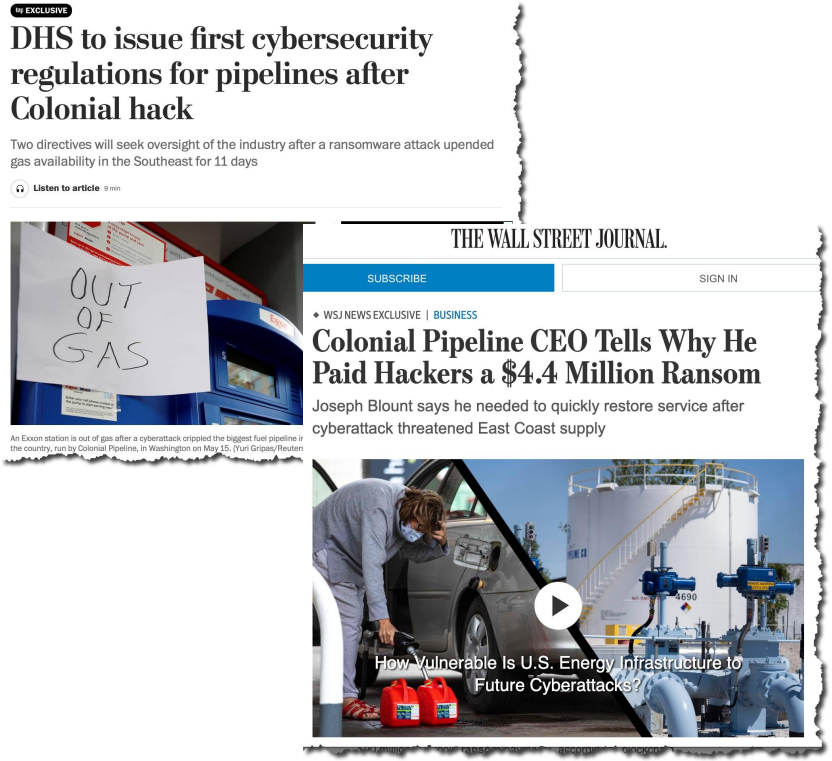
Google Cloud

Google Cloud's Approach

Gianluca Varisco

Security Practice Lead, France

Recent events



EXCLUSIVE

DHS to issue first cybersecurity regulations for pipelines after Colonial hack

Two directives will seek oversight of the industry after a ransomware attack upended gas availability in the Southeast for 11 days

Listen to article 9 min

An Exxon station is out of gas after a cyberattack crippled the biggest fuel pipeline in the country, run by Colonial Pipeline, in Washington on May 15. (Yuri Gripas/Reuters)

THE WALL STREET JOURNAL.

SUBSCRIBE SIGN IN

WSJ NEWS EXCLUSIVE | BUSINESS

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom

Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supply

- REvil ransomware used against 1,500 Kaseya customers (Jul ‘21)
- Bombardier, Inc., data leaked by CLOP ransomware (Feb ‘21)
- W&T Offshore hit by Nefilim that stole over 800 GB of personnel and financial data (May ‘20)
- Ragnar Locker ransomware used against Portuguese energy company Energias de Portugal and asked for 1,580 in BTC (Apr ‘20)
- WannaCry used against West Bengal State Electricity Distribution Company (India), Iberdrola (Spain), Petrobras (Brazil), Gas Natural (Spain), and PetroChina (China).

Attacker tactics *remain consistent*

Phishing

80%

of attacks start with a phishing email.

Targeted threats are extremely difficult to detect.

Email-borne threats

94%

of malware was installed via malicious emails and attachments.

Attackers rapidly change tactics to defeat email security measures.

Ransomware

21%

of Americans have have experienced a ransomware attack .

46% say their company paid the ransom.

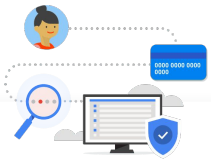
Five reasons to trust Google Cloud

1. You own and **control** your data, not Google
2. Your data and applications are **available when you need them**
3. Your **data protection is core** to everything we do
4. You can satisfy your **compliance** and **regulatory requirements**
5. You can progress towards your **environmental** and **social goals**

You can control how Google stores and accesses your sensitive data

Data Residency

Configure key GCP Services and Workspace Apps to store your data in the locations you select



Assured Workloads

Secure workloads to prevent deployments outside selected geo boundaries and limit access by Google support personnel based on predefined attributes

Access Transparency

Audit Google's access to your data and require explicit approval with justifications for support or engineering access

Cryptographic Control

Store and manage encryption keys outside Google Cloud and and only approve requests for decryption based on clear justifications

Confidential Computing

Preserve the confidentiality of your data while it is being processed and configure end-to-end ubiquitous data encryption for a verifiable control

Google’s vision of sovereignty is not only about data protection

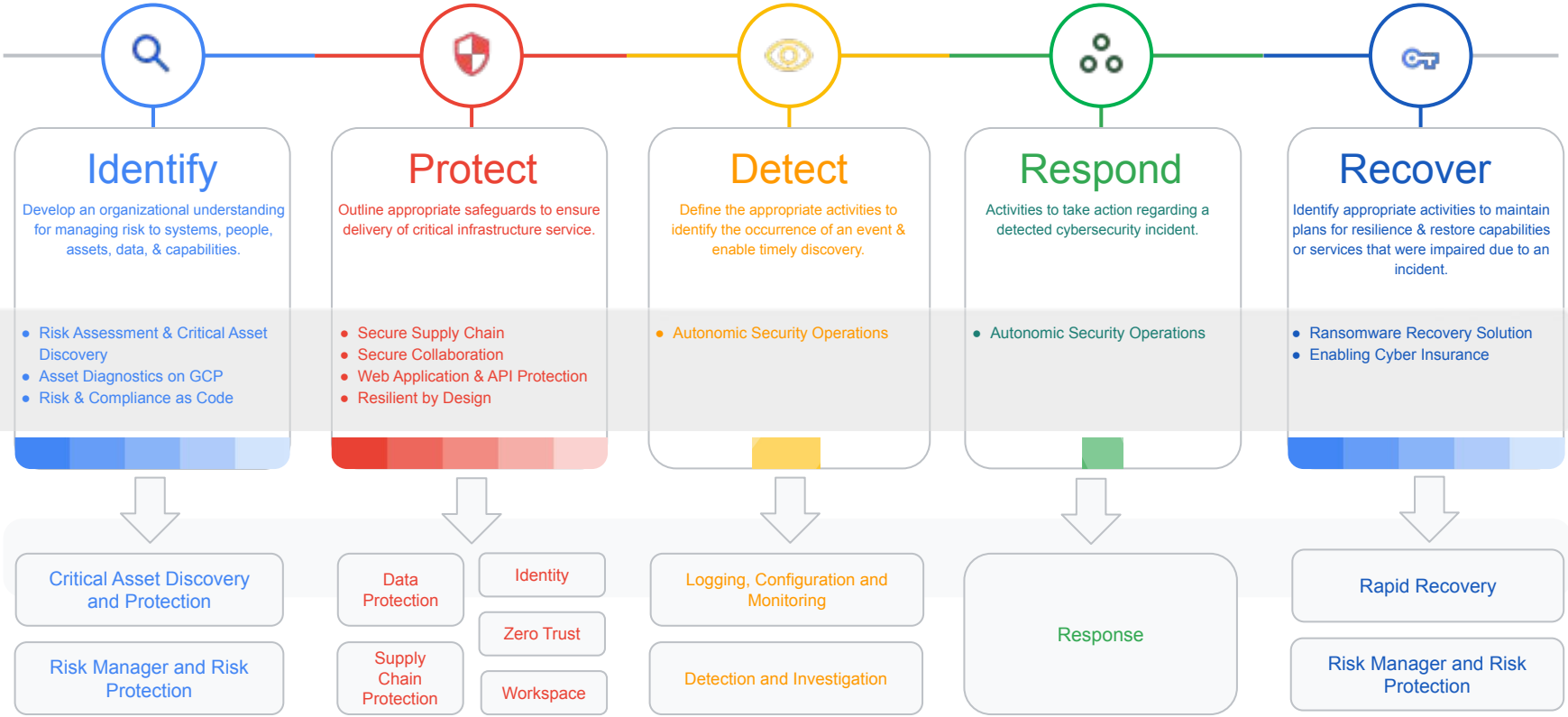
Google’s global infrastructure is resilient and scalable by design

Leverage the same built-in protection, and global network that Google uses

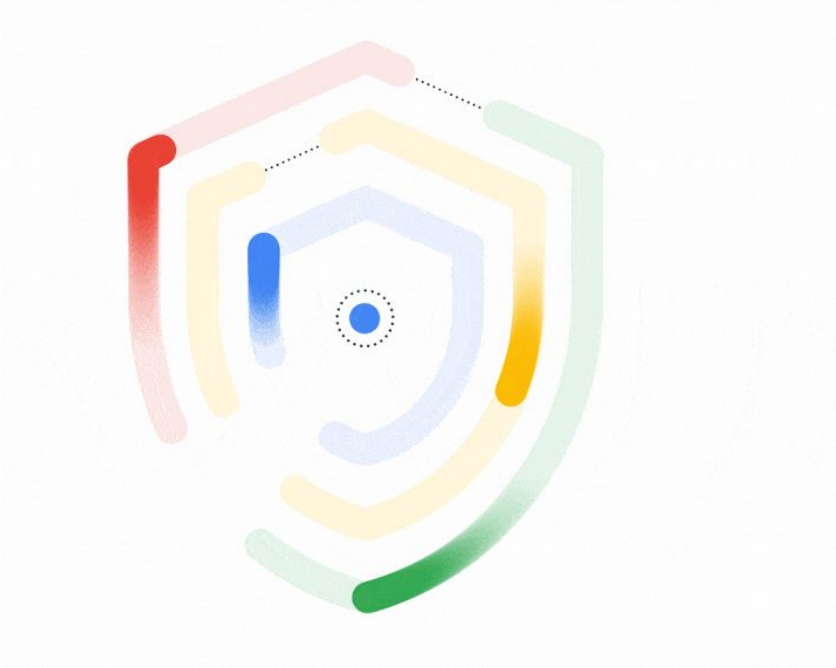
- 29 Regions, 88 availability zones
- 146 Network Edge Locations
- Thousands of Edge Nodes

100% Carbon Neutral

Google Cloud Security & Resilience Framework: 5 functions



Thank you !



Google Cloud