Microsoft

hypothesis

Indeks Keamanan Data

Tren, wawasan, dan strategi
untuk mengamankan data

Prakata

Di masa yang ditandai dengan lonjakan data, semakin jelas bahwa data organisasi tidak lain adalah sumber kehidupan organisasi. Berlimpahnya data yang dibuat dan digunakan oleh organisasi mendukung operasi penting, memberikan informasi untuk pengambilan keputusan strategis dan global, dan membentuk kemungkinan untuk masa depan organisasi. Data bukan sekadar sumber daya – data adalah jantung perusahaan modern.

Namun, dengan meningkatnya ketergantungan pada data, muncul kenyataan pahit bahwa kerentanan dalam bayang-bayang digital itu nyata dan menyebar dengan cepat. Ancaman siber, pembobolan data, dan insiden risiko orang dalam bukan lagi hal yang jarang terjadi; ancaman ini menyebar dan meningkat, sehingga menimbulkan risiko bagi organisasi yang bergantung pada data. 89% pengambil keputusan yang kami survei baru-baru ini mengatakan bahwa mereka memandang postur keamanan data mereka sangat penting bagi kesuksesan secara keseluruhan.

Dalam laporan resmi ini, kami memulai eksplorasi tentang keharusan mendasar: perlindungan data organisasi Anda. Saya dan tim sangat antusias untuk berbagi temuan kami dengan Anda – dan kami berharap untuk dapat memulai dialog tentang cara untuk terus mendorong keamanan data secara kolektif menuju keunggulan. Pembelajaran kami mencontohkan bagaimana keamanan data saat berada di titik kritis – meskipun para pengambil keputusan keamanan setuju bahwa hal ini sangat penting bagi keamanan data mereka, dan sebagian besar mengatakan bahwa mereka yakin dengan apa yang mereka lakukan, namun pada saat yang sama mereka mengalami banyak sekali insiden dan tantangan keamanan data. Dan, 80% pemimpin yang kami ajak bicara mengakui bahwa pendekatan terpadu dan terbaik lebih unggul daripada solusi titik, tetapi sebagian besar perusahaan masih menggunakan sistem multi-alat yang terfragmentasi untuk melindungi data – yang sering mengakibatkan lebih banyak insiden keamanan, bukannya lebih sedikit.

Kami mengajak Anda untuk membaca dan membagikan laporan terbaru ini dan menjadikannya sebagai awal percakapan baru dengan tim kami mengenai cara terbaik untuk mengamankan masa depan bersama.

Rudra Mitra
Wakil Presiden Korporat
Keamanan dan Kepatuhan Data Microsoft

Pengantar

Mencegah pembobolan data dan insiden keamanan lainnya terus menjadi perhatian utama bagi para pengambil keputusan keamanan dan risiko – serta menjadi landasan bagi setiap program keamanan siber – karena satu pembobolan saja dapat menyebabkan kerusakan reputasi dan keuangan yang signifikan. Organisasi ditugaskan untuk melindungi berbagai macam data sensitif – termasuk informasi karyawan dan pelanggan, kekayaan intelektual, perkiraan keuangan, dan data operasional.

Untuk memahami praktik dan tren keamanan data saat ini serta mengidentifikasi peluang bagi organisasi untuk meningkatkan keamanan data, Microsoft menugaskan lembaga penelitian independen, Hypothesis Group, untuk melakukan survei multinasional terhadap lebih dari 800 profesional keamanan data. Laporan ini menyajikan lima temuan utama dari penelitian ini, termasuk tren, wawasan, dan strategi untuk mengamankan data.

Temuan Penting

1

Para pengambil keputusan berpikir data mereka terlindungi, namun kenyataannya tidak sesuai dengan persepsi.

Meskipun sebagian besar pengambil keputusan mengatakan bahwa mereka puas dan percaya diri dengan solusi keamanan data mereka, namun mereka masih mengalami rata-rata 59 insiden keamanan data per tahun, dengan dampak yang merugikan.

2

Memiliki lebih banyak alat bukan berarti keamanan atau efisiensi data menjadi lebih baik – justru sebaliknya.

80% pengambil keputusan setuju bahwa solusi yang komprehensif dan terintegrasi lebih unggul daripada solusi terbaik manual – namun pendekatan organisasi terhadap alat bantu terus terfragmentasi, dengan menggunakan rata-rata lebih dari 10 alat bantu keamanan data. Namun, organisasi yang memiliki paling banyak alat juga mengalami lebih banyak insiden keamanan data, menunjukkan bahwa semakin besar proliferasi alat, semakin lemah keamanannya.

3

Organisasi selalu dibebani oleh tekanan insiden keamanan data eksternal dan internal, terutama pada data bisnis.

50% organisasi yang disurvei pernah mengalami serangan ransomware atau malware dalam satu tahun terakhir – serta banyak pengambil keputusan yang tidak yakin bahwa organisasi mereka sepenuhnya siap untuk mencegah dan mengatasi serangan di masa depan. Secara internal, orang dalam yang berbahaya menjadi perhatian utama. Selain itu, organisasi sangat prihatin dengan kerentanan data bisnis mereka. Hal ini sekali lagi menggarisbawahi pentingnya platform keamanan yang menangani risiko secara komprehensif.

Temuan Penting

4

Organisasi membutuhkan Cloud dan AI untuk mendorong transformasi digital – tetapi hal tersebut juga merupakan lokasi data yang paling rentan.

Aplikasi cloud dan teknologi AI telah menjadi hal yang penting bagi kolaborasi dan produktivitas organisasi – namun, evolusi ini juga menciptakan risiko yang lebih dinamis dan beragam. Ketika organisasi menggunakan AI, sangat penting untuk melakukan peningkatan keamanan data agar dapat digunakan secara bertanggung jawab dan aman.

5

Otomatisasi dan AI menjanjikan jalan untuk perlindungan yang lebih baik.

Organisasi ingin agar tim mereka menghabiskan lebih sedikit waktu untuk deteksi dan lebih banyak waktu untuk pencegahan. Otomatisasi dapat memungkinkan tim untuk lebih fokus pada tindakan proaktif, sementara penggunaan AI untuk keamanan data membantu organisasi menjadi lebih strategis dan lebih cerdas dalam menghadapi ancaman di masa depan.

1

Para pengambil keputusan berpikir data mereka terlindungi, namun kenyataannya tidak sesuai dengan persepsi.

Para pengambil keputusan berpikir data mereka terlindungi, namun kenyataannya tidak sesuai dengan persepsi.

Di permukaan, para pengambil keputusan memproyeksikan tingkat kepercayaan dan kepuasan yang tinggi terhadap solusi keamanan data mereka. Mayoritas organisasi setuju bahwa kontrol keamanan data mereka cukup memadai untuk mencegah pembobolan data, mereka merasa bahwa mereka mengetahui di mana sebagian besar data mereka berada, dan bahwa mereka dapat mendeteksi sebagian besar risiko di sekitar data.

Di saat yang sama, organisasi terus mengalami insiden keamanan data dalam jumlah yang cukup besar – rata-rata 59 insiden dalam 12 bulan terakhir, seperlima di antaranya dianggap 'parah'. Dampak dari insiden ini sangat luas karena rata-rata, organisasi memperkirakan bahwa total biaya finansial dari insiden keamanan data yang paling parah adalah sekitar USD 244 ribu – yang berarti insiden tahunan dapat menelan biaya hingga USD 15 juta. Selain biaya-biaya ini, empat dari 10 pengambil keputusan juga mengatakan biaya operasional untuk memulihkan insiden keamanan data dan kerugian bisnis akibat kerusakan reputasi sangat memprihatinkan.

Selain itu, 92% menghadapi tantangan, terutama di bidang biaya, integrasi, dan waktu untuk mengimplementasikan, yang menghambat kemampuan mereka untuk berinvestasi lebih lanjut dalam keamanan data, menggarisbawahi kebutuhan akan solusi yang lebih ramah anggaran dan hemat tenaga kerja.

Persepsi keyakinan dalam kesiapan keamanan data berbeda dari realitas insiden yang dialami organisasi. Meskipun penting bagi organisasi untuk mengetahui di mana data berada dan mendeteksi risiko, langkah-langkah ini secara individu, atau secara terpisah, tidak cukup untuk membantu organisasi mencegah insiden yang membuat para pengambil keputusan keamanan data dan risiko terjaga di malam hari.

Seperti yang dikatakan oleh seorang CISO (Chief Information Security Officer) di bidang layanan keuangan, "Saya tidak bisa mengatakan kepada direksi saya, 'Saya telah mengamankan datanya, hanya saja saya tidak melindunginya'... hal terakhir yang ingin kami lihat adalah bank kami gagal tampil di halaman depan Wall Street Journal."

59

Jumlah rata-rata insiden keamanan data dalam 12 bulan terakhir

HINGGA
USD 15 Juta

Biaya tahunan insiden keamanan yang parah

2

Memiliki lebih banyak alat bukan berarti keamanan atau efisiensi data menjadi lebih baik – justru sebaliknya.

Memiliki lebih banyak alat bukan berarti keamanan atau efisiensi data menjadi lebih baik – justru sebaliknya.

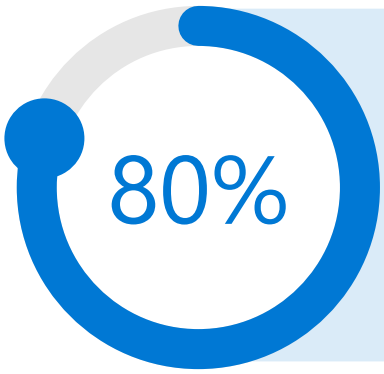
Organisasi mulai menyadari bahwa pendekatan solusi titik selama bertahun-tahun telah menciptakan kesenjangan dalam visibilitas dan efisiensi karena alat keamanan data yang terpisah-pisah. Tren tersebut kini memberi harapan akan adanya solusi terintegrasi untuk keamanan data dengan 80% responden setuju bahwa platform keamanan data yang komprehensif dengan solusi terintegrasi lebih unggul daripada menggunakan beberapa solusi terbaik yang harus diintegrasikan dan dikelola secara manual.

Namun, meskipun sebagian besar menganggap solusi terintegrasi lebih unggul, penggunaan alat keamanan data sangat banyak dan terfragmentasi.

Hasilnya, organisasi melaporkan bahwa mereka rata-rata menggunakan 10 alat keamanan data untuk mengatasi risiko keamanan data, termasuk Pencegahan Kehilangan Data, Perlindungan Informasi, Manajemen Risiko Orang Dalam, Manajemen Informasi & Peristiwa Keamanan (SIEM), Broker Keamanan Akses Cloud, dan banyak lagi. Bahkan untuk organisasi dengan lebih dari 5.000 karyawan, terdapat lebih banyak jumlah rata-rata alat.

Memiliki lebih banyak alat mungkin menciptakan rasa aman yang palsu, karena mereka yang menggunakan lebih banyak alat (16+) lebih percaya diri dengan postur keamanan data mereka dibandingkan dengan mereka yang menggunakan lebih sedikit alat (61% vs 56%).

Namun, rasa aman tersebut bertentangan dengan penelitian yang dilakukan, karena organisasi dengan 16 alat atau lebih, juga mengalami lebih banyak insiden keamanan data pada tahun lalu – rata-rata 133 insiden – dibandingkan dengan organisasi yang memiliki lebih sedikit alat yang mengalami 48 insiden.

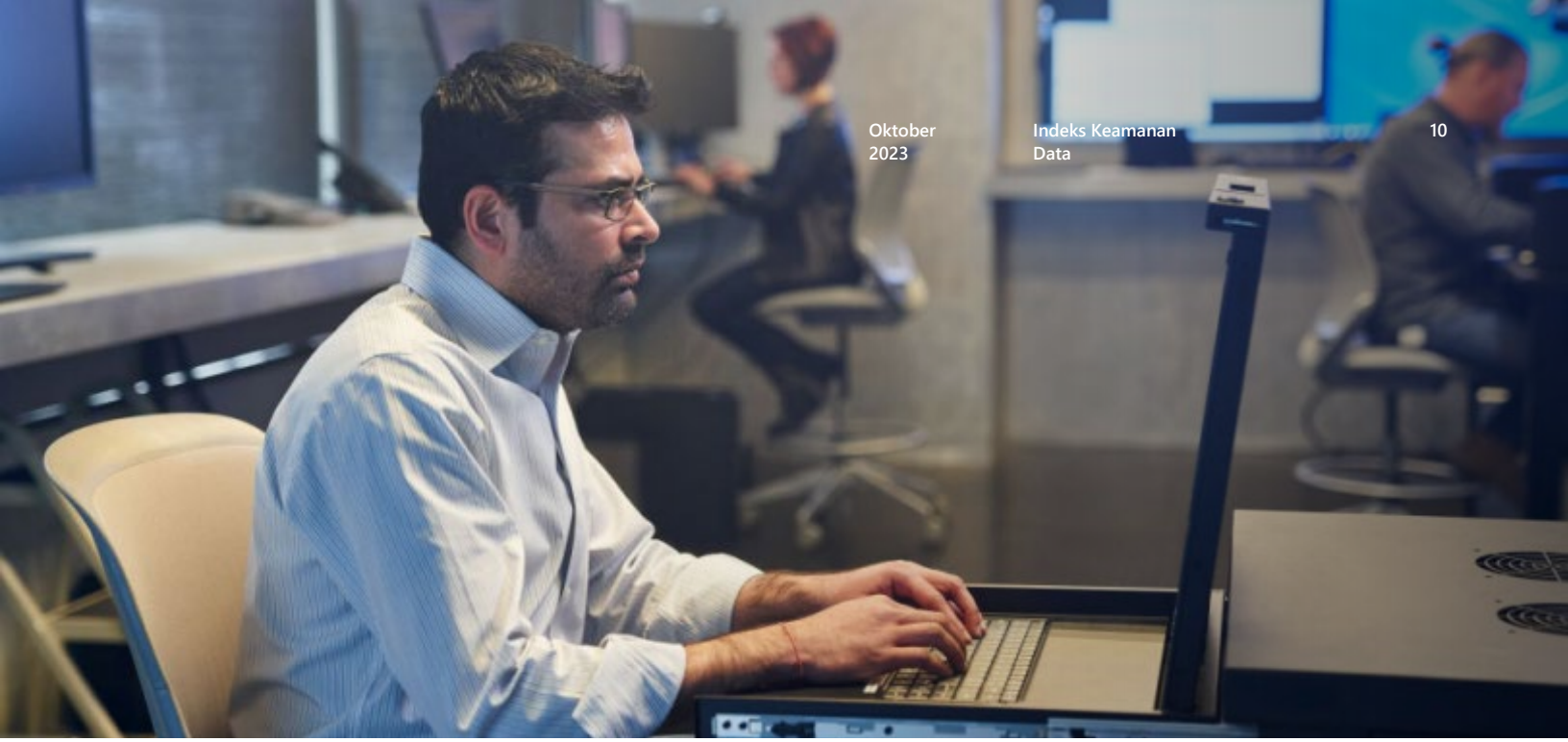


Setuju bahwa platform keamanan yang komprehensif dengan solusi terintegrasi lebih unggul daripada menggunakan beberapa solusi terbaik yang harus diintegrasikan dan dikelola secara manual.

2,8x

Lebih banyak insiden keamanan data dalam satu tahun terakhir

Untuk organisasi dengan 16 alat atau lebih (dibandingkan dengan organisasi dengan lebih sedikit alat)



Alasan untuk keamanan data yang lebih baik melalui solusi yang lebih terintegrasi dan lebih sedikit alat menjadi lebih kuat lagi ketika melihat sentimen dan praktik dari mereka yang lebih memilih solusi terbaik atau lebih banyak alat.

"Bagaimana data akan dikumpulkan, diagregasi, dan digunakan dari beberapa sistem? Banyak titik data yang berbeda perlu disatukan dalam satu ekosistem agar dapat benar-benar berfungsi. Atau, Anda benar-benar memiliki keamanan data versi keju Swiss."

Wakil Presiden
Manufaktur/Produksi IT

Pertama, beberapa alat keamanan data yang berbeda dapat menyebabkan kesenjangan dalam visibilitas dan lebih banyak data bayangan. Faktanya, mereka yang peduli dengan data bayangan cenderung lebih memilih solusi yang terbaik. Hal ini kemungkinan besar terjadi karena organisasi dengan pendekatan terbaik perlu melakukan lebih banyak upaya untuk mendapatkan visibilitas yang komprehensif ke dalam postur keamanan data mereka.

Kedua, mengelola solusi yang terpisah-pisah membawa lebih banyak kerumitan pada tim keamanan data, karena setiap solusi yang berbeda membutuhkan staf yang berdedikasi, instalasi dan pemeliharaan agen titik akhir, dan berbagai proses baru. Sebagai contoh, tinjauan dan triase peringatan, salah satu tugas yang membutuhkan staf dan sumber daya. Meningkatnya jumlah peringatan menunjukkan upaya ekstra yang diperlukan oleh tim keamanan data saat mengelola solusi yang terisolasi. Organisasi dengan lebih banyak alat menerima rata-rata 96 peringatan keamanan data per hari, sementara tim dengan lebih sedikit alat menerima kurang dari setengahnya, yaitu 44. Selain itu, mereka tidak dapat meninjau sebanyak mungkin peringatan ini seperti yang dapat dilakukan oleh tim dengan alat yang lebih sedikit (61%, dibandingkan dengan 68%). Hal ini sering kali juga mengakibatkan organisasi yang memiliki lebih banyak alat menjadi lebih reaktif dibandingkan dengan organisasi yang menggunakan lebih sedikit alat.

Terakhir, lebih banyak alat juga menunjukkan bahwa organisasi harus mengerahkan upaya ekstensif untuk mengintegrasikan wawasan dan rencana perbaikan, dan informasi dapat disalahartikan. Ketika ditanya tentang tantangan keamanan data yang paling utama, biaya untuk mengimplementasikan atau memelihara solusi keamanan data dan tantangan untuk mengintegrasikan solusi keamanan data menduduki peringkat dua teratas.

Hal ini berarti proses yang lebih lama dan lebih lambat, dengan 37% organisasi yang menggunakan 16 alat atau lebih melaporkan bahwa mereka membutuhkan waktu satu bulan atau lebih untuk menyelesaikan penyelidikan keamanan data dibandingkan dengan hanya 21% organisasi yang menggunakan lebih sedikit alat.

"Saat ini, kami sedang merangkak. Setiap sistem yang kami miliki, semuanya memiliki portal sendiri, alat sendiri, dan cara sendiri untuk menangani berbagai hal. Setiap orang memiliki caranya sendiri, sesuai dengan keahliannya. Kemudian mereka semua kembali berkumpul dan memutuskan apa yang sedang terjadi, dan kami mengatasinya dari sana. Jadi, saat ini masih banyak pekerjaan yang harus dilakukan secara manual," ujar Direktur Infrastruktur & Operasi di bidang manufaktur dan produksi.

Pada akhirnya, dengan memilih untuk terus menggunakan berbagai solusi, organisasi mengabaikan pembicaraan mereka sendiri tentang pemahaman bahwa solusi terintegrasi lebih unggul dan berjalan ke arah yang berlawanan – menghabiskan waktu dan uang mereka.

HASIL DARI MEREKA YANG MENGGUNAKAN LEBIH SEDIKIT (<16) VERSUS LEBIH BANYAK (16+) ALAT KEAMANAN DATA

	Volume Alat yang Rendah	Volume Alat yang Tinggi
Jumlah **insiden keamanan data** selama 12 bulan terakhir	48	133
Proporsi **insiden** keamanan data yang parah	19%	26%
Strategi keamanan data kami saat ini lebih bersifat **reaktif**	31%	40%
Tertantang dengan **solusi** terintegrasi	24%	39%
Tim keamanan data menghabiskan sebagian besar waktunya untuk **merespons**	19%	26%
Kami **percaya diri** dengan postur keamanan data kami	56%	61%
Jumlah rata-rata peringatan **yang diterima** setiap hari	44	96
Proporsi peringatan yang bisa kami **tinjau** setiap hari	68%	61%
Diperlukan waktu satu bulan atau lebih untuk menyelesaikan penyelidikan keamanan data	21%	37%

3

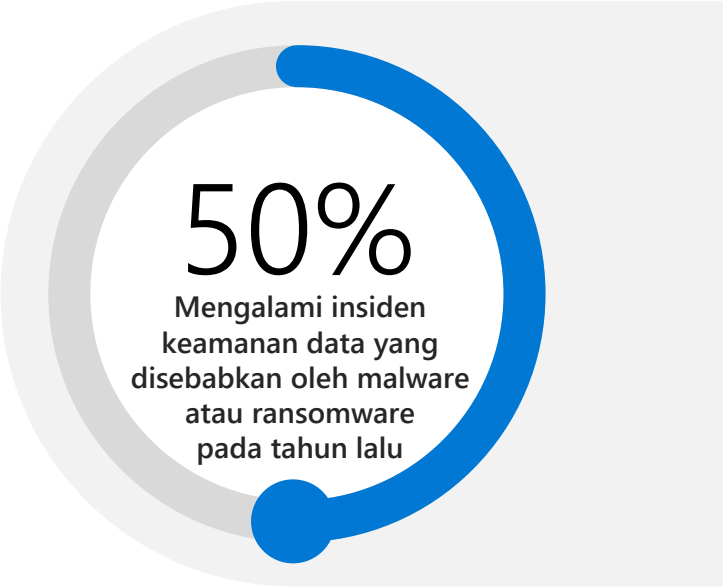
Organisasi selalu dibebani oleh tekanan insiden keamanan data eksternal dan internal, terutama pada data bisnis.

Organisasi terus dibebani oleh tekanan insiden keamanan data eksternal dan internal, terutama pada data bisnis.

Karena faktor-faktor di sekitar data – termasuk orang-orang yang berinteraksi dengan data, aktivitas di sekitar data, serta perangkat dan aplikasi yang digunakan untuk memproses data – terus berkembang, insiden keamanan data dan pembobolan data dapat terjadi kapan saja dan di mana saja. Dan, ancaman ini datang baik dari penyerang eksternal maupun personel tepercaya, termasuk karyawan, kontraktor, dan mitra. Baik secara sengaja maupun tidak, semua pihak dapat menyebabkan insiden keamanan data – yang berarti ada kebutuhan konstan untuk melindungi di banyak area.

Seorang Wakil Presiden IT di bidang jasa keuangan berkata, "Apa yang Anda coba lindungi selalu berubah. Ini adalah target yang bergerak. Hal ini akan selalu berkembang, berubah, dan fleksibel. Apa yang Anda lindungi dan tempatnya hanya akan semakin bervariasi."

Meskipun insiden keamanan data dapat berasal dari berbagai sumber, ancaman eksternal berupa insiden malware atau ransomware - contoh di mana perangkat lunak berbahaya menyusup ke sistem, memberi penyerang akses tidak sah ke sistem atau jaringan - jauh lebih umum, dengan 50% organisasi yang disurvei pernah mengalami setidaknya satu kali dalam satu tahun terakhir.



Selain itu, serangan ini merupakan serangan yang membuat organisasi merasa paling rentan, dengan 41% mengatakan bahwa mereka merasa paling tidak siap untuk menangani serangan malware atau ransomware di tahun depan. Rasa kerentanan ini bahkan lebih tinggi di antara organisasi yang lebih memilih pendekatan terbaik – 44% merasa tidak siap untuk menghadapi serangan seperti ini, dibandingkan dengan 36% organisasi yang lebih memilih solusi terintegrasi.

Mengamankan dan mencegah risiko orang dalam juga merupakan hal yang paling penting bagi para pengambil keputusan. 35% mengatakan bahwa mereka perlu memperkuat pertahanan terhadap orang dalam yang berbahaya dan akun yang disusupi, dan sepertiganya mengkhawatirkan insiden orang dalam yang tidak disengaja. Meskipun insiden orang dalam yang berbahaya mungkin bukan penyebab utama pembobolan keamanan data, namun ini adalah jenis insiden paling umum kedua yang paling tidak siap dicegah oleh para pengambil keputusan.

"Setidaknya sebulan sekali, saya menerima telepon dari direktur yang panik... 'kami telah mengalami suatu peristiwa, saya telah menemukan suatu peristiwa, atau tim ancaman telah menemukan suatu peristiwa'. Beberapa di antaranya tidak disengaja, beberapa di antaranya adalah orang-orang yang tidak mengetahui atau memahami hak istimewa mereka."

CISO Pemerintah AS

Orang dalam adalah individu-individu tepercaya yang biasanya telah diberi akses, atau memiliki pengetahuan tentang sumber daya, data, atau sistem perusahaan yang tidak tersedia secara terbuka untuk umum. Akibatnya, risiko keamanan data yang terkait dengan orang dalam cenderung lebih sulit dipahami dan sulit dideteksi. Seperti yang dikatakan oleh Bret Arsenault, CISO Microsoft, "Pada akhirnya, tidak masalah apakah pembobolan itu disengaja atau tidak disengaja. Program risiko orang dalam harus menjadi bagian dari strategi keamanan setiap perusahaan."

RINGKASAN INSIDEN KEAMANAN DATA

Penyebab insiden keamanan data	Insiden yang paling umum terjadi dalam 12 bulan terakhir	Paling tidak siap untuk melakukan pencegahan dalam 12 bulan terakhir
Malware atau ransomware	**50%**	**41%**
Akun yang disusupi	**38%**	**35%**
Serangan penolakan layanan (DoS)	**35%**	**33%**
Orang dalam yang lalai	**32%**	**29%**
Orang dalam yang tidak sengaja	**31%**	**32%**
Orang dalam yang berbahaya	**31%**	**35%**
Properti fisik	**29%**	**29%**

Solusi keamanan data yang dipilih organisasi juga harus berfungsi untuk berbagai data sensitif, termasuk data bisnis bernilai tinggi, data operasional, dan data pribadi. Selama insiden keamanan data dalam 12 bulan terakhir, 74% organisasi memiliki data bisnis yang terekspos, 65% mengalami data operasional yang disusupi, dan 58% mengalami data pribadi yang rentan. Di antara berbagai jenis data, kekayaan intelektual, IT dan desain jaringan, serta PII telah disusupi atau diekspos paling sering.

Ke depannya, 77% organisasi menganggap data bisnis, seperti kekayaan intelektual dan kode sumber, sebagai data yang paling rentan. Hal ini terutama karena data bisnis memainkan peran penting dalam membangun keunggulan kompetitif dan menghasilkan pendapatan. Namun, mengidentifikasi dan mengklasifikasikan data tersebut dapat menjadi tantangan, karena pengenalan pola tradisional, ekspresi reguler, atau teknologi pencocokan fungsi mungkin tidak secara efektif mengidentifikasi konten yang tidak memiliki format string atau kata kunci tertentu. Pada akhirnya, organisasi membutuhkan teknologi yang lebih canggih untuk membantu menemukan dan melindungi data sensitif yang rentan tersebut.

JENIS DATA YANG PALING BERISIKO DALAM 12 BULAN KE DEPAN

77% **Data Bisnis**		64% **Data Operasional**		63% **Data Pribadi**	
Kekayaan intelektual	**30%**	IT dan desain jaringan	**29%**	Informasi Identifikasi Pribadi (PII)	**31%**
Kode sumber	**28%**	Laporan keuangan	**18%**	Informasi sumber daya manusia (penggajian, resume, dll.)	**21%**
Rencana bisnis	**27%**	Laporan penjualan dan pendapatan	**15%**	Data industri kartu pembayaran (PCI)	**18%**
Rahasia dagang	**24%**	Pengadaan & faktur	**12%**	Informasi Kesehatan yang Dilindungi (PHI)	**18%**
File merger & akuisisi	**20%**	Dokumen/ perjanjian hukum	**12%**	Kredensial	**17%**
Spesifikasi konstruksi	**18%**	Proses manufaktur/file batch	**11%**		

4

Organisasi membutuhkan Cloud dan AI untuk mendorong transformasi digital – tetapi keduanya juga merupakan lokasi data yang paling rentan.

Organisasi membutuhkan Cloud dan AI untuk mendorong transformasi digital – tetapi keduanya juga merupakan lokasi data yang paling rentan.

Kolaborasi melalui aplikasi dan platform cloud, yang dikombinasikan dengan teknologi AI baru, secara signifikan meningkatkan produktivitas karyawan dan memungkinkan pengaturan kerja yang fleksibel, sehingga membuat aplikasi cloud dan teknologi AI menjadi penting bagi organisasi. Rata-rata, organisasi saat ini menggunakan 147 layanan cloud publik yang mencakup SaaS, PaaS, dan IaaS.[1] Dan, 66% organisasi telah mengembangkan strategi AI, dengan 36% di antaranya telah mengimplementasikannya.[2] Namun, evolusi ini telah menciptakan risiko yang lebih dinamis dan beragam, karena sulitnya mendefinisikan batasan data secara jelas di berbagai lingkungan.

1. Measuring Risk and Risk Governance (Mengukur Risiko dan Tata Kelola Risiko), Cloud Security Alliance (CSA), 2022
2. Penelitian AI keamanan data Microsoft, Hypothesis, Mar 2023

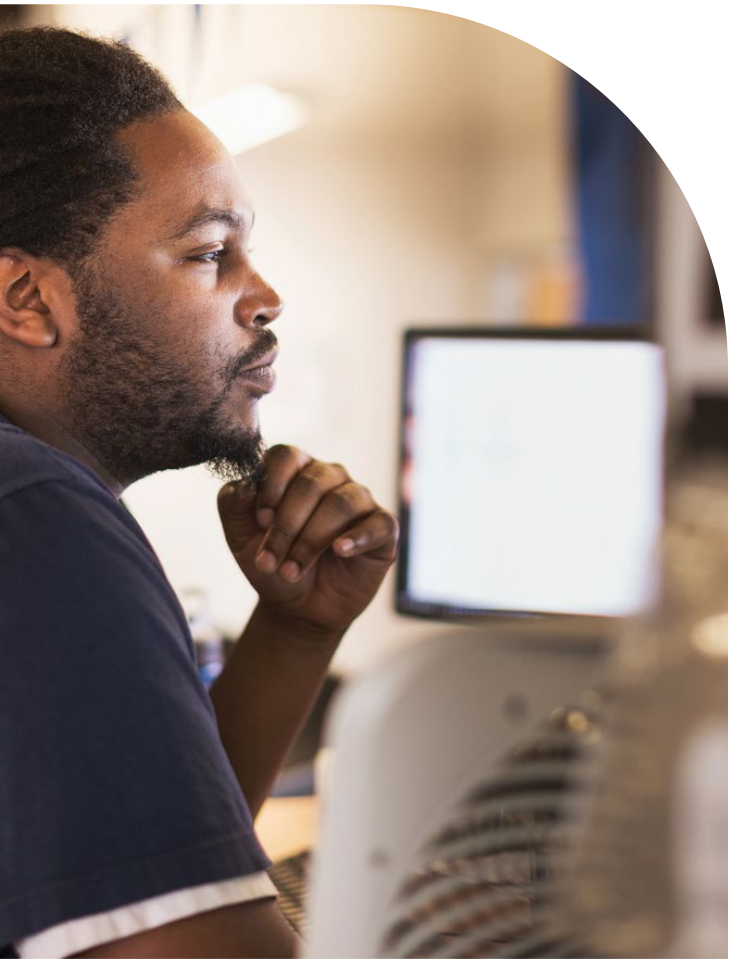
Bahkan kini semakin penting untuk memiliki solusi keamanan data yang tepat untuk lokasi-lokasi dengan produktivitas data yang tinggi. Dalam 12 bulan terakhir, 42% organisasi melaporkan insiden keamanan pada penyimpanan cloud dan 31% pada email, pesan instan, atau alat rapat online. Insiden tampaknya paling sering terjadi di tempat yang paling banyak menghasilkan produktivitas dan kolaborasi.

Mengelola jenis insiden ini membutuhkan sumber daya, dan 79% organisasi melaporkan bahwa tim keamanan data mereka membutuhkan lebih banyak orang untuk mengelola tanggung jawab keamanan data penting secara efektif. Namun, di antara organisasi yang menyatakan bahwa mereka membutuhkan lebih banyak orang, mayoritas (57%) lebih memilih pendekatan terbaik. Preferensi ini menyoroti bahwa organisasi yang menggunakan lebih banyak solusi mungkin akan lebih sulit untuk mengidentifikasi risiko yang sebenarnya di antara berbagai aktivitas pengguna.

RINGKASAN LOKASI DATA

Lokasi Data	Disusupi dalam 12 bulan terakhir	Paling berisiko
Penyimpanan cloud (misalnya, Box, OneDrive, Google Drive)	42%	54%
Email/Pesan instan/Alat rapat online	31%	39%
Platform sebagai layanan (PaaS)	29%	34%
Infrastruktur sebagai layanan (IaaS)	28%	36%
AI (misalnya, ChatGPT, Bard, dll.)	27%	38%
Basis data / data lake berbasis SaaS	27%	41%
Titik akhir / perangkat	25%	36%
Repositori / bagian file / basis data on-prem	24%	28%
Data bayangan	21%	23%
Aplikasi lini bisnis	17%	25%
Alat Pengembang	16%	23%

Dengan lebih dari sepertiga organisasi yang menerapkan strategi AI, dan lebih banyak lagi yang akan menerapkannya, AI diadopsi dengan kecepatan yang belum pernah terjadi sebelumnya, jauh lebih cepat dibandingkan dengan adopsi cloud dan email di masa lalu. Ketika organisasi menggunakan AI, sangat penting untuk meningkatkan keamanan data agar dapat digunakan secara bertanggung jawab dan mencegah risiko. AI dianggap sebagai lokasi yang paling berisiko untuk insiden keamanan data, dibandingkan dengan lokasi lainnya, dan 27% organisasi telah mengalami pembobolan keamanan data AI. Kekhawatiran organisasi terhadap risiko penggunaan AI berpusat pada kurangnya kontrol terhadap data yang dibagikan dengan AI, kurangnya kontrol untuk mendeteksi dan memitigasi penggunaan AI yang berisiko, kurangnya transparansi mengenai bagaimana model AI generatif dilatih, dan kebocoran informasi rahasia melalui AI.



"AI bagus untuk produktivitas dan efisiensi, tetapi memiliki potensi risiko keamanan dan data." Pernyataan seorang Pengambil Keputusan Keamanan di sebuah perusahaan.

Meskipun ada kekhawatiran seputar AI, para pengambil keputusan juga dapat melihat potensinya, terutama karena vendor di pasar mengembangkan inovasi untuk membantu memberdayakan bisnis melalui penggunaan AI yang bertanggung jawab. Namun, untuk memanfaatkan AI lebih lanjut, organisasi melaporkan bahwa kontrol utama yang mereka butuhkan adalah mendeteksi konten berbahaya atau berisiko dalam AI, mengenkripsi, menyamarkan, atau menganonimkan data sebelum data tersebut diunggah ke AI, dan mengidentifikasi data sensitif yang dihasilkan oleh AI.

5 KONTROL KEAMANAN DATA TERATAS YANG DIPERLUKAN UNTUK AI

1. **Mendeteksi konten berbahaya atau berisiko** di AI
2. **Mengenkripsi, menyamarkan, atau menganonimkan data** sebelum diunggah ke AI
3. **Mengidentifikasi data sensitif** yang dihasilkan oleh AI
4. **Mencegah data sensitif agar tidak diunggah** ke AI
5. **Mendeteksi manipulasi model atau data** di AI

5

Otomatisasi dan AI menjanjikan jalan untuk perlindungan yang lebih baik.

Otomatisasi dan AI menjanjikan jalan untuk perlindungan yang lebih baik.

Dalam dunia yang ideal, tanpa kendala berdasarkan prioritas atau anggaran organisasi, separuh dari organisasi ingin menjadi lebih proaktif dalam hal manajemen keamanan data, menghabiskan lebih banyak waktu untuk hal-hal seperti penemuan data sensitif dan risiko terkait di sekitarnya serta pencegahan insiden keamanan data. Saat ini, lebih dari separuh organisasi menghabiskan sebagian besar waktu mereka untuk berfokus pada tindakan reaktif seperti deteksi insiden, respons, dan investigasi. Deteksi dan respons terhadap insiden keamanan data ini sangat memakan waktu – sebagian besar organisasi membutuhkan waktu sekitar satu bulan untuk menyelesaikan insiden keamanan data dan untuk beberapa organisasi, penyelesaiannya bisa memakan waktu hingga enam bulan.

Manfaat mengadopsi strategi yang lebih proaktif terbukti, karena organisasi yang disurvei yang lebih proaktif telah mengalami insiden keamanan data dengan biaya yang lebih rendah, lebih mungkin dapat menyelidiki insiden tersebut dalam waktu kurang dari satu bulan, dan lebih mungkin meyakini bahwa kontrol pertahanan mereka cukup memadai dalam mencegah pembobolan data.

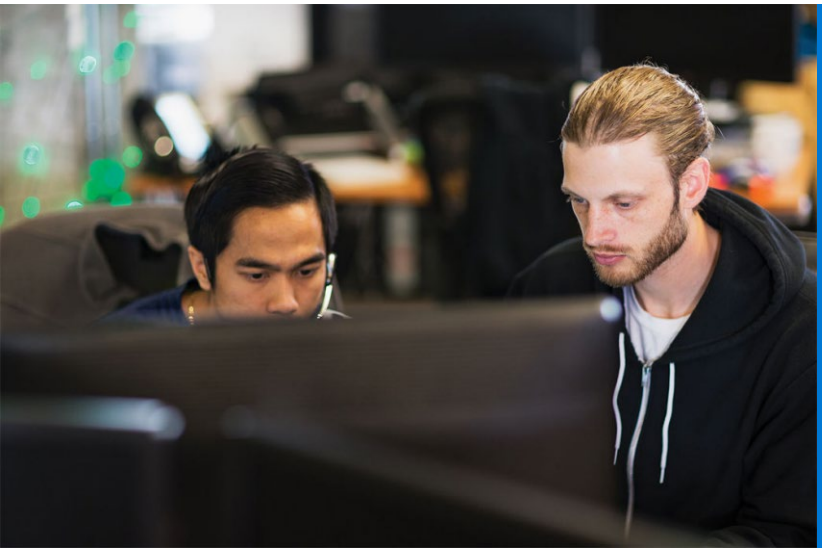
Meskipun organisasi menyadari bahwa langkah-langkah keamanan data yang proaktif dapat membantu mengurangi risiko keamanan data, namun mereka tidak membuat kemajuan dalam mengimplementasikan langkah-langkah tersebut. Sebagai contoh, organisasi yang ingin lebih proaktif dengan mengalokasikan lebih banyak waktu untuk pencegahan lebih cenderung memilih solusi terbaik, yang sebenarnya menuntut upaya yang lebih besar dalam menangani tindakan reaktif ketika menyatukan sinyal deteksi dan kontrol respons.

HASIL DARI ORGANISASI YANG LEBIH PROAKTIF VS. ORGANISASI YANG LEBIH REAKTIF	Lebih Proaktif	Lebih Reaktif
Dampak biaya rata-rata insiden keamanan data dalam 12 bulan terakhir	**USD 207 ribu**	**USD 330 ribu**
Menyelesaikan penyelidikan keamanan data dalam waktu rata-rata kurang dari sebulan	**80%**	**68%**
Kontrol pertahanan kami cukup memadai dalam mencegah pembobolan data	**77%**	**68%**

Karena sumber daya dan staf yang terbatas serta alokasi upaya antar aktivitas yang mungkin tidak ideal, organisasi mencari teknologi untuk membantu mereka menyisihkan lebih banyak waktu untuk aktivitas proaktif. Otomatisasi adalah salah satu cara bagi organisasi untuk meluangkan waktu untuk pendekatan yang lebih proaktif terhadap keamanan data. 74% organisasi yang disurvei lebih memilih mitigasi risiko semi atau sepenuhnya otomatis, yang memungkinkan tim keamanan meminimalkan dampak potensi insiden keamanan data sebelumnya daripada tinjauan manual. Selain itu, organisasi menyadari banyak tugas lain yang dapat memperoleh manfaat dari otomatisasi, seperti pembuatan laporan keamanan data, otomatisasi alur kerja manajemen insiden, dan respons serta investigasi insiden. Sebagian besar tugas utama yang ingin diotomatisasi oleh tim keamanan adalah tindakan reaktif. Dengan mengotomatiskan tugas-tugas ini, organisasi dapat meringankan beban tim keamanan data mereka, sehingga mereka dapat mengambil sikap yang lebih proaktif.

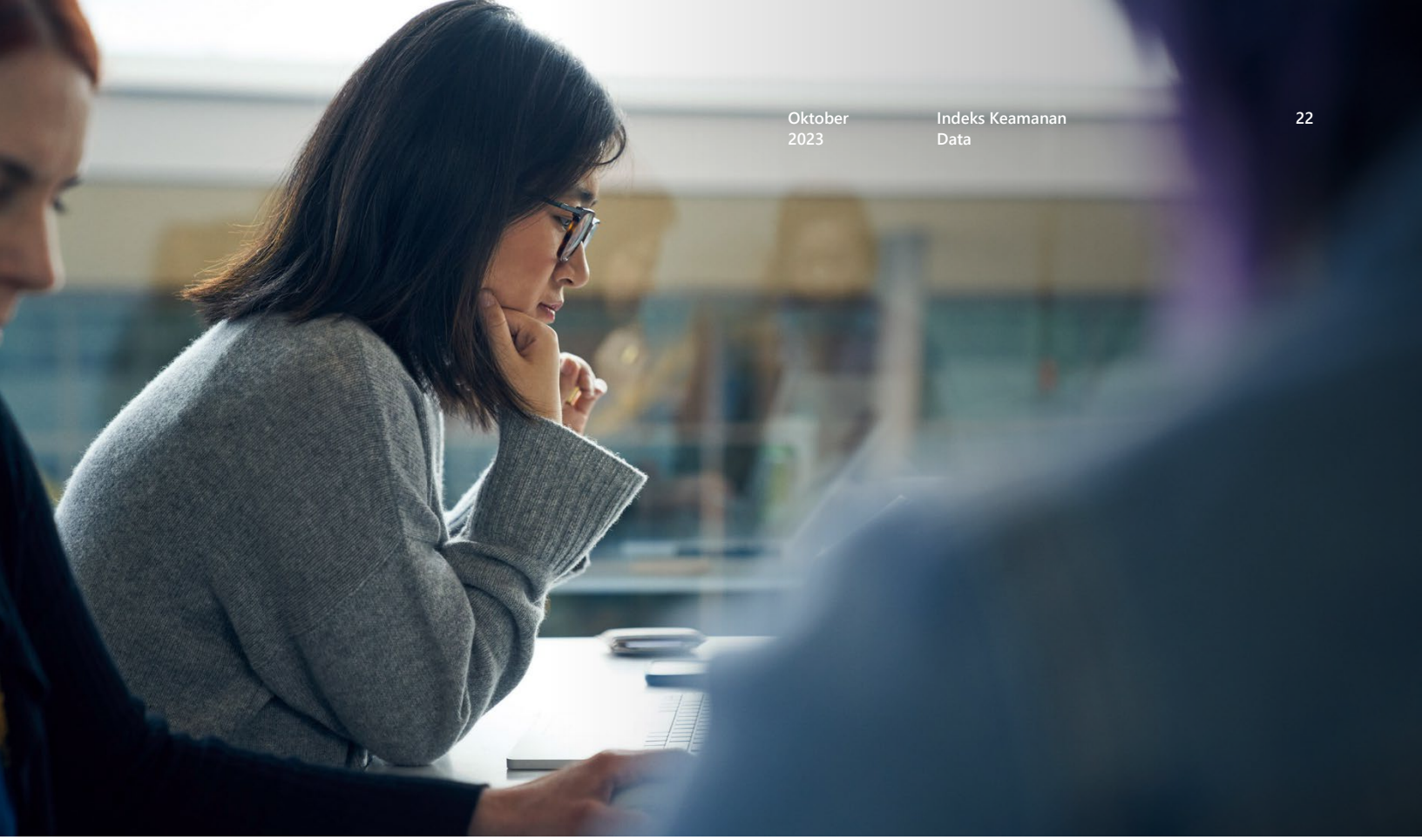
5 AREA TERATAS YANG INGIN DIOTOMATISASI/ DIRINGANKAN OLEH TIM KEAMANAN DATA

Reaktif	1	Menciptakan alur kerja otomatis untuk manajemen dan respons insiden
	2	Membuat laporan keamanan data
Reaktif	3	Merespons dan menangani insiden keamanan data
	4	Mengalihkan insiden ke tim yang tepat (misalnya, SOC, hukum, SDM) selama investigasi
	5	Menginvestigasi insiden keamanan data



"Ada begitu banyak data yang berisiko untuk dievaluasi secara manual. AI dapat membantu mempercepat waktu respons tim kami dan melindungi data karena kami kekurangan sumber daya."

Pengambil Keputusan Keamanan Inggris



Menggunakan AI untuk keamanan data juga dapat membantu organisasi menjadi lebih strategis dan lebih cerdas dalam menghadapi ancaman di masa depan. Teknologi ini mempercepat respons terhadap insiden yang terdeteksi, memberikan waktu bagi para profesional keamanan data untuk menyelidiki lebih lanjut. Serupa dengan otomatisasi, organisasi mengutip banyak skenario di mana AI dapat membantu memberikan keamanan yang lebih kuat, **sehingga menghemat waktu tim.** Skenario teratas untuk penggunaan AI termasuk secara otomatis memblokir pembagian data yang tidak sesuai, mendeteksi risiko keamanan data yang kritis/aktivitas data yang tidak normal, dan menyelidiki potensi insiden keamanan data.

Dengan memanfaatkan kelebihan AI dan otomatisasi serta bergerak menuju solusi yang lebih terintegrasi, organisasi dapat menerapkan strategi keamanan data yang lebih proaktif, dan menyiapkan diri untuk masa depan yang lebih aman.

SKENARIO TERATAS DI MANA AI DIGUNAKAN

Memblokir secara otomatis pembagian data yang tidak sesuai

Mendeteksi risiko keamanan data kritis / aktivitas data yang tidak normal

Rekomendasi untuk mengamankan lingkungan data Anda dengan lebih baik

Menginvestigasi potensi insiden keamanan data

Menyempurnakan kebijakan keamanan data

Rekomendasi Akhir

- Mengadopsi platform terintegrasi untuk memperkuat postur keamanan data
- Melindungi dari insiden keamanan data baik dari luar maupun dalam dengan pendekatan pertahanan yang mendalam
- Meningkatkan strategi keamanan data Anda dengan AI dan otomatisasi

Mengadopsi platform terintegrasi untuk memperkuat postur keamanan data

Menurut temuan dalam penelitian ini, solusi yang lebih sedikit dapat memberikan keamanan yang lebih baik. Hal ini mungkin terlihat berlawanan dengan intuisi, namun organisasi harus memerangi rasa percaya diri palsu yang muncul dari banyak solusi yang terisolasi. Konsolidasi vendor menawarkan pendekatan strategis yang tidak hanya mengurangi biaya tetapi juga meningkatkan keamanan.

Para pengambil keputusan keamanan data dapat memulai transformasi ini dengan memberdayakan tim mereka untuk mendedikasikan lebih banyak waktu untuk pekerjaan strategis seperti meneliti dan merencanakan kontrol keamanan baru serta mengoptimalkan kebijakan keamanan – sesuatu yang disetujui oleh 84% pengambil keputusan untuk dilakukan. Proses ini melibatkan penggantian solusi lama yang terkotak-kotak, yang sering dianggap sebagai 'yang terbaik dari yang terbaik' namun gagal terintegrasi secara efektif dengan alat lain.

Para pengambil keputusan dapat membina kolaborasi yang erat dengan tim mereka untuk menetapkan tujuan program keamanan data dan indikator kinerja utama (KPI). Kemudian dilanjutkan dengan mendefinisikan persyaratan solusi dan mengidentifikasi fitur-fitur yang tidak bisa dinegosiasikan. Pendekatan ini memberdayakan mereka untuk menentukan vendor yang mampu menyediakan alat yang selaras dengan tujuan menyeluruh mereka. Yang terpenting, hal ini mendorong pola pikir yang berpikiran maju dan membantu tim agar tidak terlalu terpaku pada praktik-praktik yang ada atau kasus-kasus penggunaan yang terisolasi, sehingga mereka dapat mengimplementasikan perubahan-perubahan yang diperlukan menuju pendekatan yang lebih terintegrasi.

Platform keamanan data yang terintegrasi harus memberdayakan tim keamanan untuk melakukan semua tugas penting berikut ini dengan lancar:

1. Menemukan dan melindungi data sensitif dalam lanskap digital mereka.
2. Mendeteksi risiko kritis yang terkait dengan data ini.
3. Mencegah penggunaan data sensitif secara tidak sah namun tidak berdampak pada aktivitas bisnis yang sah.

Dengan menerapkan strategi keamanan data yang terintegrasi, organisasi dapat mencapai tingkat perlindungan yang lebih tinggi sekaligus menyederhanakan infrastruktur keamanan mereka.

Melindungi dari insiden keamanan data baik dari luar maupun dalam dengan pendekatan pertahanan yang mendalam

Insiden keamanan data biasanya diakibatkan oleh penyerang eksternal, orang dalam yang berbahaya, atau orang dalam yang tidak sengaja. Organisasi harus mengambil langkah-langkah untuk melindungi data mereka, baik dengan mencegah akses yang tidak diizinkan dari ancaman eksternal maupun dengan memitigasi risiko pencurian oleh orang dalam atau pemaparan data yang tidak disengaja.

Untuk mengatasi tantangan ini, organisasi dapat mengadopsi pendekatan pertahanan yang mendalam terhadap keamanan data. Strategi ini serupa dengan perlindungan museum terhadap karya seni yang tak ternilai harganya: kamera keamanan canggih yang dilengkapi dengan intelijen ancaman memantau pengunjung, sistem tiket yang mengatur identitas dan akses ke museum, dan langkah-langkah keamanan yang ketat di sekitar karya seni yang beroperasi serupa dengan kontrol keamanan data yang melindungi data Anda yang berharga. Langkah-langkah ini mencegah potensi insiden, baik yang berasal dari pelaku kejahatan eksternal maupun individu yang sudah berada di dalam lingkungan organisasi.

Memerangi risiko keamanan data yang terus berkembang membutuhkan upaya bersama di seluruh organisasi untuk menerapkan strategi pertahanan yang mendalam ini. Kolaborasi tim keamanan data dengan departemen lain, seperti Pusat Operasi Keamanan (SOC), dapat mengoptimalkan investasi keamanan data. Khususnya, 66% organisasi yang menganggap diri mereka proaktif berinteraksi dengan tim SOC mereka, dibandingkan dengan 54% organisasi yang menganggap sebaliknya.

Seperti halnya kerja sama antar tim keamanan, solusi keamanan data juga harus terintegrasi secara mulus dengan sistem lain, seperti solusi XDR (Extended Detection and Response/Deteksi dan Respons yang Diperluas) atau IAM (Identity and Access Management/Manajemen Identitas dan Akses), agar dapat secara efektif mencegah insiden keamanan data baik dari eksternal maupun internal. Integrasi ini memungkinkan organisasi untuk melakukan investigasi dan respons yang komprehensif terhadap insiden keamanan, mendapatkan pemahaman menyeluruh tentang data, pelaku, dan aktivitas yang terdampak, serta merespons dengan berbagai kontrol mitigasi. Akibatnya, hal ini memberdayakan mereka untuk membuat tanggapan yang informatif, tepat, dan cepat untuk meminimalkan dampak dari potensi insiden keamanan.

Meningkatkan strategi keamanan data Anda dengan AI dan otomatisasi

Otomatisasi dan AI dapat membantu organisasi menjadi lebih proaktif dalam hal keamanan data. Berikut ini adalah beberapa rekomendasi bagi organisasi Anda untuk memulai perjalanan otomatisasi dan AI:

- Menemukan data sensitif: Manfaatkan AI untuk membantu mengidentifikasi data sensitif dan menerapkan kebijakan perlindungan, termasuk enkripsi dan manajemen hak. Hal ini sangat berharga untuk data bisnis yang mungkin menimbulkan tantangan untuk dideteksi melalui teknologi pengenalan pola tradisional. Organisasi dapat memanfaatkan teknologi klasifikasi, seperti pembelajaran mesin atau pengklasifikasi bertenaga AI, yang dikenal karena kecerdasan dan kemampuan untuk menemukan konten sensitif dengan cepat berdasarkan konteks data atau kategori bisnis. Sebagai alternatif, organisasi dapat menggunakan teknologi pencocokan data yang tepat untuk menemukan data operasional atau data pribadi.

  Selain itu, seiring dengan berkembangnya peraturan industri (misalnya, GDPR, HIPAA, atau PCI DSS) dan lanskap data yang semakin dinamis, maka sangat penting untuk memiliki teknologi klasifikasi canggih yang dapat disesuaikan dan mudah beradaptasi untuk mengidentifikasi kategori baru data sensitif.

- Mendeteksi risiko keamanan data yang kritis: Manfaatkan kekuatan AI untuk menentukan risiko kritis yang terkait dengan data sensitif Anda dan mengalokasikan sumber daya secara strategis untuk mengatasi potensi insiden berisiko tinggi. Teknologi AI dapat menghasilkan peringatan dengan akurasi tinggi, sehingga tim keamanan dapat menghemat waktu berharga yang digunakan untuk memilah-milah banyak peringatan positif palsu. Selain itu, AI dapat membantu organisasi dalam mengidentifikasi risiko yang sulit dipahami, terutama ketika pelaku kejahatan berusaha menghindari deteksi. Sangat penting untuk memanfaatkan kecepatan alat berat untuk mengalahkan para pelaku ancaman ini.

- Mencegah insiden keamanan data secara dinamis: Gunakan AI dan otomatisasi untuk menyesuaikan kontrol pencegahan dan mitigasi Anda secara otomatis berdasarkan risiko yang dinilai, sehingga memungkinkan strategi keamanan data yang lebih mudah beradaptasi dan proaktif. Ketika solusi berbasis AI mendeteksi dan mengevaluasi risiko, kontrol pencegahan otomatis dapat dengan cepat digunakan untuk melindungi data, menerapkan kontrol mitigasi secara tepat pada area berisiko tinggi. Misalnya, dalam kasus-kasus di mana indikator awal tujuan eksfiltrasi data terdeteksi oleh pengguna berisiko tinggi, organisasi dapat menerapkan kebijakan Pencegahan Kehilangan Data (DLP) yang lebih ketat, yang secara proaktif tetap berada di depan dalam menghadapi potensi insiden keamanan data.

Kami berharap wawasan dan rekomendasi dalam laporan ini dapat membantu Anda untuk meningkatkan postur keamanan data Anda dan membentengi organisasi Anda dari risiko yang terus berkembang.

Untuk mempelajari lebih lanjut tentang Keamanan Data Microsoft, lihat https://aka.ms/DataSecurityNews

Rincian Tujuan Penelitian, Metodologi, dan Perekrutan Audiens

Tujuan dari penelitian ini mencakup:

1. Memahami lanskap keamanan data, termasuk prioritas, pola pikir, dan tantangan

2. Memetakan sebab dan akibat dari insiden keamanan data dan mengidentifikasi tindakan yang dapat dilakukan oleh tim keamanan data untuk meningkatkan postur keamanan data

3. Mempelajari masa depan keamanan data, termasuk strategi dan inovasi yang muncul seputar penggunaan AI untuk keamanan data

Metodologi:

Survei online multinasional selama 15 menit dilakukan pada tanggal 28 Juli-9 Agustus 2023, di antara 822 pengambil keputusan keamanan data.

Pertanyaan-pertanyaan seputar lanskap keamanan data, bagaimana tim keamanan data mengalokasikan sumber daya mereka, insiden keamanan data, dan sikap terhadap dan penggunaan kecerdasan buatan (AI) untuk keamanan data.

Untuk memenuhi kriteria penyaringan, Pengambil Keputusan Keamanan Data harus:

Pengambil keputusan CISO dan pengambil keputusan yang berdekatan (C-2 ke atas) dengan ruang lingkup keamanan data

Bekerja di organisasi Perusahaan (500+ karyawan; berbagai ukuran)

Perpaduan antara industri yang diatur dan yang tidak diatur (bukan pendidikan, pemerintah, atau nirlaba)

Dari 822 Pengambil Keputusan Keamanan Data yang disurvei untuk penelitian ini, yang melengkapi berdasarkan negara adalah sebagai berikut:

US	329
Inggris	322
Australia	171