Microsoft 365

Panduan Eksekutif Membangun Kesiapan AI

Model operasional bersama untuk CIO dan CISO untuk membantu beralih dari ambisi AI menuju kesiapan organisasi.





03
Cara menggunakan panduan ini

04
Ringkasan Eksekutif: Ambisi AI bisa jadi melampaui kesiapan organisasi

05
Kesenjangan kesiapan: Nilai faktor-faktor yang mungkin memperlambat adopsi AI

06
Kerangka kerja fondasi siap AI yang aman

09
Tiga pergeseran yang dapat membantu membangun kesiapan AI

10
Langkah berikutnya sesuai peran

11
Mulai membangun kesiapan AI Anda

Cara menggunakan panduan ini

Panduan ini memberi CIO dan CISO kerangka kerja bersama untuk membangun fondasi yang dapat membantu organisasi mereka mengungkap kesiapan AI dan memberdayakan transformasi bisnis. Kerangka kerja ini dapat membantu menentukan area di organisasi Anda yang mungkin terdapat kesenjangan, kemudian menentukan langkah-langkah Anda untuk mengatasinya. Kerangka kerja ini disusun dalam satu ide: transformasi frontier dimulai dengan fondasi aman yang membantu menyatukan produktivitas, keamanan, data, dan manajemen. Gunakan informasi dalam panduan ini sebagai pedoman untuk:

1. **Menyelaraskan.** Diskusikan dan sepakati area kesenjangan kesiapan apa saja yang memperlambat nilai AI.
2. **Menilai.** Gunakan lima langkah dalam kerangka kerja fondasi siap AI yang aman untuk menentukan dampak dan area berisiko tertinggi di organisasi Anda sebagai titik awal.
3. **Bertindak.** Bangun rencana bersama untuk menentukan area untuk memulai dan cara melakukan penskalaan seiring waktu.

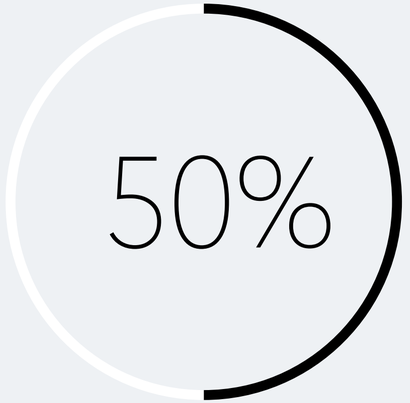


Ambisi AI bisa jadi melampaui kesiapan organisasi.

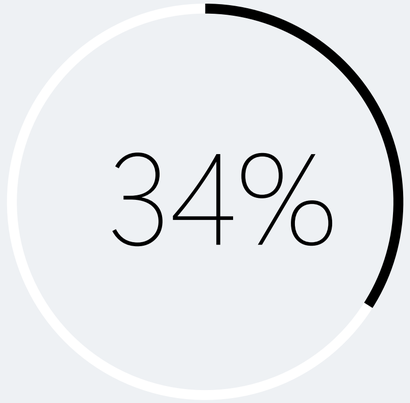
AI sudah tersebar luas. Menurut Laporan Perkembangan AI di Perusahaan, Deloitte tahun 2026, mereka yang disurvei mengatakan bahwa organisasi mereka telah memperluas akses pekerja mereka ke AI sebesar **50%** dalam hanya satu tahun[1] dan **34%** melaporkan bahwa perusahaan mereka mulai menggunakan AI untuk mentransformasi produk, proses, dan model bisnis mereka secara mendalam[1]. Ambisi tinggi ini muncul karena karyawan sudah mulai mengonsepkan kembali cara mereka menyelesaikan pekerjaan dengan AI. Mereka sedang bereksperimen, menciptakan alur kerja baru, dan mungkin bergerak lebih cepat daripada yang dapat diantisipasi oleh organisasi mereka. Pada saat yang sama, sistem, kebijakan, dan model operasional di sekitarnya sering kali terus memperkuat cara kerja sebelumnya.

Indeks Tren Kerja Microsoft 2026 menyebut hal ini sebagai Paradoks Transformasi[2] dengan karyawan siap dan mulai menemukan kembali cara mereka bekerja, tetapi sistem organisasi di sekitar mereka—metrik, insentif, dan norma-norma—terus memperkuat cara bekerja yang sebelumnya. Kekuatan yang sama yang mempercepat adopsi AI bisa menjadi penghambatnya. Kesenjangan ini bukan hanya tentang adopsi teknologi. Hal ini juga dapat diperkuat dengan kesiapan organisasi Anda untuk AI dalam skala besar di beberapa bagian yang sangat spesifik: di berbagai alat, data, identitas, titik akhir, dan kontrol Anda—pada dasarnya merupakan fondasi Anda.

Ketika organisasi Anda beroperasi dari fondasi yang terhubung dan aman, Anda akan mendapatkan kepercayaan diri untuk mengembangkan AI dalam skala besar. Landasan AI yang kokoh ini lebih dari sekadar infrastruktur—melainkan merupakan model operasional. Dengan menghubungkan orang, konten, komunikasi, alur kerja, identitas, dan perangkat pada platform terpadu, organisasi juga dapat menyematkan keamanan, kepatuhan, dan manajemen ke dalam alur kerja. Hal ini membantu menciptakan kepercayaan dan kendali untuk mentransformasi alur kerja dan membangun dampak bisnis. Kesempatan ini bukan hanya untuk mengikuti perkembangan AI, tetapi juga untuk mengonsepkan kembali cara menyelesaikan pekerjaan. Ini bukan tentang seberapa cepat organisasi Anda mengadopsi dan meningkatkan skala pengalaman AI, tetapi bagaimana Anda dapat membantu mewujudkan transformasi secara aman.



Akses pekerja yang lebih luas ke AI dalam satu tahun dilaporkan oleh para pemimpin bisnis yang disurvei.[1]



dari para pemimpin yang disurvei melaporkan penggunaan AI untuk mentransformasi produk, proses, dan model bisnis.[1]

Kesenjangan kesiapan: Nilai faktor-faktor yang mungkin memperlambat adopsi AI

Para karyawan mengadopsi AI untuk bekerja dengan cara baru, tim menemukan kasus penggunaan baru, dan uji coba awal menunjukkan potensi peningkatan produktivitas. Di berbagai perusahaan, para pemimpin melihat potensi untuk transformasi yang lebih luas dan berskala lebih besar. Tantangannya bukanlah pada kurangnya antusiasme pada AI. Tantangannya adalah bahwa fondasi operasional tidak selalu berkembang dengan kecepatan yang sama dengan perubahan cara kerja karyawan.

Dalam laporan Indeks Tren Kerja 2026, **lebih dari 60%** pengguna AI yang disurvei[2] mengatakan bahwa AI telah memungkinkan mereka menghabiskan lebih banyak waktu untuk pekerjaan bernilai tinggi dan **lebih dari 50%** mengatakan mereka menyelesaikan pekerjaan yang tidak dapat mereka lakukan setahun yang lalu[2]. Namun, pada saat yang sama, **satu dari empat** pengguna AI yang sama ini[2] mengatakan bahwa mereka merasa kepemimpinan mereka secara konsisten selaras dengan pendekatan mereka terhadap AI.

Seiring karyawan mengadopsi cara kerja yang berbasis AI, proses lama, alat yang terfragmentasi, kontrol yang tidak konsisten, dan data yang tidak terkelola dapat memperlambat kemajuan. Momentum yang mendorong adopsi AI dapat mengungkap sistem yang dibangun untuk era yang berbeda. Inilah kesenjangan kesiapan – dan sering kali itu semua menjadi tantangan yang mendasar.

Ada dua area utama yang dapat berkontribusi pada tantangan mendasar ini: pengalaman yang terputus dan kekhawatiran pada keamanan.

- **2/3 Eksekutif senior yang disurvei** mengatakan bahwa organisasi mereka sangat kompleks dan tidak efisien.[3]
- **Lebih dari 90% CIO dan CTO yang disurvei** mengatakan AI generatif sudah mendorong atau akan mendorong investasi keamanan siber yang lebih besar.[4]

Mari jelajahi beberapa skenario ilustratif untuk mempertimbangkan letak kesenjangan kesiapan yang dapat muncul di seluruh pengalaman karyawan dan keamanan. Skenario pertama berkaitan dengan pengalaman karyawan. CIO dapat mulai mengenali adanya lebih banyak laporan frustrasi karyawan terkait dengan waktu yang mereka perlukan untuk menemukan informasi atau mengakses semua aplikasi atau alat yang mereka butuhkan untuk menyelesaikan pekerjaan. Masalah-masalah ini dapat mengindikasikan adanya kesenjangan kesiapan akibat pengalaman yang terputus di berbagai aplikasi, alur kerja, perangkat, dan data yang mungkin menjadi masalah yang lebih besar seiring dengan peningkatan skala AI.

Skenario kedua berkaitan dengan sisi keamanan. Seiring semakin banyak orang mulai bereksperimen dan menggunakan AI dalam alur kerja sehari-hari mereka, CISO mungkin akan melihat potensi peningkatan insiden terkait berbagi informasi yang berlebihan atau peningkatan penggunaan alat AI yang tidak sah. Isu-isu ini dapat menyoroti kesenjangan kesiapan terkait tata kelola data dan manajemen akses.

Bersama-sama, kesenjangan ini dapat menciptakan gesekan yang dapat membuat penerapan AI dalam skala perusahaan menjadi lebih sulit dicapai. Apa yang awalnya merupakan tantangan terpisah antara produktifitas, keamanan, dan TI dapat berkembang menjadi tantangan dasar bersama. Seiring meningkatnya adopsi AI, kesenjangan dalam kesiapan ini dapat menjadi lebih terlihat dan lebih berdampak.

Meskipun ini merupakan contoh hipotetis tentang bagaimana kesenjangan kesiapan dapat muncul, contoh-contoh ini menggambarkan bagaimana biaya peluang bukan hanya tertinggal dalam adopsi AI. Ini menciptakan kesenjangan yang semakin meluas antara apa yang dapat dicapai karyawan Anda dengan AI dan apa yang dipersiapkan organisasi Anda untuk pengembangan. Karyawan mungkin siap untuk melakukan inovasi dalam pekerjaan mereka; pertanyaannya adalah apakah fondasi Anda siap untuk mendukung perubahan tersebut.

Itulah mengapa penskalaan AI juga tentang menyelaraskan bisnis, TI, dan keamanan di seputar model operasi bersama. Organisasi yang dapat menangkap potensi AI, tidak hanya sekadar menerapkan lebih banyak AI. Mereka memperkuat fondasi mereka untuk memungkinkan produktivitas, keamanan, dan manajemen untuk bekerja bersama, dalam skala besar.

Pemeriksaan Kesiapan

Sebelum mengembangkan AI lebih lanjut, mulailah dengan dua pertanyaan:

- Di bagian apa di organisasi Anda yang menurut Anda adopsi AI dapat berjalan lebih cepat dari kebijakan yang terkait dengan penggunaan dan akses AI?
- Dapatkah AI secara aman mengakses konteks organisasi secara memadai untuk menyempurnakan proses kerja secara signifikan?

Untuk para CIO, pertimbangkan berikut ini:

- Apakah kami memiliki fondasi operasional untuk menskalakan AI ke seluruh organisasi?

Untuk para CISO, pertimbangkan berikut ini:

- Apakah kami memiliki landasan kendali yang memadai untuk menskalakan AI dengan keyakinan?

Kerangka kerja fondasi siap AI yang aman

Apa yang dibutuhkan untuk membangun fondasi yang aman dan siap AI? Satu kerangka kerja dapat membantu Anda mengelola pendekatan untuk mulai membangun fondasi dengan lima langkah yang dirancang untuk bekerja bersama.

Di setiap area: pekerjaan yang terhubung, kesiapan data, akses yang aman, pengelolaan dalam skala besar, serta perlindungan dan respons - dapat membantu untuk mengidentifikasi area yang berpotensi sebagai area paling kritikal untuk organisasi Anda memulai, dan kemudian membangun, mengonsolidasi, mentransformasi, dan mengembangkan seiring waktu.



1.

Pekerjaan yang Terhubung

Buat grafik kerja yang terhubung antarpersonel, konten, percakapan, dan proses bisnis sehingga AI dapat memiliki konteks organisasi berdasarkan bagaimana pekerjaan berlangsung di organisasi Anda. Ketika alat-alat terhubung, karyawan dapat beralih dari kasus penggunaan AI yang terisolasi ke alur kerja yang didukung AI yang mencakup rapat, dokumen, aplikasi bisnis, dan alat kolaborasi.

Dari mana memulai
Identifikasi alat produktivitas, sistem kolaborasi, dan data yang bernilai tinggi untuk memprioritaskan koneksi dengan alat yang paling sering digunakan karyawan.

Dampak potensial
Karyawan mungkin menghabiskan lebih sedikit waktu untuk mencari[1] informasi, beralih antaraplikasi, dan menciptakan kembali konteks, sementara AI memberikan wawasan, rekomendasi, dan tindakan yang didasarkan pada cara kerja organisasi yang sebenarnya.

Pemeriksaan Kesiapan

Untuk para CIO, pertimbangkan berikut ini:
- Bisakah AI mengakses orang, konten, percakapan, dan alur kerja yang dibutuhkan karyawan untuk bekerja lebih efektif?

Untuk para CISO, pertimbangkan berikut ini:
- Bisakah AI mengakses konteks organisasi tanpa menciptakan kesenjangan visibilitas, tata kelola, atau keamanan baru?

2.

Kesiapan Data

Temukan, klasifikasikan, beri label, lindungi, dan kelola data bernilai tinggi sehingga AI beroperasi dengan kesadaran — dan kepekaan tercermin dalam apa yang dihasilkannya dengan menghormati keamanan, kepatuhan, dan kebijakan bisnis. Ketika data dikelola, dapat dicari, dan terhubung, AI dapat mendasarkan respons pada pengetahuan organisasi, bukan pada informasi yang tidak lengkap atau sudah usang.

Dari mana memulai
Jangan menunggu strategi pelabelan yang lengkap. Prioritaskan pencegahan bocornya informasi Anda yang paling sensitif seperti data keuangan, pelanggan, dan kekayaan intelektual terlebih dahulu dengan kebijakan Pencegahan Kehilangan Data (Data Loss Prevention/DLP). Pada saat yang sama, identifikasi dan lakukan pelabelan otomatis pada data Anda yang paling sensitif yang menciptakan nilai bisnis dan risiko terbesar. Setelah itu, kembangkan program klasifikasi dan tata kelola data yang lebih luas di seluruh organisasi Anda.

Dampak potensial
Karyawan dan agen dapat bekerja dengan informasi sensitif yang tepercaya, sementara para pemimpin tetap memiliki visibilitas, kendali, dan keyakinan bahwa data digunakan dan dilindungi dalam alur kerja yang didukung AI. Kebijakan tetap ini melekat pada data sensitif saat data tersebut berpindah di seluruh organisasi Anda dan saat disimpan, dibagikan, atau diakses.

Pemeriksaan Kesiapan

Untuk para CIO, pertimbangkan berikut ini:
- Apakah data kita yang paling berharga dapat ditemukan, diatur, dan digunakan oleh agen dan alat AI?

Untuk para CISO, pertimbangkan berikut ini:
- Bisakah AI membedakan informasi sensitif dari informasi lainnya dan menerapkan perlindungan yang sesuai?

3.

Akses Aman

Bangun lapisan kepercayaan yang membantu Anda memverifikasi pengguna, perangkat, dan permintaan akses sehingga personel dan AI dapat mengambil serta bertindak berdasarkan informasi organisasi secara aman tanpa meningkatkan risiko. Ketika identitas, akses, dan izin diselaraskan, karyawan dan agen AI dapat mengakses informasi yang dibutuhkan untuk menyelesaikan pekerjaan dengan aman sehingga organisasi dapat memperluas adopsi AI di seluruh tim, peran, dan proses bisnis.

Dari mana memulai
Mulai dengan memperkuat kebijakan Autentikasi Multifaktor (MFA) dan Akses Bersyarat untuk semua pengguna. Kontrol ini membantu memberikan perlindungan sekaligus menciptakan fondasi untuk akses yang aman ke alat AI yang telah disetujui.

Dampak potensial
Karyawan dan agen memperoleh akses aman ke informasi dan pengalaman yang didukung AI, sementara tim keamanan mempertahankan kontrol atas bagaimana data dan sistem sensitif diakses di berbagai identitas, perangkat, dan agen.

Pemeriksaan Kesiapan

Untuk para CIO, pertimbangkan berikut ini:
- Dapatkah karyawan mengakses informasi dan alat AI yang mereka butuhkan dengan aman tanpa hambatan yang tidak perlu?

Untuk para CISO, pertimbangkan berikut ini:
- Bisakah kita memverifikasi bahwa setiap pengguna, perangkat, dan agen AI tepercaya sebelum memberikan akses?

Catatan: Kelima langkah tersebut merupakan kemampuan yang saling terkait, yang memungkinkan Anda menentukan urutan implementasi terbaik untuk organisasi Anda.

4.

Pengelolaan dalam Skala Besar

Jaga agar pengguna, perangkat, aplikasi, dan PC Cloud tetap sehat dan terkelola — diperluas hingga ke lini depan, kontraktor, agen, dan perangkat pribadi Anda. Sebagai contoh, organisasi yang memiliki tenaga kerja musiman dapat menyediakan PC Cloud yang aman dengan kebijakan organisasi, aplikasi, dan perlindungan yang sudah terintegrasi, untuk dengan cepat mengintegrasikan tim ini ke lingkungan terkelola yang sama yang digunakan oleh karyawan—alih-alih mengirim, mengelola, dan memulihkan perangkat fisik untuk setiap individu. Ketika titik akhir dikelola dan diamankan, AI dapat diterapkan secara konsisten dan aman di seluruh tenaga kerja tanpa memperhatikan perangkat, lokasi, atau gaya kerja.

Dari mana memulai
Fokuslah terlebih dahulu pada kontrol kebijakan perangkat yang tidak terkelola dan pribadi melalui kebijakan perlindungan aplikasi dan kepatuhan sebelum memperluas kemampuan manajemen. Membawa titik akhir ke kerangka kerja manajemen bersama dapat memfasilitasi manfaat keamanan dan operasional secara langsung sekaligus menciptakan fondasi untuk adopsi AI yang lebih luas.

Dampak potensial
Karyawan mendapatkan pengalaman terpadu di perangkat korporat, frontline, dan pribadi, sementara TI memperoleh visibilitas, kontrol, dan konsistensi yang dibutuhkan untuk menskalakan AI secara aman.

Pemeriksaan Kesiapan

Untuk para CIO, pertimbangkan berikut ini:
- Bisakah kita secara konsisten mengelola dan mengatur pengguna, perangkat, aplikasi, serta titik akhir yang diaktifkan AI di seluruh organisasi?

Untuk para CISO, pertimbangkan berikut ini:
- Bisakah kontrol keamanan dan kepatuhan diskalakan secara konsisten ke seluruh karyawan, kontraktor, pekerja garis depan, dan agen AI?

5.

Melindungi dan Merespons

Korelasikan sinyal di seluruh organisasi Anda untuk mendeteksi, menyelidiki, dan merespons ancaman di berbagai identitas, perangkat, data, dan alur kerja yang didukung AIuntuk membantu menjaga ketahanan organisasi seiring dengan meningkatnya adopsi AI. Ketika kontrol perlindungan diintegrasikan ke fondasi, organisasi dapat dengan percaya diri memperluas AI ke lebih banyak pengguna, lebih banyak data, dan lebih banyak skenario bisnis.

Dari mana memulai
Mulailah dengan mengidentifikasi risiko paparan secara menyeluruh di seluruh identitas, titik akhir, data, sumber daya cloud, dan aplikasi. Daripada menunggu insiden terjadi, pahami bagian yang paling berisiko dan tindakan apa yang akan berdampak signifikan dalam mengurangi risiko tersebut. Setelah itu, gunakan AI dalam strategi pertahanan Anda untuk membantu tim keamanan menghubungkan sinyal, memprioritaskan respons, dan melakukan investigasi ancaman dengan lebih cepat.

Dampak potensial
Karyawan dapat menggunakan AI secara aman untuk mendukung produktivitas mereka dengan lebih sedikit gangguan, sementara tim keamanan mendapatkan visibilitas untuk mendeteksi dan merespons ancaman dengan lebih cepat.

Pemeriksaan Kesiapan

Untuk para CIO, pertimbangkan berikut ini:
- Mampukah operasi keamanan kita mengimbangi kecepatan dan skala yang diperkenalkan AI dalam bisnis?

Untuk para CISO, pertimbangkan berikut ini:
- Bisakah kita mendeteksi, menyelidiki, dan mengatasi ancaman dengan cepat sebelum berdampak pada data, operasi, atau alur kerja berbasis AI?

> Dengan melakukan konsolidasi pada Microsoft 365, kami telah menciptakan lingkungan tempat Copilot dapat beroperasi secara optimal. Inilah kemungkinan sebab kita dapat melihat penggunaan aktif harian Copilot mencapai 90% hingga 95%.

Elaine Smith
Pemimpin Program untuk Copilot PepsiCo

Baca kisah lengkapnya: Studi Kasus Pelanggan

Catatan: Kelima langkah tersebut merupakan kemampuan yang saling terkait, yang memungkinkan Anda menentukan urutan implementasi terbaik untuk organisasi Anda.

Tiga pergeseran yang dapat membantu membangun kesiapan AI

Setiap langkah dalam kerangka kerja dasar yang aman dirancang untuk memperkuat bagian spesifik dari lingkungan operasional untuk menghubungkan pekerjaan, data yang siap, akses yang aman, pengelolaan dalam skala besar, serta melindungi dan merespons.

Bersama-sama, langkah-langkah ini membantu memberdayakan momentum perusahaan untuk transformasi AI yang lebih luas dengan membantu organisasi Anda membangun kesiapan. Hasilnya bukan hanya fondasi yang kuat, tetapi serangkaian perubahan praktis yang dapat membantu mengembangkan praktik organisasi dengan konteks, kendali, dan kepercayaan diri.

Pergeseran 1. Dari alat dan informasi yang terpisah-pisah menuju kecerdasan kerja yang terhubung.

AI menjadi lebih bermanfaat ketika mampu mengambil pelajaran dari cara kerja yang sebenarnya terjadi di berbagai aspek seperti orang, konten, percakapan, rapat, aplikasi, dan alur kerja. Ketika informasi tetap terperangkap dalam alat-alat yang tidak terhubung, AI hanya dapat memberikan jawaban parsial dan karyawan masih menghabiskan waktu untuk mencari, beralih konteks, dan membangun kembali informasi pendukung. Landasan kerja yang terhubung membantu memberikan konteks organisasi yang dibutuhkan AI untuk menghasilkan wawasan yang relevan, merangkum pekerjaan yang sedang berlangsung, merekomendasikan langkah berikutnya, dan mendukung tindakan di seluruh alur kerja. Yang tak kalah penting, pengalaman kerja itu sendiri harus mengikuti karyawan kapan pun pekerjaan dilakukan—di seluruh perangkat fisik, lingkungan cloud, lokasi, dan tim—tanpa kehilangan konteks, akses, atau kesinambungan. Baik seseorang adalah karyawan tetap, kontraktor, atau kontributor berbasis proyek, mereka dapat tetap terhubung ke aplikasi, informasi, kebijakan, dan pengalaman AI yang sama yang mendukung pekerjaan produktif. Pergeseran ini dapat membantu organisasi beralih dari pengalaman yang terputus ke lingkungan kerja yang lebih siap AI, membantu mengaktifkan AI agar dapat melampaui peningkatan produktivitas individu, dan membawa perubahan yang lebih luas di seluruh tim dan proses bisnis.

Pergeseran 2. Dari berbagi data berlebihan dan risiko akses menuju kontrol dan data yang terlindungi:

Seiring dengan meluasnya penggunaan AI, organisasi membutuhkan keyakinan bahwa data sensitif dapat ditemukan, diatur, dan hanya tersedia bagi orang, perangkat, dan agen yang tepat. Tanpa fondasi tersebut, AI dapat memperbesar kesenjangan yang ada terkait berbagi informasi berlebihan, akses, dan kepatuhan. Pergeseran ini adalah tentang menjadikan perlindungan sebagai bagian dari model operasional: mengklasifikasikan dan memberi label pada data bernilai tinggi, menerapkan kebijakan DLP dan akses, memverifikasi identitas dan kondisi perangkat, serta memastikan kebijakan tetap melekat pada data saat disimpan, dibagikan, diakses, dan digunakan dalam alur kerja yang didukung AI. Hasilnya adalah lingkungan yang lebih tepercaya tempat karyawan dan agen dapat memanfaatkan konteks bisnis yang relevan, sementara para pemimpin mempertahankan visibilitas, tata kelola, dan kendali.

Pergeseran 3. Dari sinyal yang terfragmentasi menuju pertahanan terpadu yang dapat diskalakan.

Penerapan AI dalam skala besar meningkatkan kecepatan, volume, dan kompleksitas pekerjaan, yang juga dapat meningkatkan jumlah sinyal yang perlu dipahami dan ditindaklanjuti oleh tim keamanan. Fondasi yang lebih kuat membantu tim menghubungkan identitas, titik akhir, data, aplikasi, dan sinyal ancaman ke wawasan risiko yang lebih lengkap. Juga membantu mengintegrasikan AI ke dalam strategi pertahanan, mendukung investigasi, respons, dan penentuan prioritas sambil mempertahankan kontrol yang konsisten di seluruh pengguna, perangkat, PC Cloud, agen, dan alur kerja yang didukung AI. Pergeseran ini dapat membantu organisasi meningkatkan skala AI dengan ketahanan sekaligus memberdayakan kendali dalam cara AI diterapkan, dipantau, dan dilindungi.

Langkah berikutnya sesuai peran.

Gunakan ketiga pergeseran tersebut sebagai sesi kerja eksekutif untuk mengubah kesiapan AI menjadi rencana yang berurutan. Tujuannya bukanlah untuk mengatasi setiap kesenjangan fundamental secara sekaligus, melainkan untuk menyepakati titik temu prioritas antara CIO dan CISO, aspek apa saja yang perlu dimodernisasi oleh CIO guna membuka peluang peningkatan skala, serta aspek apa saja yang perlu diperkuat oleh CISO demi menjaga kepercayaan seiring dengan berkembangnya adopsi AI.

Mulailah bersama. Selaraskan pada landasan yang siap untuk AI.

Mulailah dengan tampilan bersama tentang arah ambisi AI yang bergerak lebih cepat daripada model operasional yang mendasarinya. Keselarasan antara CIO dan harus berfokus pada alur kerja, data, identitas, perangkat, dan kontrol yang paling penting untuk tahapan adopsi AI berikutnya.

1. Alur kerja berbasis AI mana yang harus kita kembangkan selanjutnya, dan fondasi apa yang perlu disiapkan sebelum kita melakukan ekspansi?
2. Di mana kita membutuhkan konteks yang lebih terhubung , tata kelola yang lebih kuat, atau kepemilikan yang lebih jelas agar AI dapat digunakan secara bermanfaat dan tepercaya?
3. Kesenjangan kesiapan mana yang, jika diatasi terlebih dahulu, akan menciptakan kepercayaan terbesar bagi bisnis?

Fokus CIO. Modernisasi infrastruktur digital.

CIO dapat membantu mengubah AI dari penggunaan yang terisolasi menjadi momentum perusahaan dengan menyederhanakan infrastruktur digital, menghubungkan alat dan alur kerja yang digunakan karyawan serta memodernisasi pengalaman titik akhir dan ruang kerja sehingga AI dapat beroperasi di seluruh bisnis dengan lebih sedikit hambatan.

1. Bagaimana produktivitas, kolaborasi, dan strategi titik akhir kita perlu berkembang seiring semakin terintegrasinya AI dalam pekerjaan sehari-hari?
2. Kelompok karyawan, perangkat, atau pola kerja mana saja yang membutuhkan pengalaman yang lebih konsisten sebelum AI dapat diterapkan secara luas?
3. Di mana konsolidasi dan modernisasi dapat mengurangi kompleksitas sekaligus meningkatkan nilai yang didapatkan karyawan dari AI?

Fokus CISO. Perluas kepercayaan dan kendali.

CISO dapat menskalakan AI dengan keyakinan dengan membantu memastikan data sensitif dapat ditemukan dan dilindungi, akses dikelola di seluruh pengguna, perangkat, dan agen, serta sinyal keamanan disatukan untuk membantu mendeteksi dan merespons ancaman karena AI dapat meningkatkan kecepatan dan kompleksitas risiko.

1. Kontrol apa yang perlu diterapkan pada data, identitas, perangkat, dan agen seiring dengan semakin banyaknya alur kerja yang menggunakan AI?
2. Di mana kita membutuhkan visibilitas yang lebih baik sebelum memperluas akses AI ke informasi sensitif atau proses berdampak tinggi?
3. Bagaimana model deteksi, respons, dan tata kelola kita harus beradaptasi seiring AI dan agen mengambil peran yang lebih besar?

Mulai membangun kesiapan AI Anda.

Transformasi AI dapat berkembang ketika pekerjaan terhubung, data terlindungi, akses diatur, titik akhir dikelola, dan sinyal keamanan bekerja bersama. Seiring pekerjaan menjadi semakin terdistribusi dan dinamis, organisasi dapat memperoleh manfaat dari lingkungan kerja yang konsisten dan teratur, dengan aplikasi, data, kebijakan, dan pengalaman tetap terhubung di semua lingkungan fisik maupun cloud.

Ketika pengalaman kerja mengikuti karyawan tanpa kehilangan konteks, AI dapat membantu memberikan wawasan yang lebih relevan, mendukung tindakan di seluruh alur kerja, dan meningkatkan skala secara lebih efektif di seluruh organisasi. Itulah fondasi yang dirancang Microsoft 365 untuk membantu organisasi membangun—mengintegrasikan produktivitas, keamanan, kepatuhan, identitas, pengelolaan titik akhir, dan AI ke dalam satu platform terintegrasi sehingga para CIO, CISO, dan pemimpin bisnis dapat maju bersama.

Ajakan bertindak →

1. **Mulailah bersama.** Lakukan penyelarasan pada alur kerja, data, identitas, perangkat, dan kontrol yang paling penting untuk fase adopsi AI selanjutnya.
2. **Membangun dengan Microsoft 365.** Gunakan fondasi terintegrasi di seluruh Microsoft 365 Suites dan Microsoft 365 Copilot, serta Windows 365 untuk menghubungkan pekerjaan, melindungi data, mengatur akses, mengelola dalam skala besar, dan merespons dengan percaya diri.
3. **Menskalakan dengan percaya diri.** Urutkan langkah-langkah pertama yang menciptakan momentum — dimulai dengan kasus penggunaan bernilai tertinggi dan data berisiko tertinggi — lalu perluas seiring fondasi menguat.

Sumber:
1 Laporan Deloitte tentang Perkembangan AI di Perusahaan 2026, PDF, Sebuah survei terhadap lebih dari 3.200 pemimpin Bisnis dan TI di 24 negara di organisasi dengan 1 atau beberapa implementasi AI yang digunakan setiap hari.
2 Indeks Tren Kerja 2026, Data Telemetri Microsoft 365 didasarkan pada sinyal produktivitas Microsoft 365 yang telah diagregasi dan dianonimkan, serta survei terhadap 20.000 pekerja tetap atau wiraswasta berbasis pengetahuan yang menggunakan AI di tempat kerja di 10 pasar antara 18 Februari 2026 dan 7 April 2026. Pasar global yang disurvei meliputi: Australia, Brasil, Prancis, Jerman, India, Italia, Jepang, Belanda, Inggris Raya, dan Amerika Serikat.
3 Laporan McKinsey tentang perkembangan organisasi tahun 2026 Survei skala besar terhadap para pemimpin di seluruh dunia yang diikuti oleh 10.000 lebih eksekutif senior di 15 negara dan 16 industri.
4 NTT Data Research Reveals C-Suite Misalignment Over GenAI Adoption, 20 Juni 2025. Survei terhadap 2.300 lebih pengambil keputusan senior di bidang GenAI, yang terdiri dari 1.500 pemimpin tingkat C-Suite di 34 negara.

© 2026 Microsoft Corporation. Hak cipta dilindungi undang-undang. Dokumen ini disediakan "sebagaimana adanya". Informasi dan pandangan yang disampaikan dalam dokumen ini, termasuk URL dan referensi situs web Internet lainnya, dapat berubah tanpa pemberitahuan. Anda menanggung risiko dalam menggunakannya. Dokumen ini tidak memberi Anda hak hukum apa pun atas kekayaan intelektual untuk produk Microsoft mana pun. Anda dapat menyalin dan menggunakan dokumen ini sebagai referensi dan untuk tujuan internal.