Google Cloud

A comprehensive strategy for managing sensitive data in the cloud

Security Summit

Solving for the future of security.

05/17/22

Nelly Porter

Group Product Manager

Google Cloud

Matthew Presson

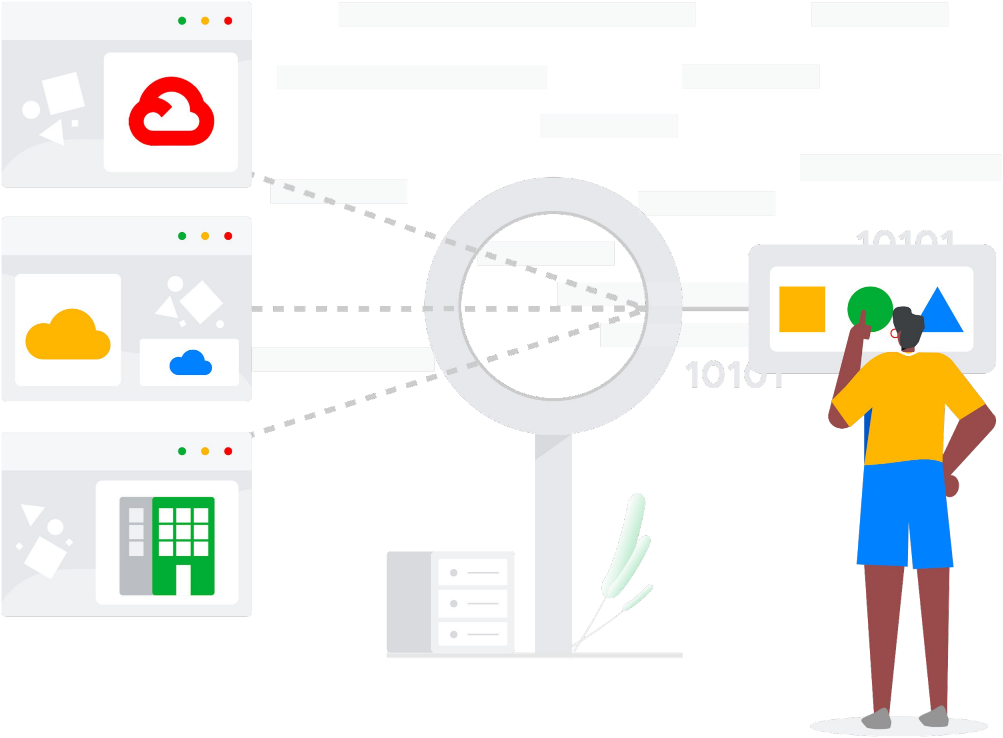
Lead Security Architect,
Product Security

Bullish

Data powers your business

Data is one of your greatest assets

Data can also be one of your biggest risks



Data Protection
Challenges

Key concerns for customers

- How do I protect my sensitive data and my IP?
- How do I protect my clients' and users' data?
- How do I stay compliant with data protection regulations?
- How do I collaborate with other companies processing their sensitive data?

Understand your data risk

Low

Moderate

High

Example:
Public Data

Example:
Business sensitive data

Example:
Secret data / Intellectual Property

Defense In Depth

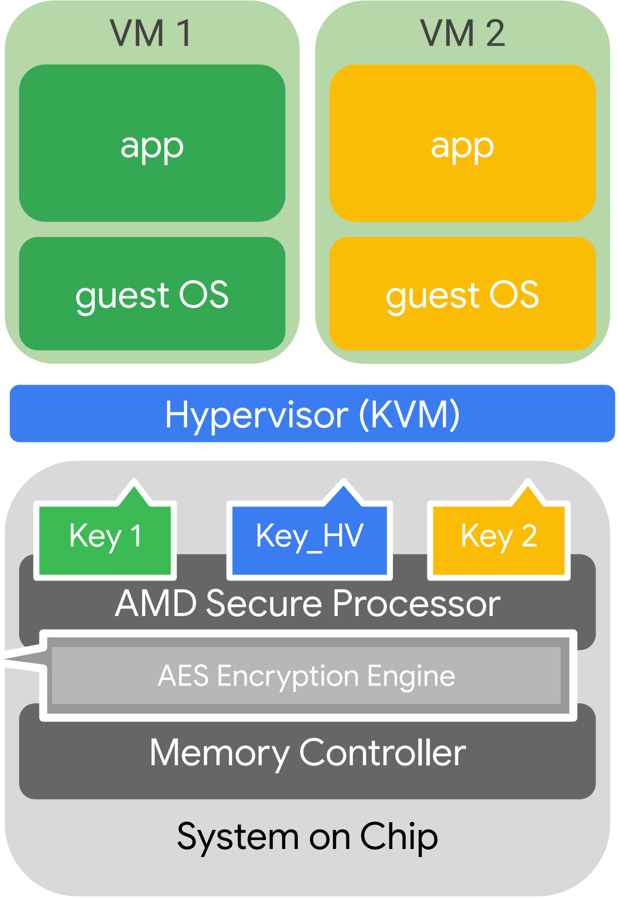
Limit the visibility and access to sensitive data

Encryption is the key to safeguard sensitive data

- Encryption at rest
- Encryption in transit
- **What about processing sensitive data?**

What is Confidential VM?

- Just like a regular GCE VM
  - Anything that runs on VM runs on CVM
- Data encrypted while in-use
  - Memory encrypted, decrypted only on CPU chip
  - A key per VM
    - Random, ephemeral, generated by HW
    - Not extractable from HW



Google Confidential Computing protect from

01

Accidental data **leakage**

02

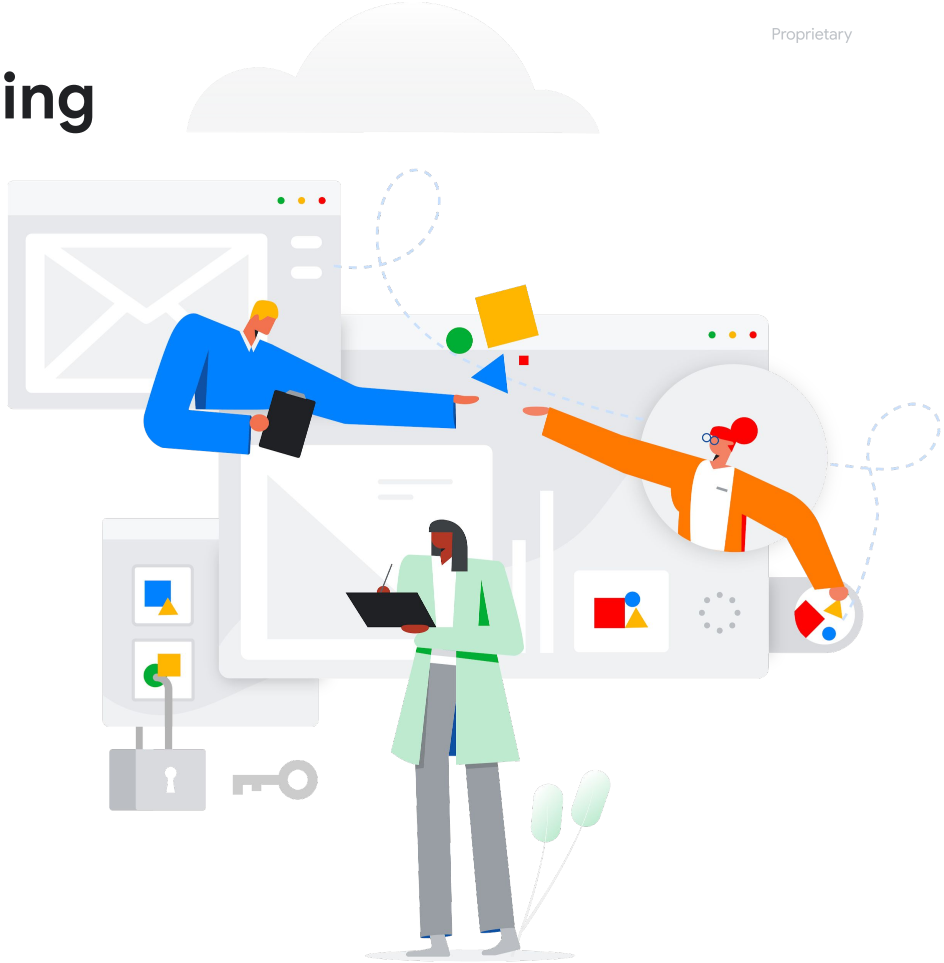
Malicious administrators

03

“Curious” neighbors

04

Cloud infrastructure bugs



Confidential Computing

example use cases

Collaborate securely without trusting

CC opens a new door to collaborative analysis and modeling

Protect PII and adhere to regulations

Key management, client data protection, multi-party analytics

Privacy in Blockchain transactions

There is no going back in the blockchain - make blockchain calculations private

Customer Spotlight - Bullish

Bullish - A new breed of Exchange

Google Confidential Computing

Securing sensitive data and workloads in the cloud — our handling of digital assets, from deposit to withdrawal.

Our Security Requirements
Data is protected in-transit, at-rest, and in-use
Fully-verifiable execution stack
Control and provide our own disk images
Control and provide our own verification keys
Rollback protections
Cryptographically-verifiable software and services
Defaults to a fail-secure state
Easy to implement

Google Cloud Summit

Thank you for joining