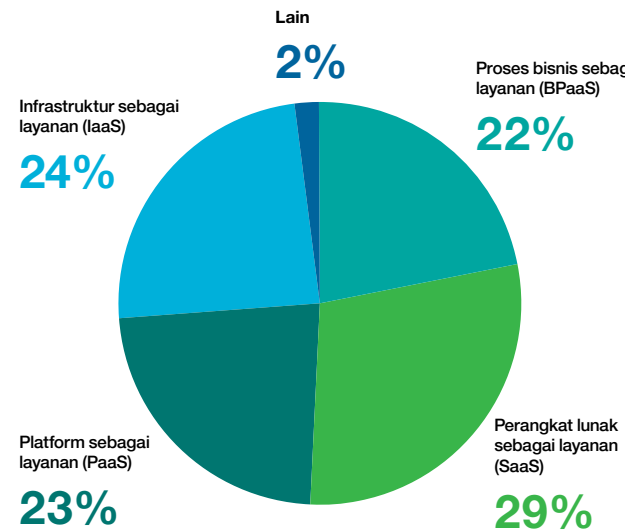
Jenis layanan yang paling umum adalah IaaS, PaaS, dan SaaS. Cara termudah untuk menggambarkan perbedaan adalah mempertimbangkan susunan TI Anda. Di bagian bawah, ada infrastruktur Anda--yang termasuk perangkat keras, server, dan jaringan Anda--yang bertindak sebagai fondasi TI. Di atas infrastruktur ini ada platform perangkat lunak atau perangkat lunak tengah yang memberikan peralatan yang diperlukan pengembang Anda untuk menerapkan aplikasi bisnis. Dan di bagian paling atas ada aplikasi bisnis yang melakukan antarmuka dengan karyawan internal dan pelanggan.

IaaS memungkinkan organisasi untuk mengelola platform perangkat lunak dan perangkat lunak tengah fisik yang sudah ada serta aplikasi bisnis, tetapi melakukan outsource manajemen infrastruktur dasar mereka. Perusahaan melakukan hal ini dengan tujuan memanfaatkan cloud dalam waktu singkat, sementara meminimalkan dampak serta meningkatkan investasi yang ada.

PaaS memungkinkan perusahaan untuk melakukan outsource pada infrastruktur serta perangkat lunak tengah dan perangkat lunak. Ini menyingkirkan beban besar pada perusahaan dari sudut pandang TI dan memungkinkannya untuk berfokus pada mengembangkan aplikasi bisnis inovatif.

SaaS adalah pilihan paling ekstrem, yang melakukan outsource pada semua TI dan memungkinkan organisasi untuk lebih fokus pada kekuatan inti mereka (misalnya perawatan kesehatan, layanan finansial), dan bukan menghabiskan banyak waktu dan investasi teknologi pada hal-hal yang bisa diserahkan kepada ahli teknologi.

Dengan setiap langkahnya, dari IaaS, PaaS, hingga SaaS, organisasi menyerahkan beberapa tingkat kendali ke sistem yang menyimpan, mengelola, dan mendistribusikan data sensitif mereka. Peningkatan kepercayaan yang diberikan ke pihak ketiga ini juga meningkatkan risiko.



Gambar 1: Pertanyaan jajak pendapat: “Bagaimana anggaran yang saat ini dialokasikan untuk layanan cloud ‘publik’ dibagi antara jenis-jenis cloud berikut?”

Sumber: Ed Anderson dan Sid Nag, “Tren Pasar: Tren Penerapan Cloud Memilih Cloud Publik dengan Sentuhan Hibrida,” Gartner, 4 Agustus 2016. ID: G00294424.

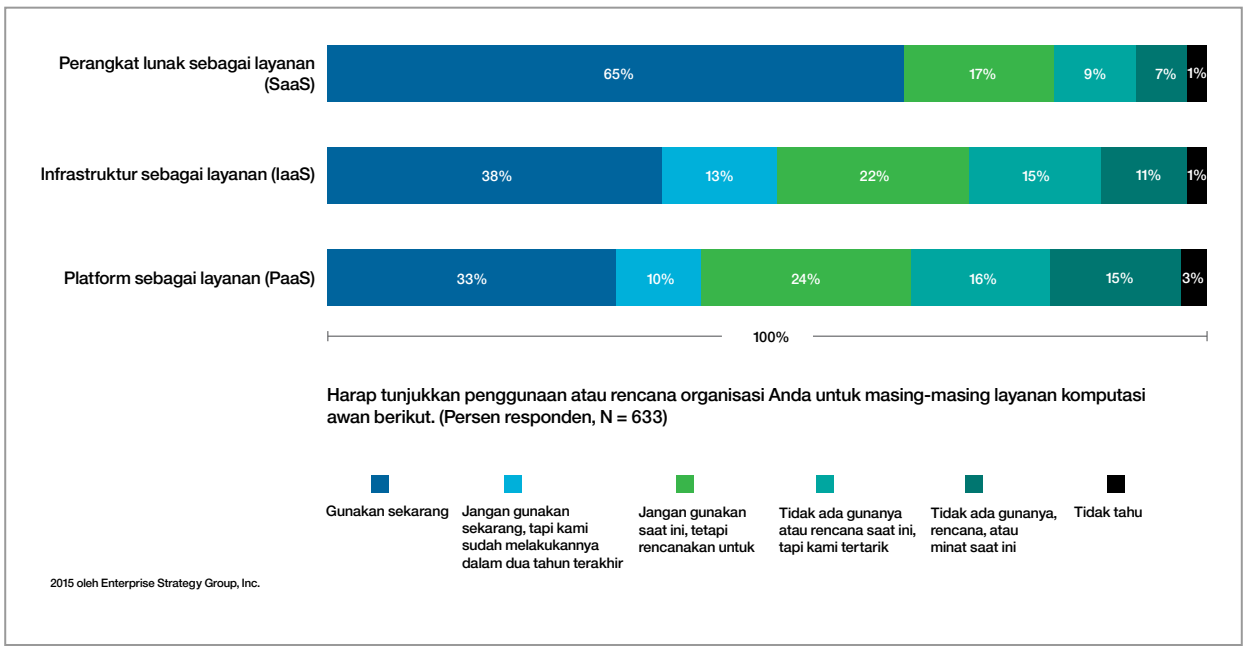
1.3 Menerapkan lingkungan cloud

"Menggunakan cloud" bukanlah biner. Studi yang dilakukan pada lebih dari 600 pembuat keputusan TI perusahaan menunjukkan bahwa sebagian besar firma yang disurvei telah menerapkan setidaknya beberapa aplikasi SaaS; kurang dari 20 persen responden tidak memiliki rencana atau ketertarikan dalam menerapkan SaaS.

Penerapan PaaS, yang menuntut komitmen lebih dalam pada penyimpanan data dan komputasi di luar tempat, dapat dipahami tertinggal aplikasi cloud sedikit demi sedikit, tetapi 67 persen responden menggunakan, pernah menggunakan, atau berencana menggunakan PaaS.

Penerapan infrastruktur cloud--IaaS--yang memindahkan beban penginstalan dan perawatan infrastruktur fisik dari perusahaan ke penyedia khusus, berada secara statistik antara PaaS dan SaaS. Pada saat survey ini, 73 persen responden menggunakan atau merencanakan untuk menggunakan sejenis infrastruktur cloud, atau telah bereksperimen dengan infrastruktur tersebut.

Tantangan perlindungan data cloud virtual dan privat



2.1 Tantangan keamanan cloud

Cloud sangat sesuai untuk penyimpanan data jangka panjang tingkat perusahaan--dengan skala ekonomi baik dalam peralatan dan administrasi yang dapat membuat pusat data berbasis cloud menjadi tempat lebih cerdas untuk menyimpan informasi penting bisnis daripada tumpukan server di lorong. Itu karena bahkan seiring menurunnya pengeluaran untuk mendapatkan penyimpanan, biaya peningkatan penggunaan bisnis dan personel untuk mengelola penyimpanan akan terus naik. Namun, walaupun menempatkan penyimpanan data di tangan administrator khusus dapat menghemat uang dan waktu, hal itu juga dapat memunculkan tantangan keamanan serius dan menciptakan tingkat risiko baru.

Penting untuk menyadari bahwa apa pun model penerapan atau jenis layanan--prinsip keamanan data mendasar tidak boleh berubah. Yang berubah adalah kini data sensitif Anda berada di banyak tempat, baik di dalam dinding perusahaan Anda dan di bagian luarnya. Hal ini berarti kendali keamanan harus mengikuti ke mana pun data Anda pergi. Saat mengevaluasi teknologi keamanan data, pilih solusi yang beroperasi dalam beberapa lingkungan secara transparan dan simultan. Pastikan solusi keamanan data bersifat dinamis dan adaptif di seluruh lingkungan sehingga Anda tidak perlu secara serampangan memasang perlindungan data tambahan.

Menjaga data tetap aman di mana saja, dari siapa saja

Hal paling penting dari tantangan ini sudah jelas: data sensitif kini ada di mana-mana, di dalam dan di luar firewall Anda, dan dikelola oleh orang-orang yang Anda gaji serta pihak ketiga. Anda tidak dapat lagi melindungi data sensitif hanya dengan mengunci akses jaringan. Bahkan, Anda bergantung pada jaringan untuk mengakses dan membagikan data. Hal ini berarti menyerahkan keamanan data sebagian besar ke tangan lebih banyak orang daripada masa lalu dan banyak orang yang tidak lagi bekerja secara langsung untuk perusahaan Anda. Secara umum, dalam lingkungan cloud, penyedia layanan cloud (CSP) memiliki kemampuan untuk mengakses data sensitif Anda, yang membuat CSP menjadi garda depan baru dalam ancaman dari dalam. Selain itu, penjahat siber tahu bahwa CSP menyimpan sejumlah besar data penting. Kedua risiko ini membuat kemampuan seperti enkripsi data dan pengawasan aktivitas data menjadi bagian yang sangat berharga dalam strategi keamanan Anda.

2.2 Tantangan keamanan cloud

Portabilitas data adalah salah satu alasan penyimpanan cloud menjadi pilihan ekonomis. Pengeluaran infrastruktur (dari barang tetap ke biaya energi) bervariasi secara geografis dan waktu dalam hari. Begitu pula biaya penyimpanan dan performa di antara jenis media berubah-ubah. Penyimpanan tape, disk putar, dan berbentuk solid semuanya berkembang dalam hal kapasitas, kecepatan dan keandalan, dan teknologi penyimpanan gabungan yang paling ekonomis untuk perusahaan dapat berubah dengan cepat. Oleh karena itu, dengan penyimpanan cloud, besok data Anda dapat berada di tempat yang berbeda, di media yang berbeda dari tempatnya sekarang. Virtualisasi juga mengalami hal yang sama. Bukan hanya data berbasis cloud, tetapi juga sumber daya komputasi berbasis cloud dapat berpindah--secara transparan dan cepat--baik dalam lokasi dan dasar perangkat keras.

Sifat perubahan cloud berarti pendekatan keamanan untuk penyimpanan berbasis cloud harus mencakup beberapa jenis penyimpanan. Pendekatan Anda juga harus mempertimbangkan salinan, baik pencadangan jangka panjang atau salinan sementara yang dibuat saat perpindahan data. Untuk mengatasi tantangan tersebut, pilih solusi lintas platform dan terapkan enkripsi kuat.

Bahkan jika data Anda tidak disimpan dalam jumlah besar di cloud, baik saat data Anda pergi dan kembali ke perusahaan Anda dan rute yang ditempuh data adalah perhatian penting. Bahkan untuk data yang sebagian besar disimpan dengan dienkripsi dan firewall di tempat, jika ada bagian yang terekspos saat dikirimkan ke pencadangan luar lokasi atau untuk pemrosesan pihak ketiga, data sensitif hanya seaman tautan terlemah dalam rantai pemrosesan data.

Secara efektif menjaga data saat berada di cloud membutuhkan tindakan pencegahan pasif (seperti memblokir akses ke port yang tidak disetujui) dan pencegahan aktif, seperti terus-menerus memindai akses data mencurigakan. Tindakan terbaik yang bisa Anda ambil adalah menerapkan enkripsi untuk data sensitif Anda. Walaupun deteksi malware atau analisis perilaku yang dirancang untuk mengenali akses mencurigakan dapat membantu menghindari pelanggaran data internal atau eksternal--dan memberikan fungsi berharga--enkripsi membantu melindungi data di mana pun data berada, dalam diam maupun saat berpindah.

2.3 Tantangan keamanan cloud

Implikasi administratif dan regulasi

Kenyataan komputasi dan penyimpanan berbasis cloud artinya mengamankan data sensitif di cloud dan sistem cloud hibrida jarang selancar yang diharapkan administrator. Peralatan keamanan yang menawarkan antarmuka terpadu di seluruh titik akhir cloud--dari server farm di luar lokasi khusus hingga komputer virtual di infrastruktur cloud publik--adalah awal yang baik menuju mewujudkan janji administrasi jarak jauh efisien.

Yang sama pentingnya adalah persyaratan regulasi dan kedaulatan data--dengan kata lain, peraturan yang membahas keamanan dan perlindungan data ketika data sensitif disimpan secara fisik di tempat khusus. Menyimpan data di cloud dapat membuat data sensitif disimpan di lokasi di mana peraturan yang lebih ketat daripada peraturan di rumah asli data diterapkan. Perlindungan lebih ketat bagi data pribadi individual di dalam negara-negara Uni Eropa (UE), contohnya, diamanatkan dalam persyaratan Regulasi Perlindungan Data Umum (GDPR) UE. Persyaratan tersebut berlaku bahkan bagi perusahaan yang terletak di wilayah lain di dunia yang memiliki dan mengakses data pribadi penduduk EU.

Mengetahui siapa yang mengakses data Anda: *IBM® Security Guardium® dapat membantu mengamankan cloud dan infrastruktur cloud hibrida Anda dengan pengawasan dan peralatan penilaian yang memperlihatkan kelainan dan kerapuhan.*

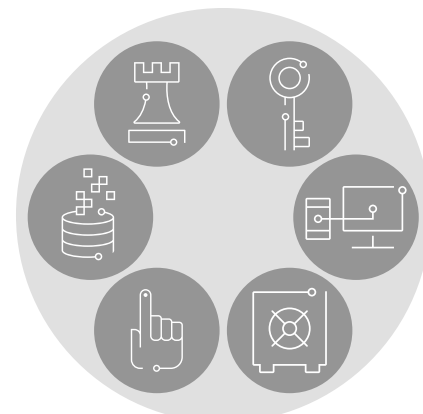
3.1 Tantangan organisasional

3

Organisasi masih ditantang saat mencoba mengamankan data sensitif mereka, dan regulasi rumit adalah salah satu alasannya. Forrester menunjuk bahwa di masa kini, “sebagian besar arsitek perusahaan dan ahli keamanan berjuang untuk meningkatkan keamanan data atau memenuhi persyaratan kepatuhan, karena silo data yang tumbuh dan meningkatnya volume data. Menerapkan kebijakan kontrol akses yang seragam ke seluruh database, gudang data, Hadoop, oSQL, dan file menjadi sangat menantang.”[2]

Virtualisasi memiliki potensi untuk membuat penerapan kontrol keamanan dan mekanisme kepatuhan menjadi lebih mudah, tetapi hanya jika lingkungan cloud virtual atau privat dapat mendukung mengamankan data sensitif dengan secara seragam menangani persyaratan kepatuhan, kebutuhan kontrol akses, persyaratan privasi, persyaratan kerapuhan, dan kebutuhan produktivitas.

Tantangan perlindungan data cloud virtual dan privat



Kepatuhan
Kendali akses
Privasi
Produktivitas
Kerapuhan

Gambar 2: Melindungi data yang disimpan cloud masih memerlukan administrator untuk memperhatikan aspek keamanan dari keamanan dan privasi hingga kepatuhan regulasi di beberapa domain.

3.2 Tantangan organisasional

Kepatuhan

Pikirkan tentang di mana data sensitif berada dalam lingkungan cloud. Penting untuk mengidentifikasi dan mengklasifikasi jenis data sensitif dan menerapkan kebijakan untuk penggunaannya, baik dalam cloud publik atau dalam lingkungan cloud privat. Jika data dalam cloud publik, Anda perlu memahami bagaimana penyedia infrastruktur cloud merencanakan untuk melindungi data sensitif Anda.

Dalam kasus mana pun, memahami di mana data terletak, domain informasi apa yang ada, dan bagaimana hubungannya dalam perusahaan akan membantu organisasi menentukan kebijakan yang tepat untuk mengamankan dan mengenkripsi data tersebut dan mendemonstrasikan kepatuhan dengan regulasi misalnya Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Security Content Automation Protocol (SCAP), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), dan Health Information Technology for Economic and Clinical Health Act (HITECH). Regulasi kepatuhan terus muncul, dan organisasi tetap bertanggungjawab bahkan setelah data berpindah ke cloud.

Privasi

Tantangan lain untuk administrator akses data adalah memastikan hanya mereka yang memiliki alasan bisnis valid yang bisa mengakses informasi pribadi. Sebagai contoh, dokter perlu melihat informasi sensitif seperti gejala dan data prognosis pasien, sementara petugas tagihan hanya perlu nomor asuransi pasien dan alamat penagihan.

3.3 Tantangan organisasional

Kendali akses

Penjahat siber memiliki intensi yang jahat dan mengganggu. Mereka bisa jadi ilmuwan komputer jahat yang mencoba pamer atau membuat pernyataan politik, atau penyusup terorganisir yang kuat. Negara asing telah mensponsori peretas untuk mengumpulkan intelegensi dari organisasi pemerintah. Penyerang bahkan bisa saja karyawan yang tidak puas Pelanggaran juga bisa secara tidak sengaja--contohnya, ketika izin salah ditetapkan pada tabel database, atau jika kredensial karyawan diretas. Praktik terbaik menyarankan mengautorisasi pengguna akhir baik yang istimewa maupun biasa dengan “keistimewaan terkecil” untuk meminimalkan penyalahgunaan keistimewaan dan kesalahan. Organisasi harus melindungi data dari serangan internal dan eksternal dalam lingkungan cloud fisik, virtual, dan privat.

Pertahanan perimeter adalah hal yang penting, tetapi sama pentingnya untuk melindungi data sensitif itu sendiri. Jika perimeter dilanggar, data sensitif harus sudah diamankan (dan tidak dapat digunakan oleh pencuri) untuk meminimalkan dampak pelanggaran dan memastikan peretas tidak punya kendali bebas. Pertahanan harus menyertakan solusi keamanan data berlapis, sehingga administrator dapat memahami apa yang terjadi di dalam cloud privat--sebagai contoh, dengan memahami pola akses data dan perilaku pengguna istimewa.

Tantangannya adalah memberikan akses yang tepat dan perlindungan data seiring memenuhi kebutuhan bisnis dan memastikan data dikelola dalam dasar “perlu mengetahui”--di mana pun lokasinya.

Produktivitas

Kebijakan privasi dan keamanan harus memungkinkan dan meningkatkan, bukan mengganggu operasi bisnis. Kebijakan tersebut harus dibangun ke dalam operasi harian dan berfungsi tanpa hambatan di dalam dan seluruh lingkungan--dalam lingkungan cloud privat, lingkungan cloud publik, lingkungan di lokasi, dan lingkungan hibrida--tanpa mengganggu produktivitas pengguna. Misalnya, jika cloud privat diterapkan untuk memfasilitasi pengujian aplikasi, pertimbangkan untuk menggunakan enkripsi atau tokenisasi untuk memitigasi risiko memaparkan data sensitif.

3.4 Tantangan organisasional

Kerapuhan

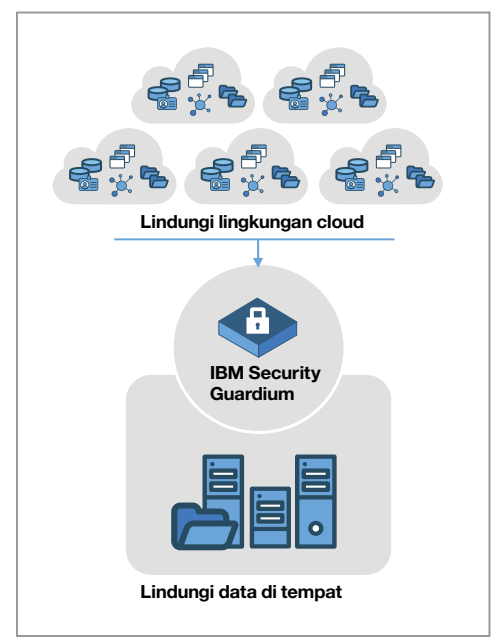
Di masa ini, organisasi memiliki berbagai teknologi keamanan untuk melindungi data perusahaan dan mendukung kepatuhan. Tetapi jumlah kerapuhan penyimpanan data sangat luas, dan penjahat dapat mengeksploitasi bahkan jendela peluang terkecil. Penting untuk memahami kerapuhan dari semua sudut pandang dan mengembangkan pendekatan untuk mengatasinya. Kerapuhan umum termasuk hilangnya patch, kesalahan konfigurasi dan pengaturan sistem standar. Kompleksitas ini semakin sulit untuk dilacak dan dikelola karena tempat penyimpanan data menjadi virtual.

Seiring organisasi bergerak ke cloud privat serta publik, contohnya, solusi tersebut tidak selalu dapat diskalakan. Selain itu, beberapa pendekatan enkripsi terikat pada perangkat keras atau sumber daya jaringan tertentu. Dalam lingkungan cloud, administrator tidak dapat bergantung pada akses ke infrastruktur perangkat keras tingkat rendah.

Masalah lain yang sering muncul adalah ketika cloud privat digunakan untuk pengujian atau pengembangan aplikasi. Database baru dibuat dan dinonaktifkan secara berkala. Data harus dilindungi karena database ini dibuat secara dinamis untuk mendukung pengujian dan pengembangan. Pendekatan keamanan data yang dapat diskalakan untuk lingkungan cloud privat berarti seiring dibuatnya database baru ini, database tersebut ditemukan secara otomatis dan data yang berada di sana diklasifikasikan, diawasi, dan dilindungi secara otomatis.

Terakhir, pikirkan tentang penggunaan peralatan lokal yang ada di tempat saat ini untuk keamanan data--misalnya, rutinitas masking data atau skrip pengawasan aktivitas database. Apakah ada perubahan pengkodean yang diperlukan agar dapat berfungsi di database virtual? Kemungkinannya, investasi signifikan akan diperlukan untuk memperbarui solusi lokal ini--kemudian Anda masih harus menghadapi tantangan besar. Secara idealnya, seiring penambahan database baru atau sumber data lain, proses dan prosedur keamanan akan dilakukan tanpa intervensi manual. Secara singkat, strategi keamanan harus dibangun di dalam infrastruktur lingkungan cloud apa pun.

Pendekatan perlindungan data



4.1 Pendekatan perlindungan data

Organisasi harus memusatkan keamanan data dan kontrol perlindungan dalam lingkungan cloud privat dan publik, dan juga bagian perusahaan lainnya, serta memastikan pemisahan tugas sehingga administrator data tidak sekaligus menjadi administrator keamanan atau auditor. Elemen utama dari strategi cloud yang aman termasuk:

- Memahami di mana data sensitif berada dan siapa yang memiliki akses. Organisasi tidak dapat melindungi data sensitif dengan enkripsi atau menerapkan kendali akses kuat kecuali mereka tahu di mana letaknya, dan bagaimana keterkaitannya dengan perusahaan.
- Menjaga keamanan data sensitif terstruktur dan tidak terstruktur, online dan offline, dengan teknologi yang tepat, serta menetapkan persyaratan akses yang benar.
- Melindungi data di luar produksi, dalam pengembangan, pengujian, dan lingkungan jaminan kualitas.
- Mengawasi akses dengan aman dan terus-menerus pada data sensitif—di mana pun data berada.
- Mendemonstrasikan kepatuhan untuk lolos dalam audit dengan laporan yang telah disusun bagi auditor dan dengan alur kerja otomatis sehingga Anda bisa memberikan laporan yang tepat kepada orang yang tepat di waktu yang tepat untuk pengiriman.

Strategi perlindungan komprehensif bagi semua lingkungan cloud dan cloud hibrida harus memberikan peringatan perilaku mencurigakan kepada administrator keamanan. Organisasi juga harus mempertimbangkan solusi keamanan data yang memberikan dukungan kepatuhan otomatis untuk menyingkat proses kepatuhan.

Proses keamanan data untuk lingkungan cloud harus terus-menerus melacak data dan memberikan wawasan tentang siapa yang mengakses aplikasi di seluruh data, database, gudang dan file berbagi, lingkungan big data, dan banyak lagi. Pendekatan tersebut dapat memastikan perlindungan 360 derajat untuk data organisasi sensitif, di mana pun lokasinya.

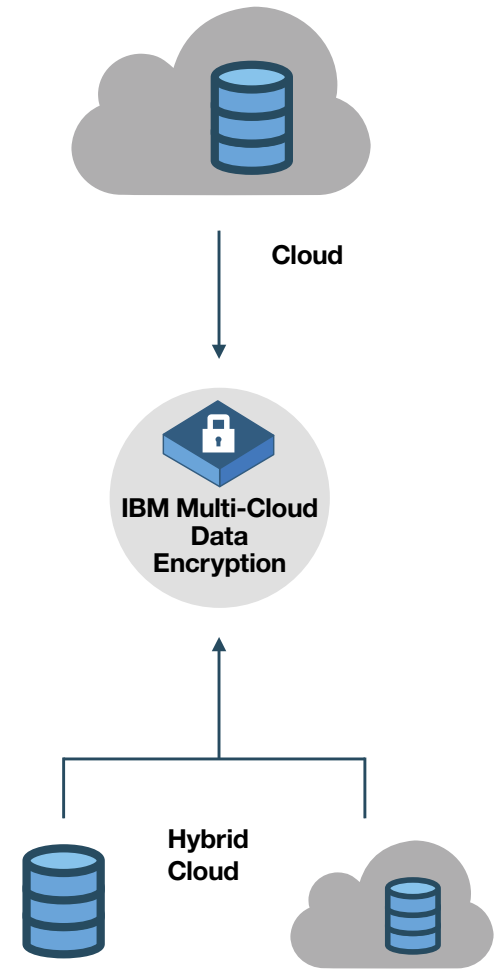
4.2 Pendekatan perlindungan data

Beban regulasi pada pemegang data (serta risiko pelanggaran) dapat membuat perusahaan mempertimbangkan kewaspadaan penyimpanan berbasis cloud yang baru atau diperluas. Enkripsi kuat adalah jawaban paling tepat untuk tantangan mengamankan data sensitif, di dalam atau luar lokasi, namun enkripsi meningkatkan masalah rumit tentang portabilitas dan jaminan akses. Data hanya tergantung pada keamanan dan keandalan kunci yang melindunginya. Bagaimana kunci tersebut dicadangkan? Dapatkah data dipindahkan secara transparan di antara penyedia data, atau dibagikan antara penyimpanan lokal dan berbasis cloud?

Enkripsi Data Multi-Cloud IBM melindungi data cloud (dan cloud hibrida), dan melakukannya dengan mempertimbangkan portabilitas dan persyaratan kepatuhan. Untuk membuat kunci enkripsi dapat diakses dan terus tersedia, dapat diintegrasikan dengan manajer kunci lanjutan.

Selain itu, IBM Security Key Lifecycle Manager dapat membantu pelanggan yang memerlukan perlindungan data yang lebih ketat, berbasis pada penyimpanan yang dienkripsi perangkat keras, untuk menyederhanakan dan memusatkan manajemen kunci enkripsi, tanpa khawatir data terpapar di lingkungan cloud virtual.

Manajemen kunci adalah inti dari lingkungan enkripsi yang aman.



5.1 Kesimpulan

Untuk memastikan data terlindung dalam lingkungan virtual dan cloud, organisasi harus memahami data jenis apa yang masuk ke lingkungan tersebut, bagaimana akses pada data tersebut dapat diawasi, jenis kerapuhan apa yang ada, dan bagaimana kepatuhan dapat didemonstrasikan. Perlindungan harus dibangun di dalam lingkungan cloud sejak awal dengan tujuan pertama membantu organisasi mendemonstrasikan kepatuhan.

Saat memilih solusi keamanan dan perlindungan data, pilih solusi yang dapat diskalakan dan dapat diperluas di seluruh infrastruktur TI--melindungi lingkungan fisik, virtual, dan cloud dari serangan eksternal berbahaya, penipuan, akses yang tidak sah, dan pelanggaran dalam. Solusi tersebut harus berjalan dalam lingkungan cloud tanpa pengaturan dan konfigurasi khusus, atau pengeluaran tambahan. Pendekatan tersebut akan memberikan platform efisien untuk keamanan data dan penyampaian privasi, membantu mengelola biaya dengan mengurangi sumber daya keamanan data, serta memberikan ketangkasan dan fleksibilitas yang lebih baik dengan layanan mandiri untuk keamanan dan privasi.

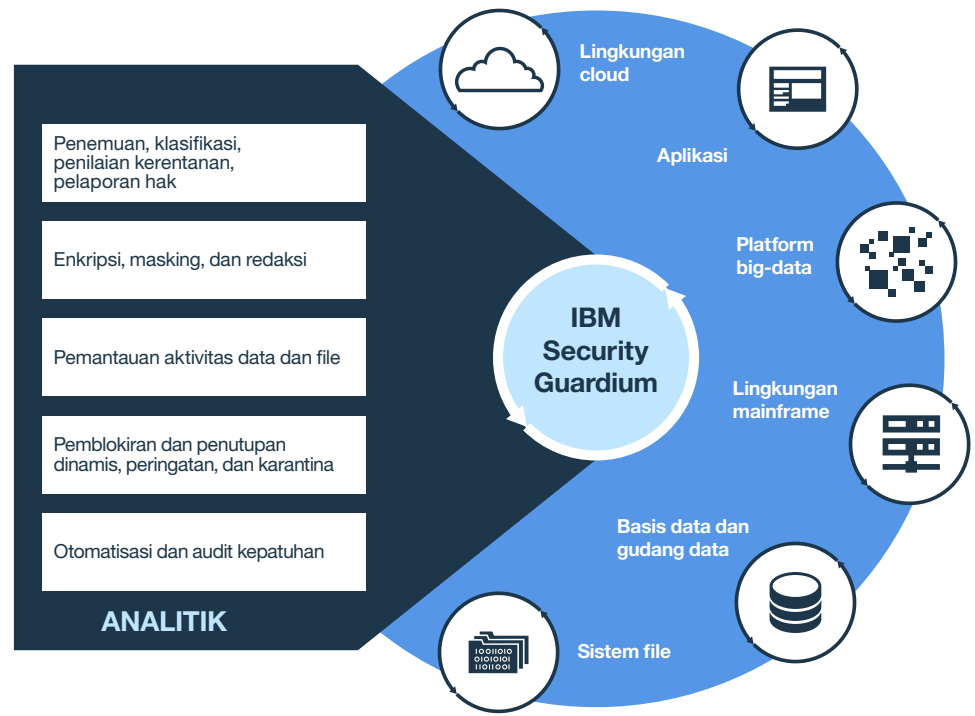
Guardium dapat membantu mendukung strategi cloud Anda dengan:

- Pengawasan aktivitas data dan file, penilaian kerapuhan, redaksi data dan enkripsi data, pemblokiran dinamis, karantina dan peringatan
- Penemuan otomatis dan klasifikasi data sensitif di cloud
- Masking data statis dan dinamis untuk memastikan model dengan akses paling sederhana untuk sumber daya cloud
- Laporan kepatuhan dan audit yang telah disusun, dirancang khusus untuk berbagai peraturan, untuk mendemonstrasikan kepatuhan dan alur kerja kepatuhan otomatis--di tempat dan lingkungan cloud

5.2 Kesimpulan

Perangkat lunak guardium memberikan solusi menyeluruh untuk infrastruktur fisik, virtual, dan cloud melalui kontrol keamanan terpusat dan otomatis di berbagai lingkungan heterogen. Guardium membantu mempersingkat kepatuhan dan mengurangi risiko, serta menawarkan gambar yang siap diinstal untuk penerapan IaaS di platform cloud besar seperti IBM SoftLayer®, Microsoft Azure, dan Amazon Web Services, serta beroperasi di seluruh lingkungan Microsoft Windows, UNIX, dan Linux ™.

Arsitektur Guardium yang fleksibel memungkinkan beberapa model penerapan yang berbeda. Anda dapat memilih arsitektur sistem yang sesuai dengan perusahaan Anda: Semua komponen Guardium dapat diterapkan di cloud, atau Anda dapat memilih untuk menyimpan beberapa komponen tersebut, seperti manajer pusat, di lokasi.



Gambar 3: Guardium memberikan perlindungan data ujung ke ujung di berbagai lingkungan dan platform teknologi.

5.3 Kesimpulan

Fleksibilitas ini memungkinkan pelanggan yang sudah ada untuk memperluas strategi perlindungan data mereka dengan mudah ke cloud tanpa memengaruhi penerapan yang sudah ada.

Pengumpul pengawasan input yang diterapkan di cloud dapat dengan mudah memberikan data ke manajer pusat, memastikan tampilan tunggal dan terpadu dari ancaman perlindungan data Anda, di mana pun data berada.

Kendali keamanan yang menjauhkan penjahat siber dari penyimpanan data--atau mendeteksi gangguan dengan cepat--adalah alat yang penting. Tetapi dalam era data portabel, perpindahan beban kerja dan visualisasi, membuat data aman dengan enkripsi sama pentingnya.

Solusi keamanan data IBM membantu melindungi data sensitif sehingga organisasi dapat tenang karena data mereka terlindungi dalam virtualisasi kompleks dan lingkungan cloud.

5.4 Sumber daya tambahan

Tentang IBM Keamanan solusi

IBM Security menawarkan salah satu portofolio paling canggih dan terintegrasi dari produk dan layanan keamanan perusahaan. Portofolio, didukung oleh riset dan pengembangan ternama X-Force®, memberikan kecerdasan keamanan untuk membantu organisasi secara holistik melindungi anggota, infrastruktur, data, dan aplikasi mereka, menawarkan solusi untuk manajemen identitas dan akses, keamanan database, pengembangan aplikasi, manajemen risiko, manajemen titik akhir, keamanan jaringan, dan banyak lagi.

Solusi tersebut memungkinkan organisasi untuk secara efektif mengelola risiko dan menerapkan keamanan terintegrasi untuk mobile, cloud, media sosial, dan arsitektur bisnis perusahaan lainnya. IBM mengoperasikan salah satu organisasi riset, pengembangan, dan penyampaian keamanan terluas di dunia, mengawasi 15 milyar acara keamanan per hari di lebih dari 130 negara, dan memiliki lebih dari 3.000 paten keamanan.

Untuk informasi selengkapnya tentang keamanan data, kepatuhan, dan cloud, kunjungi **ibm.com**/guardium.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589, U.S.A.

Diproduksi di Amerika Serikat
Mei 2017

1. Thomas J. Bittman, "Cloud Privat Internal Bukan Untuk Perusahaan Paling Umum," *Gartner*22 Mei 2015.

2. Noel Yuhanna, "Virtualisasi Data Perusahaan, Q1 2015," *The Forrester Wave*11 Maret 2015.

Harap Daur Ulang

WGM12362-IDID-00