# Keamanan Menjadi Prioritas Bisnis Generasi Era Digital di Asia untuk Mencapai Pertumbuhan Berkelanjutan

2024/25 Tech Insider

# Ringkasan eksekutif

Bisnis generasi era digital (DNB) muncul di era internet dan dibangun menggunakan teknologi terkini yang tersedia saat diciptakan.

Tanpa terbebani oleh teknologi dan proses lama, generasi era digital di berbagai industri seperti game, ritel, dan pendidikan bergerak mengikuti perkembangan teknologi untuk memenuhi kebutuhan pelanggan dalam bekerja, hidup, dan bermain secara online.

Menurut firma riset teknologi IDC, DNB diperkirakan akan membelanjakan hingga $128,9 miliar untuk teknologi pada tahun 2026.

Pada bulan Maret hingga Mei 2024, Akamai bersama firma riset pihak ketiga, TechnologyAdvice, melakukan survei online guna mengetahui prioritas investasi teknologi DNB di seluruh Asia dan kekhawatiran terbesar para pemimpin teknologi mereka.

Lebih dari 200 pemimpin teknologi dari Australia, Asia Tenggara, India, dan Tiongkok menanggapi survei ini.

Apa saja prioritas bisnis dan tantangan teknologi DNB di Asia? Apa yang dicari oleh perusahaan-perusahaan berbasis teknologi ini dalam penyedia solusi mereka? Apakah semua generasi era digital memiliki kesamaan?

Baik karena persaingan pasar yang makin ketat maupun basis konsumen yang berkembang pesat, hampir 9 dari 10 DNB yang disurvei akan memprioritaskan efisiensi dan produktivitas dalam 12 bulan ke depan.

Ini memperkuat data industri yang menunjukkan peningkatan pesat adopsi cloud di kalangan DNB. Perkiraan tingkat pertumbuhan 2021-2026 untuk pengeluaran teknologi pada solusi berbasis cloud adalah 37%, lebih tinggi daripada perangkat lunak non-cloud (16%) dan layanan TI (11%).

Arsitektur modular cloud-native yang dibangun di sekitar layanan mikro yang beroperasi secara independen dan berkomunikasi melalui API ini memungkinkan DNB di wilayah ini untuk dengan cepat meningkatkan skala dan memenuhi peningkatan digitalisasi pelanggan.

Namun, ini bisa dengan cepat berubah menjadi matriks perangkat lunak, sistem, dan layanan yang kompleks, yang berpotensi meningkatkan risiko kerentanan siber bagi DNB.

Terlepas dari tahap perjalanan cloud mereka, DNB di kawasan ini sangat menyadari bahwa masalah keamanan merupakan celah terbesar dalam performa infrastruktur cloud mereka.

Faktanya, infrastruktur TI mereka yang makin rumit dapat menjadi kelemahan dalam peningkatan postur keamanan siber, karena banyak yang menganggap tantangan ini lebih signifikan dibandingkan masalah anggaran atau kepatuhan.

Masalah yang timbul akibat meningkatnya kompleksitas teknologi juga bisa menjadi peringatan bagi mereka yang mempertimbangkan adopsi cloud atau ingin memperdalam migrasi ke cloud.

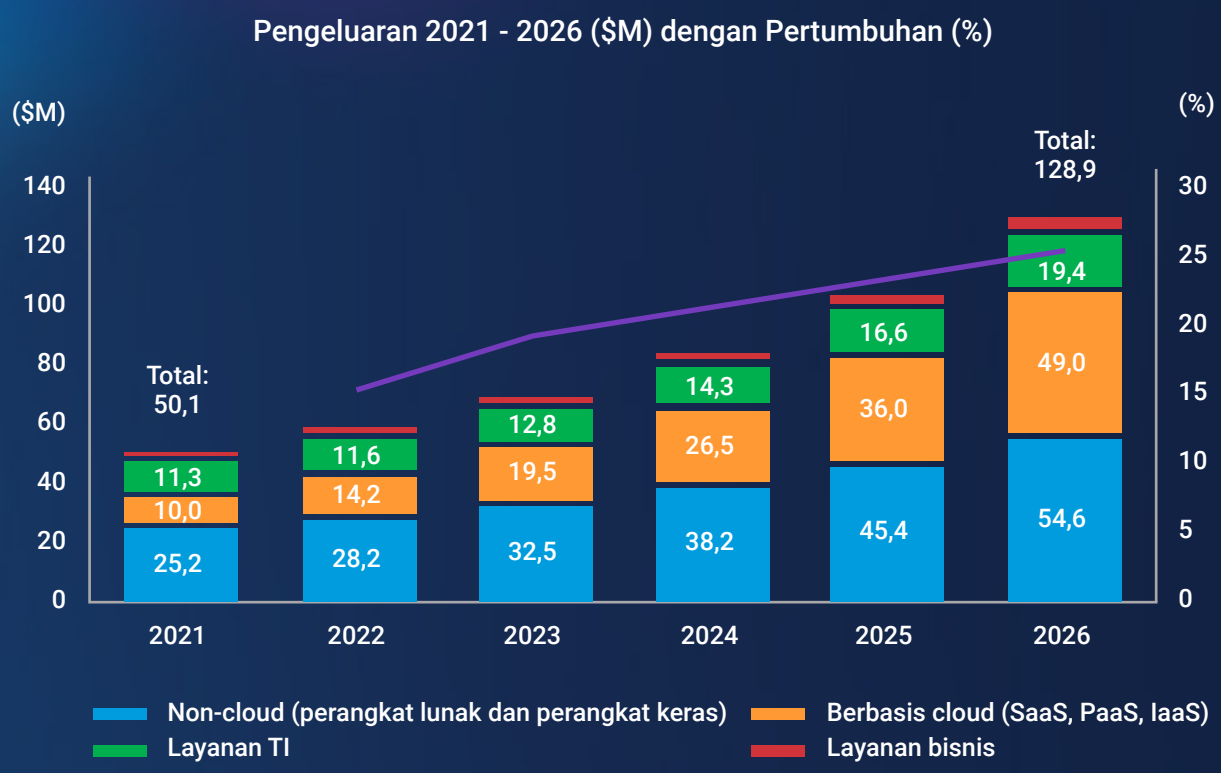
Temukan strategi yang dapat diimplementasikan untuk memitigasi risiko-risiko ini dalam dokumen ini.

# DNB memanfaatkan cloud untuk meningkatkan kecepatan dan efisiensi

Menurut IDC Digital Native Business, Start-Ups and Scale-Ups CIS, segmen pasar generasi era digital adalah "kelompok organisasi yang baru muncul dan berkembang pesat, sangat berfokus pada teknologi, dan mengalokasikan anggaran besar untuk teknologi karena hal ini merupakan inti dari model bisnis mereka".

Terlepas dari industri atau pasarnya, DNB memanfaatkan teknologi sebagai pembeda dan untuk meningkatkan kelincahan mereka.

Pada dasarnya, DNB menerapkan prinsip-prinsip desain cloud-native saat membangun infrastruktur teknologi mereka. Nyatanya, DNB semakin banyak menginvestasikan dana mereka dalam teknologi berbasis cloud, dengan proyeksi tingkat pertumbuhan sebesar 37,3% untuk periode 2021-2026.




## Tingkat pertumbuhan segmen terpilih

- Berbasis cloud (SaaS, PaaS, IaaS) CAGR 37,3%
- Non-cloud (perangkat lunak dan perangkat keras) CAGR 16,7%
- Layanan TI CAGR 11,5%
- Layanan bisnis CAGR 10,4%

**Total CAGR pasar**

**20,8%**

*Sumber: Siaran Pers IDC, Pengeluaran Teknologi Bisnis Digital-Native Asia/Pasifik dari 2022-2026 Diperkirakan Tumbuh dengan CAGR sebesar 20,8% dan Mencapai US$128,9 Miliar pada Tahun 2026, Perkiraan IDC, 19 April 2023*

Infrastruktur teknologi DNB dirancang dengan arsitektur layanan mikro yang dapat dikomposisikan, memberikannya fleksibilitas, kelincahan, dan kecepatan pasar yang penting untuk menghadapi perkembangan ruang digital yang pesat.

Survei menunjukkan bahwa tiga dari empat DNB di wilayah ini menggunakan teknologi cloud dengan fokus pada efisiensi dan produktivitas.

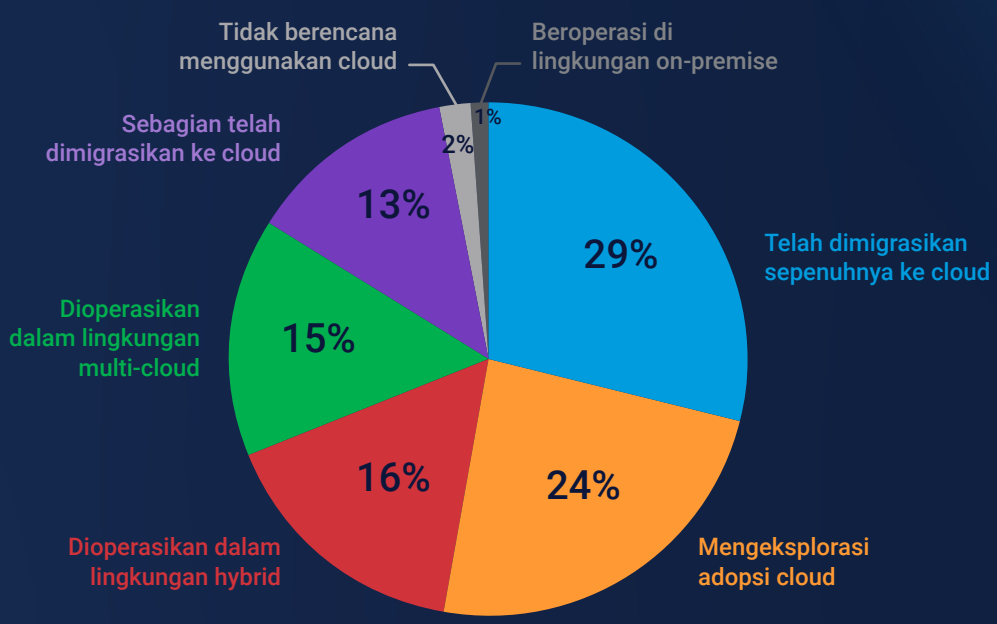
Sebanyak 74% responden telah sepenuhnya bermigrasi ke cloud atau mengadopsi teknologi cloud.

Namun, 26% responden belum memiliki rencana untuk mengadopsi cloud atau masih dalam tahap penjajakan, dan angka ini konsisten di seluruh wilayah (19% di Australia, 20% di India, dan 29% di ASEAN).

Keengganan ini mungkin disebabkan oleh perusahaan-perusahaan besar yang sudah lama berkecimpung di industri yang sangat teregulasi, ditambah dengan pendekatan kehati-hatian terhadap cloud yang terus menjadi penghalang adopsi cloud.

Namun, ada pencairan saat DNB meningkatkan investasi mereka pada cloud. Hal ini dibuktikan dengan tingkat pertumbuhan yang tinggi dalam belanja teknologi cloud.

## Sejauh mana perjalanan adopsi cloud perusahaan Anda saat ini?




## Prioritas bisnis utama dalam 12 bulan ke depan

# Menjaga keamanan online

Hal yang umum adalah bagaimana DNB mahir dalam teknologi. Namun, kemahiran ini mungkin terbatas pada bidang-bidang spesialis.

Meskipun DNB mungkin terlahir di cloud, mereka mungkin juga kesulitan untuk memanfaatkan potensi penuh dari teknologi yang sedang berkembang di cloud, data, dan kecerdasan buatan (AI).

Kami memetakan tantangan migrasi cloud yang dihadapi responden, sesuai dengan tahapan mereka dalam perjalanan cloud.

Terdapat kesulitan dalam memahami pengeluaran cloud di antara para responden yang telah sepenuhnya bermigrasi ke cloud dan yang masih menjajaki adopsi cloud.

Meskipun sebagian besar penyedia layanan cloud transparan mengenai harga, rincian biayanya sering kali kompleks. DNB perlu memiliki pemahaman yang mendalam serta waktu yang cukup untuk memprediksi dan menghitung biaya terkait layanan mikro dan penerapan multi-cloud, yang skalanya bervariasi bergantung pada berbagai faktor. Sebagai contoh, faktor apa yang mendorong skalabilitas—apakah permintaan dari pengguna akhir atau komunikasi antar proses?

### 3 tantangan teratas yang dihadapi dalam migrasi cloud

| | Mengelola dampak keamanan | Memilih penyedia cloud yang tepat | Menilai kelayakan teknis |
|---|---|---|---|
| Telah dimigrasikan sepenuhnya ke cloud | 45% | 53% | 57% |
| Mengeksplorasi adopsi cloud | 63% | 62% | 52% |
| Dioperasikan dalam lingkungan hybrid | 74% | 49% | 54% |
| Dioperasikan dalam lingkungan multi-cloud | 50% | 44% | 47% |
| Sebagian telah dimigrasikan ke cloud | 45% | 41% | 41% |

Tantangan lainnya:
Memahami alokasi kecepatan cloud, memprioritaskan aplikasi yang akan dimigrasikan, melakukan restrukturisasi/memilih instance terbaik, menilai biaya on-prem vs cloud, kurangnya pakar teknis, memahami kebergantungan aplikasi

Situasi ini telah mendorong DNB untuk memilih penyedia cloud yang menawarkan harga yang mudah dipahami tanpa mengorbankan performa, keandalan, atau dukungan.

Namun, mengelola dampak keamanan terus menjadi tantangan yang konsisten, terlepas dari posisi DNB dalam perjalanan cloud mereka—baik itu yang dioperasikan di lingkungan hybrid, multi-cloud, atau yang baru saja bermigrasi sebagian ke cloud.

Faktanya, sebagian besar responden survei melihat keamanan sebagai celah terbesar dalam infrastruktur cloud mereka saat ini.

*Akamai mempertahankan harga yang sederhana dan transparan dengan biaya keluar yang sangat rendah, tunjangan keluar bulanan yang besar, dan alat untuk memaksimalkan pusat data dan beban lalu lintas cloud.*

*Kombinasi semua ini mewakili banyak peluang untuk mengoptimalkan biaya untuk aplikasi data dan lalu lintas yang intensif dengan memanfaatkan jejak global Akamai.*

Ketika memilih penyedia layanan cloud, fitur keamanan lebih penting daripada performa, reputasi, skalabilitas, dan biaya.

**Menurut Anda, di mana letak celah terbesar dalam hal performa atau kemampuan infrastruktur cloud Anda?**

| | Keamanan | Latensi jaringan | Penyimpanan dan pengambilan data | Sumber daya komputasi |
|---|---|---|---|---|
| Telah dimigrasikan sepenuhnya ke cloud | 65% | 65% | 67% | 47% |
| Mengeksplorasi adopsi cloud | 81% | 58% | 67% | 62% |
| Dioperasikan dalam lingkungan hybrid | 74% | 66% | 49% | 46% |
| Dioperasikan dalam lingkungan multi-cloud | 84% | 66% | 66% | 63% |
| Sebagian telah dimigrasikan ke cloud | 69% | 62% | 62% | 24% |

**Faktor-faktor saat memilih penyedia cloud**

# Pola pikir yang mengutamakan teknologi - kelemahan DNB?

Di sinilah teknologi dapat menjadi keuntungan sekaligus tantangan bagi DNB.

Sebagian besar responden menyebutkan bahwa infrastruktur TI mereka yang rumit adalah hambatan utama dalam memperkuat keamanan siber mereka.

Generasi era digital mengadopsi prinsip desain cloud-native dengan mengutamakan layanan mikro dan API untuk terhubung.

API ini mempercepat implementasi teknologi dan kecepatan ke pasar, memungkinkan DNB untuk melakukan iterasi dengan cepat dan menyediakan fungsionalitas secara efisien.

Namun, kecepatan dan komposabilitas tersebut harus dibayar dengan kerumitan ketika pengembang yang terikat dengan berbagai layanan tidak memiliki insentif untuk fokus pada operasi DNB.

Tim keamanan dan teknologi akan menghadapi tantangan karena sebagian besar alat keamanan tidak mendukung lingkungan hybrid, dan keamanan cloud yang terintegrasi biasanya hanya berfokus pada penyedia cloud itu sendiri.

Sebagai contoh, penyedia game lebih memilih bekerja sama dengan penyedia infrastruktur cloud yang merupakan mitra tepercaya daripada sekadar vendor, mengingat bahwa pengembangan game memerlukan waktu bertahun-tahun.

Perusahaan game dan tim pengembangnya menginginkan wawasan menyeluruh tentang semua aspek komputasi cloud, termasuk performa, alokasi sumber daya, latensi, dan throughput, serta harga yang dapat diprediksi dan transparansi dalam penagihan.

Infrastruktur komputasi cloud yang terdistribusi dengan model bayar sesuai pemakaian dan bayar sesuai kebutuhan sangat menarik bagi penyedia game yang ingin memantau biaya operasional yang tidak langsung terkait dengan pengembangan atau peningkatan game.

Temuan survei menunjukkan bahwa DNB dihadapkan pada infrastruktur TI yang semakin kompleks, yang berdampak pada postur keamanan siber organisasi mereka.

**Tantangan terbesar dalam meningkatkan postur keamanan siber**

| | Infrastruktur TI yang rumit | Persyaratan kepatuhan setempat | Kekurangan tenaga ahli | Kendala anggaran | Ancaman yang berkembang pesat |
|---|---|---|---|---|---|
| Telah dimigrasikan sepenuhnya ke cloud | 43% | 7% | 13% | 12% | 25% |
| Mengeksplorasi adopsi cloud | 37% | 6% | 10% | 27% | 21% |
| Dioperasikan dalam lingkungan hybrid | 49% | 3% | 9% | 23% | 17% |
| Dioperasikan dalam lingkungan multi-cloud | 59% | 13% | 13% | 6% | 9% |
| Sebagian telah dimigrasikan ke cloud | 31% | 7% | 17% | 14% | 31% |

# Menyeimbangkan risiko vs manfaat

Berikut kenyataan yang dihadapi: Menerapkan kebijakan keamanan yang konsisten di seluruh cloud tidaklah mudah.

DNB yang lebih muda mungkin menikmati kecepatan yang ditawarkan oleh teknologi cloud, namun seiring pertumbuhan bisnis, mereka perlu menyeimbangkan risiko dan manfaat dari setiap inovasi teknologi. Setiap teknologi inovatif memperkenalkan lapisan kompleksitas tambahan.

Lalu, bagaimana cara Anda menyeimbangkan kecepatan ke pasar dan adopsi pelanggan dengan keamanan, kepatuhan, dan pengelolaan untuk mencegah pelanggaran atau penyalahgunaan?

Hal ini tetap menjadi tantangan utama dalam meningkatkan keamanan siber, terlepas dari posisi DNB dalam perjalanan cloud mereka.

> ***Akamai Connected Cloud adalah platform terbuka yang mengadopsi arsitektur open-source dan multi-cloud. Arsitektur ini dirancang khusus untuk memudahkan pengembang dalam memanfaatkan aplikasi dan perangkat lunak yang mereka pilih, sambil menyediakan layanan yang mendukung beban kerja yang dapat diskalakan secara global, teroptimasi secara regional, dan memiliki latensi rendah.***

Teknologi cloud kini telah berkembang dari sekadar menyediakan infrastruktur menjadi menawarkan berbagai layanan, termasuk manajemen infrastruktur.

Menjalankan infrastruktur cloud-native membawa risiko konsentrasi serta tantangan infrastruktur yang kompleks.

Berikut adalah beberapa hal yang perlu Anda pertimbangkan, terlepas dari posisi Anda dalam proses adopsi cloud:

### Adopsi strategi multi-cloud

Organisasi perlu menerapkan pendekatan multi-cloud untuk menghindari ketergantungan pada vendor, meningkatkan fleksibilitas, dan mengoptimalkan penggunaan layanan cloud.

Menurut survei Forrester Research terhadap para pemimpin TI, persyaratan utama untuk vendor cloud adalah kemampuan untuk menerapkan dan mengeksekusi dari cloud ke edge

Ketergantungan yang berlebihan pada satu vendor dapat membatasi pilihan teknologi di masa depan dan memberi vendor tersebut pengaruh besar terhadap arah teknologi organisasi.

Memanfaatkan platform terdistribusi yang agnostik memungkinkan generasi era digital untuk mengakses data mentah dengan mudah dan cepat, serta memperoleh wawasan dari data yang tersebar di berbagai sistem.

### Tinjau dan ulangi secara rutin

Tinjau biaya cloud secara berkala untuk menganalisis dan mengoptimalkan pengeluaran cloud, mengidentifikasi area yang dapat dihemat, dan mengoptimalkan penggunaan sumber daya.

Gunakan data pemantauan dan analisis real-time untuk mengidentifikasi area yang dapat dioptimalkan, seperti alokasi sumber daya, manajemen biaya, dan peningkatan keamanan.

Pemantauan dan pengoptimalan rutin memastikan bahwa Anda mendapatkan nilai bisnis maksimal dari investasi cloud Anda.

---

### Terapkan framework pengelolaan cloud

Semakin banyak aplikasi dan proses bisnis yang bergantung pada penyedia cloud tertentu, semakin besar dampak potensial dari masalah layanan cloud, yang dapat meningkatkan kekhawatiran mengenai kelangsungan bisnis.

Kembangkan dan terapkan kebijakan pengelolaan cloud untuk mengelola sumber daya cloud secara efektif, memastikan kepatuhan, serta mengontrol biaya.

Model ini harus mencakup kontrol akses, langkah-langkah keamanan, manajemen biaya, dan persyaratan kepatuhan. Model pengelolaan yang jelas membantu memastikan konsistensi dan penerapan praktik terbaik di seluruh organisasi.

Organisasi juga mungkin kesulitan memenuhi tuntutan peraturan untuk mengatasi risiko konsentrasi, terutama jika berbagai badan pengatur memiliki pendekatan yang berbeda terhadap risiko ini.

# Memprioritaskan keamanan API lanjutan

API merupakan pusat dari DNB dalam menghubungkan arsitektur non-cloud, cloud, dan multi-cloud.

API memungkinkan DNB mencapai tingkat konektivitas, produktivitas, dan kelincahan yang baru dengan menghubungkan aplikasi internal, mempercepat proses bersama mitra bisnis, dan menyediakan layanan data kepada konsumen.

Dalam upaya mencapai kecepatan dan inovasi berbasis teknologi, aplikasi dan proses bisnis yang menggunakan API sering kali diluncurkan dan digunakan lebih cepat daripada yang dapat dievaluasi oleh tim keamanan.

Kesalahan konfigurasi dan kerentanan, ditambah dengan kurangnya keahlian keamanan API, membuat DNB yang inovatif rentan terhadap potensi ancaman siber.

Faktanya, survei industri terhadap 631 profesional keamanan siber menunjukkan bahwa satu dari dua pengembang menghabiskan hingga setengah waktu mereka untuk melakukan refactoring dan perbaikan API.

> ***31%*** *dari lalu lintas yang dilindungi oleh Akamai merupakan lalu lintas API. Akamai menyediakan alat untuk mempertahankan kontrol yang konsisten atas aplikasi dan beban kerja Anda dengan kemampuan pengoptimalan pengalaman pengguna yang terintegrasi.*

DNB di seluruh Asia secara konsisten menjadikan keamanan API sebagai prioritas utama untuk mendukung pertumbuhan bisnis yang berkelanjutan.

Baik saat ekspansi di Australia maupun saat memperluas pangsa pasar di India dan ASEAN, DNB menempatkan keamanan API lanjutan sebagai prioritas utama dalam investasi keamanan siber, di atas keamanan web/aplikasi dan teknologi anti-phishing.

**Urutkan area investasi keamanan siber berikut dari yang paling penting (atas) hingga yang paling kurang penting (bawah).**

1. Keamanan API lanjutan
2. Keamanan aplikasi web
3. Teknologi anti-phishing
4. Mitigasi distributed denial-of-service (DDoS)
5. Teknologi terkait Zero Trust

**Kondisi kesalahan keamanan API**

Implementasi cepat proses bisnis penting melalui API + Kurangnya visibilitas ke API = API yang salah konfigurasi atau rentan

Menurut data lalu lintas Akamai, sektor manufaktur mencatat persentase serangan API tertinggi di seluruh Asia Pasifik dan Jepang.

Hal ini mungkin sebagian disebabkan oleh meningkatnya konektivitas sektor infrastruktur penting ini melalui API, serta potensi gangguan pada rantai pasokan.

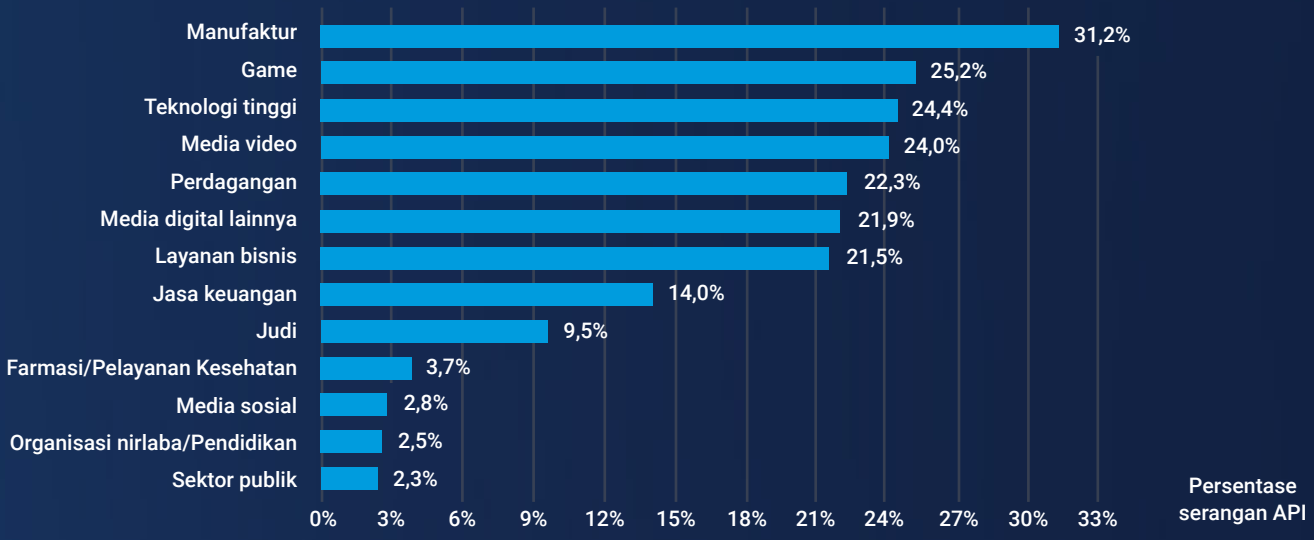
Pada saat yang sama, industri yang sangat bergantung pada teknologi digital, seperti game, teknologi tinggi, media video, dan perdagangan, juga menjadi sasaran serangan API.

Alasan mengapa generasi era digital sering menjadi target adalah karena sebagian besar bisnis mereka bergantung pada API, mereka memiliki infrastruktur cloud yang luas, dan merupakan sasaran yang lebih menarik untuk phishing, kompromi akun, dan ransomware dibandingkan dengan perusahaan dan arsitektur tradisional.

Local File Inclusion (LFI) tetap menjadi vektor serangan API utama, tetapi data tahun 2023 juga mengungkapkan vektor tambahan seperti injeksi perintah (CMDi) dan pemalsuan permintaan sisi server (SSRF). Vektor-vektor ini menimbulkan risiko yang signifikan pada API yang rentan, salah konfigurasi, atau tidak terdokumentasi.

Permintaan bot juga menjadi salah satu area yang perlu diperhatikan. Selama periode pelaporan 12 bulan yang sama, 40% dari lebih dari dua triliun permintaan bot yang mencurigakan ditujukan ke API.

APJ: Serangan API secara vertikal (1 Januari 2023 - 31 Desember 2023)




APJ: Serangan API berdasarkan vector (1 Januari 2023 - 31 Desember 2023)

## Pertimbangan penting terkait keamanan API

Kerentanan keamanan API selalu berubah seiring waktu. Dengan memahami beberapa risiko keamanan API terbesar, organisasi Anda bisa tetap selangkah lebih maju dalam menghadapi ancaman.

### Penemuan dan visibilitas

Versi API lawas atau sebelumnya yang belum dihentikan atau didokumentasikan dengan benar dapat meningkatkan risiko bagi bisnis. Misalnya, API shadow ada dan beroperasi di luar lingkup pengelolaan dan bisa menjadi titik kelemahan.

### Perlindungan runtime

Karena API dijalankan untuk bertukar data secara aktif, mungkin sulit bagi alat keamanan konvensional untuk membedakan antara permintaan yang sah dan permintaan berbahaya yang diajukan API. Ancaman yang bersifat mengelabui seperti penyalahgunaan logika API dikenal sulit terdeteksi karena mampu berbaur dengan permintaan API yang biasa.

### Uji API

Uji keamanan API harus diintegrasikan di setiap fase pengembangan untuk meningkatkan keamanan tanpa mengganggu kecepatan. Dari perspektif biaya dan perbaikan, lebih mudah untuk memperbaiki masalah selama fase pengembangan API daripada setelah API dirilis ke dalam tahap produksi dan digunakan secara aktif.

### Akses sumber daya yang tidak diautentikasi

Autentikasi dan otorisasi lebih rumit untuk skenario mesin-ke-mesin. Pengguna atau sistem mungkin dapat mengakses sumber daya API tanpa memberikan autentikasi apa pun, hal ini sering disebabkan karena adanya kesalahan dalam penerapan atau konfigurasi API.

### Data sensitif di URL

Data sensitif di URL kerap disimpan di tempat yang mudah diakses oleh penyerang, seperti log dan cache, sehingga menimbulkan risiko kebocoran data sensitif dan masalah kepatuhan yang cukup besar.

### Kebijakan permissive cross-origin resource

API bisa mengizinkan permintaan dari berbagai sumber yang lebih luas (seperti protokol, domain, dan port) daripada yang diperlukan.

# Pentingnya mengutamakan keamanan API sejak awal

Sembilan dari sepuluh DNB yang disurvei menyatakan bahwa keamanan API sebagai fitur produk yang penting saat mengevaluasi penyedia solusi cloud/keamanan.

Seiring meningkatnya laju inovasi teknologi dan koneksi pihak ketiga, DNB memerlukan dukungan dari vendor mereka untuk mengidentifikasi potensi tautan lemah yang dapat dieksploitasi oleh lawan siber.

Keamanan API perlu diintegrasikan ke dalam setiap tahap proses pengembangan. Kurangnya kerangka kerja pengujian API dan alat uji API tertentu bisa membuat makin banyak API yang rentan dipublikasikan, yang bisa meningkatkan terjadinya insiden terkait keamanan API. Kurangnya visibilitas terhadap penyalahgunaan logika bisnis API menjadi faktor lain yang menyebabkan pelanggaran dan penipuan data API.

Misalnya, bagaimana tim keamanan mengetahui kapan API sedang disalahgunakan saat beroperasi? Serangan apa yang menargetkan API organisasi Anda saat ini?

Tim keamanan mungkin tidak sepenuhnya memahami tujuan endpoint API, misalnya, dan akan mengalami kesulitan untuk mengetahui beban kerja back-end yang berinteraksi dengan endpoint tersebut atau tipe data yang dipertukarkan. Tim pengembangan mungkin juga terlalu yakin dengan kemampuan mereka untuk memperbaiki bug di akhir siklus pengembangan.

Penemuan dan pembuatan profil yang didukung AI merupakan tren penting dalam keamanan API, tetapi pendekatan yang mengutamakan keamanan di awal proses pengembangan (DevSecOps) membantu memperkecil kerentanan DNB sejak dini, sehingga membantu membangun prinsip pengembangan API yang aman sejak awal.

Mengidentifikasi celah keamanan API tingkat lanjut sejak awal ini dapat membantu membangun struktur keamanan siber yang lebih kuat.

**Seberapa pentingkah fitur-fitur produk berikut ini saat mengevaluasi penyedia solusi cloud atau keamanan?**

| | Sangat penting | Penting | Agak penting | Biasa saja | Kurang penting |
|---|---|---|---|---|---|
| Keamanan API | 45,60% | 45,10% | 7,40% | 1,90% | 0,00% |
| Kebijakan keamanan cloud yang bisa disesuaikan | 31,20% | 53,90% | 8,40% | 6,50% | 0,00% |
| Kemampuan komputasi edge | 29,80% | 47,00% | 15,80% | 6,00% | 0,90% |
| Observabilitas | 28,40% | 52,10% | 11,20% | 7,00% | 0,90% |
| Analisis dan pelaporan real-time | 45,60% | 34,40% | 11,20% | 7,40% | 1,40% |
| Zero Trust | 32,60% | 39,10% | 14,40% | 9,30% | 0,90% |

## Celah keamanan API yang umum

### Upaya akses sumber daya yang tidak diautentikasi

Celah keamanan ini lebih mendesak dibandingkan peringatan postur akses sumber daya yang tidak diautentikasi, yang dijelaskan di bagian sebelumnya, di mana kita melihat upaya tertentu untuk mengakses sumber daya API sensitif tanpa autentikasi yang relevan. Meski upaya yang diamati tidak berhasil, skenario ini menunjukkan upaya aktif untuk menemukan dan memanfaatkan kerentanan API, yang pada akhirnya mungkin berhasil tanpa intervensi langsung.

### Upaya fuzzing parameter path

Fuzzing parameter path adalah contoh lain dari pengiriman sengaja data yang tidak sesuai atau rusak sebagai bagian dari permintaan API, dengan fokus pada bagian-bagian URL yang digunakan oleh API RESTful untuk menentukan sumber daya atau operasi tertentu. Ini adalah teknik lain yang digunakan penyerang untuk melakukan pengintaian guna menemukan API yang berpotensi rentan, yang dapat dijadikan sasaran upaya pencurian data atau gangguan layanan.

### Scraping data

Scraping data adalah pengambilan data secara otomatis dari API dengan cara dan jumlah yang tidak sesuai dengan tujuan penggunaan dan ketentuan layanan API. Penyerang sering kali mengumpulkan data ini secara perlahan agar tidak terdeteksi dan untuk mencuri kekayaan intelektual, mengumpulkan data sensitif pelanggan, atau mendapatkan keuntungan. Jika teknik scraping data yang dilakukan dengan perlahan dan bertahap tidak terdeteksi dalam API, serangan ini bisa mengakibatkan pelanggaran data yang signifikan.

### Properti JSON yang tidak biasa

Aktivitas API dengan payload JSON yang tidak biasa, seperti tipe data yang tidak terduga, ukuran yang tidak normal, atau kompleksitas yang berlebihan, bisa menandakan adanya upaya aktif untuk memanfaatkan API yang rentan. Aktivitas ini dapat mengindikasikan adanya upaya untuk melakukan berbagai tindakan berbahaya, seperti serangan injeksi, penolakan layanan, pencurian data, atau pemanfaatan kelemahan logika API.

### Perjalanan waktu yang tidak mungkin dilakukan

Ketika menganalisis aktivitas API, ada beberapa skenario yang stempel waktu, geolokasi, atau urutan panggilan API-nya tidak logis. Ini menunjukkan bahwa penyerang berupaya memanipulasinya dengan cara tertentu. Selain itu, jenis perilaku ini dapat menunjukkan beberapa kemungkinan ancaman seperti manipulasi data sebagai bagian dari aktivitas penipuan.

# Pendekatan keamanan API modern

API modern adalah penghubung utama yang mendukung layanan mikro, multi-cloud, integrasi tanpa batas, dan ekspansi cepat. API ini merupakan elemen penting tetapi rentan dalam aplikasi atau beban kerja dan harus dirancang, dikembangkan, dan diterapkan dengan benar untuk mengoptimalkan hasil bisnis.

Namun, organisasi cenderung menerapkan langkah-langkah keamanan yang sama meski permintaan API modern cenderung memiliki karakteristik unik, seperti permintaan dengan frekuensi tinggi.

### 1 Menerapkan penemuan API otomatis

Pastikan API yang Anda sediakan dan gunakan diidentifikasi dengan benar agar terlindung dari pelanggaran keamanan terkait API, ketergantungan yang tidak diketahui, dan inkonsistensi yang tidak terduga. Integrasi langsung ke sumber data API akan membantu mengurangi kompleksitas dan beban operasional.

### 2 Mengelola postur API

Evaluasi keamanan API meliputi pendeteksian kesalahan konfigurasi, penerapan uji penetrasi, atau penggunaan alat penilaian otomatis yang secara proaktif memindai masalah konfigurasi seperti API yang menampilkan data sensitif dalam URL. Tanggapan otomatis memastikan bahwa pihak yang relevan seperti tim pengembangan API dapat dipanggil untuk memperbaiki masalah sebagai bagian dari alur kerja penanganan.

### 3 Pelindungan runtime API

Ini meliputi pendeteksian pola yang mengindikasikan aktivitas berbahaya. Mesin deteksi anomali, yang dilatih dengan set data serangan serupa, dapat mengidentifikasi ancaman dan memberi tahu pihak-pihak terkait. Alur kerja penanganan dapat mulai dilakukan untuk membuat permintaan perbaikan atau menghalangi potensi ancaman jika terdeteksi lalu lintas API yang tidak normal.

### 4 Uji keamanan proaktif

Uji keamanan API melalui pemindaian dinamis dan fuzzing dapat mengidentifikasi kerentanan teknis yang mungkin tidak terdeteksi sebagai kesalahan konfigurasi selama penilaian awal.

Seiring dengan makin tingginya tingkat keamanan API Anda, pengujian keamanan harus diintegrasikan secara lebih ketat ke dalam siklus pengembangan API, dengan kerentanan yang segera diatasi ketika ditemukan — sebelum mencapai tahap produksi. Artinya, kolaborasi antara tim keamanan dan pengembangan amatlah penting.

### 5 Ekosistem keamanan API

Memiliki ekosistem teknologi yang kaya dan kuat di mana solusi keamanan API-nya dapat terintegrasi secara langsung dan beroperasi bersama dengan teknologi pihak ketiga bisa memangkas biaya dan mempercepat waktu implementasi. Hal ini juga memberikan visibilitas lalu lintas API yang lebih luas dari sumber data, tanggapan terhadap ancaman yang lebih cepat melalui alur kerja otomatis, dan postur keamanan API yang lebih baik secara keseluruhan.

# Australia/Selandia Baru: Dari tahap awal hingga berkembang pesat

Laporan analis menunjukkan rendahnya permintaan domestik dan permintaan tenaga kerja di Australia/Selandia Baru (ANZ) dalam beberapa tahun mendatang.

Pelanggan telah merasakan tekanan keuangan seiring rendahnya peningkatan upah dan inflasi yang berkelanjutan.

Mungkin sebagai tanggapan atas kondisi ekonomi saat ini, para responden DNB dari ANZ mengutamakan efisiensi dan ketahanan organisasi.

Adanya perubahan cara pandang yang menganggap bahwa teknologi cloud kini menjadi komponen penting bagi bisnis, Sebanyak 97% responden telah menggunakan teknologi cloud atau mempertimbangkan untuk menggunakan cloud.

Organisasi-organisai di ANZ mungkin semakin maju dalam pemanfaatan teknologi cloud untuk meningkatkan efisiensi operasional mereka di tengah melambatnya laju ekonomi.

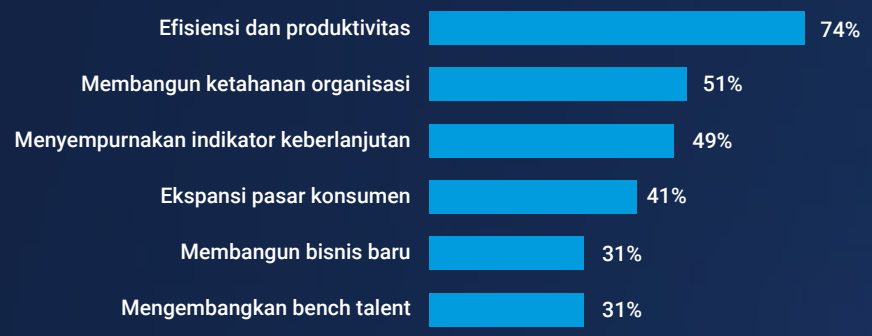
## Ringkasan prediksi penting

| Tahun | 2020 | 2021 | 2022 | 2023 | 2024f | 2025f | 2026f |
|---|---|---|---|---|---|---|---|
| PDB riil[1] (% perubahan rata-rata tahunan) | -1,4 | 5,6 | 2,4 | 0,6 | 0,5 | 1,5 | 2,5 |
| Tingkat pengangguran (sa; kuartal Des.) | 4,9 | 3,2 | 3,4 | 4,0 | 5,1 | 5,5 | 5,0 |
| Inflasi IHK (% perubahan tahunan; kuartal Des.) | 1,4 | 5,9 | 7,2 | 4,7 | 2,6 | 2,0 | 2,0 |
| Suku bunga acuan (Akhir kuartal Des.) | 0,25 | 0,75 | 4,25 | 5,50 | 5,50 | 4,75 | 4,00 |

[1] Berbasis produksi

*Sumber: Statistics NZ, REINZ, Bloomberg, ANZ Research*

## Prioritas bisnis utama dalam 12 bulan ke depan



Misalnya, tak hanya memanfaatkan cloud publik perangkat lunak terpisah sebagai solusi berbasis layanan untuk menggantikan infrastruktur, seperti pemulihan bencana, kini ANZ memanfaatkan cloud ke tingkat yang lebih tinggi, yang mendorong transformasi digital dan inovasi di seluruh organisasi.

Kematangan relatif dalam penggunaan cloud ini telah mengubah cara pandang, cloud yang awalnya dianggap sebagai penghambat kinerja bisnis kini justru menjadi elemen penting bagi bisnis.

Sektor publik berperan penting dalam mendorong penggunaan cloud di Australia dan Selandia Baru.

Selandia Baru mengajukan kebijakan pemerintah yang mengutamakan cloud pada tahun 2012 sementara Australia melakukannya pada tahun 2015.

Perusahaan-perusahaan Australia diperkirakan menghabiskan $15.4 miliar untuk cloud publik pada tahun 2024, hingga 19,7% dari 2023 (sumber: Gartner).

Organisasi ANZ yang lebih dulu memanfaatkan teknologi digital mungkin memiliki aplikasi lama yang tidak dirancang untuk cloud, tidak dikontainerisasi, atau tidak berbasis layanan mikro. Artinya, mereka harus lebih banyak mengeluarkan biaya untuk aplikasi tersebut, dibandingkan aplikasi yang dirancang khusus untuk cloud.

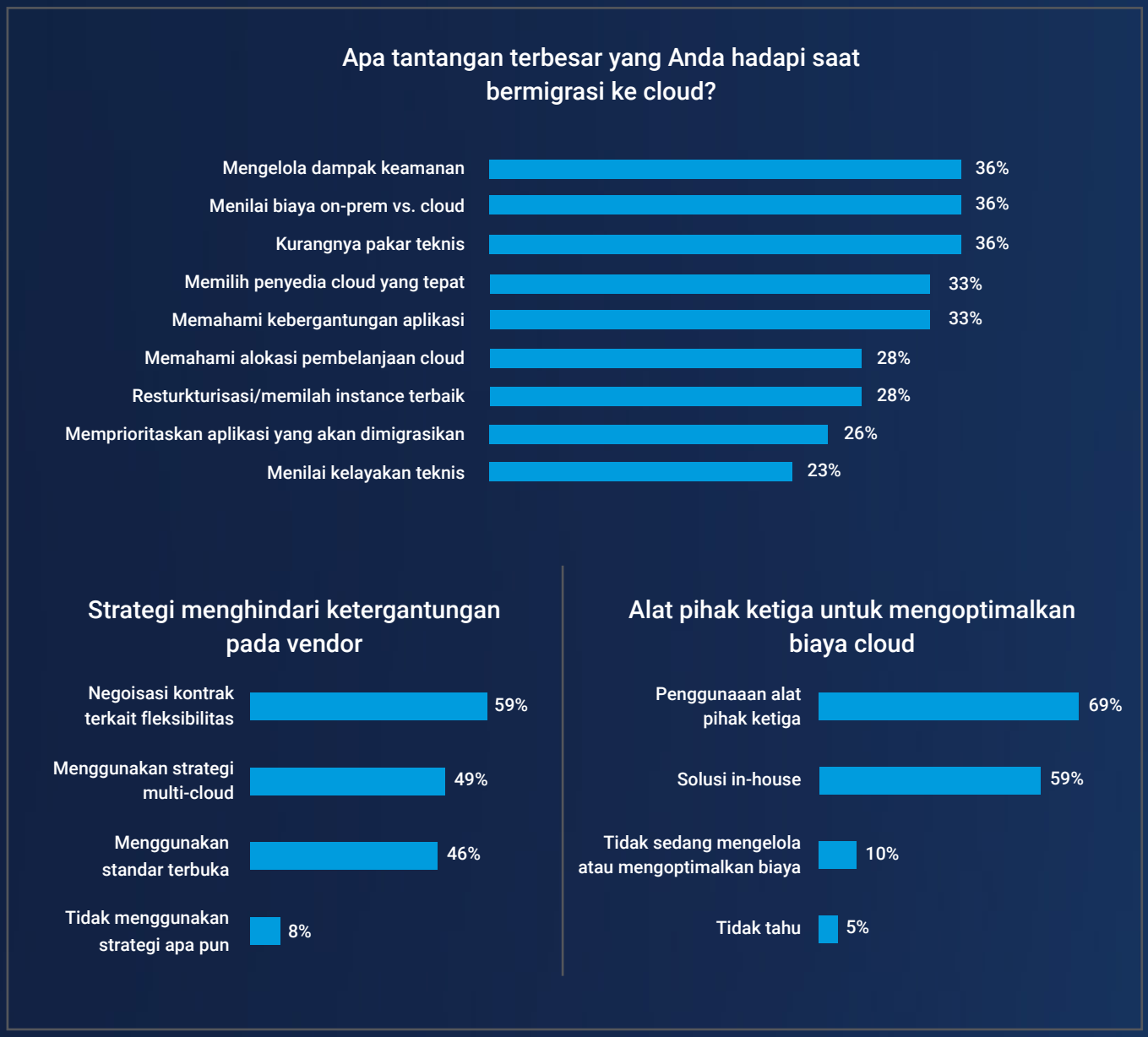
**Sejauh mana perjalanan adopsi cloud perusahaan Anda saat ini?**


Responden survei ANZ menyebutkan bahwa biaya, masalah keamanan, dan kurangnya pakar teknis menjadi kendala utama dalam proses migrasi ke cloud.

Tingkat penggunaan teknologi yang makin luas, disertai tekanan inovasi dan ekonomi yang lesu, mendorong organisasi untuk mengurangi penggunaan cloud yang tidak perlu.

Penghitungan biaya untuk cloud tidaklah sederhana karena perlu keahlian dan waktu untuk memperkirakan dan menguraikan biaya penerapan layanan mikro serta multi-cloud. Biaya penerapan ini berbeda-beda tergantung faktor.

Solusi manajemen biaya cloud seperti FinOps memperkenalkan akuntabilitas keuangan ke dalam model pengeluaran variabel cloud. Pengguna bertanggung jawab atas keputusan terkait pengeluaran biaya dengan mengetahui penggunaan cloud organisasi dan potensi peningkatan produktivitas




Para pemimpin TI ANZ memanfaatkan alat pihak ketiga, layanan terkelola, dan negosiasi kontrak dengan jumlah pengeluaran yang lebih tinggi atau tingkat pertumbuhan yang lebih besar untuk mendapatkan potongan harga.

Menggabungkan manajemen operasi cloud dengan tata kelola keuangan dapat melindungi organisasi dari penskalaan otomatis yang tidak terbatas yang dapat menghabiskan anggaran cloud tahunan Anda dalam semalam.

Ini menunjukkan bahwa DNB cukup matang dalam menggunakan cloud karena memanfaatkan alat pihak ketiga dan layanan terkelola untuk mendukung staf khusus mencapai skala yang efisien dan berkelanjutan.

*Jaringan global Akamai terintegrasi ke dalam* ***1.200*** *jaringan di seluruh dunia dan mempertahankan interkoneksi yang dioptimalkan dengan semua penyedia cloud utama untuk memastikan layanan selalu tersedia, transfer data cepat, dan skala yang tak terbatas.*

# Perlu lebih banyak data sensitif untuk meningkatkan pengalaman pelanggan

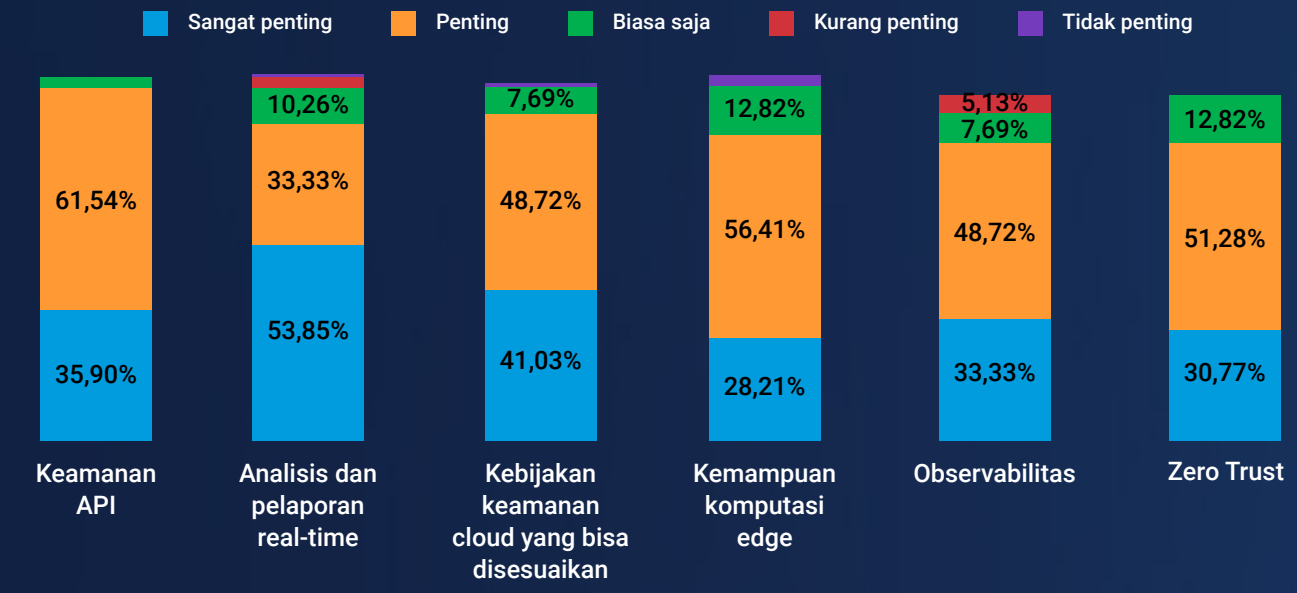
Dengan penerapan digital pelanggan yang relatif matang, pelaku bisnis di ANZ ingin mengumpulkan, memproses, menganalisis, dan mengambil tindakan berdasarkan data real-time demi menghadirkan pengalaman pengguna yang optimal.

Sebanyak 87% responden di ANZ menyebutkan analisis dan pelaporan real-time merupakan fitur produk yang amat penting dalam mengevaluasi penyedia solusi cloud/keamanan.

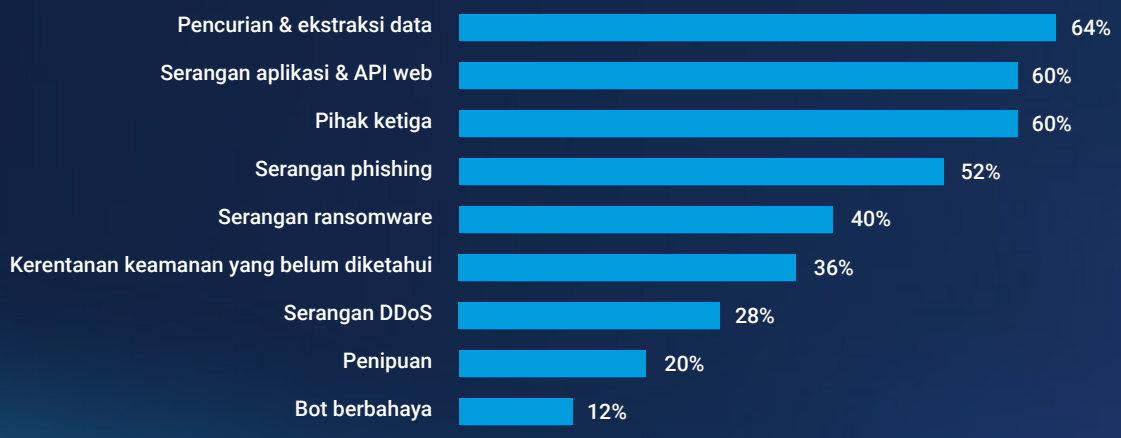
Di saat yang sama, upaya untuk menghadirkan pengalaman pelanggan yang lebih luas di antara generasi era digital di ANZ juga berisiko membuat mereka terpapar serangan siber yang menargetkan data pribadi dan keuangan yang berharga.

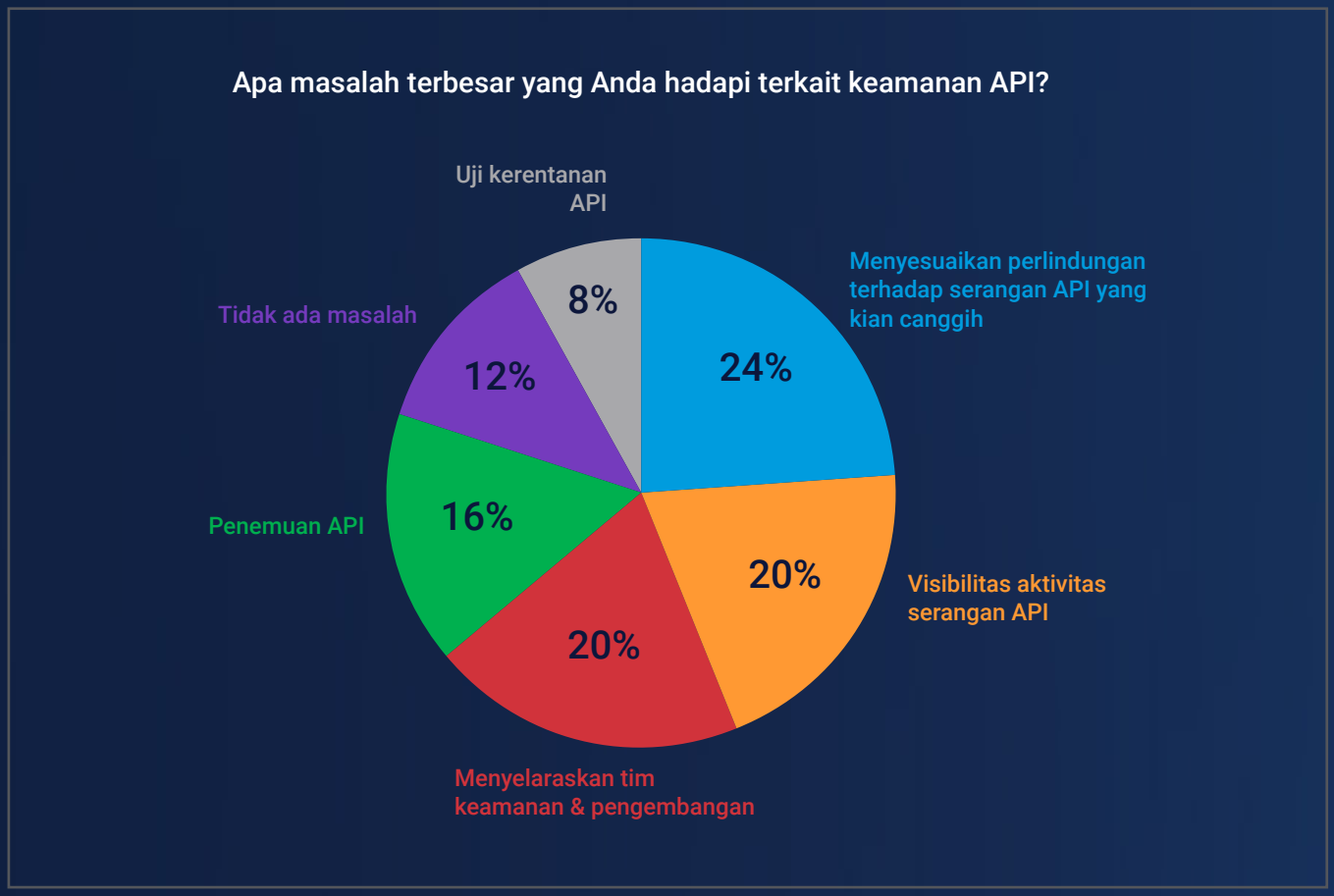
Menurut laporan Akamai terkait Keamanan Siber dalam Jasa Keuangan, serangan terhadap aplikasi web dan API serta pencurian dan ekstraksi data merupakan acaman siber yang paling diwaspadai para pemimpin TI di Australia.

### Seberapa penting fitur produk berikut dalam mengevaluasi penyedia solusi cloud/keamanan?




### Ancaman siber yang paling diwaspadai para pemimpin TI di Australia






Selain itu, terdapat dimensi keamanan, seperti yang dirasakan para pemimpin TI ANZ bahwa masalah terbesar mereka terkait keamanan API adalah mendapatkan visibilitas aktivitas serangan API (20%) dan mengadaptasi perlindungan atas serangan API yang lebih canggih (24%).

Seperti kata pepatah, “kita tidak bisa melindungi apa yang tak nampak”. Banyak perusahaan bahkan tidak sadar berapa banyak API yang benar-benar mereka miliki, jadi sulit untuk mengukur risikonya.

Salah satu kejutan terbesar bagi para perusahaan yang meningkatkan visibilitas aktivitas API mereka adalah jumlah endpoint shadow yang dijalankan dari dalam lingkungan tanpa sepengetahuan mereka.

Hasilnya, 97% responden ANZ menandai keamanan API sebagai fitur produk vital/penting saat mengevaluasi penyedia solusi cloud/keamanan.

Di sini lah analisis dan pelaporan real-time memungkinan deteksi dan tanggapan yang lebih cepat serta mengurangi kerusakan jika terjadi serangan siber.

# Menyatukan ASEAN: Ekonomi digital mendorong pertumbuhan regional

Asia Tenggara adalah pasar internet dengan pertumbuhan tercepat di dunia, terdapat 125.000 pengguna baru di internet setiap harinya (Sumber: World Economic Forum).

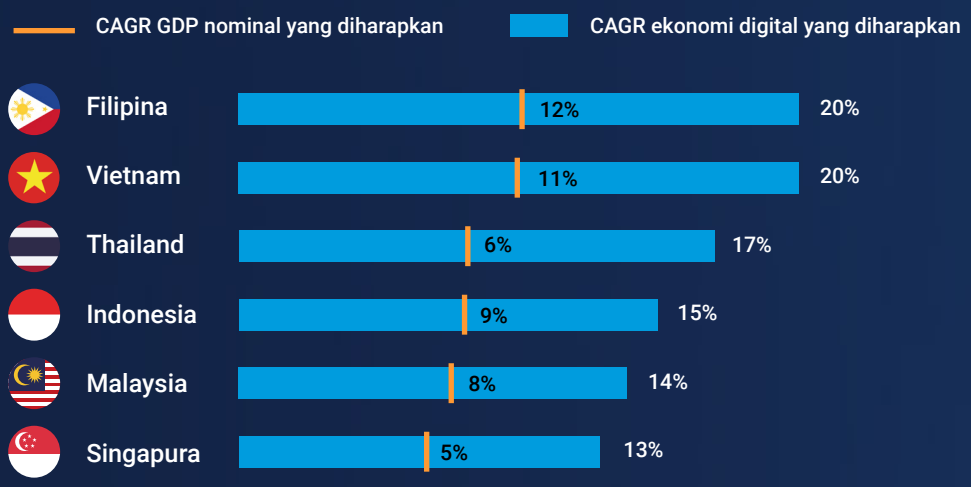
Generasi era digital serta milenial dan Gen Z yang terhubung diperkirakan menjadi 75% konsumen ASEAN dan 70% konsumen Indonesia pada tahun 2030 (Sumber: World Economic Forum).

Kenyataannya, nilai pasar kotor ekonomi digital melebihi pertumbuhan GDP di seluruh negara di ASEAN (Sumber: e-conomy SEA 2023).

Meski konsumen ASEAN secara cepat beradaptasi dengan kehidupan digital, infrastruktur regional masih memerlukan penyesuaian. Generasi muda yang melek teknologi digital memiliki ekspektasi tinggi terhadap uptime server dan latensi rendah.

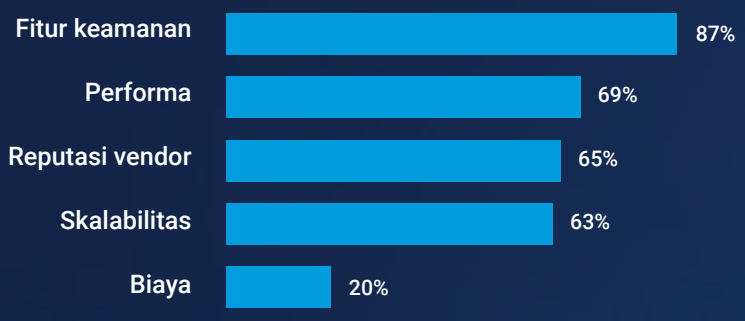
Oleh karena itu, performa dan reputasi vendor diperkirakan mendapat peringkat yang tinggi, yaitu 69% dan 65% secara berturut-turut, untuk pemilihan vendor di antara responden ASEAN.

## Pertumbuhan GMV ekonomi digital vs. pertumbuhan GDP (2023-2025)




(Sumber: e-conomy SEA 2023, Google, Temasek, dan Bain & Company)

## Faktor yang memengaruhi pemilihan vendor cloud



Di saat yang bersamaan, latensi jaringan menjadi masalah dari waktu ke waktu bagi DNB di ASEAN.

Wilayah ini masih perlu memastikan adanya koneksi internet berkecepatan tinggi dan andal serta ketersediaan listrik yang merata di daerah pinggiran kota dan pedesaan. Ketimpangan konektivitas masih ditemukan di negara-negara yang terpisah secara geografis seperti Indonesia dengan 17.508 kepulauannya (sumber tidak resmi mencantumkan jumlah pulau mendekati 25.000!).

Dua dari tiga responden menyebutkan bahwa latensi jaringan menjadi jurang pemisah dalam performa dan kapabilitas infrastruktur cloud perusahaannya.

Demi menunjang pertumbuhan berkelanjutan ini, pemerintah masing-masing daerah secara aktif berinvestasi dalam konektivitas.

Baru-baru ini Indonesia telah menyelesaikan proyek Palapa Ring, yang mengusung konektivitas internet 4G ke daerah-daerah terluar, dengan lebih dari 35.000 km kabel serat optik yang terbentang di daratan dan lautan Indonesia.

> *Akamai menyediakan infrastruktur di lebih banyak daerah dibandingkan penyedia lain, sumber daya komputasi cloud di bagian core dan edge, serta kemampuan untuk menyediakan dan menskalakan aplikasi latensi rendah dan intensif data secara global yang dirancang untuk memenuhi preferensi wilayah setempat.*

# Keamanan API adalah fitur produk penting untuk ASEAN

DNB ASEAN sangat sadar bahwa API membantu operasional perusahaan mereka dan memfasilitasi kolaborasi dengan vendor dan mitra ekosistem lain.

Para responden ASEAN memiliki kepercayaan tertinggi (99%) dalam mengenali dan memitigasi serangan canggih API dibandingkan rekan mereka di ANZ (69%) dan India (91%).

Hampir semua responden ASEAN (99%) menandai keamanan API sebagai hal vital/penting.

Namun, API sprawl itu nyata, dan pertumbuhan yang cepat berarti tidak adanya visibilitas, yang dengan cepat dapat berubah menjadi masalah keamanan dan kepatuhan.

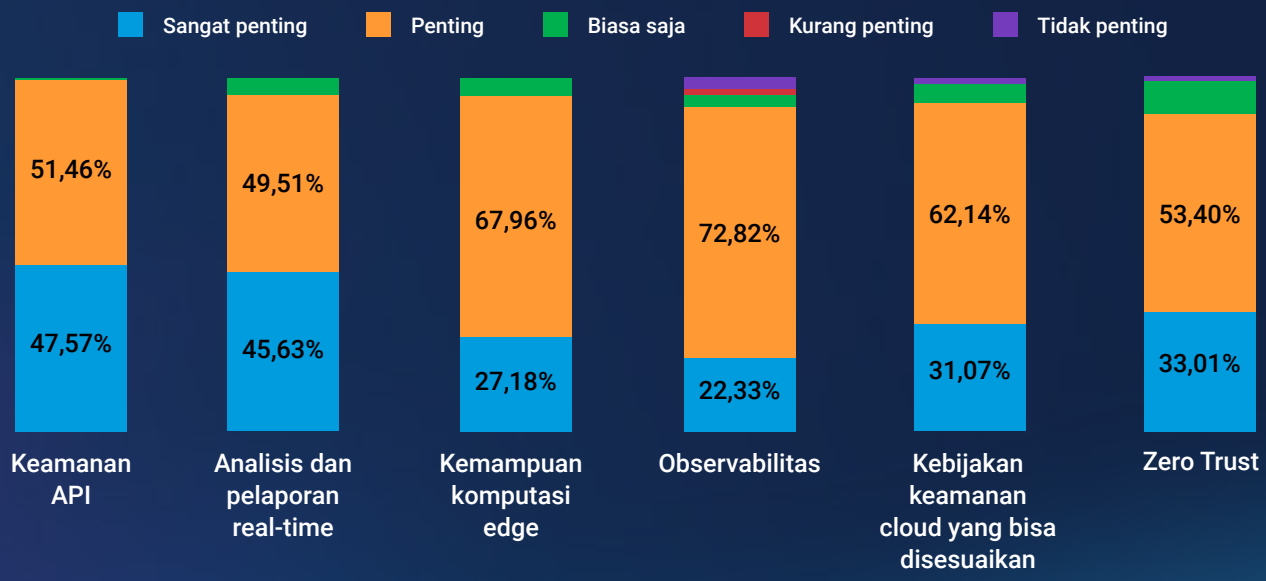
Visibilitas adalah hal fundamental dalam keamanan API. Setelah titik buta seperti API shadow atau API rouge diketahui, tim keamanan dapat mulai menangani kerentanan yang sebelumnya tidak disadari.

Oleh karena itu, analisis dan pelaporan real-time dinilai sebagai hal vital/penting oleh 95% responden ASEAN. Tanpa pemeliharaan yang tepat, API dapat menjadi sumber kebocoran data, pelanggaran kepatuhan, dan kekurangan dalam tata kelola perusahaan.

**Seberapa percaya Anda dalam mengenali dan memitigasi serangan canggih API seperti yang tercantum di OWASP API Top 10?**

| Geografi | Percaya/Sangat percaya |
|---|---|
| ASEAN | 99% |
| ANZ | 69% |
| India | 91% |

**Seberapa penting fitur produk berikut dalam mengevaluasi penyedia solusi cloud/keamanan?**



# Pertumbuhan digital yang belum pernah terjadi sebelumnya menghadirkan kekhawatiran terhadap phising

Tingginya tingkat proses adopsi digital menjadi pedang bermata ganda bagi DNB ASEAN

Adopsi digital terjadi secara cepat sehingga pelanggan tidak lagi mengacuhkan perihal privasi saat mereka bertukar informasi online. Phising telah berkembang dari serangan berbasis email menjadi serangan yang kini juga menyertakan perangkat seluler dan media sosial.

Akibatnya, wilayah ASEAN mengalami salah satu tingkat phishing tertinggi, dengan hampir 500.000 kasus yang dilaporkan pada tahun 2023.

Perlindungan data dan undang-undang privasi di seluruh ASEAN sangat bergantung pada kemampuan pemerintah masing-masing untuk menyesuaikan diri terhadap tren komunikasi digital yang berubah dengan cepat. Misalnya, tautan yang dapat diklik dalam pesan teks masih menjadi taktik penipuan yang populer, meski beberapa negara kini telah menerapkan kebijakan untuk memblokir metode phising yang umum ini.

Responden DNB ASEAN memprioritaskan investasi dalam teknologi anti-phishing lebih dulu dibanding rekannya di wilayah yang sama.

Phishing tidak akan hilang.

Meningkatnya AI generatif akan membuat percobaan phishing lebih meyakinkan dan memperluas opsi bagi para pelaku kejahatan untuk menargetkan korban mereka. Bagaimana pun juga, fokus utama phishing adalah sifat manusia, bukan kerentanan perangkat lunak atau eksploit sistem.

Di titik ini lah strategi bertahan dengan menyerang diperlukan. Simulasi phishing, yang digabungkan dengan perlindungan kuat pada endpoint, dapat membantu DNB menguasai permainan phishing.

### Phishing finansial dideteksi dan diblokir di Asia Tenggara pada tahun 2023

| Negara | Jumlah phishing finansial |
|---|---|
| Filipina | 163.279 |
| Malaysia | 124.105 |
| Indonesia | 97.465 |
| Vietnam | 36.130 |
| Thailand | 25.227 |
| Singapura | 9.502 |
| Total: | 455.708 |

*Sumber: Kaspersky, 2024*

### Urutkan area investasi keamanan siber berikut dari yang paling penting (atas) hingga yang paling kurang penting (bawah).

1. Teknologi anti-phishing
2. Keamanan API lanjutan
3. Keamanan aplikasi web
4. Teknologi terkait Zero Trust
5. Mitigasi distributed denial-of-service (DDoS)

# India: “I” untuk Inovasi

India telah menjadi episentrum inovasi dan DNB selama lebih dari satu dekade serta menjadi sumber utama untuk arsitektur dan eksperimentasi cloud-native.

DNB di India berfokus pada pertumbuhan dan inovasi, dengan integrasi AI paling tinggi di dalam infrastruktur cloud (98%) dan hampir semua DNB sudah berada di cloud atau dalam tahap mengeksplorasi adopsi cloud.

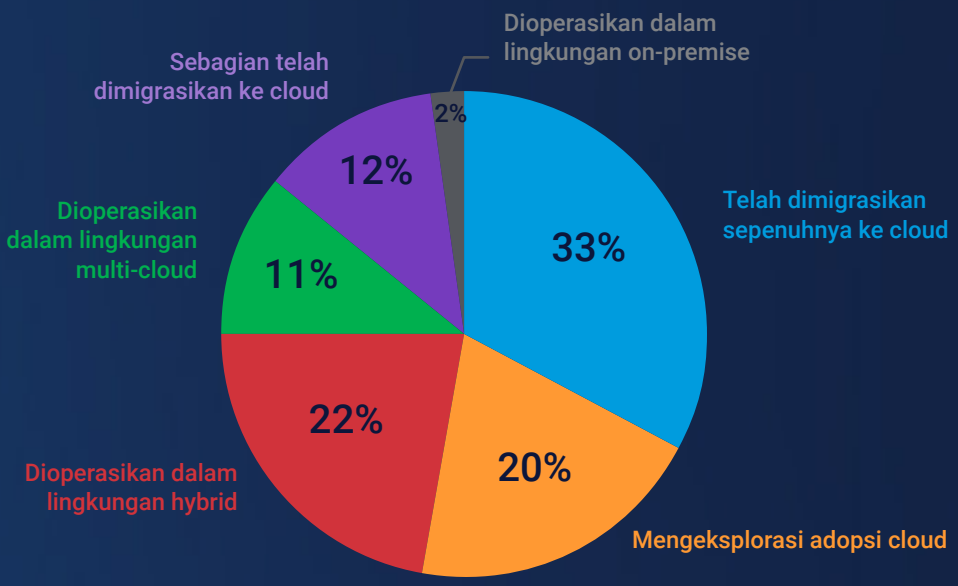
Seiring dengan kematangan DNB di India, mereka mulai mencari pertumbuhan yang berkelanjutan dengan mengalihkan fokus pada keamanan dan optimalisasi biaya serta meninjau pemilihan vendor lebih baik.

Pelanggan DNB awal di India adalah para perusahaan teknologi itu sendiri.

Didukung oleh API, DNB India mampu memberi dukungan dan pakar teknologi untuk perusahaan-perusahaan dunia tanpa secara langsung mengakses data pelanggannya. Sejak awal, DNB India telah melakukan investasi dalam tenaga ahli, API, dan sistem yang dibangun secara khusus.

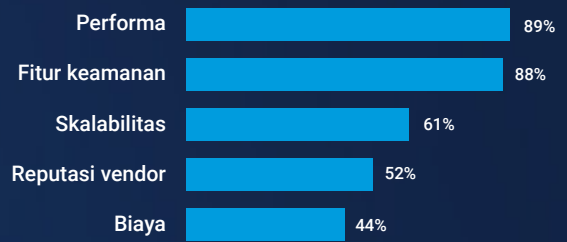
Dengan warisan dalam keunggulan teknologi yang kuat, generasi digital di India menilai performa vendor sebagai prioritas teratas dibandingkan negara sekitarnya (kedua di ASEAN dan keempat di ANZ)/

Sejauh mana perjalanan adopsi cloud perusahaan Anda saat ini?




Tingkat integrasi teknologi AI saat ini dalam infrastruktur cloud


Faktor yang memengaruhi pemilihan vendor cloud



# “I” juga untuk kepiawaian in-house

Keunggulan generasi era digital India adalah pendekatan do-it-yourself (lakukan sendiri) terkait manajemen biaya cloud dibandingkan negara setara sekitarnya.

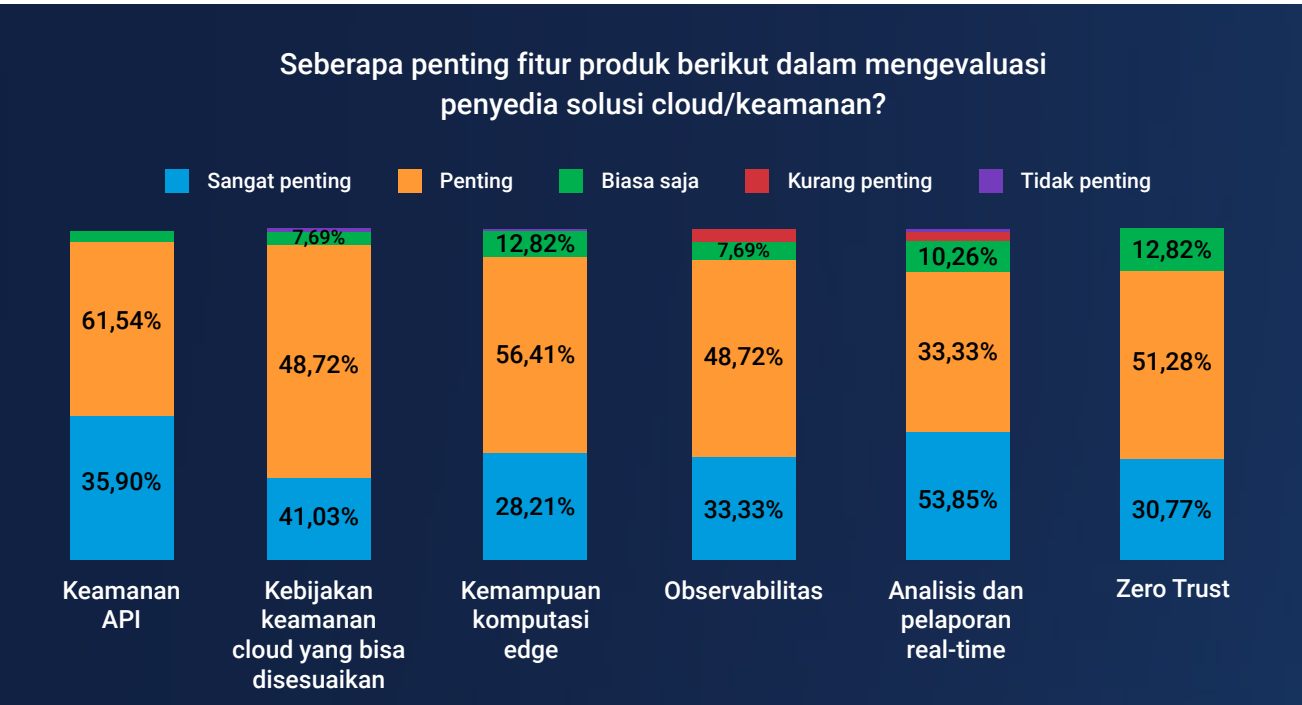
Di India, sebanyak 73% responden dilaporkan menggunakan solusi in-house untuk mengelola dan mengoptimalkan biaya cloud, berbanding terbalik dengan ASEAN (78%) dan ANZ (69%), yang lebih memilih menggunakan alat pihak ketiga.

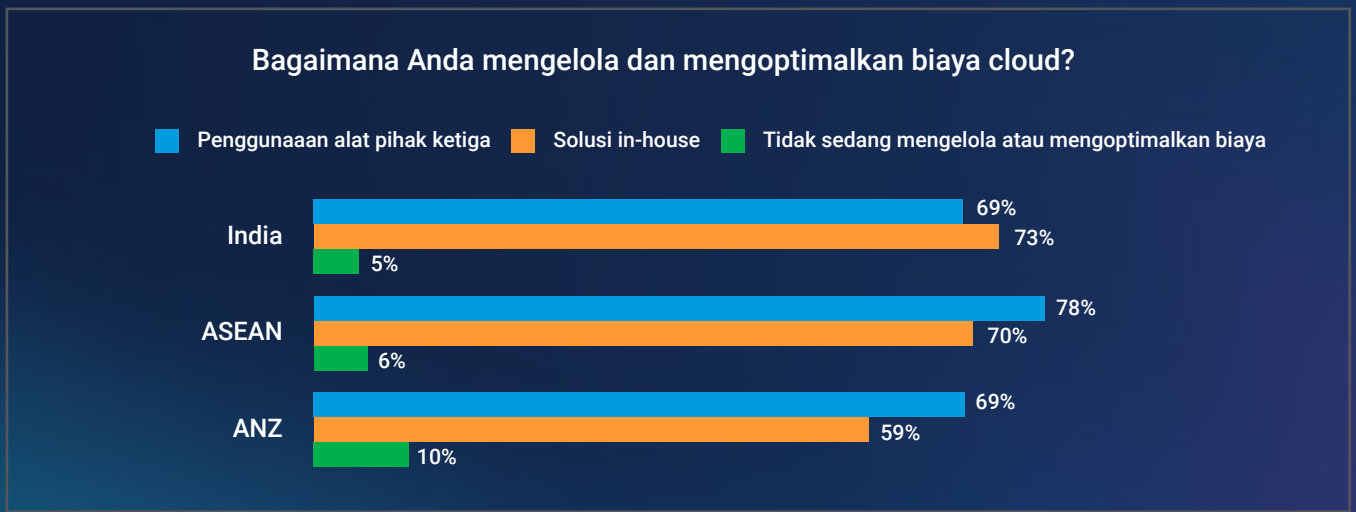
Preferensi responden ANZ untuk menggunakan alat pihak ketiga mungkin dikarenakan kurangnya keahlian TI setempat.

Misalnya, dibutuhkan 5.000 pekerja keamanan siber dalam setahun di ANZ, tetapi sistem edukasi lokal diperkirakan hanya memproduksi sekitar 2.000 pekerja dengan keahlian keamanan siber di tahun 2026.

Sebaliknya, India memiliki talenta berpengalaman yang melimpah, didukung kekuatannya sebagai hub layanan teknologi dunia secara historis.

Lebih dari 1.600 capability center global (GCC) di India saat ini menyediakan dukungan untuk perusahaan di seluruh dunia, dan jumlah ini digadang-gadang akan meningkat pada tahun 2030, dengan sekitar 2.500 GCC yang mempekerjakan 4.5 juta orang dan menghasilkan $100 miliar.




# DIY membuat DNB India menjadi rentan

Pendekatan DIY bisnis digital India dalam mengelola infrastruktur teknologinya dapat menyebabkan mereka rentan seiring dengan skala dan kematangan organisasinya.

Mengintegrasikan berbagai sistem dengan beberapa API akan memperluas potensi permukaan serangan. Masalah ini akan semakin buruk untuk perusahaan yang didirikan di cloud dan dioperasikan sepenuhnya secara online.

Tiga dari lima responden di India menyebutkan pengelolaan dampak keamanan terkait infrastruktur dan migrasi cloud sebagai masalah teratas. Bahkan tiga dari empat responden menyebutkan keamanan sebagai kesenjangan terbesar dalam infrastruktur cloud perusahaan.

DNB India perlu meninjau kedua sudut pandang untuk melihat kerentanan organisasi mereka dan skenario pontesi serangan. Lanskap ancaman siber berkembang sangat cepat, dengan metode dan alat ancaman baru yang semakin canggih.

DNB India mungkin perlu lepas dari belenggu swasembada teknologi melalui kerja sama dengan pihak ketiga yang memiliki keahlian spesialis dan memanfaatkan efisiensi yang ditawarkan teknologi berkembang.


Saat ini, sebagian besar responden survei (41%) menyebutkan infrastruktur TI yang rumit sebagai tantangan terbesar mereka dalam memperbaiki postur keamanan siber perusahaan. Sebagai perbandingan, 36% responden ANZ menyebutkan infrastruktur TI yang rumit sebagai tantangan.

Upaya untuk mengelola keamanan siber secara in-house tanpa bantuan pakarnya setiap saat bukanlah lagi menjadi opsi yang dapat dipertimbangkan, khususnya untuk pasar yang berkembang pesat seperti India yang juga menjadi salah satu target serangan siber teratas.

Ini akan menjadi teka-teki bagi infrastruktur teknologi India.

> *Platform cloud yang didistribusikan oleh Akamai menawarkan kendali atas penempatan dan penskalaan sumber daya komputasi kepada pengembang. Pengembang memiliki kuasa dan fleksibilitas untuk menentukan tempat data diperoleh, diproses, dan dikelola.*

# Bersama makin kuat

Survei menawarkan wawasan terobosan terkait tantangan yang dihadapi oleh para pemimpin teknologi di generasi era digital Asia saat mereka menerima AI, komputasi cloud, dan big data demi memberikan pengalaman yang lebih baik dan lebih cepat kepada pelanggan.

Namun, akan terdengar naif jika kita menggeneralisasi semua generasi era digital.

Riset ini memisahkan nuansa dalam kematangan cloud/API dan postur keamanan siber generasi era digital dalam berbagai geografi dan industri di seluruh Asia Pasifik.

Misalnya, orang-orang di industri atau geografi yang sangat teratur mencari keseimbangan antara keamanan dan privasi dengan pengalaman pengguna.

Bagi generasi era digital yang mementingkan waktu dalam hitungan milidetik, mereka mencari kemampuan mutakhir yang memungkinkan pengalaman personal dengan optimalisasi hyperlocal.

Pada dasarnya, arsitektur berbasis cloud memperoleh keuntungan dari API dan endpoint yang dibangun dengan baik serta memungkinkan generasi era digital untuk meningkatkan/memperluas skala dan memberikan pengalaman yang personal.

Sebagian besar perusahaan tidak memiliki kontrol visibilitas dan keamanan asli yang diperlukan untuk mengunci cloud secara efektif. Agar lingkungan umum dan multi-cloud aman, para praktisi keamanan harus dapat melihat gerak aplikasi, beban kerja, dan arus lalu lintas dalam lingkungan tersebut.

Akamai mengubah metode arsitektur cloud perusahaan, dengan menekankan desain yang lebih terdistribusi, terdesentralisasi, latensi rendah, dan dapat diukur secara global—ideal untuk beban kerja dengan performa tinggi yang perlu dioperasikan di dekat pengguna akhir.

Dorongan kami untuk membangun wilayah komputasi inti dalam pasar yang sulit diakses telah menghasilkan jejak yang disalurkan secara masif, mencakup lebih dari 4.100 PoP edge di 131 negara.

Hubungi kami dan cari tahu mengapa perusahaan maju dunia memilih Akamai untuk membangun, mengirim, dan mengamankan pengalaman digital mereka.

## Metodologi

Survei ini memaparkan wawasan melalui riset lapangan terhadap para pemimpin TI di seluruh wilayah. Survei dilakukan pada Maret–Mei 2024.

## Alasan

Laporan ini melihat lebih dalam untuk memahami cara generasi era digital melihat tren dan ancaman yang akan datang. Temuan ini berfungsi sebagai tolok ukur yang dibangun berdasarkan wawasan lapangan saat ini

## Siapa

Chief information officer, chief technology officer, IT director, dan VP dari industri berikut:

- Penerbangan
- Media/siaran/penerbitan
- Ecommerce/internet
- Game
- Perhotelan
- Teknologi informasi
- Ritel/grosir

## Lokasi

- Australia
- Selandia Baru
- India
- Singapura
- Indonesia
- Thailand
- Malaysia
- Vietnam