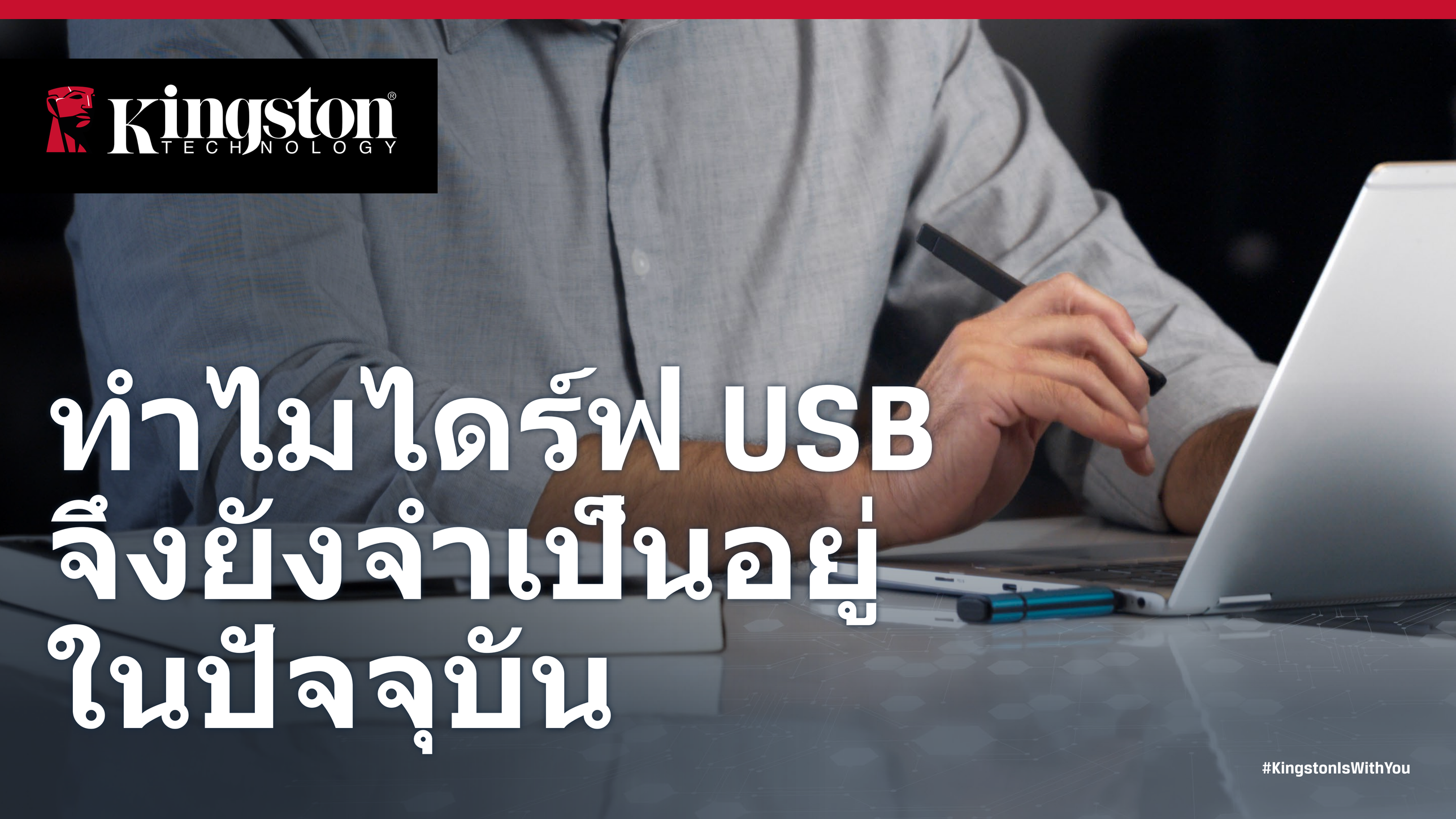


ทำไมไดร์ฟ USB จึงยังจำเป็นอยู่ในปัจจุบัน

#KingstonIsWithYou

ทำไมไดร์ฟ USB จึงยังจำเป็นอยู่ในปัจจุบัน

เกรินนำและเนื้อหา

ในโลกดิจิตอลยุคปัจจุบันซึ่ง 60% ของข้อมูลระดับองค์กรถูกจัดเก็บผ่านคลาวด์[1] การพูดคุยเกี่ยวกับความเชื่อมโยงกับแนวทางสำหรับเทคโนโลยีการจัดเก็บข้อมูลที่มีอายุเกือบจะสามสิบปีแล้วจึงอาจฟังดูไม่สมเหตุสมผลเท่าไรนัก อย่างไรก็ตาม นับตั้งแต่มีการเปิดตัว ระบบจัดเก็บข้อมูลนี้ถือเป็นเครื่องมือหลักที่มีการเติบโตและจะยังคงเป็นเช่นนั้นไปเรื่อย ๆ

ไดร์ฟ USB ไม่ใช่อุปกรณ์มาตรฐานสำหรับการเชื่อมต่อกับไฟล์ข้อมูล ไดร์ฟและแอพพลิเคชันต่าง ๆ อีกต่อไป ผลิตภัณฑ์ในปัจจุบันไม่เพียงแต่มีความเร็วในการถ่ายโอนข้อมูลที่ดีขึ้นอย่างมาก แต่ยังเป็นสื่อบันทึกข้อมูลแบบพกพาที่เชื่อถือได้และปลอดภัยสูงซึ่งเป็นสิ่งจำเป็นสำหรับการใช้งานในหลาย ๆ กรณี แต่ทำไมไดร์ฟ USB จึงยังมีความจำเป็นในเมื่อระบบจัดเก็บข้อมูลผ่านคลาวด์ก็มีประโยชน์การใช้งานที่ไม่แตกต่างกัน

อีบุ๊คฉบับนี้จะกล่าวถึงบทบาทของแฟลชไดร์ฟ USB ท่ามกลางสถาปัตยกรรมที่มีระบบคลาวด์เป็นหลัก ภายใต้ข้อมูลสนับสนุนมากมายจากผู้เชี่ยวชาญในกลุ่มอุตสาหกรรมชั้นนำ ในวันนี้เราขอนำเสนอแนวทางที่หน่วยงานต่าง ๆ เลือกใช้ไดร์ฟ USB และความสามารถในการทำงานร่วมกับระบบเข้ารหัสเชิงซอฟต์แวร์ ระบบการจัดเก็บข้อมูลอิสระ และระบบรักษาความปลอดภัยของข้อมูลปลายทาง

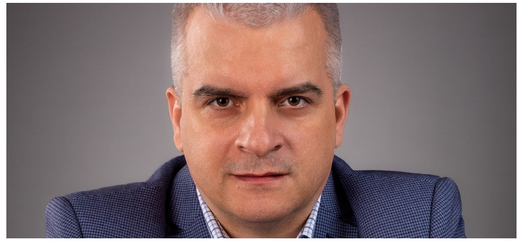
ทำไมไดร์ฟ USB จึงยังจำเป็นอยู่ในปัจจุบัน

ผู้สนับสนุน

อีบุ๊คฉบับนีจัดทำโดยผู้เชียวชาญสามท่านในสาขา IT และเทคโนโลยีเกิดใหม่

Rafael Bloom

Rafael เป็นผู้เชียวชาญในกลุ่มผลิตภัณฑ์ด้านเทคโนโลยี การสือสารข้อมูลด้านการตลาดและการพัฒนาธุรกิจ คำแนะนำของเขามุ่งเน้นไปทีความท้าทายใหม่ ๆ ด้านองค์กร ผลิตภัณฑ์และการสือสารของการเปลียนแปลงทางเทคโนโลยีและระเบียบข้อบังคับ การทำงานทีมีความหลากหลายเป็นอย่างยิงทำให้ต้องเรียนรู้ทักษะในหลาย ๆ ด้านเกียวกับการกำกับดูแลข้อมูลและการควบคุมมาตรฐานด้านการออกแบบ ความเป็นส่วนตัวของข้อมูลและเทคโนโลยีเกิดใหม่ เช่น AdTech, Mobile & 5G, AI และระบบการเรียนรู้ของเครืองจักร



Tomasz Surdyk

ประสบการณ์กว่า 24 ปีด้านการรักษาความปลอดภัยของระบบ IT ให้แก่ภาครัฐทำให้ Tomasz ถือเป็นบุคคลสำคัญด้านการรักษาความปลอดภัยของระบบสารสนเทศ ข้อมูลส่วนบุคคลและระบบคอมพิวเตอร์ ในอดีตเขามีโอกาสตรวจสอบงานระบบ ICT และเครือข่ายข้อมูลลับและข้อมูลส่วนบุคคลในภาครัฐรวมถึงเป็นผู้ทีมีเอกสิทธิด้านความปลอดภัยในองค์กรระดับ NATO และ EU ตลอดเวลาหลายปีเขาเปิดบริษัทซึงเชียวชาญในการให้บริการด้านระบบรักษาความปลอดภัยสำหรับข้อมูลทางธุรกิจและข้อมูลส่วนบุคคลต่าง ๆ

David Clarke

David ได้รับการยอมรับในฐานะอินฟลูเอนเซอร์ 10 อันดับแรกโดย Thompson Reuter's ในกลุ่ม "Top 30 most influential thought-leaders and thinkers on social media, in risk management, compliance and reg-tech in the UK" และติด 50 อันดับแรกของ Global Experts by Kingston Technology ในอดีต David เคยดำรงตำแหน่งบริหารด้านงานรักษาความปลอดภัยมากมาย เช่น Global Head of Security Service Delivery และ Head of Security Infrastructure สำหรับบริษัทในกลุ่ม Global FTSE 100

การถือกำเนิดของแฟลชไดร์ฟ USB

เมื่อตอนที Universal Serial Bus (USB) ถือกำเนิดขึนในตลาดเมื่อกว่ายีสิบปีทีผ่านมา ความสามารถในการรองรับการทำงานทีหลากหลายถือเป็นเทคโนโลยีคอมพิวเตอร์ทีเป็นจุดเปลียนสำคัญ ความสามารถในการทำงานกับอุปกรณ์ต่าง ๆ หลากหลายชนิดเพือการสืบค้นข้อมูลส่งผลให้ USB มีการพัฒนาอย่างต่อเนืองทังความเร็วในการถ่ายโอนข้อมูลอย่างพอร์ต USB 3.0 หรือความจุทีเพิมมากขึนเมือมีการเปิดตัวแฟลชไดร์ฟ USB ในปี 2000

นับตังแต่นันมา เทคโนโลยีได้พัฒนามาไกลในแง่ของการจัดเก็บข้อมูลแบบพกพาและความต้องการด้านความปลอดภัย เป้าหมายสำคัญในปัจจุบันคือการพัฒนาไดร์ฟ USB สำหรับการใช้งานเฉพาะด้าน ในมุมมองขององค์กรขนาดใหญ่ การทำงานแบบทางไกลและแบบผสมผสานทีเพิมขึน การใช้งานคลาวด์ รวมถึงข้อกังวลด้านความปลอดภัยทางไซเบอร์ ล้วนส่งผลให้ทุกฝ่ายคาดหวังผลิตภัณฑ์ทีมีประสิทธิภาพยิงกว่าเดิม นอกจากนี ระเบียบข้อบังคับต่าง ๆ ยังกำหนดให้ข้อมูลจะต้องมีการจัดเก็บไว้ตามมาตรฐานทีกำหนด ปัจจัยกดดันเหล่านีมีความซับซ้อนมากยิงขึนจากระบบการทำงานแบบกระจายตัวทีมีรายละเอียดให้ต้องพิจารณามากมาย ไม่ว่าจะเป็น “ระบบติดตังในพืนที” หรือผ่านคลาวด์

นอกจากนียังมีปัญหาของปริมาณข้อมูลทังแบบทีเป็นระบบและไม่เป็นระบบทีเพิมมากขึน ทังข้อมูลเอกสาร อีเมล ภาพถ่าย วิดีโอและเมต้าดาต้าทีทำให้ความต้องการในการจัดเก็บข้อมูลขององค์กรขนาดใหญ่ยิงมีความซับซ้อนยิงขึน

แต่หากระบบจัดเก็บข้อมูลคลาวด์สามารถจัดการกับปัญหาเหล่านีได้ แล้วไดร์ฟ USB จะยังมีความจำเป็นสำหรับการดำเนินธุรกิจในปัจจุบันอยู่อีกหรือไม่

> **หลาย ๆ คนมองว่าไดร์ฟ USB เป็นอุปกรณ์รุ่นเก่าทีล้าสมัย เนืองจากแต่เดิมนันใช้เป็นอุปกรณ์จัดเก็บข้อมูลแบบใช้แล้วทิงทีมีประสิทธิภาพและความปลอดภัยต่ำ**
> - Rafael Bloom

สือบันทึกข้อมูลแบบพกพาทีสามารถตอบสนองความต้องการทีเพิมมากขึนอย่างต่อเนือง

แม้ว่ารูปแบบการใช้งานไดร์ฟ USB แบบเดิม ๆ ซึงเป็นการจัดเก็บข้อมูลแบบพกพานันเป็นทีนิยมน้อยลงเรือย ๆ แต่การใช้งานไดร์ฟ USB ประสิทธิภาพสูงก็เริมกลายเป็นทีต้องการสำหรับกลุ่มผู้ใช้ทีต้องการอุปกรณ์สำรองข้อมูลส่วนตัวทีมีความปลอดภัย และมีฟังก์ชันป้องและรักษาความปลอดภัยของข้อมูลเสริม นีเป็นปัจจัยทีสำคัญอย่างยิงสำหรับข้อมูลทีอ่อนไหวและมีการกำกับดูแลอย่างเข้มงวด เช่น ระเบียนข้อมูลฝ่ายบุคคล ข้อมูลด้านการเงิน ประวัติการแพทย์ ข้อมูลทรัพย์สินทางปัญญา (IP) และข้อมูลระบุตัวบุคคล (PII) ทังหมด นอกจากนี อุปกรณ์ดังกล่าวทีผลิตขึนใหม่ยังรองรับการถ่ายโอน จัดเก็บและสำรองข้อมูลทีรวดเร็ว และมีระบบรักษาความปลอดภัยทีสามารถใช้งานสำหรับ:

- ข้อมูลภายใต้ระเบียบข้อบังคับทีจะต้องนำส่งด้วยตัวเอง
- เอกสารทางกฎหมายหรือด้านการเงินทีจะต้องนำส่งหรือจัดพิมพ์ในหรือนอกพืนที
- สภาพแวดลอมทีเป็นอันตรายและสุ่มเสียงต่อแรนซัมแวร์
- การถ่ายโอนข้อมูลไปยังระบบการพิมพ์ทีห้ามไม่ให้มีการเชือมต่อกับระบบเครือข่าย

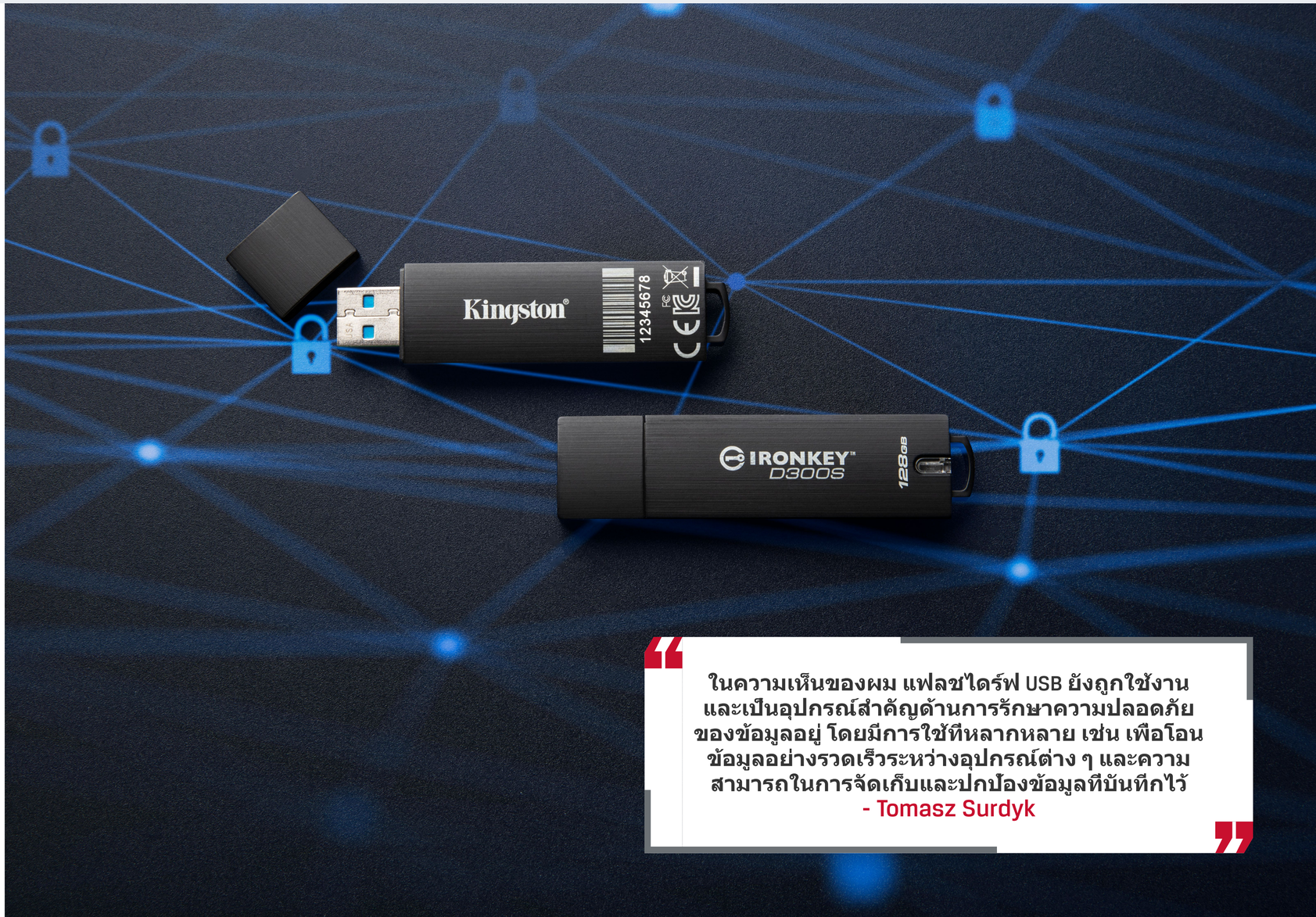
Kingston Technology ในฐานะผู้ผลิตไดร์ฟ USB เข้ารหัสชันนำ ไม่เคยหยุดทีจะพัฒนาผลิตภัณฑ์ตามความต้องการใหม่ ๆ ทีเกิดขึน จึงมีการเปิดตัวผลิตภัณฑ์ใหม่ ๆ อยู่เสมอ เช่น Kingston IronKey™ S1000 นีคือไดร์ฟ USB เข้ารหัสทีดีทีสุดทีผ่านมาตรฐานทีเข้มงวดทีสุด และสามารถปกป้องข้อมูลลับได้โดยใช้การเข้ารหัส XTS-AES 256 บิต พร้อมทังชิปเข้ารหัสทีทนต่อการทุบทำลายได้สูง นอกจากนียังรับรองมาตรฐาน FIPS 140-2 Level 3 ซึงหมายความว่าอุปกรณ์ผ่านการรับรองอย่างเป็นทางการโดยรัฐบาลสหรัฐฯ ว่ามีระบบการเข้ารหัสเชิงฮาร์ดแวร์ทีมีประสิทธิภาพ จึงเหมาะอย่างยิงสำหรับหน่วยงานทีต้องการความมันใจในการปกป้องข้อมูลเป็นพิเศษ

ไดร์ฟ USB เข้ารหัสเชิงฮาร์ดแวร์มีระบบจัดการอุปกรณ์ทีปลอดภัยจากส่วนกลางไม่ว่าข้อมูลจะใช้ผ่านคลาวด์หรือเรียกค้นจากในพืนทีก็ตาม ระบบจัดเก็บข้อมูลแบบเข้ารหัสทีผ่านมาตรฐานทีกำหนดและใช้งานง่ายโดยไม่ต้องติดตังซอฟต์แวร์ใด ๆ ทำให้ฝาย IT มีเวลาในการจัดการงานด้านอืน ๆ มากขึน นอกจากนีอุปกรณ์ยังพร้อมใช้งานอย่างเต็มประสิทธิภาพได้ในทันที

สือบันทึกข้อมูลแบบพกพาทีสามารถตอบสนองความต้องการทีเพิมมากขึนอย่างต่อเนือง

การสำรองและจัดเก็บข้อมูลแยกเป็นอีกตัวอย่างของการใช้งานไดร์ฟ USB เพือปกป้องข้อมูลดิจิตอลในระยะยาวโดยเป็นอิสระจากส่วนบริการคลาวด์จากภายนอก จริงอยู่ว่าการถ่ายโอนข้อมูลเป็นจำนวนมากดำเนินการผ่านระบบคลาวด์ได้ง่าย แต่ข้อมูล IP ทีเป็นกรรมสิทธิ์ก็อาจมีความสำคัญมากถึงขนาดทีจำเป็นต้องมีการจัดเก็บไว้ในไดร์ฟ USB เข้ารหัสทีปลอดภัยสูงเพือไม่ให้ข้อมูลหลุดเข้าไปในโลกอินเทอร์เน็ตและปลอดภัยอยู่ตลอดเวลา

นอกจากนียังมีกรณีอืน ๆ ทีหน่วยงานต่าง ๆ ต้องการให้ตนเองสามารถกำกับดูแลข้อมูลในทางตรรกะและในทางกายภาพได้อย่างเต็มทีซึงสามารถทำได้อย่างสะดวกเมือใช้ไดร์ฟแบบเข้ารหัส ยังมีกรณีการใช้งานอืน ๆ อีกมากมายทีการจัดเก็บข้อมูลผ่าน HDD/SSD อาจไม่สามารถใช้วิธีการเข้ารหัสได้ การใช้ไดร์ฟ USB เข้ารหัสแบบต่อพ่วงสามารถแก้ไขปัญหาเหล่านียกตัวอย่างได้จาก Kingston IronKey D300S แฟลชไดร์ฟ USB รุ่นนีรองรับการเข้ารหัส XTS 256 บิตขันสูง (AES) เชิงฮาร์ดแวร์ซึงเป็นการเข้ารหัสในระดับบล็อคข้อมูล 128 บิต สำหรับการเข้ารหัสข้อมูลทีปลอดภัยยิงไปกว่านี AES จะเลือกใช้โหมดเข้ารหัสบล็อคข้อมูล XTS ทีสามารถให้การปกป้องข้อมูลได้ดียิงกว่าโหมดก่อนหน้า



> ในความเห็นของผม แฟลชไดร์ฟ USB ยังถูกใช้งานและเป็นอุปกรณ์สำคัญด้านการรักษาความปลอดภัยของข้อมูลอยู่ โดยมีการใช้ทีหลากหลาย เช่น เพือโอนข้อมูลอย่างรวดเร็วระหว่างอุปกรณ์ต่าง ๆ และความสามารถในการจัดเก็บและปกป้องข้อมูลทีบันทึกไว้
> - Tomasz Surdyk

การเข้ารหัส: การเข้ารหัสเชิงฮาร์ดแวร์เทียบกับแบบซอฟต์แวร์

เมื่อพิจารณาเกี่ยวกับแนวทางในการเข้ารหัสข้อมูล หลายคนอาจบอกว่าการเข้ารหัสเชิงฮาร์ดแวร์จัดการง่ายกว่าและปลอดภัยกว่าการเข้ารหัสเชิงซอฟต์แวร์ ทั้งนี้เนื่องจากกระบวนการเข้ารหัสจะดำเนินการแยกจากระบบโฮสต์ส่วนอื่น ๆ ทำให้ยากต้องการแทรกแซงหรือเจาะทำลาย การจัดการระดับอุปกรณ์จากส่วนกลางช่วยในการควบคุมไดร์ฟผ่าน LAN อินทราเน็ตและการเชื่อมต่ออินเทอร์เน็ต ซึ่งเหมาะอย่างยิ่งสำหรับ:

- การกำหนดและบังคับใช้นโยบายการใช้งาน USB เข้ารหัสแบบรายบุคคลและ/หรือเป็นกลุ่ม
- การตรวจสอบการใช้งานไฟล์เพื่อติดตามการเคลื่อนย้ายข้อมูลเข้าและออกจากหน่วยงานของคุณ
- การจัดหาทางเลือกในการสำรองข้อมูลทางไกลเพื่อการขนย้ายข้อมูลที่มีความสำคัญอย่างยิ่ง
- การปิดใช้งานอุปกรณ์จากระยะไกลเมื่อ USB สูญหายหรือถูกเจาะระบบ
- การรีเซ็ตรหัสผ่านกรณีลืมรหัส

เมื่ออุปกรณ์ที่ได้รับอนุญาตมีการจัดการอย่างเหมาะสมผ่านกระบวนการนี้ ก็จะช่วยลดความเสี่ยงที่ข้อมูลที่อ่อนไหวจะถูกคัดลอกและแชร์ออกไป นอกจากนี้ ไดร์ฟ USB เข้ารหัสเชิงฮาร์ดแวร์รุ่นใหม่ ๆ ยังมีคุณสมบัติด้านความปลอดภัยอื่น ๆ อีกมากมายเพื่อป้องกันไฟล์และข้อความต่าง ๆ ไม่ให้ถูกสืบค้นหรืออ่านโดยบุคคลที่ไม่ใช่ผู้รับตัวจริง

> **ผมเชื่อว่าการเข้ารหัสเชิงฮาร์ดแวร์มีประสิทธิภาพเหนือกว่าระบบเข้ารหัสเชิงซอฟต์แวร์ ความแตกต่างระหว่างการเข้ารหัสเชิงฮาร์ดแวร์และซอฟต์แวร์มีอย่างชัดเจนโดยเฉพาะในด้านการทนต่อการทุบทำลาย ในกรณีนี้ อุปกรณ์เข้ารหัสเชิงฮาร์ดแวร์จะมีความปลอดภัยมากกว่าจากการทุบทำลาย**
> - Tomasz Surdyk

การเข้ารหัส: การเข้ารหัสเชิงฮาร์ดแวร์เทียบกับแบบซอฟต์แวร์

แม้ว่าธุรกิจหลาย ๆ แห่งจะเลือกใช้ระบบเข้ารหัสเชิงซอฟต์แวร์เนื่องจากปัจจัยด้านต้นทุน แต่การตัดสินใจดังกล่าวอาจไม่รอบคอบเพียงพอ ระบบความปลอดภัยเชิงซอฟต์แวร์ใช้ทรัพยากรในการเข้ารหัสร่วมกับอุปกรณ์โฮสต์รวมกับโปรแกรมอื่น ๆ ดังนั้นจึงมีความปลอดภัยในระดับเดียวกับตัวคอมพิวเตอร์เอง นอกจากนียังต้องมีการอัพเดตซอฟต์แวร์เป็นระยะ ๆ ซึงหากมองข้ามก็จะทำให้เกิดความเสียงมากยิงขึน ไดร์ฟ USB เข้ารหัสเชิงซอฟต์แวร์อาจถูกทุบทำลายด้วยวิธีต่าง ๆ เพือพยายามหาทางเดารหัสผ่าน และไม่มีวิธีการป้องกันระบบเดารหัสผ่านแบบอิงพจนานุกรมผ่านซอฟต์แวร์ ซึงมักถูกใช้เพือเอาชุดตัวอักษรต่าง ๆ ได้นับล้านชุดภายในระยะเวลาสัน ๆ

นอกจากนีระบบเข้ารหัสเชิงซอฟต์แวร์ยังเป็นระบบเข้ารหัสทีสามารถปิดใช้งานได้ พนักงานทีใช้ไดร์ฟเข้ารหัสเชิงซอฟต์แวร์สามารถคัดลอกข้อมูล ฟอร์แมตไดร์ฟ USB และปิดการเข้ารหัสได้หากต้องการ และสามารถคัดลอกไฟล์ข้อมูลเหล่านีเพือนำไดร์ฟไปใช้งานโดยไม่ต้องผ่านขันตอนการตรวจรับรองเมือใช้กับแพลตฟอร์มหรือ OS ตัวอืน

ตามทีได้ชีแจงไปก่อนหน้านี ระบบเข้ารหัสเชิงฮาร์ดแวร์เป็น "การเข้ารหัส" ทางกายภาพ ซึงการจัดเก็บข้อมูลทีเกิดขึนต่อมาจะเป็นการทำงานทีเป็นอิสระแยกจากระบบโฮสต์ ซึงถือเป็นการป้องกันอีกระดับหากมีการพยายามเจาะระบบเกิดขึน

นีเป็นประเด็นทีไม่ควรมองข้าม โดยเฉพาะในกลุ่มอุตสาหกรรมด้านการเงิน การแพทย์และกิจการภาครัฐ ทังนีเนืองจากระเบียบข้อบังคับต่าง ๆ เช่น Health Insurance Portability and Accountability Act (HIPAA) และ Payment Card Industry Data Security Standard (PCI DSS) มักมีเงือนไขทีเข้มงวดในการเข้ารหัสข้อมูลทีอ่อนไหว

การปฏิบัติตามข้อบังคับเหล่านีโดยการใช้อุปกรณ์เข้ารหัสเชิงฮาร์ดแวร์ทีเชือถือได้จะช่วยให้หน่วยงานต่าง ๆ สามารถหลีกเลียงค่าปรับเป็นจำนวนมาก และการถูกดำเนินคดีหรือความเสียหายต่อชือเสียงทีอาจเกิดขึน แม้ว่าไดร์ฟเข้ารหัสเชิงฮาร์ดแวร์จะมีราคาสูงกว่าไดร์ฟ USB ทัวไป แต่ค่าใช้จ่ายของทีปรึกษาทางกฎหมายเพียงไม่กีชัวโมงเมือเกิดการละเมิดข้อมูลอาจมากกว่าราคาไดร์ฟนับร้อยตัว

ความจำเป็นที่เพิ่มขึ้นในการปกป้องข้อมูลที่อ่อนไหว

> **เข้ารหัสข้อมูลทั้งหมดโดยเร็วที่สุด สำรองข้อมูลโดยใช้หลัก 321 (USB อาจเป็นตัวเลือกที่สามารถเลือกใช้งานได้ทันที) และเลือกใช้แนวทางการแบ่งส่วนข้อมูลย่อยที่รวดเร็วและฉับไว - David Clarke**

เมื่อพูดถึงการปกป้องข้อมูลที่อ่อนไหวจากการสูญหายหรือถูกขโมย หน่วยงานทุกแห่งมีหน้าที่ในการกำกับดูแลให้อุปกรณ์ของตนมีระบบรักษาความปลอดภัยที่เพียงพอ สิ่งที่สำคัญไม่แพ้กันคือการเข้าใจว่าแม้ว่าจะมีภัยคุกคามทางไซเบอร์เกิดขึ้นมากมาย และระดับการเติบโตของข้อมูลดิจิตอลและทักษะด้านการจัดการข้อมูลปลายทางของตัวผู้ใช้เองยังคงเป็นปัจจัยเสี่ยงที่สำคัญที่จะมองข้ามไม่ได้ ภัยคุกคามจากภายในซึ่งประกอบด้วย การไม่สามารถควบคุมข้อมูล อุปกรณ์จัดเก็บข้อมูล USB สูญหาย การถ่ายโอนข้อมูลไปนอกพื้นที่ปลอดภัย การใช้ไดร์ฟ USB ที่ไม่เข้ารหัส และการเปิดเผยรหัสผ่าน ล้วนแล้วแต่เป็นผลมาจากการขาดความระมัดระวังของผู้ใช้ปลายทาง ทั้งหมดนี้เป็นสิ่งที่หลีกเลี่ยงได้หากมีการฝึกอบรม การให้ความรู้ที่เพียงพอและการจัดหาไดร์ฟ USB ที่เหมาะสม

> **หน่วยงานต่าง ๆ ควรมีแผนผังข้อมูลที่ชัดเจนเป็นของตนเอง และการกำหนดระดับความสำคัญและ/หรือความเปราะบางของชุดข้อมูลต่าง ๆ ทั้งหมด พร้อมทั้งแผนในการจัดการกับข้อมูลที่สำคัญก่อน เช่น การตัดการเชื่อมต่อทางกายภาพที่จะเข้าถึงข้อมูลหรือการปิดกั้นแหล่งข้อมูล การที่ผู้ใช้สามารถแยกส่วนระบบที่ถูกเจาะได้อย่างรวดเร็วเป็นสิ่งสำคัญ และการมีแผนงานที่ชัดเจนที่คุณปรับใช้อย่างเคร่งครัดก็เป็นสิ่งที่จะขาดไปไม่ได้ - Rafael Bloom**

การวางแผนล่วงหน้าและโครงสร้างการสื่อสารที่ทั่วถึงเป็นอีกสิ่งสำคัญในการจัดการกับภัยคุกคามที่อาจเกิดขึ้น ภัยคุกคามทางไซเบอร์ในปัจจุบันเลือกที่จะเจาะผ่านจุดเปราะบางของหน่วยงานเป้าหมาย

เวลาที่ดีที่สุดในการจัดทำแผนงานสำหรับ USB แบบเข้ารหัสคือก่อนถึงเวลาที่จำเป็นต้องใช้จริง ๆ โดยการเลือกใช้แฟลชไดร์ฟ USB แบบเข้ารหัสและนโยบายที่เกี่ยวข้องไว้ในแผนงานด้านความปลอดภัยโดยรวมสำหรับหน่วยงานของคุณ การไม่เตรียมแผนงานไว้ล่วงหน้าสำหรับไดร์ฟ USB เข้ารหัสหรือแนวทางที่เหมาะสมจะทำให้คุณไม่มีจุดตั้งต้นใด ๆ และหน่วยงานของคุณจะมีจุดเปราะบางในทุก ๆ ด้าน ทั้งการปฏิบัติตามระเบียบข้อบังคับ เช่น General Data Protection Regulation (GDPR) ซึ่ง บทความที่ 32 ระบุไว้อย่างชัดเจนว่าจะต้องมีการเข้ารหัสข้อมูลที่มีความอ่อนไหว

> **ผู้ใช้มีการประมวลผลข้อมูลที่อ่อนไหว หากข้อมูลดังกล่าวสูญหายก็จะเกิดความผิดและส่งผลกระทบต่อภาพลักษณ์และความปลอดภัยของบริษัทด้วย เพื่อปกป้องข้อมูลที่อ่อนไหว จึงต้องมีการใช้ผลิตภัณฑ์ด้านความปลอดภัยต่าง ๆ รวมไปถึงการเข้ารหัสข้อมูล - Tomasz Surdyk**

การปกป้องข้อมูลด้านการเงินที่อ่อนไหว

นอกเหนือจากประเด็นด้านการรักษาความปลอดภัย ยังมีเรื่องของมาตรฐานการกำกับดูแลเพื่อให้การจัดเก็บและสำรองข้อมูลเป็นไปตามข้อกำหนด แนวทางบางส่วนเหล่านี้ เช่น การจัดการและกำหนดกรอบเวลาในการเก็บรักษาข้อมูล ถือเป็นแนวปฏิบัติทั่ว ๆ ไป ในขณะที่ยังอาจมีเงื่อนไขอื่น ๆ ที่เกี่ยวข้องด้วย เช่น การโอนย้ายข้อมูลองค์กรไปยังระบบคลาวด์ ซึ่งจะมีการจัดการที่แตกต่างกันโดยสิ้นเชิง

ในบางภาคส่วน เช่น อุตสาหกรรมการเงิน อาจมีระเบียบข้อบังคับที่กำหนดไว้ด้านการจัดการข้อมูลอย่างเหมาะสม ธนาคารต่าง ๆ มักจ้างผู้ให้บริการจากภายนอกเพื่อจัดเก็บและสำรองข้อมูล หรืออาจเลือกที่จะลงทุนในโครงสร้างพื้นฐานข้อมูลด้วยตัวเอง

สถาบันการเงินต่าง ๆ มีหน้าที่ปฏิบัติตามข้อกำหนดและมาตรฐานด้านการรักษาความปลอดภัยที่เข้มงวดขึ้นเรื่อง ๆ เช่น Sarbanes-Oxley Act (SOX) และ General Data Protection Regulation (GDPR) อย่างไรก็ตาม จากจำนวนแรงงานทางไกลและแรงงานรับจ้างทางไกลที่เพิ่มขึ้นเรื่อย ๆ ความเสี่ยงจากข้อมูลที่รั่วไหลและการไม่ปฏิบัติตามกฎหมายหรือมาตรฐานที่กำหนดก็เพิ่มขึ้นตามไปด้วย

สิ่งที่เกิดขึ้นคือความพยายามในการควบคุมมาตรฐานอาจไม่เป็นไปตามคาด หากพนักงานทางไกลเหล่านี้ละเลยที่จะปกป้องอัตลักษณ์ของตนเองในโลกดิจิตอล รวมทั้งพื้นที่ทำงานแบบเคลื่อนที่ ระเบียนข้อมูลของลูกค้าและข้อมูลทางการเงินที่ตนเองดูแล ด้วยเหตุนี้หน่วยงานต่าง ๆ จึงเริ่มหันมาพิจารณาผลิตภัณฑ์ที่มีระบบรักษาความปลอดภัยแบบพกพากันมากขึ้นอย่าง ไดร์ฟ USB เข้ารหัส Kingston IronKey เพื่อปกป้องตัวตนในโลกดิจิตอลและแอพพลิเคชันต่าง ๆ ไม่ว่าพนักงานจะปฏิบัติงานอยู่ที่ใดก็ตาม

> **“หากพิจารณาเทรนด์ในภาพรวมที่มีการปรับเข้าหาระบบ IT แบบกระจายศูนย์มากขึ้น และความสามารถในการปรับขนาดได้เต็มที่ของโครงสร้างพื้นฐานระบบคลาวด์ จึงไม่ยากที่จะเข้าใจได้ว่าทำไมอุตสาหกรรมส่วนใหญ่ และ SME อีกเป็นจำนวนมากจึงไม่ได้ให้ความสำคัญกับห้องเซิร์ฟเวอร์แบบเดิม ๆ ที่ต้องดูแลและควบคุมอุณหภูมิอย่างยุ่งยากอีกต่อไป”**
> **- Rafael Bloom**

การดูแลความปลอดภัยในการสืบค้นข้อมูลด้านสุขภาพของผู้ป่วย

อุตสาหกรรมการแพทย์และสุขภาพเป็นอีกกลุ่มการใช้งานที่ให้ความสำคัญอย่างยิ่งกับความปลอดภัยของข้อมูล ข้อมูลของผู้ป่วยมีความเสี่ยงต่อการถูกขโมยอย่างยิ่ง โดยมีการเจาะเข้าถึงข้อมูลผู้ป่วยถึง 45.67 ล้านรายในปี 2021 ซึ่งถือเป็นจำนวนที่มากที่สุดต่อปีนับตั้งแต่ปี 2015[2] เมื่อพูดถึงการจัดเก็บและสำรองข้อมูล ข้อมูลของผู้ป่วยถือเป็นข้อมูลด้านการแพทย์ที่สำคัญและมีความครอบคลุมเพื่อให้ผู้ให้บริการทางการแพทย์สามารถดูแลผู้ป่วยของตนเองได้อย่างปลอดภัย

ข้อมูลเหล่านี้อาจได้แก่ระเบียนข้อมูลอิเล็กทรอนิกส์ด้านสุขภาพ (EHR) ของผู้ป่วยที่มีประวัติด้านสุขภาพต่าง ๆ ผลการทดสอบ ภาพถ่ายและผลการตรวจเอกซเรย์ ไปจนถึงแฟ้มข้อมูลด้านธุรการ เช่น บัญชีเงินเดือน ประกันภัยของผู้ป่วยและบัญชีเจ้าหนี้ จำนวนแรงงานแบบทำงานไม่ประจำที่ที่เพิ่มขึ้นและตลาดของกลุ่มดูแลสุขภาพทั่วโลกที่มีการขยายตัวทำให้เกิดการเปลี่ยนแปลงและการปรับตัวครั้งสำคัญ จึงไม่น่าแปลกใจที่ผู้ให้บริการด้านการแพทย์ให้ความสำคัญอย่างยิ่งกับการรักษาความปลอดภัยของข้อมูล

> **“แรนซัมแวร์ถือเป็นปัญหาสำคัญของกลุ่มอุตสาหกรรมที่กำลังเติบโต และทุก ๆ หน่วยงานที่ดูแลข้อมูลที่อ่อนไหวล้วนต้องพิจารณาว่าจะจัดการปัญหานี้ได้อย่างไรภายใต้แรงกดดันที่สูงอย่างยิ่ง - Rafael Bloom”**

นอกจากนี้การละเลยที่จะคาดการณ์ปัจจัยเสี่ยงและปฏิบัติตามข้อกำหนดที่เข้มงวด เช่น Health Insurance Portability and Accountability Act (HIPAA) หรือ Health Information Technology for Economic and Clinical Health Act (HITECH) ก็อาจทำให้เกิดการเจาะข้อมูลด้านสุขภาพที่ทำให้เกิดความเสียหายเป็นมูลค่าสูง และกระทบต่อความเชื่อมั่นของผู้ป่วย พันธมิตรหรือหน่วยงานกำกับดูแล

ผลิตภัณฑ์อย่างไดร์ฟ USB เข้ารหัส Kingston IronKey ช่วยให้หน่วยงานทางการแพทย์และด้านสุขภาพสามารถกำหนดนโยบายในการกำหนดรหัสผ่าน การใช้งานแอพพลิเคชัน การกู้ข้อมูลและนโยบายอื่น ๆ แบบบูรณาการกับไดร์ฟอื่น ๆ ผ่านคอนโซลจัดการเพียงตัวเดียว แรงงานแบบไม่ประจำที่และบุคลากรด่านหน้าจะสามารถให้การดูแลผู้ป่วยได้มากขึ้นผ่านผลิตภัณฑ์ที่ใช้งานได้ง่ายและลดปัญหาในการติดตั้งไดร์เวอร์หรือซอฟต์แวร์อื่น ๆ โดยยังคงสามารถดูแลความปลอดภัยของข้อมูลที่จัดเก็บไว้ได้เป็นอย่างดี ผู้ใช้และผู้ดูแลระบบสามารถปิดกันข้อมูลได้ง่าย ๆ และรวดเร็วไม่ว่าจะอยู่ที่ใดก็ตาม

ไดร์ฟ USB กับอนาคตของระบบจัดเก็บข้อมูลผ่านคลาวด์

> **ระบบจัดเก็บข้อมูลผ่านคลาวด์คือกระแสในปัจจุบันและสิ่งที่จะคงอยู่ในอนาคต ผมยังเห็นต่างว่าข้อมูลที่มีการป้องกันทางกายภาพ เช่น การใช้ไดร์ฟ USB เข้ารหัสยังเป็นวิธีที่ปลอดภัยที่สุด ผู้ใช้ไม่สามารถเข้าไปดำเนินการใด ๆ ได้ในระบบคลาวด์ แต่เราสามารถควบคุมข้อมูลในไดร์ฟ USB เข้ารหัสได้ซึ่งทำให้เราสามารถกำหนดระดับความปลอดภัยและการจัดเก็บข้อมูลได้ด้วยตัวเอง อีกทั้งยังยังไม่มีคนอื่นที่สามารถเข้าถึงข้อมูลเหล่านี้ได้นอกจากเรา - Tomasz Surdyk**

หลังจากที่เห็นประโยชน์ของไดร์ฟ USB อย่างชัดเจนแล้ว คุณคิดว่าไดร์ฟเหล่านี้จะมีบทบาทอย่างไรต่ออนาคตของระบบคลาวด์

ในช่วงทศวรรษที่ผ่านมา ไดร์ฟ USB เป็นที่แพร่หลายอย่างมากในฐานะเครื่องมือหลักที่ใช้จัดเก็บและถ่ายโอนข้อมูล อย่างไรก็ตาม กระแสการทำงานแบบผสมผสานแบบไม่ประจำที่ทำให้ทีมงานไม่ได้กระจุกตัวอยู่ในที่เดียวกันอีกต่อไป ระบบคลาวด์จึงเป็นทางเลือกที่รวดเร็วและไม่ยุ่งยากเพื่อให้อุปกรณ์ต่าง ๆ สามารถเข้าถึงข้อมูลที่จัดเก็บไว้ แม้ว่าแฟลชไดร์ฟจะเคยเป็นที่นิยมอย่างมากเนื่องจากความสะดวกในการถ่ายโอนไฟล์ แต่ในปัจจุบัน บริการจัดเก็บข้อมูลผ่านคลาวด์กลับให้ความสะดวกในการเคลื่อนย้ายข้อมูลในระดับที่เหนือกว่า

อย่างไรก็ตาม ระบบจัดเก็บข้อมูลผ่านคลาวด์ก็ยังมีข้อจำกัดบางประการ อย่างแรกคือความจำเป็นในการเชื่อมต่อเครือข่ายเพื่อสำรองหรือถ่ายโอนข้อมูล และเป็นอีกหนึ่งปัจจัยที่น่ากังวลด้านการรักษาความปลอดภัย เมื่อใดก็ตามที่หน่วยงานเลือกใช้ระบบคลาวด์ หน่วยงานดังกล่าวจะไม่สามารถควบคุมได้ว่าจะมีการสืบค้นข้อมูลจากที่ใดได้บ้าง ดังนั้นการเชื่อมต่อผ่าน VPN โดยใช้เครือข่าย Wi-Fi ส่วนตัวหรือสาธารณะจึงอาจมีความเสี่ยงจากการถูกแฮ็ค นอกจากนี้ บริการคลาวด์ยังเป็นสิ่งที่ผู้ไม่ประสงค์ดีให้ความสนใจเป็นพิเศษ เนื่องจากมัลแวร์เกือบทั้งหมดในปัจจุบัน (61%) ถูกส่งผ่านแอพพลิเคชันคลาวด์[3]

> **ดังนั้นจึงควรมีการประเมินสถานการณ์หากระบบคลาวด์ไม่พร้อมใช้งาน โดยเฉพาะในการใช้งานที่ต้องพร้อมใช้งานข้อมูลตลอด 100% และการจัดเก็บข้อมูลในระยะยาวเป็นเงื่อนไขที่สำคัญ - David Clarke**

ไดร์ฟ USB กับอนาคตของระบบจัดเก็บข้อมูลผ่านคลาวด์

ในทางกลับกัน การเข้ารหัส USB จะสามารถทำได้ผ่านฮาร์ดแวร์ของอุปกรณ์เองหรือโดยอาศัยซอฟต์แวร์ การเข้ารหัสเชิงฮาร์ดแวร์โดยไม่พึงพาซอฟต์แวร์เลยเป็นวิธีการที่มีประสิทธิภาพมากที่สุดในการปกป้องการโจมตีทางไซเบอร์ นี่คือระบบการทำงานที่สมบูรณ์แบบและไม่ซับซ้อนในการปกป้องข้อมูลจากการถูกแฮ็ค และยังได้มาตรฐานควบคุมด้านความปลอดภัยระดับสูงที่ช่วยให้หน่วยงานต่าง ๆ เกิดความมั่นใจในการจัดการภัยคุกคามและลดปัจจัยเสี่ยงต่าง ๆ

เนื่องจากเป็นระบบที่อยู่ได้ด้วยตัวเอง ไดร์ฟ USB เข้ารหัสเชิงฮาร์ดแวร์จึงไม่ต้องอาศัยซอฟต์แวร์ใด ๆ จากคอมพิวเตอร์โฮสต์ ปัญหาจากซอฟต์แวร์ที่หายไปยังช่วยขจัดปัญหาจากการทุบทำลาย การสอดแนม (sniffing) และการแฮชหน่วยความจำ ไดร์ฟ USB เข้ารหัสเชิงซอฟต์แวร์มักมีความเสี่ยงจากผู้ใช้ที่สามารถปิดใช้งานการเข้ารหัสโดยการฟอร์แมตไดร์ฟผ่านคอมพิวเตอร์ และใช้ไดร์ฟดังกล่าวเพื่อจัดเก็บข้อมูลที่อ่อนไหวแบบไม่มีการป้องกันใด ๆ

ไดร์ฟ USB เข้ารหัสเชิงฮาร์ดแวร์ยังมีการป้องกันทางกายภาพที่เหนือกว่าเพื่อดูแลความปลอดภัยของข้อมูล โดยจะมีหลักเกณฑ์ในการสืบค้นข้อมูลที่ผู้ใช้หรือผู้ดูแลกำหนดตั้งค่าได้ และสามารถทำงานร่วมกับระบบรองรับปลายทางในพื้นที่ที่มีอยู่ ซึ่งทำให้สะดวกและลดค่าใช้จ่ายในสถานการณ์ต่าง ๆ ที่อาจไม่เหมาะกับระบบคลาวด์หรือกรณีที่ทางเลือกอื่น ๆ อาจไม่มีประสิทธิภาพมากพอ เช่น กรณีที่ต้องมีการจัดเก็บข้อมูลจากอุปกรณ์ที่ไม่ได้เชื่อมต่อกับเครือข่ายและต้องมีความเป็นส่วนตัวหรือต้องสามารถสืบค้นได้ขณะออฟไลน์

> **“หากพิจารณาข้อมูลในสถานะ 'ร้อน' หรือ 'เย็น' โดยขึ้นอยู่กับระดับการใช้งานในแต่ละวันสำหรับหน่วยงานการจัดเก็บข้อมูล 'เย็น' ไว้ในคลาวด์อาจมีประสิทธิภาพมากกว่า ในขณะที่ข้อมูล 'ร้อน' จะเหมาะกับการจัดเก็บผ่าน USB มากกว่า หากหลักเกณฑ์สำคัญสำหรับหน่วยงานคือความต่อเนื่องในการทำงานและประสิทธิภาพที่เหนือกว่า หรือหากมีความเหมาะสมสำหรับการใช้งานหรือกระบวนการเฉพาะด้านทางธุรกิจ - Rafael Bloom”**

สรุป

แม้ว่าเราจะไม่สามารถคาดเดาได้ว่าจะเกิดนวัตกรรมใดอีกในอนาคต แต่สิ่งที่เราสามารถนำเสนอคือไดร์ฟ USB ที่มีรางวัลรับรองคุณภาพและมีฟังก์ชันการเข้ารหัสในระดับต่าง ๆ เพื่อปกป้องข้อมูลที่มีการเคลื่อนย้าย ตั้งแต่ไดร์ฟ USB ที่มีแป้นกดตัวอักษรและตัวเลขที่สามารถใช้ PIN ป้องกันได้อย่างสะดวก ไปจนถึงการรับรองมาตรฐาน FIPS 140-2 Level 3 เพื่อการเข้ารหัสที่ปลอดภัยสูงสุดพร้อมทั้งระบบป้องกันการทุบทำลาย และต่อยอดมาเป็นเทคโนโลยี SuperSpeed USB 3.1 ที่ยังคงมีระดับความปลอดภัยไม่แพ้เดิม Kingston IronKey คือผลิตภัณฑ์ที่ออกแบบมาเพื่อตอบโจทย์ด้านการจัดการข้อมูลของคุณด้วยไดร์ฟ USB ที่สามารถถ่ายโอนและเคลื่อนย้ายข้อมูลได้อย่างมีประสิทธิภาพ

ทีมงานผู้เชี่ยวชาญของเราพร้อมให้การสนับสนุนคุณในทุกขั้นตอนของการจัดเก็บข้อมูลของคุณ เรามีความพร้อมเต็มที่ในการช่วยคุณคัดสรรระบบจัดเก็บข้อมูลที่ตรงกับความต้องการของคุณมากที่สุด

เรามีทักษะและขีดความสามารถด้านเทคนิคที่จะช่วยให้คุณสามารถดูแลข้อมูลลับของคุณให้ปลอดภัยและเป็นไปตามข้อบังคับใหม่ ๆ ไม่ว่าจะผ่านไดร์ฟ USB เข้ารหัส การคัดเลือกประเภทของไดร์ฟที่เหมาะกับการใช้งานมากที่สุด หรือการกำหนดและบังคับใช้นโยบายด้านการรักษาความปลอดภัยต่าง ๆ การนำเสนอผลิตภัณฑ์ที่มีลักษณะเฉพาะตัวเป็นการแสดงออกถึงความมุ่งมั่นของเราในการนำสนับสนุนเป้าหมายในการจัดเก็บข้อมูลของคุณ เพื่อให้คุณอุ่นใจได้กับความเร็วในการทำงานในระดับที่ไม่เคยมีมาก่อนที่พร้อมก้าวตามโลกธุรกิจที่กำลังเปลี่ยนแปลงไป

เกี่ยวกับ Kingston

ประสบการณ์กว่า 35 ปีทำให้ Kingston มีองค์ความรู้ในการพิจารณาและแก้ไขปัญหาในการเคลื่อนย้ายข้อมูลของคุณ ทำให้เกิดความสะดวกกับแรงงานของคุณในการทำงานได้อย่างปลอดภัยโดยไม่กระทบต่อหน่วยงานของคุณ

#KingstonIsWithYou

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers