การเอาชนะความท้าทายในการปกป้องข้อมูลทีอยู่ทีนี, และในทุกๆ ที

การรักษาข้อมูลทีสำคัญให้ปลอดภัยในยุคของการประมวลผลแบบคลาวด์

คลิกเพื่อข้ามไปยังบทถัดไป

การ deploy cloud

องค์กรต่างๆ กำลังเคลื่อนไปใช้งานคลาวด์อย่างรวดเร็ว โดยใช้ประโยชน์จากโครงสร้างพื้นฐานในฐานะการให้บริการ (IaaS) ซอฟต์แวร์ในฐานะการให้บริการ (SaaS) และแพลตฟอร์มในฐานะการให้บริการ (PaaS) เพื่อเป็นวิธีใหม่ในการเพิ่มประสิทธิภาพทางธุรกิจแม้ว่าสภาพแวดล้อมเหล่านี้จะมีความเสี่ยงใหม่ๆ ของข้อมูลที่อ่อนไหวก็ตาม

ความท้าทายด้านความปลอดภัยบนคลาวด์

การปรับใช้ระบบคลาวด์มักหมายถึงข้อมูลที่สำคัญถูกเก็บไว้ในสถานที่ซึ่งคุณไม่สามารถควบคุมและจัดการโดยบุคคลที่สามซึ่งอาจเข้าถึงได้โดยไม่ต้องแจ้งให้ทราบ

ความท้าทายขององค์กร

ความท้าทายเมื่อปกป้องข้อมูลในคลาวด์ รวมถึงการตรวจสอบการปฏิบัติตามกฎระเบียบ, การควบคุมการเข้าถึงการตรวจสอบ, ความมั่นใจความเป็นส่วนตัว, การปรับปรุงประสิทธิภาพการผลิตและการแก้ไขช่องโหว่ - ในขณะที่ใช้ประโยชน์จากข้อมูลในสถานที่ของคุณและข้อมูลบนคลาวด์ของคุณร่วมกันเพื่อขับเคลื่อนธุรกิจของคุณไปข้างหน้า

วิธีการปกป้องข้อมูล

เทคโนโลยีความปลอดภัยและการป้องกันข้อมูลควรทำงานในหลาย ๆ สภาพแวดล้อม (ทางกายภาพ, บนคลาวด์และแบบไฮบริด) ในเวลาเดียวกัน โซลูชันความปลอดภัยข้อมูลของคุณควรเป็นแบบอัตโนมัติ, แบบไดนามิกและแบบปรับได้ และควรจัดเตรียมความสามารถในการเข้ารหัสที่สอดคล้องและยืดหยุ่น

ข้อสรุป

ในขณะที่คลาวด์กลายเป็นที่แพร่หลายความปลอดภัยพื้นฐานยังคงเหมือนเดิม การรักษาความปลอดภัยและปกป้องข้อมูลและสนับสนุนการปฏิบัติตามกฎระเบียบ

1.1 การปรับใช้สภาพแวดล้อมแบบคลาวด์

เมื่อไม่กี่ปีที่ผ่านมา หลายองค์กรหันมาใช้สภาพแวดล้อมคลาวด์แบบส่วนตัว (private cloud) เพื่อช่วยเพิ่มความยืดหยุ่นและควบคุมค่าใช้จ่าย - ส่วนใหญ่เกิดจากความไม่พร้อมและขาดการควบคุมในสภาพแวดล้อมคลาวด์แบบสาธารณะ (public cloud) อย่างไรก็ตามในทุกวันนี้ การตัดสินใจที่จะ "ใช้งานบนคลาวด์" นั้นมีการใช้งานแบบไบนารีน้อยลงและมีตัวเลือกให้เลือกมากมายโดยครอบคลุมรูปแบบการปรับใช้ที่แตกต่างกัน (สาธารณะ, ส่วนตัวและไฮบริด) และประเภทการให้บริการ รวมถึง IaaS, PaaS และ SaaS

ด้วยตัวเลือกที่ละเอียดยิ่งขึ้น การปรับใช้ระบบคลาวด์ได้แยกส่วนตามสายงานธุรกิจแทนที่จะเป็นการตัดสินใจด้านไอทีที่ทำให้เป็นมาตรฐาน และในขณะที่รายการตัวเลือกระบบคลาวด์ใหม่นั้นมีอยู่มากมาย องค์กรส่วนใหญ่จะนำสภาพแวดล้อมแบบไฮบริดผสมมาใช้ประโยชน์เพื่อการลงทุนที่มีอยู่ในเมนเฟรมคอมพิวเตอร์, ฐานข้อมูลในสถานที่, การกระจายข้อมูลบิ๊กดาต้า, ระบบไฟล์และอื่นๆ อีกมาก[1]

ระบบคลาวด์ส่วนตัว (Private Cloud) เป็นโครงสร้างพื้นฐานด้านไอทีที่ดำเนินการเฉพาะสำหรับองค์กรเดียว ไม่ว่าจะเป็นการจัดการภายในหรือโดยบุคคลที่สาม ด้วยระบบคลาวด์ส่วนตัว (Private Cloud) องค์กรต่างๆจะควบคุมสแต็กของซอฟต์แวร์ทั้งหมด รวมถึงแพลตฟอร์มพื้นฐานตั้งแต่โครงสร้างพื้นฐานฮาร์ดแวร์ไปจนถึงเครื่องมือวัด บริการคลาวด์ส่วนตัวมีไว้สำหรับการใช้งานหน่วยธุรกิจขององค์กรเดียว (หรือแชร์กับพันธมิตรคู่ค้าเท่านั้น)[1] อย่างไรก็ตามเมื่อเวิร์กโหลดย้ายไปยังคลาวด์ส่วนตัว การรักษาความปลอดภัยข้อมูลในสภาพแวดล้อมเสมือนจะมีความสำคัญมากขึ้นโดยเฉพาะอย่างยิ่งเมื่อเวิร์กโหลดที่มีระดับความน่าเชื่อถือแตกต่างกันถูกรวมเข้าด้วยกันเพื่อทำงานบนฮาร์ดแวร์ทางกายภาพเดียวกัน งานวิจัยของการ์ทเนอร์แสดงให้เห็นว่าจะยังคงมีการใช้และการลงทุนอย่างมีนัยสำคัญในระบบคลาวด์ส่วนตัวต่อไป องค์กรเกือบทุกแห่งที่การ์ตเนอร์สำรวจต้องการใช้ประโยชน์จากโมเดลแบบไฮบริดคลาวด์ - ด้วยองค์ประกอบคลาวด์ทั้งแบบส่วนตัวและแบบสาธารณะ องค์กรต่างๆ ใช้ตัวเลือกการประมวลผลแบบคลาวด์สาธารณะ (Public Cloud) เบ็ดเสร็จเพื่อให้สามารถทำงานได้เร็วขึ้น ให้บริการที่ลื่นไหลและเพื่อเพิ่มความคล่องตัวทางธุรกิจและกระตุ้นนวัตกรรม การประมวลผลแบบคลาวด์สาธารณะจะช่วยเติมเต็มบทบาทสำคัญสำหรับนวัตกรรมและเป็นผลให้คาดว่าจะเติบโตที่ร้อยละ 15.2 ตลอดทั้งปี 2019[1]

เมื่อกล่าวถึงสภาพแวดล้อมแบบคลาวด์ ไม่ว่าจะเป็นในระบบคลาวด์สาธารณะหรือสภาพแวดล้อมที่เป็นส่วนตัว การควบคุมความปลอดภัยของข้อมูลและการป้องกันจะต้องปกป้องข้อมูลที่มีความละเอียดอ่อน - และรองรับข้อกำหนดทั้งของภาครัฐและภาคอุตสาหกรรมที่เพิ่มขึ้นอย่างต่อเนื่อง

1.2 การปรับใช้สภาพแวดล้อมแบบคลาวด์

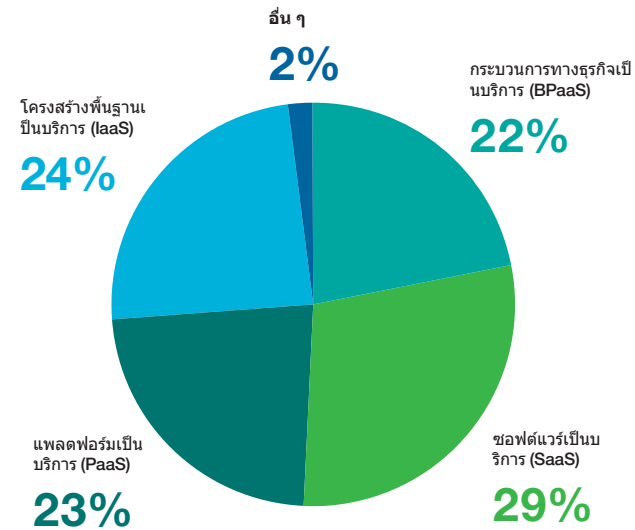
ประเภทบริการที่พบมากที่สุดคือ IaaS, PaaS และ SaaS วิธีที่ง่ายที่สุดในการมองเห็นความแตกต่างคือการพิจารณาจาก IT stack ของคุณ ที่ด้านล่างคุณมีโครงสร้างพื้นฐานของคุณ - ซึ่งรวมถึงฮาร์ดแวร์, เซิร์ฟเวอร์และเครือข่ายของคุณ - โดยทำหน้าที่เป็นฐานรากด้านไอทีของคุณ เหนือโครงสร้างพื้นฐานนี้ คุณจะมีซอฟต์แวร์หรือแพลตฟอร์มมิดเดิลแวร์ที่ให้เครื่องมือที่นักพัฒนาซอฟต์แวร์ของคุณต้องการเพื่อปรับใช้แอปพลิเคชันธุรกิจ และที่ด้านบนสุด คุณจะมีแอปพลิเคชันธุรกิจที่เชื่อมต่อกับพนักงานและลูกค้าภายใน

IaaS ช่วยให้องค์กรต่างๆ สามารถดูแลรักษาซอฟต์แวร์ที่มีอยู่จริงและแพลตฟอร์มมิดเดิลแวร์และแอปพลิเคชันทางธุรกิจ แต่จัดหาการจัดการโครงสร้างพื้นฐานที่จำเป็นจากภายนอก บริษัทต่างๆ ดำเนินการด้วยความตั้งใจที่จะใช้ประโยชน์จากคลาวด์อย่างรวดเร็วในขณะที่ลดผลกระทบและใช้ประโยชน์จากการลงทุนที่มีอยู่

PaaS จะช่วยให้บริษัทต่างๆ จัดหาโครงสร้างพื้นฐานรวมถึงมิดเดิลแวร์หรือซอฟต์แวร์จากภายนอกได้ ซึ่งจะเป็นการลดภาระที่สำคัญของบริษัทจากมุมมองด้านไอทีและช่วยให้บริษัทสามารถมุ่งเน้นไปที่การพัฒนาแอปพลิเคชันทางธุรกิจที่เป็นนวัตกรรมได้

SaaS เป็นตัวเลือกที่ยอดเยี่ยมที่สุดซึ่งให้บริการด้านไอทีทั้งหมดและช่วยให้องค์กรโฟกัสไปที่จุดแข็งหลักของพวกเขา (เช่น การดูแลสุขภาพ, การให้บริการทางการเงิน) แทนการใช้เวลาและการลงทุนด้านเทคโนโลยีที่สามารถให้ผู้เชี่ยวชาญด้านเทคโนโลยีทำแทนได้

ในแต่ละขั้นตอนตั้งแต่ IaaS ถึง PaaS ถึง SaaS หลายองค์กรต่างยอมแพ้ต่อการควบคุมระบบที่จัดเก็บ, จัดการและแจกจ่ายข้อมูลที่ละเอียดอ่อนของพวกเขา ทำให้ต้องเพิ่มความไว้วางใจต่อบุคคลที่สามที่ทำให้มีความเสี่ยงเพิ่มขึ้นอีกด้วย



ภาพที่ 1: คำถามสำรวจความคิดเห็น "งบประมาณในปัจจุบันจัดสรรให้กับบริการคลาวด์ "สาธารณะ" อย่างไรระหว่างระบบคลาวด์ประเภทต่อไปนี้"

แหล่งที่มา: Ed Anderson และ Sid Nag, "Market Trends: Cloud Adoption Trends Favor Public Cloud With a Hybrid Twist," Gartner, 4 สิงหาคม 2016 ID: G00294424

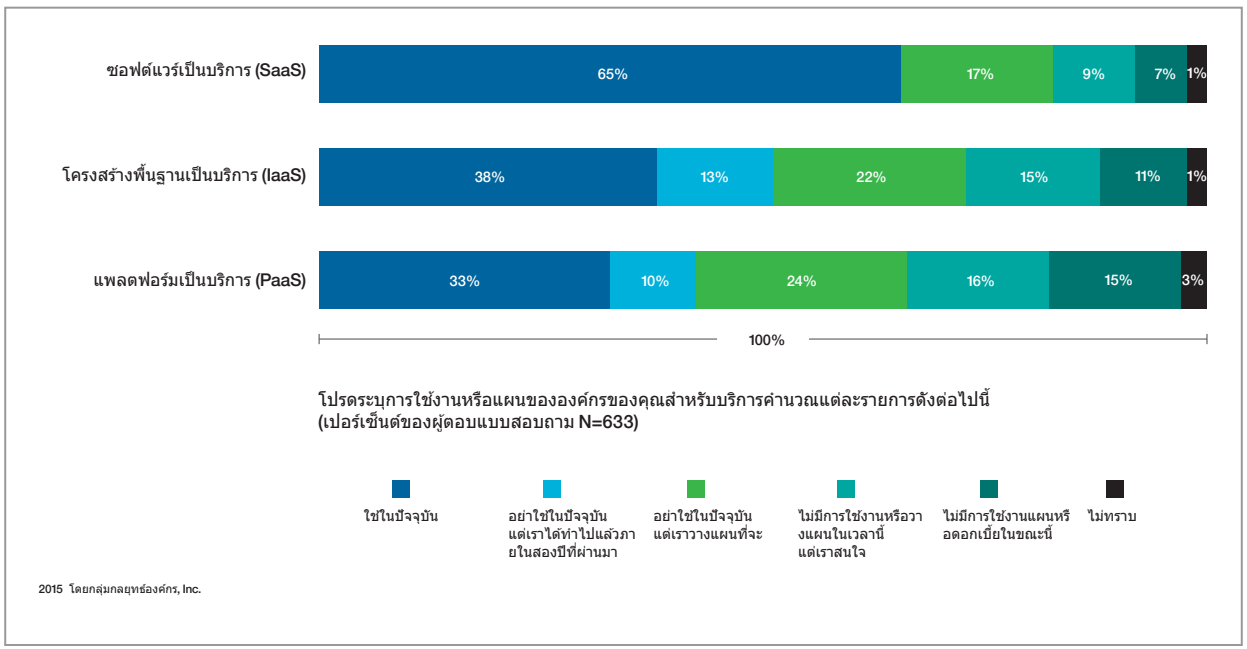
1.3 การปรับใช้สภาพแวดล้อมแบบคลาวด์

"การใช้คลาวด์" ไม่ใช่ไบนารี จากการศึกษาผู้มีอำนาจตัดสินใจด้านไอทีขององค์กรมากกว่า 600 คน แสดงให้เห็นว่าบริษัทส่วนใหญ่ที่ทำการสำรวจที่อย่างน้อยได้นำแอปพลิเคชัน SaaS ไปใช้ น้อยกว่าร้อยละ 20 ของผู้ตอบแบบสอบถามไม่มีแผนหรือความสนใจในการใช้บริการ SaaS

การปรับใช้ PaaS ซึ่งต้องมีการจัดเก็บข้อมูลและประมวลผลนอกสถานที่นั้นทำความเข้าใจได้ช้ากว่าแอปพลิเคชันคลาวด์ทีละส่วน แต่ 67% ของผู้ตอบแบบสอบถามใช้, เคยใช้หรือวางแผนที่จะใช้งาน PaaS

การใช้โครงสร้างพื้นฐานคลาวด์ - IaaS - ซึ่งย้ายการติดตั้งและบำรุงรักษาโครงสร้างพื้นฐานทางกายภาพจากองค์กรไปยังผู้ให้บริการเฉพาะ อยู่ระหว่างค่าสถิติของ PaaS และ SaaS ในการสำรวจนี้ 73% ของผู้ตอบแบบสอบถาม "ใช้หรือวางแผนที่จะใช้" โครงสร้างพื้นฐานคลาวด์บางรูปแบบหรือเคยทดลองใช้มาแล้ว

ความท้าทายในการปกป้องข้อมูลบนคลาวด์เสมือนและส่วนตัว



2.1 ความท้าทายด้านความปลอดภัยบนคลาวด์

คลาวด์เหมาะอย่างยิ่งสำหรับการจัดเก็บข้อมูลระยะยาวระดับองค์กร - ด้วยความทีประหยัดจากขนาดทั้งอุปกรณ์และการจัดการทีสามารถทำให้ดาต้าเซ็นเตอร์บนคลาวด์เป็นสถานทีทีชาญฉลาดในการจัดเก็บข้อมูลทางธุรกิจทีสำคัญได้มากกว่าสแต็กเซิร์ฟเวอร์ในห้องโถง นั่นเป็นเพราะแม้ว่าค่าใช้จ่ายในการจัดหาพืนทีจัดเก็บลดลง แต่ค่าใช้จ่ายในการใช้งานทางธุรกิจทีเพิมขึนและบุคลากรในการจัดการพืนทีจัดเก็บยังคงเพิมขึนอย่างต่อเนืองอย่างไรก็ตามในขณะทีการจัดเก็บข้อมูลอยู่ในการดูแลของผู้ดูแลระบบโดยเฉพาะ ซึงจะสามารถช่วยประหยัดเงินและเวลา แต่ยังสามารถสร้างความท้าทายด้านความปลอดภัยทีร้ายแรงและสร้างความเสียงในระดับใหม่

สิงสำคัญคือต้องตระหนักคือไม่ว่ารูปแบบการปรับใช้หรือประเภทบริการจะเป็นแบบใด - หลักการพืนฐานของความปลอดภัยของข้อมูลไม่ควรเปลียนแปลง สิงทีเปลียนแปลงไปคือข้อมูลทีละเอียดอ่อนของคุณตังอยู่ในหลายสถานทีทังภายในกำแพงของบริษัทเองและภายนอกสถานที ซึงหมายความว่าการควบคุมความปลอดภัยจำเป็นต้องมีอยู่ในทีทีข้อมูลของคุณไปถึง เมือประเมินเทคโนโลยีความปลอดภัยของข้อมูล, เลือกโซลูชันทีทำงานในสภาพแวดล้อมทีหลากหลายอย่างทีโปร่งใสและดำเนินงานพร้อมๆ กัน ควรตรวจสอบให้แน่ใจว่าโซลูชันความปลอดภัยของข้อมูลนันมีการเปลียนแปลงตลอดเวลาและปรับตัวเข้ากับสภาพแวดล้อมต่างๆ ได้อย่างเต็มที ดังนันคุณไม่จำเป็นต้องใช้ "การป้องกัน" ข้อมูลเพิมเติมอีกs.

รักษาข้อมูลให้ปลอดภัยทุกๆ ที จากทุกๆ คน

สิงทีสำคัญทีสุดของความท้าทายเหล่านีเห็นได้ชัด: ข้อมูลทีมีความละเอียดอ่อน ทุกๆ ทีในตอนนีทังภายในและภายนอกไฟร์วอลล์ของคุณ กำลังได้รับการจัดการอย่างใดอย่างหนึงโดยบุคคลทีสาม คุณไม่สามารถปกป้องข้อมูลทีสำคัญของคุณได้ต่อไปด้วยการปิดล็อคการเข้าถึงเครือข่ายอย่าง่ายๆ ทีจริงแล้วคุณต้องพึงพาเครือข่ายในการเข้าถึงและแชร์ข้อมูลของคุณ ซึงจะทำให้ความปลอดภัยของข้อมูลส่วนใหญ่อยู่ในมือของผู้คนมากกว่าในอดีต และมีบุคคลจำนวนมากทีไม่ได้ทำงานโดยตรงกับบริษัทของคุณอีกต่อไป โดยทัวไปแล้วในสภาพแวดล้อมแบบคลาวด์ ผู้ให้บริการคลาวด์ (Cloud Service Providers) จะมีความสามารถในการเข้าถึงข้อมูลทีสำคัญของคุณ ซึงทำให้ CSP เป็นเขตแดนใหม่ในการคุกคามจากภายใน นอกจากนี อาชญากรไซเบอร์ก็รู้ว่า CSP จัดเก็บข้อมูลสำคัญจำนวนมากอีกด้วย ความเสียงทังสองอย่างนีทำให้ความสามารถเช่น การเข้ารหัสข้อมูลและการตรวจสอบข้อมูลกิจกรรมเป็นส่วนทีมีค่า โดยเฉพาะอย่างยิงของกลยุทธ์การรักษาความปลอดภัยของคุณ

2.2 ความท้าทายด้านความปลอดภัยบนคลาวด์

การโอนย้ายข้อมูลเป็นเหตุผลหนึ่งที่พื้นที่เก็บข้อมูลบนคลาวด์เป็นทางเลือกที่ประหยัด ค่าใช้จ่ายด้านโครงสร้างพื้นฐาน (จากอสังหาริมทรัพย์ไปสู่ค่าใช้จ่ายด้านพลังงาน) มีความแตกต่างกันอย่างมากตามสภาพทางภูมิศาสตร์และแม้กระทั่งตามห้วงเวลาของวัน ต้นทุนการจัดเก็บและประสิทธิภาพของสื่อประเภทเดียวกันก็เปลี่ยนไปเช่นกัน เทป, ดิสก์แบบหมุนและที่เก็บข้อมูลแบบ Solid-Stage Storageล้วนมีความก้าวหน้าด้านความจุ, ความเร็วและความน่าเชื่อถือ รวมถึงเทคโนโลยีการจัดเก็บข้อมูลแบบผสมผสานที่ประหยัดที่สุดสำหรับองค์กรที่สามารถเปลี่ยนแปลงได้อย่างรวดเร็ว ดังนั้น ด้วยที่เก็บข้อมูลบนคลาวด์ ข้อมูลของคุณในวันพรุ่งนี้ อาจอยู่ในสถานที่ที่แตกต่างกันในสื่อที่แตกต่างจากที่ตั้งของวันนี้ เช่นเดียวกับการจำลองเสมือน ไม่เพียงแต่ข้อมูลบนคลาวด์เท่านั้น แต่ยังมีทรัพยากรการประมวลผลบนคลาวด์ที่อาจเปลี่ยนได้ - อย่างโปร่งใสและรวดเร็ว - ทั้งในที่ตั้งและฮาร์ดแวร์ลักษณะที่เปลี่ยนแปลงของระบบคลาวด์ หมายความถึงวิธีการรักษาความปลอดภัยสำหรับพื้นที่เก็บข้อมูลบนคลาวด์จำเป็นต้องใช้ที่เก็บข้อมูลประเภทต่างๆ วิธีการของคุณจะต้องพิจารณาถึงการทำสำเนาไม่ว่าจะเป็นการสำรองข้อมูลระยะยาวหรือสำเนาชั่วคราวที่สร้างขึ้นในระหว่างการเคลื่อนย้ายข้อมูล เพื่อจัดการกับความท้าทายเหล่านี้ให้เลือกโซลูชันข้ามแพลตฟอร์มและใช้การเข้ารหัสที่รัดกุม

แม้ว่าข้อมูลของคุณจะไม่ได้รับการจัดเก็บไว้ในระบบคลาวด์เป็นหลัก แต่ทั้งแบบฟอร์มที่ทิ้งข้อมูลและส่งคืนให้กับองค์กรของคุณและข้อมูลเส้นทางจะถือว่ามีความสำคัญ แม้ในเบื้องต้นจะเก็บข้อมูลที่เข้ารหัสและไฟร์วอลล์ไว้ที่ไซต์งาน หากส่วนหนึ่งส่วนใดถูกเปิดเผยเมื่อถูกส่งไปยังการสำรองข้อมูลนอกสถานที่หรือสำหรับการประมวลผลโดยบุคคลที่สาม ข้อมูลที่ละเอียดอ่อนจะมีความปลอดภัยเหมือนกันกับจุดอ่อนที่สุดในห่วงโซ่การประมวลผลข้อมูล

การปกป้องข้อมูลของคุณอย่างมีประสิทธิภาพเมื่ออยู่ในคลาวด์นั้นมีทั้งมาตรการเชิงป้องกันและการป้องกัน (เช่น การปิดกั้นการเข้าถึงพอร์ตที่ไม่ผ่านการอนุมัติ) และมาตรการที่ใช้งานอยู่เช่น การสแกนเพื่อเข้าถึงข้อมูลที่น่าสงสัยอย่างต่อเนื่อง ในหมู่มาตรการที่คุณสามารถทำได้คือการใช้การเข้ารหัสสำหรับข้อมูลที่ละเอียดอ่อนของคุณ ขณะที่การตรวจจับมัลแวร์หรือการวิเคราะห์พฤติกรรมที่ออกแบบมาเพื่อการเข้าถึงที่น่าสงสัย สามารถช่วยป้องกันการรั่วไหลของข้อมูลภายในและภายนอก - และให้บริการฟังก์ชันที่มีคุณค่าในสิทธิของตนเอง - การเข้ารหัสจะช่วยปกป้องข้อมูลในทุกที่ที่มีอยู่ ไม่ว่าจะอยู่นิ่งๆ หรือกำลังมีการเคลื่อนย้าย

2.3 ความท้าทายด้านความปลอดภัยบนคลาวด์

ผลกระทบของการบริหารและกฎระเบียบ
ความเป็นจริงของการจัดเก็บและการประมวลผลบนระบบคลาวด์หมายความว่าการรักษาความปลอดภัยข้อมูลที่มีความละเอียดอ่อนบนระบบคลาวด์และระบบคลาวด์ไฮบริดนั้นไม่ได้ราบรื่นดังที่ผู้ดูแลระบบคาดหวัง เครื่องมือรักษาความปลอดภัยที่ให้บริการอินเทอร์เฟซแบบครบวงจรในคลาวด์ปลายทาง - ตั้งแต่ฟาร์มเซิร์ฟเวอร์นอกสถานที่ไปจนถึงเครื่องเสมือนในโครงสร้างพื้นฐานคลาวด์สาธารณะ - เป็นการเริ่มต้นที่ดีในการตระหนักถึงความคาดหวังของการดูแลระยะไกลที่มีประสิทธิภาพ

ที่สำคัญพอๆ กันคือข้อกำหนดด้านกฎระเบียบและอธิปไตยของข้อมูล - กล่าวอีกนัยหนึ่งคือกฎเกณฑ์ที่ระบุถึงความปลอดภัยของข้อมูลและการป้องกันเมื่อข้อมูลที่ละเอียดอ่อนถูกเก็บไว้ในสถานที่เฉพาะ การจัดเก็บข้อมูลในระบบคลาวด์อาจส่งผลให้ข้อมูลที่ละเอียดอ่อนถูกเก็บไว้ในสถานที่ซึ่งกฎหมายที่เข้มงวดมีผลบังคับใช้มากกว่าในที่อยู่เดิมของข้อมูล ตัวอย่างเช่น การป้องกันที่เข้มงวดสำหรับข้อมูลส่วนบุคคลของบุคคลภายในประเทศในกลุ่มสหภาพยุโรป (EU) ได้รับคำสั่งจากข้อกำหนดของกฎหมายว่าการคุ้มครองข้อมูลทั่วไปของสหภาพยุโรป (GDPR) ข้อกำหนดเหล่านี้บังคับใช้กับบริษัทที่อยู่ในภูมิภาคอื่นๆ ของโลกที่เก็บและเข้าถึงข้อมูลส่วนบุคคลของผู้อยู่อาศัยในสหภาพยุโรป

รู้ว่าใครกำลังเข้าถึงข้อมูลของคุณ:
IBM® Security Guardium® สามารถช่วยรักษาความปลอดภัยให้ระบบคลาวด์และโครงสร้างพื้นฐานคลาวด์แบบไฮบริดของคุณด้วยเครื่องมือตรวจสอบและประเมินที่เปิดเผยความผิดปกติและความเสี่ยงต่างๆ

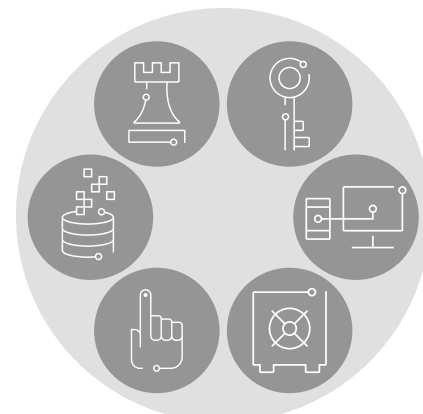
3.1 ความท้าทายขององค์กร

3

องค์กรต่างๆ ยังคงถูกท้าทายอย่างมากเมื่อพยายามปกป้องข้อมูลที่มีความละเอียดอ่อนและกฎระเบียบที่ซับซ้อนก็เป็นอีกเหตุผลหนึ่ง บริษัทวิจัย Forrester Researc ชี้ให้เห็นว่าในวันนี้ "สถาปนิกองค์กรและผู้เชี่ยวชาญด้านความปลอดภัยส่วนใหญ่ต้องดิ้นรนเพื่อปรับปรุงความปลอดภัยของข้อมูลหรือปฏิบัติตามข้อกำหนดเนื่องจากการเติบโตของข้อมูลแบบ silo และปริมาณข้อมูลที่เพิ่มขึ้น การใช้นโยบายควบคุมการเข้าถึงอย่างสม่ำเสมอในฐานข้อมูล, คลังข้อมูล, Hadoop, NoSQL และไฟล์ต่างๆ กลายเป็นสิ่งที่ท้าทายอย่างยิ่ง"[2]

การจำลองเสมือน (Virtualization) มีแนวโน้มที่จะทำให้การใช้การควบคุมความปลอดภัยและกลไกการปฏิบัติตามกฎระเบียบสะดวกขึ้น แต่เฉพาะในกรณีที่สภาพแวดล้อมคลาวด์เสมือนหรือแบบส่วนตัวถึงจะรองรับการรักษาความปลอดภัยข้อมูลที่มีความสำคัญได้

ความท้าทายในการปกป้องข้อมูลบนคลาวด์เสมือนและส่วนตัว



การปฏิบัติตาม
การควบคุมการเข้าถึง
ความเป็นส่วนตัว
ประสิทธิภาพการผลิต
ช่องโหว่

ภาพที่ 2: การปกป้องข้อมูลที่จัดเก็บบนคลาวด์ยังต้องการให้ผู้ดูแลระบบให้การดูแลด้านความปลอดภัยจากการรักษาความปลอดภัยและความเป็นส่วนตัวไปจนถึงการปฏิบัติตามกฎระเบียบในหลายๆ โดเมน

3.2 ความท้าทายขององค์กร

การปฏิบัติตามข้อกำหนด

ให้ลองนึกถึงว่าข้อมูลที่มีความละเอียดอ่อนอยู่ที่ไหนในสภาพแวดล้อมคลาวด์ สิ่งสำคัญคือการระบุและจำแนกประเภทข้อมูลที่ละเอียดอ่อน และกำหนดนโยบายสำหรับการใช้งานไม่ว่าจะในระบบคลาวด์สาธารณะหรือในระบบคลาวด์ส่วนตัว หากข้อมูลอยู่ในคลาวด์สาธารณะ คุณต้องเข้าใจว่าผู้ให้บริการโครงสร้างพื้นฐานคลาวด์มีแผนอย่างไรในการปกป้องข้อมูลที่มีความละเอียดอ่อนของคุณ

ไม่ว่าในกรณีใด การทำความเข้าใจว่ามีข้อมูลอยู่ที่ใด, โดเมนใดที่มีข้อมูลอยู่และความสัมพันธ์เหล่านี้ทั่วทั้งองค์กรจะช่วยให้องค์กรกำหนดนโยบายที่เหมาะสมสำหรับการรักษาความปลอดภัยและการเข้ารหัสข้อมูลนั้น และแสดงการปฏิบัติตามกฎระเบียบ เช่น Sarbanes-Oxley (SOX) บัตรชำระเงินมาตรฐานความปลอดภัยของข้อมูลอุตสาหกรรม (PCI DSS), โปรโตคอลการรักษาความปลอดภัยเนื้อหาอัตโนมัติ (SCAP), พระราชบัญญัติการจัดการความปลอดภัยข้อมูลของรัฐบาลกลาง (FISMA), พระราชบัญญัติประกันสุขภาพแบบพกพาและความรับผิดชอบพระราชบัญญัติ (HIPAA) และเทคโนโลยีสารสนเทศด้านสุขภาพสำหรับกฎหมายเศรษฐกิจและสุขภาพ (HITECH) กฎระเบียบด้านการปฏิบัติตามกฎระเบียบยังคงมีอยู่และองค์กรต่างๆ ยังคงรับผิดชอบแม้กระทั่ง ข้อมูลที่ย้ายไปยังระบบคลาวด์

ความเป็นส่วนตัว

ความท้าทายอีกประการหนึ่งสำหรับผู้ดูแลระบบในการเข้าถึงข้อมูล คือ การรับรองว่าผู้ที่มีเหตุผลทางธุรกิจที่ถูกต้องเท่านั้นที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ เช่น แพทย์จำเป็นต้องดูข้อมูลที่ละเอียดอ่อนด้านอาการของผู้ป่วยและข้อมูลการคาดการณ์สถานะของโรค ในขณะที่เจ้าหน้าที่เก็บเงินต้องการเพียงหมายเลขประกันและที่อยู่สำหรับการเรียกเก็บเงินของผู้ป่วย

3.3 ความท้าทายขององค์กร

การควบคุมการเข้าถึง

อาชญากรไซเบอร์มีเจตนาที่ไร้ศีลธรรมและสร้างความวุ่นวาย พวกเขาอาจเป็นนักวิทยาศาสตร์คอมพิวเตอร์ที่พยายามจะอวดหรือแสดงความคิดเห็นทางการเมืองหรืออาจจะเป็นผู้บุกรุกที่มีความชำนาญ รัฐต่างชาติที่ให้การสนับสนุนแฮ็กเกอร์เพื่อรวบรวมข้อมูลจากหน่วยงานรัฐบาล ผู้โจมตีที่อาจไม่พอใจพนักงาน การละเมิดยังอาจเกิดขึ้นโดยบังเอิญ เช่น เมื่อการอนุมัติสิทธิ์ถูกตั้งค่าอย่างไม่ถูกต้องในตารางฐานข้อมูลหรือเมื่อข้อมูลรับรองของพนักงานถูกเจาะ แนวทางปฏิบัติที่ดีที่สุดแนะนำให้อนุญาตผู้ใช้ปลายทางทั้งที่ได้รับสิทธิพิเศษและสามัญด้วย "สิทธิ์ที่อนุมัติให้น้อยที่สุด" เพื่อลดการใช้สิทธิ์และข้อผิดพลาดให้น้อยลง องค์กรควรปกป้องข้อมูลจากการโจมตีทั้งภายในและภายนอกในสภาพแวดล้อมคลาวด์ทั้งแบบกายภาพ, แบบเสมือนและแบบส่วนตัว

การป้องกันขอบเขตเองก็มีความสำคัญ และมีความสำคัญเท่าเทียมกันกับการปกป้องข้อมูลที่มีความละเอียดอ่อน หากมีการละเมิดขอบเขต ข้อมูลที่ละเอียดอ่อนจะต้องมีการรักษาความปลอดภัยอยู่แล้ว (และใช้ไม่ได้กับขโมย) เพื่อลดผลกระทบของการละเมิดและให้แน่ใจว่าไม่เปิดช่องว่างให้แฮ็กเกอร์ดำเนินการโดยอิสระ การป้องกันควรรวมถึงโซลูชันการรักษาความปลอดภัยข้อมูลแบบเลเยอร์ ดังนั้นผู้ดูแลระบบสามารถเข้าใจสิ่งที่เกิดขึ้นภายในระบบคลาวด์ส่วนตัว - ตัวอย่างเช่น โดยการทำความเข้าใจรูปแบบการเข้าถึงข้อมูลและพฤติกรรมผู้ใช้ที่ได้รับสิทธิพิเศษ

ความท้าทายคือการให้การเข้าถึงที่เหมาะสมและการปกป้องข้อมูลในขณะที่ตอบสนองความต้องการทางธุรกิจและสร้างความมั่นใจว่าข้อมูลนั้นได้รับการจัดการบนพื้นฐาน "จำเป็น-ต้อง-รู้" ไม่ว่าจะอยู่ที่ไหนก็ตาม

ประสิทธิภาพการผลิต

นโยบายความปลอดภัยและความเป็นส่วนตัวควรเป็นใช้งานและมีการยกระดับ ให้ไม่รบกวนการดำเนินธุรกิจ โดยควรสร้างไว้ในการปฏิบัติงานประจำวันและใช้งานได้อย่างราบรื่นทั้งภายในและทั่วทุกสภาพแวดล้อม - ในสภาพแวดล้อมคลาวด์ส่วนตัว, สภาพแวดล้อมคลาวด์สาธารณะ, คลาวด์แบบ on-premise - โดยไม่มีผลกระทบต่อประสิทธิภาพการผลิตของผู้ใช้ ตัวอย่างเช่น เมื่อปรับใช้คลาวด์ส่วนตัวเพื่ออำนวยความสะดวกในการทดสอบแอปพลิเคชันให้พิจารณาใช้การเข้ารหัสหรือ Token เพื่อลดความเสี่ยงในการเปิดเผยข้อมูลที่มีความละเอียดอ่อน

3.4 ความท้าทายขององค์กร

ช่องโหว่

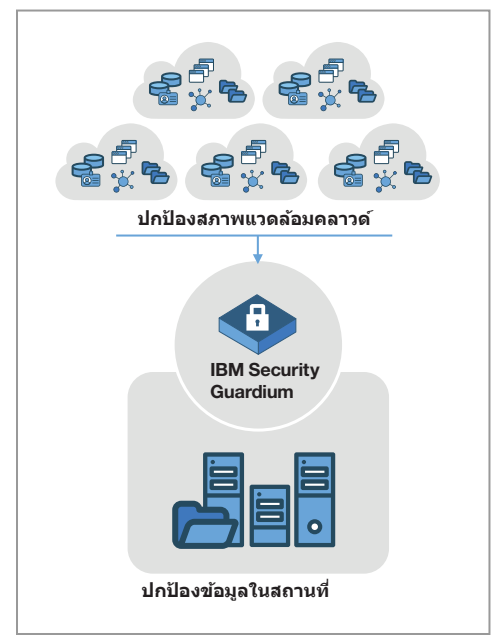
ปัจจุบันองค์กรต่างๆ มีเทคโนโลยีด้านการรักษาความปลอดภัยที่หลากหลายเพื่อปกป้องข้อมูลขององค์กรและสนับสนุนการปฏิบัติตามกฎระเบียบ แต่จำนวนช่องโหว่ของที่เก็บข้อมูลมีมากมายและอาชญากรสามารถใช้ประโยชน์ได้แม้จากช่องโหว่ที่เล็กที่สุด สิ่งสำคัญคือต้องเข้าใจช่องโหว่จากทุกมุมมองและพัฒนาวิธีการจัดการช่องโหว่เหล่านั้น ช่องโหว่ที่พบบ่อยๆ ได้แก่ โปรแกรมแก้ไขที่ขาดหายไป, การกำหนดค่าผิดพลาดและการตั้งค่าระบบเริ่มต้น ความซับซ้อนนี้ยากยิ่งขึ้นในการติดตามและจัดการเมื่อที่เก็บข้อมูลกลายเป็นเสมือนจริง

เช่น ในขณะที่องค์กรย้ายไปสู่ระบบคลาวด์ส่วนตัวและสาธารณะ แต่โซลูชันเหล่านี้ไม่ได้ปรับขนาดตามไปด้วย นอกจากนี้ วิธีการเข้ารหัสบางอย่างยังเชื่อมโยงกับฮาร์ดแวร์หรือทรัพยากรเครือข่ายโดยเฉพาะอีกด้วย ในสภาพแวดล้อมแบบคลาวด์ ผู้ดูแลระบบไม่สามารถเชื่อถือการเข้าถึงโครงสร้างพื้นฐานฮาร์ดแวร์ระดับต่ำได้

ปัญหาอื่นๆ ที่มักเกิดขึ้นเมื่อมีการใช้คลาวด์ส่วนตัวคือการใช้สำหรับการทดสอบหรือการพัฒนาแอปพลิเคชัน ฐานข้อมูลใหม่จะถูกสร้างและถูกเลิกใช้งานอย่างสม่ำเสมอ ข้อมูลจะต้องได้รับการปกป้องเนื่องจากฐานข้อมูลเหล่านี้ถูกสร้างขึ้นแบบไดนามิกเพื่อรองรับการทดสอบและการพัฒนา วิธีการรักษาความปลอดภัยข้อมูลที่ปรับขนาดได้สำหรับสภาพแวดล้อมคลาวด์ส่วนตัว หมายความว่าเมื่อฐานข้อมูลใหม่เหล่านี้ถูกสร้างขึ้น และจะถูกค้นพบโดยอัตโนมัติและข้อมูลที่มีอยู่อยู่ในนั้นจะถูกจำแนก, ตรวจสอบและป้องกันโดยอัตโนมัติ

สุดท้ายให้นึกถึงการใช้เครื่องมือที่ผลิตขึ้นเองที่มีอยู่ในปัจจุบันเพื่อความปลอดภัยของข้อมูล ตัวอย่างเช่น ขั้นตอนการปกปิดข้อมูลหรือสคริปต์การตรวจสอบกิจกรรมฐานข้อมูล จำเป็นต้องมีการเปลี่ยนแปลงการเข้ารหัสเพื่อให้สามารถทำงานบนฐานข้อมูลเสมือนจริงได้หรือไม่? มีโอกาสที่จะต้องลงทุนที่สำคัญในการอัปเดตโซลูชันที่ผลิตเองเหล่านี้ - จากนั้นคุณจะยังคงเผชิญกับความท้าทายที่สำคัญ เป็นสิ่งที่ดีที่จะมีการเพิ่มฐานข้อมูลใหม่หรือแหล่งข้อมูลอื่นๆ กระบวนการและขั้นตอนการรักษาความปลอดภัยควรดำเนินการโดยไม่มีการแทรกแซงแบบ Manual สรุปคือกลยุทธ์ความปลอดภัยควรถูกสร้างขึ้นในโครงสร้างของสภาพแวดล้อมคลาวด์

วิธีการปกป้องข้อมูล



4.1 วิธีการปกป้องข้อมูล

องค์กรควรมองหาการรวมศูนย์รักษาความปลอดภัยของข้อมูลและการควบคุมการป้องกันในสภาพแวดล้อมคลาวด์ส่วนตัวและสาธารณะ เช่นเดียวกับในส่วนที่เหลือขององค์กรและให้แน่ใจว่ามีการแบ่งแยกหน้าที่เพื่อให้ผู้ดูแลข้อมูลไม่ได้เป็นผู้ดูแลระบบรักษาความปลอดภัยหรือผู้ตรวจสอบ องค์ประกอบสำคัญของกลยุทธ์คลาวด์ที่ปลอดภัยประกอบด้วย:

- ทำความเข้าใจว่ามีข้อมูลสำคัญอยู่ที่ไหนและใครบ้างที่สามารถเข้าถึงได้ องค์กร ไม่สามารถปกป้องข้อมูลที่สำคัญด้วย การเข้ารหัสหรือใช้การควบคุมการเข้าถึงที่ ยากลำบาก เว้นแต่ว่าพวกเขารู้ว่าอยู่ที่ไหน และเกี่ยวข้องกับองค์กรอย่างไร.
- ปกป้องข้อมูลที่มีความละเอียดอ่อนและไม่มีโครงสร้างทั้งแบบออนไลน์และออฟไลน์ด้วยเทคโนโลยีที่เหมาะสมและกำหนดข้อกำหนดการเข้าถึงที่เหมาะสม
- การปกป้องข้อมูลนอกเหนือจากการผลิต ในการพัฒนาการทดสอบและสภาพแวดล้อม การประกันคุณภาพ
- ตรวจสอบการเข้าถึงข้อมูลที่สำคัญอย่างปลอดภัย และต่อเนื่องไม่ว่าจะอยู่ที่ไหน
- แสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดเพื่อส่งการตรวจสอบด้วยรายงานที่สร้างไว้ล่วงหน้าสำหรับ ผู้ตรวจสอบบัญชีและด้วยขั้นตอนการทำงานอัตโนมัติ เพื่อให้คุณสามารถรับรายงานที่ถูกต้องกับคนที่เหมาะสม ในเวลาที่เหมาะสมสำหรับการออกจากระบบ

กลยุทธ์การป้องกันที่ครอบคลุมสำหรับสภาพแวดล้อมคลาวด์และไฮบริดคลาวด์ทั้งหมด ควรมีการแจ้งเตือนเกี่ยวกับพฤติกรรมที่น่าสงสัยให้กับผู้ดูแลความปลอดภัย องค์กรควรพิจารณาโซลูชันความปลอดภัยของข้อมูลที่ให้การสนับสนุนการปฏิบัติตามกฎระเบียบโดยอัตโนมัติเพื่อปรับปรุงกระบวนการปฏิบัติตาม

กระบวนการรักษาความปลอดภัยของข้อมูลสำหรับสภาพแวดล้อมคลาวด์จำเป็นต้องติดตามข้อมูลอย่างต่อเนื่องและให้ข้อมูลเชิงลึกว่าใครกำลังเข้าถึงข้อมูลระหว่างแอปพลิเคชันฐาน, ฐานข้อมูล, คลังสินค้าและการแชร์ไฟล์, สภาพแวดล้อมบิ๊กดาต้าและอื่น ๆ วิธีการดังกล่าวสามารถช่วยให้มั่นใจในการปกป้องแบบ 360 องศาสำหรับข้อมูลองค์กรที่มีความละเอียดอ่อนไม่ว่าจะอยู่ที่ใด

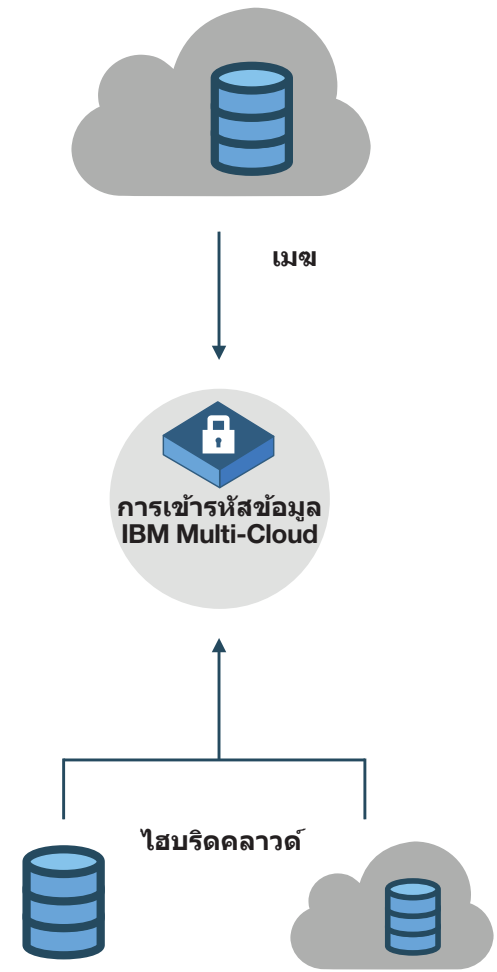
4.2 วิธีการปกป้องข้อมูล

ภาระด้านกฎระเบียบของผู้ถือครองข้อมูล (เช่นเดียวกับความเสี่ยงของการละเมิด) สามารถทำให้องค์กรต่างๆ พิจารณาที่เก็บข้อมูลบนคลาวด์แบบใหม่หรือแบบขยายอย่างรอบคอบ การเข้ารหัสที่รัดกุมเป็นคำตอบที่ชัดเจนที่สุดสำหรับความท้าทายในการรักษาความปลอดภัยข้อมูลที่มีความละเอียดอ่อนทั้งในและนอกสถานที่ แต่การเข้ารหัสทำให้เกิดปัญหาที่ซับซ้อนของการถ่ายโอนและการรับประกันการเข้าถึงข้อมูลนั้นจะดีพอๆ กับความปลอดภัยและความน่าเชื่อถือของกุญแจที่ใช้ป้องกัน แล้วมีการสำรองกุญแจไว้อย่างไร ข้อมูลจะถูกย้ายอย่างชัดเจนในหมู่ผู้ให้บริการคลาวด์หรือใช้ร่วมกันระหว่างการจัดเก็บบนคลาวด์และภายในเครื่องได้หรือไม่?

IBM Multi-Cloud Data Encryption จะปกป้องข้อมูลคลาวด์ (และไฮบริด - คลาวด์) และทำเช่นนั้นโดยคำนึงถึงความสะดวกในการถ่ายโอนและความสอดคล้องตามข้อกำหนด เพื่อให้สามารถเข้าถึงคีย์การเข้ารหัสและพร้อมใช้งานได้อย่างน่าเชื่อถือ โดยสามารถรวมกันกับตัวจัดการคีย์ขั้นสูงได้

นอกจากนี้ IBM Security Key Lifecycle Manager สามารถช่วยลูกค้าที่ต้องการการปกป้องข้อมูลที่เข้มงวดยิ่งขึ้นโดยใช้อุปกรณ์จัดเก็บข้อมูลที่เข้ารหัสด้วยฮาร์ดแวร์เพื่อลดความซับซ้อนของการจัดการคีย์เข้ารหัสโดยไม่ต้องกลัวการเปิดเผยข้อมูลในสภาพแวดล้อมคลาวด์เสมือน

การจัดการคีย์คือหัวใจสำคัญของสภาพแวดล้อมการเข้ารหัสที่ปลอดภัย



5.1 บทสรุป

เพื่อให้แน่ใจว่าข้อมูลได้รับการปกป้องในสภาพแวดล้อมเสมือนและระบบคลาวด์ องค์กรจำเป็นต้องเข้าใจว่าข้อมูลใดที่จะเข้าสู่สภาพแวดล้อมเหล่านี้, วิธีการเข้าถึงข้อมูลที่สามารถตรวจสอบได้, ช่องโหว่ประเภทใดที่มีอยู่ และวิธีการที่แสดงให้เห็นถึงการปฏิบัติตาม การปกป้องควรสร้างไว้ในสภาพแวดล้อมคลาวด์ตั้งแต่เริ่มต้น โดยมีเป้าหมายระยะที่หนึ่งในการช่วยให้องค์กรต่างๆ แสดงให้เห็นถึงการปฏิบัติตาม

เมื่อเลือกโซลูชันความปลอดภัยและการป้องกันข้อมูล ให้เลือกโซลูชันที่ปรับขนาดได้และขยายได้ในโครงสร้างพื้นฐานด้านไอที - ปกป้องสภาพแวดล้อมทางกายภาพเสมือนและคลาวด์จากการโจมตีจากภายนอกที่เป็นอันตราย, การทุจริตหลอกลวง, การเข้าถึงโดยไม่ได้รับอนุญาต โซลูชันเหล่านี้จะต้องทำงานในสภาพแวดล้อมแบบคลาวด์โดยไม่มีการตั้งค่าพิเศษ, การกำหนดค่าหรือค่าใช้จ่ายเพิ่มเติมใดๆ วิธีการดังกล่าวจะให้แพลตฟอร์มที่มีประสิทธิภาพสำหรับความปลอดภัยของข้อมูลและการส่งมอบความเป็นส่วนตัว, ช่วยจัดการต้นทุนโดยการลดการใช้ทรัพยากรรักษาความปลอดภัยของข้อมูลและให้ความคล่องตัวและความยืดหยุ่นที่มากขึ้นด้วยการบริการตนเองเพื่อความปลอดภัยและความเป็นส่วนตัว

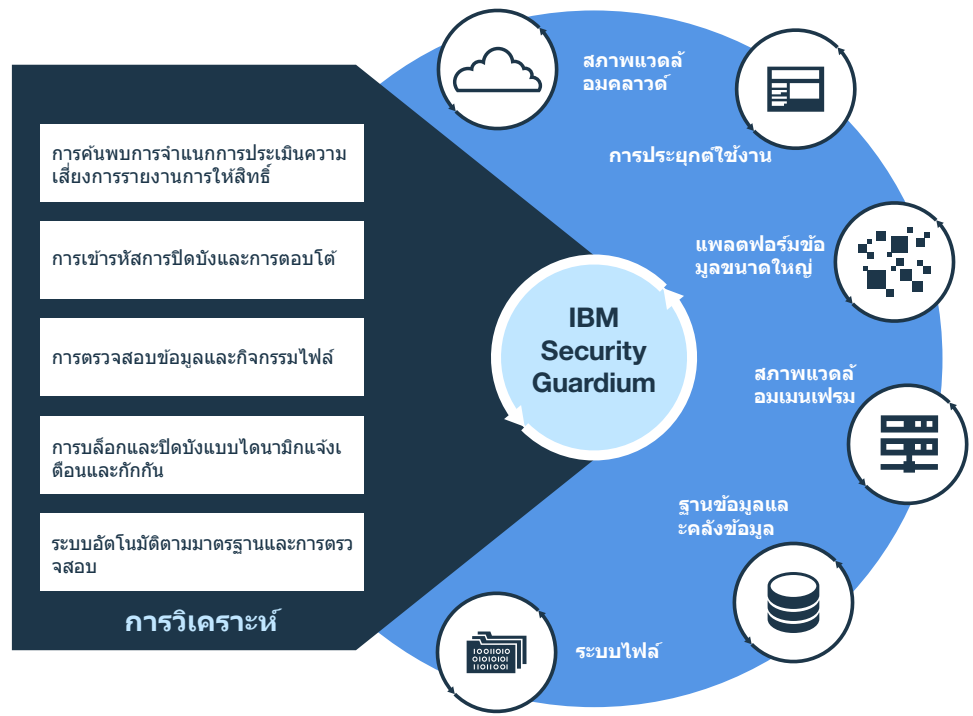
Guardium สามารถช่วยสนับสนุนกลยุทธ์คลาวด์ของคุณด้วย:

- การตรวจสอบการทำงานของข้อมูลและไฟล์, การประเมินความเสี่ยง, การตอบโต้ข้อมูลและการเข้ารหัสข้อมูล, การบล็อกแบบไดนามิก, การกักกันและการแจ้งเตือน
- การค้นพบอัตโนมัติและการจำแนกข้อมูลที่สำคัญในระบบคลาวด์
- การปิดบังข้อมูลแบบคงที่และแบบไดนามิกเพื่อให้แน่ใจว่าแบบจำลองสิทธิ์การเข้าถึงให้น้อยที่สุดสำหรับทรัพยากรคลาวด์
- สร้างรายงานการตรวจสอบและการปฏิบัติตามกฎล่วงหน้าซึ่งปรับแต่งสำหรับกฎระเบียบที่แตกต่างกันเพื่อแสดงให้เห็นถึงการปฏิบัติตามกฎระเบียบและทำให้เวิร์กโฟลว์ของการปฏิบัติตามกฎระเบียบโดยอัตโนมัติในสถานที่และสภาพแวดล้อมคลาวด์

5.2 บทสรุป

ซอฟต์แวร์ Guardium เป็นโซลูชันที่ครอบคลุมสำหรับโครงสร้างพื้นฐานทางกายภาพเสมือนจริงและระบบคลาวด์ผ่านการควบคุมความปลอดภัยอัตโนมัติแบบรวมศูนย์ในสภาพแวดล้อมที่ต่างกัน Guardium ช่วยเพิ่มความคล่องตัวในการปฏิบัติตามกฎระเบียบและลดความเสี่ยงและนำเสนอภาพพร้อมติดตั้งสำหรับการปรับใช้ IaaS บนแพลตฟอร์มคลาวด์ที่สำคัญเช่น IBM SoftLayer®, Microsoft Azure และ Amazon Web Services และทำงานบนสภาพแวดล้อม Microsoft ® Windows, UNIX และ Linux ™

สถาปัตยกรรม Guardium ที่ยืดหยุ่นช่วยให้สามารถใช้งานได้ในรุ่นที่แตกต่างกันหลายรุ่น คุณสามารถเลือกสถาปัตยกรรมระบบที่เหมาะกับองค์กรของคุณ: ส่วนประกอบ Guardium ทั้งหมดสามารถนำไปใช้ในระบบคลาวด์หรือคุณสามารถเลือกที่จะเก็บส่วนประกอบบางอย่างเช่น central manager, on-premises



ภาพที 3: Guardium ให้การปกป้องข้อมูลแบบครบวงจรในทุกสภาพแวดล้อมและแพลตฟอร์มเทคโนโลยี

5.3 บทสรุป

ความยืดหยุ่นนี้จะช่วยให้ลูกค้าปัจจุบันสามารถขยายกลยุทธ์การปกป้องข้อมูลไปยังคลาวด์ได้อย่างง่ายดายโดยไม่ส่งผลต่อการปรับใช้ที่มีอยู่

ตัวรวบรวมการตรวจสอบ input ที่ปรับใช้ในระบบคลาวด์สามารถป้อนข้อมูลไปยังตัวจัดการส่วนกลางได้อย่างง่ายดาย ทำให้มั่นใจว่าจะมีมุมมองแบบรวมที่รวมของภัยคุกคามการป้องกันข้อมูลของคุณไม่ว่าข้อมูลจะอยู่ที่ใดก็ตาม

การควบคุมความปลอดภัยที่จะกันไม่ให้อาชญากรไซเบอร์เข้าถึงที่เก็บข้อมูล - หรือตรวจจับการบุกรุกที่ประสบความสำเร็จอย่างรวดเร็ว - เป็นเครื่องมือที่มีความสำคัญ แต่ในยุคของข้อมูลแบบพกพา การเปลี่ยนภาระงานและการจำลองเสมือนจริง ทำให้การรักษาความปลอดภัยของข้อมูลด้วยการเข้ารหัสนั้นมีความสำคัญ

โซลูชันความปลอดภัยของข้อมูลของ IBM ช่วยปกป้องข้อมูลที่มีความละเอียดอ่อนเพื่อให้องค์กรสามารถมั่นใจได้ว่าข้อมูลของพวกเขาได้รับการปกป้องในสภาพแวดล้อมเสมือนจริงและระบบคลาวด์ที่ซับซ้อน

5.4 แหล่งข้อมูลเพิ่มเติม

เกี่ยวกับ IBM การรักษาความปลอดภัย โซลูชัน
โซลูชัน Security ของ IBM ถือเป็นชุดผลิตภัณฑ์และบริการด้านความปลอดภัยระดับองค์กรระดับสูงที่ทำงานได้แบบบูรณาการและมีคุณภาพในระดับสูงสุด เป็นกลุ่มผลิตภัณฑ์ที่สนับสนุนโดยฝ่ายวิจัยและพัฒนา IBM® X-Force® ที่มีชื่อเสียงระดับโลกให้ข้อมูลการรักษาความปลอดภัย เพื่อช่วยองค์กรแบบองค์รวมในการปกป้องบุคลากร โครงสร้างพื้นฐานข้อมูลและการใช้งาน นำเสนอโซลูชันเพื่อการระบุตัวตนและการเข้าถึงการจัดการ ความปลอดภัยของฐานข้อมูล การพัฒนาแอปพลิเคชัน การจัดการความเสี่ยง การจัดการปลายทาง การรักษาความปลอดภัยเครือข่ายและอื่น ๆ

โซลูชันเหล่านี้จะช่วยองค์กรในการจัดการความเสี่ยงและการดำเนินการรักษาความปลอดภัยแบบบูรณาการสำหรับโทรศัพท์มือถือ คลาวด์ โซเชียลมีเดียและสถาปัตยกรรมทางธุรกิจอื่นๆ ได้อย่างมีประสิทธิภาพ IBM ถือเป็นผู้วิจัยและพัฒนาด้านระบบความปลอดภัยที่ครอบคลุมที่สุดรายหนึ่งของโลก โดยมีการติดตามกรณีด้านความปลอดภัยถึง 15,000 รายการในแต่ละวันครอบคลุมกว่า 130 ประเทศ และมีสิทธิบัตรระบบความปลอดภัยกว่า 3,000 รายการ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความปลอดภัยของข้อมูล, การปฏิบัติตามและคลาวด์ โปรดไปที่ **ibm.com**/guardium.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589, U.S.A.

ผลิตในสหรัฐอเมริกา
พฤษภาคม 2017

1. Thomas J. Bittman, “Internal Private Cloud Is Not for Most Mainstream Enterprises,” *Gartner,* 22 พฤษภาคม 2015

2. Noel Yuhanna, “Enterprise Data Virtualization, Q1 2015,” *The Forrester Wave,* 11 มีนาคม 2015

กรุณานำไปรีไซเคิล

WGM12362-THTH-00