Perlindungan Data Sektor Publik

Bhredipta Socarana - 2022

Daftar Materi

1. Pengantar
2. Perlindungan kedaulatan dan residensi data
3. Enkripsi data dan manajemen kunci
4. Mengidentifikasi potensi insiden keamanan
5. Mengurangi ancaman orang dalam
6. Mendeteksi dan mencegah ancaman terhadap data
7. Permintaan Data
8. Upaya peningkatan perlindungan data

Pengantar

PeduliLindungi

Pengantar


Reliability and security
Lower costs
Increased scalability
Microsoft Azure
Manage data storage simple
Faster time to market

Ketentuan perlindungan kedaulatan dan residensi data

Banyak pelanggan sektor publik yang mempertimbangkan adopsi cloud membutuhkan keyakinan bahwa data pelanggan dan pribadi disimpan di area geografis tertentu. Prinsip kunci dalam menjaga data pelanggan saat tidak aktif, saat transit, dan sebagai bagian dari permintaan dukungan yang dimulai pelanggan memandu semua interaksi dengan data.

Definisi Data Pribadi

Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan /atau nonelektronik.
(Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik / PP 71/2019)

Data ini tidak hanya mencakup data pelanggan atau jenis pengidentifikasi pribadi lainnya yang jelas seperti nama dan alamat, tetapi juga mencakup pengidentifikasi pribadi unik, tetapi nama samaran seperti Kemungkinan Pengidentifikasi Unik (PUID) dan Pengidentifikasi Unik Global (GUID) yang dihasilkan secara otomatis melalui operasi layanan cloud.

Ketentuan Residensi Data

- PP 71/2019 mengatur bahwa semua data yang dikelola oleh organisasi yang menyediakan sistem elektronik seperti situs, platform, dan aplikasi **untuk keperluan pemerintahan dan/atau menjalankan tugas pemerintah** wajib menyimpan datanya di pusat data yang berlokasi di Indonesia, kecuali teknologi penyimpanan tidak tersedia di dalam negeri.
- Organisasi yang mengumpulkan dan menyimpan data BUKAN **untuk keperluan pemerintahan dan/atau menjalankan tugas pemerintah** dapat menyimpan datanya di pusat data yang tidak berlokasi di Indonesia
- Pengiriman data pribadi dari satu organisasi lain wajib mematuhi ketentuan pengiriman data pribadi yang diatur dalam regulasi,

Perlindungan kedaulatan dan residensi data

Banyak pelanggan sektor publik yang mempertimbangkan adopsi cloud membutuhkan keyakinan bahwa data pelanggan dan pribadi disimpan di area geografis tertentu. Prinsip kunci dalam menjaga data pelanggan saat tidak aktif, saat transit, dan sebagai bagian dari permintaan dukungan yang dimulai pelanggan memandu semua interaksi dengan data.

Klasifikasi data

- **Data pelanggan** adalah semua data yang pelanggan berikan ke Microsoft untuk dikelola atas nama pelanggan melalui penggunaan layanan online Microsoft oleh pelanggan.
- **Konten pelanggan** adalah subset data pelanggan dan mencakup, misalnya, konten yang disimpan di akun Microsoft Azure Storage pelanggan.
- **Data pribadi** berarti informasi apa pun yang terkait dengan perseorangan tertentu, seperti nama dan informasi kontak pengguna akhir pelanggan. Namun, data pribadi juga dapat mencakup data yang bukan data pelanggan, seperti ID pengguna yang dapat dibuat dan ditetapkan Azure ke setiap administrator pelanggan - data pribadi tersebut dianggap nama samaran karena tidak dapat mengidentifikasi individu dengan sendirinya.
- **Data dukungan dan konsultasi** berarti semua data yang diberikan oleh pelanggan ke untuk mendapatkan Dukungan atau Layanan Profesional.

Kedaulatan data

Kedaulatan data menyiratkan residensi data, dan kepatuhan terhadap aturan dan persyaratan yang menentukan siapa yang memiliki kontrol atas dan akses ke data pelanggan yang disimpan di cloud, serta kewajiban pemeliharaan platform atau permintaan dukungan yang dimulai pelanggan sesuai hukum yang berlaku

Data tidak aktif

Data pelanggan di cloud selalu direplikasi untuk membantu memastikan ketahanan dan ketersediaan yang tinggi. Cloud menyalin data pelanggan untuk melindunginya dari kegagalan perangkat keras sementara, penonaktifan jaringan atau daya, dan bahkan bencana alam besar-besaran. Salinan tersebut adalah data yang tidak aktif sehingga pemanfaatan data nya perlu dilakukan peninjauan ulang oleh pengelola data, khususnya jika ada larangan pengiriman data di luar lokasi cloud.

Data saat transit

Enkripsi data saat transit membantu melindungi data dari penyadapan. Data saat transit berlaku untuk skenario berikut yang melibatkan data yang berpindah antara: i) Pengguna akhir pelanggan , ii) Pusat data lokal pelanggan, dan iii) Pusat data utama lainnya sebagai bagian dari operasi layanan.

Enkripsi data dan manajemen kunci

Enkripsi data di cloud adalah alat penting untuk mengurangi risiko dan alat ini diharapkan oleh pelanggan pemerintah di seluruh dunia. Enkripsi data menyeluruh yang menggunakan cipher tingkat lanjut adalah bagian dasar untuk menjamin kerahasiaan dan integritas data pelanggan di cloud

Enkripsi data tidak aktif

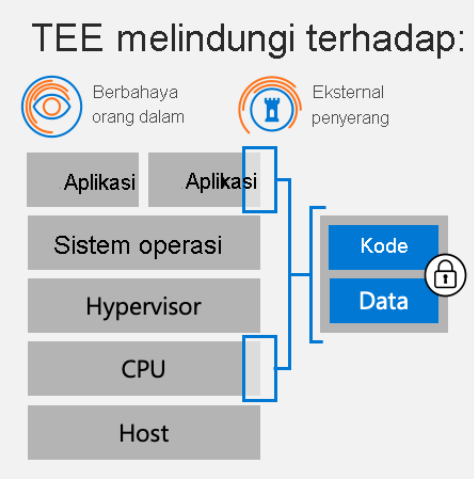
Ppsi enkripsi data tidak aktif perlu untu melindungi data yang disimpan dalam Cloud. Di Microsoft, Opsi ini mencakup kunci enkripsi yang dikelola Microsoft dan kunci enkripsi yang dikelola pelanggan, serta bergantung pada beberapa kunci dan layanan enkripsi, seperti Azure Key Vault dan Microsoft Azure Active Directory.

Enkripsi data saat transit

- Keamanan Lapisan Transportasi (TLS) untuk membantu melindungi data saat berjalan antara pelanggan dan layanan Azure.
- Transaksi dapat dipaksa terjadi melalui HTTPS.
- Enkripsi saat transit untuk komputer virtual dapat menggunakan Protokol Desktop Jarak Jauh (RDP) untuk mengaktifkan perlindungan TLS. Atau, Secure Shell (SSH) dapat digunakan untuk koneksi terenkripsi ke komputer virtual Linux.
- Enkripsi VPN memungkinkan pelanggan menggunakan Azure VPN Gateway untuk mengirim lalu lintas terenkripsi antara Virtual Network (VNet) mereka dan infrastruktur lokal mereka di internet publik.
- ExpressRoute memungkinkan pelanggan membuat koneksi privat antara infrastruktur lokal mereka dan Azure dengan beberapa opsi enkripsi data.

Contoh Inovasi Microsoft dalam Enkripsi Data

Komputasi rahasia Azure



Komputasi rahasia Azure adalah sekumpulan kemampuan keamanan data yang menawarkan enkripsi data saat sedang digunakan. Komputasi rahasia memastikan bahwa ketika data berada dalam keadaan yang diperlukan untuk pemrosesan data yang efisien dalam memori, data dilindungi di dalam trusted execution environment (TEE, juga dikenal sebagai enklave).

TEE berarti tidak ada cara untuk melihat data atau operasi dari luar enklave dan hanya perancang aplikasi yang memiliki akses ke data TEE. Akses ditolak oleh orang lain, termasuk administrator Azure. TEE membantu memastikan hanya kode yang diotorisasi yang dapat mengakses data. Azure menyediakan TEE berbasis perangkat keras menggunakan teknologi Intel Software Guard Extensions (SGX).

Mengidentifikasi potensi insiden keamanan

Dalam mengelola insiden keamanan dan ketersediaan untuk layanan terdapat proses respon insiden 5 langkah yaitu:

Proses tersebut bertujuan untuk memulihkan layanan secepat mungkin setelah masalah terdeteksi dan penyelidikan dimulai.

Jika Insiden Keamanan Melibatkan Data Pribadi

- Regulasi yang berlaku di Indonesia mengatur bahwa apabila terdapat kegagalan perlindungan keamanan sistem suatu platform, aplikasi dan situs, yang mengakibatkan kegagalan atau gangguan sistem maka pengelola nya wajib untuk memberitahukan dalam kesempatan pertama kepada Aparat Penegak Hukum dan/atau Kementerian Terkait
- Kegagalan Sistem: terhentinya sebagian atau seluruh fungsi Sistem Elektronik yang bersifat esensial sehingga Sistem Elektronik tidak berfungsi sebagaimana mestinya.
- Gangguan Sistem:setiap tindakan yang bersifat destruktif atau berdampak serius terhadap Sistem Elektronik sehingga Sistem Elektronik tersebut tidak bekerja sebagaimana mestinya.
- Jika kegagalan tersebut mengakibatkan kegagalan pelindungan data pribadi, maka pengelola wajib untuk memberikan notifikasi kepada pengguna secara tertulis dalam waktu 14 hari sejak diketahui terjadinya kegagalan. Notifikasi wajib menjelaskan alasan atau latar belakang kegagalan pelindungan

Tanggung Jawab Bersama (Study Case: Microsoft)

- Pelanggan bertanggung jawab untuk memantau sumber daya mereka sendiri yang disediakan di Azure.
- Microsoft bertanggung jawab untuk memantau dan memulihkan insiden keamanan dan ketersediaan memengaruhi platform Azure dan memberi tahu pelanggan tentang pelanggaran keamanan apa pun yang melibatkan data pelanggan atau pribadi.
- Sejalan dengan model tanggung jawab bersama, Microsoft tidak memeriksa, menyetujui, atau memantau aplikasi pelanggan individual yang disebarkan di Azure.

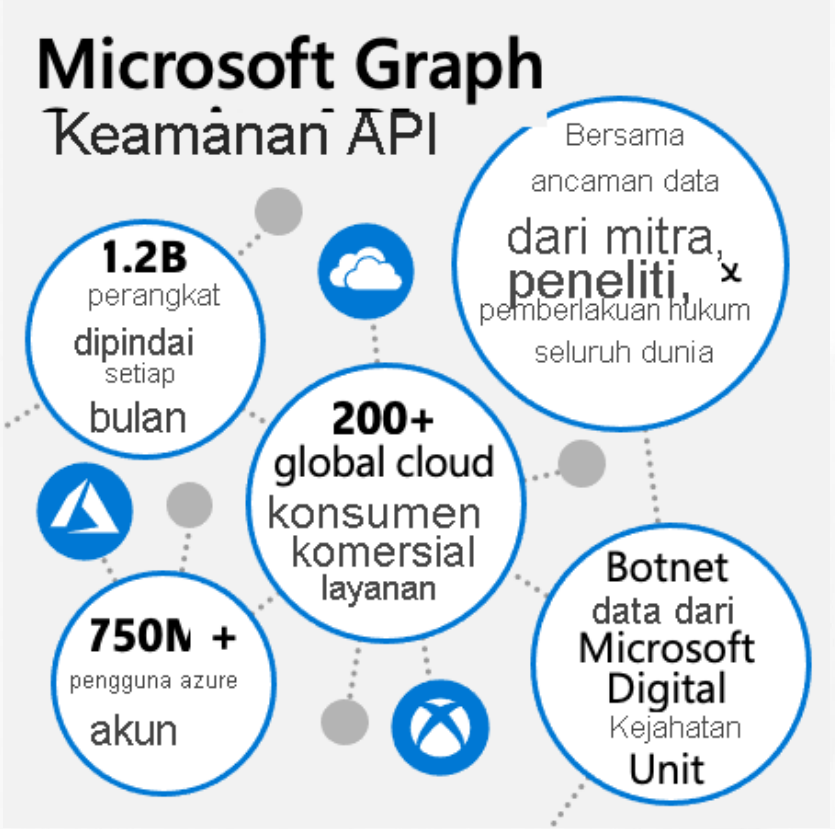
Mendeteksi dan mencegah ancaman terhadap data

Inovasi Microsoft dalam Deteksi dan Mencegah Ancaman Terhadao Data

Microsoft menggunakan perlindungan ekstensif untuk platform cloud Azure dan menawarkan berbagai layanan Azure untuk membantu pelanggan memantau dan melindungi sumber daya cloud yang disediakan dari serangan. Pelanggan dapat menyebarkan berbagai layanan Azure untuk melindungi aplikasi dan data mereka serta mengandalkan proses manajemen insiden keamanan dan privasi yang matang yang diberlakukan.

Microsoft Graph Security API

- Pelanggan pemerintah yang menggunakan Azure mendapatkan manfaat yang cukup besar dari penelitian keamanan yang dilakukan Microsoft untuk melindungi platform cloud.
- Analisis ancaman global Microsoft adalah salah satu yang terbesar di industri ini dan berasal dari salah satu rangkaian sumber telemetri ancaman yang paling beragam. Ini adalah volume dan keragaman telemetri ancaman yang membuat algoritma pembelajaran mesin Microsoft diterapkan pada telemetri tersebut begitu kuat.
- Microsoft Graph Security API menggunakan analitik tingkat lanjut untuk menggabungkan sejumlah besar sinyal keamanan dan inteligensi ancaman dari seluruh produk, layanan, dan mitra Microsoft untuk memerangi ancaman siber.
- Setiap bulan Microsoft memindai lebih dari 400 miliar pesan email untuk pengelabuan dan perangkat lunak jahat, memproses 450 miliar autentikasi, menjalankan lebih dari 18 miliar pemindaian halaman, dan memindai lebih dari 1,2 miliar perangkat terkait ancaman. Yang penting, data ini selalu melalui batas privasi dan kepatuhan yang ketat sebelum digunakan untuk analisis keamanan.
- Microsoft Graph Security API memberikan pandangan terhadap lanskap ancaman yang berkembang dan memungkinkan inovasi cepat untuk mendeteksi dan merespons ancaman. Model pembelajaran mesin dan alasan AI atas sinyal keamanan yang luas untuk mengidentifikasi kerentanan dan ancaman.



Mengurangi Ancaman Orang Dalam

Ancaman orang dalam biasanya ditandai sebagai potensi untuk menyediakan koneksi pintu belakang dan akses pengguna istimewa penyedia layanan cloud ke sistem dan data pelanggan. Penyediaan cloud membutuhkan kontrol ketat dan jaminan pencegahan akses yang tidak sah.

Mengurangi akses data orang dalam

Mekan berikut diberlakukan untuk membatasi akses orang dalam ke data pelanggan:

- Tidak ada hak akses default dan pemberlakuan ketentuan akses Just-in-Time (JIT) untuk mengurangi risiko terkait hak akses.
- Kontrol yang mencegah akses ke sistem produksi, kecuali jika diizinkan secara khusus melalui sistem manajemen akses istimewa **JIT**.
- Penempatan pelanggan yang bertanggung jawab untuk menyetujui akses orang dalam untuk skenario dukungan dan pemecahan masalah (**Customer Lockbox**).
- **Enkripsi data** dengan opsi untuk kunci enkripsi yang dikelola pelanggan. Data terenkripsi hanya dapat diakses oleh entitas yang memiliki kunci.
- **Pemantauan pengguna** terhadap akses eksternal ke sumber daya Cloud yang disediakan, yang mencakup pemberitahuan keamanan.
- Pembatasan dan proses kontrol akses yang sama diberlakukan pada seluruh teknisi, termasuk karyawan tetap dan subprosesor/vendor Cloud.

Data untuk dukungan dan pemecahan masalah pelanggan

- Kontrol penyedia Cloud yang baik akan sangat memberikan keleluasaan pengguna dalam memberikan persetujuan kepada pihak yang membutuhkan akses.
- Namun, permasalahan akses dapat terjadi kapan saja. Diperlukan dukungan untuk pemecahan masalah pelanggan yang tersedia setiap saat.
- Untuk menjamin keamanan, dalam upaya memberikan pemecahan masalah akses, penyedia Cloud tetap membutuhkan akses log untuk memberikan dukungan kepada pelanggan.

Persyaratan kontrol akses

Dengan menggunakan alur kerja akses terbatas, akses ke data pelanggan dikontrol, dicatat, dan dicabut dengan hati-hati saat tidak lagi diperlukan. Persyaratan kontrol akses ditetapkan oleh kebijakan berikut:

- Tidak ada akses ke data pelanggan, secara default.
- Tidak ada akun pengguna atau administrator pada komputer virtual pelanggan (VM).
- Berikan hak istimewa paling sedikit yang diperlukan untuk menyelesaikan permintaan tugas, audit, dan akses log.

Penghapusan, retensi, dan penghancuran data

- Pelanggan selalu mengendalikan data yang disimpan di Cloud termasuk kendali mengakses, mengekstrak, dan menghapus data yang disimpan.
- Penyedia Cloud harus mengambil langkah yang diperlukan untuk memastikan pelanggan terus memiliki data mereka dan memenuhi kewajiban lain sesuai regulasi yang berlaku

Mengurangi Ancaman Orang Dalam

Simulasi Implementasi Kontrol Akses	Teknisi Cloud dapat diberi akses ke data pelanggan menggunakan kredensial sementara melalui akses **Just-in-Time (JIT)**. Akses dapat diberikan jika ada insiden yang dicatat dan menjelaskan alasan akses, catatan persetujuan, data apa yang diakses, dan sebagainya. Akses JIT berfungsi dengan autentikasi multifaktor yang mengharuskan teknisi Microsoft menggunakan smartcard untuk mengonfirmasi identitas mereka. Semua akses ke sistem produksi dilakukan menggunakan Secure Admin Workstations (SAW) yang konsisten dengan panduan yang dipublikasikan tentang mengamankan akses istimewa.

Contoh Inovasi Microsoft dalam Mengurangi Ancaman Orang Dalam

Customer Lockbox

Customer Lockbox for Azure adalah layanan yang memungkinkan pelanggan mengontrol cara teknisi Microsoft mengakses data mereka. Sebagai bagian dari alur kerja dukungan, teknisi Microsoft mungkin memerlukan akses tinggi ke data pelanggan. Customer Lockbox menempatkan pelanggan yang bertanggung jawab atas keputusan tersebut dengan mengizinkan pelanggan Menyetujui/Menolak permintaan tinggi tersebut. Customer Lockbox adalah ekstensi alur kerja JIT dan dilengkapi dengan pembuatan log audit penuh yang diaktifkan. Kemampuan Customer Lockbox tidak diperlukan untuk kasus dukungan yang tidak melibatkan akses ke data pelanggan. Untuk sebagian besar skenario dukungan, akses ke data pelanggan tidak diperlukan dan alur kerja seharusnya tidak memerlukan Customer Lockbox. Teknisi Microsoft sangat bergantung pada log untuk mempertahankan layanan Azure dan memberikan dukungan pelanggan.

Teknisi Microsoft akan memulai permintaan Customer Lockbox jika diperlukan untuk memproses tiket dukungan yang dimulai pelanggan. Customer Lockbox tersedia untuk pelanggan dari semua wilayah publik Azure.

Crash dump komputer virtual tamu

Pada setiap node Azure, ada Hypervisor yang berjalan langsung di perangkat keras. Hypervisor membagi node menjadi beberapa Komputer Virtual (VM) Tamu, seperti yang dijelaskan dalam dokumentas online Microsoft. Setiap node juga memiliki satu Root VM khusus, yang menjalankan Host OS.

Saat Komputer Virtual Tamu (VM pelanggan) mengalami gangguan, data pelanggan mungkin dimuat dalam file cadangan memori pada Komputer Virtual Tamu. Secara default, teknisi Microsoft tidak memiliki akses ke Komputer Virtual Tamu dan tidak dapat meninjau crash dump pada Komputer Virtual Tamu tanpa persetujuan pelanggan. Proses yang sama yang melibatkan otorisasi pelanggan eksplisit digunakan untuk mengontrol akses ke crash dump Komputer Virtual Tamu jika pelanggan meminta agar gangguan komputer virtual mereka diselidiki. Seperti yang dijelaskan sebelumnya, keamanan akses dijaga oleh sistem manajemen akses istimewa JIT dan Customer Lockbox sehingga semua tindakan dicatat dan diaudit. Fungsi pemaksaan utama untuk menghapus cadangan memori dari Komputer Virtual Tamu adalah proses rutin penggambaran ulang komputer virtual yang biasanya terjadi setidaknya setiap dua bulan.

Permintaan Data

Perlu langkah-langkah yang kuat untuk melindungi data pelanggan dari akses atau penggunaan yang tidak sesuai oleh orang yang tidak berwenang dan memastikan semua permintaan termasuk apabila ada permintaan pemerintah dan penegak hukum, mengikuti prosedur yang ketat,

Ketentuan Permintaan Akses Data dan Sistem

- Dalam regulasi yang berlaku, permintaan akses dan/atau sistem situs, aplikasi, dan platform dapat digunakan untuk tujuan: 1) pengawasan, dan 2) penegakan hukum pidana.
- Untuk tujuan pengawasan, permintaan akses data dan/atau sistem harus melampirkan: i) dasar kewenangan Kementerian atau Lembaga; ii) maksud dan tujuan serta kepentingan permintaan; iii) deskripsi secara spesifik Sistem Elektronik yang diminta; dan iv) pejabat dari Kementerian atau Lembaga yang akan mengakses Sistem Elektronik yang diminta.
- Untuk tujuan penegakan hukum pidana, permintaan akses harus melampirkan: i) dasar kewenangan Aparat Penegak Hukum; ii) maksud dan tujuan serta kepentingan permintaan; iii) deskripsi secara spesifik jenis Data Elektronik yang diminta; iv) tindak pidana yang sedang disidik, dituntut, atau disidangkan; v) surat penetapan dari ketua pengadilan negeri yang berwenang
- Data yang diberikan hanya data individual Indonesia dan/atau badan usaha yang didirikan berdasarkan hukum Indonesia

Menanggapi permintaan data pemerintah: Study Case Microsoft

- Microsoft membatasi akses oleh karyawan dan subkontraktor serta dengan hati-hati menentukan persyaratan untuk merespons permintaan pemerintah untuk data pelanggan. Tidak ada saluran pintu belakang dan tidak ada akses langsung atau tanpa batas oleh pemerintah ke data pelanggan.
- Microsoft memberlakukan persyaratan khusus untuk permintaan pemerintah dan penegak hukum terkait data pelanggan. Jika penegak hukum menghubungi Microsoft dengan permintaan data pelanggan, Microsoft akan mencoba mengalihkan lembaga penegak hukum untuk meminta data tersebut langsung dari pelanggan. Jika dipaksa untuk mengungkapkan data pelanggan kepada penegak hukum, Microsoft akan segera memberi tahu pelanggan dan memberikan salinan permintaan, kecuali jika dilarang oleh hukum
- Permintaan pemerintah untuk data pelanggan harus mengikuti undang-undang yang berlaku baik melalui panggilan pengadilan atau yang setara surat perintah, perintah pengadilan, atau yang setara untuk data konten.
- Microsoft berpengalaman menolak permintaan data pelanggan oleh penegak hukum, baik dengan memberi tahu pemerintah yang meminta bahwa informasi yang diminta tidak dapat diungkapkan dan menjelaskan alasan penolakan permintaan tersebut, atau bahkan melalui proses pengadilan.

Memperluas dan menyesuaikan perlindungan data

- Peningkatan secara berkala perlu dilakukan untuk meningkatkan pengelolaan postur keamanan dan pelindungan secara terpadu untuk membatasi paparan ancaman mereka, melindungi sumber daya cloud, merespon insiden, dan meningkatkan kepatuhan terhadap regulasi yang ada.
- Peningkatan upaya pelindungan data dapat dilakukan melalui:


Memantau keamanan di seluruh beban kerja lokal dan cloud.


Menggunakan analitik dan inteligensi tingkat lanjut untuk mendeteksi serangan.


Menggunakan kontrol akses dan aplikasi untuk memblokir aktivitas berbahaya.


Menemukan dan memperbaiki kerentanan sebelum dapat dieksploitasi.


Menyederhanakan penyelidikan saat merespons ancaman.


Menerapkan kebijakan untuk mengikuti standar keamanan

Contoh Inovasi Microsoft dalam Peningkatan Pelindungan Data

- **Azure Monitor** membantu pelanggan meningkatkan ketersediaan dan performa aplikasi dengan memberikan solusi komprehensif untuk mengumpulkan, menganalisis, dan bertindak pada sistem cloud dan perangkat lokal.
- **Azure Policy** memungkinkan tata kelola sumber daya Azure yang efektif dengan membuat, menetapkan, dan mengelola kebijakan atas sumber daya yang tersedia agar sesuai dengan standar keamanan dan privasi pelanggan.
- **Azure Firewall** adalah layanan keamanan jaringan terkelola berbasis cloud yang melindungi sumber daya Azure Virtual Network pelanggan.
- **Azure Network Watcher** memungkinkan pelanggan memantau, mendiagnosis, dan mendapatkan informasi mengenai performa dan kesehatan jaringan virtual Azure. **Azure DDoS Protection** memberikan kemampuan mitigasi Penolakan Layanan Terdistribusi (DDoS) untuk membantu pelanggan melindungi sumber daya Azure mereka dari serangan. Pemantauan lalu lintas yang selalu aktif memberikan deteksi serangan DDoS hampir real-time, dengan mitigasi otomatis serangan segera setelah terdeteksi.
- **Microsoft Sentinel** adalah platform SIEM cloud-native yang menggunakan AI untuk membantu pelanggan menganalisis data dalam jumlah besar dari berbagai sumber, termasuk pengguna, aplikasi, server dengan cepat di seluruh perusahaan. Dengan Microsoft Sentinel, pelanggan dapat: (i) **Mengumpulkan** data, (ii) **Mendeteksi** ancaman, (iii) **Menyelidiki** ancaman dan memburu aktivitas yang mencurigakan, dan (iv) **Merespons** insiden dengan cepat
- **Azure Advisor** membantu pelanggan menganalisis konfigurasi sumber daya dan telemetri penggunaan, dan memberikan rekomendasi solusi untuk membantu pelanggan meningkatkan efektivitas biaya, performa, ketersediaan tinggi, dan keamanan sumber daya Azure.

Terima Kasih