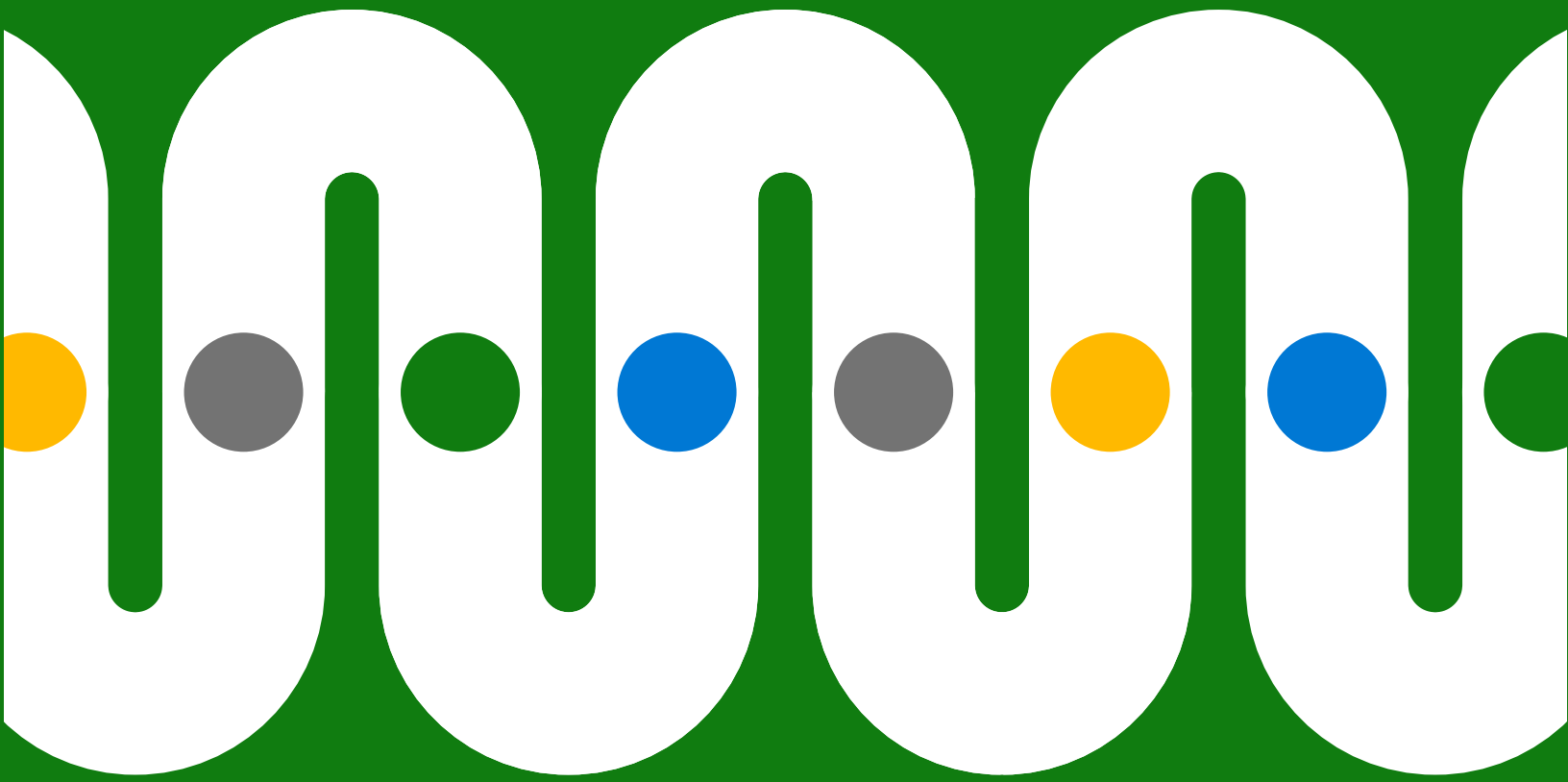
Microsoft Security

3 Langkah Melindungi Data Secara Menyeluruh



Daftar isi

Survei para pengambil keputusan kepatuhan menunjukkan bahwa 95% prihatin dengan tantangan perlindungan data.[2]

Pengantar

Organisasi telah melihat peningkatan besar dalam jejak digital mereka dengan kerja hibrid, meluas jauh melampaui kantor tradisional.

Itu menyebabkan semakin banyak fragmentasi dan eksfiltrasi data — semuanya diperumit dengan pertumbuhan yang cepat di berbagai aplikasi, perangkat, dan lokasi. Banyak pekerja juga telah beralih peran dalam pencarian pemenuhan atau fleksibilitas yang lebih besar, dan itu menambah ditambahkan ke tantangan ini, menciptakan titik buta baru di seluruh kawasan data yang terus berkembang.[1]

Semua faktor ini membuat CIO dan CISO mempertimbangkan kembali pendekatan mereka terhadap perlindungan informasi. Dalam survei pelacakan lebih dari 500 pembuat keputusan kepatuhan AS, hampir semua (95 persen) prihatin dengan tantangan perlindungan data.[2]

[1] "Bagaimana Microsoft dapat membantu mengurangi risiko orang dalam selama Perombakan Besar, Alym Rayani", Microsoft Security. 28 Februari 2022.

[2] "September 2021 survey of 512 US compliance decision-makers ditugaskan oleh Microsoft dari Vital Findings".

Tim TI dan keamanan mencari cara yang lebih baik untuk mengelola seluruh siklus hidup data, di lingkungan multicloud, cloud hibrid, dan lokal. Pendekatan menyeluruh ini melibatkan tiga langkah utama:

Langkah 1: Mengidentifikasi data

Tentukan tempat data, jenis data, dan bagaimana data digunakan atau dibagikan

Langkah 2: Mengklasifikasikan data

Mengklasifikasikan dan melabeli data sehingga Anda tahu kebijakan yang tepat dan mitigasi risiko untuk diterapkan

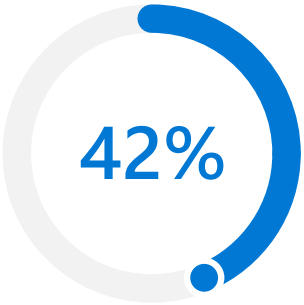
Langkah 3: Mencegah kehilangan data

Menyeimbangkan antara pengurangan risiko dan fleksibilitas untuk karyawan Anda dengan deteksi dan kontrol cerdas

Tujuan dari pendekatan ini? Untuk menutup kesenjangan dan meminimalkan risiko tanpa mengorbankan produktivitas.

Langkah 1

Mengidentifikasi data



Ketika ditanya berapa banyak data mereka yang "gelap," 42% organisasi mengatakan setidaknya setengah.[3]

Data "tersembunyi" ini dapat menggunakan berbagai bentuk — mulai dari lampiran email dan catatan panggilan pelanggan hingga log mesin dan rekaman video.

Jika Anda tidak dapat mengidentifikasi data, tempatnya, jenisnya, dan bagaimana data digunakan atau dibagikan, maka tidak mungkin untuk menerapkan kebijakan atau perlindungan yang tepat padanya.

Organisasi modern terus menghasilkan data dalam jumlah besar. Bukan hanya dokumen, email, dan pesan, tetapi semuanya dari rekaman keamanan hingga data geolokasi, semuanya diperparah dengan proliferasi di seluruh aplikasi, perangkat, dan penyimpanan, di lokasi dan di cloud.

Mengidentifikasi semua data ini bisa jadi sulit, dan 42 persen organisasi mengatakan bahwa setidaknya setengah dari data mereka adalah "gelap."[3] Yaitu, informasi dikumpulkan tetapi tidak diketahui atau tidak digunakan untuk tujuan bisnis. Terkadang data menjadi gelap ketika pekerja yang membuatnya mengalihkan proyek atau peran; sering kali tidak ada sistem untuk mengidentifikasi data pada titik pembuatan atau modifikasi.

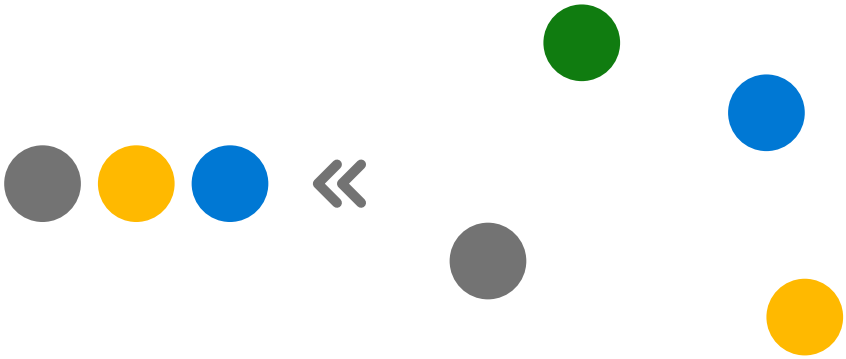
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. Juli 2022.

Ingin membangun alur kerja penemuan menyeluruh di satu platform?

Pelajari tentang penemuan data di Microsoft Purview **Microsoft.com**.

Tantangan ini hanya akan tumbuh. Jumlah data baru yang dibuat, ditangkap, direplikasi, dan dikonsumsi diharapkan lebih dari dua kali lipat pada tahun 2026, dengan data perusahaan berkembang lebih dari dua kali lebih cepat dari data konsumen.[4]

Kecerdasan buatan (AI) dan pembelajaran mesin (ML) dapat membantu, dengan mengenali data sensitif — seperti alamat email, data kesehatan, nomor kartu kredit, atau kekayaan intelektual — dan mengklasifikasikannya secara otomatis. AI dan ML juga dapat meningkatkan akurasi klasifikasi dan meninjau data secara retroaktif. Proses identifikasi ini dapat menjangkau seluruh kawasan data Anda, melestarikan, mengumpulkan, menganalisis, meninjau, dan mengekspor konten di mana pun adanya, di semua cloud.



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. Mei 2022.

Langkah 2

Mengklasifikasikan data

Klasifikasi data yang tepat membantu Anda menentukan kebijakan yang tepat dan mitigasi risiko untuk memastikan berbagai jenis data yang tidak disengaja atau sengaja disalahgunakan atau diakses tanpa otorisasi. Enkripsi dan pemberian cap air dapat melindungi data bahkan lebih jauh, saat diam, dalam transit, dan saat digunakan.

Tetapi klasifikasi dan kebijakan harus mengikuti data saat data bergerak di seluruh organisasi. Kebijakan pelabelan dan perlindungan tidak dapat dibatasi pada dokumen terpisah, tetapi harus mencakup seluruh kawasan digital Anda — dari penyimpanan lokal hingga penyimpanan berbasis cloud, dari perangkat lunak sebagai layanan hingga aplikasi asli OS.

Pendekatan klasifikasi tradisional melibatkan pekerjaan manual yang cukup besar yang menjalankan risiko kesalahan atau secara tidak sengaja mengabaikan data penting. Pengklasifikasi bawaan dan dapat dilatih dapat membantu mengotomatisasi proses ini, dan solusi terintegrasi memungkinkan administrator mengelola kebijakan secara terpusat, di semua sistem.

Klasifikasi dan kebijakan keduanya perlu mengikuti data saat data bergerak.

Misalnya, jika karyawan pemasaran menyalin nomor kartu kredit dari dokumen Microsoft Word ke dalam Excel, klasifikasi dan kebijakan tersebut harus secara otomatis berlaku untuk kedua dokumen tersebut.

Ingin lebih baik dalam mengelola dan melindungi data sensitif di seluruh lingkungan Anda?

Pelajari tentang klasifikasi dan perlindungan data di Microsoft Purview di **Microsoft.com**.

Langkah 3

Mencegah kehilangan data

Setelah mengidentifikasi dan mengklasifikasikan data, solusi pencegahan kehilangan data dapat memberlakukan kebijakan perlindungan menyeluruh yang mengurangi ancaman seperti data gelap dan eksfiltrasi data, sehingga karyawan saat ini dan mantan karyawan tidak — secara sengaja atau tidak sengaja — berbagi, mengekspos, atau mentransfer data sensitif tanpa otorisasi.

Solusi pencegahan kehilangan data cerdas menggunakan konteks untuk menemukan keseimbangan antara menyediakan fleksibilitas dan memblokir tindakan berisiko tinggi. Misalnya, individu mungkin dapat melanjutkan tindakan setelah diingatkan tentang potensi risiko dan kebijakan yang berlaku. Ini dapat membantu melindungi data sensitif sementara juga melatih pengguna untuk lebih memahami risiko.

Solusi pencegahan kehilangan data membantu melindungi kekayaan intelektual dan data bisnis penting lainnya, sekaligus juga meningkatkan kepatuhan pada peraturan seperti GDPR (General Data Protection Regulation), HIPAA (Health Information Portability and Accountability Act), dan CCPA (California Consumer Privacy Act).

Pendekatan yang komprehensif terhadap pencegahan kehilangan data memberlakukan kebijakan di seluruh organisasi Anda secara konsisten, melindungi titik "tautan yang paling lemah" dalam siklus hidup data.

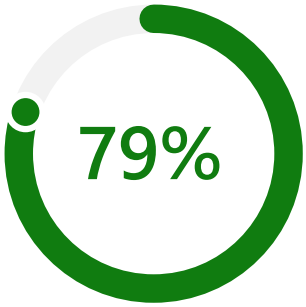
Kebijakan pencegahan kehilangan data dapat mencegah tindakan di luar kepatuhan.

Misalnya, jika seorang karyawan mencoba mengunduh spreadsheet dengan nomor kartu kredit ke flash drive atau mengunggahnya ke penyimpanan cloud, kebijakan pencegahan kehilangan data dapat mengidentifikasi aktivitas yang tidak mematuhi dan mencegahnya.

Ingin deteksi cerdas dan kontrol informasi sensitif?

Pelajari tentang pencegahan kehilangan data di Microsoft Purview di **Microsoft.com**.

Jangan pasang alat perlindungan data. Bangun perlindungan data.



Survei pengambil keputusan kepatuhan menunjukkan bahwa 79% telah membeli beberapa produk kepatuhan dan perlindungan data.

Mayoritas telah membeli tiga atau lebih.[5]

Banyak organisasi telah mencoba pendekatan "bolt-on" untuk perlindungan informasi, menggunakan beberapa solusi untuk mengelola bagian terpisah dari siklus hidup data. Namun hal ini memaksa tim keamanan, tata kelola data, kepatuhan, dan hukum Anda untuk menyatukan kerja tambal sulam yang sering kali tidak efektif dan menghabiskan sumber daya.

Pendekatan "bawaan" dapat menutup kesenjangan, menyatukan identifikasi data, klasifikasi data, dan pencegahan kehilangan data. Dengan solusi terintegrasi, lebih mudah untuk mengelola dan memberlakukan kebijakan secara terpusat. Juga mengurangi waktu pelatihan untuk pengguna, yang menerima pemberitahuan kebijakan dengan cara yang familier, secara bawaan dalam aplikasi.

[5] "February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) ditugaskan oleh Microsoft dengan MDC Research."

Solusi bawaan dan terintegrasi: Microsoft Purview

Microsoft Purview membantu Anda menghadapi tantangan tempat kerja yang terdesentralisasi dan kaya data saat ini, dengan seperangkat solusi komprehensif yang membantu Anda mengatur, melindungi, dan mengelola seluruh kawasan data Anda.

Melampaui tata kelola.

Pelajari lebih lanjut tentang melindungi data dengan Microsoft Purview >

Tertarik dengan area tertentu dari perlindungan data? Dapatkan informasi lebih detail tentang bagaimana Microsoft Purview dapat membantu Anda dengan:

Penemuan data >

Perlindungan dan klasifikasi data >

Pencegahan kehilangan data >

Microsoft Security