



Data Security & the General Data Protection Regulation

James Leonard - UK Regional Manager

Joel Solomons - Sales Engineer EMEA

Google Cloud - Privacy & Security

GDPR - What we're doing?

ChromeOS Security

Questions

The image features a blue flag with twelve yellow stars, the flag of the European Union, waving on a silver pole. The background is a bright blue sky with a soft, out-of-focus sun flare on the right side. The text "GDPR at a glance" is overlaid in white, bold, sans-serif font across the center of the image.

GDPR at a glance

General Data Protection Regulation at a glance

- The most significant piece of European data protection legislation to be introduced in 20 years
- Harmonizes EU data protection law
- Strengthens the rights that individuals have regarding personal data
- Security is at the core of GDPR
- Data transfers mechanism enhanced



General Data Protection Regulation at a glance

- New aspects:
 - Applies to providers
 - Incident notifications
 - Data Deletion or Return
 - Sub-processors
 - Fines (up to 4% of turnover)

Google is committed to GDPR compliance across G Suite & Google Cloud Platform



Security & Compliance in the Cloud

Joel Solomons
Solutions Engineer
Google Cloud



Quick Quiz

Who owns the data stored within G Suite? **You.**

What are core services? **The services provided under the G Suite agreement and adhere to the privacy and security commitments in our agreement. We also offer 24/7 free support for these services.**

Is advertising part of G Suite for Education? **No.**



Smarter with Gartner

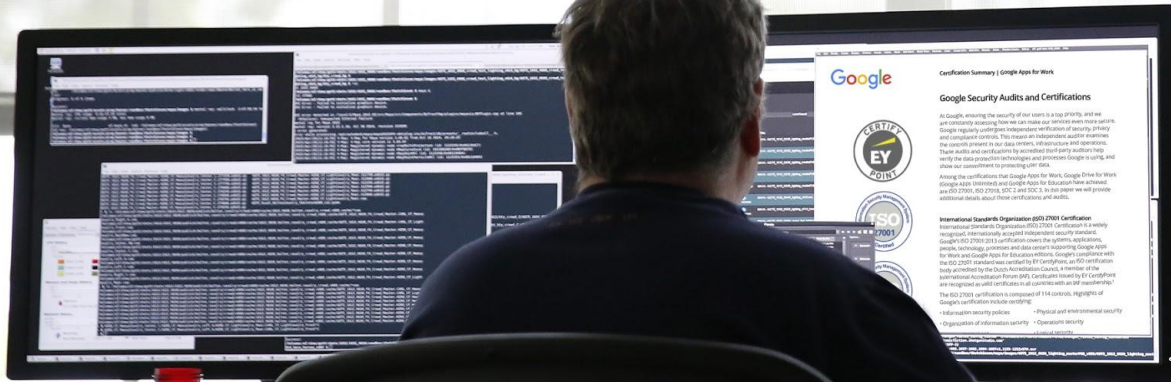
Smarter With **Gartner**

IT

Through 2020, public cloud infrastructure as a service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centers.

Gartner concluded that the security posture of major cloud providers is as good as or better than most enterprise data centers and security should no longer be considered a primary inhibitor to the adoption of public cloud services. However, it is not as simple as moving on-premises workloads to the cloud, and security teams should look to leverage the programmatic infrastructure of public cloud IaaS. Automating as much of the process as possible will remove the potential for human error — generally responsible for successful security attacks.

How to help build **trust**, keep **control** and stay **compliant**?



G Suite



Aol.

Deloitte.



The Economist



NESTE



FedEx

INTUIT.

Office DEPOT



JBER



Chrome/Android



sears



NETFLIX



SCHEELS

chico's



Maps & APIs



BURBERRY



Walgreens

First Data.



GCP



AVAYA



PHILIPS

The New York Times



FIS



Google for Education

Google



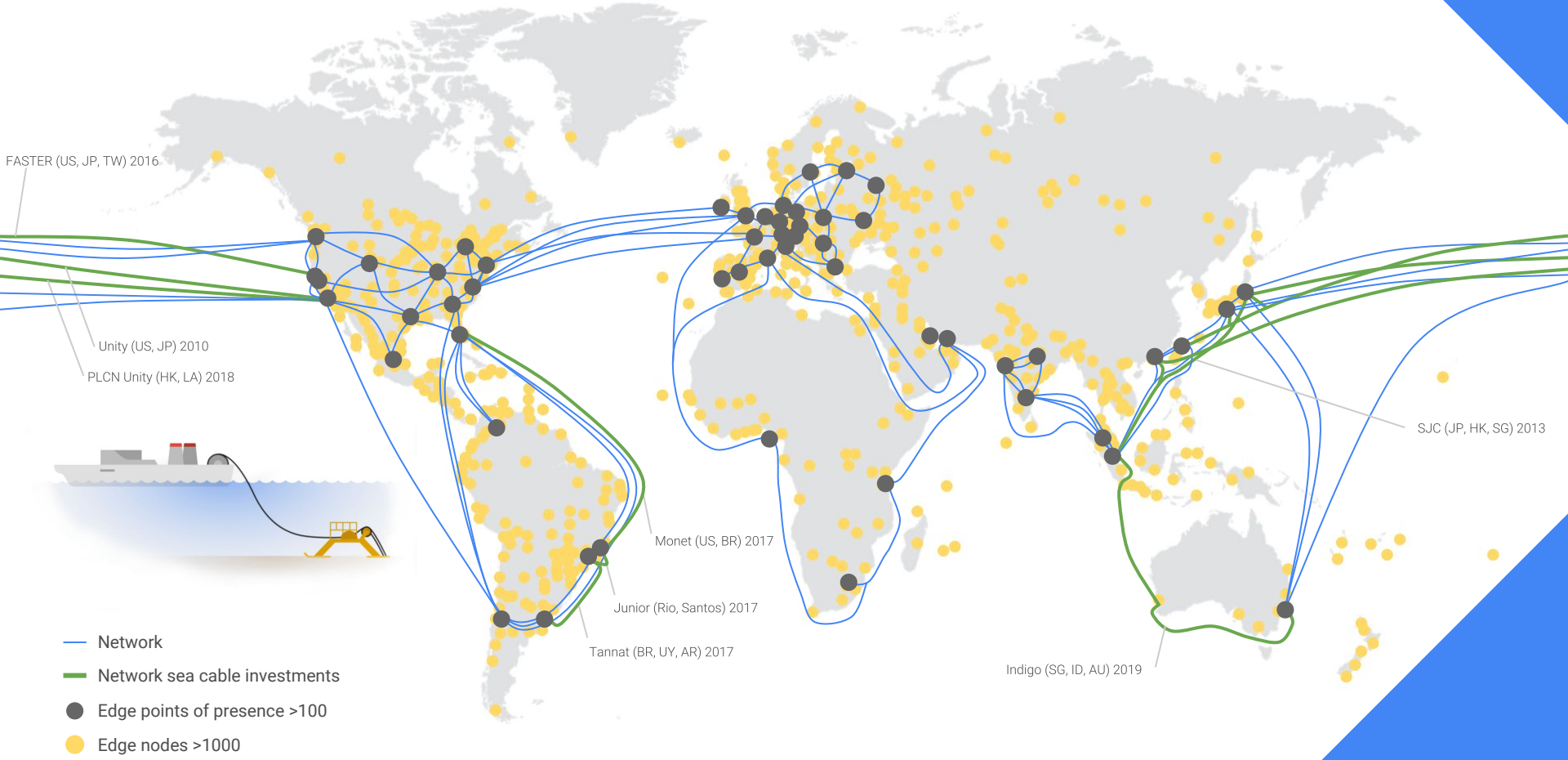
7* Cloud products with 1 billion users

Web scale, intelligent automation

Google for Education



Google Cloud Network



Securing the entire stack

 [Mobile] Usage

 Operations

 Deployment

 Application

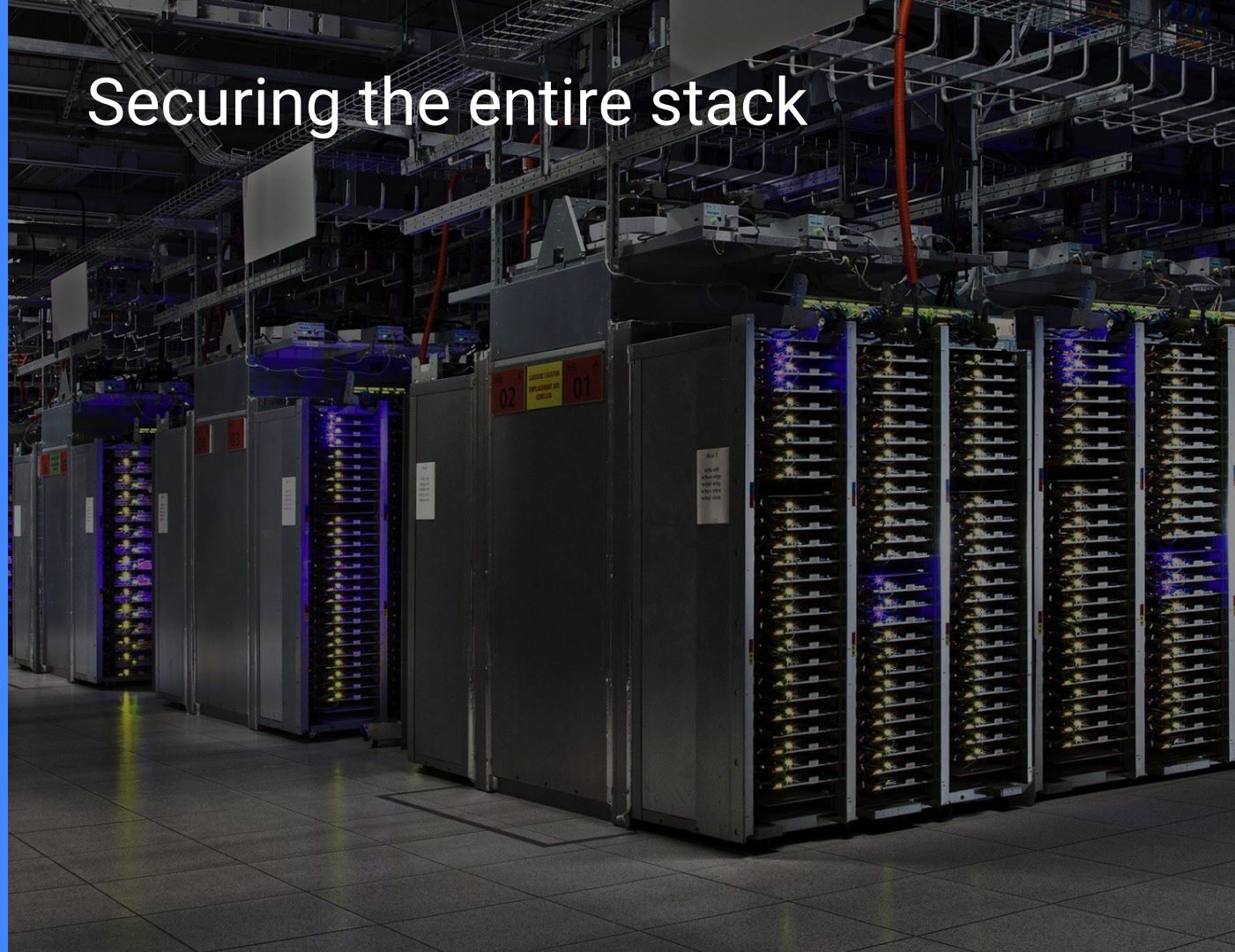
 Network

 Storage










 OS + IPC

 Boot

 Hardware



Infrastructure security in depth

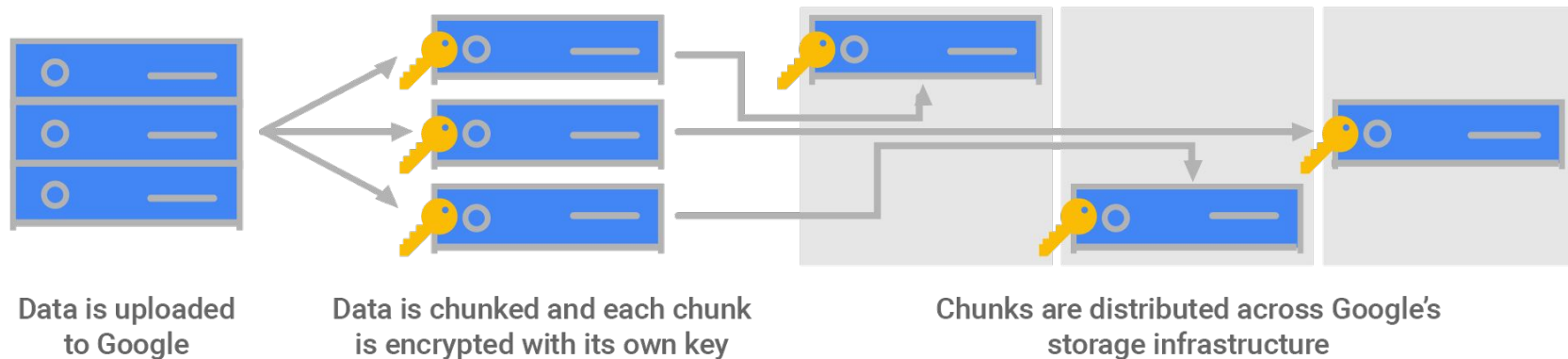
	Usage	Audit Logging	Safe Browsing API	BeyondCorp	Security Key Enforcement		
	Operations	Compliance & Certifications	Live Migration Infra maintenance & patching	Threat analysis and intelligence	Open Source Forensics tools	Anomaly Detection (Infrastructure)	Incident Response (Infrastructure)
	Deployment	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	



Encryption by default

- At rest and in transit
- Use our keys or bring your own

Data is 'chunked' for encryption and storage



Two chunks will not have the same encryption key, even if they are part of the same Google Cloud Storage object, owned by the same customer, or stored on the same machine

Making compliance easier

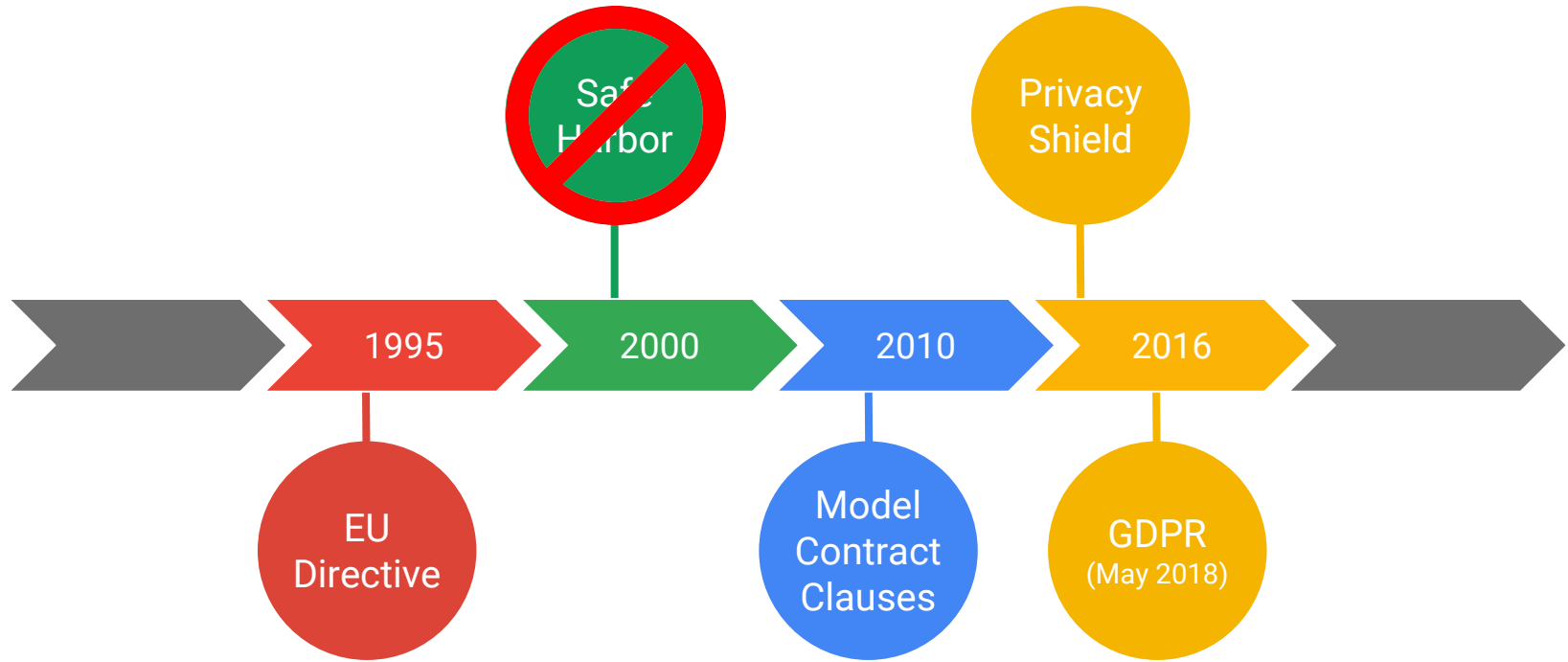


Privacy Shield
Framework



...

A history of data privacy in the EU



GDPR the new gold standard

- Harmonize the data protection landscape
- Expect Ethics - Documentation - Security
- Fines matter but also brand damage
- Applicable to processors
- Internet friendly.
More data transfer mechanisms



You are the
data controller



We are a data
processor





 The Keyword Latest Stories Product News Topics

GOOGLE CLOUD MAY 3, 2017

Google Cloud: Our Commitment to the General Data Protection Regulation (GDPR)

WRITTEN BY

Suzanne Frey
DIRECTOR, SECURITY, TRUST & PRIVACY, GOOGLE CLOUD

Marc Crandall
DIRECTOR OF DATA PROTECTION AND COMPLIANCE, GOOGLE CLOUD

Contracts



Scope

IP

Portability

Deletion

Notification

Audits

Security

Sub-process

Transfers

International Data Transfers under the GDPR



Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
 - (a) a legally binding and enforceable instrument between public authorities or bodies;
 - (b) binding corporate rules in accordance with Article 47;
 - (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
 - (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
 - (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
 - (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.



GOOGLE CLOUD

FEB 6, 2017

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



Technical risk

Legal risk

Political risk

Cultural risk

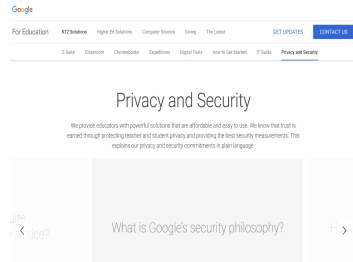
Learn more and next steps

1



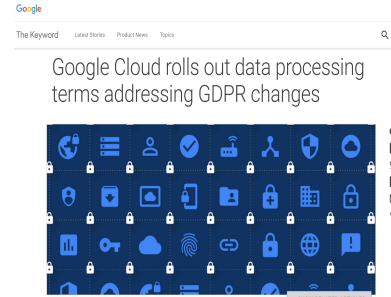
[Google Cloud Blog](#)

2



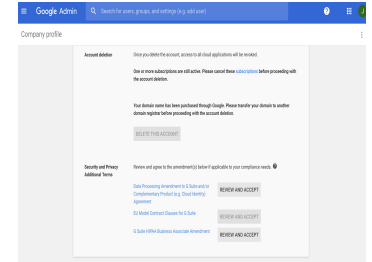
[Google for Education Trust Page](#)

3

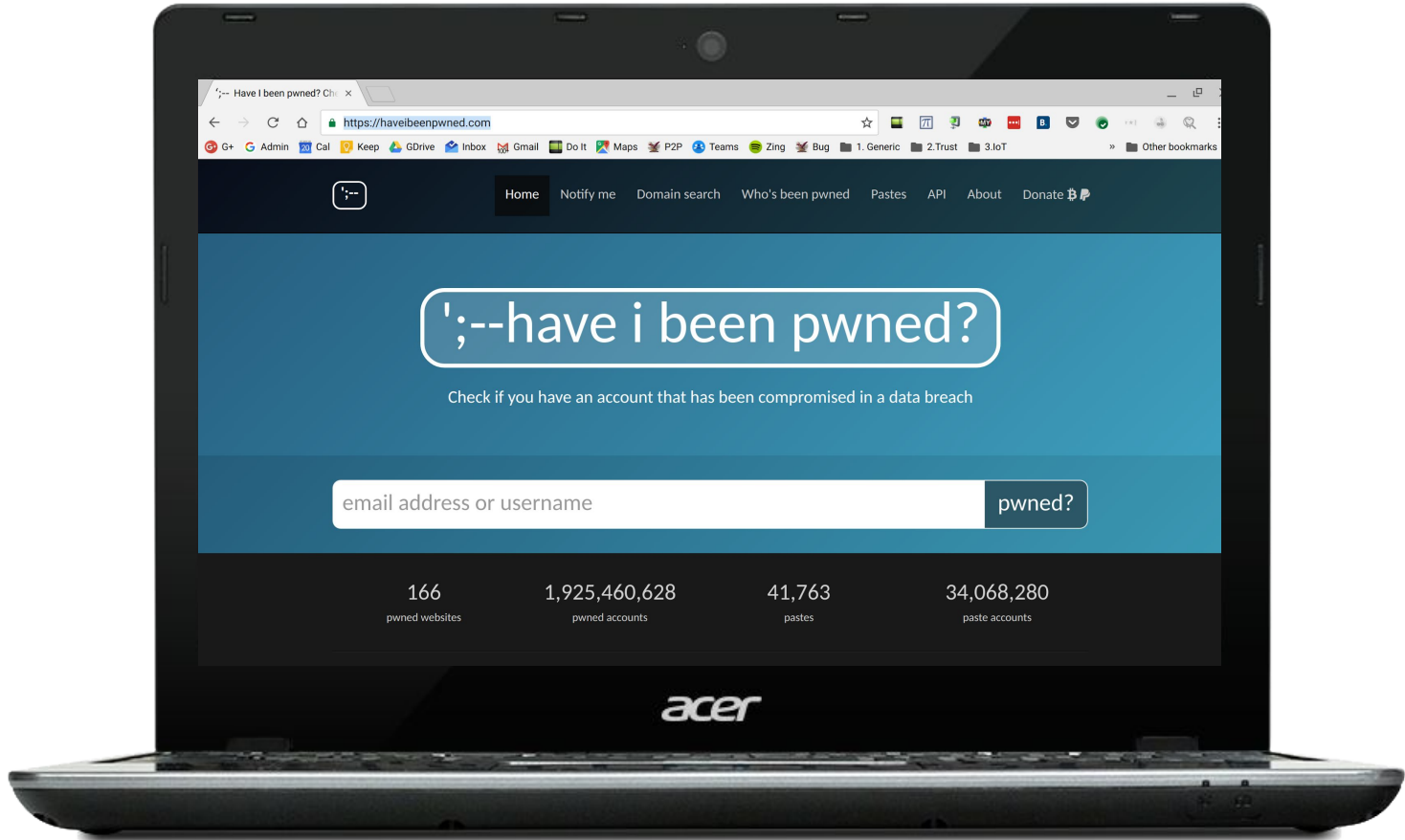


[New DPA just launched \(last month\)](#)

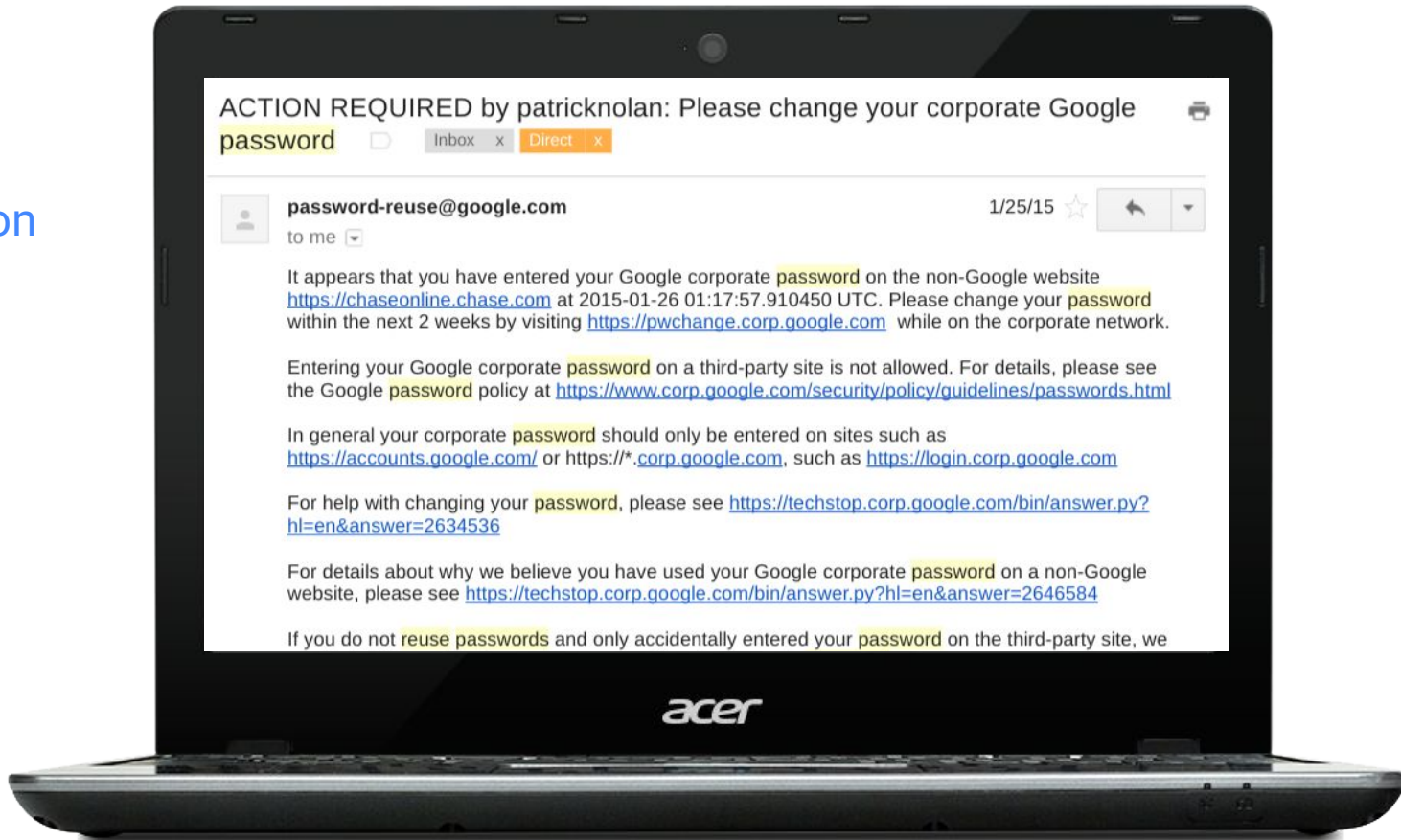
4



[Accept the new DPA and MCC in your Admin console](#)

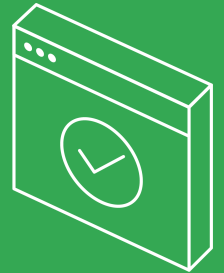
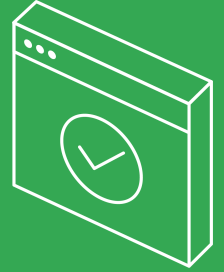
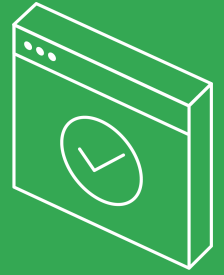


Install Password Alert Chrome Extension



ChromeOS

Google for Education



Chrome OS Security

Security, a cornerstone of Chrome OS, designed in from day one



Speed



Simplicity



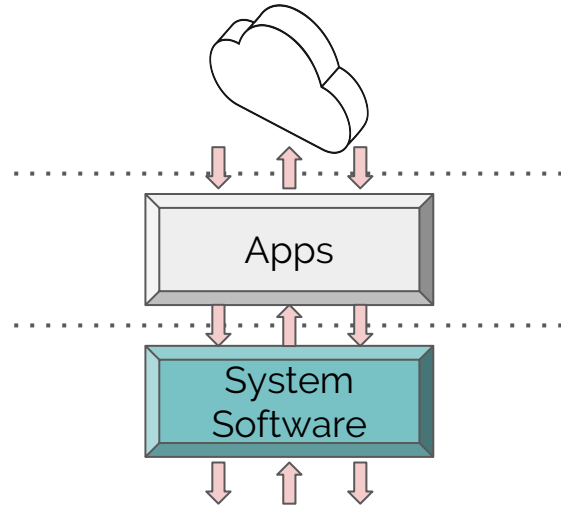
Security



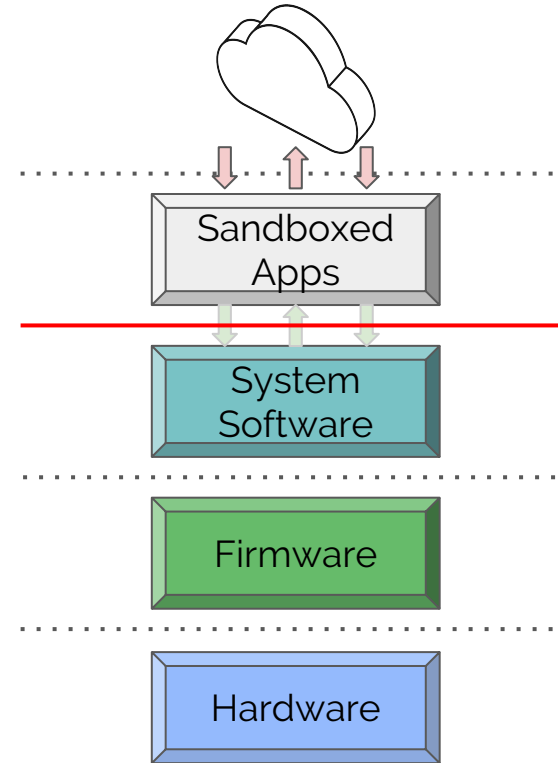
Scalability

Chrome OS Security

With Chrome OS, Apps are kept isolated and sandboxed, security applied at all levels



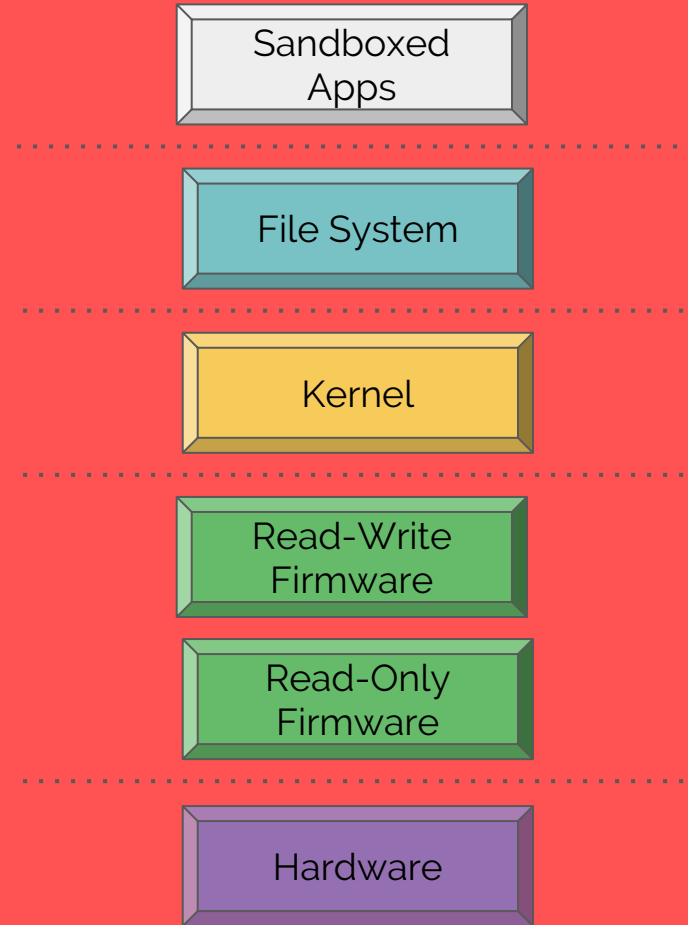
With legacy OSs, Apps have the same privileges and power as you



Chrome OS Security

“Defense in Depth”

- Make it hard to get into the system, but assume that an attacker will
- Put another layer of defenses in place to make it difficult to get to the next level
- Repeat



Chrome OS Security

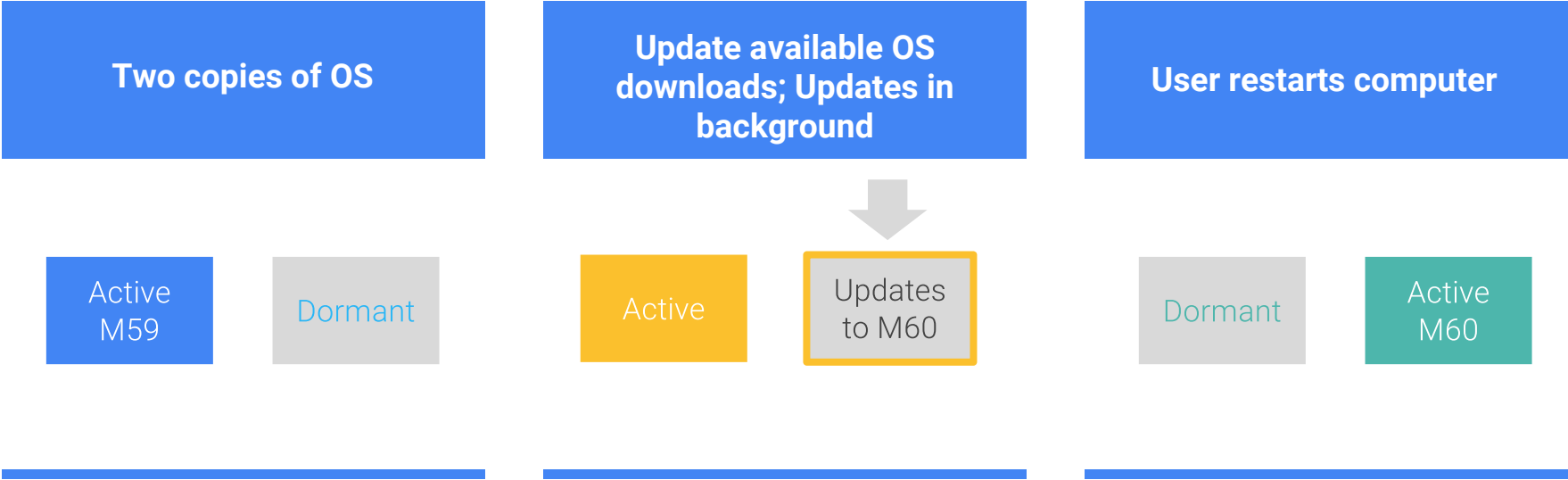
Security built in at the Hardware level

- Google approved Hardware Reference Designs
- All Chrome OS devices required to follow Reference Schematics
- Ensure 'Root of Trust' Read-Only
- Ensure first executed code is from 'Root of Trust'
- Non-compliance = No Software builds



Chrome OS Security

Two copies - background automatic updates for Firmware and Software



Chrome OS Security

In Summary...

Hardware design to guarantee a 'root of trust'

+

Google Signed images and Verified Boot

+

Read-only Root Filesystem

=

A very secure OS and

No need for Antivirus Software!



A man with a beard and glasses, wearing a light blue button-down shirt, is sitting at a desk in a dimly lit office. He is looking down at a tablet computer he is holding with both hands. In the background, there is a grey sofa, a desk with a white mug, and a corkboard with papers and sticky notes on the wall. The overall atmosphere is professional and focused.

What can you do?

Where should you start?

1

Familiarize yourself with GDPR, and seek legal advice

2

Know the data that you collected

3

Review current controls; address any gaps

4

Consider leveraging data protection features on Google Cloud

5

Monitor regulatory guidance and/or seek ongoing legal advice

Q & A

