Microsoft 365

จากการกำกับดูแลสู่ข้อมูลเชิงลึก: การจัดการความเสี่ยงของ Shadow AI

สารบัญ

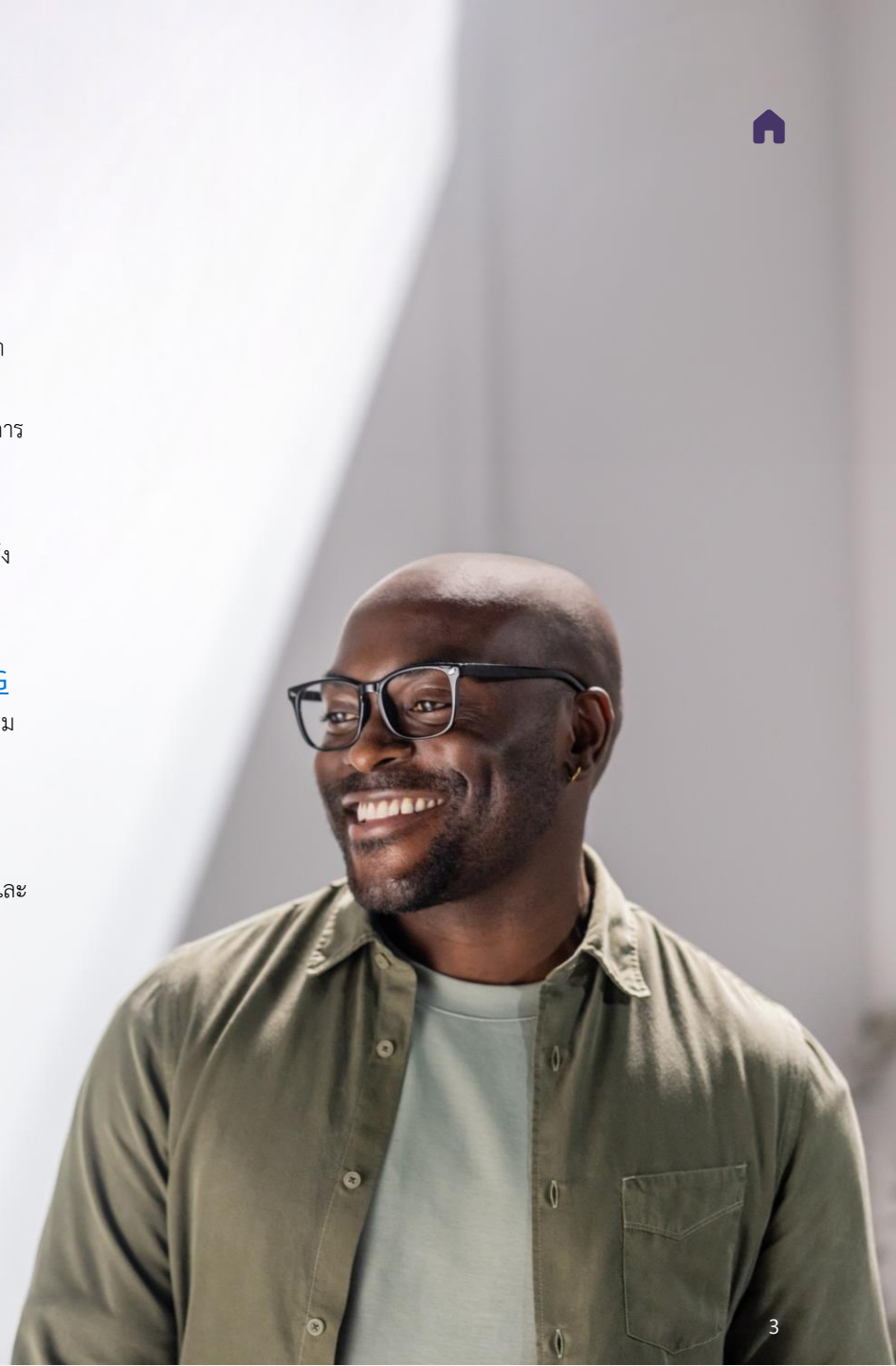
บทนำ

จากรายงานดัชนีแนวโน้มการทำงานล่าสุด พบว่ากว่า 80% ของบุคลากรในสายงานความรู้ที่ทำการสำรวจใน 31 ประเทศ (รวมถึงพนักงานและผู้นำ) รายงานว่าพวกเขารู้สึกไม่มีเวลาหรือพลังงานเพียงพอในการทำงานของตนเอง นอกจากนี้ ผู้นำธุรกิจกว่า 50% ที่ทำการสำรวจ รายงานว่าผลิตภาพที่จำเป็นต่อการเพิ่มขึ้นเพื่อให้บรรลุเป้าหมาย[1] ตาม รายงานดัชนีแนวโน้มการทำงานของ Microsoft ปี 2024 พนักงานจำนวนมากกำลังมองหาเครื่องมือ AI เชิงสร้างใหม่เพื่อแก้ไขช่องว่างนี้ และไม่รอการอนุมัติอย่างเป็นทางการจากฝ่ายไอทีก่อนที่จะเริ่มใช้เครื่องมือเหล่านี้

หากมีการใช้เครื่องมือโดยไม่อยู่ภายใต้การดูแลของฝ่ายไอที อาจก่อให้เกิดความเสี่ยงด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดต่อองค์กรได้ และ Shadow AI ซึ่งเป็นการใช้เครื่องมือ AI โดยไม่ได้รับการอนุมัติจากฝ่ายไอที ก็กำลังกลายมาเป็นรูปแบบล่าสุดของ Shadow IT ในสถานที่ทำงานในปัจจุบัน

เมื่อการนำ AI มาใช้ขยายตัวอย่างรวดเร็ว ผู้นำธุรกิจกำลังเตรียมพร้อมและดำเนินการเพื่อบรรเทาความเสี่ยงที่อาจเกิดขึ้นจากเครื่องมือเหล่านี้ จาก การศึกษาของ iSMG เมื่อเร็ว ๆ นี้พบว่าผู้นำธุรกิจที่เข้าร่วมการสำรวจมากกว่า 70% รายงานว่าการรับรองความเป็นส่วนตัวและความปลอดภัยของข้อมูลเป็นความท้าทายหลักในการผสานรวม AI เชิงสร้างใหม่เข้ากับโครงสร้างพื้นฐานไอทีที่มีอยู่[2] นอกจากนี้ CIO และ CTO ที่เข้าร่วมการสำรวจมากกว่า 90% ระบุว่า AI เชิงสร้างใหม่ได้ขับเคลื่อน หรือจะขับเคลื่อนการลงทุนด้านการรักษาความปลอดภัยทางไซเบอร์เพิ่มมากขึ้นในองค์กรของตน[3]

ในอีบุ๊กนี้ คุณจะได้สำรวจสถานการณ์ทั่วไปที่มีการใช้ Shadow AI, ทำความเข้าใจถึงความเสี่ยงที่อาจเกิดขึ้นกับองค์กร, เรียนรู้ 5 วิธีในการจัดการความเสี่ยงเหล่านั้น และดูว่า Microsoft 365 E3 สามารถช่วยได้อย่างไร



[1] รายงานดัชนีแนวโน้มการทำงานปี 2025, Microsoft Inc., เมษายน 2025. Microsoft วิเคราะห์ข้อมูลการสำรวจพนักงานในสายงานความรู้ที่ทำงานเต็มเวลาหรือประกอบอาชีพอิสระจำนวน 31,000 คน ใน 31 ประเทศ ระหว่างวันที่ 6 กุมภาพันธ์ 2025 ถึง 24 มีนาคม 2025, แนวโน้มตลาดแรงงานของ LinkedIn และสัญญาณด้านประสิทธิภาพการทำงานของ Microsoft 365 นับล้านล้านรายการ

[2] การศึกษา AI เชิงสร้างใหม่ประจำปีครั้งที่ 2 ของ iSMG: รางวัลทางธุรกิจเทียบกับความเสี่ยงด้านความปลอดภัย, อ้างอิงจากผลสำรวจของผู้เชี่ยวชาญด้านธุรกิจและการรักษาความปลอดภัยทางไซเบอร์กว่า 360 คนในไตรมาสที่ 3 จากภูมิภาค 6 แห่ง (อเมริกาเหนือ ยุโรป เอเชีย อเมริกาใต้ ออสเตรเลีย และแอฟริกา)

[3] การสร้างสมดุลด้านความปลอดภัยของ AI: จากความเสี่ยงสู่นวัตกรรม" NTT DATA, มิถุนายน 2025, อ้างอิงตามข้อมูลจากผลสำรวจของ NTT DATA จากผู้มีอำนาจตัดสินใจด้าน GenAI ระดับอาวุโสกว่า 2,300 ราย ซึ่งประกอบด้วยผู้นำระดับ C-Suite จำนวน 1,500 รายใน 34 ประเทศ

Shadow AI คืออะไร และทำไมการมองเห็นได้จึงมีความสำคัญ

Shadow AI หมายถึงการใช้เครื่องมือและแอปพลิเคชันปัญญาประดิษฐ์โดยพนักงาน โดยไม่ได้รับการอนุมัติหรือการกำกับดูแลอย่างชัดเจนจากฝ่ายไอที ซึ่งมักเกิดขึ้นนอกเหนือขอบเขตการดูแลด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดอย่างเป็นทางการ เมื่อพนักงานมองหาวิธีเพิ่มประสิทธิภาพการทำงาน และรับมือกับความต้องการที่เพิ่มขึ้นในปริมาณงานของตน พวกเขาอาจเลือกใช้โซลูชันที่ไม่ได้รับการอนุมัติเหล่านี้ เพื่อปรับปรุงกระบวนการทำงาน ทำงานร่วมกัน หรือสร้างเนื้อหาใหม่เป็นประจำ โดยไม่ได้ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้น Shadow AI ไม่สามารถมองเห็นได้โดยฝ่ายไอที ทำให้องค์กรต่าง ๆ พบว่าเป็นเรื่องยากที่จะทราบว่ามีการใช้แอปพลิเคชันใดและแอปพลิเคชันใดก่อให้เกิดความเสี่ยงมากที่สุด

ทำไมการมองเห็น Shadow AI ได้จึงมีความสำคัญ

เมื่อฝ่ายไอทีไม่ทราบถึงการใช้งานแอปพลิเคชันหรือบริการใด ๆ ก็จะไม่สามารถรักษาความปลอดภัยหรือให้การสนับสนุนได้ *ช่องว่างด้านการมองเห็นได้* นี้ทำให้เป็นเรื่องยากต่อการระบุ จัดการ หรือบรรเทาภัยคุกคามที่อาจเกิดขึ้นได้อย่างแม่นยำ ซึ่งเกี่ยวข้องกับการเปิดเผยข้อมูลที่ละเอียดอ่อน การไม่ปฏิบัติตามกฎระเบียบ และการสูญเสียการควบคุมข้อมูลที่เป็นกรรมสิทธิ์ ผู้นำด้านไอทีและธุรกิจจำเป็นต้องมีความสามารถในการตรวจสอบการใช้ Shadow AI ในองค์กรของตน จัดการกับความเสี่ยงใหม่ ๆ ที่เกิดจากการใช้ AI และตัดสินใจว่าควรอนุญาตให้ใช้เครื่องมือใดโดยมีกรอบการกำกับดูแลที่เหมาะสม โอกาสสำหรับองค์กรคือการเปลี่ยน Shadow AI จากความเสี่ยงให้กลายเป็นโอกาสในการพัฒนาวิธีการทำงานใหม่ ๆ อย่างปลอดภัย ในการดำเนินการนี้ องค์กรควรสร้างสมดุลที่เหมาะสม โดยเปิดโอกาสให้พนักงานใช้เครื่องมือ AI ที่มีประโยชน์ภายใต้กรอบการกำกับดูแลและรักษาความปลอดภัย เพื่อบรรเทาความเสี่ยงที่อาจเกิดขึ้น

ข้อมูลเชิงลึก

คุณไม่สามารถรักษาความปลอดภัยในสิ่งที่คุณมองไม่เห็นได้ เมื่อฝ่ายไอทีไม่ทราบว่ามีการใช้งานแอปพลิเคชันหรือบริการใดอยู่ ก็จะไม่สามารถรักษาความปลอดภัยให้กับสิ่งนั้นได้ นี่คือหัวใจของปัญหา Shadow AI และเน้นย้ำว่าเหตุใดจึงจำเป็นต้องใช้แนวทางใหม่ การห้ามใช้เครื่องมือจากภายนอกทั้งหมดนั้นไม่ใช่วิธีที่นำไปใช้ได้จริง หากพนักงานรู้สึกว่าเครื่องมือ AI เหล่านี้มีความสำคัญต่อการบรรลุเป้าหมายของตน ดังนั้น องค์กรควรเปิดเผยการใช้ Shadow AI เพื่อให้มองเห็นได้ว่าพนักงานกำลังใช้เครื่องมือใดบ้าง กำหนดมาตรการควบคุมที่เหมาะสม และนำเสนอทางเลือกที่ปลอดภัยและได้รับการอนุมัติ ซึ่งตอบโจทย์ความต้องการขององค์กร กล่าวสั้น ๆ คือ ความท้าทายคือการเสริมศักยภาพให้ทีมด้วย AI *โดยไม่*ลดทอนการรักษาความปลอดภัย

Shadow AI ในสถานที่ทำงาน: ตัวอย่างสถานการณ์และความเสี่ยงที่อาจเกิดขึ้น

Shadow AI เกิดขึ้นจากพนักงานที่ต้องการเพิ่มประสิทธิภาพและผลลัพธ์ในการทำงาน หรือทดลองใช้เทคโนโลยีใหม่ ต่อไปนี้เป็นตัวอย่างสมมติหลาย ๆ กรณีเพื่อแสดงให้เห็นว่าอาจมีการนำเครื่องมือ AI ที่ไม่ได้รับอนุญาตไปใช้ได้อย่างไร และความเสี่ยงที่อาจเกิดขึ้นจากการใช้งานเหล่านั้น:

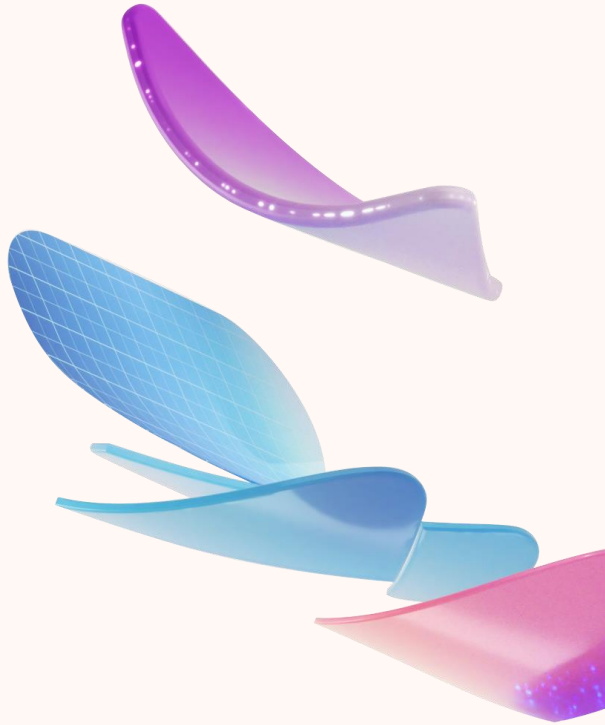
บทบาท	สถานการณ์ตัวอย่าง	ความเสี่ยงที่อาจเกิดขึ้นจากเครื่องมือที่ไม่ได้รับอนุญาต
การตลาด	การใช้เครื่องมือสร้างเนื้อหา AI เชิงสร้างใหม่เพื่อสร้างข้อความทางการตลาดหรือการออกแบบโดยใช้ข้อมูลแบรนด์ของบริษัท	การรั่วไหลของข้อมูลแบรนด์หรือผลิตภัณฑ์ที่มีความละเอียดอ่อน การสูญเสียการควบคุมว่าบริการ AI ภายนอกอาจจัดเก็บหรือใช้สินทรัพย์ที่สร้างสรรค์ของบริษัทอย่างไร
การเงิน	การอัปโหลดข้อมูลทางการเงินขององค์กรเข้าสู่บริการวิเคราะห์ หรือการแสดงภาพที่ขับเคลื่อนด้วย AI เพื่อให้ได้ข้อมูลเชิงลึกอย่างรวดเร็ว	การเปิดเผยข้อมูลทางการเงินที่เป็นความลับ (งบประมาณ การคาดการณ์) กับบุคคลที่สาม อาจมีความเสี่ยงต่อการละเมิดข้อกำหนดการปฏิบัติตามกฎระเบียบ (เช่น GDPR) หากมีการรวมข้อมูลลูกค้าหรือพนักงานโดยไม่มีการปกป้องที่เหมาะสม
ฝ่ายสนับสนุนลูกค้า	การนำข้อมูลลูกค้าหรือบันทึกการแชทจากฝ่ายสนับสนุนเข้าสู่เครื่องมือ AI เพื่อร่างคำตอบหรือสรุปกรณีต่าง ๆ	การละเมิดกฎความเป็นส่วนตัวและการจัดการข้อมูล ซึ่งข้อมูลของลูกค้าที่ละเอียดอ่อนอาจถูกจัดเก็บไว้ภายนอกระบบของบริษัท ไม่มีการรับประกันการเก็บรักษาข้อมูล หรือการลบข้อมูลอย่างถูกต้องโดยผู้ให้บริการ AI
พนักงานส่วนหน้า – การค้าปลีก	ผู้จัดการร้านค้าใช้แอป AI เพื่อจัดตารางเวลากะพนักงานบนโทรศัพท์ของตนเพื่อเพิ่มประสิทธิภาพการจัดกะทำงานของพนักงาน	ข้อมูลพนักงานของบริษัท (ชื่อพนักงาน ตารางเวลา) ถูกอัปโหลดไปยังแอปที่ไม่ได้รับการอนุมัติ ซึ่งเสี่ยงต่อปัญหาด้านความเป็นส่วนตัว อาจเกิดปัญหาตารางเวลาที่ขัดแย้งหรือการละเมิดนโยบายขึ้นได้ หากข้อเสนอแนะของ AI ไม่สอดคล้องกับกฎระเบียบด้านแรงงาน
พนักงานส่วนหน้า – การดูแลสุขภาพ	พยาบาลหรือแพทย์ที่ใช้แชทบอท AI เพื่อช่วยร่างบันทึกการดูแลผู้ป่วยหรือตอบคำถามทางการแพทย์	ข้อมูลสุขภาพของผู้ป่วย (PHI) อาจถูกเปิดเผยต่อบริการภายนอกโดยไม่มีมาตรการป้องกัน ซึ่งถือเป็นการละเมิดข้อกำหนดด้านการปฏิบัติตามและการรักษาความลับ นอกจากนี้ คำแนะนำทางการแพทย์ของ AI อาจยังไม่ผ่านการตรวจสอบ และอาจก่อให้เกิดความเสี่ยงด้านความปลอดภัย

ในกรณีแต่ละอย่างข้างต้น พนักงานแต่ละคนมีเจตนาดีและต้องการเพิ่มประสิทธิภาพในการทำงาน แต่สุดท้ายองค์กรอาจต้องเผชิญกับความเสี่ยงที่ตามมา

ข้อมูลของบริษัทอาจถูกกระจายไปยังแพลตฟอร์มที่ไม่ได้รับอนุญาต สร้าง *ปัญหาด้านการกำกับดูแลข้อมูล* แอปที่ไม่ได้รับการตรวจสอบอาจนำมัลแวร์หรือช่องโหว่ด้านความปลอดภัยเข้ามา ขยายพื้นผิวของการโจมตีไปยังพื้นที่ที่อยู่นอกการควบคุมของฝ่ายไอที อาจมีผลกระทบต่อการปฏิบัติตามกฎระเบียบด้วย จากมุมมองของฝ่ายสนับสนุนด้านไอที หากเกิดปัญหากับเครื่องมือ Shadow AI เจ้าหน้าที่ให้ความช่วยเหลืออาจไม่สามารถช่วยเหลือผู้ใช้ได้ เนื่องจากไม่มีข้อมูลหรือการควบคุมเครื่องมือดังกล่าว

5 วิธีในการจัดการความเสี่ยงของ Shadow AI

ด้วยกลยุทธ์และเครื่องมือที่เหมาะสม คุณสามารถเปลี่ยน Shadow AI จากภัยคุกคามที่อาจเกิดขึ้นให้กลายเป็นโอกาสในการส่งเสริมวัฒนธรรมแห่งนวัตกรรมที่ปลอดภัย เสริมศักยภาพให้ทีมของคุณด้วยเครื่องมือ AI ที่ช่วยเพิ่มประสิทธิภาพการทำงาน *ขณะเดียวกัน* ก็ยังคงมีการกำกับดูแลที่จำเป็นเพื่อปกป้องธุรกิจของคุณ นี่คือการเปลี่ยนจากการพูดว่า “ไม่ ไม่มีทาง” ไปสู่การพูดว่า “ใช่ แต่ต้องมีมาตรการป้องกันที่เหมาะสม” เคล็ดลับทั้ง 5 ข้อต่อไปนี้ออกแบบมาเพื่อช่วยให้คุณจัดการและควบคุม Shadow AI ในองค์กร:



01 ค้นพบร่องรอยการใช้ Shadow AI ในองค์กร เพื่อประเมินและจัดลำดับความสำคัญของความเสี่ยง

คุณไม่สามารถป้องกันในสิ่งที่คุณมองไม่เห็นได้ ตรวจสอบการใช้งานแอปพลิเคชันในองค์กรจากบันทึกกิจกรรม เมื่อคุณทราบว่ามีการใช้งานแอปใดอยู่ คุณสามารถระบุเครื่องมือที่เหมาะสมเพื่อจัดการข้อมูลที่ละเอียดอ่อน พร้อมทั้งระบุแอปที่ไม่สอดคล้องกับนโยบายการรักษาความปลอดภัยและการปฏิบัติตามข้อบังคับ ด้วยข้อมูลเชิงลึกเหล่านี้ คุณจึงสามารถตัดสินใจได้ดีขึ้นว่าคุณต้องการอนุญาต ตรวจสอบ หรือจำกัดแอปพลิเคชันใดบ้างเพื่อบรรเทาความเสี่ยงที่อาจเกิดขึ้น

02 ดำเนินการมาตรการที่ให้ผลลัพธ์รวดเร็วด้วยนโยบายการรักษาความปลอดภัยและการปฏิบัติตามข้อบังคับ

ใช้หรือดำเนินการแก้ไขนโยบายเพื่อบรรเทาความเสี่ยงที่อาจเกิดขึ้นจากการใช้ Shadow AI คุณสามารถใช้นโยบายการเข้าถึงแบบมีเงื่อนไขเพื่อจำกัดการใช้งานแอปพลิเคชันที่มีความเสี่ยงสูง ใช้นโยบายการป้องกันการสูญหายของข้อมูลสำหรับข้อมูลที่มีความละเอียดอ่อน เพื่อลดการเปิดเผยข้อมูลมากเกินไปและการรั่วไหลของข้อมูล และบังคับใช้การรับรองความถูกต้องโดยใช้หลายปัจจัย และการปฏิบัติตามข้อกำหนดของอุปกรณ์สำหรับผู้ใช้ทุกคน ขั้นตอนเหล่านี้จะช่วยลดความเสี่ยงที่เห็นชัดเจนที่สุดได้อย่างรวดเร็ว แม้ว่าคุณจะยังไม่มีข้อมูลครบถ้วนเกี่ยวกับแอปพลิเคชัน AI ที่กำลังใช้งานอยู่ก็ตาม

03 ให้ข้อมูลและความรู้แก่พนักงานเกี่ยวกับความเสี่ยงของ Shadow AI ที่อาจเกิดขึ้น

บ่อยครั้งที่พนักงานไม่ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นกับองค์กรจากการใช้เครื่องมือ AI ที่ไม่ได้รับอนุญาต สื่อสารถึงความเสี่ยงของ Shadow AI อย่างสม่ำเสมอ โดยใช้การแจ้งเตือน การป้องกันการสูญหายของข้อมูลที่เหมาะสม การเตือนนโยบายของบริษัท และการฝึกอบรมสั้น ๆ เพื่อชี้นำผู้ใช้ไปสู่แนวทางปฏิบัติที่ปลอดภัยยิ่งขึ้น โดยไม่ต้องใช้มาตรการบังคับที่เข้มงวด

04 จัดหาเครื่องมือ AI ที่ได้รับการอนุมัติเพื่อลดความเสี่ยงเพิ่มเติม

หากเป็นไปได้ ควรจัดหาเครื่องมือ AI ที่ได้รับการอนุมัติให้พนักงานใช้เป็นทางเลือกแทนเครื่องมือที่ไม่ได้รับอนุญาต วิธีที่ยอดเยี่ยมในการลดปัญหา Shadow AI คือการตอบสนองรูปแบบการใช้ที่พบบ่อยที่สุดในองค์กรด้วยโซลูชันที่ได้รับการอนุมัติ ซึ่งช่วยให้ฝ่ายไอทีสามารถรักษาการมองเห็นได้และการควบคุม พร้อมทั้งให้การสนับสนุนผู้ใช้สำหรับปัญหาที่เกิดขึ้น

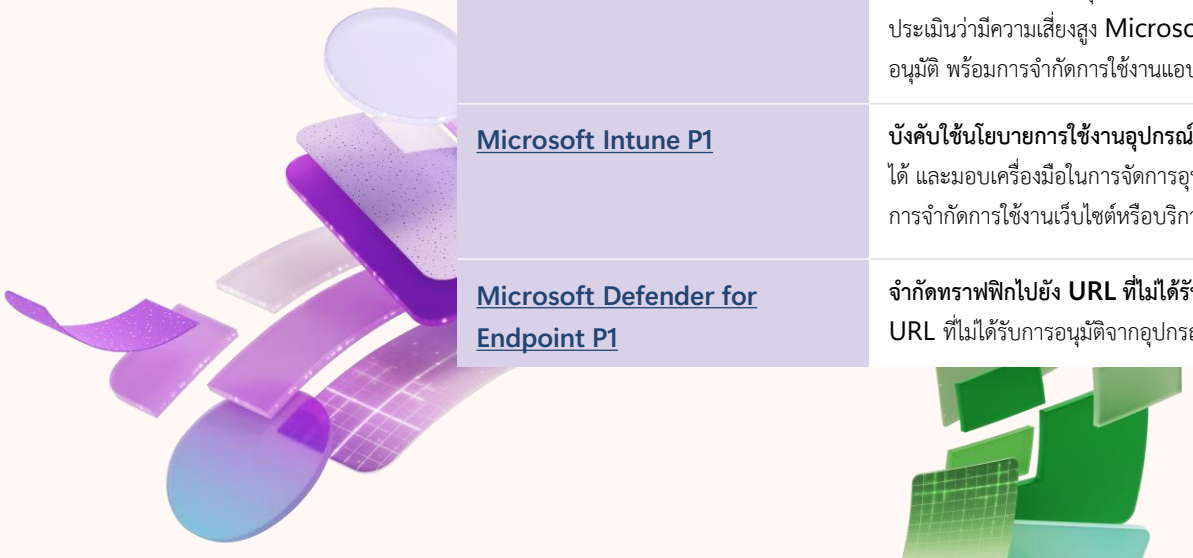
05 สร้างการกำกับดูแลอย่างต่อเนื่อง

ผสานรวมการตรวจสอบเข้ากับกิจวัตรการกำกับดูแลด้านไอที โดยตรวจสอบบันทึกกิจกรรมและรายงานอย่างสม่ำเสมอ ปรับปรุงนโยบายเมื่อมีบริการ AI ใหม่ ๆ ปรากฏขึ้น และแจ้งให้ผู้นำทราบถึงความคืบหน้า (เช่น การลดการใช้แอปที่ไม่ได้รับการอนุมัติหรือเหตุการณ์ที่ป้องกันไว้ได้) การทำเช่นนี้จะช่วยให้คุณลดความเสี่ยงที่อาจเกิดขึ้นได้ทั้งในปัจจุบันและอนาคตเมื่อสภาพแวดล้อมมีการเปลี่ยนแปลง

ด้วยการดำเนินการตามขั้นตอนข้างต้น คุณสามารถเสริมสร้างทั้งนวัตกรรมและการรักษาความปลอดภัยได้ พนักงานสามารถใช้โซลูชัน AI ที่ได้รับการอนุมัติเพื่อทำงานได้ และฝ่ายไอทียังคงควบคุมและดูแลการปฏิบัติตามข้อกำหนดสำหรับเครื่องมือเหล่านั้น

ค้นพบและจัดการความเสี่ยงของ Shadow AI ด้วย Microsoft 365 E3

Microsoft 365 E3 มอบขีดความสามารถให้แก่องค์กรในการค้นหา Shadow IT ประเมินความเสี่ยงที่อาจเกิดขึ้น และดำเนินนโยบายด้านการรักษาความปลอดภัยและการปฏิบัติตามข้อบังคับ โดยไม่เป็นอุปสรรคต่อการสร้างนวัตกรรม ชุดความสามารถด้านประสิทธิภาพการทำงาน การรักษาความปลอดภัย และการจัดการแบบผสานรวมนี้สามารถช่วยให้คุณรับมือกับความท้าทายของ Shadow AI ได้โดยตรง



Microsoft 365 E3 Solution	โซลูชันนี้ช่วยให้คุณจัดการความเสี่ยงที่อาจเกิดขึ้นจาก Shadow AI ได้อย่างไร
Cloud App Discovery	**ค้นพบและดำเนินการกับแอปพลิเคชันที่ไม่ได้รับอนุญาต** Cloud App Discovery ช่วยให้คุณอัปโหลดบันทึกกิจกรรมและสร้างรายงานแบบสแนปช็อต เพื่อให้เห็นภาพรวมการใช้งานแอปบนระบบคลาวด์มากกว่า 31,000 รายการ รวมถึงแอปพลิเคชัน AI เชิงสร้างใหม่กว่า 400 รายการ คุณสามารถตรวจสอบได้ว่ามีการใช้งานอะไรบ้างในองค์กร ใครเป็นผู้ใช้งาน และมีความถี่ในการใช้งานมากน้อยเพียงใด ข้อมูลนี้ช่วยให้คุณสามารถการตัดสินใจอย่างรอบรู้ว่าควรอนุญาตหรือจำกัดการใช้งานแอปใดบ้าง
Microsoft Purview Data Loss Prevention (DLP)	**ลดความเสี่ยงในการรั่วไหลของข้อมูลที่ละเอียดอ่อน** Microsoft Purview DLP ช่วยให้คุณสามารถสร้างและดำเนินนโยบายที่ตรวจจับข้อมูลที่ละเอียดอ่อน และบล็อกหรือจำกัดการแชร์ข้อมูลผ่านบริการ Microsoft 365 สำหรับอีเมลและไฟล์ได้ ตัวอย่างเช่น คุณสามารถกำหนดกฎเพื่อเฝ้าระวัง ตรวจสอบ หรือหยุดผู้ใช้ไม่ให้แชร์ข้อมูลที่ละเอียดอ่อนผ่านอีเมลหรือการแชร์ไฟล์ พร้อมแจ้งเตือนผู้ใช้
Microsoft Entra ID P1	**จัดการการเข้าถึงแอประบบคลาวด์** Microsoft Entra ID P1 เปิดใช้งานนโยบายการเข้าถึงแบบมีเงื่อนไข เพื่อกำหนดว่าใครที่สามารถเข้าถึงแอปพลิเคชันใด ภายใต้เงื่อนไขใด ตัวอย่างเช่น คุณสามารถกำหนดให้ต้องมีการรับรองความถูกต้องโดยใช้หลายปัจจัย หรือแม้แต่จำกัดการเข้าสู่ระบบด้วยข้อมูลประจำตัวขององค์กรสำหรับแอปที่คุณประเมินว่ามีความเสี่ยงสูง Microsoft Entra ID P1 มอบการเข้าถึงทรัพยากรระบบคลาวด์ให้กับบุคคลที่เหมาะสม บนอุปกรณ์ที่ผ่านการตรวจสอบ ภายใต้เงื่อนไขที่ได้รับอนุมัติ พร้อมการจำกัดการใช้งานแอปที่ไม่ได้รับการอนุมัติ
Microsoft Intune P1	**บังคับใช้นโยบายการใช้งานอุปกรณ์และแอป** Microsoft Intune P1 ช่วยให้คุณสามารถอนุญาตให้นำอุปกรณ์ที่มีการจัดการและปฏิบัติตามข้อกำหนดมาใช้ในการทำงานได้ และมอบเครื่องมือในการจัดการอุปกรณ์เหล่านั้นให้กับคุณ ตัวอย่างเช่น ระบบนี้สามารถป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตบนพีซีขององค์กร หรือกำหนดค่าเพื่อการจำกัดการใช้งานเว็บไซต์หรือบริการเฉพาะ
Microsoft Defender for Endpoint P1	**จำกัดทราฟฟิกไปยัง URL ที่ไม่ได้รับการอนุมัติ** Microsoft Defender for Endpoint P1 ช่วยลดความเสี่ยงจากเว็บไซต์ที่คุณมองว่าเสี่ยง โดยบล็อกการเข้าถึง URL ที่ไม่ได้รับการอนุมัติจากอุปกรณ์ที่มีการจัดการ ตัวอย่างเช่น พนักงานที่พยายามเข้าเว็บไซต์ AI ที่มีความเสี่ยงบนแล็ปท็อปของบริษัท จะถูกบล็อกไม่ให้เข้าถึงเว็บไซต์นั้น

ก้าวต่อไปในการเดินทางสู่การนำ AI มาใช้ →

ทุกอย่างเริ่มต้นด้วยการตระหนักรู้ เครื่องมือที่เหมาะสม และแผนงานเชิงรุก Microsoft 365 E3 มีเครื่องมือที่ช่วยให้องค์กรของคุณสร้างรากฐานการรักษาความปลอดภัย และกรอบงานการกำกับดูแลที่มีประสิทธิภาพสำหรับโซลูชัน AI คุณจะสามารถตรวจสอบเครื่องมือที่ไม่ได้รับอนุญาต เปิดใช้งานนโยบายต่าง ๆ เพื่อปกป้องข้อมูลที่ละเอียดอ่อน และรักษาการควบคุมทั้งการเข้าถึงของผู้ใช้และการรักษาความปลอดภัยของอุปกรณ์ เตรียมพร้อมที่จะเปลี่ยนจากแนวทางการแบบเชิงรับ (ค้นหาและบล็อก Shadow AI หลังจากที่มันปรากฏขึ้น) ไปสู่แนวทางเชิงรุกมากขึ้นในการแนะนำการใช้งาน AI ให้เป็นช่องทางที่ปลอดภัยและได้รับการจัดการ ทำ การประเมินความปลอดภัยสำหรับ AI และเรียนรู้ว่า คุณสามารถปรับปรุงมาตรการรักษาความปลอดภัยสำหรับ AI ได้อย่างไร เรียนรู้เพิ่มเติมเกี่ยวกับความสามารถที่รวมอยู่ใน Microsoft 365 for Enterprise