แนวโน้มและกลยุทธ์การสำรองและกู้คืนข้อมูลในอนาคต

บทนำ: การเปลี่ยนผ่านจากการ “สำรองข้อมูล” สู่ “ความยืดหยุ่นทางไซเบอร์”

การจัดการข้อมูลได้ก้าวข้ามจากการเป็นเพียงงานด้านการบำรุงรักษาไปสู่บทบาทเชิงกลยุทธ์ที่สำคัญยิ่งในองค์กรยุคใหม่ ดังที่นักคณิตศาสตร์ชาวอังกฤษ Clive Humby ได้กล่าวไว้ตั้งแต่ปี 2006 ว่า “ข้อมูลคือน้ำมันแห่งยุคใหม่” ข้อมูลเป็นสินทรัพย์ที่ทรงคุณค่าที่สุดสำหรับธุรกิจยุคใหม่ เป็นพลังขับเคลื่อนนวัตกรรม, การตัดสินใจเชิงธุรกิจ, และการสร้างปฏิสัมพันธ์กับลูกค้า การสูญเสียข้อมูลไม่ว่าจะด้วยเหตุผลใดก็ตามจึงสามารถนำไปสู่ความเสียหายทางการเงินและชื่อเสียงอย่างมหาศาล

ภูมิทัศน์ของภัยคุกคามในปัจจุบันมีความหลากหลายและซับซ้อนกว่าในอดีตมาก ไม่ได้จำกัดอยู่แค่เพียงความล้มเหลวของฮาร์ดแวร์หรือภัยธรรมชาติเท่านั้น แต่ยังรวมถึงความผิดพลาดของมนุษย์ เช่น การลบข้อมูลโดยไม่ได้ตั้งใจ และที่สำคัญที่สุดคือการโจมตีทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะการโจมตีจากแรนซัมแวร์ที่จ้องจะเข้ารหัสและเรียกค่าไถ่ข้อมูล ผู้โจมตีมีความชาญฉลาดมากขึ้นและมุ่งเป้าโจมตีไปที่ระบบสำรองข้อมูลโดยตรง ซึ่งเคยเป็นปราการด่านสุดท้าย ความเข้าใจนี้ได้สร้างกระบวนทัศน์ใหม่จากเดิมที่เน้นเพียงแค่การสำรองข้อมูล (Backup) ไปสู่การสร้าง “ความยืดหยุ่นทางไซเบอร์” (Cyber Resilience) ที่ครอบคลุมมากขึ้น

โดยผู้เขียนได้วิเคราะห์เชิงลึกเกี่ยวกับแนวโน้มของเทคโนโลยีการสำรองข้อมูลและกู้คืนข้อมูลในอนาคต และแบ่งการนำเสนอออกเป็นสามส่วนหลักเพื่อสร้างความเข้าใจที่ครอบคลุม: ส่วนแรกจะกล่าวถึงเทคโนโลยีหลักที่กำลังเข้ามาเปลี่ยนแปลงอุตสาหกรรม, ส่วนที่สองจะเจาะลึกกรอบการทำงานเชิงกลยุทธ์ที่จำเป็นต่อการรับมือกับภัยคุกคามในปัจจุบัน, และส่วนสุดท้ายจะระบุความท้าทายและนำเสนอแนวทางปฏิบัติที่ดีที่สุดเพื่อช่วยให้องค์กรสามารถนำกลยุทธ์เหล่านี้ไปปรับใช้ได้อย่างเป็นรูปธรรม

ส่วนที่ 1: การเปลี่ยนผ่านของเทคโนโลยีหลัก

1.1 ปัญญาประดิษฐ์ (AI) และแมชชีนเลิร์นนิง (ML): ขับเคลื่อนการจัดการข้อมูลให้ชาญฉลาด

ปัญญาประดิษฐ์ (AI) และแมชชีนเลิร์นนิง (ML) ได้กลายเป็นเครื่องมือสำคัญที่ช่วยยกระดับกระบวนการสำรองข้อมูลและกู้คืนข้อมูลให้ก้าวข้ามขีดจำกัดแบบเดิม ๆ จากที่เคยเป็นเพียงนวัตกรรมที่น่าสนใจ สองเทคโนโลยีนี้ได้เข้ามามีบทบาทในฐานะเครื่องมือเชิงกลยุทธ์ที่ช่วยให้การจัดการข้อมูลมีประสิทธิภาพ, รวดเร็ว, และชาญฉลาดมากขึ้น

การประยุกต์ใช้ AI ในด้านนี้ครอบคลุมหลายมิติ การใช้งานที่โดดเด่นที่สุดประการหนึ่งคือ **การตรวจจับความผิดปกติ (Anomaly Detection)** AI สามารถวิเคราะห์พฤติกรรมของข้อมูลและระบบในแบบเรียลไทม์เพื่อตรวจจับสัญญาณของการโจมตีที่กำลังเกิดขึ้นได้อย่างรวดเร็ว ซึ่งเป็นสิ่งที่การวิเคราะห์ด้วยมนุษย์เพียงอย่างเดียวไม่สามารถทำได้ ระบบที่ขับเคลื่อนด้วย ML สามารถตรวจพบแรนซัมแวร์ได้ภายในเวลาไม่ถึงหนึ่งนาที เมื่อ AI ตรวจพบพฤติกรรมที่ผิดปกติ เช่น การเข้ารหัสไฟล์จำนวนมากอย่างรวดเร็ว ก็จะสามารถแจ้งเตือนทีมรักษาความปลอดภัยได้ทันทีเพื่อยับยั้งการโจมตีและจำกัดความเสียหาย

นอกจากนี้ AI ยังช่วยในการ **วิเคราะห์เชิงคาดการณ์ (Predictive Analytics)** โดยการวิเคราะห์ข้อมูลในอดีตเพื่อทำนายความล้มเหลวที่อาจเกิดขึ้นในอนาคต เช่น ความเสี่ยงที่ฮาร์ดแวร์จะล้มเหลวหรือปัญหาคอขวดของระบบ ทำให้องค์กรสามารถวางแผนเชิงรุกเพื่อป้องกันเหตุการณ์ไม่พึงประสงค์ได้ ในแง่ของการเพิ่มประสิทธิภาพ AI มีบทบาทในการ **ปรับปรุงการทำงานให้เป็นแบบอัตโนมัติ** โดยสามารถปรับตารางการสำรองข้อมูลให้เหมาะสมที่สุด (Adaptive Backup Scheduling) ตามปริมาณงานหรือโหลดของเครือข่าย เพื่อลดการหยุดชะงักในการทำงานประจำวัน ซึ่งช่วยลดภาระงานของทีมไอทีที่ต้องใช้เวลากว่า 2 ชั่วโมงต่อวันในการเฝ้าระวังและแก้ไขปัญหาการสำรองข้อมูล

บทบาทของ AI ไม่ได้ทำงานอย่างโดดเดี่ยว แต่เป็นการทำงานร่วมกับเทคโนโลยีอื่น ๆ โดยเฉพาะกับพื้นที่จัดเก็บข้อมูลแบบเปลี่ยนแปลงไม่ได้ (Immutable Storage) ที่เปรียบเสมือนป้อมปราการด่านสุดท้ายที่แข็งแกร่งที่สุดที่รับประกันว่าสำเนาข้อมูลที่ “สะอาด” จะไม่ถูกแตะต้อง อย่างไรก็ตาม ป้อมปราการนี้จะไม่มีประสิทธิภาพสูงสุดหากไม่มี “ยามเฝ้าระวัง” ที่ดีพอ AI คือ “ยามเฝ้าระวัง” ที่คอยตรวจจับพฤติกรรมที่น่าสงสัยและแจ้งเตือนก่อนที่แรนซัมแวร์จะสามารถเข้าไปถึงป้อมปราการสำรองข้อมูลได้สำเร็จ ดังนั้น การลงทุนใน AI จึงเป็นการเสริมประสิทธิภาพและเพิ่มความเร็วในการตอบสนองให้กับกลยุทธ์การป้องกันด้วย Immutable Storage ทำให้องค์กรมีทั้งการป้องกันเชิงรุกและการกู้คืนเชิงรับที่สมบูรณ์แบบ

กรณีศึกษาจากการนำ AI ไปใช้ในอุตสาหกรรมโทรคมนาคมแสดงให้เห็นว่าการใช้ AI สามารถเพิ่มความแม่นยำในการจำแนกข้อมูลเครือข่ายที่เข้ารหัสได้ถึง 26.2% ทำให้องค์กรสามารถตรวจจับและตอบสนองต่อภัยคุกคามได้รวดเร็วยิ่งขึ้น นอกจากนี้ CrowdStrike ยังเป็นตัวอย่างที่โดดเด่นในการใช้ AI เพื่อวิเคราะห์พฤติกรรมของภัยคุกคามและป้องกันการโจมตีที่ซับซ้อนก่อนที่จะสร้างความเสียหาย ซึ่งเป็นการตอกย้ำถึงบทบาทของ AI ในการสร้างระบบการปกป้องข้อมูลที่ชาญฉลาดและตอบสนองได้ทันท่วงที

1.2 พื้นที่จัดเก็บข้อมูลแบบเปลี่ยนแปลงไม่ได้ (Immutable Storage): เกราะป้องกันด่านสุดท้ายที่แข็งแกร่งที่สุด

ในยุคที่การโจมตีด้วยแรนซัมแวร์มีเป้าหมายโดยตรงที่ข้อมูลสำรอง การพึ่งพาเพียงแค่การสำรองข้อมูลแบบดั้งเดิมจึงไม่เพียงพออีกต่อไป พื้นที่จัดเก็บข้อมูลแบบเปลี่ยนแปลงไม่ได้ หรือ Immutable Storage ได้กลายเป็นเทคโนโลยีที่ได้รับการยอมรับอย่างกว้างขวางในฐานะเกราะป้องกันที่แข็งแกร่งที่สุด แนวคิดหลักของ Immutable

Storage คือการใช้หลักการ Write-Once, Read-Many (WORM) ซึ่งหมายความว่าเมื่อข้อมูลถูกเขียนและบันทึกไว้ในระบบแล้ว จะไม่สามารถแก้ไข, ลบ, หรือเขียนทับได้จนกว่าจะสิ้นสุดระยะเวลาการเก็บรักษาที่กำหนดไว้

ประสิทธิภาพของ Immutable Storage ในการป้องกันภัยคุกคามมีอยู่หลายประการ ประการแรกคือ **การป้องกันแรนซัมแวร์** เนื่องจากแรนซัมแวร์ทำงานโดยการเข้ารหัสข้อมูล ทำให้ไม่สามารถเปลี่ยนแปลงข้อมูลใน Immutable Storage ได้ ส่งผลให้องค์กรมีสำเนาข้อมูลที่ "สะอาด" และไม่ถูกแตะต้องเสมอสำหรับการกู้คืน ประการที่สองคือ **การป้องกันความผิดพลาดของมนุษย์** แม้แต่ผู้ดูแลระบบที่มีสิทธิ์สูงสุด (Root/Admin) ก็ไม่สามารถเปลี่ยนแปลงหรือลบข้อมูลที่ถูกป้องกันไว้ได้ ซึ่งช่วยลดความเสี่ยงจากการกระทำโดยไม่ได้ตั้งใจหรือจากภัยคุกคามภายในองค์กร นอกจากนี้ยังช่วยให้องค์กรสามารถปฏิบัติตามข้อกำหนดทางกฎระเบียบด้านการเก็บรักษาข้อมูลได้อย่างง่ายดาย

รูปแบบการนำ Immutable Storage ไปใช้สามารถแบ่งออกได้เป็นหลายประเภท ซึ่งแต่ละประเภทมีข้อดีที่แตกต่างกัน ได้แก่:

- **On-Premises:** องค์กรจะจัดเก็บข้อมูลไว้ในฮาร์ดแวร์ของตัวเอง ข้อดีคือสามารถควบคุมได้เองทั้งหมดและมีความเร็วในการเข้าถึงข้อมูลสูงเพื่อการกู้คืนที่รวดเร็ว
- **Cloud-based:** ใช้บริการพื้นที่จัดเก็บข้อมูลบนคลาวด์ ข้อดีคือปรับขนาดได้อย่างยืดหยุ่นตามความต้องการและมีการจำลองข้อมูลข้ามศูนย์ข้อมูลทางภูมิศาสตร์ ช่วยปกป้องข้อมูลในกรณีที่เกิดภัยพิบัติระดับภูมิภาค
- **Air-gapped:** เป็นวิธีการที่แยกเซิร์ฟเวอร์สำรองข้อมูลออกจากเครือข่ายหลักโดยสิ้นเชิง ซึ่งถือเป็น "มาตรฐานทองคำ" สำหรับการปกป้องข้อมูลสำรอง เนื่องจากทำให้ผู้โจมตีไม่สามารถเข้าถึงข้อมูลสำรองได้เลย แม้ว่าจะเจาะระบบหลักได้สำเร็จ

แนวโน้มในปัจจุบันไม่ได้อยู่ที่การเลือกใช้ Immutable Storage แบบใดแบบหนึ่ง แต่เป็นการหลอมรวมเทคโนโลยีเข้าด้วยกันอย่างชาญฉลาดเพื่อสร้างระบบที่ยืดหยุ่นและครอบคลุม องค์กรจำนวนมากกำลังใช้โซลูชันแบบไฮบริด (Hybrid) ที่เก็บข้อมูลสำรองไว้ใน Immutable Storage บน On-Premises เพื่อการกู้คืนที่รวดเร็ว (Fast Recovery) ในกรณีที่เกิดเหตุการณ์ไม่รุนแรง ขณะเดียวกันก็เก็บสำเนาไว้บนคลาวด์ในรูปแบบ Immutable อีกชั้นหนึ่งเพื่อป้องกันภัยพิบัติทางกายภาพ การใช้กลยุทธ์นี้ร่วมกับหลักการ Air-gapping เชิงตรรกะหรือเชิงกายภาพช่วยให้มั่นใจได้ว่าสำเนาที่สำคัญที่สุดยังคงปลอดภัยแม้ระบบหลักจะถูกเจาะโดยสมบูรณ์

1.3 การก้าวสู่ยุค Multi-Cloud และ Hybrid Cloud: ความยืดหยุ่นที่มาพร้อมกับความท้าทาย

องค์กรจำนวนมากกำลังขับเคลื่อนไปสู่กลยุทธ์การใช้บริการคลาวด์ที่หลากหลาย หรือ Multi-Cloud โดยมีเหตุผลสำคัญหลายประการ การใช้ Multi-Cloud ช่วยให้องค์กรสามารถหลีกเลี่ยงการผูกติดกับผู้ให้บริการรายเดียว (Vendor Lock-in) ซึ่งอาจทำให้การย้ายข้อมูลมีค่าใช้จ่ายสูงและยุ่งยาก นอกจากนี้ยังเปิดโอกาสให้องค์กรสามารถเลือกใช้บริการที่ "ดีที่สุด" (Best-of-breed) จากผู้ให้บริการแต่ละรายเพื่อตอบสนองความต้องการเฉพาะทาง และ

ยังช่วยให้สามารถปฏิบัติตามข้อกำหนดด้านกฎระเบียบที่เข้มงวดของแต่ละประเทศ (Data Residency) ได้อย่างมีประสิทธิภาพ

อย่างไรก็ตาม การเปลี่ยนผ่านนี้ไม่ได้ปราศจากความท้าทาย การจัดการสภาพแวดล้อมที่หลากหลายซึ่งประกอบด้วยระบบ On-Premises, Private Cloud, และ Public Cloud ก่อให้เกิดความซับซ้อนใหม่ ๆ หนึ่งในความท้าทายที่สำคัญที่สุดคือการบริหารจัดการที่กระจัดกระจาย การใช้เครื่องมือสำรองข้อมูลหลายตัวเพื่อรองรับแต่ละสภาพแวดล้อมทำให้ประสิทธิภาพลดลง และองค์กรกว่าครึ่งหนึ่งต้องใช้เวลามากกว่าสองชั่วโมงต่อวันในการเฝ้าระวัง, จัดการ, และแก้ไขปัญหาการสำรองข้อมูล นอกจากนี้ การควบคุมต้นทุนคลาวด์ให้เหมาะสมยังเป็นความท้าทายอันดับต้น ๆ สำหรับองค์กร ซึ่งต้องหาทางสร้างสมดุลระหว่างประสิทธิภาพกับต้นทุนที่จำกัด

แม้ว่าแนวโน้มการใช้โครงสร้างพื้นฐานจะเป็นแบบกระจายตัว แต่แนวโน้มของการบริหารจัดการข้อมูลสำรองกลับกำลังมุ่งสู่ “การรวมศูนย์” (Unified Visibility) เพื่อแก้ปัญหาความซับซ้อนที่เกิดขึ้น องค์กรกำลังมองหาโซลูชันที่นำเสนอการจัดการแบบรวมศูนย์ (Centralized Console) หรือแดชบอร์ดเดียว (Single Pane of Glass) เพื่อให้ทีมไอทีสามารถบริหารจัดการและตรวจสอบงานสำรองข้อมูลทั้งหมดได้จากที่เดียว ซึ่งช่วยให้การบังคับใช้นโยบายมีความสอดคล้องกันและลดความเสี่ยงที่ข้อมูลจะขาดการป้องกันในส่วนใดส่วนหนึ่ง

การนำกลยุทธ์ไฮบริดคลาวด์ไปใช้ในเชิงปฏิบัติได้ถูกพิสูจน์แล้วว่าช่วยเพิ่มประสิทธิภาพและลดต้นทุนให้กับองค์กรขนาดใหญ่ ตัวอย่างเช่น Coca-Cola และ Toyota ที่ใช้ไฮบริดคลาวด์เพื่อจัดการซัพพลายเชนและข้อมูลขนาดใหญ่ ขณะที่ Dropbox ใช้กลยุทธ์นี้เพื่อจัดการข้อมูลจำนวนมหาศาลและลดต้นทุน นอกจากนี้ยังมีกรณีศึกษาที่ชี้ให้เห็นว่าการใช้โซลูชันไฮบริดคลาวด์สามารถช่วยให้องค์กรประหยัดค่าใช้จ่ายได้อย่างมีนัยสำคัญเมื่อเทียบกับการใช้พับลิกคลาวด์เพียงอย่างเดียว

1.4 การเติบโตของบริการ X-as-a-Service: จากการลงทุนสู่การใช้บริการ

ในยุคที่องค์กรต้องการความคล่องตัวและต้องการลดภาระการลงทุนในโครงสร้างพื้นฐาน บริการการสำรองและกู้คืนข้อมูลแบบครบวงจรได้กลายเป็นทางเลือกที่น่าสนใจ โดยเฉพาะอย่างยิ่งบริการ **BaaS (Backup as a Service)** และ **DRaaS (Disaster Recovery as a Service)** ซึ่งช่วยให้องค์กรสามารถเปลี่ยนรูปแบบค่าใช้จ่ายจากการลงทุนแบบครั้งเดียว (Capital Expenditure, CAPEX) ไปสู่ค่าใช้จ่ายตามการใช้งาน (Operating Expenditure, OPEX)

แม้ว่าทั้งสองบริการจะมีเป้าหมายในการปกป้องข้อมูล แต่ก็มีวัตถุประสงค์และการใช้งานที่แตกต่างกันอย่างชัดเจน:

- **BaaS** เน้นการสำรองข้อมูลและกู้คืนไฟล์ในระดับย่อย (File-level Recovery) หรือข้อมูลเก่า โดยมีจุดประสงค์หลักเพื่อป้องกันข้อมูลสูญหายจากเหตุการณ์เล็ก ๆ เช่น การลบโดยไม่ได้ตั้งใจ BaaS เป็นทางเลือกที่คุ้มค่าและเหมาะสำหรับองค์กรที่สามารถยอมรับระยะเวลาการหยุดทำงานได้

- **DRaaS** เน้นการกู้คืนระบบทั้งหมดเพื่อความต่อเนื่องทางธุรกิจ (Business Continuity) ออกแบบมาเพื่อรับมือกับภัยพิบัติขนาดใหญ่ที่ทำให้ระบบหลักล้มเหลว DRaaS มีจุดเด่นด้านความรวดเร็วในการกู้คืน (Recovery Time Objective, RTO) ที่สามารถทำได้ภายในไม่กี่นาทีหรือชั่วโมง และมักมีค่าใช้จ่ายสูงกว่าเนื่องจากต้องมีการจำลองสภาพแวดล้อมทั้งหมดไว้ล่วงหน้า

เพื่อช่วยให้เข้าใจความแตกต่างที่สำคัญระหว่างสองบริการนี้ได้อย่างชัดเจน รายงานดังกล่าวนำเสนอการเปรียบเทียบในรูปแบบตาราง:

คุณสมบัติ	**BaaS (Backup as a Service)**	**DRaaS (Disaster Recovery as a Service)**
วัตถุประสงค์	การสำรองและกู้คืนข้อมูลเฉพาะส่วน	ความต่อเนื่องทางธุรกิจและการกู้คืนระบบทั้งหมด
ขอบเขตการกู้คืน	การกู้คืนไฟล์, ฐานข้อมูล, หรือเซิร์ฟเวอร์เฉพาะส่วน	การกู้คืนสภาพแวดล้อมไอทีทั้งหมด, รวมถึง VM, OS, และข้อมูล
ความเร็วในการกู้คืน (RTO)	นานกว่า (ใช้เวลาหลายชั่วโมงถึงวัน)	รวดเร็วกว่า (ใช้เวลาไม่กี่นาทีถึงชั่วโมง)
การกู้คืนข้อมูล (RPO)	ระยะเวลาการสำรองข้อมูลอาจเป็นรายวัน/สัปดาห์	ระยะเวลาการจำลองข้อมูลเป็นแบบเรียลไทม์หรือไม่กี่นาที
ต้นทุน	ต่ำกว่า เพราะส่วนใหญ่จ่ายค่าพื้นที่จัดเก็บ	สูงกว่า เพราะต้องมีการจำลองและเตรียมทรัพยากรไว้ล่วงหน้า
ความซับซ้อน	เรียบง่ายกว่าและง่ายต่อการกำหนดค่า	ซับซ้อนกว่าและต้องมีการวางแผนการกู้คืนอย่างละเอียด
กลุ่มผู้ใช้หลัก	ธุรกิจขนาดเล็กและขนาดกลาง	องค์กรขนาดใหญ่ที่มีแอปพลิเคชันสำคัญที่ยอมรับการหยุดทำงานไม่ได้

นอกจาก BaaS และ DRaaS แล้ว ตลาด **SaaS Backup** ยังมีการเติบโตอย่างรวดเร็วและเป็นเทรนด์ที่น่าจับตามองอย่างยิ่ง โดย Gartner คาดการณ์ว่าภายในปี 2028 องค์กร 75% จะให้ความสำคัญกับการสำรองข้อมูลแอปพลิเคชัน SaaS เป็นความต้องการที่สำคัญ ปัจจัยสำคัญที่อยู่เบื้องหลังการเติบโตนี้คือการขาดความเข้าใจใน **โมเดลความรับผิดชอบร่วมกัน (Shared Responsibility Model)** ของผู้ให้บริการคลาวด์

หลายองค์กรเข้าใจผิดว่าผู้ให้บริการ SaaS (เช่น Microsoft 365, Google Workspace, Salesforce) มีหน้าที่รับผิดชอบในการปกป้องข้อมูลของผู้ใช้งานทั้งหมด แต่ในความเป็นจริงแล้ว ผู้ให้บริการมีหน้าที่รับผิดชอบเพียงแค่ “ความปลอดภัยของคลาวด์” (Security *of* the Cloud) ซึ่งหมายถึงการดูแลโครงสร้างพื้นฐาน, ฮาร์ดแวร์, และเครือข่าย ในขณะที่ “ความปลอดภัยในคลาวด์” (Security *in* the Cloud) ซึ่งครอบคลุมถึงการจัดการข้อมูล, การตั้งค่า, และการปกป้องข้อมูลของผู้ใช้งาน เป็นความรับผิดชอบของลูกค้าเอง ช่องว่างด้านความรับผิดชอบนี้ทำให้ข้อมูล SaaS มีความเสี่ยงที่จะสูญหายจากความผิดพลาดของมนุษย์, การโจมตีทางไซเบอร์, หรือความผิดพลาดของผู้ให้บริการ ด้วยเหตุนี้ ตลาด SaaS Backup จึงเติบโตขึ้นอย่างมาก เนื่องจากองค์กรต่าง ๆ ตระหนักถึงความจำเป็นในการลงทุนในโซลูชันจากผู้ให้บริการภายนอก (Third-party) เพื่อเติมเต็มช่องว่างด้านการปกป้องข้อมูลนี้

เพื่อสร้างความเข้าใจที่ชัดเจนในประเด็นนี้ รายงานดังกล่าวนำเสนอการสรุปโมเดลความรับผิดชอบร่วมกันสำหรับ SaaS:

ส่วนที่รับผิดชอบ	**ผู้ให้บริการ SaaS (เช่น Microsoft, Google)**	**ลูกค้า (องค์กรผู้ใช้งาน)**
โครงสร้างพื้นฐาน	รับผิดชอบในการปกป้องโครงสร้างพื้นฐานทั้งหมด (ฮาร์ดแวร์, ซอฟต์แวร์, เครือข่าย)	ไม่ต้องรับผิดชอบ
ความพร้อมใช้งานของบริการ	รับผิดชอบในการทำให้บริการพร้อมใช้งานอยู่เสมอ	ไม่ต้องรับผิดชอบ
การจัดการข้อมูล	จัดการการจัดเก็บข้อมูลแบบรวมศูนย์	รับผิดชอบในการปกป้องและจัดการข้อมูลของตนเอง
การกู้คืนข้อมูล	สามารถกู้คืนข้อมูลในภาพรวมได้	รับผิดชอบในการกู้คืนข้อมูลของผู้ใช้งานแต่ละราย, ไฟล์, และการกู้คืนแบบเจาะจง
การปฏิบัติตามข้อกำหนด	รับผิดชอบในการปฏิบัติตามกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐาน	รับผิดชอบในการปฏิบัติตามกฎระเบียบที่เกี่ยวข้องกับข้อมูลของลูกค้าและผู้ใช้

ส่วนที่ 2: กรอบการทำงานเชิงกลยุทธ์เพื่อความยืดหยุ่นทางไซเบอร์

2.1 Zero Trust Data Resilience (ZTDR): หลักการ "ไม่เชื่อใจและตรวจสอบเสมอ"

ในโลกที่การโจมตีทางไซเบอร์กลายเป็นสิ่งที่หลีกเลี่ยงไม่ได้ การป้องกันจึงไม่ใช่แค่การสร้างกำแพงที่แข็งแกร่งเท่านั้น แต่ยังรวมถึงการเตรียมพร้อมที่จะรับมือเมื่อกำแพงนั้นถูกเจาะทะลุได้ การนำหลักการ Zero Trust มาปรับใช้กับระบบการสำรองข้อมูลและการกู้คืนจึงมีความสำคัญอย่างยิ่ง แนวคิดของ Zero Trust Data Resilience (ZTDR) คือการสันนิษฐานไว้ก่อนว่าผู้ใช้, อุปกรณ์, หรือแม้แต่เครือข่ายใด ๆ ก็อาจเป็นภัยคุกคามได้จนกว่าจะได้รับการตรวจสอบและยืนยันอย่างชัดเจน การใช้หลักการนี้กับข้อมูลสำรองซึ่งเป็นปราการด่านสุดท้ายจึงเป็นสิ่งจำเป็นอย่างยิ่ง

ZTDR ตั้งอยู่บนสามหลักการสำคัญที่ทำงานร่วมกันเพื่อสร้างระบบนิเวศการปกป้องข้อมูลที่แข็งแกร่ง:

1. **การแยกส่วนเครือข่าย (Network Segmentation) และ Air-gapping:** หลักการนี้เน้นการลดพื้นที่การโจมตีโดยการแยกซอฟต์แวร์และพื้นที่จัดเก็บข้อมูลสำรองออกจากเครือข่ายหลัก หากระบบหลักถูกโจมตี ข้อมูลสำรองก็จะยังคงปลอดภัยและสามารถกู้คืนได้ การใช้หลักการ Air-gapping เชิงกายภาพหรือเชิงตรรกะถือเป็นแนวทางปฏิบัติที่ได้รับการแนะนำอย่างยิ่ง
2. **การควบคุมสิทธิ์ที่เข้มงวด (Least Privilege):** หลักการนี้กำหนดว่าผู้ดูแลระบบหรือบัญชีผู้ใช้งานใด ๆ ควรได้รับสิทธิ์ในการเข้าถึงข้อมูลเท่าที่จำเป็นที่สุดเท่านั้น โดยไม่ควรมีบุคคลใดบุคคลหนึ่งที่มีสิทธิ์มากพอที่จะสามารถแก้ไขหรือลบข้อมูลสำรองทั้งหมดได้ การใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) ก็เป็นสิ่งจำเป็นในการเพิ่มชั้นการป้องกัน
3. **การใช้พื้นที่จัดเก็บแบบเปลี่ยนแปลงไม่ได้ (Immutable Storage):** ดังที่ได้กล่าวไปแล้วในส่วนที่ 1.2 Immutable Storage เป็นองค์ประกอบสำคัญของ ZTDR เพราะช่วยรับประกันว่าสำเนาข้อมูลสำรองจะไม่สามารถเปลี่ยนแปลง, แก้ไข, หรือลบได้ แม้ว่าผู้โจมตีจะสามารถเข้าถึงระบบได้ก็ตาม

หลักการทั้งสามนี้จะทำงานร่วมกันเพื่อสร้างแนวป้องกันที่หลายชั้น (Multi-layered Security) ซึ่งสอดคล้องกับแนวคิดของ Zero Trust ที่ว่าไม่มีการป้องกันใดที่สมบูรณ์แบบ ดังนั้นจึงต้องเตรียมพร้อมสำหรับเหตุการณ์ที่เลวร้ายที่สุดเสมอ

หลักการสำคัญของ ZTDR	คำอธิบาย	วัตถุประสงค์เชิงกลยุทธ์
การแยกส่วนเครือข่าย (Network Segmentation) และ Air-gapping	แยกซอฟต์แวร์สำรองข้อมูลและพื้นที่จัดเก็บออกจากกันและจากเครือข่ายหลัก	ลดพื้นที่การโจมตี (Attack Surface) และจำกัดขอบเขตความเสียหาย (Blast Radius) หากเกิดเหตุการณ์ไม่พึงประสงค์

หลักการสำคัญของ ZTDR	คำอธิบาย	วัตถุประสงค์เชิงกลยุทธ์
การควบคุมสิทธิ์ที่เข้มงวด (Least Privilege)	กำหนดสิทธิ์การเข้าถึงแก่ผู้ดูแลระบบเฉพาะเท่าที่จำเป็นที่สุด พร้อมใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA)	ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและลดความเสี่ยงจากภัยคุกคามภายในองค์กร
การใช้พื้นที่จัดเก็บแบบเปลี่ยนแปลงไม่ได้ (Immutable Storage)	จัดเก็บข้อมูลสำรองในรูปแบบที่ไม่สามารถแก้ไข, ลบ, หรือเข้ารหัสได้	รับประกันว่าองค์กรมีสำเนาข้อมูลที่ "สะอาด" และพร้อมใช้งานสำหรับการกู้คืนหลังการโจมตีเสมอ

2.2 การเปลี่ยนจาก "การป้องกัน" สู่ "การกู้คืน": กลยุทธ์ Cyber Resilience

ในอดีต องค์กรมักจะมุ่งเน้นไปที่การป้องกันการโจมตี (Cybersecurity) แต่ในปัจจุบัน แนวคิดที่ครอบคลุมและยั่งยืนกว่าคือ **ความยืดหยุ่นทางไซเบอร์ (Cyber Resilience)** แนวคิดนี้ไม่ได้จำกัดอยู่แค่การป้องกันการโจมตีเท่านั้น แต่คือความสามารถในการรักษาการดำเนินงานที่สำคัญและให้บริการได้อย่างต่อเนื่อง แม้จะเผชิญกับเหตุการณ์ทางไซเบอร์ที่รุนแรง ซึ่งถือเป็นการผสมผสานระหว่างมาตรการรักษาความปลอดภัยที่แข็งแกร่งเข้ากับแผนการกู้คืนระบบจากภัยพิบัติและความต่อเนื่องทางธุรกิจ

ในขณะที่ Cyber Resilience เป็นกลยุทธ์ภาพรวม **การกู้คืนทางไซเบอร์ (Cyber Recovery)** เป็นกระบวนการเฉพาะที่ใช้เพื่อนำข้อมูลและระบบกลับคืนสู่สถานะที่ "สมบูรณ์" หลังจากการโจมตี โดยไม่ได้เป็นเพียงการคัดลอกไฟล์แบบดั้งเดิม แต่เป็นกระบวนการที่ซับซ้อนกว่ามาก ซึ่งต้องมีการวางแผนเชิงรุก, การทดสอบอย่างต่อเนื่อง, และการใช้เครื่องมือขั้นสูงเพื่อตรวจสอบและป้องกันไม่ให้มัลแวร์ที่อาจซ่อนตัวอยู่ถูกนำกลับเข้ามาในระบบในระหว่างการกู้คืน ซึ่งถือเป็นส่วนสำคัญที่แยก Cyber Recovery ออกจาก Disaster Recovery แบบดั้งเดิม

2.3 การวัดผลความสำเร็จ: การทำความเข้าใจ RPO และ RTO

การวางแผนการสำรองและกู้คืนข้อมูลจะไม่มีประสิทธิภาพหากไม่มีการกำหนดเป้าหมายที่ชัดเจนและสามารถวัดผลได้ **RPO (Recovery Point Objective)** และ **RTO (Recovery Time Objective)** จึงเป็นสองตัวชี้วัดที่สำคัญที่สุดในกระบวนการวางแผนการกู้คืนระบบจากภัยพิบัติ

- **RPO (Recovery Point Objective):** คือปริมาณข้อมูลสูงสุดที่องค์กรยอมรับที่จะสูญเสียได้หลังจากการหยุดชะงักของระบบ ตัวอย่างเช่น หากองค์กรกำหนด RPO ไว้ที่ 15 นาที หมายความว่าข้อมูลที่สร้างขึ้นในช่วง 15 นาทีก่อนเกิดเหตุการณ์อาจสูญหายได้ การมี RPO ที่สั้นลงจะช่วยลดการสูญเสียข้อมูล แต่ก็ต้อง

แลกมากับความถี่ในการสำรองข้อมูลที่มากขึ้น, พื้นที่จัดเก็บที่มากขึ้น, และทรัพยากรด้านคอมพิวเตอร์และเครือข่ายที่มากขึ้นเช่นกัน

- **RTO (Recovery Time Objective):** คือระยะเวลาสูงสุดที่องค์กรสามารถยอมให้ระบบ, แอปพลิเคชัน, และกระบวนการที่สำคัญหยุดทำงานได้หลังจากเกิดเหตุการณ์ RTO มีความสำคัญอย่างยิ่งในการวางแผนความต่อเนื่องทางธุรกิจ เพราะเป็นตัวกำหนดว่าองค์กรจะต้องกลับมาดำเนินการได้เร็วแค่ไหน

RPO และ RTO ไม่ได้เป็นเพียงตัวเลขทางเทคนิค แต่เป็นตัวเลขที่สะท้อน "ความต้องการทางธุรกิจ" อย่างแท้จริง ซึ่งต้องได้รับการกำหนดโดยผู้บริหารและทีมงานจากทุกแผนกผ่านการวิเคราะห์ผลกระทบทางธุรกิจอย่างละเอียด ตัวเลขเหล่านี้จะทำหน้าที่เป็น "โจทย์" ในการเลือกใช้เทคโนโลยีและวางแผนการสำรองข้อมูลและการกู้คืน ตัวอย่างเช่น หากองค์กรมีแอปพลิเคชันที่มีความสำคัญสูงสุดและต้องการ RPO ที่ใกล้เคียงศูนย์ (Near-Zero RPO) และ RTO ที่สั้นมากในระดับนาที ก็จำเป็นต้องพิจารณาใช้เทคโนโลยีอย่าง **Continuous Data Protection (CDP)** ซึ่งเป็นเทคโนโลยีที่ทำการสำรองข้อมูลแบบเรียลไทม์ แทนที่จะเป็นการสำรองแบบตามช่วงเวลาแบบดั้งเดิม CDP สามารถลด RPO ให้เหลือเพียงไม่กี่วินาทีและ RTO ให้เหลือไม่กี่นาที ทำให้องค์กรสามารถกลับมาดำเนินการได้อย่างรวดเร็วหลังเหตุการณ์ไม่คาดฝัน

ส่วนที่ 3: ความท้าทายและการนำแนวทางปฏิบัติที่ดีที่สุดไปใช้

3.1 อุปสรรคสำคัญที่องค์กรต้องเผชิญ

แม้ว่าเทคโนโลยีและกลยุทธ์การปกป้องข้อมูลจะก้าวหน้าไปมาก แต่รายงานตลาดล่าสุดยังคงชี้ให้เห็นถึงช่องว่างที่น่ากังวล:

- **การขาดความพร้อมและการทดสอบ:** รายงานของ Kaseya ปี 2025 ชี้ให้เห็นว่าองค์กรจำนวนมากยังคงขาดความพร้อมในการรับมือกับเหตุการณ์ภัยพิบัติ มีเพียง 15% ขององค์กรเท่านั้นที่ทำการทดสอบการสำรองข้อมูลเป็นประจำทุกวัน และมีเพียง 11% ที่ทดสอบการกู้คืนระบบจากภัยพิบัติเป็นประจำทุกวัน ที่น่าตกใจคือ 12% ยอมรับว่าไม่เคยทำการทดสอบการกู้คืนระบบเลย นอกจากนี้ ยังมีช่องว่างระหว่างความคาดหวังและความเป็นจริง โดย 60% ของผู้ตอบแบบสำรวจเชื่อว่าพวกเขาสามารถกู้คืนระบบได้ภายในหนึ่งวัน แต่มีเพียง 35% เท่านั้นที่ทำได้จริง
- **ต้นทุนที่ควบคุมยาก:** รายงาน Kaseya ระบุว่าราคาเป็นความท้าทายหลักสำหรับองค์กรที่ต้องการเปลี่ยนโซลูชันการสำรองข้อมูล โดยเฉพาะอย่างยิ่งต้นทุนที่ซ่อนอยู่ในการจัดการ Multi-Cloud ซึ่งถือเป็นความท้าทายที่ใหญ่ที่สุดในการย้ายปริมาณงานไปสู่คลาวด์
- **ความซับซ้อนและการผูกติดกับผู้ให้บริการ (Vendor Lock-in):** การที่องค์กรส่วนใหญ่ใช้เครื่องมือสำรองข้อมูลมากกว่าสามตัว ส่งผลให้ประสิทธิภาพในการจัดการลดลง และการผูกติดกับผู้ให้บริการรายเดียวก็เป็นอุปสรรคสำคัญ เนื่องจากทำให้การโยกย้ายข้อมูลมีค่าใช้จ่ายสูงและยุ่งยาก

3.2 แนวทางปฏิบัติเพื่อความสำเร็จในการปกป้องข้อมูลในอนาคต

เพื่อให้องค์กรสามารถรับมือกับความท้าทายเหล่านี้ได้อย่างมีประสิทธิภาพและสร้างระบบการปกป้องข้อมูลที่แข็งแกร่งและยืดหยุ่นได้ในระยะยาว ควรปฏิบัติตามแนวทางสำคัญดังนี้:

- **ยึดมั่นในหลักการ 3-2-1 และ 3-2-1-1-0:** หลักการ **3-2-1** เป็นแนวทางปฏิบัติที่ได้รับการยอมรับในระดับสากล โดยระบุว่าควรมีสำเนาข้อมูลอย่างน้อย **3** ชุด, จัดเก็บไว้บนสื่อบันทึก **2** ประเภทที่แตกต่างกัน, และมีสำเนาอย่างน้อย **1** ชุดที่เก็บอยู่นอกสถานที่ เพื่อเพิ่มความทนทานต่อภัยพิบัติ Veeam ได้ขยายหลักการนี้ไปสู่ **3-2-1-1-0** โดยเพิ่มการมีสำเนาอย่างน้อย **1** ชุดที่เก็บแบบเปลี่ยนแปลงไม่ได้ (Immutable) หรือ Air-gapped และมีการยืนยันการกู้คืนได้อย่างสมบูรณ์แบบโดยไม่มีข้อผิดพลาด **0** ครั้ง
- **การทดสอบอย่างสม่ำเสมอ:** รายงานหลายฉบับเน้นย้ำถึงความสำคัญของการทดสอบการกู้คืนระบบอย่างต่อเนื่องเพราะ “การสำรองข้อมูลที่ไม่ถูกทดสอบคือการสำรองข้อมูลที่เชื่อถือไม่ได้” การทดสอบช่วยให้องค์กรสามารถระบุช่องว่างในกระบวนการและแก้ไขได้อย่างทันท่วงที และการทดสอบยังช่วยฝึกฝนทีมงานให้มีความคุ้นเคยกับขั้นตอนการกู้คืนในกรณีที่เกิดเหตุฉุกเฉินจริง
- **การใช้ระบบอัตโนมัติ (Automation):** การจัดการข้อมูลสำรองด้วยตนเองต้องใช้เวลาและมีความเสี่ยงจากความผิดพลาดของมนุษย์สูง การใช้ระบบอัตโนมัติเข้ามาช่วยจัดการกระบวนการสำรองข้อมูลจึงเป็นสิ่งจำเป็น ระบบอัตโนมัติสามารถช่วยกำหนดตารางการสำรองข้อมูลที่แน่นอน, ลดความเสี่ยงจากการลืมหรือความผิดพลาด, และช่วยให้ทีมไอทีมีเวลาไปมุ่งเน้นงานเชิงกลยุทธ์อื่น ๆ ที่สำคัญกว่า
- **การจัดลำดับความสำคัญของข้อมูล:** การปกป้องข้อมูลทั้งหมดในระดับเดียวกันไม่เพียงแต่จะสิ้นเปลืองค่าใช้จ่าย แต่ยังไม่มีประสิทธิภาพ องค์กรควรใช้ RPO และ RTO เป็นเกณฑ์ในการแบ่งประเภทข้อมูล (Data Tiers) ออกเป็นระดับความสำคัญต่าง ๆ ตัวอย่างเช่น จัดให้ข้อมูลที่มีความสำคัญสูงสุด (Tier 1) มี RPO/RTO ที่สั้นที่สุด และใช้โซลูชันเช่น DRaaS หรือ CDP ในขณะที่ข้อมูลที่มีความสำคัญน้อยกว่า (Tier 2/3) อาจใช้โซลูชัน BaaS หรือการสำรองแบบดั้งเดิมที่ประหยัดกว่า การทำเช่นนี้ช่วยให้องค์กรสามารถควบคุมทั้งความเสี่ยงและต้นทุนได้ในเวลาเดียวกัน

ส่วนที่ 4: บทสรุปและข้อเสนอแนะเชิงกลยุทธ์สำหรับองค์กร

อนาคตของเทคโนโลยีการสำรองและกู้คืนข้อมูลได้ก้าวไปไกลกว่าการเป็นเพียงการคัดลอกไฟล์ แต่เป็นการสร้างระบบนิเวศที่ครอบคลุม (Ecosystem) ซึ่งประกอบไปด้วยเทคโนโลยี (AI, Immutable Storage, Multi-Cloud), กลยุทธ์ (Zero Trust, Cyber Resilience), และแนวทางปฏิบัติ (3-2-1-1-0, การทดสอบ) ที่ทำงานร่วมกันเพื่อสร้างความยืดหยุ่นทางธุรกิจที่แท้จริง เพื่อนำพาองค์กรให้ก้าวทันกับแนวโน้มเหล่านี้และสร้างความได้เปรียบในการแข่งขัน ผู้บริหารระดับสูงและผู้เชี่ยวชาญด้านไอทีควรพิจารณาข้อเสนอแนะเชิงกลยุทธ์ดังต่อไปนี้:

1. **ลงทุนในความยืดหยุ่น (Resilience-as-a-Strategy):** เปลี่ยนมุมมองจากการมองการสำรองข้อมูลเป็นค่าใช้จ่ายไปเป็นการลงทุนในความต่อเนื่องทางธุรกิจ โดยตระหนักว่าการป้องกันเพียงอย่างเดียวไม่เพียงพอ และต้องพร้อมที่จะกู้คืนและดำเนินธุรกิจต่อไปได้แม้จะเผชิญกับเหตุการณ์ทางไซเบอร์ที่รุนแรง

2. **บูรณาการเทคโนโลยีเชิงรุก:** พิจารณานำเทคโนโลยีขั้นสูงอย่าง AI และแมชชีนเลิร์นนิงมาเป็นส่วนหนึ่งของระบบป้องกัน เพื่อเพิ่มความสามารถในการตรวจจับภัยคุกคามในแบบเรียลไทม์ ขณะเดียวกันก็ใช้ Immutable Storage เป็นเกราะป้องกันด่านสุดท้ายที่รับประกันว่าข้อมูลที่สำคัญที่สุดจะยังคงปลอดภัยและสามารถกู้คืนได้เสมอ
3. **ทำความเข้าใจโมเดลความรับผิดชอบ:** ตระหนักถึงบทบาทและความรับผิดชอบของตนเองในโมเดล Shared Responsibility โดยเฉพาะสำหรับข้อมูลที่อยู่บนแอปพลิเคชัน SaaS และลงทุนในโซลูชัน SaaS Backup จากผู้ให้บริการภายนอกที่เหมาะสมเพื่อเติมเต็มช่องว่างด้านการปกป้องข้อมูล
4. **เน้นการบริหารจัดการที่รวมศูนย์:** แม้จะใช้กลยุทธ์ Multi-Cloud แต่ควรเลือกโซลูชันที่สามารถบริหารจัดการระบบสำรองข้อมูลทั้งหมดได้จากศูนย์กลางผ่านแดชบอร์ดเดียว ซึ่งจะช่วยลดความซับซ้อนและเพิ่มประสิทธิภาพในการทำงานของทีมไอที
5. **ทดสอบ ทดสอบ และทดสอบ:** กำหนดให้การทดสอบการกู้คืนเป็นส่วนหนึ่งของวัฒนธรรมองค์กรอย่างสม่ำเสมอ เนื่องจากความสามารถในการกู้คืนที่แท้จริงจะถูกพิสูจน์ได้จากการทดสอบเท่านั้น การมีแผนที่ดีเยี่ยมแต่ไม่เคยถูกทดสอบอาจนำไปสู่ความล้มเหลวที่ร้ายแรงที่สุดในเวลาที่สำคัญที่สุด

ผลงานที่อ้างอิง

1. https://www.unitrends.com/media/downloads/resources/The-State-of-Backup-and-Recovery-Report-2025.pdf
2. https://www.netapp.com/cyber-resilience/what-is-backup-recovery/
3. https://storware.eu/blog/challenges-of-enterprise-data-backup-and-disaster-recovery/
4. https://www.sangfor.com/th/glossary/cybersecurity/what-is-ransomware-attack-and-how-does-it-work
5. https://digitalisationworld.com/blog/57907/five-ways-ai-is-revolutionising-the-data-backup-industry
6. https://www.rubrik.com/insights/what-are-cyber-resilience-and-cyber-recovery
7. https://www.datacore.com/glossary/what-is-cyber-resilience/
8. https://www.a-host.co.th/data-management-trends-in-2024/
9. https://blog.cloudhm.co.th/cloud-trends-in-2024/
10. https://www.flashbackdata.com/ai-data-recovery/
11. https://corptec.com.au/blog/hycu/multi-cloud-backup-and-disaster-recovery-trends-2025/
12. https://corptec.com.au/blog/hycu/multi-cloud-backup-and-disaster-recovery-trends-2025/

13. https://www.quickserv.co.th/knowledge-base/solutions/Ransomware ภัยคุกคามร้ายแรงในยุคดิจิทัล และวิธีป้องกันด้วยเทคโนโลยีล้ำสมัยจาก IBM
14. https://www.techtalkthai.com/netapp-new-capabilities-using-ai-to-protect-ransomware-attack-on-storage/
15. https://fastneuron.com/forum/showthread.php?tid=6537
16. https://www.supermicro.com/en/glossary/continuous-data-protection
17. https://www.kaseya.com/press-release/kaseya-report-outlines-top-trends-in-backup-and-recovery-in-2025/
18. https://www.aisecuredata.com/ai-data-security-case-studies/
19. https://www.crowdstrike.com/en-us/blog/the-evolving-role-of-ai-in-data-protection/
20. https://cloudian.com/guides/data-backup/immutable-storage-benefits-types-and-uses/
21. https://www.ibm.com/think/topics/immutable-storage
22. https://panzura.com/blog/ransomware-attacks-immutable-data-architecture
23. https://www.veeam.com/blog/ransomware-recovery-what-you-need-to-know.html
24. https://onestopitservices.konicaminolta.co.th/th/protect-business-data-backup-from-ransomeware/
25. https://wasabi.com/glossary/vendor-lock-in
26. https://destor.com/resources/blog/understanding-vendor-lock-in-and-its-impact-on-data-storage
27. https://taikun.cloud/what-are-some-real-examples-of-companies-using-hybrid-cloud/
28. https://nfina.com/case-studies/hybrid-cloud-case-study/
29. https://stonefly.com/blog/baas-vs-raas-vs-draas-comparison/
30. https://www.sysgroup.com/insights/5-benefits-of-baas-and-draas-for-your-organisation/
31. https://cyberfortress.com/blog/backup-as-a-service-baas-vs-disaster-recovery-as-a-service-draas-understanding-the-difference/
32. https://www.nakivo.com/blog/baas-vs-draas-comparison/
33. https://monsterconnect.co.th/backup-vs-disaster-recovery-vs-draas/
34. https://itbrief.co.nz/story/gartner-predicts-rise-in-saas-backup-prioritisation-by-2028
35. https://itbrief.co.nz/story/gartner-predicts-rise-in-saas-backup-prioritisation-by-2028
36. https://rewind.com/shared-responsibility/
37. https://aws.amazon.com/compliance/shared-responsibility-model/
38. https://www.ibm.com/think/topics/saas-backup
39. https://www.commvault.com/glossary-library/saas-data-protection

40. https://www.veeam.com/whitepapers/extending-zero-trust-to-data-backup-and-recovery_wp.pdf
41. https://tribulant.com/blog/security/securing-backups-in-a-zero-trust-world-what-you-need-to-know/
42. https://www.splunk.com/en_us/blog/learn/rpo-vs-rto.html
43. https://www.acronis.com/en-us/blog/posts/rto-rpo/
44. https://www.enterpriseitpro.net/zerto-platform-continuous-data-protection/
45. https://www.snaplogic.com/glossary/continuous-data-protection
46. https://en.wikipedia.org/wiki/Continuous_data_protection
47. https://www.flexential.com/resources/blog/continuous-data-protection-zerto
48. https://academy.cloudally.com/articles/top-8-microsoft-365-backup-best-practices-for-2025/
49. https://www.ibm.com/think/topics/backup-disaster-recovery