Microsoft 365

ปลดล็อกศักยภาพของ AI ด้วยรากฐานที่ปลอดภัย

สารบัญ

บ ท นำ

โอกาสของ AI และความจำเป็นด้านความปลอดภัย

ช่องว่างด้านศักยภาพของผลิตภาพกำลังขยายตัวท่ามกลางกลุ่มแรงงานในปัจจุบัน จากรายงานดัชนีแนวโน้มการทำงานล่าสุด พบว่า **มากกว่า 80%** ของบุคลากรสายงานความรู้ที่ได้รับการสำรวจใน 31 ประเทศ ทั้งในระดับพนักงานทั่วไปและระดับผู้นำ รายงานว่าพวกเขารู้สึกมีเวลาและพลังงานไม่เพียงพอในการทำงาน[1] ในขณะเดียวกัน **มากกว่า 50%** ของผู้นำธุรกิจที่เข้าร่วมการสำรวจ ระบุว่าจำเป็นต้องเพิ่มผลิตภาพเพื่อให้บรรลุเป้าหมาย[1] นี่เป็นโอกาสในการประเมินวิธีการทำงานของเรา และแนวทางแก้ปัญหาที่เป็นไปได้เพื่อช่วยเชื่อมช่องว่างนี้ AI รวมถึงเอเจนต์ ถือเป็นทางเลือกที่มีความหวังในการแก้ไขปัญหานี้ **มากกว่า 80%** ของผู้นำที่เข้าร่วมการสำรวจ รายงานว่าพวกเขารู้สึกมั่นใจว่าองค์กรของตนจะเริ่มใช้เอเจนต์ AI เพื่อขยายขีดความสามารถของแรงงานในอีก 12–18 เดือนข้างหน้า[1]

การก้าวสู่ AI อย่างรวดเร็วนี้มีข้อควรพิจารณา: ควรสร้างสมดุลระหว่างนวัตกรรมกับความปลอดภัยที่แข็งแกร่งและการคุ้มครองข้อมูลส่วนบุคคล เพื่อบรรเทาความเสี่ยงที่อาจเกิดขึ้น การศึกษาของ iSMG เมื่อเร็ว ๆ นี้พบว่าผู้นำธุรกิจที่เข้าร่วมการสำรวจ **มากกว่า 70%** รายงานว่าการรับรองความเป็นส่วนตัวและความปลอดภัยของข้อมูล เป็นความท้าทายหลักในการผสานรวม AI เชิงสร้างใหม่เข้ากับโครงสร้างพื้นฐานไอทีที่มีอยู่[2] ผู้นำต้องเผชิญกับความจำเป็นสองประการ: เร่งการปรับใช้ AI เพื่อเพิ่มประสิทธิภาพการทำงานและปกป้องข้อมูลในยุคใหม่นี้

อีบุ๊กเล่มนี้จะนำเสนอข้อมูลเชิงลึกเกี่ยวกับกรณีตัวอย่าง AI ที่อาจก่อให้เกิดความเสี่ยง แนวทางในการจัดการความเสี่ยงเหล่านั้นด้วย Microsoft 365 E3 และรายการตรวจสอบเพื่อสนับสนุนองค์กรในการเริ่มต้นหรือเตรียมความพร้อมสำหรับการนำ AI มาใช้ในระดับองค์กร เตรียมพร้อมที่จะใช้งาน AI ด้วยความมั่นใจ: ช่วยให้องค์กรของคุณสร้างสรรค์นวัตกรรมด้วย AI โดยไม่กระทบต่อมาตรฐานความปลอดภัยหรือการปฏิบัติตามกฎระเบียบขององค์กร

ความตั้งใจที่ดีกับความเสี่ยงที่อาจเกิดขึ้น: สถานการณ์ตัวอย่างของ AI

ความเสี่ยงหลักในการใช้และนำ AI มาใช้งานมักเกิดจากพนักงานที่มีเจตนาดีที่มุ่งมั่นปฏิบัติงานและสร้างผลลัพธ์ที่มากขึ้น ในการเร่งเพิ่มประสิทธิภาพการทำงาน สมาชิกในทีมอาจเผลอแบ่งปันข้อมูลที่ละเอียดอ่อนกับเครื่องมือ AI หรือใช้แอปพลิเคชันที่ยังไม่ได้รับการอนุมัติจากฝ่ายไอทีโดยไม่ได้ตั้งใจ ซึ่งอาจสร้างความเสี่ยงและอาจทำให้องค์กรเผชิญกับภัยคุกคามใหม่ ๆ

ลองพิจารณาตัวอย่างสองกรณีเพื่ออธิบายประเด็นนี้ โดยกรณีหนึ่งเป็นผู้ปฏิบัติงานด้านข้อมูลในสำนักงาน และอีกกรณีเป็นผู้ปฏิบัติงานหน้างาน

ในตัวอย่างสมมติเหล่านี้ คุณจะได้เรียนรู้ว่า 1) วิธีการใช้ AI ด้วยเจตนาดีอาจนำไปสู่การละเมิดความปลอดภัยหากขาดการกำกับดูแลที่เหมาะสม และ 2) วิธีลดความเสี่ยงที่อาจเกิดขึ้นด้วยระบบรักษาความปลอดภัยที่แข็งแกร่ง

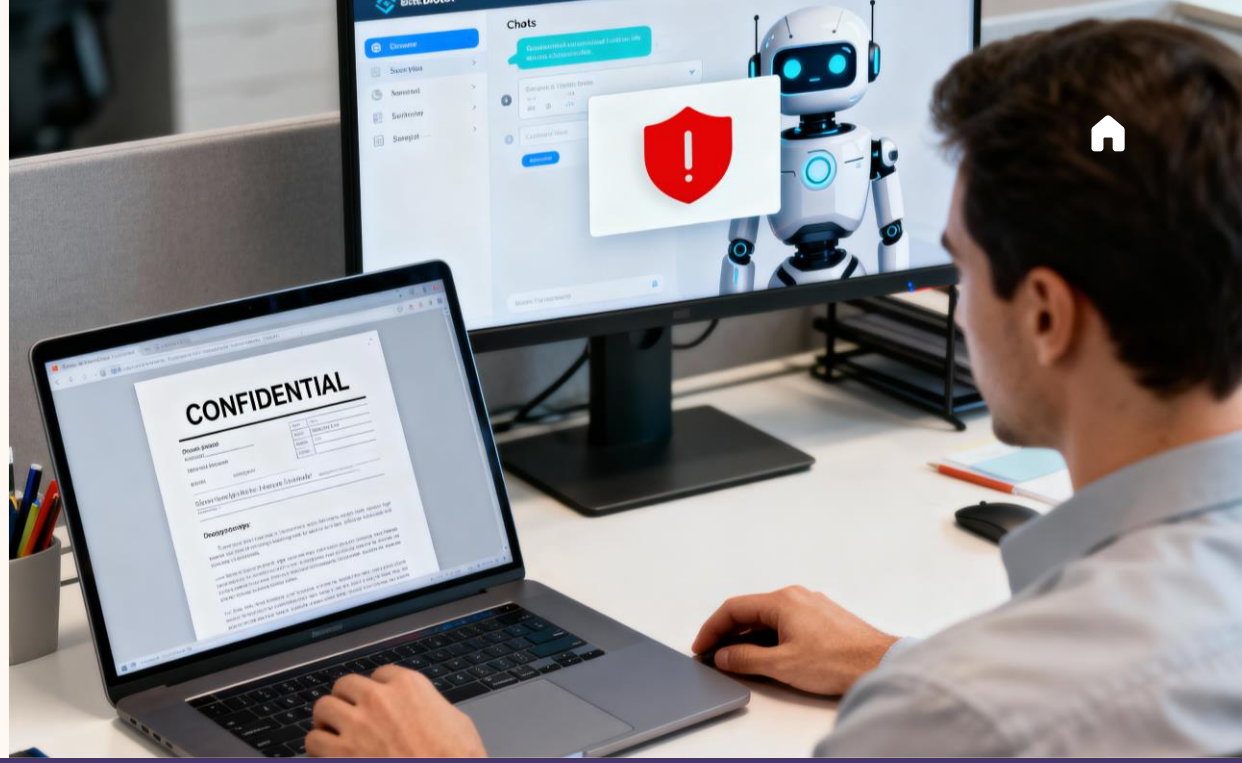
สถานการณ์ตัวอย่างที่ 14

ผู้จัดการฝ่ายการตลาดผลิตภัณฑ์ ใช้ประโยชน์จากเครื่องมือ AI เพื่อร่างข่าวประชาสัมพันธ์

ผู้จัดการฝ่ายการตลาดผลิตภัณฑ์ของบริษัทผู้ผลิตรายหนึ่ง ต้องเร่งการร่างข่าวประชาสัมพันธ์เกี่ยวกับผลิตภัณฑ์ใหม่ที่จะเปิดตัวในอีกไม่กี่เดือนข้างหน้า ภายใต้กำหนดเวลาที่จำกัด เพื่อระดมความคิดและเร่งกระบวนการเขียน พนักงานคัดลอกและวางข้อความบางส่วนจากแผนงานผลิตภัณฑ์ที่เป็นความลับ และการคาดการณ์ทางการเงินภายในองค์กรลงในผู้ช่วยเขียน AI ออนไลน์ฟรี เครื่องมือ AI สามารถสร้างย่อหน้าที่เรียบเรียงอย่างดีได้อย่างรวดเร็ว จากนั้นพนักงานได้นำไปใช้ในร่างข่าวประชาสัมพันธ์ อย่างไรก็ตาม เครื่องมือนี้ยังไม่ได้รับการตรวจสอบหรืออนุมัติจากองค์กร

ความเสี่ยงที่อาจเกิดขึ้น:

เมื่อใช้บริการ AI ภายนอกนี้ พนักงานได้อัปโหลดข้อมูลที่ละเอียดอ่อนของบริษัท (แผนผลิตภัณฑ์และข้อมูลทางการเงิน) ไปยังระบบของบุคคลที่สามโดยที่ทีมไอทีไม่สามารถมองเห็น และไม่สามารถจัดการหรือควบคุมได้ เมื่อข้อมูลถูกแบ่งปันกับเครื่องมือ AI บริษัทจะสูญเสียการควบคุมข้อมูลดังกล่าว เนื่องจากอยู่นอกเหนือขอบเขตที่ได้รับอนุญาต ตอนนี้ องค์กรไม่รู้ว่าข้อมูลจะถูกจัดเก็บไว้นานเท่าใด ใครบ้างที่เข้าถึงข้อมูลนั้นได้ หรือบุคคลที่สามจะนำข้อมูลนั้นไปใช้อย่างไร สิ่งที่เริ่มต้นจากความสำเร็จด้านผลิตภาพที่รวดเร็วได้กลายเป็นเหตุการณ์การรั่วไหลของข้อมูล สถานการณ์นี้สะท้อนถึงความเสี่ยงภายในที่อาจเกิดขึ้น เมื่อพนักงานที่มีเจตนาดีแบ่งปันข้อมูลที่ละเอียดอ่อนกับเครื่องมือ AI ที่ไม่ได้รับอนุญาต ซึ่งสร้างความเสี่ยงในการถูกโจมตีได้ง่ายให้กับองค์กร



การลดความเสี่ยงด้วย **Microsoft 365 E3:**

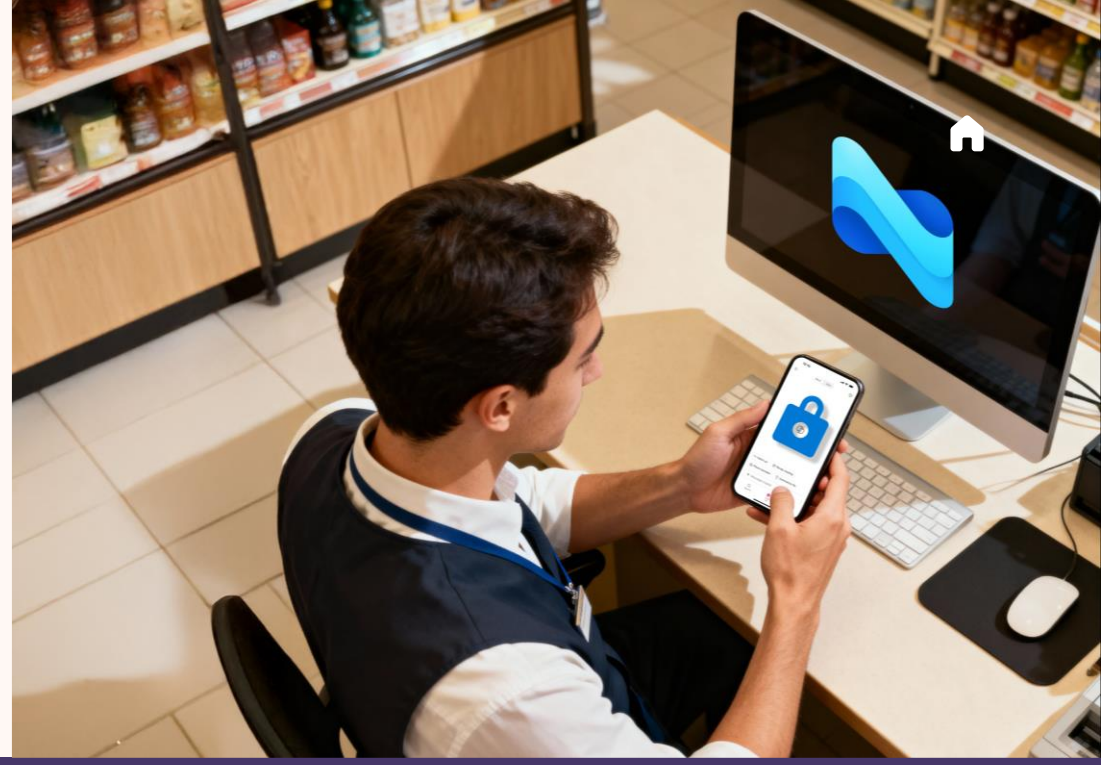
Microsoft 365 E3 มีคุณสมบัติและฟีเจอร์หลายอย่างที่สามารถช่วยป้องกันไม่ให้เกิดผลลัพธ์นี้ได้ **Microsoft Purview Information Protection Plan 1** ช่วยให้คุณสามารถใช้ป้ายชื่อระดับความลับและการเข้ารหัสกับเอกสาร เช่น แผนงานผลิตภัณฑ์หรือเอกสารโครงการทางการเงินได้ หากเอกสารเหล่านี้ได้รับการจัดประเภทและเข้ารหัสด้วยป้ายชื่อระดับความลับ เช่น *เป็นความลับ* พร้อมการเข้ารหัส การเข้าถึงเอกสารอาจถูกจำกัดไว้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น นอกจากนี้ **Cloud app discovery** ยังสามารถช่วยระบุแอป AI เชิงสร้างใหม่บนระบบคลาวด์ที่กำลังถูกใช้งาน (จากแอปจำนวนมากในแคตตาล็อกแอปคลาวด์) ว่าใครเป็นผู้ใช้ และใช้งานบ่อยแค่ไหน ฝ่ายไอทีอาจตรวจพบว่าพนักงานกำลังใช้เครื่องมือ AI นี้ และดำเนินการเพื่อจำกัดการใช้งานด้วย **Microsoft Defender for Endpoint P1** หรือจัดหาทางเลือกที่ได้รับอนุมัติ Microsoft 365 E3 มีเครื่องมือและความสามารถต่าง ๆ ที่ช่วยให้องค์กรเพิ่มการมองเห็นและลดความเสี่ยงได้อย่างมีประสิทธิภาพ

Öà Ï àþè ¼ãì¼ÝÛí Ù ½è Â AI ÏŒÝÞí ¼Ëí ÔÒàÕà è Ï ÛïÝ

สถานการณ์ตัวอย่างที่ 24

ผู้จัดการร้านค้าปลีกใช้ AI เพื่อร่างตารางงานและบันทึกผลการปฏิบัติงานของพนักงาน

ผู้จัดการร้านค้าของเครือข่ายค้าปลีกขนาดใหญ่กำลังเผชิญกับงานบริหารจำนวนมาก และค้นพบแอปการทำงาน AI ฟรีที่สัญญาว่าจะช่วยเหลือเรื่องการจัดตารางงานและการจัดทำเอกสาร เพื่อประหยัดเวลา ผู้จัดการจึงอัปโหลดสเปรดชีตที่มีรายชื่อพนักงาน หมายเลขโทรศัพท์ ค่าจ้างรายชั่วโมง ตารางเวลาทำงานที่ต้องการ และบันทึกผลการปฏิบัติงานล่าสุดลงในเครื่องมือ AI พวกเขาขอให้แอป AI สร้างตารางการทำงานที่เหมาะสม และจัดทำสรุปผลการประเมินพนักงานสำหรับการประชุมรายบุคคลที่กำลังจะมาถึง



ความเสี่ยงที่อาจเกิดขึ้น:

โดยการอัปโหลดข้อมูลพนักงานนี้ไปยังแอป AI ที่ยังไม่ได้รับการรับรอง ผู้จัดการได้เปิดเผยข้อมูลระบุตัวบุคคลที่สำคัญของพนักงานของตนแก่ระบบของบุคคลที่สาม ซึ่งอยู่นอกเหนือการควบคุมและการกำกับดูแลของบริษัท การกระทำดังกล่าวอาจก่อให้เกิดความเสี่ยงต่อการละเมิดความเป็นส่วนตัว และปัญหาด้านการปฏิบัติตามกฎหมายแรงงาน ฝ่ายทรัพยากรบุคคลและฝ่ายไอทีของบริษัทไม่สามารถตรวจสอบได้ว่าข้อมูลพนักงานถูกจัดเก็บอยู่ที่ใด ข้อมูลดังกล่าวถูกเก็บไว้นานเท่าใด หรือใครที่อาจเข้าถึงข้อมูลนี้ได้ สิ่งที่เริ่มต้นจากความพยายามในการเพิ่มประสิทธิภาพกลับกลายเป็นปัญหาทางกฎหมาย สิทธิความเป็นส่วนตัว และความไว้วางใจของพนักงานอย่างร้ายแรง

การลดความเสี่ยงด้วย Microsoft 365 E3:

ความสามารถในการจัดการอุปกรณ์และแอปพลิเคชันของ Microsoft 365 E3 สามารถช่วยลดความเสี่ยงในสถานการณ์ในสายงานปฏิบัติการเช่นนี้ได้ ด้วย **Microsoft Intune P1** ทีมไอทีของผู้ค้าปลีกสามารถบังคับใช้การป้องกันแอปพลิเคชัน เพื่อช่วยบังคับใช้กฎกับแอปพลิเคชันที่เข้าถึงข้อมูลงาน เช่น การจำกัดการคัดลอก/วาง และการถ่ายโอนข้อมูลไปยังแอปที่ไม่มีการจัดการ หากผู้ค้าปลีกสร้างนโยบายการเข้าถึงแบบมีเงื่อนไขผ่าน **Microsoft Entra ID P1** พวกเขาอาจช่วยบล็อกการลงชื่อเข้าใช้บัญชีองค์กรจากแอปหรืออุปกรณ์ที่ไม่มีการจัดการได้ ในสถานการณ์นี้ หากโทรศัพท์ของผู้จัดการไม่เป็นไปตามข้อกำหนด หรือแอปไม่ได้รับการจัดการ นโยบายเหล่านี้อาจช่วยป้องกันไม่ให้พวกเขาเข้าถึง และอัปโหลดไฟล์บริษัทที่มีการจำกัดการเข้าถึงไปยังแอปพลิเคชัน Shadow AI ได้

ข้อมูลเชิงลึกที่สำคัญ: ในสถานการณ์ทั้งสอง จุดมุ่งหมายของพนักงานเป็นไปในเชิงบวก นั่นคือการปรับปรุงประสิทธิภาพการทำงานด้วย AI อย่างไรก็ตาม ผลลัพธ์อาจเป็นด้านลบได้ หากไม่มีมาตรการป้องกันและนโยบายที่เหมาะสมรองรับ ตัวอย่างเหล่านี้เน้นย้ำให้เห็นว่าการนำ AI มาใช้โดยปราศจากมาตรการป้องกันอาจนำมาซึ่งความเสี่ยงใหม่ ๆ และความเสี่ยงเพิ่มเติมต่อองค์กร เป้าหมายไม่ใช่เพื่อกีดกันการใช้งาน AI แต่เพื่อสนับสนุนการใช้งานอย่างมีความรับผิดชอบ ในส่วนถัดไปจะเป็นการตรวจสอบความสามารถพื้นฐานที่ควรพิจารณา เมื่อประเมินโซลูชันที่อาจช่วยเพิ่มขีดความสามารถด้านผลิตภาพ และขีดความสามารถของ Microsoft 365 E3 ที่ช่วยให้องค์กรกำหนดมาตรการป้องกันเพื่อรักษาข้อมูลที่ละเอียดอ่อนให้อยู่ในช่องทางที่ปลอดภัยและได้รับการอนุมัติ

สร้างรากฐานที่ปลอดภัยและรองรับ AI ด้วย Microsoft 365 E3

องค์กรของคุณพร้อมที่จะปรับขนาด AI แล้วหรือยัง ตรวจสอบรายการตรวจสอบด้านล่างและเรียนรู้ว่า Microsoft 365 E3 สามารถช่วยได้อย่างไร

เมื่อการนำ AI มาใช้มีแนวโน้มเพิ่มขึ้นอย่างรวดเร็ว การประเมินเสถียรภาพการรักษาความปลอดภัยขององค์กร และการระบุช่องโหว่ที่อาจเกิดขึ้นก่อนขยายการใช้งาน AI ถือเป็นสิ่งจำเป็น Microsoft 365 E3 ได้รับการออกแบบให้เป็นพื้นฐานด้านประสิทธิภาพการทำงานและความปลอดภัยที่รองรับ AI โดยผสานเครื่องมือด้านข้อมูลประจำตัว ความปลอดภัย การปฏิบัติตามข้อกำหนด และการจัดการที่หลากหลาย เพื่อช่วยให้องค์กรของคุณขยายการใช้งาน AI ได้อย่างมั่นใจ

ใช้รายการตรวจสอบต่อไปนี้เป็นจุดเริ่มต้น เพื่อทำความเข้าใจสถานะปัจจุบันขององค์กรของคุณ หากมีรายการใดที่ยังไม่ได้ดำเนินการอย่างครบถ้วน องค์กรของคุณอาจได้รับความเสี่ยงที่ไม่จำเป็น

บังคับใช้นโยบายระบบบริหารจัดการตัวตนและการเข้าถึงทรัพยากรที่รัดกุม เช่น การรับรองความถูกต้องโดยใช้หลายปัจจัย (MFA) และการเข้าถึงแบบมีเงื่อนไข

Microsoft 365 E3 ประกอบด้วย **Microsoft Entra ID P1** ซึ่งช่วยให้สามารถบังคับใช้นโยบายระบบบริหารจัดการตัวตน และการเข้าถึงทรัพยากรที่มีความแข็งแกร่งได้ ทั้งในสภาพแวดล้อมระบบคลาวด์และภายในองค์กร โซลูชันอย่างเช่น MFA และนโยบายการเข้าถึงแบบมีเงื่อนไขจะตรวจสอบการลงชื่อเข้าใช้แต่ละครั้ง และจำกัดหรืออนุญาตการเข้าถึงตามเกณฑ์ เช่น บทบาทของผู้ใช้ สภาพการทำงานของอุปกรณ์ และตำแหน่งที่ตั้ง ซึ่งช่วยลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาตและการแบ่งปันข้อมูลโดยไม่จำเป็น ตัวอย่างเช่น คุณสามารถกำหนดสิทธิ์การเข้าถึงแอปพลิเคชัน AI เฉพาะกลุ่มพนักงานที่ระบุ และกำหนดให้ใช้ MFA ในการเข้าสู่ระบบ ซึ่งช่วยลดความเสี่ยงของการถูกบุกรุกบัญชีผู้ใช้ นโยบายการเข้าถึงแบบมีเงื่อนไขสามารถปกป้องข้อมูลสำคัญเพิ่มเติมได้ โดยการป้องกันไม่ให้พนักงานเข้าถึงแอปพลิเคชันที่ไม่ได้รับอนุญาตด้วยข้อมูลรับรองขององค์กร และอุปกรณ์ที่ใช้ร่วมกันสามารถบังคับใช้ข้อกำหนดการลงชื่อออก เพื่อป้องกันการใช้งานเซสชันที่ไม่ได้รับอนุญาต

เปิดใช้งานการทำงานร่วมกันอย่างปลอดภัยบนอุปกรณ์ปลายทางและอุปกรณ์ต่าง ๆ ที่มีการจัดการ

Microsoft 365 E3 มอบความปลอดภัยสำหรับอุปกรณ์ปลายทางแบบอัจฉริยะผ่านโซลูชันต่าง ๆ เช่น **Intune P1**, **Defender for Endpoint P1** และ **Windows E3** เครื่องมือเหล่านี้ช่วยจัดการและเพิ่มความปลอดภัยให้กับพีซี อุปกรณ์เคลื่อนที่ และแอปต่าง ๆ องค์กรสามารถบังคับใช้การกรองเว็บเพื่อบล็อกเว็บไซต์ที่มีความเสี่ยง (รวมถึงเครื่องมือ AI ที่ไม่ได้รับการอนุมัติ) และอัปเดตอุปกรณ์อยู่เสมอด้วยแพตช์ความปลอดภัยผ่าน **Windows Autopatch** และ **Autopilot** มาตรการเหล่านี้ช่วยให้อุปกรณ์มีความปลอดภัย ได้รับการจัดการ และอัปเดตด้วยแพตช์ความปลอดภัยอย่างต่อเนื่อง ซึ่งช่วยลดพื้นผิวของการโจมตี การจัดการอุปกรณ์ปลายทางและการจัดการอุปกรณ์ที่รวมเป็นหนึ่งเดียว ช่วยให้องค์กรสามารถรักษาความปลอดภัยของอุปกรณ์ทำงาน และรักษาความสอดคล้องของแอปพลิเคชัน ไม่ว่าจะเป็นอุปกรณ์ส่วนตัวของพนักงานหรืออุปกรณ์ที่บริษัทจัดหาให้

ปกป้องข้อมูลโดยใช้ฟีเจอร์ต่าง ๆ เช่น ป้ายชื่อระดับความลับ และนโยบายการป้องกันการสูญหายของข้อมูล

Microsoft 365 E3 มีขีดความสามารถหลักของ **Purview** ได้แก่ ป้ายชื่อระดับความลับ การเข้ารหัส และการป้องกันการสูญหายของข้อมูล (DLP) เพื่อปกป้องข้อมูลที่มีความละเอียดอ่อนในเอกสารและอีเมลต่าง ๆ เมื่อเผยแพร่นโยบายป้ายชื่อแล้ว พนักงานสามารถจัดประเภทไฟล์ที่มีข้อมูลทางการเงิน ข้อมูลส่วนบุคคล หรือทรัพย์สินทางปัญญาได้ (เช่น ข้อมูลที่มีป้ายชื่อระดับความลับ "เป็นความลับ") โดยใช้การเข้ารหัสและการควบคุมการเข้าถึง นโยบาย DLP อาจตรวจจับและจำกัดการแชร์ข้อมูลที่ไม่ได้รับอนุญาตใน **Exchange Online และ SharePoint Online/OneDrive for Business** แม้ในขณะที่ใช้ **Microsoft 365 Copilot** การป้องกันเหล่านี้ยังคงมีผลบังคับใช้: Copilot ให้ความสำคัญกับป้ายชื่อระดับความลับสูงสุด และป้องกันไม่ให้ผู้ใช้ที่ไม่มีสิทธิ์เข้าถึงหรือประมวลผลเนื้อหาที่ได้รับการป้องกัน

สามารถติดตามการใช้งานเครื่องมือ AI ที่ไม่ได้รับอนุญาต และดำเนินการอย่างเหมาะสมโดยอิงข้อมูล

Microsoft 365 E3 ประกอบด้วย **Cloud app discovery** ซึ่งช่วยให้คุณเข้าใจว่าแอปพลิเคชัน AI ใดบ้างที่อยู่ระหว่างการใช้งาน (จากแอปที่อยู่ในแคตตาล็อกแอปคลาวด์) ใครเป็นผู้ใช้งาน และคะแนนความเสี่ยงที่เกี่ยวข้อง เพื่อให้คุณสามารถกำหนดแนวทางปฏิบัติที่เหมาะสมตามข้อมูลนั้นได้ หากเห็นว่ามีความเสี่ยงมากเกินไป ฝ่ายไอทีสามารถใช้ **Defender for Endpoint P1** เพื่อจำกัดสิทธิ์ของผู้ใช้ในการเข้าถึง URL ดังกล่าวบนอุปกรณ์ Windows 11 ที่มีการจัดการ ตัวอย่างเช่น หากคุณพบว่าผู้ใช้ 100 รายกำลังใช้เครื่องมือสร้างภาพ AI ที่ฝ่ายไอทียังไม่ได้ทำการตรวจสอบหรืออนุมัติ ฝ่ายไอทีสามารถดำเนินการตรวจสอบเครื่องมือดังกล่าวตามมาตรฐานความปลอดภัยและการปฏิบัติตามกฎระเบียบขององค์กร หากพบว่ามีความเสี่ยง ทีมไอทีสามารถแนะนำทางเลือกที่ได้รับอนุมัติ ขีดความสามารถเหล่านี้ช่วยให้คุณลดความเสี่ยงจาก Shadow AI และตัดสินใจโดยอิงตามข้อมูลเกี่ยวกับการใช้ AI ที่เหมาะสมสำหรับองค์กรของคุณได้

จัดหาแอปพลิเคชัน AI ที่ได้รับอนุมัติ เช่น Microsoft 365 Copilot

การจัดหาแอปพลิเคชัน AI ที่ได้รับอนุมัติจะส่งมอบคุณค่าอย่างมีนัยสำคัญ โดยเปิดโอกาสให้พนักงานเข้าถึงเครื่องมือที่มีประสิทธิภาพและได้รับการอนุมัติ ซึ่งสอดคล้องกับมาตรฐานการรักษาความปลอดภัยและการปฏิบัติตามข้อกำหนดขององค์กร ตัวอย่างเช่น แทนที่พนักงานจะหันไปใช้เครื่องมือสร้างภาพ AI หรือแชทบอทที่ยังไม่ได้รับการตรวจสอบ ฝ่ายไอทีสามารถนำเสนอทางเลือกที่ได้รับอนุมัติ เช่น **Microsoft 365 Copilot** – ซึ่งได้รับการดูแล สนับสนุน และผสานรวมเข้ากับนโยบายที่มีอยู่ของบริษัท **Microsoft 365 Copilot** นำเสนอโซลูชัน AI ที่ปลอดภัยระดับองค์กรซึ่งผสานรวมอย่างลึกซึ้งกับชุดโปรแกรมเพิ่มประสิทธิภาพการทำงาน **Microsoft 365 Copilot** ช่วยให้พนักงานทำงานได้อย่างมีประสิทธิภาพมากขึ้น ทำให้งานประจำเป็นอัตโนมัติ และสร้างข้อมูลเชิงลึก ทั้งหมดนี้โดยยึดหลักตามนโยบายข้อมูลประจำตัวและการคุ้มครองข้อมูลส่วนบุคคล แนวทางนี้จะช่วยลด Shadow IT จำกัดการรั่วไหลของข้อมูล และให้องค์กรสามารถมองเห็นและควบคุมการใช้งาน AI ได้

ความสามารถเหล่านี้ไม่ได้ทำงานแยกกัน แต่ช่วยเสริมซึ่งกันและกันเพื่อสร้างการป้องกันที่ผสมผสานและมีหลายชั้น นโยบายการปกป้องข้อมูลประจำตัว อุปกรณ์ และการคุ้มครองข้อมูลส่วนบุคคลทำงานร่วมกันเพื่อช่วยให้คุณลดภัยคุกคาม เมื่อทีมรักษาความปลอดภัยทราบว่ามีมาตรการควบคุมเช่นนี้อยู่ การรักษาความปลอดภัยก็อาจกลายเป็นตัวสนับสนุนนวัตกรรมมากกว่าที่จะเป็นอุปสรรค

Microsoft 365 E3 ช่วยให้คุณสามารถกำหนดแนวทางป้องกันที่เหมาะสมเพื่อให้องค์กรของคุณนำนวัตกรรม AI มาใช้โดยไม่กระทบต่อการรักษาความปลอดภัย

ก้าวต่อไปบนเส้นทางการปรับใช้ AI

องค์กรต่าง ๆ ล้วนกำลังพยายามค้นหาว่า AI จะช่วยให้บรรลุเป้าหมายได้ดีที่สุดอย่างไร แม้ว่า AI จะมีศักยภาพที่น่าดึงดูดใจ แต่การนำมาใช้ต้องควบคู่ไปกับมาตรการป้องกันที่แข็งแกร่ง ด้วย Microsoft 365 E3 คุณไม่จำเป็นต้องเลือกอย่างใดอย่างหนึ่ง คุณจะได้รับชุดโซลูชันที่ทรงพลัง ซึ่งยกระดับมาตรการรักษาความปลอดภัยและการปฏิบัติตามข้อกำหนด พร้อมช่วยให้องค์กรของคุณนำ AI มาใช้ได้อย่างมั่นใจ

ประเมินความพร้อมด้านการรักษาความปลอดภัย AI ของคุณ

Microsoft มีบริการ **Security for AI Assessment**[3] แบบประเมินออนไลน์นี้ (ที่ security-for-ai-assessment.microsoft.com) จะให้ข้อเสนอแนะเพื่อเสริมสร้างความปลอดภัยของ AI ตามข้อมูลที่คุณให้ไว้ ช่วยให้คุณประเมินความปลอดภัยของ AI ในปัจจุบันของคุณตามเสาหลักสำคัญ 4 ประการ: **เตรียมความพร้อม ค้นหา ปกป้อง** และ **กำกับดูแล** ตลอดจนคำแนะนำที่นำไปปฏิบัติจริง

ศึกษาข้อมูลเพิ่มเติมและร่วมงานกับ Microsoft

ศึกษาข้อมูลเชิงลึกเกี่ยวกับความสามารถของ Microsoft 365 E3 และวิธีที่จะช่วยคุณนำ AI มาใช้ด้วยความมั่นใจ www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab คุณสามารถติดต่อทีมดูแลบัญชี Microsoft หรือคู่ค้าของคุณได้เช่นกัน

1. รายงานดัชนีแนวโน้มการทำงานประจำปี 2025: ปีที่บริษัทแนวหน้าได้ถือกำเนิด Microsoft, Inc., เมษายน 2025. Microsoft ได้วิเคราะห์ข้อมูลจากการสำรวจพนักงานที่ทำงานเต็มเวลาและผู้ประกอบอาชีพอิสระจำนวน 31,000 คน ผู้ปฏิบัติงานในสายงานความรู้ใน 31 ประเทศ ระหว่างวันที่ 6 กุมภาพันธ์ 2025 ถึง 24 มีนาคม 2025, แนวโน้มตลาดแรงงานของ LinkedIn และสัญญาณการทำงานของ Microsoft 365 นับล้านล้านรายการ
2. การศึกษา AI เชิงสร้างใหม่ประจำปีครั้งที่สอง: ผลประโยชน์ทางธุรกิจกับความเสี่ยงด้านความปลอดภัย, iSMG, Inc., กุมภาพันธ์ 2025 จากการสำรวจของผู้เชี่ยวชาญด้านธุรกิจและการรักษาความปลอดภัยทางไซเบอร์กว่า 360 ราย ดำเนินการในไตรมาสที่ 3 ปี 2024
3. การประเมินความปลอดภัยสำหรับ AI: security-for-ai-assessment.microsoft.com/ ความแม่นยำของผลลัพธ์ขึ้นอยู่กับความแม่นยำในการป้อนข้อมูลของคุณ รายงานฉบับนี้มีวัตถุประสงค์เพื่อให้ข้อมูลเท่านั้น และไม่ได้รับประกันประสิทธิภาพหรือผลลัพธ์ ไม่ควรตีความว่าเป็นข้อผูกมัดจาก Microsoft ผลลัพธ์ที่แท้จริงอาจแตกต่างกันไปขึ้นอยู่กับปัจจัยต่าง ๆ เช่น สถานที่ การซื้อ วิธีการ และการใช้งาน Microsoft ไม่รับประกันโดยชัดแจ้งหรือโดยนัยเกี่ยวกับเนื้อหาของรายงานหรือเว็บไซต์นี้
4. สถานการณ์ที่นำเสนอเป็นเพียงเรื่องสมมติและมีวัตถุประสงค์เพื่อประกอบการอธิบายเท่านั้น