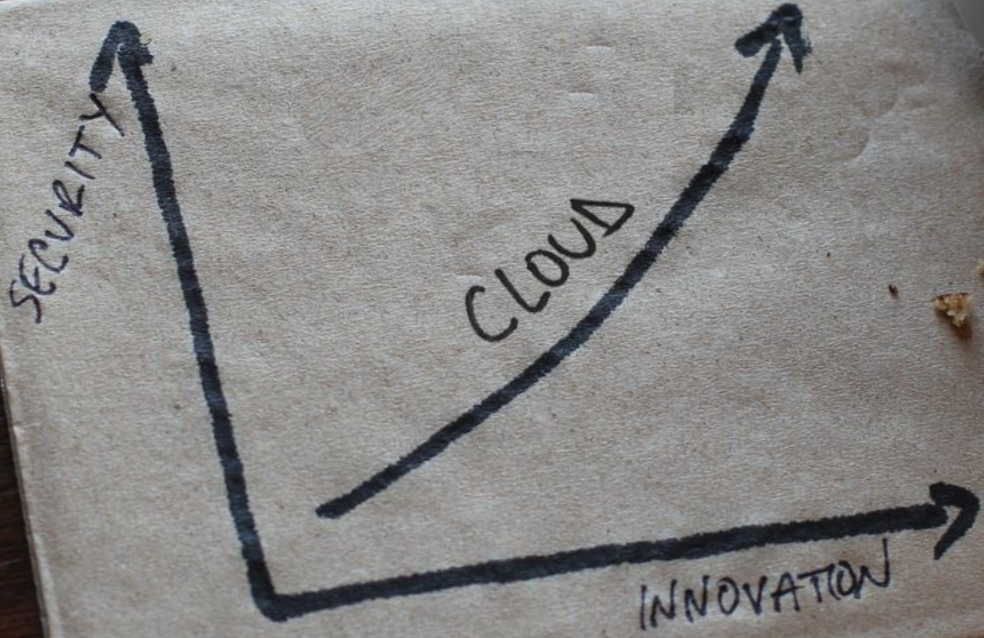




Security, compliance and GDPR and Google Cloud

Google Cloud



Through 2020, public cloud workloads will suffer at least 60% fewer security incidents than those in traditional data centers

Gartner[®]

Clouds Are Secure: Are You Using Them Securely?

Published: 21 July 2016 ID: G00299720



Seven cloud
products with
one billion
users each



Customer data and Google Cloud

The data you put into our system is yours

We do not scan it for advertisements
nor sell it to third parties

**Cloud benefits from security investment
across our whole business**



Google Cloud Security Fundamentals



Protection

Secure core infrastructure designed, built, and operated to help prevent threats



Control

Security controls to help meet policy, regulatory, and business objectives



Compliance

Working to meet our responsibilities and make compliance easier for customers



Protection

Secure core infrastructure designed, built, and operated to help prevent threats





Usage



Operations



Deployment



Application



Network



Storage



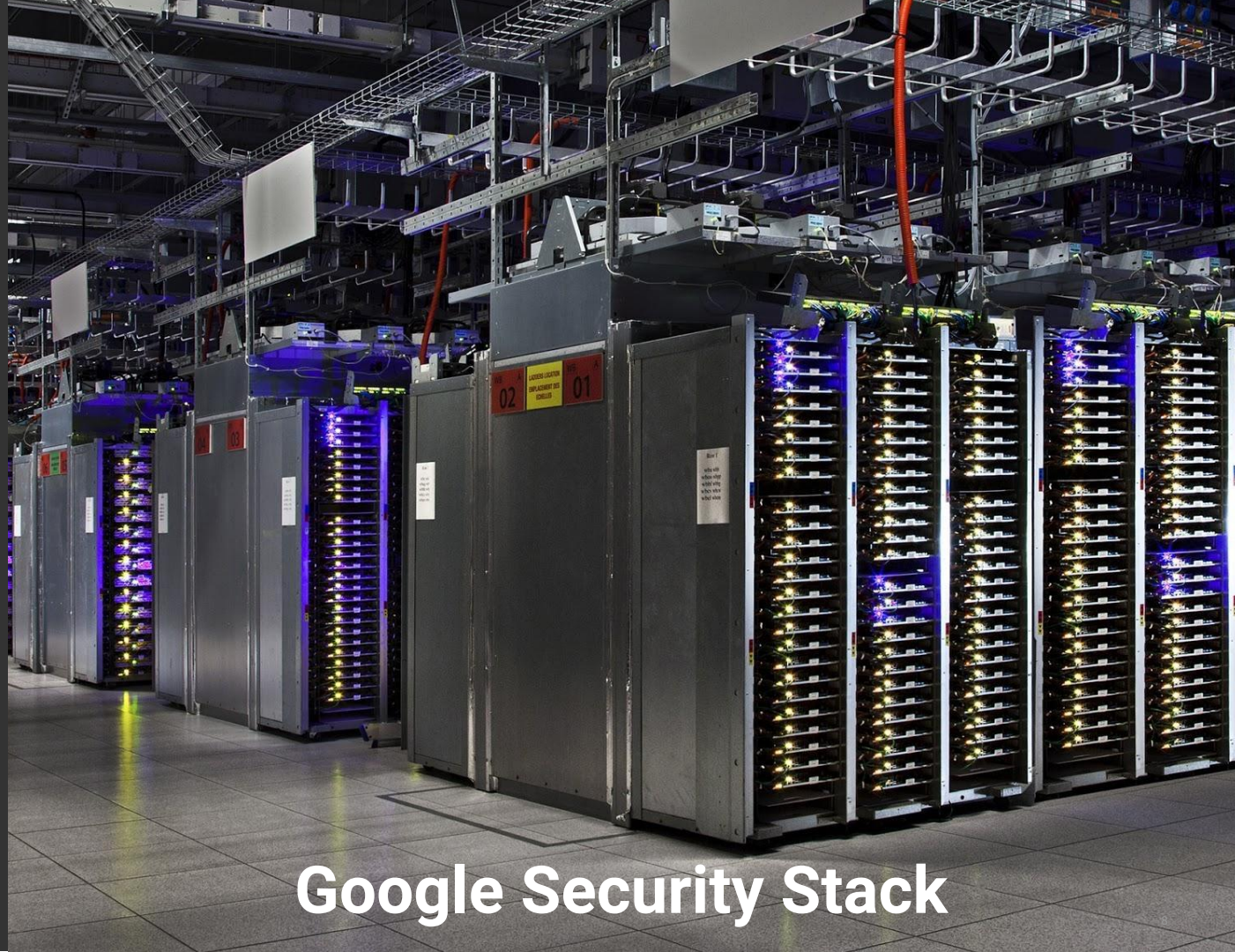
OS + IPC



Boot












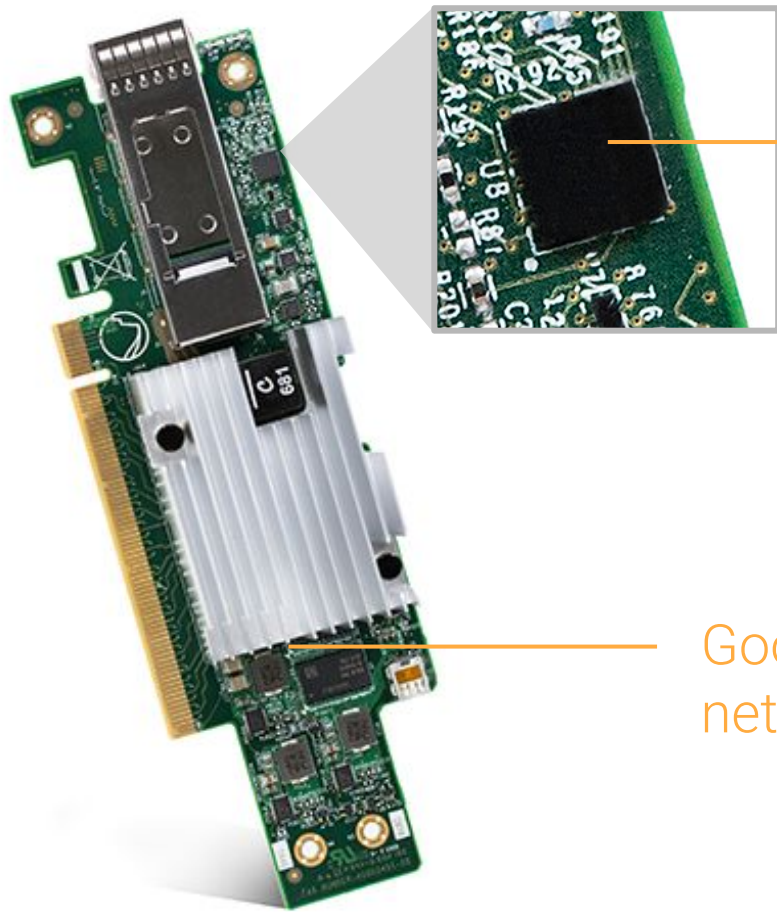
Hardware



Google Security Stack

Infrastructure security in depth

	Usage	Audit Logging	Safe Browsing API	BeyondCorp	Security Key Enforcement		
	Operations	Compliance & Certifications	Live Migration Infra maintenance & patching	Threat analysis and intelligence	Open Source Forensics tools	Anomaly Detection (Infrastructure)	Incident Response (Infrastructure)
	Deployment	Google Services TLS encryption with perfect forward secrecy	Certificate Authority	Free and automatic certificates	DDoS Mitigation (PaaS & SaaS)		
	Application	Peer code review & Static Analysis (Infrastructure SLDC)	Source code provenance (Infrastructure)	Binary Verification (Infrastructure code)	WAF (PaaS & SaaS Use cases)	IDS/ IPS (PaaS & SaaS Use cases)	Web Application Scanner (Google Services)
	Network	Infrastructure RPC encryption in transit between data centres	DNS	Global Private Network	Andromeda SDN Controller	Jupiter Datacenter Network	B4 SDN Network
	Storage	Encryption at rest	Logging	Identity and Access Management	Global at scale Key Management Service		
	OS + IPC	Hardened KVM Hypervisor	Authentication for each host and each job	Curated Host Images	Encryption of Interservice Communications		
	Boot	Trusted Boot	Cryptographic Credentials				
	Hardware	Purpose-built Chips	Purpose-built Servers	Purpose-built Storage	Purpose-built Network	Purpose-built Data Centers	



Titan

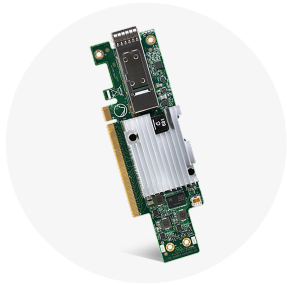
Google's purpose-built chip to establish hardware root of trust for both machines and peripherals on cloud infrastructure

Google's purpose-built network controller



Purpose-built hardware infrastructure

Provenance from the bottom of the stack to the top



Purpose-built
chips



Purpose-built
servers



Purpose-built
storage



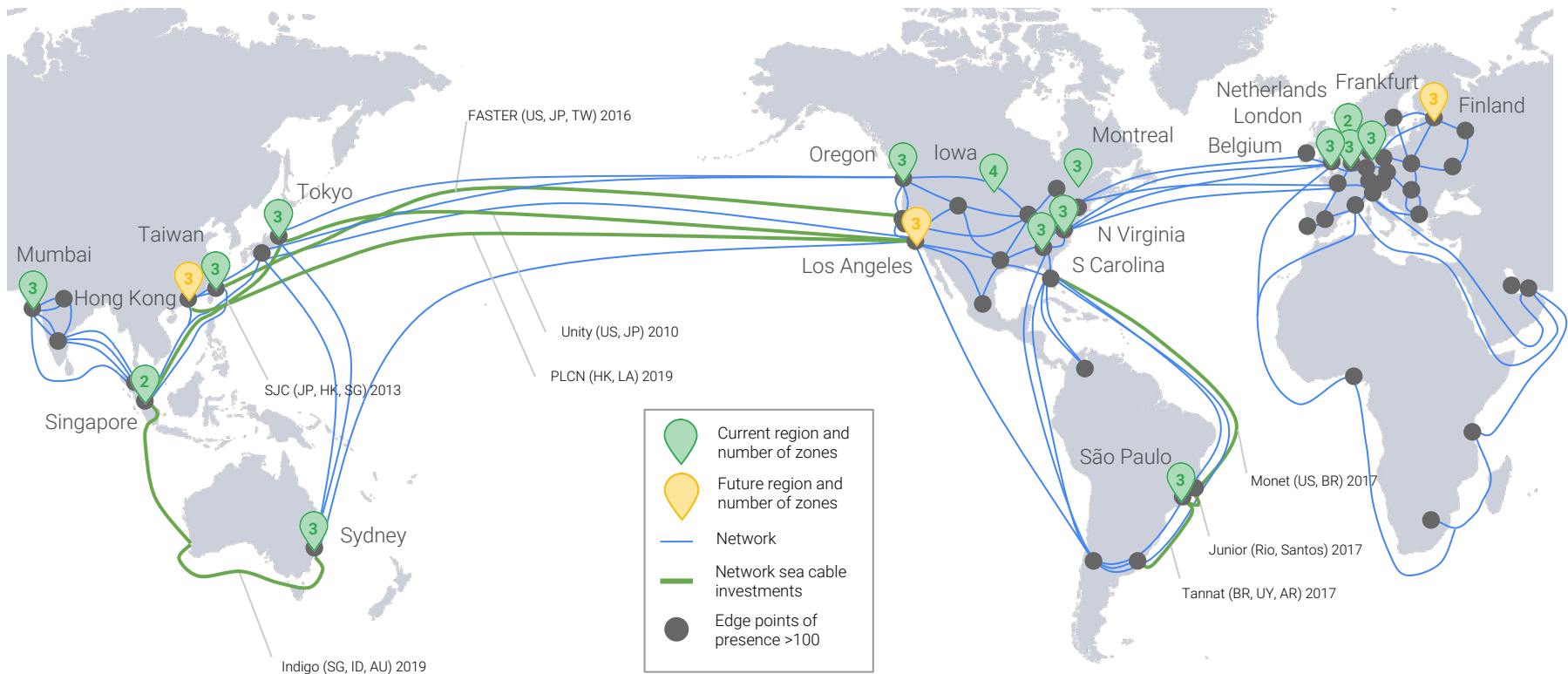
Purpose-built
network



Purpose-built
data centers

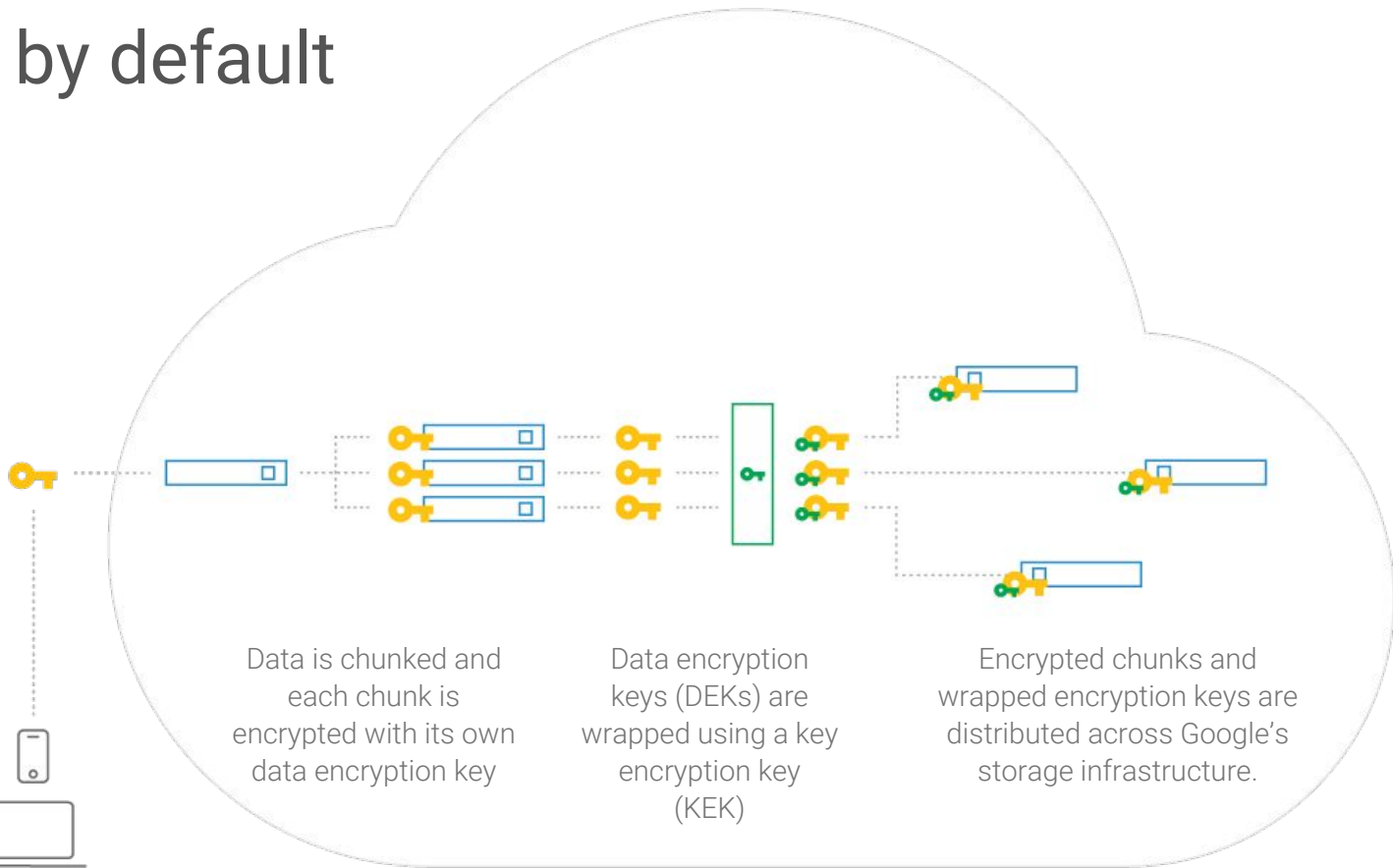
Reduced “vendor in the middle” risk

GCP Infrastructure



Encryption by default

All connections to Google Cloud require TLS



Google Project Zero

Google's Project Zero security team discovered a vulnerability affecting modern microprocessors. Since then, Google engineering teams have been working to protect our customers from the vulnerability across the entire suite of Google products.

All G Suite applications have already been updated to prevent all known attack vectors.

GCP has already been updated to prevent all known vulnerabilities

Spectre

Meltdown

Variant 1
CVE-2017-5753

Variant 2
CVE-2017-5715

Variant 3
CVE-2017-5754

<http://googleprojectzero.blogspot.co.uk/>



Keeping ahead of today's threats

Customers continually surfacing new requirements

Cloud customers across
every geography and vertical

7 consumer services with
more than 1bn users

Significant sustained investment

\$30.9bn in network investments
over the last 3 years

Global team of leading security
engineers & researchers

Vulnerability Rewards Program

Community engagement

Open source contributions
High impact vulnerability and
other security research

Control

Security controls to help meet policy, regulatory, and business objectives



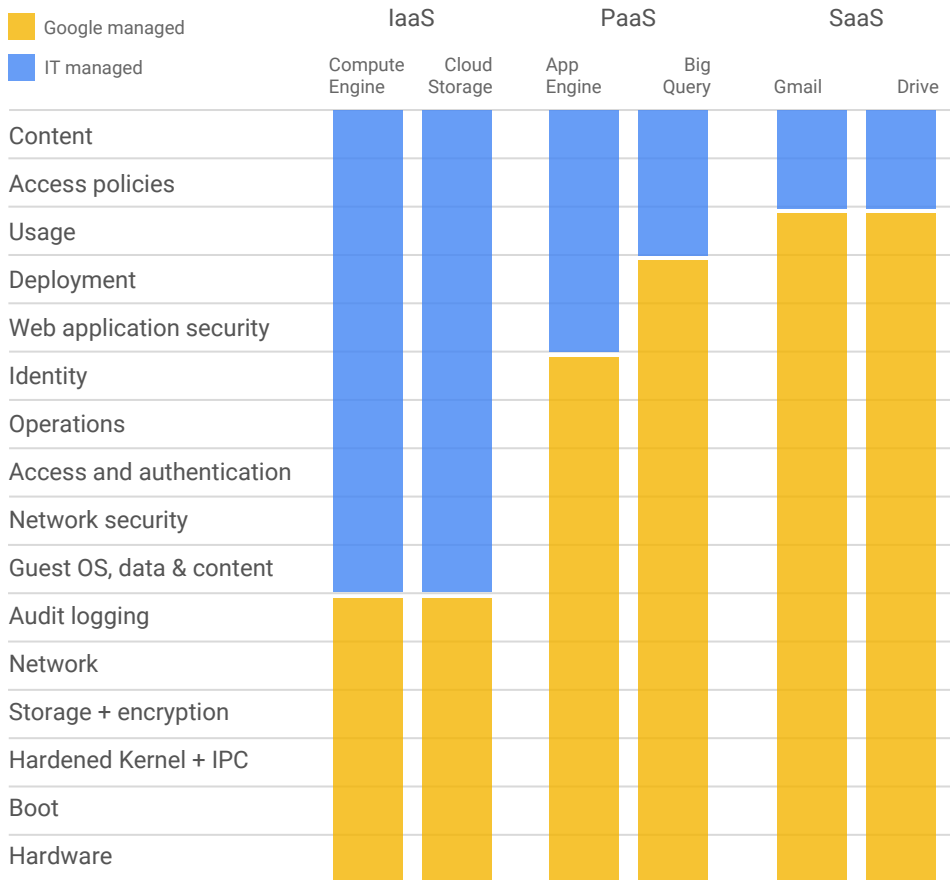


Cloud security requires collaboration

We are responsible for securing Google's infrastructure

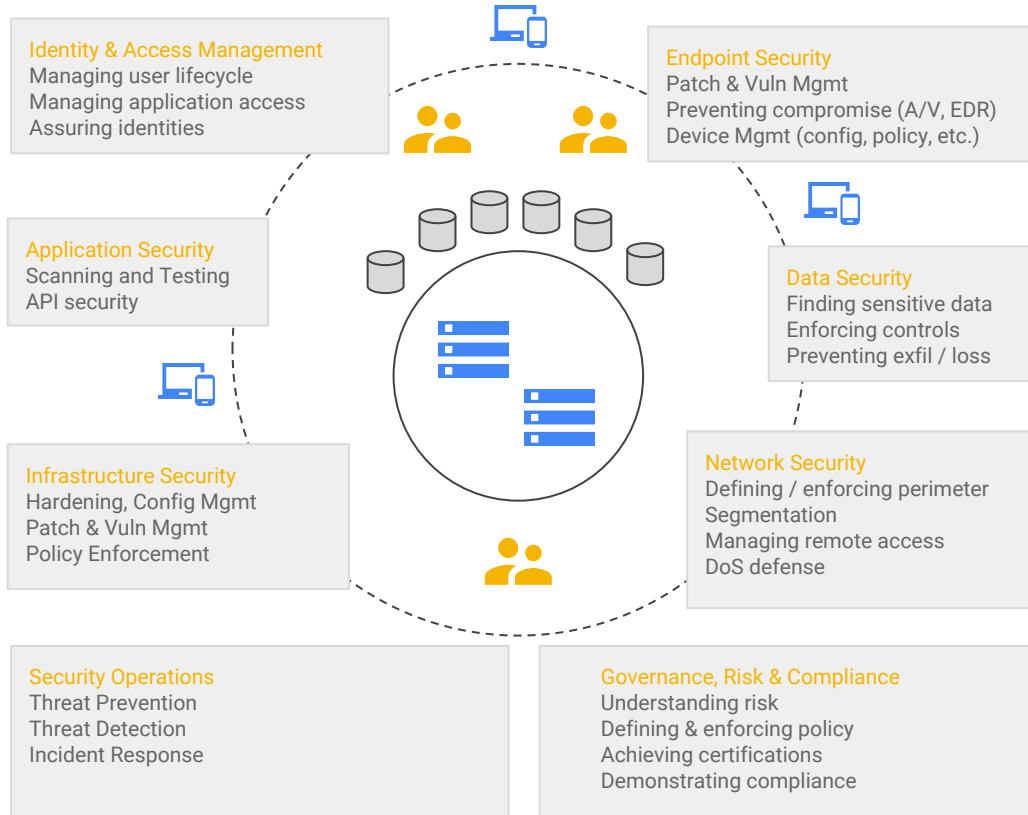
You are responsible for securing your data

We help you with best practices, templates, products & solutions





Security program activities



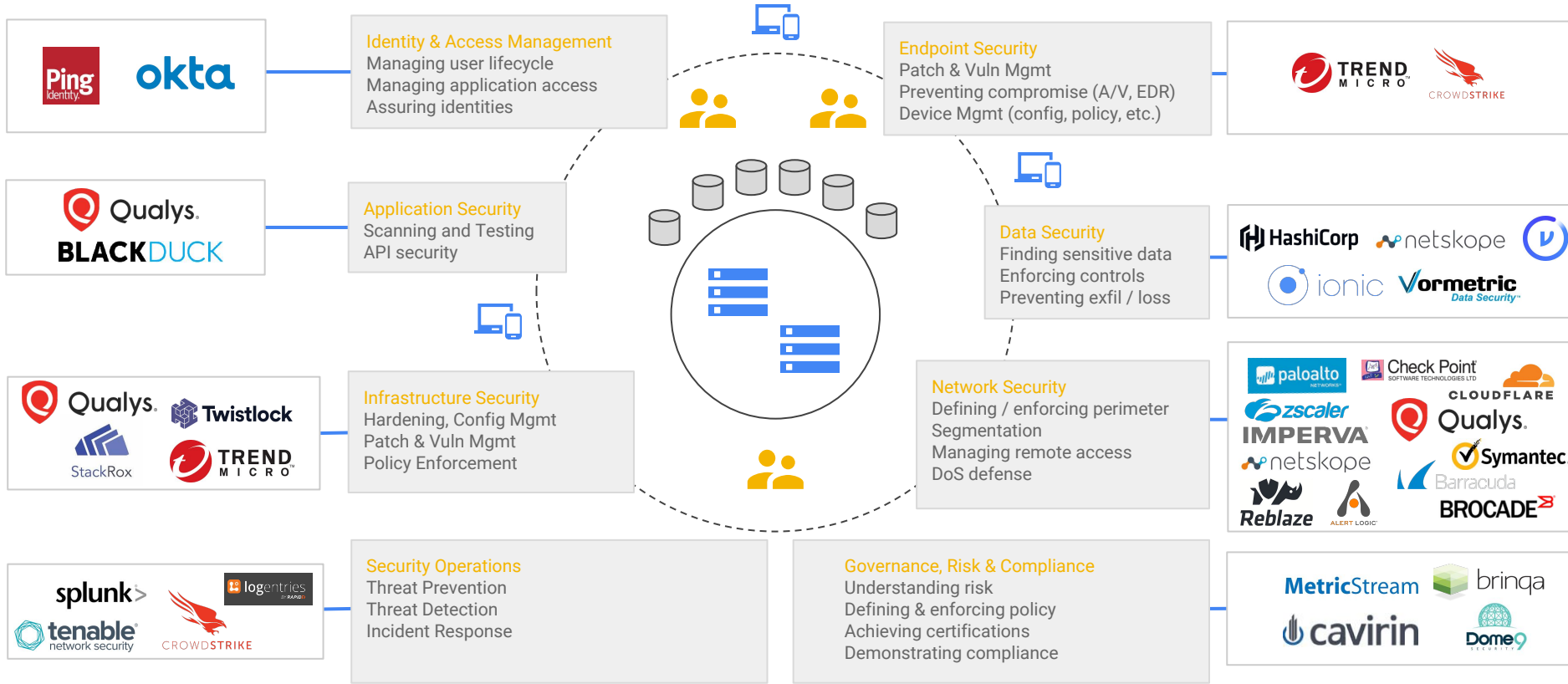


Google Cloud security controls





Supported by an ecosystem of technology partners



🔍 Compliance

Meeting our responsibilities
and making compliance easier
for customers



Compliance



Information Security



Cloud Security



Cloud Privacy

Compliance

600+

Security Engineers

160

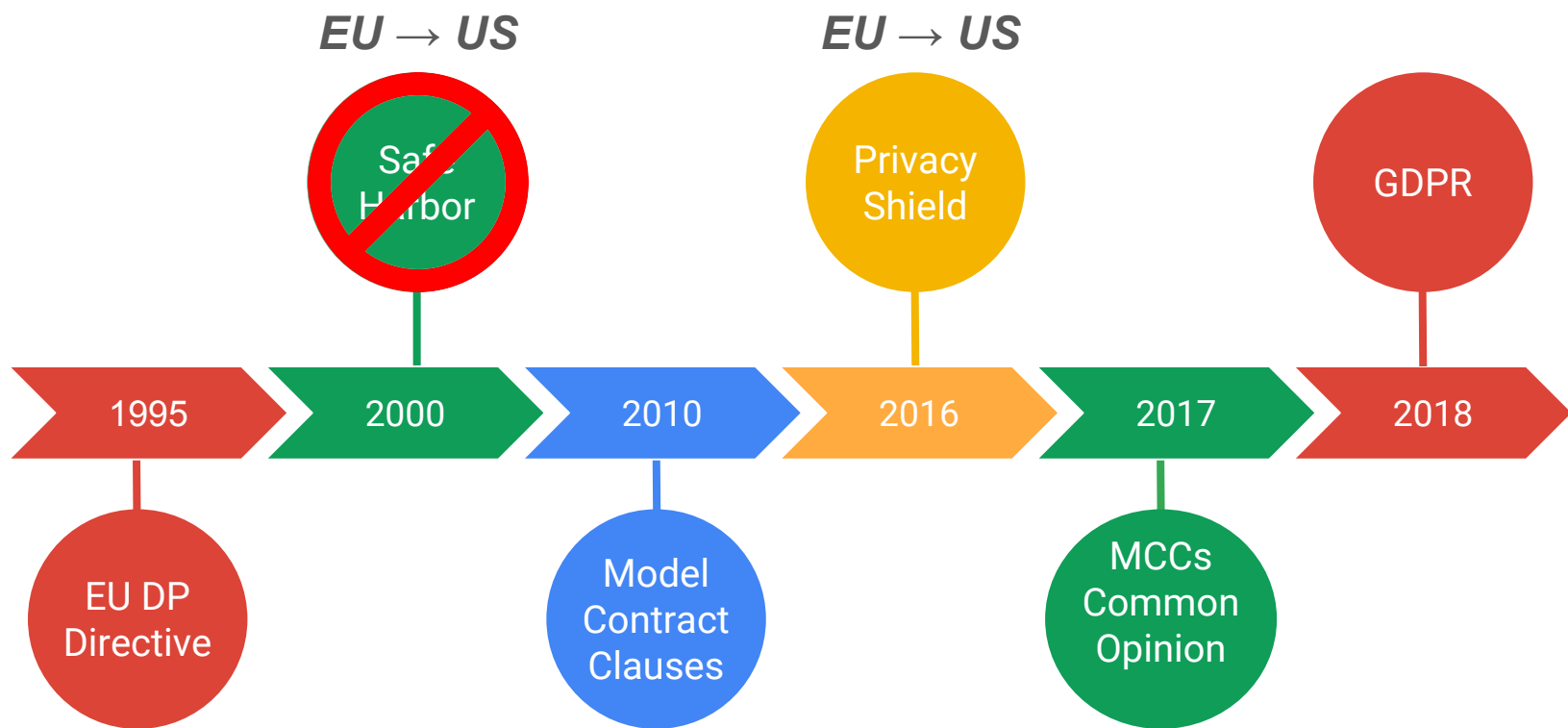
Academic Research Papers on Security

700+

CVE's discovered



EU Privacy Compliance



EU data protection authorities confirm compliance of Google Cloud commitments for international data flows

WRITTEN BY

Marc Crandall
HEAD OF GLOBAL COMPLIANCE, GOOGLE CLOUD

Matthew O'Connor
HEAD OF SECURITY AND COMPLIANCE, GOOGLE CLOUD
PLATFORM

What does the GDPR mean for customers, Google and Cloud adoption?



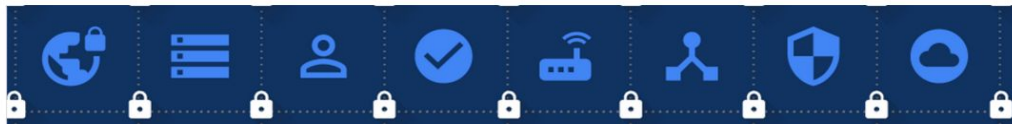
GDPR will require new terms to be put into place - available now

Data breach notification timelines will apply regardless of platform (on-premise or cloud)

Fines for non-compliance can range from 20M EUR to 4% of revenue (whichever is greater)

<https://www.google.com/cloud/security/gdpr/>

Google Cloud rolls out data processing terms addressing GDPR changes

**Nathaly Rey**

Head of EMEA Data Protection and Compliance, Google Cloud

Marc Crandall

Director of Data Protection and Compliance, Google Cloud

Published Oct 12, 2017

On May 25, 2018, the most significant piece of European data protection legislation to be introduced in 20 years will come into force when the EU's [General Data Protection Regulation \(GDPR\)](#) replaces its 1995 Data Protection Directive. We know that preparing for this regulatory change is a priority for the millions of organizations who rely on our cloud services to run their businesses, and it's equally a priority for us.

Yesterday we rolled out the [Data Processing Amendment \(Version 2.0\)](#) for G Suite and the [Data Processing and Security Terms \(Version 2.0\)](#) for Google Cloud Platform (GCP), both of which have been specifically updated to reflect the GDPR. We're making these terms available well in advance of the entry into force of the GDPR to facilitate our customers' compliance assessments and GDPR readiness when using Google Cloud services. Our customers can opt in now to these updated versions within the admin consoles for [G Suite](#) and [GCP](#) (as applicable).

Google is committed to GDPR compliance and to helping our customers with their own compliance journeys. Further information regarding Google Cloud and the GDPR is available on our Cloud GDPR [website](#). ■

POSTED IN: [GOOGLE CLOUD](#)

<https://goo.gl/5rTWFv>

 @bagibson

You are the **data controller**
We are a **data processor**



Our data protection commitments



We put our commitments in writing and evolve them based on feedback from our customers & regulators



New data processing terms addressing GDPR changes



Our employees are required to sign a confidentiality agreement & complete confidentiality & privacy trainings

Data return (reversibility)

1

You can export and download your data from Google Cloud services

2

Few easy steps to create an archive of your records or use the data in another service

- Choose which Google products to include in your archive
- Choose how your archive is delivered

3

We are continually working to enhance the robustness of the data export capabilities.

Data deletion

- 1 Built-in functionality for a complete data deletion
- 2 Data is deleted from the systems within a maximum period of 180 days following deletion instructions
- 3 Data deletion commitments in our data processing terms for several years

Assistance to the controllers

- 1 Functionality to help access, rectify, restrict the processing of, or delete personal data
- 2 Dedicated channel for data protection related enquiries
- 3 Contractual commitments around incident notification

Google Cloud useful compliance tools



2-step verification



Security keys



^ Security

2-step verification

Adds an extra layer of security by requiring the user to enter a verification code in addition to their username and password. ?

Status: Not enrolled and not enforced

Security Keys

This user doesn't have any security keys ?

ADD NEW KEY

! Registering a security key will automatically enroll the user in 2-step verification.

Password strength

8 character password. ?

Password strength rating



Application specific passwords

The user has not created any application-specific passwords. ?

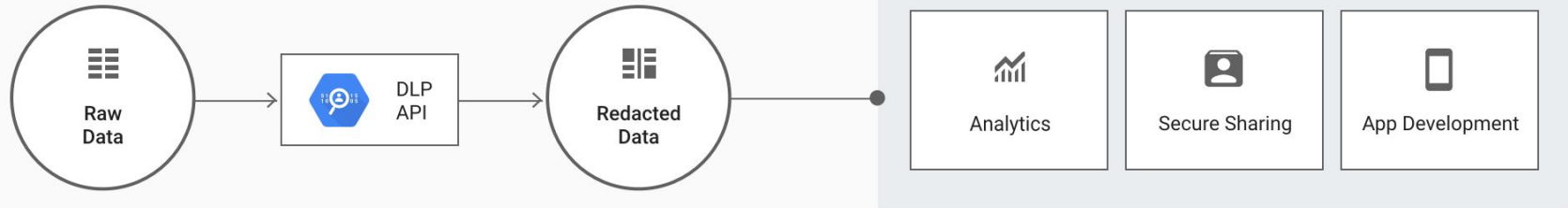
Authorized access

The user has not authorized any service to access their Google Account. ?

“An organization cannot properly protect
PII it does not know about.”

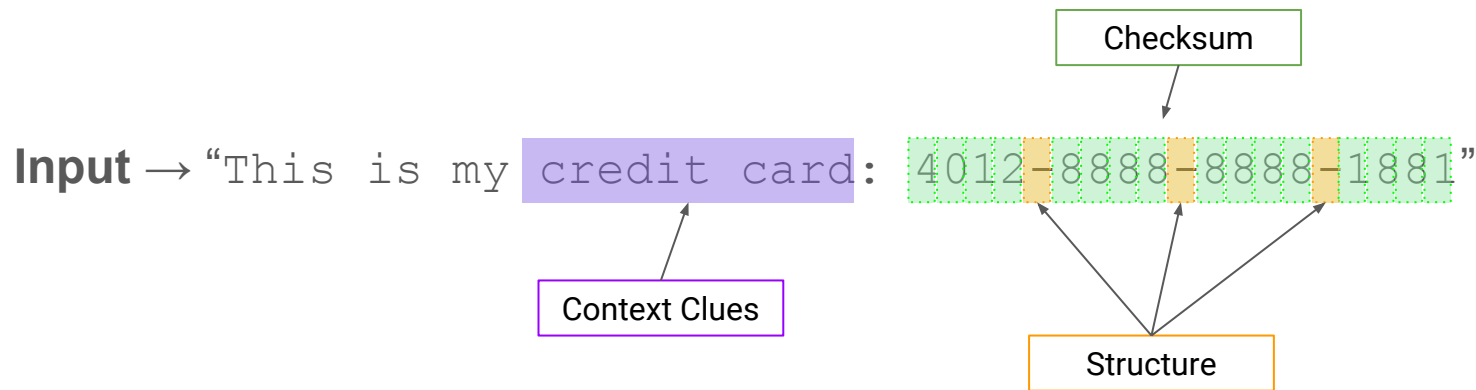
NIST Special Publication 800-122 Guide to Protecting the
Confidentiality of Personally Identifiable Information (PII)

Data Loss Protection API & data classification



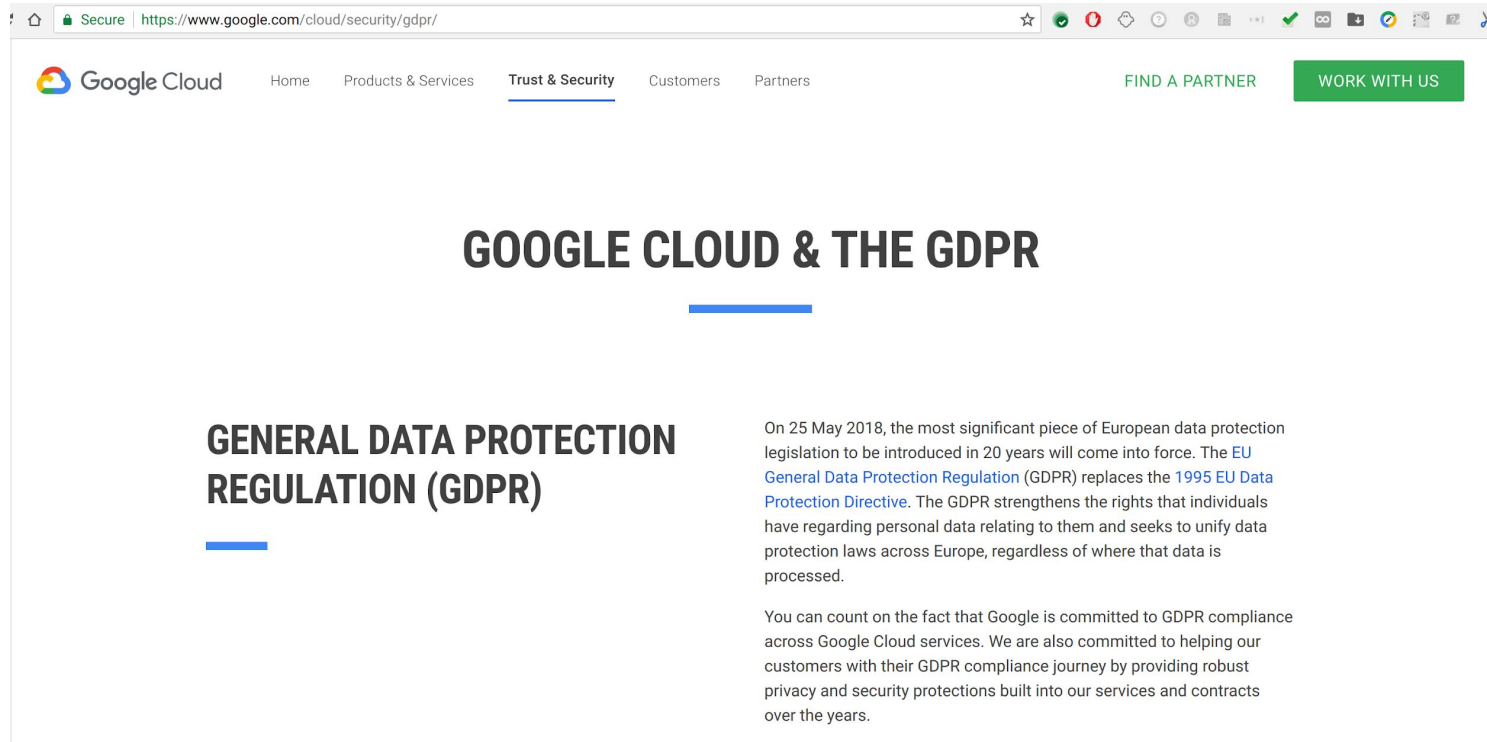
Sensitive Data Classification

(unstructured data example)



Output → “CREDIT_CARD_NUMBER, High confidence”

Check our online resources



The screenshot shows a web browser window with the URL <https://www.google.com/cloud/security/gdpr/>. The page header includes the Google Cloud logo, navigation links for Home, Products & Services, Trust & Security (which is underlined), Customers, and Partners. On the right side of the header, there are two buttons: "FIND A PARTNER" and "WORK WITH US".

GOOGLE CLOUD & THE GDPR

GENERAL DATA PROTECTION REGULATION (GDPR)

On 25 May 2018, the most significant piece of European data protection legislation to be introduced in 20 years will come into force. The [EU General Data Protection Regulation \(GDPR\)](#) replaces the [1995 EU Data Protection Directive](#). The GDPR strengthens the rights that individuals have regarding personal data relating to them and seeks to unify data protection laws across Europe, regardless of where that data is processed.

You can count on the fact that Google is committed to GDPR compliance across Google Cloud services. We are also committed to helping our customers with their GDPR compliance journey by providing robust privacy and security protections built into our services and contracts over the years.

Brian A Gibson

bagibson@google.com | [linkedin.com/in/bagibson](https://www.linkedin.com/in/bagibson) | twitter.com/bagibson

Google Cloud

