



ข้อมูลด้านการรักษา
ความปลอดภัยของส่วน
การทำงานปลายทางที่มี
ประสิทธิภาพ โดยความ
ร่วมมือกับ Matrix42

MATRIX42

#KingstonIsWithYou

ข้อมูลด้านการรักษาความปลอดภัยของส่วนการทำงาน ปลายทางที่มีประสิทธิภาพ โดยความร่วมมือกับ Matrix42

เกริ่นนำ

การปกป้องข้อมูลคือเงื่อนไขเบื้องต้นที่ธุรกิจ ภาครัฐและบุคคลทั่วไป
ในปัจจุบันต่างให้ความสำคัญ

การเจาะข้อมูล การแฮ็คและปัจจัยจากบุคคลคือสิ่งที่เราพบได้เป็นประจำเมื่อเกิดปัญหา
หรือความเสี่ยงด้านการละเมิดความปลอดภัยของข้อมูลทั่วโลก ต้นทุนทางการเงินและชื่อ
เสียงจากการละเมิดข้อมูลอาจส่งผลกระทบอย่างร้ายแรง เงื่อนไขสำหรับระบบรักษาความ
ปลอดภัยทางคอมพิวเตอร์และกลยุทธ์ Endpoint DLP ขั้นสูง (ระบบป้องกันการสูญหายของ
ข้อมูล) ล้วนต้องอาศัยผลิตภัณฑ์จัดเก็บข้อมูลและหน่วยความจำที่พึงพาได้

การใช้ระบบเข้ารหัส สื่อบันทึกข้อมูลและหน่วยความจำที่ทำงานได้รวดเร็วร่วมกับการปรับ
ใช้แนวทางที่เหมาะสม มาตรฐานและนโยบายที่เชื่อถือได้ล้วนเป็นองค์ประกอบที่สำคัญ
อย่างยิ่ง โน้ตบุ๊กหรือไดรฟ์ USB ที่สูญหายอาจทำให้บุคคลและธุรกิจต่าง ๆ ตกอยู่ในความ
เสี่ยงจากข้อมูลส่วนบุคคลหรือข้อมูลภายในที่รั่วไหล Kingston ขอเสนอระบบป้องกันภัย
คุกคามที่สามารถลดปัจจัยเสี่ยงได้ร่วมกับแผนการรักษาความปลอดภัยใหม่ ๆ หรือที่มีอยู่
ในปัจจุบัน



เนื้อหา

ในอีบุ๊กเล่มนี้ คุณจะได้พบกับระบบการทำงานปลายทางต่าง ๆ ที่ไดรฟ์ USB เข้ารหัสจาก Kingston แผนการปรับแต่งเฉพาะและซอฟต์แวร์ Matrix42 EgoSecure Data Protection สามารถเข้ามาช่วยแก้ไขปัญหากลุ่มอุตสาหกรรม เพื่อให้มีผลิตภัณฑ์ที่ตรงกับความต้องการทางธุรกิจอย่างแท้จริง

เราจะเจาะลึกรายละเอียดทั้งหกข้อนี้ และการใช้งานเพื่อจัดการปัญหาด้านการรักษาความปลอดภัยของส่วนการทำงานปลายทาง

สารบัญ

หัวข้อที่ 1	กรณีการใช้งานในกลุ่มอุตสาหกรรม - ภาครัฐ	4
หัวข้อที่ 2	กรณีการใช้งานในกลุ่มอุตสาหกรรม - การดูแลสุขภาพ	5
หัวข้อที่ 3	กรณีการใช้งานในกลุ่มอุตสาหกรรม - การเงิน	6
หัวข้อที่ 4	กรณีการใช้งานในกลุ่มอุตสาหกรรม - ยานยนต์	7
หัวข้อที่ 5	กรณีการใช้งานในกลุ่มอุตสาหกรรม - โทรคมนาคม	8
หัวข้อที่ 6	กรณีการใช้งานในกลุ่มอุตสาหกรรม - การผลิต	9
หัวข้อที่ 7	Kingston และ Matrix42 Solutions	10
	สรุป	11
	เกี่ยวกับ Kingston	12



หัวข้อที่ 1: กรณีการใช้งานในกลุ่มอุตสาหกรรม ภาครัฐ

สถานการณ์แวดล้อม:

สำหรับภาครัฐ การใช้อุปกรณ์ USB ถือเป็นสิ่งที่พบได้ทั่วไป เช่น หน่วยงานของรัฐอาจมีการคัดลอกภาพที่ถ่ายโดยผู้กระทำผิดในการจราจรและข้อมูลความผิดจากกล้องดิจิตอลไปยังระบบของหน่วยงานโดยใช้สาย USB เจ้าหน้าที่ตำรวจอาจต้องรับข้อมูลการสืบสวนผ่านอุปกรณ์บันทึกข้อมูลต่อพ่วง ข้อมูลเหล่านี้จะต้องถูกเขียนเข้าและจะต้องมีการป้องกันการสืบค้นโดยไม่ได้รับอนุญาต

ความท้าทาย:

เนื่องจากอุปกรณ์ USB ที่เป็นที่ต้องการอย่างมาก พนักงานจึงมักมีการเบิกไดรฟ์ USB เป็นประจำ การใช้อุปกรณ์บันทึกข้อมูลส่วนตัวหรือข้อมูลที่ไม่ได้รับอนุญาตจึงต้องมีการควบคุมอย่างเข้มงวดเพื่อความปลอดภัย หากพนักงานต้องการอุปกรณ์จัดเก็บข้อมูล USB ใหม่ ก็จะต้องมีส่วนงานเบิกจ่ายที่ทำงานได้อย่างรวดเร็วเพื่อให้พนักงานสามารถรวบรวมข้อมูลให้เป็นชุดเดียวกัน ปัญหาด้านการรักษาความปลอดภัยจะไม่เกิดขึ้นหากมีการใช้อุปกรณ์ USB อย่างเหมาะสม

แนวทางออก:

การประสานฟังก์ชันการควบคุมอุปกรณ์ การคัดกรองข้อมูล และการเข้ารหัสจะนำไปสู่สถานการณ์ดังต่อไปนี้

อุปกรณ์ที่ไม่รู้จักจะถูกปิดกั้นจากคอมพิวเตอร์ปลายทาง อุปกรณ์จัดเก็บข้อมูล เช่น กล้องดิจิตอลจะได้รับอนุญาตให้ใช้เฉพาะในกรณีที่กำหนด เช่น เพื่ออ่านไฟล์ภาพเท่านั้น การเขียนข้อมูลจะถูกเข้ารหัสและอนุญาตให้ทำได้ผ่านอุปกรณ์ USB ที่ได้รับอนุญาตเท่านั้น การสืบค้นข้อมูลทั้งหมดจะต้องมีการบันทึกประวัติไว้ การจัดการอุปกรณ์ที่ได้รับอนุญาตสามารถทำได้ง่าย ๆ โดยการกำหนดซีเรียลนัมเบอร์และการกำหนด ID ฮาร์ดแวร์ Matrix42 Service Management ช่วยให้ผู้ใช้สามารถแจ้งเบิกไดรฟ์ USB เฉพาะจาก Kingston Technology ผ่านโซลต์บริการตนเอง หลังจากผ่านการรับรอง อุปกรณ์ USB จะถูกอนุญาตให้ใช้อัตโนมัติใน EgoSecure Data Protection

“พนักงานของเรารู้สึกตื่นเต้นมากเกี่ยวกับอุปกรณ์ USB แบบใหม่ที่ช่วยเพิ่มความสะดวกและรวดเร็วเนื่องจากกระบวนการรับรองที่สั้นมาก เรามีความพอใจอย่างยิ่งกับแผนการปรับแต่งการใช้งานจาก Kingston Technology และการจัดการที่ไม่ยุ่งยากของ Matrix42 ผ่านฟังก์ชันการจัดการบริการและการรักษาความปลอดภัยของส่วนการทำงานปลายทาง”

หัวหน้าฝ่ายบริการ ภาครัฐ

หัวข้อที่ 2: กรณีการใช้งานในกลุ่มอุตสาหกรรม การดูแลสุขภาพ

สถานการณ์แวดล้อม:

อุปกรณ์จัดเก็บข้อมูลต่อพ่วงยังคงถูกใช้งานอย่างแพร่หลายและเป็นอุปกรณ์สำหรับแลกเปลี่ยนข้อมูลระหว่างพนักงานและหน่วยงานต่าง ๆ

เช่น โรงพยาบาลในเยอรมนีจะต้องแจ้งข้อมูลผู้ป่วยมะเร็งในปัจจุบันไปยัง Cancer Registry และสถานะการดำเนินโรค เพื่อความสะดวก ข้อมูลมักจะถูกถ่ายโอนผ่านอุปกรณ์จัดเก็บข้อมูลผ่านเครือข่ายมือถือ

แพทย์มักสืบค้นข้อมูลการวิจัยต่าง ๆ เพื่อเตรียมใช้งานโดยอาศัยไดรฟ์ USB

ความท้าทาย:

ข้อมูลผู้ป่วยถือเป็นข้อมูลที่อ่อนไหวอย่างยิ่งและจะต้องไม่ตกอยู่ในมือของผู้ที่ไม่ได้รับอนุญาต ดังนั้น จะต้องมีการยกระดับมาตรการการปกป้องข้อมูลอย่างจริงจัง หากการเชื่อมต่อเครือข่ายขาดหาย ก็อาจเกิดปัญหาอย่างมาก ไม่เฉพาะเนื่องจากเงื่อนไขด้าน GDPR แต่ยังรวมถึงสวัสดิภาพของผู้ป่วยด้วย ด้วยเหตุนี้ จึงต้องมีการควบคุม ตรวจสอบและเข้ารหัสการสืบค้นข้อมูลผ่าน USB

แนวทางออก:

EgoSecure Data Protection ผสมผสานมาตรการป้องกันต่าง ๆ เช่น การควบคุมการสืบค้น การตรวจสอบข้อมูล การคัดกรองและการเข้ารหัสแบบครบวงจร ผู้ดูแลระบบ IT สามารถตัดสินใจได้ว่าจะให้สิทธิ์การสืบค้นข้อมูลจากอุปกรณ์ใดแก่พนักงานคนใด และสามารถกำหนดข้อยกเว้น เช่น จากซีเรียลนัมเบอร์หรือ ID ฮาร์ดแวร์ รหัสประจำตัว เหล่านี้สามารถกำหนดได้ผ่านแผนงานปรับแต่งการใช้งานจาก Kingston Technology ทำให้สามารถกำหนดค่ารายการที่ต้องการใน EgoSecure Data Protection เพื่อให้อนุญาตเฉพาะอุปกรณ์ของบริษัทในการใช้งานเท่านั้น วิธีการนี้สามารถลดภาระด้านการจัดการได้อย่างมาก และเพิ่มระดับความปลอดภัยของข้อมูล (GDPR, CCPA, HIPAA ฯลฯ) เนื่องจากการใช้งานจะถูกเข้ารหัสและมีการตรวจติดตาม

“ เราต่างเคยใช้ไดรฟ์ USB เข้ารหัสจาก Kingston กันไปแล้ว ด้วย EgoSecure Data Protection เราจะมั่นใจได้ว่าจะสามารถตรวจย้อนการถ่ายโอนข้อมูลผู้ป่วยภายใต้เงื่อนไขของ EU-GDPR ”

CISO, โรงพยาบาลของมหาวิทยาลัย



สถานการณ์แวดล้อม:

ธนาคารต่าง ๆ ต้องปฏิบัติตามระเบียบข้อบังคับมากมาย หนึ่งในนี้ก็คือ PCI-DSS (Payment Card Industry Data Security Standard) PCI-DSS ครอบคลุมทั้งเงื่อนไขในการเข้ารหัสข้อมูล การวิเคราะห์ความเสี่ยงและการคัดกรองข้อมูล เป้าหมายคือเพื่อลดหรือป้องกันภัยคุกคามและความเสี่ยงด้าน IT อย่างสิ้นเชิง

ความท้าทาย:

มีปัจจัยเสี่ยงมากมายในระบบ IT สำหรับส่วนการทำงานปลายทาง พนักงานที่ต้องดูแลข้อมูลบัตรชำระเงินจากลูกค้าและธุรกิจต่าง ๆ และต้องประมวลผลข้อมูลที่อ่อนไหวจากสถาบันการเงินเป็นประจำทุก ๆ วัน จึงอยู่ในความเสี่ยงจากการแลกเปลี่ยนข้อมูลผ่านคลาวด์ USB หรือทางเว็บที่อาจติดมัลแวร์ หรือตกอยู่ในมือของบุคคลภายนอก เนื่องจากไม่มีระบบการป้องกันที่ดีพอ เหตุการณ์เช่นนี้จะทำให้ธนาคารเกิดความเสี่ยงด้านการเงินภายใต้เงื่อนไข GDPR, PCI-DSS และ Sarbanes-oxley act นอกจากนี้ อาชญากรคอมพิวเตอร์ยังพยายามเจาะระบบของธนาคารในหลากหลายรูปแบบ ด้วยวิธีการที่สร้างสรรค์มากขึ้นเรื่อย ๆ เมื่อเร็ว ๆ นี้ได้เกิดอาชญากรรมคอมพิวเตอร์เกี่ยวกับ ATM ขึ้น โดยอาศัยการตัดไฟเลี้ยงเครื่อง ระบบจะถูกเปิดใช้งานผ่านอุปกรณ์ USB สำหรับบูตเพื่อขโมยเงินจากตู้

แนวทางออก:

ระบบ IT จะต้องมีการดูแลความปลอดภัยผ่านมาตรการป้องกันหลายชั้น ซึ่งสามารถทำได้โดยอาศัยระบบควบคุมแอปพลิเคชัน ระบบควบคุมอุปกรณ์ ระบบตรวจหาความผิดปกติ UEBA (User and Entity Behaviour Analytics) การตรวจติดตามและการเข้ารหัสที่สอดคล้องกับ PreBoot Authentication Matrix42 ก็สามารถช่วยในการดูแลความปลอดภัยของระบบแบบอัตโนมัติ โดยแอปพลิเคชันและอุปกรณ์ USB เข้ารหัสที่ได้รับอนุญาตเท่านั้นที่จะสามารถใช้งานได้ นอกจากนี้ กิจกรรมที่น่าสงสัยหรืออาจเป็นอันตรายจะถูกตรวจพบ และกำหนดมาตรการจัดการแบบอัตโนมัติ ในส่วนของการใช้งานไดรฟ์ USB ไดรฟ์ USB แบบใช้งานเฉพาะด้านจาก Kingston Technology สามารถช่วยให้ความมั่นใจได้ว่าอุปกรณ์จะมีรายการทะเบียนข้อมูลที่เชื่อถือได้ กำหนดไว้เพื่อเป็นมาตรการป้องกันเบื้องต้น รวมทั้งข้อมูลจะถูกเข้ารหัสในรูปแบบที่ตรวจย้อนได้ สิ่งนี้จะช่วยยกระดับมาตรฐานการรักษาความปลอดภัยโดยไม่เพิ่มภาระให้แก่ผู้ปฏิบัติงาน

“EgoSecure Data Protection และฟังก์ชันการจัดทำรายการทะเบียนข้อมูลที่เชื่อถือได้จะอนุญาตให้มีการใช้เฉพาะไดรฟ์ USB แบบเข้ารหัสจาก Kingston เท่านั้น โดยเราจะจัดทำรายการทะเบียนข้อมูลที่เชื่อถือได้สำหรับไดรฟ์ USB เข้ารหัสจาก Kingston ผ่าน ID ฮาร์ดแวร์ประจำตัว และไม่อนุญาตให้มีการใช้งานอุปกรณ์อื่น ๆ วิธีนี้จะช่วยลดภาระในการจัดการอย่างมาก ในขณะที่การรักษาความปลอดภัยก็ดีขึ้นมากตามไปด้วย!”

ผู้จัดการฝ่าย IT บริษัทการเงิน

หัวข้อที่ 4: กรณีการใช้งานในกลุ่มอุตสาหกรรมยานยนต์

สถานการณ์แวดล้อม:

ในอุตสาหกรรมยานยนต์ การใช้อุปกรณ์ USB ถูกนำมาใช้หลายกรณีด้วยกัน เช่น ข้อมูลวิจัยที่ถูกจัดเก็บผ่านอุปกรณ์บันทึกข้อมูลต่อพ่วง และมีการแลกเปลี่ยนข้อมูลระหว่างวิศวกรในบริษัท ในการกำหนดโครงสร้างการทำงานของเครื่อง ไฟล์ต่าง ๆ จะถูกนำส่งจากระบบ IT ไปยังระบบ OT ข้อมูลทั้งหมดเหล่านี้มีความอ่อนไหวมากและจะต้องได้รับการปกป้องจากการใช้ประโยชน์ในเชิงอุตสาหกรรมหรือการโจรกรรม ไม่เช่นนั้นองค์ความรู้ที่ถูกพัฒนาขึ้นมาก็จะถูกฉกฉวยไปโดยผู้ไม่ประสงค์ดี

ความท้าทาย:

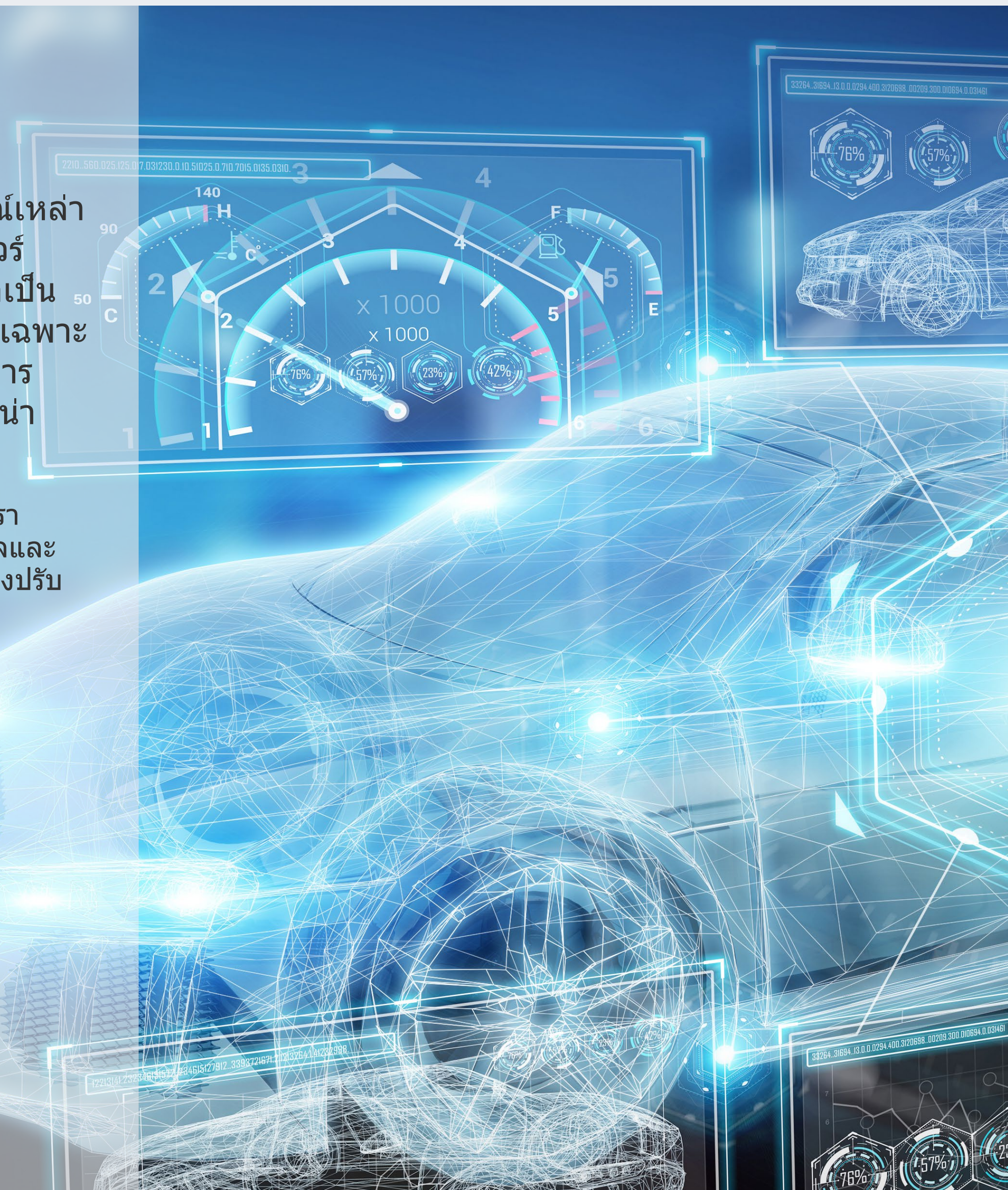
อุตสาหกรรมยานยนต์จะต้องปฏิบัติตามมาตรฐานต่าง ๆ มากมายไม่ว่าจะเป็น TISAX, ระบบป้องกันผลิตภัณฑ์ต้นแบบ} ENX, ISO27001, "ระบบการเชื่อมต่อจากภายนอก" และ GDPR สำหรับ TISAX เงื่อนไขควบคุมข้อ 9.1, 9.5 และ 10.1 กำหนดไว้ว่าการสืบค้นข้อมูลจะต้องมีการควบคุม ตรวจสอบ คัดกรองและเข้ารหัส มาตรการเหล่านี้จะต้องปฏิบัติตามร่วมกับเงื่อนไขอื่น ๆ เช่น GDPR และ ISO27001 ภายในอุตสาหกรรมยานยนต์ทั้งหมด

แนวทางออก:

ไดรฟ์ USB เข้ารหัสจาก Kingston Technology มีการปกป้องข้อมูลด้วยระบบเข้ารหัสเชิงฮาร์ดแวร์ อุปกรณ์เหล่านี้สามารถรองรับซีเรียลนัมเบอร์เฉพาะและ ID ฮาร์ดแวร์เพื่อใช้ใน EgoSecure Data Protection สำหรับจัดทำเป็นรายการทะเบียนข้อมูลที่เชื่อถือได้สำหรับการใช้งานเฉพาะด้านแบบอัตโนมัติ นอกจากนี้ ยังสามารถตรวจสอบการเคลื่อนย้ายและวิเคราะห์ข้อมูลได้หากเกิดกิจกรรมที่น่าสงสัยขึ้น

“ Matrix42 และมาตรการจาก Kingston Technology ทำให้เราสามารถปฏิบัติตามเงื่อนไข TISAX ข้อ 9.5 (การสืบค้นข้อมูลและแอปพลิเคชัน) และข้อ 10.1 (การเข้ารหัส) โดยที่ผู้ใช้ไม่ต้องปรับเปลี่ยนพฤติกรรมการใช้งานอย่างมีนัยสำคัญใด ๆ ”

CTO ชัฟฟลายเออร์กลุ่มยานยนต์



สถานการณ์แวดล้อม:

ผู้ให้บริการด้านโทรคมนาคมมีข้อมูลเป็นจำนวนมากเกี่ยวกับลูกค้าที่จัดเก็บไว้ ข้อมูลนี้มีความอ่อนไหวอย่างยิ่ง โดยเฉพาะภายใต้เงื่อนไขของ GDPR ดังนั้นจึงต้องมีการกำหนดมาตรการที่เหมาะสมเพื่อป้องกันการสูญหายของข้อมูลและการโจรกรรมข้อมูล

ความท้าทาย:

ผู้ปฏิบัติงานด้านโทรคมนาคมจะต้องพบเจอกับข้อมูลของลูกค้าเป็นประจำทุกวัน ข้อมูลส่วนใหญ่จะถูกจัดเก็บไว้ในแอปพลิเคชันทางธุรกิจ อย่างไรก็ตามอาจมีความเสี่ยงที่ข้อมูลสัญญาของลูกค้าหรือมีการส่งออกฐานข้อมูลไปยังส่วนการทำงานปลายทางหรืออุปกรณ์ต่อพ่วง ในการแลกเปลี่ยนข้อมูล ผู้ใช้มักอาศัยอุปกรณ์จัดเก็บข้อมูลแบบต่อพ่วง จึงสำคัญอย่างยิ่งที่จะต้องสามารถตรวจหารูปแบบการจัดเก็บข้อมูลที่ไม่เหมาะสม เพื่อแก้ไขปัญหาและป้องกันไม่ให้เกิดเหตุขึ้นอีก

แนวทางออก:

เพื่อลดความยุ่งยากในกระบวนการจัดซื้อจัดจ้าง ไดรฟ์ USB เข้ารหัสจาก Kingston Technology ที่มี ID เฉพาะจึงสามารถจัดซื้อได้อย่างรวดเร็วผ่านระเบียบรายชื่อที่กำหนด

ไว้ใน EgoSecure Data Protection และนำส่งผ่านแคตตาล็อกบริการของ Matrix42 การจัดเก็บและส่งออกข้อมูลอาจครอบคลุมข้อมูลที่มีความอ่อนไหวจะสามารถระบุและจัดการได้โดยวิธีการตรวจสอบแบบ Deep Content โดยอ้างอิงจากการสแกน "ข้อมูลใช้งาน" และ "ข้อมูลที่พิกเก็บไว้" การเคลื่อนย้ายข้อมูลจะถูกบันทึกประวัติไว้จากส่วนกลาง ดังนั้นผู้ปฏิบัติงานจึงสามารถขอรับฮาร์ดแวร์ใหม่เพื่อจัดเก็บข้อมูลได้อย่างรวดเร็วหลังจากมีการแจ้งเบิกและผ่านการรับรอง วิธีการนี้ยังรับประกันว่าเป็นไปตามเงื่อนไข GDPR

“ระบบบริการตนเอง Matrix42 ทำให้ผู้ใช้ของเราสามารถร้องขอสิบบันทึกข้อมูลที่ต้องการได้เมื่อต้องการ หลังจากมีการรับรองคำสั่งและจัดส่งแล้ว อุปกรณ์จะได้รับอนุญาตจากระบบควบคุมอุปกรณ์ของ EgoSecure การผสมผสานระหว่าง Matrix42 และมาตรการของ Kingston Technology ช่วยเพิ่มผลผลิตและความปลอดภัยให้กับบริษัทของเรา”

CTO ผู้ให้บริการด้านโทรคมนาคม



หัวข้อที่ 6: กรณีการใช้งานในกลุ่มอุตสาหกรรม อุตสาหกรรมการผลิต



สถานการณ์แวดล้อม:

ข้อมูลดิจิทัลคืออนาคตที่สดใส ข้อมูลที่มีคุณค่าเหล่านี้ในอุตสาหกรรมการผลิตจะประกอบไปด้วยแผนการผลิต ข้อมูลลูกค้าและซัพพลายเออร์และองค์ความรู้ของบริษัท หากข้อมูลดังกล่าวสูญหาย ไม่เพียงแต่จะส่งผลให้ถูกลงโทษอย่างรุนแรงภายใต้ GDPR แต่ยังอาจกระทบต่อชื่อเสียงของผู้ให้บริการอย่างมาก เราอาจพบเห็น USB ในแท็กซี่ ร้านซักรีด สนามบิน สถานีรถไฟ หรือที่จอดรถและสถานที่อื่น ๆ ทั่วไป

ความท้าทาย:

อุปกรณ์จัดเก็บข้อมูลมักมีข้อมูลที่มีความอ่อนไหวสูงและข้อมูลนี้ส่วนใหญ่ไม่มีการเข้ารหัสไว้ นอกจากนี้ยังมีความเสี่ยงที่เจ้าหน้าที่เทคนิคด้านการให้บริการอาจใช้ผู้ใช้บริการข้อมูลจากภายนอกเพื่อบันทึกข้อมูลอัปเดตสำหรับเครื่องจักรเพื่อการผลิต อุปกรณ์ต่อพ่วงเหล่านี้อาจมีความเสี่ยงในการนำมัลแวร์เข้าสู่เครือข่าย

แนวทางออก:

ไดรฟ์ USB เข้ารหัสจาก Kingston Technology มีการปกป้องข้อมูลด้วยระบบเข้ารหัสเชิงฮาร์ดแวร์ อุปกรณ์เหล่านี้สามารถจัดส่งพร้อมซีเรียลนัมเบอร์เฉพาะและ ID ฮาร์ดแวร์เพื่อใช้ใน EgoSecure Data Protection สำหรับจัดทำเป็นรายการทะเบียนข้อมูลที่เชื่อถือได้สำหรับการใช้งานเฉพาะด้านแบบอัตโนมัติ นอกจากนี้ ยังสามารถตรวจสอบการเคลื่อนย้ายและวิเคราะห์ข้อมูลได้หากเกิดกิจกรรมที่น่าสงสัยขึ้น

“ การเข้ารหัสข้อมูลการผลิตของเราเป็นสิ่งสำคัญอย่างยิ่งสำหรับเรา เพื่อให้เราสามารถป้องกันตนเองจากการถูกโจรกรรมข้อมูล ข้อมูลที่อ่อนไหวอย่างนี้จะอนุญาตให้ใช้งานได้ผ่านไดรฟ์ USB เข้ารหัสที่ได้รับการรับรองจาก Kingston เท่านั้น โดยจะมีการคัดกรองไฟล์ผ่าน EgoSecure Data Protection สำหรับอุปกรณ์ USB อื่น ๆ ทั้งหมด ข้อมูลการผลิตจะถูกปิดกั้นและการเขียนข้อมูลไปยังสื่อบันทึกข้อมูลต่อพ่วงจะถูกกำกับดูแลโดย EgoSecure โดยใช้ฟังก์ชันการเข้ารหัสระหว่างนำส่งและการบันทึกประวัติการทำงาน ”

ผู้บริหารฝ่ายรักษาความปลอดภัยด้าน IT
อุตสาหกรรมการผลิต



การใช้ระบบเข้ารหัส ล็อกบันทึกข้อมูลและหน่วยความจำที่ทำงานได้รวดเร็วร่วมกับการปรับใช้แนวทางที่เหมาะสม มาตรฐานและนโยบายที่เชื่อถือได้ล้วนเป็นองค์ประกอบที่สำคัญอย่างยิ่ง โน้ตบุ๊กหรือไดรฟ์ USB ที่สูญหายอาจทำให้นบุคคลและธุรกิจต่าง ๆ ตกอยู่ในความเสี่ยงจากข้อมูลส่วนบุคคลหรือข้อมูลภายในที่รั่วไหล Kingston Technology มีระบบป้องกันภัยคุกคามที่สามารถลดปัจจัยเสี่ยงได้ร่วมกับแผนการรักษาความปลอดภัยใหม่ ๆ หรือที่มีอยู่ในปัจจุบัน

ไดรฟ์ USB เข้ารหัสจาก Kingston Technology

ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์จาก Kingston Technology นำเสนอระบบป้องกันข้อมูลที่ใช้งานกับอุปกรณ์พกพาต่าง ๆ ทั้งภายในและภายนอกระบบไฟร์วอลล์ของหน่วยงาน การออกแบบที่เน้นการปกป้องข้อมูลที่ต้องการความปลอดภัยสูง ไดรฟ์เหล่านี้ช่วยให้คุณสามารถปฏิบัติตามมาตรฐาน ข้อกำหนด และข้อบังคับของกลุ่มอุตสาหกรรม ผลิตภัณฑ์ได้มาตรฐาน TAA และ FIPS และมีจำหน่ายที่ขนาดสูงสุด 128GB เหมาะอย่างยิ่งสำหรับผู้ใช้งานระดับองค์กรและหน่วยงานรัฐ



แผนการปรับแต่งบริการ เพื่อความปลอดภัย

คุณสามารถปรับแต่งไดรฟ์ USB เข้ารหัสจาก Kingston Technology ได้หลายรูปแบบตามความต้องการของหน่วยงานของคุณ เพิ่มคุณสมบัติที่เลือกเพื่อให้ได้ไดรฟ์ที่โดดเด่นและขาดไม่ได้ Kingston Technology ขอเสนอช่องทางการสั่งซื้อสินค้าที่สะดวกและง่ายดายสำหรับไดรฟ์ USB เข้ารหัสใช้งานเฉพาะด้านผ่านตัวแทนจำหน่ายที่คุณต้องการ ผลิตภัณฑ์กลุ่ม USB แบบเข้ารหัสจาก Kingston Technology ครอบคลุม DTVP30, DT4000G2 และ IKD300S. แผนงานนี้เสนอทางเลือกสำหรับความต้องการที่มักได้รับการเรียกร้องจากลูกค้า เช่น การกำหนดซีเรียลนัมเบอร์ การกำหนดรหัสผ่านสองชั้นหรือโลโก้ประจำตัว หากสั่งซื้อสินค้าขั้นต่ำ 50 ชิ้น หรือสั่งเพิ่ม 25 ชิ้น ลูกค้าสามารถกำหนดเงื่อนไขเฉพาะที่หน่วยงานของตนเองต้องการ

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection เป็นระบบจัดการความปลอดภัยแบบ 360° เพื่อการป้องกันและปกป้องอุปกรณ์ ระบบการทำงานและข้อมูล กระบวนการทำงานจะเป็นไปแบบอัตโนมัติเพื่อป้องกันและตรวจหามาตรการจัดการในกรณีที่เกิดความเสียหายขึ้น โดยไม่กระทบต่อการทำงานตามปกติ

การปกป้องข้อมูลและป้องกันภัยคุกคามทางคอมพิวเตอร์ อาจดูเป็นงานที่หนักหน่วง เจื่อนไซของการทำงานในโลก ดิจิตอลมีการเปลี่ยนแปลงไปอย่างมาก โดยผู้ปฏิบัติงาน สามารถตัดสินใจได้เองว่าจะทำงานกับอุปกรณ์ใด เมื่อไร และที่ไหน องค์ประกอบที่ลงตัวระหว่างไดรฟ์ USB เข้ารหัส เชิงฮาร์ดแวร์และการจัดการซอฟต์แวร์ของส่วนการทำงาน ปลายทางจะช่วยให้หน่วยงานต่าง ๆ สามารถควบคุม อุปกรณ์ที่ใช้ในงานในหน่วยงานของตน ดังนั้นจึงเป็นการลด ความเสี่ยงจากการละเมิดข้อมูลและยังช่วยในการปฏิบัติ ตามเงื่อนไข GDPR ได้อย่างต่อเนื่อง





เกี่ยวกับ Kingston

ประสบการณ์กว่า 30 ปีทำให้ Kingston Technology มีองค์ความรู้ที่ช่วยในการระบุและแก้ไขปัญหาด้านการรักษาความปลอดภัยสำหรับส่วนการทำงานปลายทางของคุณโดยไม่กระทบต่อการทำงานตามปกติภายในหน่วยงาน

©2021 Kingston Technology Far East Corp. (Asia Headquarters), No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan.

สงวนลิขสิทธิ์ เครื่องหมายการค้าและเครื่องหมายการค้าจดทะเบียนทั้งหมด ถือเป็นกรรมสิทธิ์ของผู้เป็นเจ้าของ

#KingstonIsWithYou