DYGISTECH

DYGISTECH CO.,LTD.

# IoT Cloud

## Data Security

MERCURY DYGISTECH

Malin 1

mDashboard

# ใครเป็นเจ้าของข้อมูล?

ลูกค้าเป็นเจ้าของข้อมูลทั้งหมด ข้อมูลจะถูกใช้เมื่อโปรแกรมเก็บข้อมูลของ Dygistech ทำงาน เราจะไม่ใช้ข้อมูลและแชร์ให้บุคคลภายนอกเด็ดขาด จะมีการเรียกดูข้อมูลผ่าน Malin1 Platform เท่านั้น

# เก็บข้อมูลไว้ที่ไหน?

ปัจจุบันเราเก็บไว้ที่ Google Cloud Data Center “asia-east1” ที่ประเทศสิงคโปร์

# How Do We Secure Your Production Data?

เรารักษาความปลอดภัยข้อมูลของคุณอย่างไร?

## การเรียกดูข้อมูลบนอุปกรณ์ของลูกค้า

- การนำข้อมูลมาแสดงผล ส่งด้วย HTTPS

(รูปแบบการสื่อสารอย่างปลอดภัยบนอินเตอร์เน็ต)

- ข้อมูลเพิ่มเติม อยู่ส่วนของ GCP Security

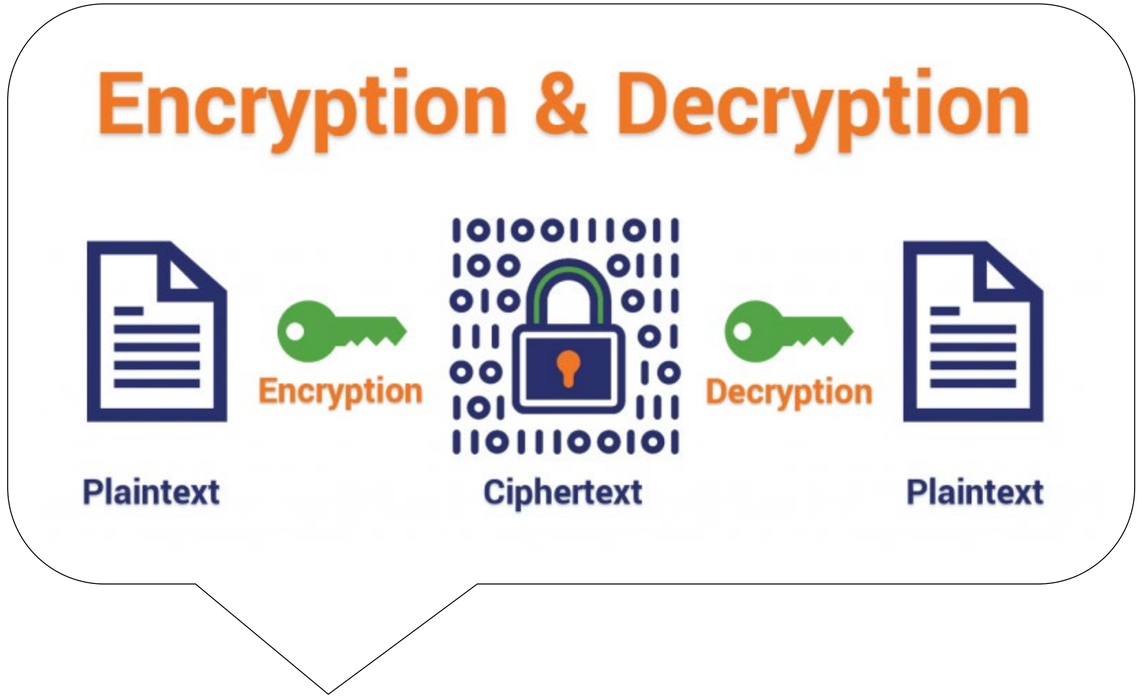
## ข้อมูลที่อยู่บน Cloud ปลอดภัยไหม?

- ข้อมูลที่ถูกเก็บเข้า Cloud ถูกเข้ารหัสด้วยวิธีการ 256-bit Advanced Encryption Standard ก่อนที่จะเก็บเข้าฮาร์ดดิสของ Google data center ซึ่งทำให้บุคคลที่ได้ข้อมูลไปอย่างไม่ถูกต้อง ไม่สามารถอ่านข้อมูลได้
- ข้อมูลเพิ่มเติม อยู่ส่วนของ GCP Security

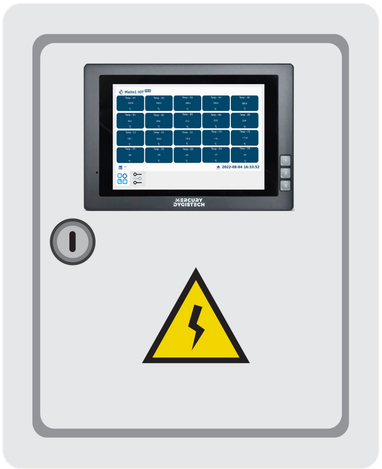
# How Do We Secure Your Production Data?

## Mercury ส่งข้อมูลไป Cloud ปลอดภัยไหม?

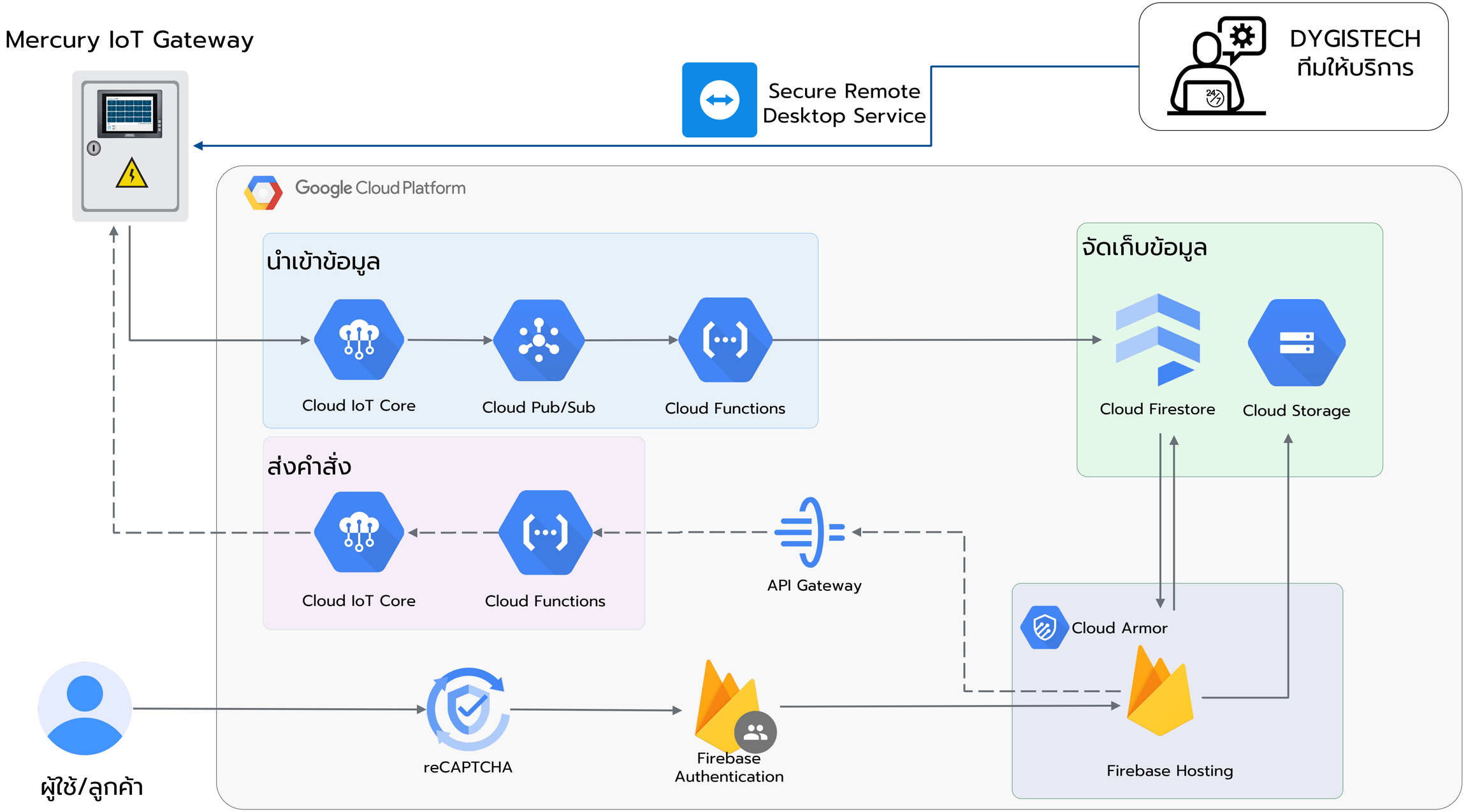
1. การส่งข้อมูลจาก Mercury อ้างอิง Standard IoT Core
2. Mercury แต่ละตัวจะมีรหัสผ่านเฉพาะตัว ซึ่งจะอยู่ในรูปแบบของ JSON Web Tokens (JWTs) ส่งผลให้ในกรณีที่ Mercury ถูกโจรกรรม แฮกเกอร์จะแฮกได้เพียงเครื่องเดียว ไม่สามารถแฮกทั้งระบบได้ และ JWTs มีอายุการใช้งานที่จำกัด ซึ่งจะต้องสร้าง JWTs ใหม่เมื่อหมดอายุการใช้งาน







# MALIN1 Platform System Architecture



# ภาพรวมความปลอดภัยของ Malin1 Platform

- ระบบ Malin1 Platform ของเราถูกออกแบบ มาโดยใช้เครื่องมือมาตรฐานของ GCP (Google Cloud Platform)
- ดังนั้นระบบความปลอดภัยมาตรฐานของ GCP จะถูกนำมาใช้เช่นเดียวันในระบบ Malin1 Platform เช่น มาตรฐานการเข้ารหัสข้อมูล เป็นต้น
- มาตรฐานความปลอดภัยของ GCP อยู่ในส่วนของ **ความปลอดภัยของ GCP**.
- ระบบของเรากำลังดำเนินการใช้คุณลักษณะด้านความปลอดภัยเพิ่มเติม ซึ่งให้บริการโดย GCP โดยมีรายละเอียดดังต่อไปนี้.

➢ **Google Cloud Armor:**

- ได้รับประโยชน์จากการป้องกัน DDoS (Distributed Denial of Service) และ WAF (Web Application Firewall) ในระดับ Google
- ตรวจจับและลดการโจมตีต่อภาระงาน Cloud Load Balancing
- กลไกที่ใช้ Adaptive Protection ML เพื่อช่วยตรวจจับและบล็อกการโจมตี Layer 7 DDoS
- ลดความเสี่ยง 10 อันดับแรกของ OWASP และช่วยปกป้องปริมาณงานในองค์กรหรือในระบบคลาวด์
- การจัดการบอทเพื่อหยุดการฉ้อโกงที่ปลายทางผ่านการผสานรวมแบบเนทีฟกับ reCAPTCHA Enterprise

➢ **reCAPTCHA Enterprise:**

- คุณสามารถปกป้องเว็บไซต์ของคุณจากการโจมตีทางเว็บทั่วไป เช่น การยัดข้อมูลรับรอง การครอบครองบัญชี และการขูดข้อมูล และช่วยป้องกันการแสวงหาผลประโยชน์ที่มีค่าใช้จ่ายสูงจากผู้ประสงค์ร้ายที่เป็นมนุษย์และผู้ที่ทำงานอัตโนมัติ

# ภาพรวมความปลอดภัยของ Malin1 Platform {ต่อ}

- **API Gateway:**
  - คุณสามารถสร้างระบบรักษาความปลอดภัย และตรวจสอบ API สำหรับแบ็กเอนด์แบบไร้เซิร์ฟเวอร์ของ Google Cloud รวมถึง Cloud Functions, Cloud Run และ App Engine API Gateway ที่สร้างขึ้นบน Envoy เพื่อเพิ่มประสิทธิภาพ ,ความสามารถในการปรับขนาดและอิสระยิ่งขึ้น
  - มีกลไกในตัวของ API Gateway รวมถึงการรับรองความถูกต้องและการตรวจสอบความถูกต้องของคีย์ ช่วยปกป้องบริการที่เผยแพร่ทางออนไลน์ มองเห็น API ของคุณผ่านบริการตรวจสอบ แจ้งเตือน บันทึก และติดตาม

- **Security Command Center:**
  - ช่วยให้สามารถมองเห็นและควบคุมจากส่วนกลาง
  - ช่วยให้สามารถค้นพบ การกำหนดค่าที่ผิดพลาดและช่องโหว่
  - รายงานและรักษาการปฏิบัติตาม
  - ตรวจจับภัยคุกคามที่กำหนดเป้าหมายเนื้อหา Google Cloud ของคุณ

# แผนงานด้านความปลอดภัยของระบบ Malin1 Platform

## ➢ ตรวจสอบและปรับปรุงมาตรฐานความปลอดภัย:

- ติดต่อผู้เชี่ยวชาญด้านความปลอดภัยบนคลาวด์ที่ผ่านการรับรองภายในประเทศ เพื่อรับรองแพลตฟอร์มของเราให้ตรงตามมาตรฐานความปลอดภัยที่ทั่วโลกล้วนยอมรับ เช่น ISO, OWASP

  OWASP Top Ten: เป็นเอกสารการรับรองมาตรฐานสำหรับนักพัฒนาและความปลอดภัยของเว็บแอปพลิเคชัน แสดงถึงความเห็นพ้องต้องกันในวงกว้างเกี่ยวกับ

  ความเสี่ยงด้านความปลอดภัยที่สำคัญที่สุดสำหรับเว็บแอปพลิเคชัน
- มุ่งเน้นที่จะพัฒนาแพลตฟอร์มและแอปพลิเคชันของเราให้ผ่านข้อกำหนด 10 อันดับแรกของ OWASP และได้รับใบรับรอง
- มีตรวจสอบมาตรฐานความปลอดภัยทุกๆ 1 ถึง 2 ปีต่อครั้ง
- ใช้เครื่องมือรักษาความปลอดภัย GCP ที่แนะนำเพิ่มเติมกับแพลตฟอร์มของเรา เพื่อปรับปรุงการรักษาความปลอดภัยให้ทันสมัย
- ตั้งทีมสนับสนุนและตอบสนองเหตุการณ์ผิดปกติ รวมถึงวางนโยบายการรับมือต่อเหตุการณ์ผิดปกติ
- ทำการตรวจสอบ Penetration Test.
- จัดทำ ISO/IEC 29110 Systems and Software Engineering Standards and Guides for Very Small Entities (VSEs).
- จัดทำ ISO/IEC 27001 is an information security standard created by the International Organization for Standardization (ISO), which provides a framework and guidelines for establishing, implementing and managing an information security management system (ISMS).

# ความปลอดภัยระหว่าง Mercury-ไปยัง-GCP (การรับรองความถูกต้อง)

แผนภาพสรุปการรับรองความถูกต้องใน Cloud IoT Core โดยใช้ MQTT:

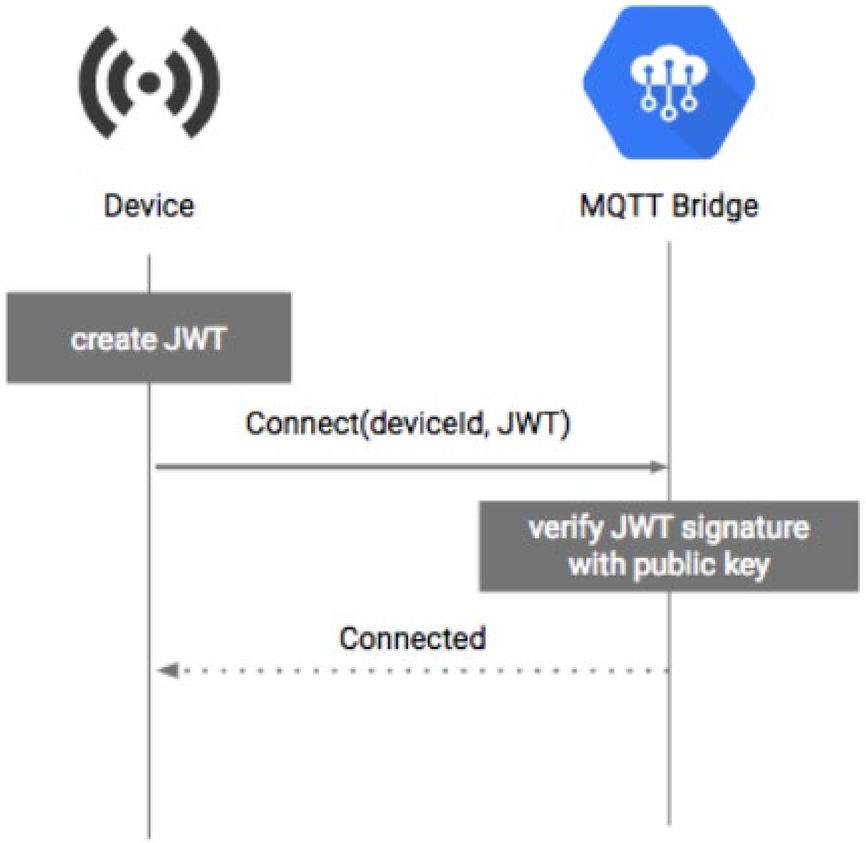
1. Mercury เตรียม JSON Web Token (JWT) ตามที่อธิบายไว้ใน การใช้ JSON Web Token JWT ลงนามด้วยคีย์ส่วนตัวจากขั้นตอนการตรวจสอบสิทธิ์.

2. เมื่อเชื่อมต่อกับ MQTT Bridge อุปกรณ์จะแสดง JWT เป็นรหัสผ่านในการ CONNECT

3. MQTT bridge ทำการตรวจสอบ JWT ด้วย public key ของ Mercury ตัวนั้นๆ ที่ได้ลงทะเบียนไว้กับระบบ

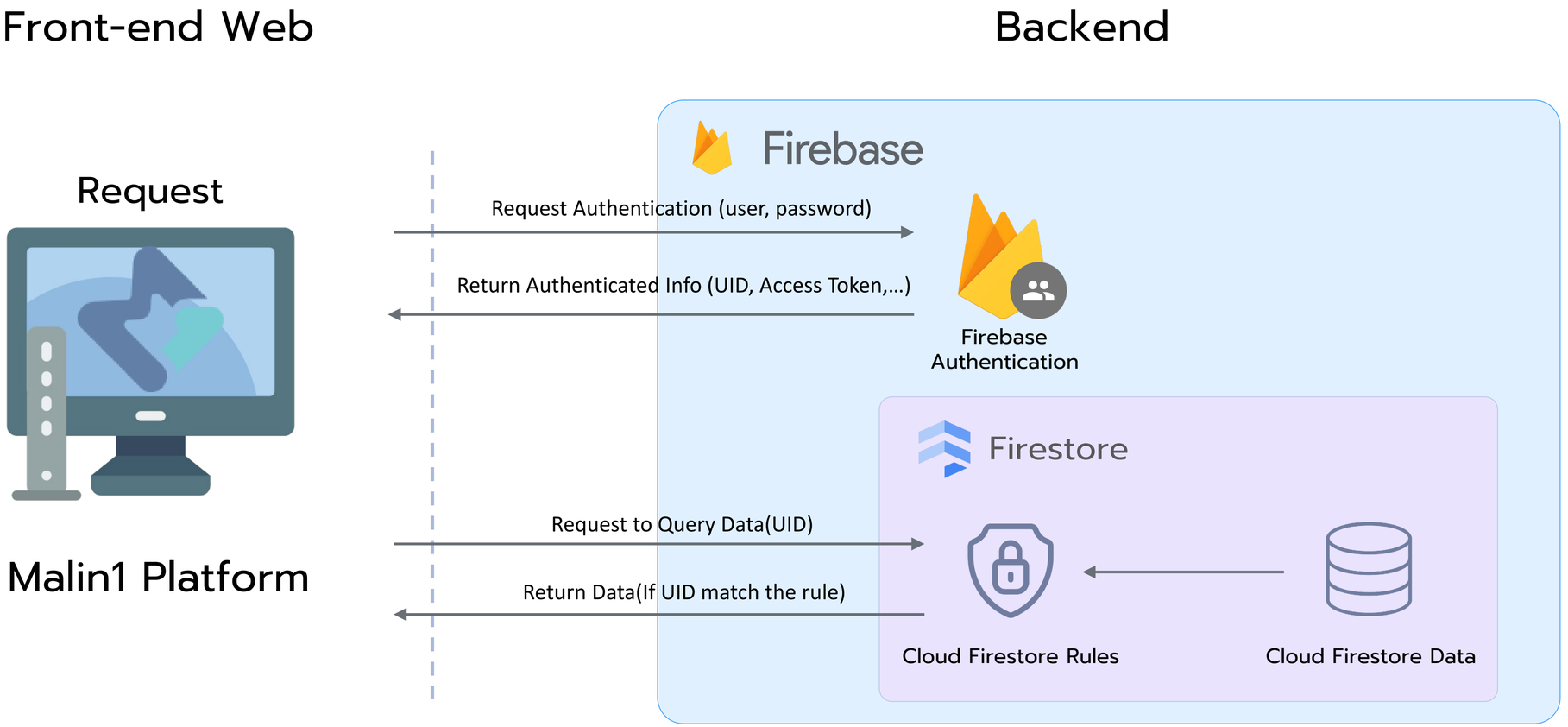
4. MQTT bridge ยอมรับการเชื่อมต่อจาก Mercury

5. MQTT bridge ตัดการเชื่อมต่อเมื่อ JWT นั้นหมดอายุ



# Malin1 Platform Authentication

- แผนผังขั้นตอนการรับรองความถูกต้อง



# Malin1 Platform แผนการดำเนินงาน ในการยืนยันตัวตนหลายปัจจัย

## Firebase MFA Method

•เรานำวิธีนี้มาใช้ในการยันยืนตัวตนหลายปัจจัย ในแพลตฟอร์ม Malin1

•การลงชื่อเข้าใช้ของผู้ใช้งาน จะดำเนินการโดยใช้การยืนยัน SMS แบบสองปัจจัย โดยมีรายละเอียดดังต่อไปนี้

**การลงชื่อเข้าใช้งานแบบการยืนยันแบบสองปัจจัย:**

•เมื่อลงชื่อผู้ใช้ด้วยปัจจัยแรกแล้ว, จากนั้นจะตรวจจับหาความผิดพลาดที่จำเป็นในการรับรองความถูกต้อง/การยืนยันแบบหลายปัจจัย. ข้อผิดพลาดนี้จะมาพร้อมตัวแก้ไข, คำใบ้ สู่การลงทะเบียนในปัจจัยที่สอง, และชุดฐานข้อมูลที่พิสูจน์ได้ว่าผู้ใช้งานผ่านการตรวจสอบสิทธิ์การยืนยันตัวตนในปัจจัยแรกสำเร็จแล้ว

•หากผู้ใช้งานละทะเบียนรูปแบบปัจจัยที่สองไว้หลากหลายรูปแบบ จะมีการถามผู้ใช้งานว่าจะเลือกตัวใด

•เริ่มการตรวจสอบ *reCAPTCHA Verifier* ตามที่ปรากฏในส่วนก่อนหน้านี้ ข้ามขั้นตอนนี้หากตัว *reCAPTCHA Verifier* ได้กำหนดไว้ล่วงหน้าแล้ว

•เริ่มการตรวจสอบ *PhoneInfoOptions* ด้วยหมายเลขมือถือของผู้ใช้งานและชุดขั้นตอนหลายปัจจัยเหล่านี้ จะมาพร้อมตัวแก้ไขความผิดพลาดที่จำเป็นในการรับรองความถูกต้อง/การยืนยันแบบหลายปัจจัย

•ส่งข้อความยืนยันไปยังโทรศัพท์ของผู้ใช้งาน

•หากคำขอล้มเหลว จะรีเซ็ต reCAPTCHA ใหม่ หลังจากนั้นจะกลับไปขั้นตอนก่อนหน้าซ้ำ เพื่อให้ผู้ใช้ลองอีกครั้ง

•เมื่อส่งรหัส SMS ไปแล้ว จะมีการถามผู้ใช้งานในการยืนยันรหัส

•เริ่มการตรวจสอบ *MultiFactorAssertion* ด้วย *PhoneAuthCredential*

•เรียกตัว *resolver.resolveSignIn()* เพื่อยืนยันความถูกต้องให้สมบูรณ์ จากนั้น คุณสามารถเข้าถึงผลลัพธ์การลงชื่อเข้าใช้ดั้งเดิมได้ ซึ่งรวมถึงข้อมูลโดยทั่วไปของผู้ให้บริการที่ระบุไว้ และข้อมูลรับรองการตรวจสอบสิทธิ์

# การยืนยันความถูกต้องของ Firebase

## การยืนยันความถูกต้องทำงานอย่างไร ?

- ขั้นแรก รับข้อมูลรับรองที่มีการยืนยันการตรวจสอบสิทธิ์จากผู้ใช้ก่อนเพื่อให้ผู้ใช้ลงชื่อเข้าใช้ในแอปของเรา:
  - ข้อมูลรับรองสามารถใช้เป็นอีเมลแอดเดรสและรหัสผ่านของผู้ใช้งานได้
  - ข้อมูลรับรองสามารถใช้เป็น OAuth token จากผู้ให้บริการส่วนตัวได้

- จากนั้นส่งข้อมูลรับรองเหล่านี้ไปยัง Firebase Authentication SDK. บริการของแบคเอนด์จะนำข้อมูลเหล่านั้นมาตรวจสอบ และส่งกลับมายังไคลเอ็นท์

- หลังจากเข้าสู่ระบบเสร็จสิ้นแล้ว
  - เราสามารถเข้าถึงแหล่งข้อมูลที่จัดเก็บไว้ในผลิตภัณฑ์ Firebase อื่นๆ ของผู้ใช้
  - เราสามารถเข้าถึงข้อมูลโดยทั่วไปในโปรไฟล์ของผู้ใช้ได้
  - เราสามารถใช้โทเคนที่มีการตรวจสอบสิทธิ์แล้ว เพื่อยืนยันตัวตนของผู้ใช้ในบริการแบคเอนด์ของเราเอง

- ผู้ใช้ที่ผ่านการรับรองความถูกต้องแล้ว สามารถอ่านและเขียนข้อมูลไปยัง Firebase Real-time Database และ Cloud Storage
  - เราสามารถควบคุมการเข้าถึงของผู้ใช้ที่ผ่านการรับรองความถูกต้องแล้วได้ โดยการปรับปรุงแก้ไข **Firebase Database Rules** and ***Storage Security Rules***.

# การยืนยันความถูกต้องของ Firebase

## วงจรชีวิตของผู้ใช้งาน

ผู้รับการยืนยันความถูกต้องจะได้รับแจ้งเตือน ดังสถานการณ์ต่อไปนี้

•เมื่อส่วนของออบเจ็คในการยืนยันจะเสร็จสิ้นในขั้นตอนแรก, และผู้ใช้ได้ลงชื่อเข้าสู่ระบบในขั้นก่อนหน้าเรียบร้อยแล้ว หรือถูกเปลี่ยนเส้นทางจากผู้ให้บริการในการลงชื่อเข้าใช้โดยเฉพาะ

•เมื่อผู้ใช้งานลงชื่อเข้าใช้ระบบ

•เมื่อผู้ใช้งานลงชื่อออกจากระบบ

•เมื่อการเข้าถึงโทเคนของผู้ที่ใช้งานอยู่นั้นถูกรีเฟรชใหม่:

- การเข้าถึงโทเคนหมดอายุ
- ผู้ใช้งานทำการเปลี่ยนรหัสผ่าน
- ผู้ใช้งานยืนยันตัวตนใหม่อีกครั้ง

# ความปลอดภัยระหว่าง Mercury-ไปยัง-GCP (มาตรฐานความปลอดภัย)

Cloud IoT Core ใช้การตรวจสอบสิทธิด้วยลายเซ็นดิจิทัล สนับสนุนทั้งโทเคนที่ลงชื่อด้วย RSA และ Elliptic Curve โดยรองรับอัลกอริทึมเฉพาะต่อไปนี้:

- **JWT RS256 (RSASSA-PKCS1-v1_5 using SHA-256 RFC 7518 sec 3.3) Dygistech เราใช้อัลกอริทึมนี้**
- JWT ES256 (ECDSA using P-256 and SHA-256 RFC 7518 sec 3.4), defined in OpenSSL as the prime256v1 curve

- อัลกอริทึม RSA เป็นที่นิยมใช้และได้รับการสนับสนุนอย่างกว้างขวางจากไลบรารีทั่วไป อย่างไรก็ตาม คีย์และลายเซ็นที่สร้างขึ้นอาจมีขนาดค่อนข้างใหญ่ (โดยทั่วไปจะเรียงตามลำดับตั้งแต่หนึ่งถึงสองกิโลไบต์) นอกจากนี้ RSA ยังสามารถใช้ทรัพยากรจำนวนมาก (ทั้งในแง่ของความยาวของคีย์และ CPU) ซึ่งอาจส่งผลต่ออุปกรณ์ที่มีทรัพยากรจำกัด.

- อัลกอริทึม Elliptic Curve ได้รับการสนับสนุนอย่างดี แต่ไม่ได้ใช้กันอย่างแพร่หลายเท่า RSA หากต้องการใช้ Elliptic Curve หาไลบรารีค่อนข้างยา อย่างไรก็ตาม คีย์และลายเซ็นที่สร้างขึ้นนั้นมีขนาดเล็กกว่าที่สร้างโดย RSA อย่างมาก ซึ่งมีประโยชน์สำหรับอุปกรณ์ที่มีทรัพยากรจำกัด

# ความปลอดภัยของ GCP (การเข้ารหัสข้อมูลที่จัดเก็บไว้)

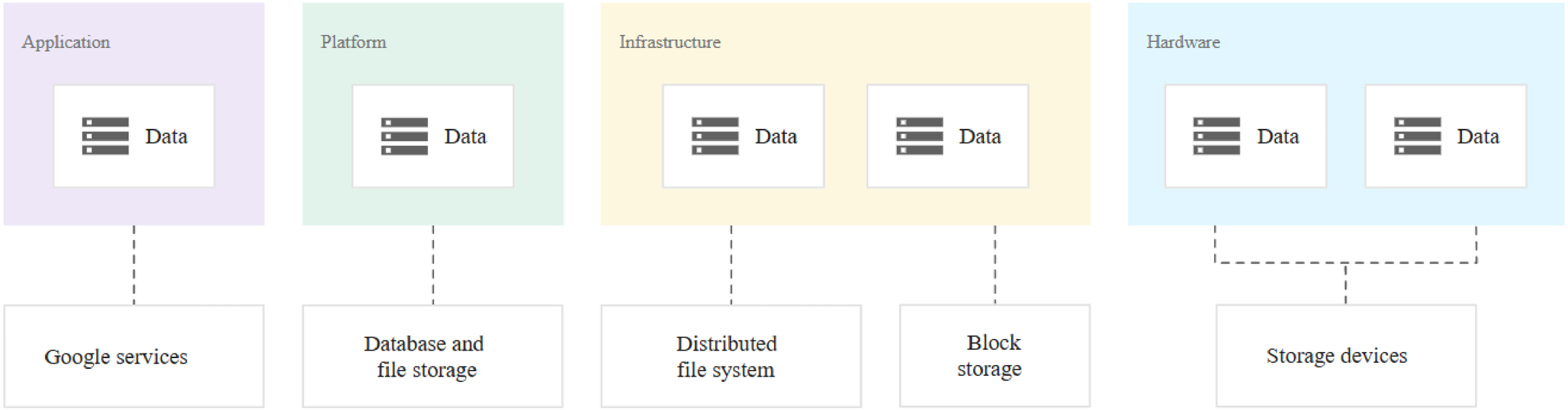
เพื่อปกป้องกันข้อมูลของลูกค้าจากผู้โจมตี  GCP เข้ารหัสเนื้อหาของลูกค้า Google ทั้งหมดที่ไม่มีการเคลื่อนไหว โดยที่คุณไม่ต้องดำเนินการใดๆ โดยใช้กลไกการเข้ารหัสอย่างน้อยหนึ่งอย่าง:

- **Encryption at rest** เป็นการเข้ารหัสที่ใช้เพื่อช่วยปกป้องข้อมูลที่จัดเก็บไว้ในดิสก์ (รวมถึงไดรฟ์โซลิดสเทต) หรือสื่อสำรองข้อมูล ข้อมูลทั้งหมดที่จัดเก็บโดย Google จะถูกเข้ารหัสที่เลเยอร์การจัดเก็บโดยใช้อัลกอริทึมมาตรฐานการเข้ารหัสขั้นสูง (AES) หรือ AES-256 เราใช้ไลบรารีการเข้ารหัสทั่วไป Tink ซึ่งรวมถึงโมดูลที่ผ่านการตรวจสอบ FIPS 140-2 ของเรา (ชื่อ BoringCrypto) เพื่อใช้การเข้ารหัสอย่างสม่ำเสมอทั่วทั้ง Google Cloud.

- **Encryption at rest ช่วยปกป้องข้อมูลอย่างไร**: ช่วยให้มั่นใจได้ว่าหากข้อมูลตกไปอยู่ในมือของผู้โจมตี ผู้โจมตีจะไม่สามารถอ่านข้อมูลได้หากไม่มีการเข้าถึงคีย์การเข้ารหัส แม้ว่าผู้โจมตีจะได้รับอุปกรณ์เก็บข้อมูลที่มีข้อมูลลูกค้า แต่ก็ไม่สามารถเข้าใจหรือถอดรหัสได้.

# ความปลอดภัยของ GCP (การเข้ารหัสข้อมูลที่จัดเก็บไว้) {ต่อ}

- **Layers of encryption:** แผนภาพต่อไปนี้แสดงการเข้ารหัสหลายชั้นที่ใช้โดยทั่วไปเพื่อปกป้องข้อมูลผู้ใช้ในศูนย์ข้อมูลการผลิตของ Google

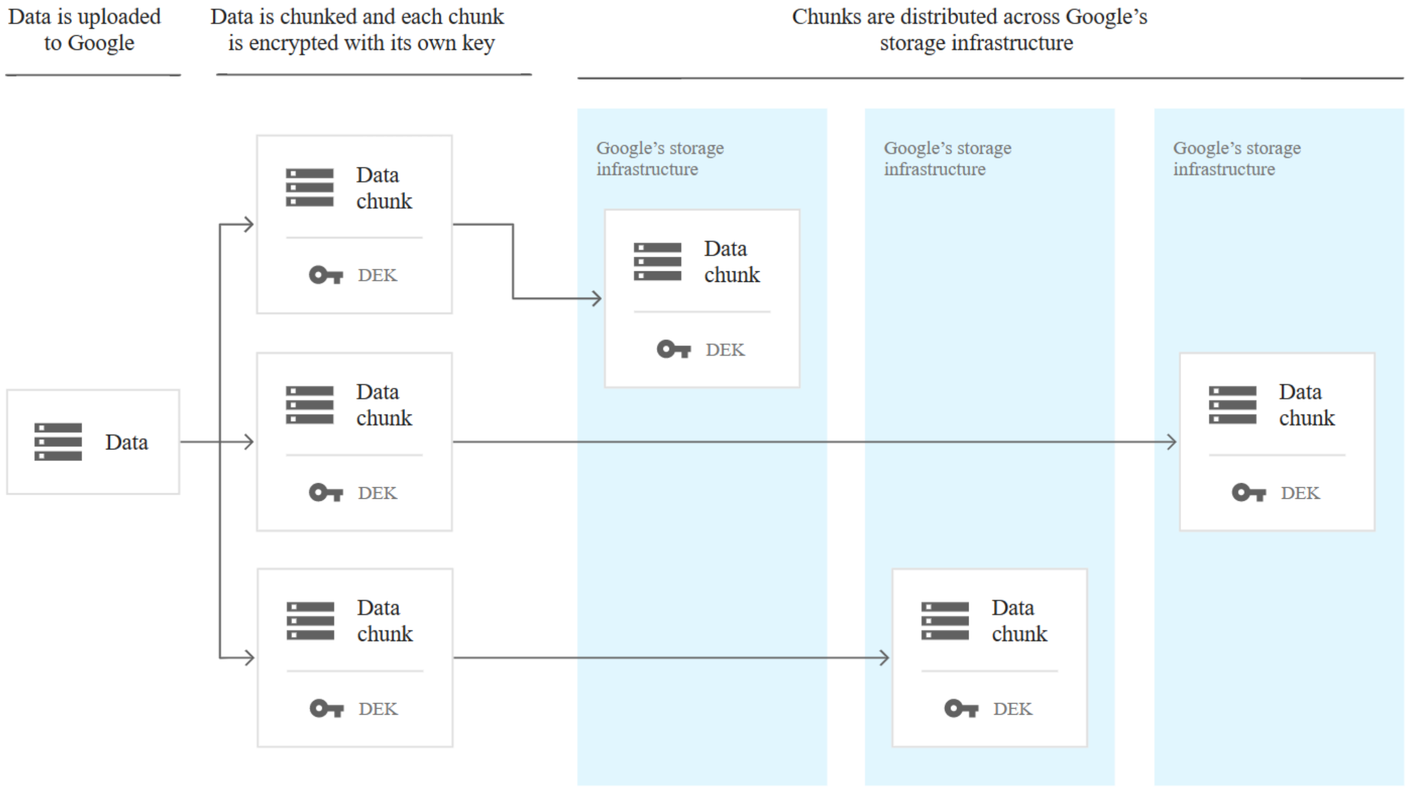


# ความปลอดภัยของ GCP (การเข้ารหัสข้อมูลที่จัดเก็บไว้) {ต่อ}

- **การเข้ารหัสที่ชั้นฮาร์ดแวร์และโครงสร้างพื้นฐาน** : ระบบจัดเก็บข้อมูลทั้งหมดของ Google ใช้สถาปัตยกรรมการเข้ารหัสที่คล้ายคลึงกัน แม้ว่ารายละเอียดการใช้งานจะแตกต่างกันไปในแต่ละระบบ ข้อมูลถูกแบ่งออกเป็นไฟล์ย่อยสำหรับการจัดเก็บ แต่ละ chunk อาจมีขนาดได้ถึงหลายกิกะไบต์ แต่ละ chunk ถูกเข้ารหัสที่ระดับพื้นที่จัดเก็บด้วยคีย์การเข้ารหัส ข้อมูลแต่ละ chunk (DEK): สองอันจะไม่มี DEK เหมือนกัน แม้ว่าจะเป็นของลูกค้าคนเดียวกันหรือจัดเก็บไว้ในเครื่องเดียวกันก็ตาม (กลุ่มข้อมูลใน Datastore, App Engine และ Pub/Sub อาจประกอบด้วยข้อมูลของลูกค้าหลายราย
- หากมีการอัปเดตข้อมูลบางส่วน ข้อมูลนั้นจะถูกเข้ารหัสด้วยคีย์ใหม่ แทนที่จะใช้คีย์ที่มีอยู่ซ้ำ การแบ่งพาร์ติชันข้อมูลแต่ละส่วนโดยใช้คีย์ที่แตกต่างกันจะจำกัดความเสี่ยงที่คีย์เข้ารหัสข้อมูลอาจถูกบุกรุกเฉพาะกลุ่มข้อมูลนั้นGoogle เข้ารหัสข้อมูลก่อนที่จะเขียนลงในระบบจัดเก็บฐานข้อมูลหรือดิสก์ฮาร์ดแวร์ การเข้ารหัสมีอยู่ในระบบจัดเก็บข้อมูลทั้งหมดของเรา แทนที่จะเพิ่มเข้ามาในภายหลัง
- แต่ละก้อนข้อมูลมีตัวระบุที่ไม่ซ้ำกัน รายการควบคุมการเข้าถึง (ACL) ช่วยให้แน่ใจว่าแต่ละอันสามารถถอดรหัสได้โดยบริการของ Google ที่ทำงานด้วยบทบาทที่ได้รับอนุญาตเท่านั้น ซึ่งจะได้รับสิทธิ์การเข้าถึง ณ เวลานั้นเท่านั้น การจำกัดการเข้าถึงนี้ช่วยป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เพิ่มความปลอดภัยและความเป็นส่วนตัวของข้อมูล
- แต่ละ chunk ถูกแจกจ่ายในระบบจัดเก็บข้อมูลของเราและจำลองแบบในรูปแบบเข้ารหัสสำหรับการสำรองข้อมูลและการกู้คืนจากภัยพิบัติ

# ความปลอดภัยของ GCP (การเข้ารหัสข้อมูลที่จัดเก็บไว้) {ต่อ}

- ไดอะแกรมต่อไปนี้แสดงวิธีการอัปโหลดข้อมูลไปยังโครงสร้างพื้นฐานของ GCP จากนั้นจึงแบ่งออกเป็นส่วนๆ ที่เข้ารหัสเพื่อจัดเก็บ :




- All data at the storage level is encrypted by DEKs, which use AES-256 by default.

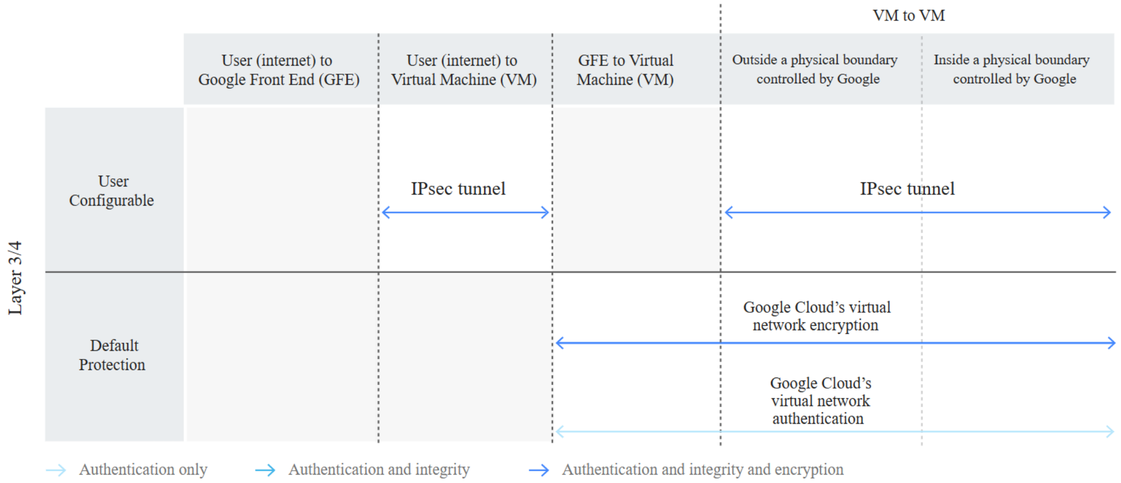
# ความปลอดภัยของ GCP (การเข้ารหัสข้อมูลในระหว่างการส่งผ่านข้อมูล)

- **Encryption in transit:** ปกป้องข้อมูลของคุณหากการสื่อสารถูกดักฟังในขณะที่ข้อมูลเคลื่อนย้ายระหว่างไซต์ของคุณกับผู้ให้บริการระบบคลาวด์หรือระหว่างสองบริการ การป้องกันนี้ทำได้โดยการเข้ารหัสข้อมูลก่อนส่ง รับรองความถูกต้องของปลายทาง และเมื่อมาถึง ถอดรหัสและตรวจสอบว่าข้อมูลไม่ได้ถูกแก้ไข ตัวอย่างเช่น มักใช้ Transport Layer Security (TLS) เพื่อเข้ารหัสข้อมูลระหว่างการส่งเพื่อความปลอดภัยในการขนส่ง และ Secure/Multipurpose Internet Mail Extensions (S/MIME) มักใช้สำหรับการเข้ารหัสข้อความอีเมล
- ปกป้องข้อมูลของคุณหลังจากสร้างการเชื่อมต่อและรับรองความถูกต้องจากผู้โจมตี:

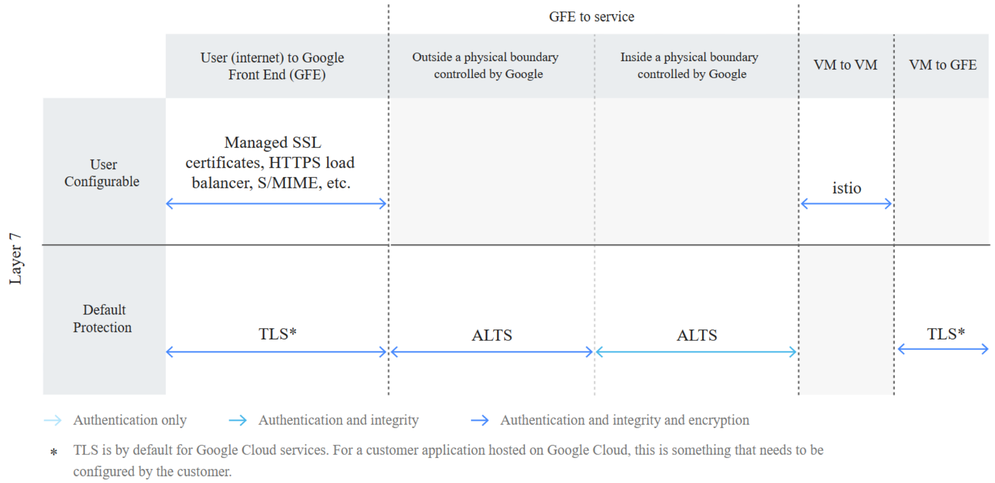
  - ขจัดความจำเป็นในการ trust เลเยอร์ล่างของเครือข่าย ซึ่งให้บริการโดย third parties ทั่วไป
  - ลดพื้นที่เสี่ยงต่อการโจมตีที่อาจเกิดขึ้น
  - ป้องกันไม่ให้ผู้โจมตีเข้าถึงข้อมูลหากมีการดักฟังการสื่อสาร

# ความปลอดภัยของ GCP (การเข้ารหัสข้อมูลในระหว่างการส่งผ่านข้อมูล){ต่อ}

- **Encryption in Transit by Default:** Google ใช้วิธีการเข้ารหัสหลายวิธี ทั้งค่าเริ่มต้นและผู้ใช้กำหนดค่าได้ สำหรับข้อมูลที่อยู่ระหว่างการส่ง ประเภทของการเข้ารหัสที่ใช้ขึ้นอยู่กับเลเยอร์ OSI ประเภทของบริการ และส่วนประกอบทางกายภาพของโครงสร้างพื้นฐาน รูปภาพด้านล่างแสดงการป้องกันทางเลือกและการป้องกันเริ่มต้นของ Google Cloud สำหรับเลเยอร์ 3, 4 และ 7




*การป้องกันตามค่าเริ่มต้นและตัวเลือกที่เลเยอร์ 3 และ 4 ทั่วทั้ง Google Cloud*




*การป้องกันตามค่าเริ่มต้นและตัวเลือกที่เลเยอร์ 7 ทั่วทั้ง Google Cloud*

# ความปลอดภัยของ GCP (การเข้ารหัสข้อมูลในระหว่างการส่งผ่านข้อมูล){ต่อ}

- **ผู้ใช้ในการเข้ารหัสส่วนFront End ของ Google :** HTTPS ให้ความปลอดภัยโดยใช้การเชื่อมต่อ TLS ซึ่งรับประกันความถูกต้อง ความสมบูรณ์ และความเป็นส่วนตัวของคำขอและการตอบกลับ ในการรับคำขอ HTTPS ผู้รับต้องการคู่คีย์สาธารณะและส่วนตัวและใบรับรอง X.509 สำหรับการตรวจสอบความถูกต้องของเซิร์ฟเวอร์จากผู้ออกใบรับรอง (CA) คู่คีย์และใบรับรองช่วยปกป้องคำขอของผู้ใช้ที่เลเยอร์แอปพลิเคชัน (เลเยอร์ 7) โดยพิสูจน์ว่าผู้รับเป็นเจ้าของชื่อโดเมนที่ต้องการร้องขอ ส่วนย่อยต่อไปนี้กล่าวถึงส่วนประกอบของผู้ใช้ในการเข้ารหัส GFE ได้แก่ TLS, BoringSSL และผู้ออกใบรับรองของ Google จำได้ว่าไม่ใช่เส้นทางของลูกค้าทั้งหมดที่จะผ่าน GFE; โดยเฉพาะอย่างยิ่ง GFE ใช้สำหรับการรับส่งข้อมูลจากผู้ใช้ไปยังบริการ Google Cloud และจากผู้ใช้ไปยังแอปพลิเคชันของลูกค้าที่โฮสต์บน Google Cloud ที่ใช้ Google Cloud Load Balancing

- **Transport Layer Security (TLS) :** เมื่อผู้ใช้ส่งคำขอไปยังบริการ Google Cloud เราจะรักษาความปลอดภัยของข้อมูลระหว่างการส่ง ให้การพิสูจน์ตัวตน ความสมบูรณ์ และการเข้ารหัส โดยใช้ HTTPS พร้อมใบรับรองจากผู้ออกใบรับรองบนเว็บ (สาธารณะ) ข้อมูลใดๆ ที่ผู้ใช้ส่งไปยัง GFE จะได้รับการเข้ารหัสระหว่างการขนส่งด้วย Transport Layer Security (TLS) หรือ QUIC GFEพิจารณาเลือกโปรโตคอลการเข้ารหัสเฉพาะกับไคลเอ็นต์โดยขึ้นอยู่กับว่าไคลเอ็นต์สามารถรองรับอะไรได้บ้าง GFE เลือกโปรโตคอลการเข้ารหัสที่ทันสมัยกว่านี้เมื่อเป็นไปได้

# ความปลอดภัยของ GCP (ความปลอดภัยของการรับส่งข้อมูลในชั้น Application)

- **Application-Level Security and ALTS :** แอปพลิเคชันจำนวนมาก ตั้งแต่เว็บเบราว์เซอร์ไปจนถึง VPN อาศัยโปรโตคอลการสื่อสารที่ปลอดภัย เช่น TLS (Transport Layer Security) และ IPSec เพื่อปกป้องข้อมูลระหว่างการขนส่ง3 ที่ Google เราใช้ ALTS ซึ่งเป็นระบบการตรวจสอบความถูกต้องร่วมกันและการเข้ารหัสการขนส่งที่ทำงานที่ชั้นแอปพลิเคชัน เพื่อปกป้องการสื่อสารของ RPC การใช้การรักษาความปลอดภัยระดับแอปพลิเคชันทำให้แอปพลิเคชันสามารถ remote peer identity ได้ ซึ่งสามารถใช้เพื่อปรับใช้นโยบายการให้สิทธิ์แบบละเอียด

# ความปลอดภัยของ GCP (การจัดเก็บและสำเนาข้อมูล)

- Google Cloud ได้รับการออกแบบมาเพื่อให้มี low latency พร้อมใช้งานสูง ปรับขนาดได้ และโซลูชันที่ทนทาน การสำเนาข้อมูลมีความสำคัญต่อการบรรลุเป้าหมายด้านประสิทธิภาพที่สำคัญเหล่านี้ สำเนาข้อมูลลูกค้าที่ซ้ำซ้อนสามารถจัดเก็บได้ทั้งใน local และระดับภูมิภาค และแม้แต่ทั่วโลก ทั้งนี้ขึ้นอยู่กับการกำหนดค่าของคุณและความต้องการของโครงการของลูกค้า

- การดำเนินการกับข้อมูลใน Google Cloud อาจทำซ้ำพร้อมกันในศูนย์ข้อมูลหลายแห่ง เพื่อให้ข้อมูลลูกค้ามีความพร้อมใช้งานสูง เมื่อการเปลี่ยนแปลงที่ส่งผลกระทบต่อประสิทธิภาพเกิดขึ้นในสภาพแวดล้อมของฮาร์ดแวร์ ซอฟต์แวร์ หรือเครือข่าย ข้อมูลลูกค้าจะถูกย้ายจากระบบหรือสิ่งอำนวยความสะดวกหนึ่งไปยังอีกระบบหนึ่งโดยอัตโนมัติ ทั้งนี้ขึ้นอยู่กับการตั้งค่าการกำหนดค่าของลูกค้า เพื่อให้โครงการของลูกค้าดำเนินการตามขนาดอย่างต่อเนื่องและไม่หยุดชะงัก

- ที่ระดับการจัดเก็บจริง ข้อมูลลูกค้าจะถูกจัดเก็บไว้เฉยๆ ในระบบสองประเภท: ระบบจัดเก็บข้อมูลที่ใช้งานอยู่และระบบจัดเก็บข้อมูลสำรอง
  - **Active storage systems** เป็นอาร์เรย์จำนวนมากของดิสก์และไดรฟ์ที่ใช้ในการเขียนข้อมูลใหม่ ตลอดจนจัดเก็บและดึงข้อมูลในสำเนาที่ทำซ้ำหลายชุด ระบบจัดเก็บข้อมูลที่ใช้งานได้รับการปรับให้เหมาะสมเพื่อดำเนินการอ่าน / เขียนแบบสดบนข้อมูลลูกค้าด้วยความเร็วและขนาด.
  - **Google’s backup storage systems** จัดเก็บสำเนาของระบบที่ใช้งานอยู่ของ Google แบบเต็มและที่เพิ่มขึ้นตามระยะเวลาที่กำหนด เพื่อช่วย Google กู้คืนข้อมูลและระบบในกรณีที่เกิดไฟดับหรือภัยพิบัติร้ายแรง ระบบสำรองข้อมูลได้รับการออกแบบมาให้รับสแนปชอตเป็นระยะๆ ของระบบ Google ซึ่งแตกต่างจากระบบที่ใช้งานอยู่ และสำเนาข้อมูลสำรองจะถูกยกเลิกหลังจากช่วงเวลาที่จำกัดเมื่อมีการสร้างสำเนาข้อมูลสำรองใหม่

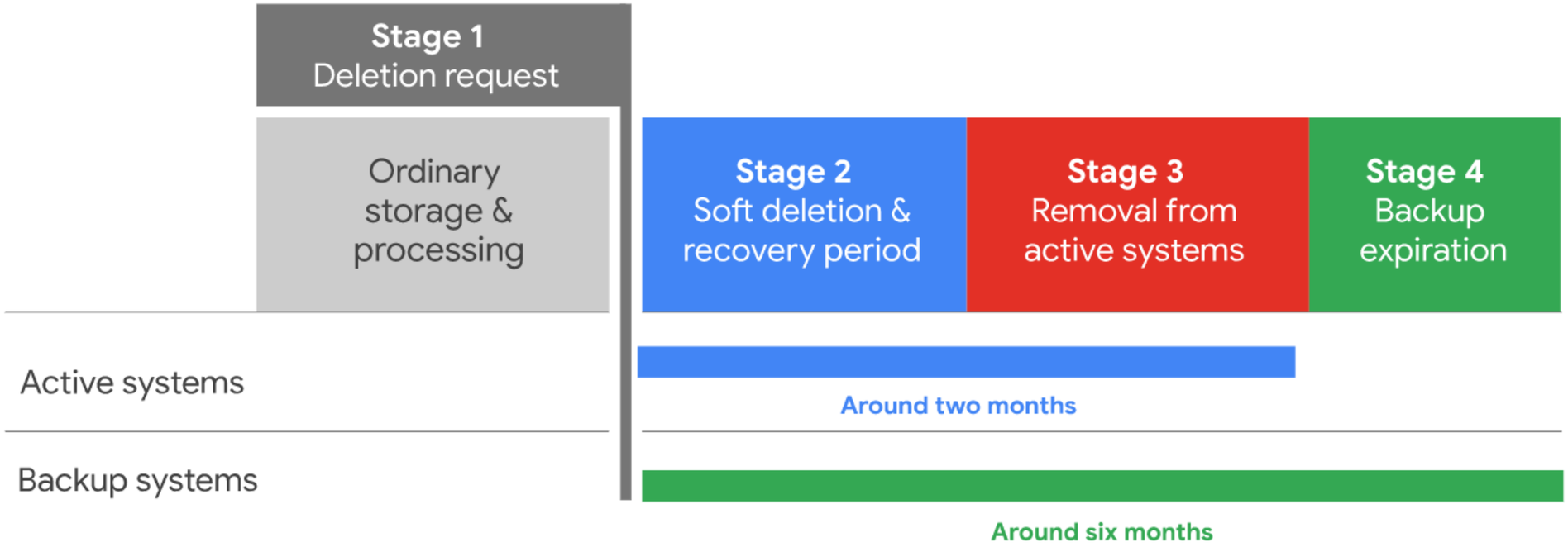
# ความปลอดภัยของ GCP (การลบข้อมูลบน Google Cloud)

ภาพรวมของกระบวนการที่ปลอดภัยซึ่งเกิดขึ้นเมื่อคุณลบข้อมูลลูกค้าที่จัดเก็บไว้ใน Google Cloud การดูแลให้มีการลบข้อมูลลูกค้าอย่างปลอดภัยเมื่อสิ้นสุดวงจรชีวิตเป็นลักษณะพื้นฐานของการทำงานกับข้อมูลบนแพลตฟอร์มคอมพิวเตอร์ใดๆ

- **Data Deletion Pipeline:**
  - **Stage 1 - Deletion request:** การลบข้อมูลลูกค้าเริ่มต้นเมื่อลูกค้าเริ่มคำขอลบ
    - **Resource Deletion:** สามารถลบได้หลายวิธีจาก Cloud Console หรือผ่าน API
    - **Project Deletion:** การลบ Project จะทำหน้าที่เป็นคำขอลบจำนวนมากสำหรับทรัพยากรทั้งหมดที่เชื่อมโยงกับหมายเลข Project ที่เกี่ยวข้อง
    - **Account Deletion:** เมื่อคุณลบบัญชี Google จะเป็นการลบ Project Google Cloud ทั้งหมดที่คุณเป็นเจ้าของแต่เพียงผู้เดียว.
  - **Stage 2 - Soft Deletion:** การลบอย่างนุ่มนวลเป็นจุดตามธรรมชาติของกระบวนการเพื่อให้มีระยะเวลาชั่วคราวภายในและระยะเวลากู้คืนสั้น ๆ เพื่อให้แน่ใจว่ามีเวลากู้คืนข้อมูลใด ๆ ที่ถูกทำเครื่องหมายให้ลบโดยอุบัติเหตุหรือข้อผิดพลาด เมื่อบัญชี Google ถูกปิด Google Cloud อาจกำหนดระยะเวลาการกู้คืนภายในสูงสุด 30 วัน ขึ้นอยู่กับกิจกรรมในบัญชีที่ผ่านมา.
  - **Stage 3 - Logical Deletion from Active Systems :** หลังจากที่ข้อมูลถูกทำเครื่องหมายให้ลบและระยะเวลากู้คืนใดๆ หมดลง ข้อมูลจะถูกลบออกจากระบบพื้นที่เก็บข้อมูลที่ใช้งานอยู่และสำรองของ Google ตามลำดับ ในระบบที่ใช้งานอยู่ ข้อมูลจะถูกลบในสองวิธี.
    - ในผลิตภัณฑ์ระบบคลาวด์ทั้งหมดภายใต้ Compute, Storage & Databases และ Big Data ยกเว้น Google Cloud Storage สำเนาของข้อมูลที่ถูกลบจะถูกทำเครื่องหมายเป็นที่เก็บข้อมูลที่มีอยู่และเขียนทับเมื่อเวลาผ่านไป
    - ใน Google Cloud Storage ข้อมูลลูกค้าจะถูกลบผ่านการลบด้วยการเข้ารหัส

# ความปลอดภัยของ GCP (การลบข้อมูลบน Google Cloud) {ต่อ}

- **Data Deletion Pipeline:**
  - **Stage 4 - Expiration from Backup Systems:** เช่นเดียวกับการลบออกจากระบบที่ใช้งานอยู่ของ Google ข้อมูลที่ถูกลบจะถูกลบออกจากระบบสำรองโดยใช้ทั้งการเขียนทับและเทคนิคการเข้ารหัส เมื่อเลิกใช้การสำรองข้อมูล ระบบจะทำเครื่องหมายเป็นพื้นที่ว่างและเขียนทับเมื่อมีการสำรองข้อมูลรายวัน / รายสัปดาห์ / รายเดือนใหม่



# ความปลอดภัยของ GCP (การลบข้อมูลบน Google Cloud) {ต่อ}

- **Deletion Timeline:** Google Cloud จะลบข้อมูลลูกค้าภายในระยะเวลาสูงสุดประมาณหกเดือน (180 วัน).
  - **Stage 2** - เมื่อส่งคำขอให้ลบแล้ว โดยทั่วไปข้อมูลจะถูกทำเครื่องหมายให้ลบทันที และเป้าหมายของเราคือดำเนินการตามขั้นตอนนี้ภายในระยะเวลาสูงสุด 24 ชั่วโมง หลังจากข้อมูลถูกทำเครื่องหมายเพื่อลบ อาจใช้ระยะเวลาการกู้คืนภายในสูงสุด 30 วัน ขึ้นอยู่กับบริการหรือคำขอลบ

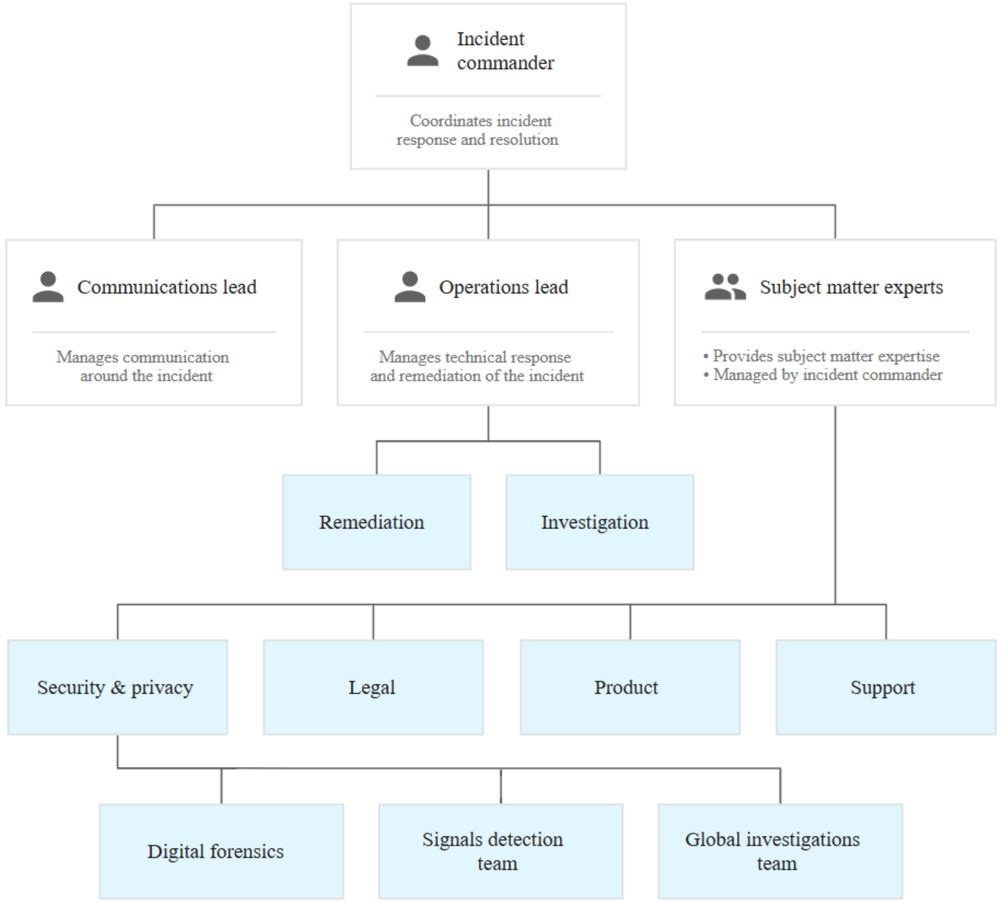
  - **Stage 3** - เวลาที่ต้องใช้ในการดำเนินการรวบรวมขยะและทำการลบแบบลอจิคัลออกจากระบบที่ใช้งานอยู่ กระบวนการเหล่านี้อาจเกิดขึ้นทันทีหลังจากได้รับคำขอให้ลบ ทั้งนี้ขึ้นอยู่กับระดับของการจำลองข้อมูลและระยะเวลาของรอบการรวบรวมขยะที่กำลังดำเนินอยู่จากคำขอลบ โดยทั่วไปจะใช้เวลาประมาณสองเดือนในการลบข้อมูลจากระบบที่ใช้งานอยู่ ซึ่งโดยปกติแล้วจะใช้เวลาเพียงพอในการทำให้รอบการรวบรวมขยะหลักสองรอบเสร็จสมบูรณ์ และตรวจสอบให้แน่ใจว่าการลบเชิงตรรกะเสร็จสมบูรณ์

  - **Stage 4** - รอบการสำรองข้อมูลของ Google ได้รับการออกแบบมาให้ข้อมูลที่ถูกลบภายในข้อมูลสำรองของศูนย์ข้อมูลหมดอายุภายในหกเดือนของคำขอลบ การลบอาจเกิดขึ้นเร็วกว่านั้นขึ้นอยู่กับระดับของการจำลองข้อมูลและระยะเวลาของรอบการสำรองข้อมูลอย่างต่อเนื่องของ Google

# ความปลอดภัยของ GCP (กระบวนการตอบสนองเหตุการณ์ผิดปกติข้อมูล)

ภาคผนวกการประมวลผลข้อมูลบนคลาวด์กำหนดเหตุการณ์ข้อมูลว่าเป็น "การละเมิดความปลอดภัยของ Google ที่นำไปสู่การทำลายโดยไม่ตั้งใจ หรือไม่ชอบด้วยกฎหมาย การสูญหาย การเปลี่ยนแปลง การเปิดเผยโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลลูกค้าในระบบที่จัดการโดยหรือควบคุมโดย Google"

- **Data incident response:** โปรแกรมตอบสนองเหตุการณ์ของ Google ได้รับการจัดการโดยทีมผู้เชี่ยวชาญในการเผชิญเหตุในหน้าที่เฉพาะต่างๆ เพื่อให้แน่ใจว่าการตอบสนองแต่ละครั้งได้รับการปรับให้เหมาะกับความท้าทายที่นำเสนอโดยเหตุการณ์แต่ละเหตุการณ์ ทีมเผชิญเหตุมืออาชีพสามารถรวมผู้เชี่ยวชาญจากทีมต่อไปนี้ได้ ทั้งนี้ขึ้นอยู่กับลักษณะของเหตุการณ์ :
    - การจัดการเหตุการณ์บนคลาวด์
    - วิศวกรรมผลิตภัณฑ์
    - วิศวกรรมความน่าเชื่อถือของไซต์
    - ความปลอดภัยและความเป็นส่วนตัวบนคลาวด์
    - นิติดิจิทัล
    - การสืบสวนทั่วโลก
    - การตรวจจับสัญญาณ
    - คำแนะนำด้านความปลอดภัย ความเป็นส่วนตัว และผลิตภัณฑ์
    - ความไว้วางใจและความปลอดภัย
    - เทคโนโลยีต่อต้านการละเมิด
    - ฝ่ายดูแลลูกค้าระบบคลาวด์



# ความปลอดภัยของ GCP (กระบวนการตอบสนองเหตุการณ์ผิดปกติข้อมูล){ต่อ}

- **Data incident response process:** ทุกเหตุการณ์ของข้อมูลมีเอกลักษณ์เฉพาะตัว และเป้าหมายของกระบวนการตอบสนองเหตุการณ์ข้อมูลคือการปกป้องข้อมูลลูกค้า คืนค่าบริการปกติให้เร็วที่สุดเท่าที่จะเป็นไปได้ และเป็นไปตามข้อกำหนดการปฏิบัติตามกฎระเบียบและสัญญา ตารางต่อไปนี้อธิบายขั้นตอนหลักในโปรแกรมตอบสนองเหตุการณ์ของ Google.

| Incident step | Goal | Description |
|---|---|---|
| **Identification** | Detection | กระบวนการแบบอัตโนมัติและแบบแมนนวลจะตรวจจับช่องโหว่และเหตุการณ์ที่อาจเกิดขึ้น |
| | Reporting | กระบวนการแบบอัตโนมัติและแบบแมนนวลจะรายงานปัญหาไปยังทีมตอบสนองเหตุการณ์ |
| **Coordination** | Triage | กิจกรรมต่อไปนี้เกิดขึ้น:<br>- เจ้าหน้าที่ตอบกลับเมื่อโทรประเมินลักษณะของรายงานเหตุการณ์<br>- เจ้าหน้าที่ตอบกลับเมื่อโทรประเมินความรุนแรงของเหตุการณ์<br>- การตอบสนองการโทรมอบหมายผู้บัญชาการเหตุการณ์ |
| | Response team engagement | กิจกรรมต่อไปนี้เกิดขึ้น:<br>- ผู้บัญชาการเหตุการณ์เสร็จสิ้นการประเมินข้อเท็จจริงที่ทราบ<br>- ผู้บัญชาการเหตุการณ์กำหนดผู้นำจากทีมที่เกี่ยวข้องและจัดตั้งทีมตอบโต้เหตุการณ์<br>- ทีมตอบสนองเหตุการณ์ประเมินเหตุการณ์และความพยายามในการเผชิญเหตุ |
| **Resolution** | Investigation | กิจกรรมต่อไปนี้เกิดขึ้น:<br>- ทีมเผชิญเหตุรวบรวมข้อเท็จจริงที่สำคัญเกี่ยวกับเหตุการณ์<br>- มีการรวมทรัพยากรเพิ่มเติมตามความจำเป็นเพื่อให้มีการแก้ไขที่เหมาะสม |
| | Containment and recovery | หัวหน้าฝ่ายปฏิบัติการดำเนินการตามขั้นตอนต่อไปนี้ทันที:<br>- จำกัด ความเสียหายอย่างต่อเนื่อง<br>- แก้ไขปัญหาพื้นฐาน<br>- กู้คืนระบบและบริการที่ได้รับผลกระทบกลับสู่การทำงานปกติ |
| | Communication | กิจกรรมต่อไปนี้เกิดขึ้น:<br>- ข้อเท็จจริงที่สำคัญได้รับการประเมินเพื่อพิจารณาว่าการแจ้งเตือนนั้นเหมาะสมหรือไม่<br>- การสื่อสารนำไปสู่การพัฒนาแผนการสื่อสารกับลูกค้าเป้าหมายที่เหมาะสม |
| **Closure** | Lessons learned | กิจกรรมต่อไปนี้เกิดขึ้น:<br>- ทีมตอบสนองเหตุการณ์ย้อนหลังเหตุการณ์และความพยายามในการเผชิญเหตุ<br>- การบัญชาการเหตุการณ์กำหนดเจ้าของสำหรับการปรับปรุงระยะยาว |
| **Continuous improvement** | Program development | มีการบำรุงรักษาทีม การฝึกอบรม กระบวนการ ทรัพยากร และเครื่องมือที่จำเป็น |
| | Prevention | ทีมงานปรับปรุงโปรแกรมการตอบสนองเหตุการณ์ตามบทเรียนที่ได้รับ |

# ปลอดภัยในการควบคุมเดสก์ท็อประยะไกล (TeamViewer)

- **การสร้างเซสชันและประเภทการเชื่อมต่อ :** หลังจากการจับมือกันผ่านเซิร์ฟเวอร์หลักของเรา 70% ของทุกกรณีจะสร้างการเชื่อมต่อโดยตรงผ่าน UDP หรือ TCP (แม้จะอยู่เบื้องหลังเกตเวย์มาตรฐาน NAT และไฟร์วอลล์ก็ตาม) การเชื่อมต่อที่เหลือจะถูกส่งผ่านเครือข่ายเราเตอร์ที่มีความซ้ำซ้อนสูงของเราผ่าน TCP หรือ https Tunneling

- **การเข้ารหัสและการรับรองความถูกต้อง :** การรับส่งข้อมูลของ TeamViewer ได้รับการรักษาความปลอดภัยโดยใช้การแลกเปลี่ยนคีย์สาธารณะ/ส่วนตัวของ RSA และการเข้ารหัสเซสชัน AES (256 บิต) เทคโนโลยีนี้ใช้ในรูปแบบที่เทียบเคียงได้กับ https/SSL และถือว่าปลอดภัยอย่างสมบูรณ์ตามมาตรฐานปัจจุบัน

- **การตรวจสอบความถูกต้องของ TeamViewer ID :** TeamViewer ID อิงตามคุณลักษณะต่างๆ ของฮาร์ดแวร์และซอฟต์แวร์ และ TeamViewer สร้างขึ้นโดยอัตโนมัติ เซิร์ฟเวอร์ TeamViewer ตรวจสอบความถูกต้องของ ID เหล่านี้ก่อนการเชื่อมต่อทุกครั้ง

- **Brute-Force Protection :** ในบริบทของการรักษาความปลอดภัยคอมพิวเตอร์ การโจมตีแบบ brute-force เป็นวิธีการลองผิดลองถูกเพื่อเดารหัสผ่านที่ป้องกันทรัพยากร ด้วยพลังการประมวลผลที่เพิ่มขึ้นของคอมพิวเตอร์มาตรฐาน เวลาที่ต้องใช้ในการเดารหัสผ่านยาวๆ จึงลดลงมากขึ้นเรื่อยๆ เพื่อเป็นการป้องกันการโจมตีจากเดรัจฉาน Force TeamViewer จะเพิ่มเวลาแฝงระหว่างความพยายามในการเชื่อมต่อแบบทวีคูณ ดังนั้นจึงใช้เวลามากถึง 17 ชั่วโมงสำหรับการพยายาม 24 ครั้ง เวลาแฝงจะถูกรีเซ็ตหลังจากป้อนรหัสผ่านที่ถูกต้องสำเร็จเท่านั้น

# สรุปข้อดี Google Cloud Platform

1.  Google Cloud platform

เป็นผู้ให้บริการ เซิร์ฟเวอร์ และซอฟต์แวร์ โดยได้รับการดูแลโดยผู้ให้บริการคลาวด์ และไม่สามารถเข้าถึงไฟล์ของผู้ใช้งานได้ จึงไม่สามารถติดไวรัสได้ นอกจากนี้ผู้ให้บริการระบบคลาวด์ ยังมีทีมผู้เชี่ยวชาญในการรักษาความปลอดภัยของเซิร์ฟเวอร์

2. การส่งข้อมูลจาก Mercury ขึ้นคลาวด์ ใช้การเข้ารหัสแบบ SHA-256 ซึ่งดีกว่าการเข้ารหัสแบบ MD5, SHA-1 โดยการเข้ารหัสแบบSHA-256 นั้นถูกใช้ในระบบ Blockchain  และ Cryptocurrency ซึ่งเป็นระบบที่มีความปลอดภัยขั้นสูงสุด

3. Firebase Authentication

- ใช้ JWTs (JSON Web Tokens) ในการตรวจสอบการเข้าระบบโดยมีการเข้ารหัส ซึ่งหมายความว่าไม่สามารถดัดแปลงหรือปลอมแปลงได้ นอกจากนี้ Firebase ยังรีเฟรซ JWTs โดยอัตโนมัติตลอดเวลา ส่งผลให้หากถูกโจรกรรมจะใช้งานได้แค่ชั่วระยะเวลาหนึ่ง
- การรีเซ็ตรหัสผ่าน จะใช้ลิงค์สำหรับการใช้งานครั้งเดียว เพื่อป้องกันไม่ให้ลิงค์นี้ถูกใช้งานซ้ำ

4. Firebase Firestore

- จะต้อง Login เท่านั้นจึงจะสามารถเข้าถึงฐานข้อมูลได้
- ฐานข้อมูลถูกสร้างขึ้นบนโครงสร้างของ GCP ซึ่งมีการรักษาความปลอดภัยสูง
- Firestore ทำซ้ำและจัดเก็บข้อมูลในศูนย์ข้อมูลหลายแห่งโดยอัตโนมัติ ซึ่งช่วยให้มั่นใจว่าข้อมูลจะพร้อมใช้งานเสมอ และสามารถกู้คืนได้ ในกรณีที่ไฟดับหรือไฟไหม้

# นโยบายการปกป้องข้อมูลลูกค้าของ **DYGISTECH**

เงื่อนไขที่พนักงาน DYGISTECH เข้าถึงข้อมูลของลูกค้า
(ในสถานการณ์ปกติพนักงานไม่ได้รับอนุญาติให้เข้าถึงข้อมูล)

*ยกเว้นกรณีดังต่อไปนี้

1. หากเราค้นพบปัญหาหรือการทำงานของระบบผิดปกติ เราจะทำการติดต่อลูกค้าเพื่อขออนุญาต ก่อนจะจัดการปัญหานั้น

2. หากลูกค้าส่งคำขอให้ทางเราแก้ปัญหา จะถือว่านี่เป็นสิทธิ์ชั่วคราวในการเข้าถึงข้อมูลลูกค้า จนกว่าเราจะแก้ไขปัญหาเสร็จ