Microsoft 365 Copilot

# ضمان أمن البيانات في عصر الذكاء الاصطناعي

**دليل لقادة تكنولوجيا المعلومات**

**الكتاب الإلكتروني**

تم كتابة هذا الدليل لقادة تكنولوجيا المعلومات الذين يحتاجون إلى تعزيز تبني الذكاء الاصطناعي مع الحفاظ على أمان بيانات مؤسساتهم.
وسيساعدك هذا على فهم المخاطر التي يفرضها الذكاء الاصطناعي على أمان البيانات والخصوصية، مع تزويدك بالرؤى اللازمة لقيادة تحول الذكاء الاصطناعي في شركتك بثقة.

# جدول المحتويات

٠١

# القواعد الجديدة للعمل المدعوم بالذكاء الاصطناعي

يفتح الذكاء الاصطناعي التوليدي أبوابًا جديدة للابتكار ويساعد الفرق على العمل بشكل أسرع وأذكى من أي وقت مضى. وبالنسبة للمؤسسات ذات التفكير المستقبلي، فإن الذكاء الاصطناعي ليس مجرد اتجاه تكنولوجي آخر - بل هو ضرورة أعمال، وضروري لكيفية عملها وتقديم القيمة والحفاظ على الميزة التنافسية.

لكن هذا التبني السريع يجلب تحديات جديدة ومضخمة يجب على قادة تكنولوجيا المعلومات معالجتها والسيطرة عليها بشكل استباقي. ويمكن لأنظمة الذكاء الاصطناعي البحث بنشاط عن المعلومات ودمجها عبر نظام البيانات بأكمله، مما يزيد من مخاطر الأمان التي تتجاوز الأدوات التقليدية. على الرغم من التوسع السريع للذكاء الاصطناعي، إلا أن ١٪ فقط من المؤسسات أفادت بدمج الذكاء الاصطناعي بشكل كامل في مهام سير العمل لديها باستخدام بروتوكولات الأمان المناسبة.[١] ومن خلال تنفيذ تدابير أمان وحوكمة قوية منذ بداية رحلتك في مجال الذكاء الاصطناعي، يمكن لفريقك حماية البيانات الحساسة بشكل فعال، والحفاظ على متطلبات الامتثال، وحماية معلومات مؤسستك، كل ذلك مع تمكين الابتكار من الازدهار.

## موجة تبني الذكاء الاصطناعي موجودة بالفعل


٠٢

# فهم تأثير الذكاء الاصطناعي على أمان البيانات

قبل الخوض في التحديات المحددة، من المهم أن نفهم كيف يغير الذكاء الاصطناعي مشهد أمان البيانات بشكل أساسي. وعلى عكس البرامج التقليدية التي لا تصل إلى البيانات إلا عند توجيهها بشكل محدد، يعمل الذكاء الاصطناعي التوليدي على معالجة المحتوى وتحليله وإنشاءه بشكل فعال بناءً على كل المعلومات التي تتلقاها.

ويُعد هذا الاختلاف مهمًا لعدة أسباب:

- يمكن لأدوات الذكاء الاصطناعي اكتشاف الروابط بين البيانات التي قد يغفلها البشر
- يمكنها تجميع المعلومات عبر مصادر متعددة تلقائيًا
- يمكنها إنشاء محتوى جديد يحتوي على عناصر من مدخلات حساسة

من المحتمل أن تكون أدوات الأمان التقليدية الخاصة بك لم يتم تصميمها مع وضع هذه الإمكانات في الاعتبار. وعلى الرغم من تتبع البرامج التقليدية مسارات يمكن التنبؤ بها عند الوصول إلى البيانات، إلا أن الذكاء الاصطناعي يمكنه اتخاذ مسارات غير متوقعة عبر نظام المعلومات البيئي الخاص بك، مما قد يؤدي إلى كشف البيانات الحساسة بطرق لم تتوقعها.

يتطلب هذا التحول الجذري اتباع نهج جديدة للأمان وحوكمة البيانات يتناول على وجه التحديد كيفية تفاعل الذكاء الاصطناعي مع أصول المعلومات الخاصة بمؤسستك.

٠٣

# تحدي الذكاء الاصطناعي الخفي

أينما كنت في رحلة تبني الذكاء الاصطناعي، فإن موظفيك يجدون بالفعل حلولهم الخاصة، مما ينشئ ما يُعرف باسم "الذكاء الاصطناعي الخفي".

يؤدي هذا الاستخدام غير المصرح به إلى إنشاء نقاط عمياء كبيرة في وضعك الأمني. وعندما يشارك الموظفون بيانات الشركة مع أنظمة الذكاء الاصطناعي الخارجية، فإنهم يتجاوزون ضوابط الأمان الحالية وينشئون ثغرات أمنية لا تكون معظم المؤسسات مستعدة لمعالجتها.

الذكاء الاصطناعي الخفي ليس مجرد مشكلة أمان، بل قد يكون أحد أعراض عدم تلبية احتياجات الإنتاجية في مؤسستك. وعندما يلجأ الموظفون إلى أدوات غير معتمدة، فإنهم بذلك يشيرون إلى أن أنظمتك الرسمية لا تلبي متطلباتهم. ويتطلب التعامل مع الذكاء الاصطناعي الخفي حوكمة أقوى وحلول إنتاجية محسنة.

## السبب وراء ظهور الذكاء الاصطناعي الخفي:

- الموظفون يتطلعون إلى تعزيز الإنتاجية من خلال قدرات الذكاء الاصطناعي المذهلة
- أحمال العمل اليومية تتجاوز الوقت والطاقة المتاحين بشكل متزايد
- الفرق تواجه ضغوطًا متزايدة لتقديم المزيد بالموارد نفسها
- أدوات الذكاء الاصطناعي توفر للمستهلك حلولاً فورية دون عوائق الموافقة
- عمليات الشراء الرسمية لتكنولوجيا المعلومات لا يمكنها أن تواكب وتيرة الابتكار

## مخاطر الذكاء الاصطناعي الخفي:

- لا توجد رؤية واضحة لبيانات الشركة التي تتم معالجتها بواسطة أنظمة الذكاء الاصطناعي الخارجية
- لا يوجد ضمان بعدم الاحتفاظ بالمعلومات السرية
- لا توجد معايير أمان متسقة عبر الأنظمة الأساسية المختلفة للذكاء الاصطناعي
- لا توجد إمكانية التدقيق لأغراض الامتثال
- لا يوجد تكامل مع البنية الأساسية الحالية للأمان

## ضع في الاعتبار السيناريو التالي:

يواجه محلل مالي صعوبة في التعامل مع جدول بيانات معقد، فيقوم بتحميله إلى أداة ذكاء اصطناعي غير مصرح بها للحصول على المساعدة. ويحتوي جدول البيانات هذا على بيانات مالية خاصة بالعملاء، ومقاييس داخلية، وتوقعات. وبينما يحصل المحلل على المساعدة التي يحتاجها، فإن البيانات المالية الحساسة لمؤسستك أصبحت الآن موجودة خارج محيط الأمان الخاص بك، وأصبحت غير مرئية تمامًا لأنظمة المراقبة الخاصة بك.

٠٤

# حقيقة جلب الذكاء الاصطناعي الخاص بك (BYOAI)

في غياب التوجيه الواضح من القيادة، يتجه الموظفون بشكل متزايد إلى تبني الذكاء الاصطناعي — ٧٨٪ من مستخدمي الذكاء الاصطناعي يتبنون نهج "جلب الذكاء الاصطناعي الخاص بك" (BYOAI) إلى العمل.[٢] ويظهر هذا الاتجاه بشكل أكثر وضوحًا في الشركات الصغيرة والمتوسطة الحجم، حيث ينخرط ٨٠٪ من الموظفين في ممارسات جلب الذكاء الاصطناعي إلى العمل (من الموظفين ممارسات إحضار أجهزتهم الخاصة من خلال أجهزة الذكاء الاصطناعي).[٢]

يأتي هذا النهج غير المعتمد مصحوبًا بجوانب سلبية كبيرة. وغالبًا ما يُبقي الموظفون استخدامهم للذكاء الاصطناعي سرًا — ويتردد **٥٢٪** منهم في الاعتراف باستخدام الذكاء الاصطناعي للمهام المهمة، ويشعر **٥٣٪** منهم بالقلق من أن استخدام الذكاء الاصطناعي يجعلهم يبدون قابلين للاستبدال.[٢] ولا تمنع هذا السرية المؤسسات من تحقيق المزايا الكاملة لتطبيق الذكاء الاصطناعي الاستراتيجي فحسب، بل تنشئ أيضًا ثغرات أمنية خطيرة في بيئة يشير فيها القادة إلى الأمان الإلكتروني وخصوصية البيانات باعتبارهما مصدر قلقهم **الأول**.[٢]

نظرًا للاستخدام واسع النطاق والنمو الحتمي للذكاء الاصطناعي، لا يدور السؤال حول ما إذا كان ينبغي السماح بالذكاء الاصطناعي في مؤسستك - بل حول طريقة توفير حل آمن يلبي احتياجات موظفيك مع الحفاظ على حماية بيانات مؤسستك.

٠٥

# المتاهة التنظيمية

إن أطر العمل والقوانين المتعلقة بخصوصية البيانات وأمنها تنشئ طبقة أخرى من التعقيد عند تبني الذكاء الاصطناعي. وعلى الرغم من أن بعض أطر العمل مصممة خصيصًا لحوكمة الذكاء الاصطناعي، إلا أن بعضها الآخر لديه تطبيقات أوسع لا تزال تؤثر على طريقة تعاملك مع المعلومات - وتظل العقوبات المفروضة على الانتهاكات شديدة.

عندما يستخدم موظفوك أدوات الذكاء الاصطناعي دون إشراف مناسب، قد يتسببون في انتهاكات للامتثال عن غير قصد. ويجعل الذكاء الاصطناعي هذا الخطر أعظم لأنه قادر على الوصول إلى المعلومات المنظمة ودمجها وعرضها بطرق لا تستطيع التقنيات التقليدية تحقيقها.

## اللوائح الأساسية التي تؤثر على استخدامك للذكاء الاصطناعي:

### اللائحة العامة لحماية البيانات

تمنح اللائحة العامة لحماية البيانات في الاتحاد الأوروبي الأشخاص السيطرة على بياناتهم الشخصية وتتطلب موافقة واضحة لمعالجتها

### قانون الذكاء الاصطناعي للاتحاد الأوروبي

إطار العمل الشامل للاتحاد الأوروبي المصمم خصيصًا لتنظيم أنظمة الذكاء الاصطناعي بناءً على مستويات المخاطر الخاصة بها

### قانون نقل التأمين الصحي والمساءلة (HIPAA)

يضع هذا القانون الفيدرالي الأمريكي للرعاية الصحية معايير صارمة للتعامل مع المعلومات الصحية المحمية

### إطار عمل إدارة مخاطر الذكاء الاصطناعي التابع للمعهد الوطني للمعايير والتقنية (NIST)

تساعد هذه الإرشادات الطوعية الأمريكية المؤسسات على معالجة المخاطر في تصميم أنظمة الذكاء الاصطناعي وتطويرها ونشرها

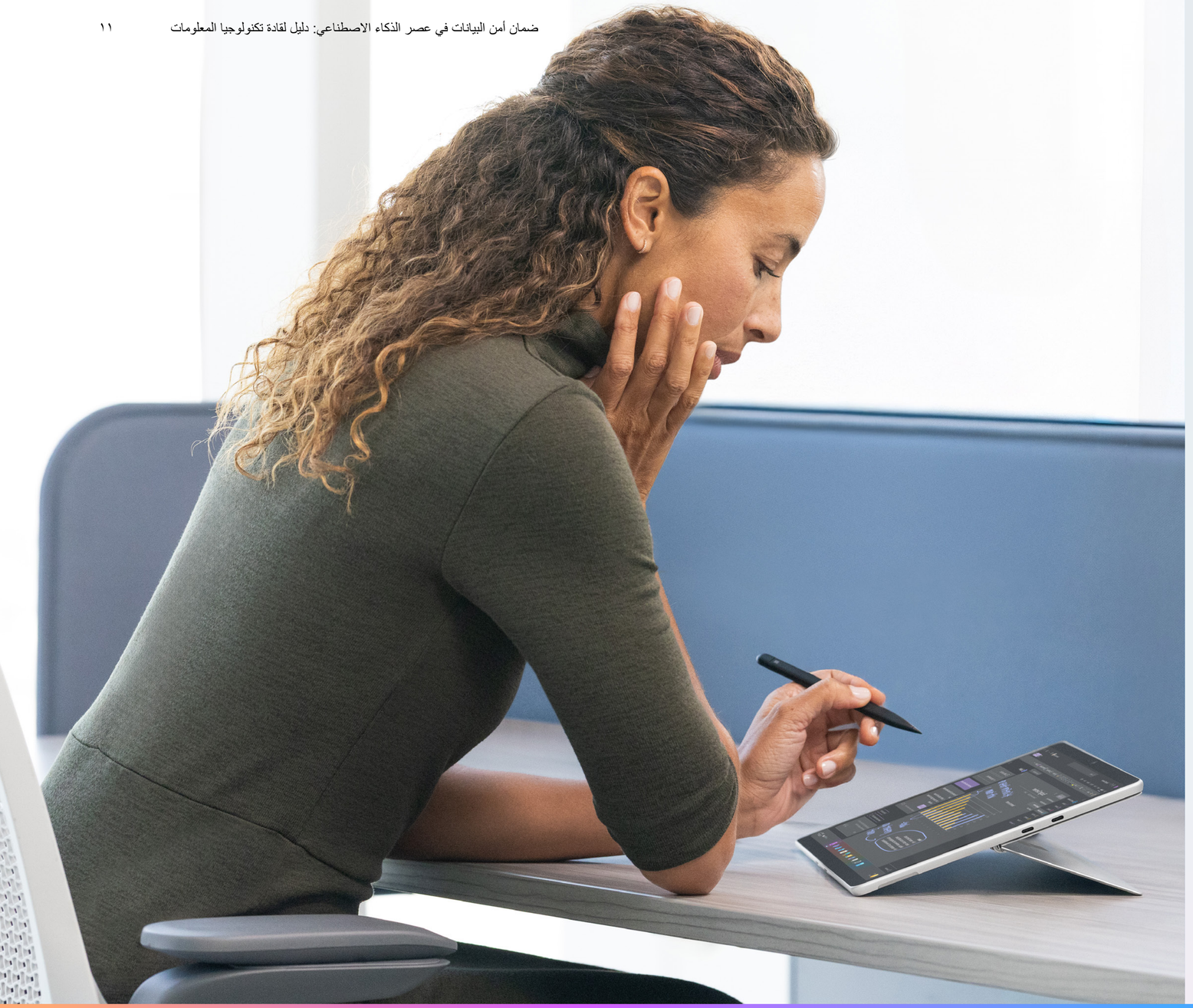
مع نمو استخدام الذكاء الاصطناعي في مؤسستك، تحتاج إلى حوكمة تساعد الأشخاص على العمل بكفاءة مع الحفاظ على امتثال مؤسستك للوائح التي تؤثر على أعمالك وعملائك.

### مخاطر الامتثال في الذكاء الاصطناعي:

- بيانات العملاء التي تتم معالجتها على خوادم خارج المناطق المعتمدة
- المعلومات الشخصية التي يتم استخدامها دون موافقة مناسبة
- البيانات الحساسة التي تبقى في الأنظمة من دون ضوابط الاحتفاظ المناسبة
- لا يوجد مسار تدقيق لكيفية الوصول إلى المعلومات المحمية واستخدامها
- المحتوى الذي تم إنشاؤه بواسطة الذكاء الاصطناعي والذي ينتهك متطلبات الامتثال الخاصة بالقطاع

### يمكن أن تؤدي هذه الانتهاكات إلى عواقب خطيرة:

- غرامات مالية كبيرة (يمكن أن تصل غرامات اللائحة العامة لحماية البيانات (GDPR) إلى ٤٪ من إيراداتك العالمية)[٤]
- متطلبات إخطار الأطراف المتأثرة بشأن خروقات البيانات
- الإجراءات القانونية من المتأثرين
- الإضرار بسمعة شركتك وثقة العملاء



٠٦

# إطار عمل يضع الأمان أولاً لتقييم حلول الذكاء الاصطناعي

مع وجود الذكاء الاصطناعي الخفي، وجلب الذكاء الاصطناعي الخاص بك (BYOAI)، واللوائح التي تنشئ مخاطر كبيرة، تحتاج إلى نهج منظم لتقييم حلول الذكاء الاصطناعي التي تضمن قدرتها على مساعدة مؤسستك في تعزيز الابتكار - مع حماية البيانات الحساسة في الوقت نفسه وضمان الامتثال للمتطلبات التنظيمية المتطورة.

يقدم إطار العمل التالي ستة أسئلة بسيطة لتقييم ما إذا كان النظام الأساسي للذكاء الاصطناعي يحقق النجاح على كلا الجبهتين.

السؤال الأول

## هل يوفر هذا أمانًا على مستوى المؤسسة من البداية؟

من خلال استخدام الحل المناسب، يتحول أمانك من مجرد الاستجابة للمشكلات بعد حدوثها، إلى البحث بشكل استباقي عن نقاط الضعف في بيانات مؤسستك - قبل أن تصبح مشكلات أكبر.

### ابحث عن الحلول التي تتيح ما يلي:

- توفير رؤية في الوقت الحقيقي عبر نظام البيانات بأكمله
- التعرف تلقائيًا على مخاطر البيانات المحتملة قبل أن تتحول إلى حوادث
- حماية المعلومات الحساسة على كل المستويات

السؤال ٢

## هل يمكنه بسهولة اعتماد ضوابط الأمان الحالية وتعزيزها؟

يجب أن تعمل سياسات الأمان الخاصة بمؤسستك مع الذكاء الاصطناعي بسلاسة. ويجب على موفر حلول الذكاء الاصطناعي الخاص بك احترام أطر عمل الأمان الحالية لديك والتكامل معها - وليس مطالبتك بإنشاء أطر عمل جديدة تمامًا.

### ابحث عن الحلول التي تتيح ما يلي:

- تبني سياسات الأمان الحالية لديك، وعلامات الحساسية، وإعدادات حماية المعلومات بسلاسة
- تطبيق عناصر تحكم وصول مفصلة على المستوى الفردي، بحيث لا يتمكن أي مستخدم من الوصول إلى البيانات التي لا ينبغي له الوصول إليها
- الإشارة بشكل نشط إلى محاولات تقويض عناصر التحكم في الوصول

السؤال ٣

## هل يتضمن هذا عناصر تحكم مدمجة في الحوكمة والخصوصية؟

نظرًا لأن أدوات الذكاء الاصطناعي تعمل بشكل أكثر استباقية، يجب أن تكون تدابير الأمان الخاصة بك استباقية أيضًا. ويؤدي تنفيذ حوكمة قوية للبيانات إلى إنشاء حدود واضحة حيث يمكن لموظفيك الابتكار بأمان دون تعريض المعلومات الحساسة للخطر.

### ابحث عن الحلول التي تتيح ما يلي:

- مركزة حوكمة الذكاء الاصطناعي من خلال فرض السياسات تلقائيًا عبر كل الأنشطة
- تضمين الكشف المبكر عن الإفراط المحتمل في مشاركة البيانات
- التوافق مع أطر العمل التنظيمية لضمان استخدام الذكاء الاصطناعي المتوافق

السؤال ٤

## هل يمكن نشر هذا بشكل متسق في المؤسسة بأكملها؟

لدى موظفيك أسلوبهم الخاص في العمل، وجداولهم الزمنية الخاصة، وقد يكونون موجودين في جميع أنحاء العالم. وينبغي أن يكون الذكاء الاصطناعي مفيدًا للجميع.

### ابحث عن الحلول التي تتيح ما يلي:

- توفير إعداد سلس وتبني سهل للذكاء الاصطناعي في مهام سير العمل اليومية
- توفير إمكانية الوصول المرنة، من الدردشة المجانية بالذكاء الاصطناعي إلى حلول العامل القابلة للتطوير
- مساعدة الموظفين على بناء طلاقة الذكاء الاصطناعي ودمجها في عملهم

السؤال ٥

## هل يتكامل هذا بسلاسة مع أطر العمل الحالية؟

تعمل شركتك حاليًا باستخدام البنية الأساسية الرقمية الخاصة بها من برامج، وتطبيقات، وغيرها.

### ابحث عن الحلول التي تتيح ما يلي:

- التوافق بسلاسة مع أدواتك وبرامجك لتقليل الانقطاع
- توفير تجربة ذكاء اصطناعي مستمرة عبر جميع التطبيقات حتى يتمكن العمل من التدفق بين الأدوات بسلاسة
- تنفيذ المهام تلقائيًا وتحسينها ضمن مهام سير العمل الحالية

السؤال ٦

## هل يتم تمكين المستخدمين من الابتكار؟

في جوهر الذكاء الاصطناعي، ينبغي له أن يعمل على تغيير الطريقة التي يتم بها إنجاز العمل. ولا يتعلق الأمر بالتشغيل التلقائي فقط، بل يتعلق أيضًا بتعزيز الإنتاجية وتحفيز الابتكار.

### ابحث عن الحلول التي تتيح ما يلي:

- تحويل حالات استنزاف الوقت إلى عمليات مبسطة
- تنفيذ المهَام المتكررة تلقائيًا
- تمكين العمال من استعادة الوقت والتركيز على الأولويات

٠٧

# Microsoft 365 Copilot:
# الذكاء الاصطناعي الذي يمكنك الوثوق به

إن Microsoft 365 Copilot هو حل الذكاء الاصطناعي التوليدي المصمم لتوفير الأمان القوي والحوكمة وعناصر التحكم في الوصول، مما يضمن النشر الآمن والابتكار المستدام. إنه يعزز الإنتاجية باستخدام أدوات بديهية مثل Copilot Chat، التي يعمل حيث تعمل أنت، وCopilot Studio، حيث يمكن لفريقك بناء عمال الذكاء الاصطناعي المخصصين دون مهارات البرمجة.

يتكامل Copilot بسلاسة داخل بيئة Microsoft 365 الخاصة بك، ويرث أذونات المستخدم، وعلامات الحساسية، وسياسات تفادي فقدان البيانات، ومتطلبات إقامة البيانات الجغرافية - دون تكوين إضافي. ومن خلال تضمين الذكاء الاصطناعي في الأدوات التي يستخدمها موظفوك بالفعل، يعمل Copilot على التخفيف من مخاطر الأمان مع الحفاظ على البيانات داخل بيئة Microsoft 365 الموثوقة لديك.

تضمن التزامات Microsoft بقاء مؤسستك تحت السيطرة:

- بياناتك آمنة أثناء الخمول وأثناء النقل
- لا تُستخدم بياناتك لتدريب نماذج الذكاء الاصطناعي
- أنت تختار المعلومات التي يتم إرسالها إلى السحابة
- أنت تتمتع بالحماية من مخاطر أمان الذكاء الاصطناعي وحقوق النشر

توفر أدوات الحوكمة المصممة خصيصًا مثل نظام Copilot Control وSharePoint Advanced Management لفرق تكنولوجيا المعلومات الرؤية وعناصر التحكم وسجلات التدقيق اللازمة للحفاظ على الامتثال.

مع Microsoft 365 Copilot، لن تحتاج إلى الاختيار بين الابتكار والأمان، بل يمكنك الحصول على كليهما.

٠٨

# المسار الآمن للتحول في الذكاء الاصطناعي

توفر ثورة الذكاء الاصطناعي فرصة فريدة لقادة تكنولوجيا المعلومات لتقديم قيمة استراتيجية من خلال تحقيق التوازن بين الابتكار والأمان.

من خلال تنفيذ أدوات الذكاء الاصطناعي الآمنة مثل Microsoft 365 Copilot، ستتمكن من تمكين الموظفين من الحصول على أدوات لتحقيق إنتاجية أكبر، مع القضاء على مخاطر الذكاء الاصطناعي الخفي. وإن المسار إلى الأمام يدور حول تمكين الابتكار بشكل آمن. وإن قيادتك في تبني الذكاء الاصطناعي الآمن سوف تضع تكنولوجيا المعلومات كعامل تمكين للتحول، مما يساعد مؤسستك على النجاح في هذا العصر الجديد مع الحفاظ على أمان البيانات وتوافقها.

**الشروع في العمل باستخدام Microsoft 365 Copilot**

**المصادر:**

[١] "الوكالة الفائقة في مكان العمل: "تمكين الموظفين من إطلاق العنان لإمكانات الذكاء الاصطناعي الكاملة"، شركة McKinsey & Company، بتاريخ ٢٨ يناير ٢٠٢٥. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

[٢] "الذكاء الاصطناعي في العمل موجود هنا. والآن يأتي الجزء الصعب"، مؤشر اتجاهات العمل من Microsoft، بتاريخ ٨ مايو ٢٠٢٤. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part.

[٣] هل سينجح الذكاء الاصطناعي في الإصلاح؟ مؤشر اتجاه العمل من Microsoft، بتاريخ ٩ مايو ٢٠٢٣. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[٤] "اللائحة (الاتحاد الأوروبي) ٦٧٩/٢٠١٦ الصادرة عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي في ٢٧ أبريل ٢٠١٦ بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات، وإلغاء التوجيه 95/46/EC (اللائحة العامة لحماية البيانات)"، البرلمان الأوروبي ومجلس الاتحاد الأوروبي، ٢٧ أبريل ٢٠١٦. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.