Microsoft 365

Dari Pengawasan ke Wawasan: Mengelola Risiko AI Bayangan

Daftar Isi

Pengantar

Dalam laporan Indeks Tren Kerja baru-baru ini, lebih dari 80% pekerja informasi yang disurvei di 31 negara—termasuk karyawan dan pemimpin—melaporkan merasa kekurangan waktu atau energi untuk melakukan pekerjaan mereka. Selain itu, lebih dari 50% pemimpin bisnis yang disurvei menyatakan bahwa produktivitas perlu meningkat untuk mencapai target[1]. Menurut Laporan Indeks Tren Kerja Microsoft 2024, banyak karyawan mencari alat AI generatif untuk menjembatani kesenjangan tersebut dan tidak menunggu persetujuan TI resmi sebelum mulai menggunakan alat tersebut.

Ketika alat beroperasi di luar pengawasan TI, alat tersebut dapat menimbulkan risiko terhadap keamanan dan kepatuhan organisasi. Dan AI Bayangan – penggunaan alat AI tanpa persetujuan TI – muncul sebagai bentuk terbaru dari TI Bayangan di tempat kerja saat ini.

Seiring dengan semakin cepatnya adopsi AI, para pemimpin bisnis berupaya agar tetap selangkah lebih maju dan meminimalkan potensi risiko yang mungkin ditimbulkan oleh alat tersebut. Dalam studi iSMG baru-baru ini, lebih dari 70% pemimpin bisnis yang disurvei melaporkan bahwa memastikan privasi dan keamanan data menjadi tantangan terbesar dalam mengintegrasikan AI generatif dengan infrastruktur TI yang sudah ada[2]. Selain itu, lebih dari 90% CIO dan CTO yang disurvei menyatakan bahwa AI Generatif telah mendorong atau akan mendorong peningkatan investasi keamanan cyber di organisasi mereka[3].

Dalam buku elektronik ini, jelajahi skenario umum di mana AI bayangan digunakan, pahami potensi risiko bagi organisasi, dapatkan lima cara untuk mengelola risiko tersebut, dan lihat bagaimana Microsoft 365 E3 dapat membantu.

[1] **Laporan Tahunan Indeks Tren Kerja 2025,** Microsoft, Inc., April 2025. Microsoft menganalisis data survei dari 31.000 pekerja informasi, baik pekerja penuh waktu maupun pekerja lepas, di 31 negara selama periode 6 Februari 2025 hingga 24 Maret 2025, tren pasar tenaga kerja LinkedIn, serta triliunan sinyal produktivitas Microsoft 365.

[2] **Studi AI Generatif Tahunan Kedua iSMG: Business Rewards vs. Security Risks,** Berdasarkan hasil survei terhadap lebih dari 360 profesional bisnis dan keamanan cyber pada kuartal ketiga di 6 wilayah (Amerika Utara, Eropa, Asia, Amerika Selatan, Australia, dan Afrika)

[3] **Tantangan Menyeimbangkan Keamanan AI: Dari Risiko ke Inovasi," NTT DATA, Juni 2025,** Berdasarkan hasil survei NTT DATA terhadap lebih dari 2.300 pembuat keputusan senior GenAI, termasuk 1.500 pemimpin C-Suite di 34 negara.

Apa itu AI Bayangan? Mengapa Visibilitas Penting?

AI Bayangan merujuk pada penggunaan alat dan aplikasi kecerdasan buatan oleh karyawan tanpa persetujuan atau pengawasan eksplisit dari departemen TI, sering kali di luar jangkauan kerangka kerja keamanan dan kepatuhan resmi. Ketika karyawan mencari cara untuk meningkatkan produktivitas dan memenuhi tuntutan pekerjaan yang semakin besar, mereka mungkin beralih ke solusi tanpa izin untuk memperlancar tugas, berkolaborasi, atau menghasilkan konten baru—sering kali tanpa menyadari potensi risiko di dalamnya. AI Bayangan tidak terpantau oleh TI, sehingga organisasi kesulitan mengetahui aplikasi apa saja yang digunakan dan mana yang paling berisiko.

Mengapa Visibilitas AI Bayangan Penting

Ketika TI tidak mengetahui suatu aplikasi atau layanan, aplikasi atau layanan tersebut tidak aman atau tidak dapat didukung. *Kesenjangan visibilitas* ini menyulitkan organisasi dalam mengidentifikasi, mengelola, atau memitigasi secara akurat ancaman potensial terkait dengan paparan data sensitif, ketidakpatuhan terhadap regulasi, dan hilangnya kontrol atas informasi milik perusahaan. Pemimpin TI dan bisnis perlu memperoleh visibilitas atas penggunaan AI Bayangan di organisasi mereka, menangani risiko baru yang terkait dengan penggunaan AI, dan memutuskan alat mana yang boleh digunakan dengan batasan yang tepat. Peluang bagi organisasi adalah mengubah AI Bayangan dari risiko menjadi kesempatan untuk berinovasi dalam menyelesaikan pekerjaan secara aman. Untuk melakukan hal ini, diperlukan keseimbangan yang lebih baik—memungkinkan karyawan menggunakan alat AI yang berguna dalam kerangka kerja yang aman dan terkendali untuk mengurangi potensi risiko.

WAWASAN

Anda tidak dapat mengamankan apa yang tidak dapat Anda lihat. Ketika TI tidak mengetahui aplikasi atau layanan yang digunakan, TI tidak dapat mengamankannya. Ini yang menjadi inti dari masalah AI Bayangan – dan hal ini menyoroti mengapa pendekatan baru diperlukan. Hanya melarang semua alat dari luar tidak praktis jika karyawan merasa alat AI ini penting untuk mencapai tujuan mereka. Sebaliknya, organisasi perlu menghadirkan AI Bayangan ke permukaan—untuk mengetahui alat apa saja yang digunakan karyawan, menetapkan kontrol yang sesuai, dan menawarkan alternatif yang aman serta telah disetujui dan memenuhi kebutuhan organisasi. Secara singkat, tantangannya adalah memberdayakan tim dengan AI *tanpa* mengorbankan keamanan.

AI Bayangan di Tempat Kerja: Contoh Skenario dan Potensi Risiko

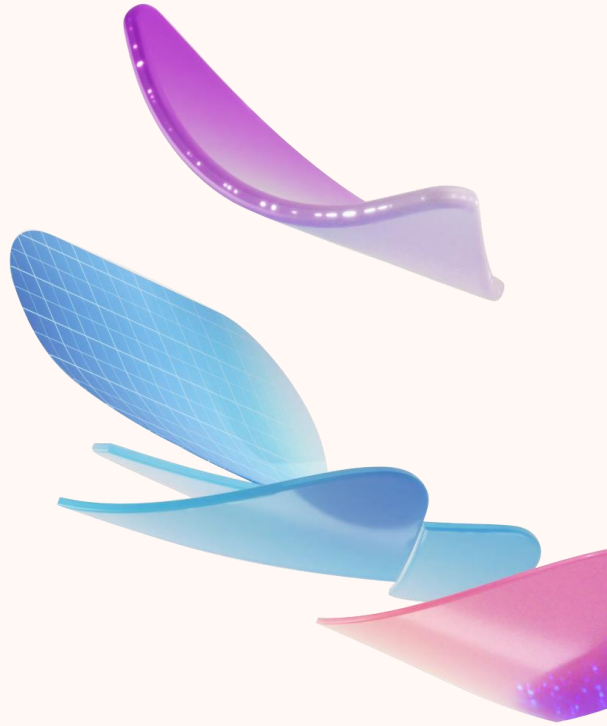
AI Bayangan muncul dari karyawan yang mungkin ingin meningkatkan produktivitas dan dampak atau mencoba teknologi baru. Berikut adalah beberapa contoh fiksi untuk menggambarkan bagaimana alat AI yang tidak berizin mungkin digunakan dan potensi risiko yang dapat ditimbulkan:

Peran	Contoh Skenario	Risiko Potensial dari Alat Tidak Berizin
Pemasaran	Menggunakan alat konten AI generatif untuk membuat materi pemasaran atau desain dengan menggunakan data merek perusahaan.	Kebocoran informasi merek atau produk yang sensitif; kehilangan kendali atas bagaimana layanan AI eksternal dapat menyimpan atau menggunakan aset kreatif perusahaan.
Keuangan	Mengunggah keuangan perusahaan ke layanan analitik berbasis AI atau visualisasi untuk wawasan cepat.	Paparan data keuangan rahasia (anggaran, proyeksi) kepada pihak ketiga; potensi pelanggaran kepatuhan (misalnya, GDPR) jika data pelanggan atau karyawan disertakan tanpa perlindungan yang memadai.
Dukungan Pelanggan	Membagikan data klien atau transkrip percakapan dukungan ke aplikasi AI untuk membantu membuat respons atau merangkum kasus.	Pelanggaran terhadap peraturan privasi dan penanganan data – informasi pelanggan yang sensitif dapat disimpan di luar sistem perusahaan; tidak ada jaminan retensi data atau penghapusan yang tepat oleh penyedia AI.
Garis Depan – Retail	Manajer toko menggunakan aplikasi penjadwalan berbasis AI di ponsel mereka untuk mengoptimalkan jadwal shift karyawan.	Data tenaga kerja perusahaan (nama karyawan, jadwal) diunggah ke aplikasi tidak berizin, berisiko menimbulkan masalah privasi. Jadwal yang saling bertentangan atau pelanggaran kebijakan dapat terjadi jika rekomendasi AI tidak selaras dengan peraturan ketenagakerjaan.
Garis Depan – Layanan Kesehatan	Perawat atau dokter menggunakan chatbot AI untuk membantu menyusun catatan perawatan pasien atau menjawab pertanyaan medis.	Informasi kesehatan pasien (PHI) dapat terekspos ke layanan eksternal tanpa perlindungan apa pun, sehingga melanggar persyaratan kepatuhan dan kerahasiaan. Saran medis AI mungkin juga tidak diverifikasi, sehingga menimbulkan risiko keselamatan.

Dalam setiap kasus di atas, karyawan individu memiliki niat baik dan ingin meningkatkan produktivitas, tetapi organisasi dapat menanggung risiko sebagai konsekuensinya.

Informasi perusahaan dapat tersebar di berbagai platform yang tidak berizin, menciptakan *tantangan tata kelola data*. Aplikasi yang tidak diperiksa dapat membawa malware atau kerentanan keamanan, memperluas permukaan serangan di luar lingkup TI. Mungkin juga ada implikasi kepatuhan. Dari perspektif dukungan TI, jika terjadi masalah dengan alat AI Bayangan, pusat bantuan mungkin tidak dapat membantu pengguna akhir karena mereka tidak memiliki akses atau kendali atasnya.

Lima Cara Mengelola Risiko AI Bayangan



Dengan strategi dan alat yang tepat, Anda dapat mengubah AI bayangan dari potensi ancaman menjadi peluang untuk mendorong budaya inovasi yang aman. Berdayakan tim Anda dengan alat produktivitas AI *sekaligus* mempertahankan pengawasan yang diperlukan untuk melindungi bisnis Anda. Ini adalah perubahan dari mengatakan "tidak, sama sekali tidak" menjadi "ya – tetapi dengan kendali pengaman yang tepat." Lima tips berikut dirancang untuk membantu Anda mengelola dan mengendalikan AI Bayangan di organisasi Anda:

01 Menemukan jejak AI Bayangan untuk mengevaluasi dan memprioritaskan risiko

Anda tidak dapat melindungi apa yang tidak dapat Anda lihat. Dapatkan visibilitas tentang aplikasi yang digunakan di organisasi Anda melalui log aktivitas Anda. Setelah mengetahui aplikasi yang digunakan, Anda dapat menentukan solusi terbaik untuk menangani data sensitif, sambil mencatat aplikasi yang tidak sesuai dengan kebijakan keamanan dan kebijakan kepatuhan Anda. Dengan wawasan ini, Anda dapat mengambil keputusan menurut informasi mengenai aplikasi mana yang akan diizinkan, dipantau, atau dibatasi untuk meminimalkan risiko yang mungkin terjadi.

02 Menerapkan keuntungan cepat dengan kebijakan keamanan dan kepatuhan

Aktifkan atau terapkan penyesuaian kebijakan untuk lebih memitigasi potensi risiko dari penggunaan AI Bayangan. Anda dapat menggunakan kebijakan akses bersyarat untuk membatasi penggunaan aplikasi berisiko tinggi, menggunakan kebijakan pencegahan kehilangan data untuk informasi sensitif guna mengurangi oversharing dan kebocoran data, serta menerapkan autentikasi multifaktor dasar dan kepatuhan perangkat untuk semua pengguna. Langkah-langkah ini dengan cepat mengurangi risiko yang paling mencolok bahkan jika Anda belum memiliki visibilitas penuh terhadap aplikasi AI yang sedang digunakan.

03 Mengedukasi karyawan tentang potensi risiko AI Bayangan

Sering kali, karyawan tidak menyadari risiko penggunaan alat AI yang tidak mendapat persetujuan TI bagi organisasi mereka. Informasikan risiko AI Bayangan secara berkala dengan memberi peringatan pencegahan kehilangan data yang strategis, pengingat kebijakan perusahaan, dan pelatihan singkat untuk membantu mengarahkan pengguna ke praktik yang lebih aman tanpa penegakan yang terlalu keras.

04 Menyediakan perangkat AI yang disetujui untuk memitigasi risiko lebih lanjut

Jika memungkinkan, tawarkan kepada karyawan alat AI yang disetujui sebagai alternatif dari alat AI yang tidak disetujui. Cara yang efektif untuk mengurangi AI Bayangan adalah dengan memenuhi kasus penggunaan yang paling umum di organisasi Anda menggunakan solusi resmi. Dengan demikian, TI dapat mempertahankan visibilitas dan kontrol, sekaligus memberikan dukungan kepada pengguna saat menghadapi masalah.

05 Menetapkan tata kelola yang berkelanjutan

Integrasikan pemeriksaan ke dalam rutinitas tata kelola TI Anda – tinjau log dan laporan aktivitas secara teratur, perbarui kebijakan saat layanan AI baru muncul, dan informasikan kepada pimpinan tentang kemajuan (seperti pengurangan penggunaan aplikasi tidak berizin atau insiden yang berhasil dicegah). Ini akan membantu Anda mengurangi potensi risiko sekarang dan di masa depan seiring perkembangan lanskap.

Dengan mengikuti langkah-langkah di atas, Anda dapat memberdayakan inovasi maupun keamanan.

Karyawan dapat menggunakan solusi AI yang disetujui di tempat kerja, dan TI menjaga kontrol serta kepatuhan terhadap alat-alat tersebut.

Menemukan dan Mengelola Risiko AI Bayangan dengan Microsoft 365 E3

Microsoft 365 E3 menyediakan organisasi dengan kemampuan untuk menemukan TI Bayangan, menilai potensi risiko, dan menerapkan kebijakan keamanan serta kebijakan kepatuhan *tanpa* menghambat inovasi. Rangkaian kemampuan produktivitas, keamanan, dan manajemen terintegrasi ini dapat memberdayakan Anda untuk mengatasi tantangan AI Bayangan secara langsung.

Solusi Microsoft 365 E3	Bagaimana ini membantu Anda mengelola potensi risiko AI Bayangan
Penemuan Aplikasi Cloud	**Temukan dan tindaklanjuti aplikasi tidak berizin.** Penemuan Aplikasi Cloud memungkinkan Anda mengunggah log aktivitas dan membuat laporan snapshot untuk memperoleh gambaran tentang lebih dari 31.000 aplikasi cloud—termasuk lebih dari 400 aplikasi AI generatif. Ini memungkinkan Anda mengetahui apa yang sedang digunakan dalam organisasi Anda, oleh siapa, dan seberapa sering. Informasi ini memungkinkan Anda membuat keputusan menurut informasi tentang aplikasi mana yang diizinkan atau dibatasi penggunaannya.
Pencegahan Kehilangan Data Microsoft Purview (DLP)	**Kurangi kebocoran data sensitif.** Microsoft Purview DLP memungkinkan Anda menentukan dan menerapkan kebijakan yang mendeteksi informasi sensitif serta memblokir atau membatasi berbagi di seluruh layanan Microsoft 365 untuk email dan file. Misalnya, Anda dapat menentukan aturan untuk memantau, mengaudit, atau menghentikan pengguna yang membagikan informasi sensitif melalui email atau berbagi file, serta memberi peringatan kepada pengguna.
Microsoft Entra ID P1	**Kelola akses ke aplikasi-aplikasi cloud.** Microsoft Entra ID P1 memungkinkan kebijakan akses bersyarat untuk mengontrol siapa yang dapat mengakses aplikasi mana dalam kondisi apa. Misalnya, Anda dapat memilih untuk mewajibkan autentikasi multifaktor atau bahkan membatasi login dengan kredensial perusahaan ke aplikasi yang telah Anda kategorikan sebagai berisiko lebih tinggi. Microsoft Entra ID P1 menyediakan akses ke sumber daya cloud untuk orang yang tepat, pada perangkat yang sesuai, dalam kondisi yang disetujui—sekaligus membatasi akses ke aplikasi yang tidak disetujui.
Microsoft Intune P1	**Terapkan kebijakan penggunaan perangkat dan aplikasi.** Microsoft Intune P1 memberi Anda kemampuan untuk mengizinkan perangkat terkelola dan patuh untuk digunakan dalam pekerjaan, serta menyediakan alat untuk mengelola perangkat tersebut. Misalnya, solusi ini dapat melarang penginstalan perangkat lunak yang tidak disetujui pada PC perusahaan, atau menerapkan konfigurasi yang membatasi akses ke situs web atau layanan tertentu.
Microsoft Defender untuk Titik Akhir P1	**Batasi lalu lintas ke URL yang tidak disetujui.** Microsoft Defender untuk Titik Akhir P1 membantu Anda mengurangi risiko dari situs yang dianggap berisiko dengan memblokir lalu lintas ke URL yang tidak disetujui dari perangkat terkelola. Misalnya, karyawan yang mencoba mengunjungi situs AI yang sudah diketahui berisiko di laptop perusahaan akan diblokir untuk mengaksesnya.

Mengambil langkah selanjutnya dalam perjalanan adopsi AI Anda →

Semuanya dimulai dengan kesadaran, alat yang tepat, dan rencana proaktif. Microsoft 365 E3 menyediakan alat untuk memungkinkan organisasi Anda membangun fondasi keamanan dan kerangka kerja tata kelola yang kuat untuk solusi AI. Anda akan dapat memperoleh visibilitas terhadap alat yang tidak disetujui, menerapkan kebijakan untuk melindungi data sensitif, dan menjaga kontrol atas akses pengguna serta keamanan perangkat. Bersiaplah untuk beralih dari sikap reaktif (menemukan dan memblokir Shadow AI setelah muncul) ke pendekatan yang lebih proaktif dengan membimbing penggunaan AI ke saluran yang aman dan telah dikelola. Ikuti Penilaian Keamanan untuk AI dan pelajari bagaimana Anda dapat meningkatkan postur keamanan Anda untuk AI. Pelajari lebih lanjut tentang kemampuan yang tercakup dalam Microsoft 365 untuk Perusahaan.