Microsoft Security

Indeks Keamanan Data

Tren, wawasan, dan strategi untuk menjaga keamanan data Anda dan menavigasi AI generatif

Laporan 2024

Prakata

Seiring dimulainya tahun kedua riset kami tentang lanskap keamanan data yang berkembang, tantangan dan peluang di hadapan kami tidak pernah lebih mendalam dari sebelumnya. Dalam satu tahun terakhir, tingkat keparahan insiden keamanan data telah meningkat. Di era yang berpusat pada data ini, strategi dan alat yang digunakan untuk menjaga data tetap terlindungi berkembang dengan sangat cepat.

Tahun ini, kami menjelajahi batas baru: peran dan dampak AI generatif (AI) pada strategi keamanan data.

AI menimbulkan kontroversi di seluruh dunia dengan kemampuan yang belum pernah terjadi sebelumnya untuk membuka lebih banyak inovasi dan efisiensi. Namun dengan potensi yang sangat besar ini, organisasi juga khawatir dengan risiko keamanan data dan bagaimana hal tersebut dapat membentuk tanggung jawab untuk tim keamanan data. Kami melihat AI menjadi akselerator bagi organisasi untuk memperkuat fondasi praktik keamanan data mereka sehingga mereka dapat mempersiapkan diri untuk meminimalkan dampak berbagi data yang berlebihan dan kebocoran data, dan menciptakan proses untuk adopsi AI yang aman. Di sisi lain, AI juga dapat membantu organisasi meningkatkan praktik keamanan data mereka dengan mengidentifikasi risiko tersembunyi dan celah dalam perlindungan, merekomendasikan kebijakan perlindungan, serta membantu menyelidiki dan memulihkan insiden keamanan dengan lebih cepat.

Tujuan dari riset kami adalah memberikan wawasan dan panduan yang dapat ditindaklanjuti kepada para pemimpin keamanan data untuk membantu tim mereka dengan percaya diri menerapkan strategi keamanan data mereka untuk secara efektif melindungi penggunaan AI serta mengintegrasikan AI dalam strategi keamanan data mereka. Meskipun jangkauan dan potensi AI luar biasa, AI hanya gelombang transformasi terbaru yang terjadi di seluruh perusahaan, seperti kerja hibrid, cloud, dan mobilitas, dalam beberapa tahun terakhir menggarisbawahi kebutuhan abadi akan visibilitas dalam penggunaannya untuk mengurangi risiko dan memaksimalkan dampak. Melalui informasi dalam pembelajaran ini, amankan data yang digunakan dalam AI dengan benar, serta gunakan AI untuk meningkatkan langkah-langkah keamanan data, akan memungkinkan produktivitas, ketahanan, dan ketangkasan yang lebih besar saat tim menavigasi tantangan di masa depan.

Kami mengundang Anda untuk menjelajahi temuan terbaru dan berharap wawasan tersebut akan membantu Anda memperkuat postur keamanan data Anda, serta menginspirasi Anda untuk merangkul AI dan membangun strategi keamanan data yang komprehensif, membuka lebih banyak inovasi dan memastikan masa depan yang lebih aman bagi kita semua.

Rudra Mitra
Wakil Presiden Korporat
Keamanan dan Kepatuhan Data Microsoft

Pengantar

Dengan organisasi mengalami rata-rata 156 insiden keamanan data setiap tahunnya, dampak dari insiden ini tetap menjadi perhatian konstan bagi para pembuat keputusan keamanan data. Ada alasan bagus mengapa: Satu insiden dapat menyebabkan kerusakan finansial dan reputasi yang besar, terutama dalam lanskap ancaman yang terus berkembang di mana penyerang mengeksploitasi setiap dan semua kemungkinan kerentanan. Ini hanya dibesar-besarkan oleh adopsi AI yang cepat, di mana tanpa perlindungan dan langkah-langkah keamanan yang memadai, pengguna dapat secara tidak sengaja atau berbahaya menempatkan data penting bisnis yang sensitif (termasuk informasi karyawan dan pelanggan, kekayaan intelektual, perkiraan keuangan, dan data operasional), dalam risiko. Saat organisasi mencari cara baru untuk melindungi berbagai data sensitif ini, banyak pembuat keputusan mengalihkan perhatiannya ke kemunculan AI yang dramatis.

Tantangan AI ada dua. Mengingat bahwa dua pertiga organisasi mengakui bahwa karyawan mereka menggunakan alat AI tidak sah, sangat penting bagi mereka untuk memastikan karyawan menggunakan alat AI dengan aman. Di saat yang bersamaan, ada peluang untuk menggunakan AI sebagai alat yang efektif dalam strategi keamanan data yang canggih.

Solusi keamanan data yang didukung AI telah berperan penting dalam mengidentifikasi dan merespons ancaman secara real time, meningkatkan kecepatan dan keakuratan keseluruhan program keamanan data, dan memberikan wawasan yang membantu mencegah insiden keamanan data sebelum terjadi. Organisasi harus mengelola risiko yang sebabkan AI selain memanfaatkan kekuatannya untuk mengidentifikasi pola yang bagi manusia mungkin sulit diproses dan dianalisis dengan kecepatan mesin, dan pada akhirnya melawan serangan cyber yang semakin canggih.

Pada tahun 2023, Microsoft menugaskan Hypothesis, sebuah lembaga riset independen, untuk melakukan survei multinasional di antara lebih dari 800 profesional keamanan data dan memulai inisiatif Indeks Keamanan Data untuk melayani mitra dan pelanggan kami dengan lebih baik dan membantu para pemimpin bisnis mengembangkan strategi keamanan data mereka sendiri.

Pada tahun 2024, laporan ini mengembangkan riset sebelumnya dengan wawasan baru di antara survei multinasional yang diperluas terhadap lebih dari 1.300 profesional keamanan data. Meskipun data mengungkapkan wawasan dan tren yang konsisten di seluruh pasar yang kami survei, kami mengungkap pembelajaran baru seputar keamanan data terbaru serta praktik dan tren AI di seluruh dunia.

Temuan Penting

1

Lanskap keamanan data tetap retak, meningkatkan kebutuhan akan strategi keamanan data yang kohesif dengan risiko konvensional dan baru yang terkait dengan penggunaan AI

Organisasi melaporkan tingkat kepuasan dan keyakinan yang tinggi dalam langkah-langkah keamanan data mereka. Namun, tingkat keparahan insiden keamanan data terus meningkat, terutama karena kesenjangan yang ditemukan organisasi antara kebijakan keamanan data mereka saat ini dan peningkatan penggunaan/pengenalan aplikasi AI. Menghadapi taruhan dan keharusan ini, banyak organisasi masih mengandalkan beberapa alat keamanan data yang dapat meningkatkan kerentanan dan risiko mereka secara keseluruhan.

2

Seiring pengguna akhir meningkatkan adopsi aplikasi AI, integritas data organisasi yang paling sensitif berada pada risiko yang lebih besar, sehingga membutuhkan lebih banyak visibilitas dan kontrol perlindungan baru

Seiring alat AI menjadi penting untuk pekerjaan sehari-hari, organisasi khawatir tentang risiko keamanan data. Mereka menyadari kebutuhan untuk memperkuat pertahanan mereka dan berkomitmen untuk mencegah insiden keamanan data yang disebabkan oleh AI — tetapi penggunaan alat ini secara tidak sah menyoroti perlunya visibilitas yang lebih kuat.

3

Para pengambil keputusan optimistis tentang potensi AI untuk meningkatkan upaya keamanan data mereka

Organisasi secara aktif berinvestasi dalam alat keamanan data yang menggabungkan AI untuk meningkatkan kemampuan deteksi dan respons. AI dapat membantu mendeteksi data yang tidak dilindungi, merekomendasikan kebijakan perlindungan, dan membantu menyelidiki dan memulihkan insiden keamanan data lebih cepat, yang pada akhirnya memungkinkan tim keamanan data untuk lebih memfokuskan waktu dan perhatian pada pekerjaan yang strategis. Penggunaan AI juga meningkatkan kepercayaan diri dan kepuasan dalam strategi keamanan data organisasi secara keseluruhan — terutama kemampuan mereka untuk merespons insiden dengan cepat dan akurat.

1

Lanskap keamanan data tetap retak, meningkatkan kebutuhan akan strategi keamanan data yang kohesif dengan risiko konvensional dan baru yang terkait dengan penggunaan AI

Terdapat keterputusan antara keyakinan pembuat keputusan dalam praktik keamanan data mereka dan tingkat perlindungan sebenarnya dari data mereka

Sebagaimana yang dilaporkan pada tahun 2023, sebagian besar pembuat keputusan yakin dengan strategi keamanan data mereka, dengan 74% melaporkan kepuasan dengan solusi mereka saat ini pada tahun 2024. Mereka merasa aman dalam kemampuan mereka untuk melacak dan mengelola data sensitif: 88% percaya bahwa mereka tahu di mana sebagian besar informasi penting mereka berada, dan 85% mengatakan data mereka diklasifikasikan dan diberi label dengan benar. Sebagian besar juga memercayai kontrol pertahanan mereka, dengan 79% yakin mereka dapat mencegah eksfiltrasi data, dan 76% menggambarkan pendekatan mereka sebagai proaktif daripada reaktif.

Namun, keyakinan mereka sedang diuji karena tingkat keparahan insiden terus berkembang. **Jumlah rata-rata insiden keamanan data tahunan tetap tinggi dari 166 pada tahun 2023 dan 156 pada tahun 2024, dan tingkat keparahan insiden ini telah meningkat dari 20% insiden menjadi keparahan 27% pada tahun 2024.**

156

insiden keamanan data

27%

insiden yang dianggap parah (meningkat dari 20% pada tahun 2023)

63%

peringatan ditinjau per hari

"Lokasi di mana platform perangkat lunak didirikan, di mana datanya disimpan, dan siapa yang akan mengakses data tersebut memperumit keamanan data dan manajemen alat dan vendor AI kami. Kami memiliki data senilai lebih dari 100 tahun yang harus kami lindungi dan atur sesuai dengan persyaratan hukum di setiap yurisdiksi tempat kami beroperasi", kata Manajer Senior untuk Tata Kelola Informasi di sebuah produsen alat berat.

Kenaikan tingkat keparahan insiden keamanan data menyebabkan peningkatan volume peringatan. **Organisasi menghadapi rata-rata 66 peringatan per hari, naik dari 52 pada tahun 2023.** Jumlah tersebut bervariasi secara signifikan menurut ukuran organisasi, dengan perusahaan menengah (500-999 karyawan) dan perusahaan besar (1.000-4.999 karyawan) menerima rata-rata 56 peringatan dan perusahaan ekstra besar (5.000+ karyawan) menerima rata-rata 80 peringatan per hari.

Mengingat banyaknya peringatan keamanan data, seharusnya tidak mengherankan bahwa sebagian besar organisasi tidak dapat mengikutinya. Rata-rata, tim keamanan data meninjau 63% dari peringatan harian mereka. Tiga puluh lima persen dari peringatan ini ternyata positif palsu. Ketidaksesuaian antara kontrol yang dirasakan dan kenyataan operasional ini membuat tim keamanan data kewalahan — mencoba menilai apakah mereka memiliki perlindungan yang tepat atau bagaimana menyempurnakannya, sambil khawatir bahwa insiden yang berpotensi serius dapat lolos dari celah.

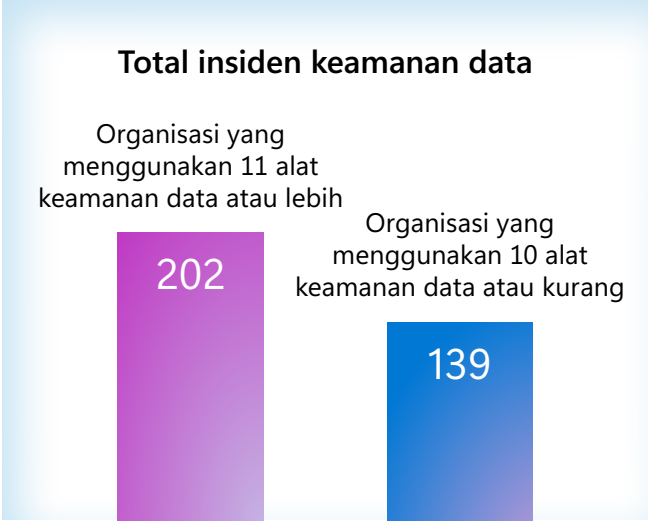
Untuk memerangi risiko data konvensional dan yang muncul terkait dengan penggunaan alat AI, terdapat peningkatan kebutuhan akan strategi keamanan data yang lebih kuat dan kohesif

Terlepas dari semakin banyaknya alat yang mereka miliki, banyak pembuat keputusan terus mengakui bahwa lebih banyak tidak selalu lebih baik. Faktanya, 21% menyebutkan kurangnya visibilitas yang terkonsolidasi dan komprehensif (dan pemahaman bersama tentang risiko) yang disebabkan oleh alat yang berbeda sebagai tantangan/risiko terbesar mereka.[1]

Sebagian besar pembuat keputusan (82%) setuju bahwa platform yang komprehensif dan terintegrasi penuh lebih unggul daripada mengelola beberapa alat yang terisolasi. **Rata-rata, mereka menangani 12 solusi keamanan data yang berbeda, menciptakan kompleksitas yang meningkatkan kerentanan mereka.** Hal ini terutama berlaku untuk organisasi terbesar: Rata-rata, perusahaan menengah menggunakan 9 alat, perusahaan besar menggunakan 11, dan perusahaan ekstra besar menggunakan 14.

Data menunjukkan hubungan kuat antara jumlah alat keamanan data yang digunakan dan frekuensi insiden keamanan data. Perusahaan menengah dan besar melaporkan rata-rata 89 insiden per tahun, sementara perusahaan ekstra besar secara mengejutkan menghadapi 248 insiden setiap tahunnya. Perbedaan mencolok ini menyoroti risiko tinggi yang dihadapi organisasi besar, bahkan ketika mereka menyatakan keyakinan yang cukup besar dalam langkah-langkah keamanan data mereka.

Pada tahun 2024, organisasi yang menggunakan lebih banyak alat keamanan data (11 atau lebih) mengalami rata-rata 202 insiden keamanan data, dibandingkan dengan 139 insiden bagi mereka yang memiliki 10 alat atau kurang.



Solusi terfragmentasi menyulitkan untuk memahami postur keamanan data karena data terisolasi dan alur kerja yang berbeda dapat membatasi visibilitas yang komprehensif terhadap potensi risiko. Ketika alat tidak terintegrasi, tim keamanan data harus membangun proses untuk menghubungkan data dan membangun pandangan risiko yang kohesif, yang dapat menyebabkan titik buta dan membuatnya menantang untuk mendeteksi dan mengurangi risiko secara efektif.

Area yang semakin menjadi perhatian adalah peningkatan insiden keamanan data dari penggunaan aplikasi AI, yang hampir dua kali lipat dari 27% pada tahun 2023 menjadi 40% pada tahun 2024. Peningkatan insiden ini didorong oleh lonjakan serangan malware dan ransomware, hingga 59% dari 50% pada tahun 2023. Serangan dari penggunaan aplikasi AI tidak hanya mengekspos data sensitif tetapi juga membahayakan fungsionalitas sistem AI itu sendiri, yang semakin memperumit lanskap keamanan data yang sudah retak. Singkatnya, ada kebutuhan yang semakin mendesak untuk strategi keamanan data yang lebih kuat dan kohesif yang dapat mengatasi risiko konvensional dan yang muncul terkait dengan penggunaan alat AI.

1. Survei September 2024 di antara pengambil keputusan keamanan, tata kelola, kepatuhan, dan privasi data yang ditugaskan oleh Microsoft dari lembaga MDC Research

Jalan untuk Maju

Kenaikan tingkat keparahan insiden keamanan data membuka peluang bagi AI untuk membantu. Organisasi yang terdepan menerapkan keamanan data yang didukung AI untuk membantu memprioritaskan insiden, mengotomatiskan klasifikasi data, dan mengidentifikasi cara untuk menyempurnakan kebijakan perlindungan saat ini. AI dapat secara otomatis mensintesis potensi keparahan peringatan insiden, memberikan tim keamanan data wawasan yang dapat ditindaklanjuti untuk respons cepat guna mengurangi waktu yang dihabiskan untuk positif palsu. Ini menyederhanakan alur kerja dan memungkinkan tim keamanan data untuk fokus pada peningkatan keamanan data yang lebih strategis dan langkah-langkah proaktif.

2

Seiring pengguna akhir meningkatkan adopsi aplikasi AI, integritas data organisasi yang paling sensitif berada pada risiko yang lebih besar, sehingga membutuhkan lebih banyak visibilitas dan kontrol perlindungan baru

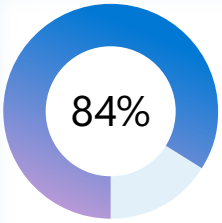
AI dengan cepat menjadi penting untuk pekerjaan sehari-hari — dan organisasi harus merangkul dan secara aktif beradaptasi dengan kenyataan baru tersebut

Adopsi alat AI yang cepat oleh karyawan telah mendorong perubahan besar dalam pendekatan organisasi terhadap keamanan data. Meskipun AI mengubah produktivitas dan alur kerja, seperti teknologi baru lainnya, AI juga dapat memperkuat risiko yang ada atau menimbulkan risiko baru yang memerlukan pendekatan berbeda untuk melindungi informasi sensitif. Hasilnya, perusahaan masih menemukan pijakan dalam lanskap yang berubah dengan cepat. Seorang Direktur Teknik dan Analisis dalam transportasi mengklaim, "kami memantau data dengan lebih hati-hati di sisi AI. Ada ketegangan antara produktivitas dan keamanan, ketepatan dan privasi."

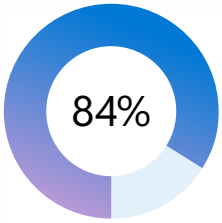
Keyakinan dalam mengamankan penggunaan AI oleh karyawan tetap beragam. Mayoritas (84%) ingin merasa lebih percaya diri dalam mengelola dan menemukan input data. Sementara 22% organisasi merasa sangat yakin dengan kemampuan mereka untuk menjaga keamanan data, sebagian besar (59%) hanya "sangat percaya diri," menunjukkan ada ruang untuk perbaikan.

Sebagian besar perusahaan (86%) mengakui bahwa mereka ingin merasa lebih optimis dalam mengelola dan menemukan data yang dihasilkan oleh alat AI.

Karena AI menjadi lebih penting untuk produktivitas sehari-hari, penggunaan aplikasi AI juga meningkatkan kekhawatiran seputar insiden keamanan data. **Hampir sepertiga (31%) organisasi mengantisipasi peningkatan insiden keamanan data akibat penggunaan AI oleh karyawan, dan 84% mengakui bahwa mereka perlu berbuat lebih banyak untuk melindungi dari risiko ini.** Kecemasan tersebut sangat tinggi di antara organisasi terbesar: sementara 26% perusahaan menengah berharap untuk melihat peningkatan insiden keamanan data terkait AI dan 29% perusahaan besar memproyeksikan peningkatan, kelompok yang jauh lebih tinggi mewakili 36% perusahaan ekstra besar memperkirakan peningkatan.



ingin merasa lebih percaya diri dalam mengelola dan menemukan input data tentang aplikasi dan alat AI



setuju bahwa mereka perlu berbuat lebih banyak untuk melindungi diri dari penggunaan aplikasi dan alat AI oleh karyawan yang berisiko

Penggunaan AI yang tidak sah tersebar luas

Empat puluh persen melaporkan bahwa aplikasi AI mereka telah dibobol atau disusupi dalam insiden keamanan data. Sekali lagi, angka ini lebih tinggi di antara organisasi yang lebih besar: perusahaan menengah melaporkan tingkat insiden 36%, perusahaan besar melaporkan 38%, dan perusahaan ekstra besar mengalami kejadian paling banyak, yaitu 44%.

Penggunaan AI yang tidak sah sering terjadi dengan karyawan yang masuk dengan kredensial pribadi atau menggunakan perangkat pribadi untuk tugas yang berhubungan dengan pekerjaan. **Rata-rata, 65% organisasi mengakui bahwa karyawan mereka menggunakan alat AI yang tidak sah.** Cara karyawan menggunakan alat AI yang tidak sah meliputi:

- 53% masuk dengan kredensial pribadi untuk tujuan kerja
- 48% menggunakan perangkat pribadi saat menggunakan AI untuk bekerja
- 47% menggunakan kredensial kerja mereka untuk menggunakan AI demi tujuan pribadi

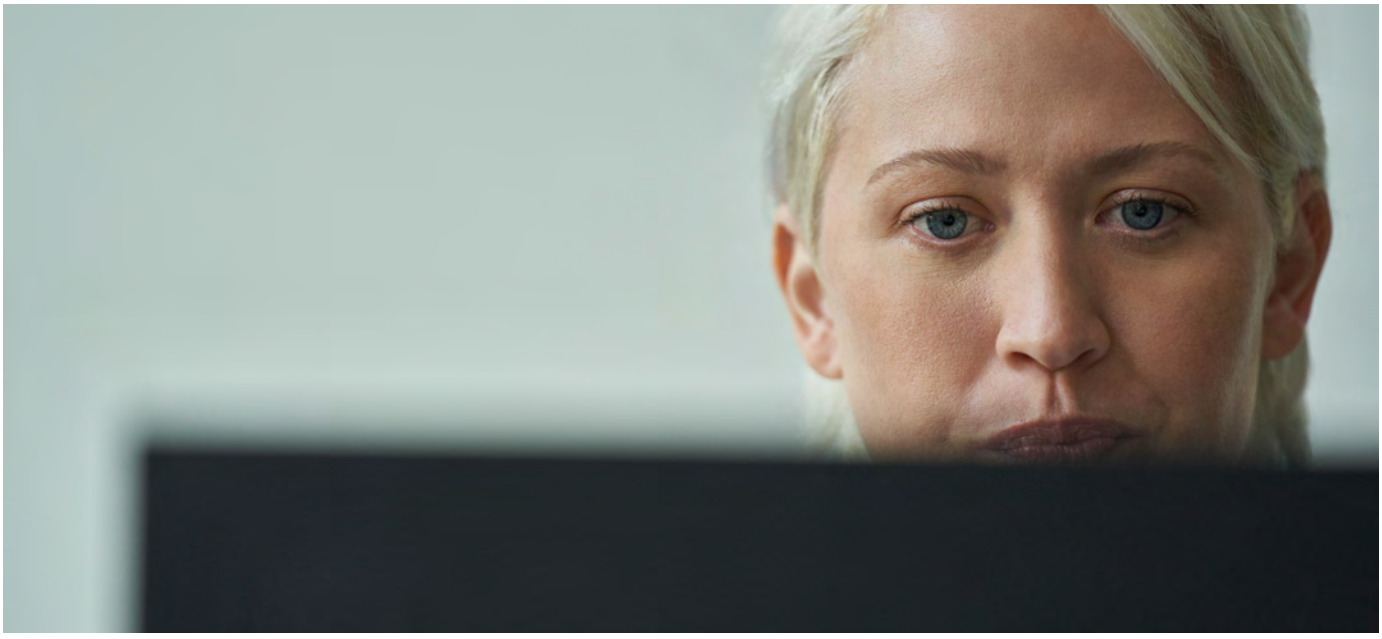
Setengah dari semua organisasi mengatakan mereka khawatir tentang kurangnya kontrol untuk mendeteksi dan mengurangi risiko ketika karyawan menggunakan aplikasi AI dengan cara yang tidak aman. Angka ini bervariasi menurut ukuran perusahaan, dengan 43% perusahaan menengah, 50% perusahaan besar, dan 54% perusahaan ekstra besar menyatakan keprihatinan tentang kemampuan mereka untuk mengelola risiko ini.

Mengingat meningkatnya penggunaan AI, diperlukan lebih banyak kontrol keamanan data

Seiring semakin melekatnya AI dalam operasi sehari-hari, organisasi menyadari perlunya perlindungan yang lebih kuat. **Sementara 96% perusahaan memiliki kekhawatiran tentang penggunaan alat ini oleh karyawan, hampir sama banyak yang bersedia berinvestasi dalam solusi untuk mengatasi masalah mereka.**

"Fokus besarnya adalah bagaimana Anda melampaui AI? Fokus keamanan adalah tentang mengurangi ukuran data, memantau data dengan lebih hati-hati. Di sisi AI, agar membuat model Anda lebih representatif untuk mengidentifikasi bias, Anda memerlukan lebih banyak data. Jadi bagaimana Anda berdamai?" kata seorang Direktur Teknik, Arsitektur, dan Analisis dalam transportasi. Sebagian besar pembuat keputusan (87%) siap meluangkan waktu dan uang untuk melatih karyawan dalam praktik aman menggunakan alat AI. **Itu karena 85% mengatakan sangat penting bagi karyawan untuk menggunakan alat ini agar tetap kompetitif.**

Hampir semua organisasi (93%) berada pada tahap tertentu dalam mengembangkan atau menerapkan kontrol seputar penggunaan AI, tetapi banyak yang masih dalam tahap awal. Hanya 39% yang telah sepenuhnya menerapkan kontrol keamanan data untuk AI, sementara 24% telah membuat kebijakan tetapi belum menerapkannya. Seorang VP Keamanan Data di bidang perhotelan mengklaim, "kita harus menyelaraskan kontrol untuk AI tetapi merangkul penggunaan AI untuk sementara waktu. Hal tersebut membuat hidup lebih baik dan membantu kita menjadi lebih efisien."



Sementara organisasi mengambil langkah-langkah untuk melindungi data sensitif agar tidak disalahgunakan dalam aplikasi AI, ada kebutuhan yang jelas untuk kontrol yang lebih komprehensif. Saat ini, 43% perusahaan fokus untuk mencegah data sensitif diunggah ke aplikasi AI, sementara 42% lainnya mencatat semua aktivitas dan konten dalam aplikasi ini untuk kemungkinan penyelidikan atau respons insiden. Demikian pula, 42% memblokir akses pengguna ke alat yang tidak sah, dan persentase yang sama berinvestasi dalam pelatihan karyawan tentang penggunaan AI yang aman.

Perusahaan dengan karyawan yang terlibat dalam penggunaan AI yang tidak sah memiliki kebutuhan yang lebih tinggi untuk jenis kontrol tertentu. **Di antara mereka yang menggunakan AI secara tidak sah, 42% memerlukan kontrol untuk mengidentifikasi pengguna berisiko berdasarkan kueri AI, dibandingkan dengan 30% untuk mereka yang tidak menggunakan secara tidak sah. Selain itu, 40% organisasi yang berurusan dengan penggunaan AI yang tidak sah memerlukan kontrol untuk mengelola siklus hidup data (seperti protokol retensi dan penghapusan), dibandingkan dengan 27% perusahaan tanpa masalah ini.**

5 kontrol AI teratas yang diperlukan

Mencegah data sensitif agar tidak diunggah ke AI	43%
Mencatat semua aktivitas dan konten di alat AI untuk kemungkinan penyelidikan atau respons insiden	42%
Memblokir akses pengguna ke alat AI yang tidak sah	42%
Melatih karyawan tentang penggunaan alat AI yang aman	42%
Mengidentifikasi pengguna berisiko berdasarkan kueri mengenai AI	41%

Jalan untuk Maju

Untuk mempertahankan postur keamanan data yang kuat, tim memerlukan serangkaian kontrol lengkap untuk menemukan, melindungi, dan mengelola data mereka di aplikasi AI. Berikut ini tiga strategi utama yang dapat digunakan tim:

Meningkatkan visibilitas penggunaan aplikasi AI dan aliran data melalui aplikasi: Memanfaatkan alat keamanan data yang dapat mendeteksi dan menggunakan aplikasi AI. Alat ini memberikan wawasan tentang daftar lengkap aplikasi AI yang digunakan beserta profil risikonya, termasuk detail seperti kontrol keamanan data yang didukung dan kepatuhan terhadap peraturan. Gunakan alat yang dapat memberikan klasifikasi yang konsisten untuk data sensitif dalam interaksi AI, dan tunjukkan tren seputar bagaimana data mengalir melalui aplikasi AI.

Membuat dan menerapkan kebijakan: Buat kebijakan berdasarkan wawasan yang diperoleh dari analisis. Kebijakan ini dapat mencakup panduan untuk aplikasi AI yang disetujui dan prosedur untuk memblokir atau membatasi penggunaan aplikasi yang tidak berizin oleh karyawan. Bahkan dalam aplikasi AI yang berizin, Anda dapat membuat kebijakan terperinci untuk memungkinkan data non-sensitif mengalir sekaligus membatasi penggunaan data bisnis yang penting dan data sensitif. Ini dapat mencakup pemblokiran tindakan tertentu, seperti menempelkan data sensitif ke alat AI berbasis browser untuk memastikan keamanan data.

Menilai risiko secara rutin dan menyempurnakan kebijakan: Buat laporan rutin yang menunjukkan tingkat risiko aplikasi AI yang digunakan, tren tentang bagaimana data sensitif mengalir melalui aplikasi ini, serta aktivitas pengguna seputar aplikasi ini. Hal ini membantu dalam menilai lanskap risiko secara keseluruhan dan membuat keputusan berdasarkan informasi tentang kebijakan keamanan data yang paling relevan.

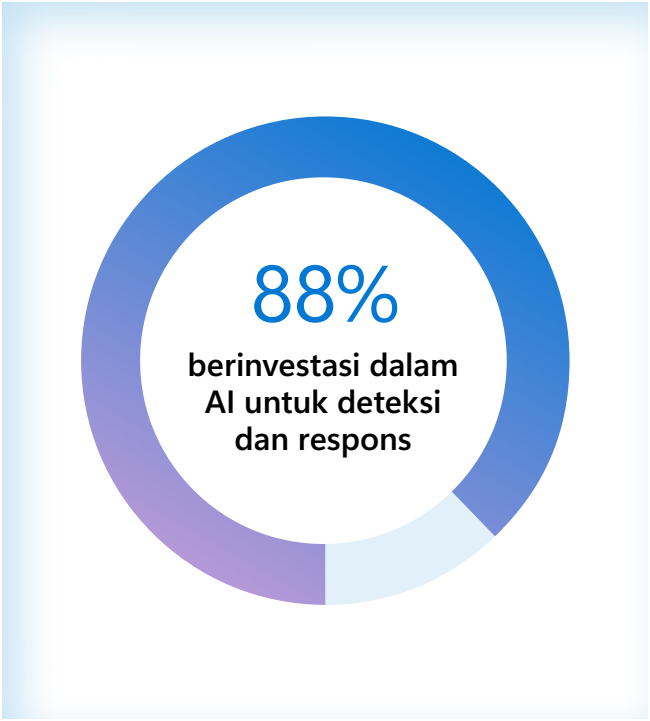
3

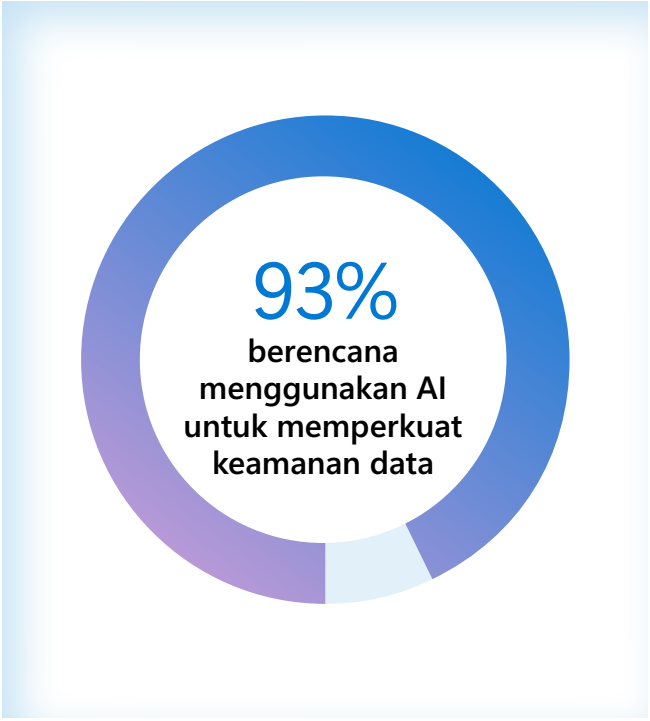
Para pengambil keputusan optimistis tentang potensi AI untuk meningkatkan upaya keamanan data mereka

Penyelidikan keamanan data sangat bergantung pada AI

Sebagian besar (88%) organisasi sudah berinvestasi dalam AI untuk meningkatkan upaya deteksi dan respons mereka — menemukan data sensitif, mendeteksi aktivitas anomali, dan secara otomatis melindungi data yang berisiko. **Tujuh puluh tujuh persen organisasi percaya bahwa AI akan mempercepat proses ini, dan 76% berpikir AI akan meningkatkan keakuratan strategi deteksi dan respons mereka.**

Sementara 73% pembuat keputusan menyatakan keprihatinan tentang penggunaan AI untuk memperkuat keamanan data, 50% mengatakan hal tersebut tidak menghambat penggunaan AI oleh mereka untuk memperkuat keamanan data dan hanya 23% mengatakan bahwa hal tersebut telah menahan mereka. Secara keseluruhan, 93% setidaknya berencana menggunakan AI untuk memperkuat keamanan data meskipun terdapat kekhawatiran.



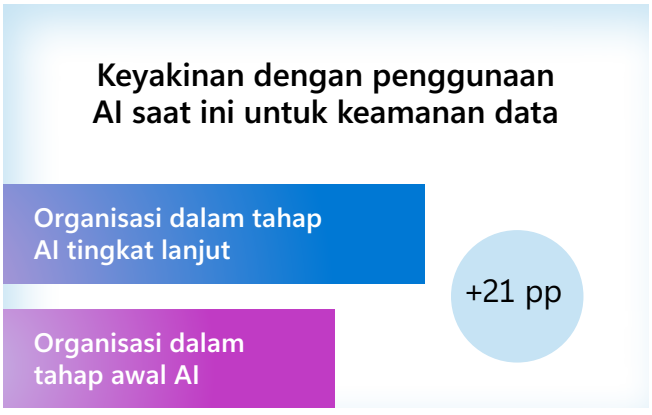


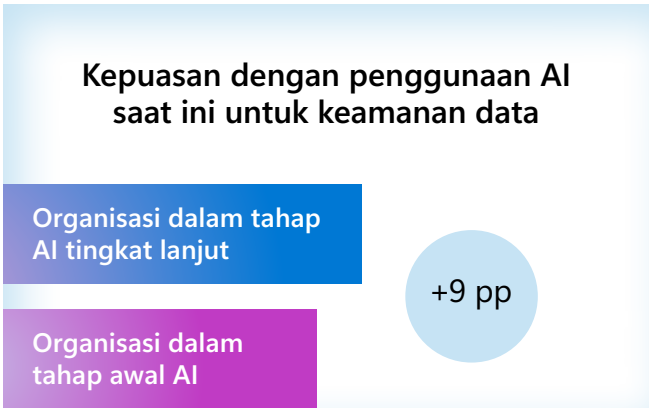
Menggunakan AI untuk memperkuat keamanan data meningkatkan visibilitas, keyakinan, dan kepuasan

Salah satu manfaat utama menggunakan AI untuk memperkuat keamanan data adalah kemampuannya untuk meningkatkan visibilitas di seluruh sistem, mengurangi kekhawatiran utama yang dimiliki pembuat keputusan untuk mengetahui di mana data disimpan dan bagaimana data diklasifikasikan (20%).[1] 88% pembuat keputusan keamanan data percaya bahwa mengintegrasikan AI ke dalam solusi keamanan data akan memungkinkan tim memiliki visibilitas yang lebih besar, yang akan memungkinkan organisasi memproses dan menganalisis data jauh lebih banyak daripada yang mungkin dilakukan. Organisasi menengah mengutamakan fokus pada pengurangan risiko jangka pendek, seperti meminimalkan kesalahan manusia dalam proses keamanan data mereka. Faktanya, 43% perusahaan menengah memprioritaskan pengurangan risiko yang disebabkan oleh kesalahan manusia, dibandingkan dengan perusahaan ekstra besar yang hanya 37%.

Sebaliknya, perusahaan besar lebih maju dalam pendekatan mereka, menekankan risiko jangka panjang dan kebutuhan akan kemampuan beradaptasi. Tingkat kecanggihan tersebut memungkinkan tim keamanan data untuk beradaptasi lebih baik dengan risiko yang berkembang — prioritas utama bagi 49% perusahaan ekstra besar, dibandingkan dengan organisasi menengah sebesar 43%.

Secara keseluruhan, organisasi yang lebih jauh dalam penggunaan AI untuk memperkuat keamanan data melaporkan tingkat kepercayaan dan kepuasan yang jauh lebih tinggi dengan strategi keamanan data mereka. **Di antara mereka yang berada dalam tahap lanjutan implementasi AI, 90% merasa yakin sekali atau sangat yakin dalam penggunaan AI untuk memperkuat keamanan data, dibandingkan dengan 69% pada tahap sebelumnya. Demikian pula, 76% organisasi dengan penggunaan AI tingkat lanjut menyatakan kepuasan dengan solusi keamanan data mereka, sementara hanya 67% dari mereka yang berada di tahap awal melaporkan hal yang sama.**





1. Survei September 2024 di antara pengambil keputusan keamanan, tata kelola, kepatuhan, dan privasi data yang ditugaskan oleh Microsoft dari lembaga MDC Research

Organisasi mengurangi jumlah insiden keamanan data dan meningkatkan manajemen peringatan dengan AI

Organisasi yang menggunakan AI untuk memperkuat operasi keamanan data mereka melaporkan peringatan yang jauh lebih sedikit. **Rata-rata, mereka yang telah menerapkan alat keamanan data berbasis AI menerima 47 peringatan per hari, dibandingkan dengan 79 peringatan bagi mereka yang belum menerapkan. Dan, mereka yang menggunakan AI dapat meninjau 66% dari peringatan harian mereka, sementara organisasi yang tidak menggunakan AI hanya berhasil meninjau 60%.**

Selain itu, mereka yang menggunakan AI untuk memperkuat keamanan data lebih cenderung juga menggunakan AI untuk mengurangi risiko (56% vs. 26%). Pengurangan volume peringatan, bersama dengan peningkatan kemampuan untuk menguranginya dengan memanfaatkan AI, tampaknya memiliki dampak dramatis pada jumlah keseluruhan insiden keamanan data. Organisasi yang telah menerapkan AI untuk memperkuat keamanan data mengalami penurunan insiden keamanan data sebesar 65% dibandingkan dengan organisasi yang tidak menggunakan AI untuk memperkuat keamanan data.

AI diharapkan memiliki dampak terbesar pada respons

Dalam hal deteksi, 33% pembuat keputusan mengharapkan AI untuk membantu mendeteksi aktivitas anomali, sementara 23% percaya AI akan membantu dalam menyelidiki potensi insiden keamanan data. 22% lainnya melihat potensi AI untuk membuat rekomendasi untuk mengamankan lingkungan data mereka dengan lebih baik.

Namun, respons menjadi bagian di mana para pembuat keputusan mengharapkan AI untuk membuat dampak yang paling mendalam. Tiga puluh empat persen percaya AI dapat secara otomatis memblokir pembagian data sensitif yang tidak pantas, dan 32% mengatakan AI akan melindungi data yang berisiko. 26% lainnya melihat AI membantu mengurangi risiko keamanan data dan menerapkan kontrol yang tepat, sementara jumlah yang sama mengharapkan AI untuk secara otomatis menandai perilaku pengguna yang berisiko.

Jalan untuk Maju

Mengintegrasikan AI ke dalam solusi keamanan data dapat membantu dengan menawarkan panduan real-time kepada tim, kemampuan ringkasan, dan dukungan bahasa natural untuk menyoroti area yang mungkin terlewatkan. Hal ini juga dapat mempercepat penyelidikan dan meningkatkan keahlian di seluruh tim keamanan data. Berikut cara kemampuan ini dapat membuat dampak:

Ringkasan pemberitahuan: Penyelidikan dapat menjadi hal yang menakutkan karena banyaknya sumber untuk dianalisis dan aturan kebijakan yang beragam. Dengan menanamkan AI dalam pencegahan kehilangan data (DLP) dan manajemen risiko orang dalam (IRM), tim dapat dengan cepat menerima ringkasan peringatan, termasuk sumber, aturan kebijakan, dan wawasan risiko pengguna untuk memahami data sensitif apa yang disusupi dan risiko pengguna terkait.

Komunikasi kontekstual: Organisasi harus mematuhi persyaratan peraturan seputar komunikasi bisnis, yang sering kali memerlukan peninjauan pelanggaran secara ekstensif. AI dapat membantu tim keamanan data menilai konten yang melanggar peraturan dan kebijakan perusahaan untuk menyoroti komunikasi berisiko tinggi yang dapat mengakibatkan insiden keamanan data.

Bahasa natural untuk kueri kata kunci: Pencarian dapat menjadi alur kerja yang kompleks dan memakan waktu selama penyelidikan, biasanya membutuhkan penggunaan bahasa kueri kata kunci. AI memungkinkan tim keamanan data untuk memasukkan permintaan pencarian dalam bahasa natural untuk menyederhanakan awal pencarian dan memungkinkan penyelidikan yang lebih canggih.

Rekomendasi Akhir

1 Melindungi nilai terhadap insiden keamanan data dengan mengadopsi platform terintegrasi

Mengadopsi platform keamanan data yang terintegrasi penuh menawarkan strategi yang lebih aman dan efisien dalam lanskap yang semakin berkembang, mengurangi kompleksitas, dan meningkatkan visibilitas sekaligus meningkatkan perlindungan. Pendekatan terpadu dapat membantu organisasi meningkatkan manajemen postur keamanan data dengan memusatkan kontrol keamanan data dan memberikan visibilitas terpadu di seluruh data, pengguna, dan aktivitas, sehingga memperkuat dan menyederhanakan deteksi dan perlindungan seputar risiko data. Dengan 82% organisasi setuju bahwa platform terintegrasi lebih unggul, langkah menuju konsolidasi tidak hanya bermanfaat — tetapi juga penting.

2 Meningkatkan visibilitas mengenai penggunaan AI secara internal untuk menilai kontrol yang diperlukan untuk penggunaan AI oleh karyawan yang tidak akan memengaruhi produktivitas

Seiring AI menjadi lebih umum di tempat kerja, AI dapat memperkuat risiko yang ada dan menimbulkan risiko baru. Organisasi mengakui bahwa mereka perlu berbuat lebih banyak untuk melindungi dari penggunaan AI yang tidak aman. Memanfaatkan kontrol dan visibilitas bawaan ke dalam aplikasi AI sangat penting untuk menjaga keamanan data tanpa mengganggu produktivitas. Melatih karyawan tentang penggunaan AI yang aman dapat membantu organisasi meminimalkan perilaku berisiko sekaligus memastikan bahwa tim terus mendapatkan manfaat dari alat-alat canggih ini.

3 Meningkatkan strategi keamanan data Anda dengan bantuan AI

AI memungkinkan tim keamanan data untuk fokus pada inisiatif yang lebih strategis daripada bereaksi terhadap ancaman konstan dan volume peringatan yang tinggi. Perusahaan dalam tahap lanjut implementasi AI lebih yakin dan lebih puas dengan solusi keamanan data mereka daripada mereka yang baru memulai. Dengan menggunakan AI sebagai bagian dari strategi keamanan data yang komprehensif, organisasi dapat meningkatkan visibilitas mereka, yang memperkuat kemampuan mereka untuk mendeteksi dan merespons risiko, yang pada akhirnya memperkuat postur keamanan data mereka secara keseluruhan.

Tujuan Penelitian

Tujuan dari penelitian ini mencakup:

1. Memahami landskap keamanan data, termasuk prioritas dan pola pikir, tantangan, dan penyebabnya serta efek insiden keamanan data.
2. Menjelajahi masa depan keamanan data, termasuk strategi dan inovasi apa yang muncul dan bagaimana organisasi berniat untuk berinvestasi di masa depan.
3. Mengungkap peran AI dalam meningkatkan keamanan data dan peran AI dalam melindungi data.

Metodologi

Survei online multinasional selama 20 menit dilakukan pada tanggal 5–23 Agustus 2024, di antara 1.376 pengambil keputusan keamanan data.

Pertanyaan berpusat seputar lanskap keamanan data dan insiden keamanan data dibandingkan dengan tahun 2023. Selain itu, survei tahun ini mencakup pertanyaan seputar mengamankan penggunaan AI oleh karyawan dan penggunaan AI untuk memperkuat keamanan data.

Perekrutan Audiens

Untuk memenuhi kriteria penyaringan, pengambil keputusan keamanan data harus:

- CISO dan pembuat keputusan yang berdekatan (C-2 dan di atasnya) dengan purview di atas keamanan data
- Bekerja di organisasi perusahaan (500+ karyawan; berbagai ukuran)
- Perpaduan antara industri yang diatur tidak diatur (bukan pendidikan, pemerintah, atau nirlaba)

Dari 1.376 pengambil keputusan keamanan data yang disurvei untuk riset ini, yang melengkapi berdasarkan negara adalah sebagai berikut:

- AS: 302
- Inggris Raya: 305
- India: 301
- Brasil: 158
- Prancis: 156
- Australia: 154

hypothesis Microsoft Security