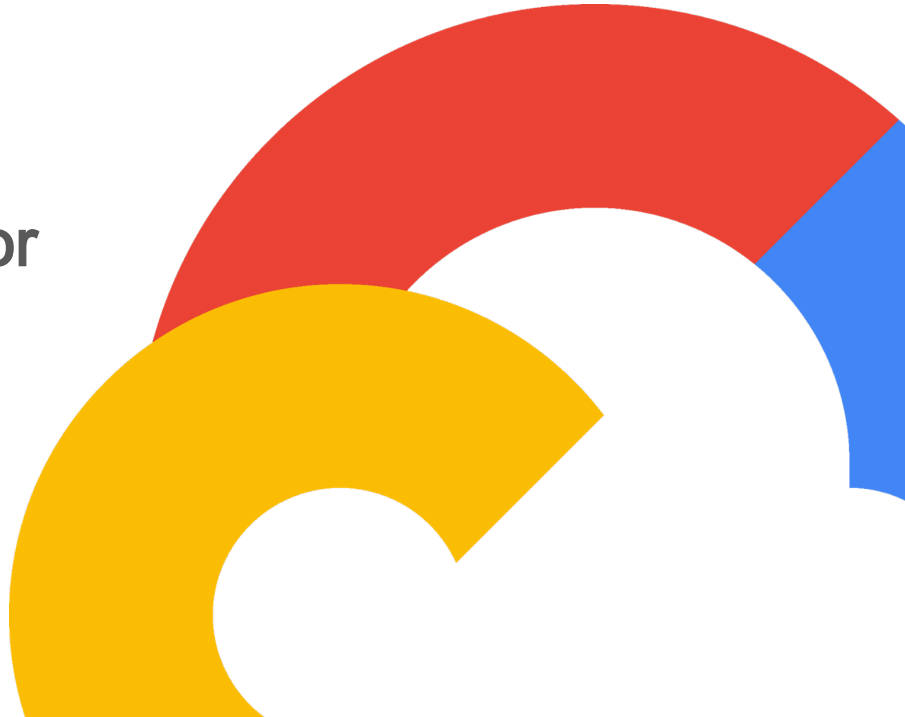
Fortifying the Cloud

Advanced Security Strategies for Global Enterprise Resilience



Iain Mulholland

Senior Director

Google Cloud CISO Security Engineering

Google Cloud

Google Cloud

A security bird's eye view

15 products,
each serving over half a billion users

Google Cloud's global network

42 regions

127 zones

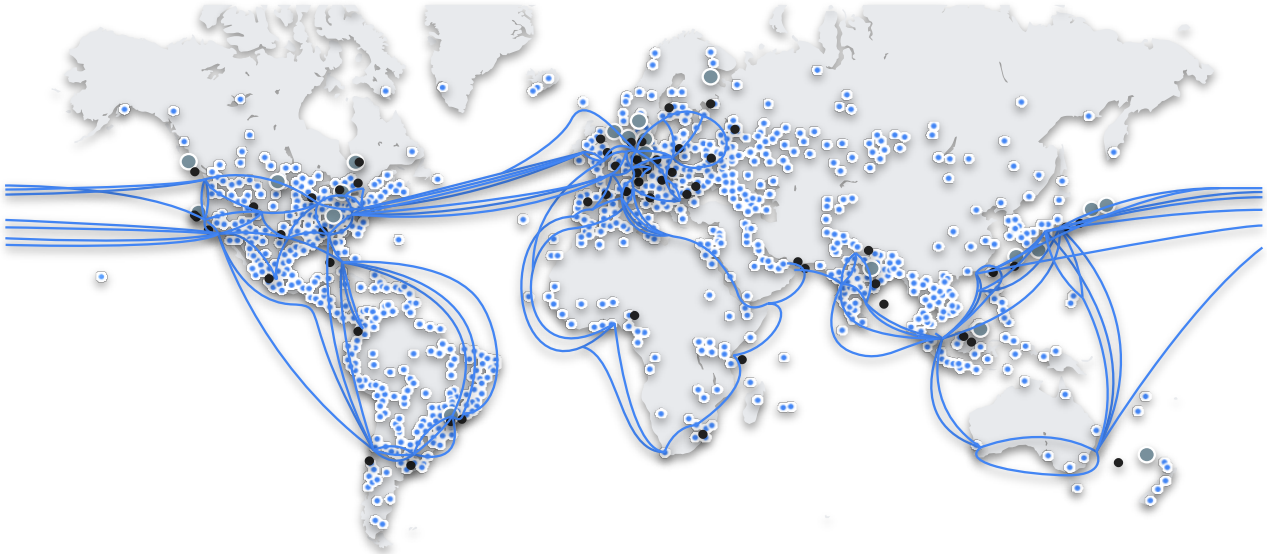
202 network edge locations

33 subsea cables

2+ million miles lit fiber

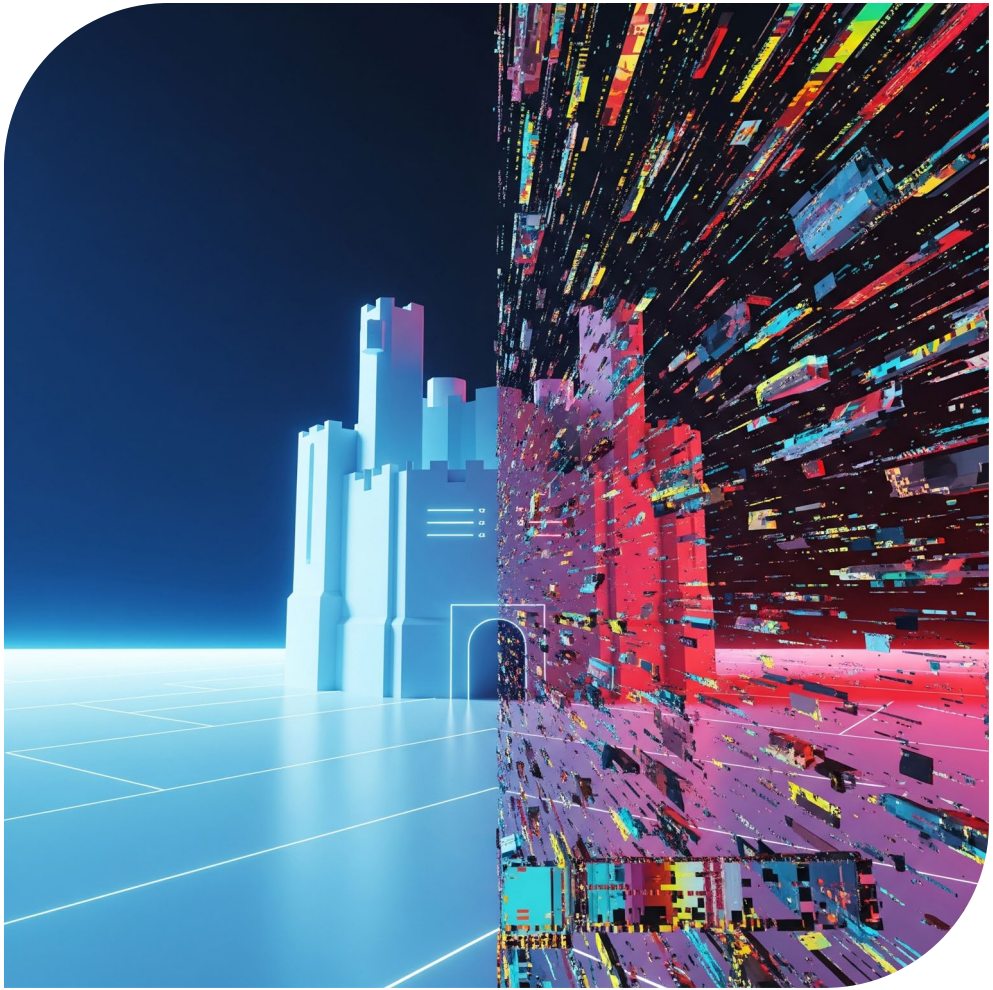
200+ countries & territories

3000+ Media CDN locations



Driving business resilience with cloud security

Security Theory vs. Reality



Cloud cyber resilience

Enhanced Scalability

- Scale resources, rapidly
- Maintain availability, despite attacks
- Pay for what/when you need

Advanced Security Infrastructure & Expertise

- Specialized security teams
- Sophisticated threat detection and prevention
- Regular updates and patching
- Shared Fate model

Robust Backup and Disaster Recovery

- Geographic redundancy
- Automated backup and recovery
- Immutable backups

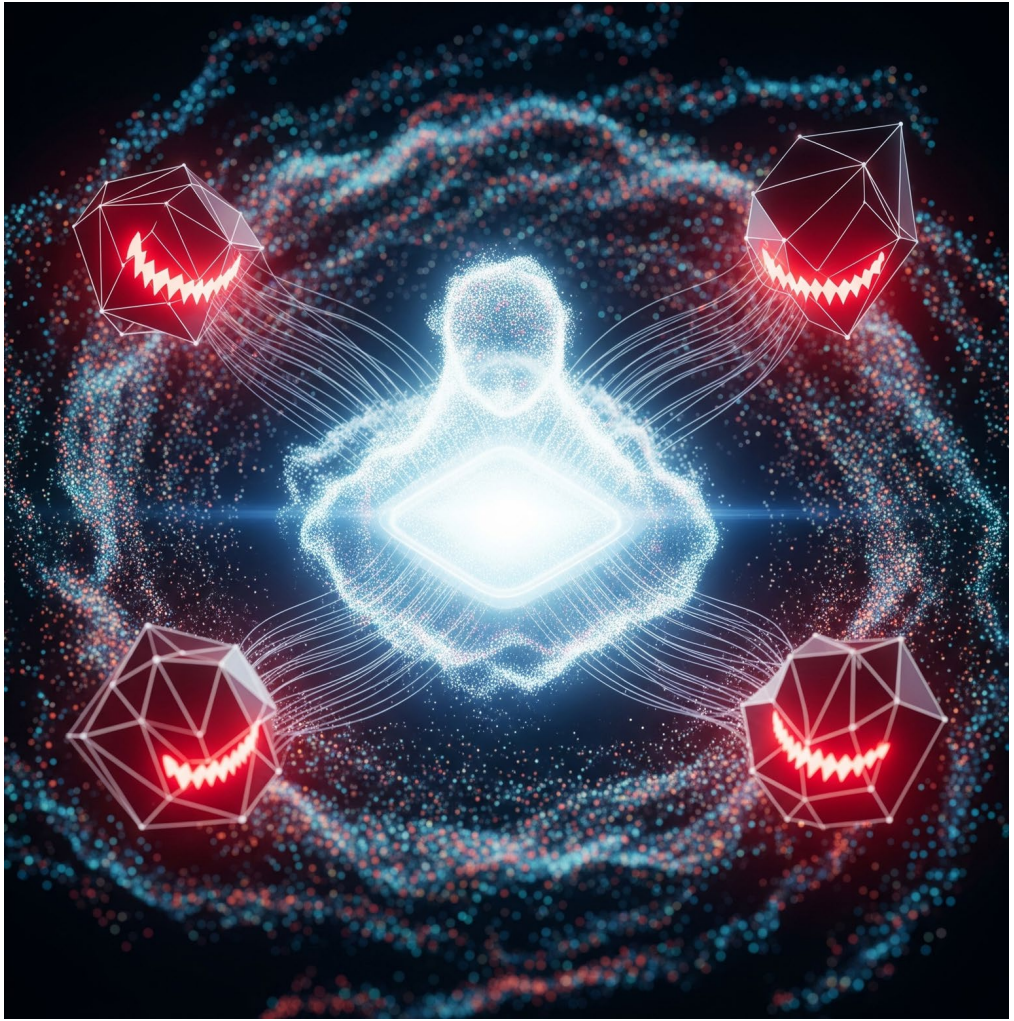
Improved Data Security & Compliance

- Data encryption
- IAM
- Compliance certifications

Managing risk in diverse geographies

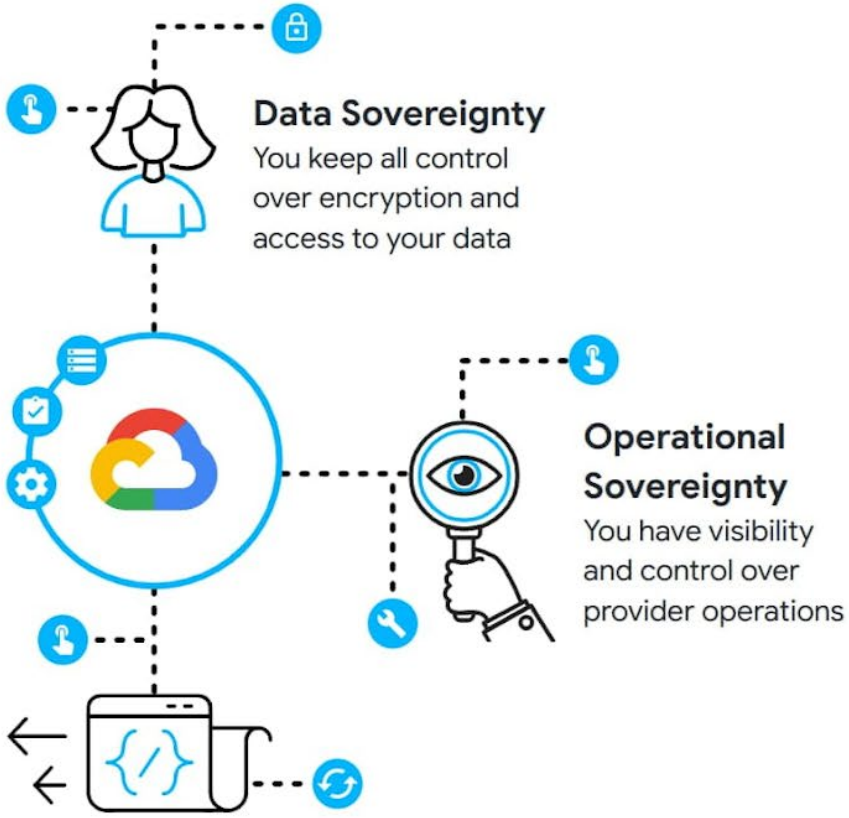
Threat Models

- Threat models are undervalued in cloud security
- Threat models differ vastly across diverse geographic locations
- Threat models are crucial to the security theory vs. reality tradeoff.

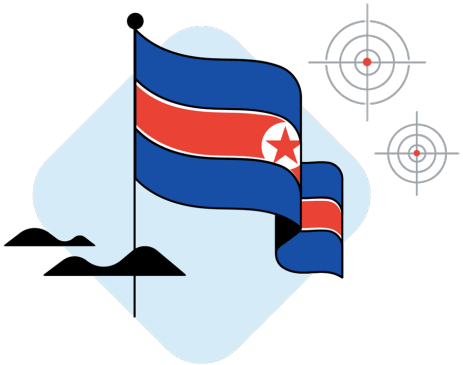


Three Pillars of Sovereignty

in Google Cloud



When global risk comes to you



THE WALL STREET JOURNAL.

North Korea Infiltrates U.S. Remote Jobs—With the Help of Everyday Americans

If your business **isn't** seeing these risks, it's **not** because you're **safe**. It's because **you're not detecting them**.

Scaling security with AI

Three AI risks facing CIOs and CISOs

Software lifecycle risks

Ensuring AI models and applications adhere to software security principles to mitigate vulnerabilities

Data governance risks

Organizing and classifying data sets used in AI training and testing to prevent leakage or tampering

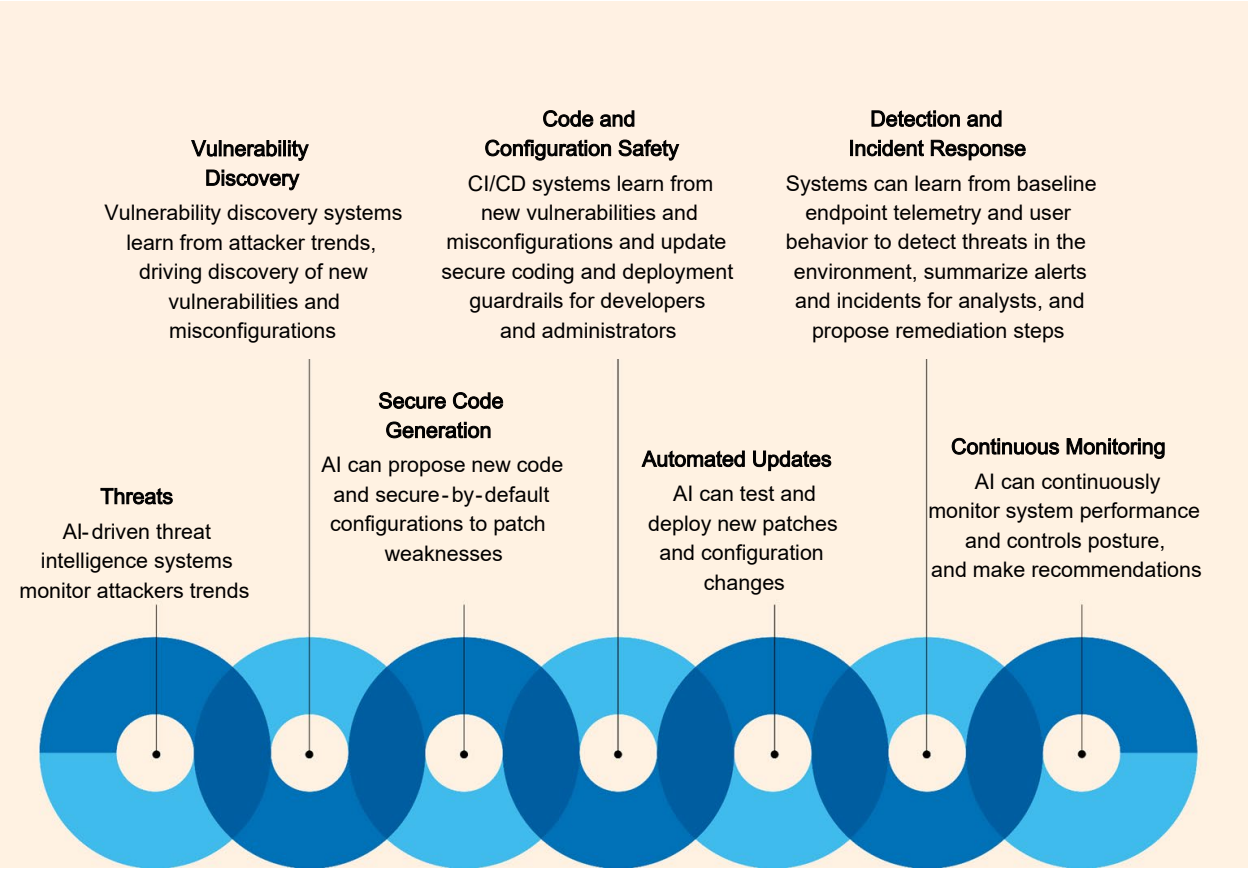
Operational risks

Putting checks and balances in place to prevent AI incidents from spilling over into business risks

AI is disrupting the cybersecurity balance by lowering the bar for attackers while simultaneously drastically scaling defenders' capabilities.

There are countless use cases for GenAI in defense

AI experts can knit together these systems and workflows to create self-healing networks.



We've used AI in our platform defenses for a decade

Google Workspace

100 million

spam messages are blocked from reaching customers daily through Gmail using **TensorFlow**

99.9%

of phishing attempts are blocked by Gmail

Google Play Protect

200 billion

apps scanned daily by machine learning to detect and block malicious content or behaviors

515,000

malicious apps detected and blocked by real-time scanning

AI: Defenders' Advantage

Vulnerability Discovery : Where AI is right now

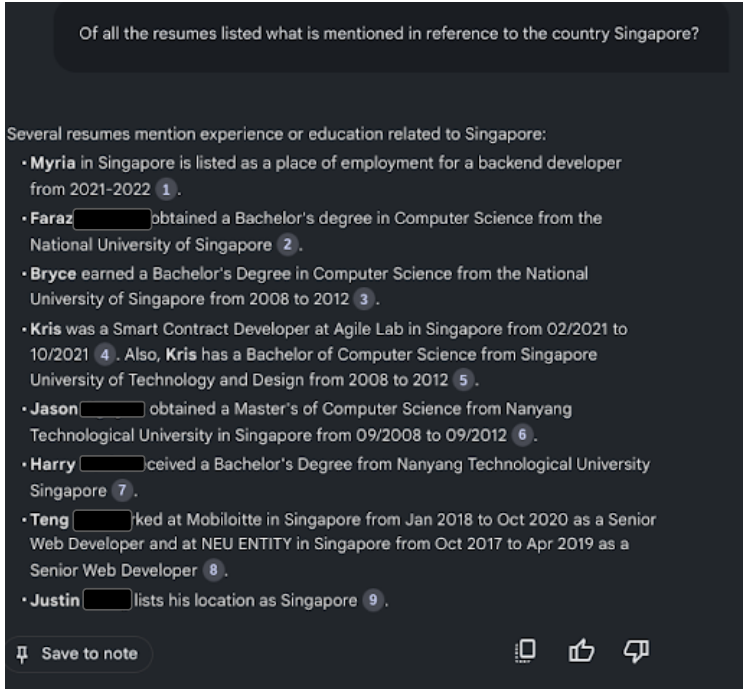
- Performing at beginner level on CTF challenges

- Identified real-world vulnerability in SQLite

North Korean IT Worker Resumes

NotebookLM analysis of resumes by DPRK IT Workers showed:

- A single DPRK IT worker often handles multiple personas
- Those personas sometimes share resume details (education, work experience, etc)
- These overlaps can be used to cluster IT Worker resumes, aiding in attribution



AI powers vulnerability prioritization

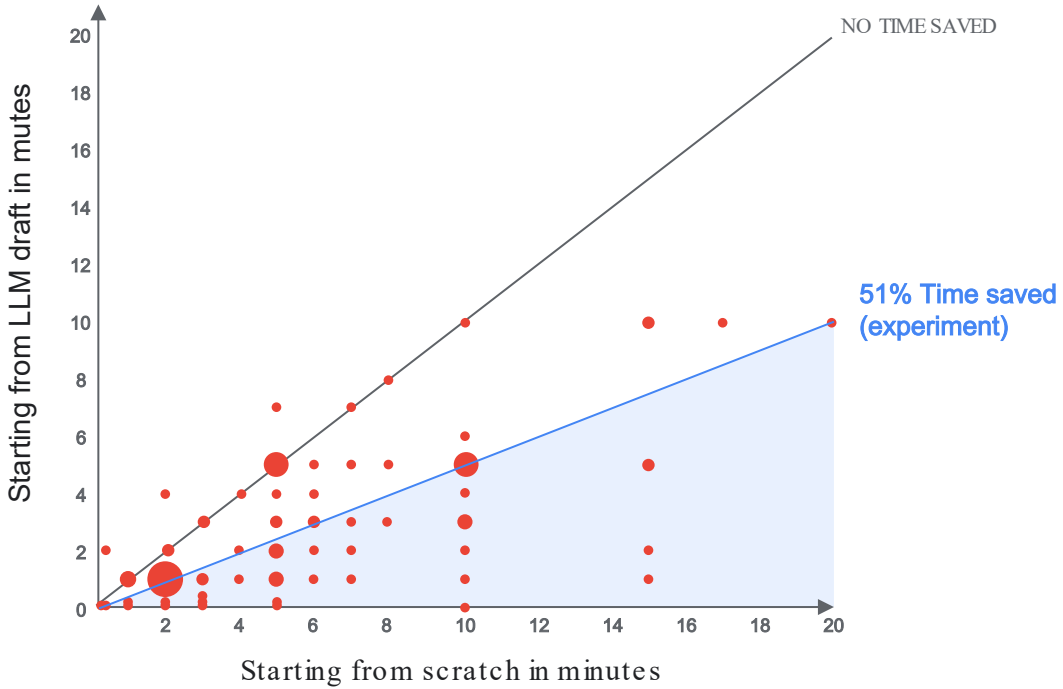
01 — Scales vulnerability analysis effectively

02 — Enhances risk assessment by identifying patterns of vulnerabilities

03 — Automates classifying and analyzing large vulnerability volumes quickly

04 — Improves vulnerability prioritization for focused remediation

LLM are able to help incident teams write incident summaries 51% faster



AI For Cyber Defenders Now

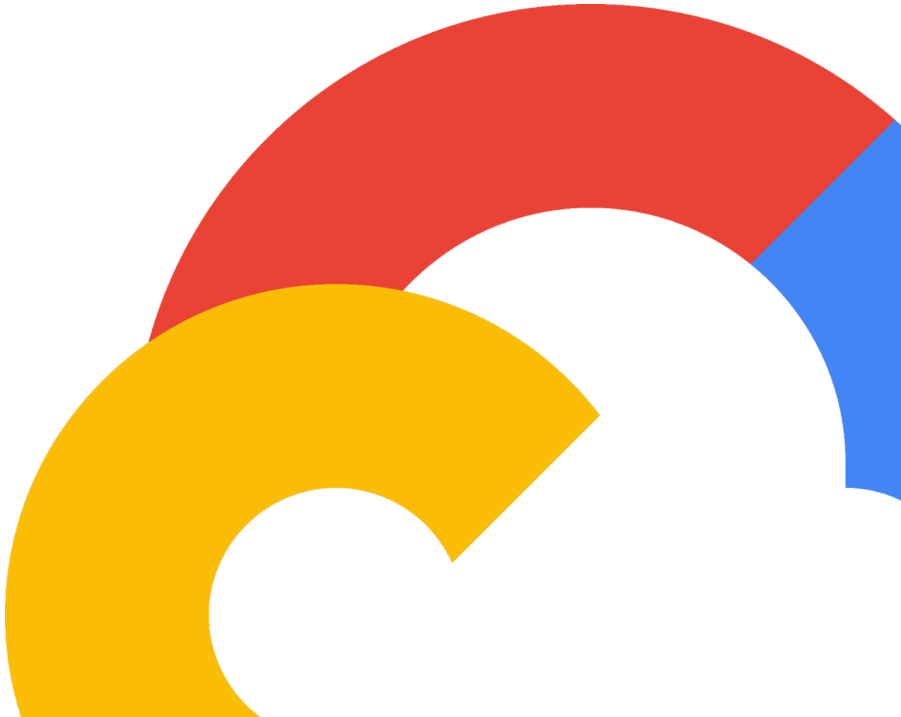
- AI scales defender capabilities significantly – and drastically.
- AI helps with code safety, threat detection, and continuous monitoring.
- AI improves vulnerability discovery.
- AI can accelerate Security Analysts work
- Gemini safety and security measures can restrict content that would enhance adversary capabilities.

Cyber Resilience

Managing Geographic Risk

Scaling Security with AI

Thank you



Google Cloud