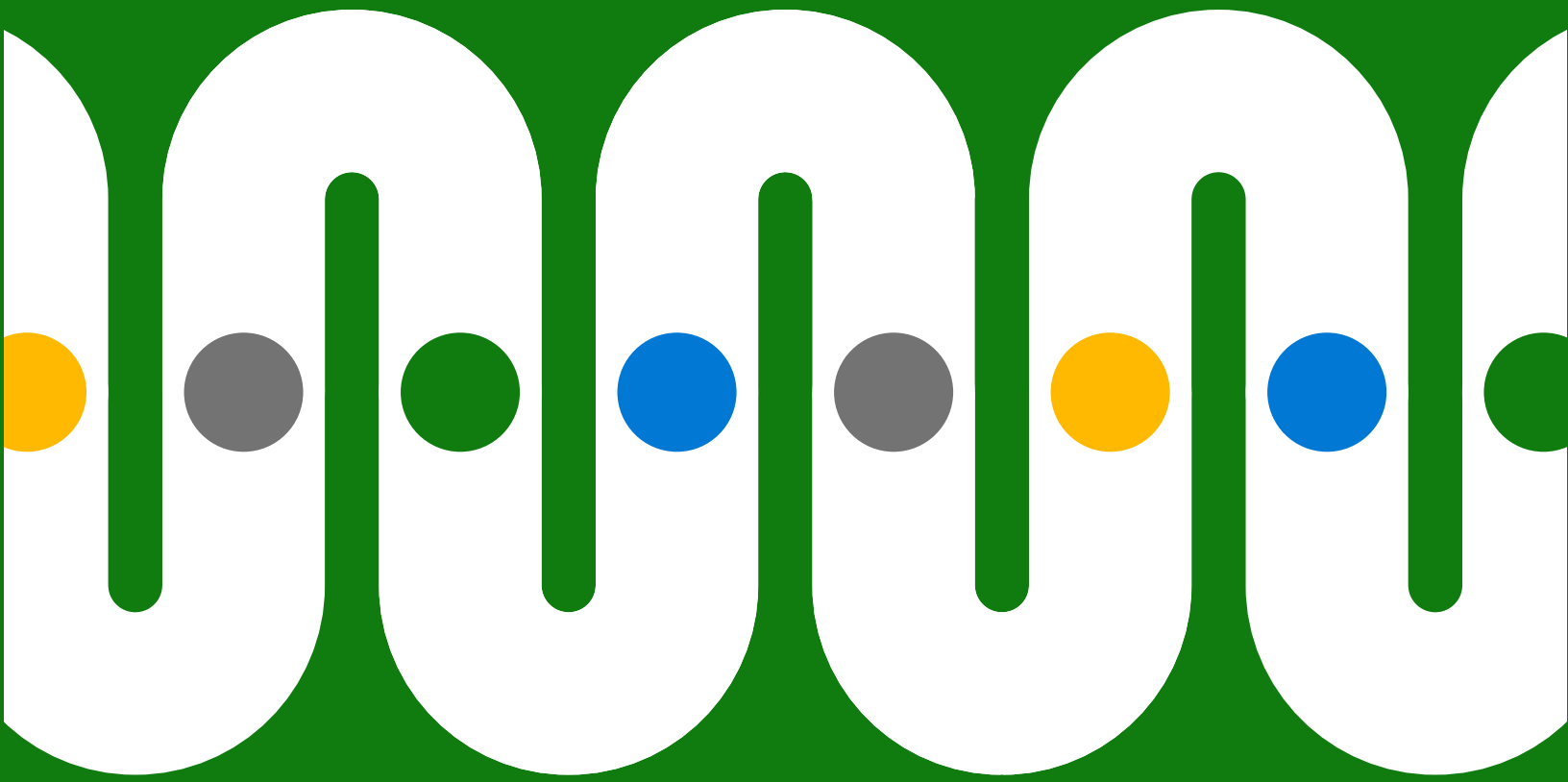
Microsoft Security

3 ขั้นตอนในการปกป้องข้อมูลของคุณแบบครบวงจร



สารบัญ

แบบสำรวจของผู้ตัดสินใจในการปฏิบัติตามกฎระเบียบแสดงให้เห็นว่า 95% มีความกังวลเกี่ยวกับความท้าทายในการปกป้องข้อมูล[2]

ข้อมูลเบื้องต้น

องค์กรต่างๆ ได้เห็นฟุตพรินต์ของระบบดิจิทัลเพิ่มขึ้นอย่างมาก พร้อมด้วยการทำงานแบบไฮบริด ซึ่งเป็นการทำงานที่ขยายไปไกลกว่าแค่ในออฟฟิศแบบเดิมๆ

ซึ่งนำไปสู่การแยกส่วนและการกรองข้อมูลที่มากขึ้น ดดยทั้งหมดนี้มีความซับซ้อนอันเนื่องมาจากการเติบโตอย่างรวดเร็วของแอปพลิเคชัน อุปกรณ์ และสถานที่ต่างๆ มากมาย นอกจากนี้ พนักงานหลายคนยังเปลี่ยนบทบาทเพื่อค้นหาการบรรลุเป้าหมายหรือความยืดหยุ่นที่มากขึ้น และนั่นทำให้มีความท้าทายเหล่านี้เพิ่มเข้ามา ซึ่งทำให้เกิดจุดบอดใหม่ๆ ในฐานข้อมูลที่เติบโตขึ้นเรื่อยๆ[1]

ปัจจัยทั้งหมดเหล่านี้มี CIO และ CISO คอยทบทวนแนวทางในการปกป้องข้อมูล จากการสำรวจที่ติดตามผู้มีอำนาจตัดสินใจด้านการปฏิบัติตามกฎระเบียบของสหรัฐฯ กว่า 500 ราย เกือบทั้งหมด (ร้อยละ 95) มีความกังวลเกี่ยวกับความท้าทายในการปกป้องข้อมูล[2]

[1] "How Microsoft can help reduce insider risk during the Great Reshuffle, Alym Rayani", Microsoft Security 28 กุมภาพันธ์ 2022

[2] "September 2021 survey of 512 US compliance decision-makers commissioned by Microsoft from Vital Findings"

ทีมไอทีและทีมรักษาความปลอดภัยกำลังมองหาวิธีที่ดีกว่าในการจัดการวงจรชีวิตข้อมูลทั้งหมด ทั่วทั้งสภาพแวดล้อมระบบมัลติคลาวด์ สภาพแวดล้อมระบบคลาวด์แบบไฮบริด และสภาพแวดล้อมภายในองค์กร วิธีการแบบครบวงจรนี้เกี่ยวข้องกับขั้นตอนสำคัญๆ สามขั้นตอน ดังนี้

ขั้นตอนที่ 1: ระบุข้อมูล

กำหนดว่าข้อมูลของคุณอยู่ที่ใด เป็นข้อมูลประเภทใด และนำไปใช้หรือแชร์อย่างไร

ขั้นตอนที่ 2: จัดประเภทข้อมูล

จัดประเภทและติดป้ายกำกับข้อมูลเพื่อให้คุณทราบนโยบายที่เหมาะสมและการลดความเสี่ยงที่จะนำไปใช้

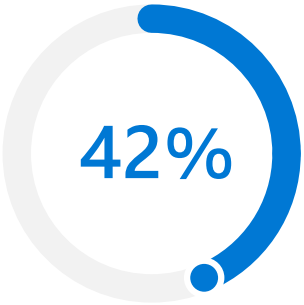
ขั้นตอนที่ 3: ป้องกันข้อมูลสูญหาย

สร้างความสมดุลระหว่างการลดความเสี่ยงและความยืดหยุ่นสำหรับบุคลากรของคุณด้วยการตรวจจับและการควบคุมอัจฉริยะ

เป้าหมายของแนวทางนี้? เพื่อปิดช่องโหว่และลดความเสี่ยงโดยไม่สูญเสียประสิทธิภาพการทำงาน

ขั้นที่ 1

ระบุข้อมูล



เมื่อถูกถามว่าข้อมูลของพวกเขา “มืดมน” มากน้อยเพียงใด 42% ขององค์กรตอบว่าอย่างน้อยก็ครึ่งหนึ่ง[3]

ข้อมูลที่ “ซ่อนอยู่” นี้มีหลายรูปแบบ ตั้งแต่ไฟล์แนบในอีเมลและบันทึกการโทรของลูกค้าไปจนถึงบันทึกการทำงานของเครื่องและฟุตเทจวิดีโอ

หากคุณไม่สามารถระบุข้อมูลของคุณได้ว่าข้อมูลอยู่ที่ใด เป็นข้อมูลประเภทใด และมีวิธีการใช้งานหรือแชร์ข้อมูลอย่างไร คุณจะไม่สามารถใช้นโยบายหรือการป้องกันที่เหมาะสมได้

องค์กรสมัยใหม่สร้างข้อมูลจำนวนมหาศาลอย่างต่อเนื่อง ไม่ใช่แค่เอกสาร อีเมล และข้อความเท่านั้น แต่ทุกอย่างตั้งแต่ฟุตเทจการรักษาความปลอดภัยไปจนถึงข้อมูลตำแหน่งทางภูมิศาสตร์ ทั้งหมดนี้ประกอบขึ้นด้วยการเพิ่มจำนวนทั่วทั้งแอป อุปกรณ์ และพื้นที่เก็บข้อมูล ทั้งภายในองค์กรและในระบบคลาวด์

การระบุข้อมูลทั้งหมดนี้อาจเป็นเรื่องยาก และ 42 เปอร์เซ็นต์ขององค์กรกล่าวว่า ข้อมูลอย่างน้อยครึ่งหนึ่งของพวกเขา “มืดมน”[3] นั่นหมายความว่า มีข้อมูลที่รวบรวมเอาไว้ แต่เป็นข้อมูลที่ไม่สามารถระบุได้หรือไม่ได้ใช้เพื่อวัตถุประสงค์ทางธุรกิจ บางครั้งข้อมูลจะมืดมนเมื่อผู้ปฏิบัติงานที่สร้างข้อมูลนั้นเปลี่ยนโครงการหรือบทบาท บ่อยครั้งที่ไม่มีระบบที่ใช้ระบุข้อมูล ณ จุดที่สร้างหรือแก้ไข

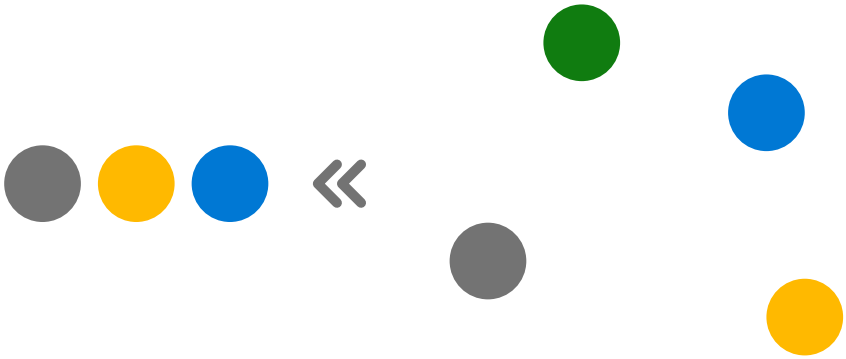
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group กรกฎาคม 2022

ต้องการสร้างเวิร์กโฟลว์การค้นหาแบบครบวงจรบนแพลตฟอร์มเดียวหรือไม่

เรียนรู้เกี่ยวกับการค้นพบข้อมูลใน Microsoft Purview ที่ **Microsoft.com**

ความท้าทายนี้มีแต่จะเพิ่มขึ้นเท่านั้น จำนวนข้อมูลใหม่ที่ถูกสร้างขึ้นมาถูกบันทึก ทำซ้ำ และใช้งานนั้น คาดว่าจะเพิ่มขึ้นกว่าสองเท่าภายในปี 2026 โดยข้อมูลองค์กรเติบโตเร็วกว่าข้อมูลผู้บริโภคมากกว่าสองเท่า[4]

ปัญญาประดิษฐ์ (AI) และการเรียนรู้ของเครื่อง (ML) สามารถช่วยได้โดยการจดจำข้อมูลที่ละเอียดอ่อน เช่น ที่อยู่อีเมล ข้อมูลสุขภาพ หมายเลขบัตรเครดิต หรือทรัพย์สินทางปัญญา และทำการจัดประเภทโดยอัตโนมัติ นอกจากนี้ AI และ ML ยังเพิ่มความแม่นยำในการจำแนกประเภทและตรวจสอบข้อมูลย้อนหลังได้อีกด้วย กระบวนการระบุตัวตนเหล่านี้สามารถครอบคลุมพื้นที่ข้อมูลทั้งหมดของคุณได้ ทำให้คุณรักษาข้อมูล รวบรวม วิเคราะห์ ตรวจสอบ และส่งออกเนื้อหาได้ทุกที่บนคลาวด์



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC พฤษภาคม 2022

ขั้นที่ 2

จัดประเภทข้อมูล

การจัดประเภทข้อมูลที่เหมาะสมช่วยให้คุณกำหนดนโยบายที่เหมาะสมและลดความเสี่ยงเพื่อให้มั่นใจว่าข้อมูลประเภทต่างๆ จะไม่ถูกใช้ในทางที่ผิดหรือเข้าถึงโดยไม่ได้ตั้งใจหรือโดยเจตนา โดยที่ไม่ได้รับอนุญาต การเข้ารหัสและทำลายน้ำสามารถปกป้องข้อมูลได้ดียิ่งขึ้นไปอีก ไม่ว่าจะเป็นข้อมูลที่ไม่ได้ใช้งาน อยู่ระหว่างการส่ง หรือใช้งานอยู่ก็ตาม

แต่การจัดประเภทและนโยบายจำเป็นต้องติดตามข้อมูลเมื่อเดินทางไปทั่วองค์กร นโยบายการติดฉลากและการป้องกันไม่สามารถจำกัดอยู่เฉพาะเอกสารที่แยกจากกัน นโยบายเหล่านี้จำเป็นต้องครอบคลุมพื้นที่ดิจิทัลทั้งหมด ตั้งแต่ในองค์กรไปจนถึงที่เก็บข้อมูลบนระบบคลาวด์ ตั้งแต่แอป Software-as-a-Service (SaaS) ไปจนถึง OS-native

แนวทางการจำแนกประเภทแบบดั้งเดิมเกี่ยวข้องกับการทำงานด้วยตนเองจำนวนมาก ซึ่งเสี่ยงต่อการเกิดข้อผิดพลาดหรือมองข้ามข้อมูลที่สำคัญโดยไม่ได้เจตนา ตัวแยกประเภทที่มีในตัวและที่ฝึกอบรมได้นั้น จะสามารถช่วยทำให้กระบวนการนี้เป็นไปโดยอัตโนมัติได้ และโซลูชันแบบรวมระบบจะช่วยให้ผู้ดูแลระบบสามารถจัดการนโยบายจากส่วนกลางได้ในทุกระบบ

ทั้งการจำแนกประเภทและนโยบายจำเป็นต้องติดตามข้อมูลในขณะเดินทาง

ตัวอย่างเช่น หากพนักงานคัดลอกหมายเลขบัตรเครดิตจากเอกสาร Microsoft Word ลงใน Excel การจำแนกประเภทและนโยบายควรใช้กับเอกสารทั้งสองโดยอัตโนมัติ

ต้องการจัดการและปกป้องข้อมูลที่ละเอียดอ่อนภายในสภาพแวดล้อมของคุณให้ดีขึ้นหรือไม่

เรียนรู้เกี่ยวกับการจำแนกประเภทและการป้องกันใน Microsoft Purview ที่ **Microsoft.com**

ขั้นที่ 3

ป้องกันข้อมูลสูญหาย

นโยบาย DLP สามารถป้องกันการดำเนินการที่ไม่เป็นไปตามกฎระเบียบได้

ตัวอย่างเช่น หากพนักงานพยายามดาวน์โหลดสเปรดชีตที่มีหมายเลขบัตรเครดิตลงในแฟลชไดรฟ์หรืออัปโหลดไปยังที่เก็บข้อมูลระบบคลาวด์ นโยบาย DLP อาจระบุว่าเป็นกิจกรรมที่ไม่เป็นไปตามข้อบังคับ และจะป้องกันไม่ให้เกิดขึ้น

เมื่อคุณระบุและจำแนกประเภทข้อมูลของคุณแล้ว โซลูชันป้องกันการสูญหายของข้อมูล (Data Loss Prevention - DLP) สามารถบังคับใช้นโยบายการป้องกันแบบครบวงจรที่บรรเทาภัยคุกคามได้ เช่น ข้อมูลที่มืดมนและการขโมยข้อมูล ดังนั้น พนักงานในปัจจุบันและในอดีตจะไม่แชร์ข้อมูลทั้งโดยตั้งใจและไม่ได้ตั้งใจ เปิดเผยหรือถ่ายโอนข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต

โซลูชัน DLP อัจฉริยะใช้บริบทเพื่อสร้างสมดุลระหว่างการให้ความยืดหยุ่นและการบล็อกการกระทำที่มีความเสี่ยงสูง ตัวอย่างเช่น บุคคลอาจจะสามารถดำเนินการต่อได้ต่อไปหลังจากที่ได้รับการแจ้งเตือนเกี่ยวกับความเสี่ยงและนโยบายที่เกี่ยวข้อง ซึ่งจะช่วยปกป้องข้อมูลที่ละเอียดอ่อน ในขณะเดียวกันก็ฝึกผู้ใช้ให้เข้าใจถึงความเสี่ยงได้ดียิ่งขึ้น

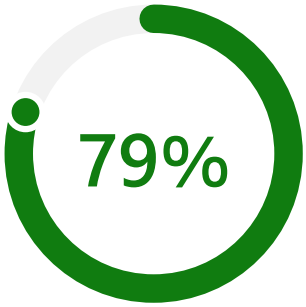
โซลูชัน DLP ช่วยปกป้องการปกป้องทรัพย์สินทางปัญญาและข้อมูลทางธุรกิจที่สำคัญอื่นๆ ทั้งยังปรับปรุงการปฏิบัติตามกฎระเบียบต่างๆ เช่น ระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป (GDPR), กฎหมายว่าด้วยการถ่ายโอนข้อมูลด้านสุขภาพและความรับผิดชอบ (HIPAA) และกฎหมายว่าด้วยความเป็นส่วนตัวของผู้บริโภคในแคลิฟอร์เนีย (CCPA)

แนวทางที่ครอบคลุมสำหรับ DLP บังคับใช้นโยบายทั่วทั้งองค์กรของคุณอย่างสม่ำเสมอ ปกป้องจุด "ลิงก์ที่อ่อนแอที่สุด" ในวงจรชีวิตของข้อมูล

ต้องการการตรวจจับอัจฉริยะและการควบคุมข้อมูลที่ละเอียดอ่อนหรือไม่

เรียนรู้เกี่ยวกับป้องกันการสูญหายของข้อมูลใน Microsoft Purview ที่ **Microsoft.com**

อย่าติดตั้งการป้องกันข้อมูล แต่จงสร้างขึ้นจากภายใน



แบบสำรวจผู้มีอำนาจตัดสินใจด้านการปฏิบัติตามกฎระเบียบพบว่า 79% ได้ซื้อผลิตภัณฑ์ด้านการปฏิบัติตามกฎระเบียบและการปกป้องข้อมูลหลายรายการ

ส่วนใหญ่ซื้อสามรายการหรือมากกว่า[5]

องค์กรหลายแห่งได้ลองใช้วิธีการแบบ “ติดตั้ง” ในการปกป้องข้อมูล โดยใช้โซลูชันที่หลากหลายเพื่อจัดการส่วนต่างๆ ของวงจรชีวิตของข้อมูล แต่สิ่งนี้บังคับให้ทีมการรักษาความปลอดภัย ทีมกำกับดูแลข้อมูล ทีมดูแลการปฏิบัติตามข้อบังคับ และทีมกฎหมายต้องเย็บข้อมูลปะติดปะต่อกัน ซึ่งมักไม่มีประสิทธิภาพและทำให้ทรัพยากรตึงเครียด

วิธีการ “สร้างใน” ตัวสามารถปิดช่องโหว่ได้ ทำเป็นการนำเอาการระบุข้อมูล การจำแนกข้อมูล และ DLP มาไว้รวมกัน ด้วยโซลูชันแบบครบวงจรช่วยให้สามารถจัดการและบังคับใช้นโยบายได้ง่ายขึ้นจากส่วนกลาง นอกจากนี้ยังลดเวลาการฝึกอบรมสำหรับผู้ใช้ที่ได้รับการแจ้งเตือนเกี่ยวกับนโยบายในวิธีที่คุ้นเคยภายในแอปพลิเคชัน

[5] "February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research."

โซลูชันแบบผสานรวมในตัว: Microsoft Purview

Microsoft Purview ช่วยให้คุณรับมือกับความท้าทายของสถานที่ทำงานที่มีข้อมูลจำนวนมากและมีลักษณะกระจาย ด้วยชุดโซลูชันที่ครอบคลุมซึ่งช่วยให้คุณควบคุม ปกป้อง และจัดการพื้นที่ข้อมูลทั้งหมดของคุณ

ไปกว่าการกำกับดูแล

เรียนรู้เพิ่มเติมเกี่ยวกับการปกป้องข้อมูลของคุณด้วย **Microsoft Purview** >

สนใจในด้านการปกป้องข้อมูลที่เฉพาะเจาะจงหรือไม่ รับข้อมูลรายละเอียดเพิ่มเติมเกี่ยวกับวิธีการที่ Microsoft Purview จะสามารถช่วยคุณได้:

การค้นพบข้อมูล >

การจัดประเภทและการปกป้องข้อมูล >

การป้องกันข้อมูลสูญหาย >

Microsoft Security