RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: EXP-F02

Google on BeyondCorp: Empowering employees with security for the cloud era

Jennifer Lin

Director, Product Management, Security & Privacy
Google Cloud

What is BeyondCorp?

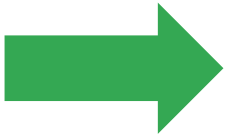
Enterprise security model based on 7+ years of building zero trust networks at Google

Shifts access controls from the network perimeter to individual devices and users

Allows employees to work more securely from any location without the need for a VPN

Increasingly embraced by enterprises and mobile ecosystem

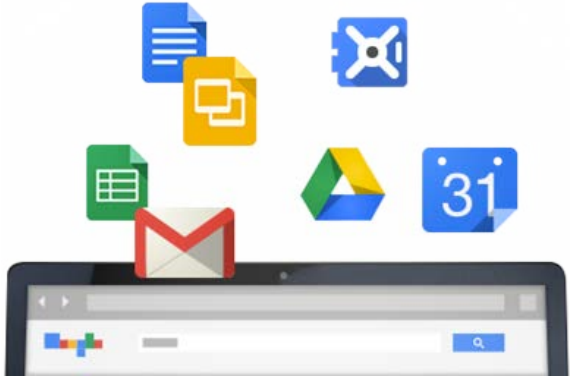
Enterprise IT has changed



On-Prem resources
Well-defined perimeter
Network-based access controls

Cloud-based resources
Dynamic perimeter
Intelligent access controls

User experience has changed



Dynamic applications

On any device

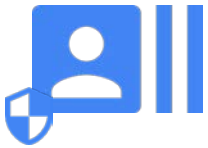
Access policy goals

I want my application to be:

- Accessed only by financial employees
- From well-managed client devices
- In home country
- Using strong user authentication
- And proper transport encryption

How do you do it?

User- and service-centric access controls



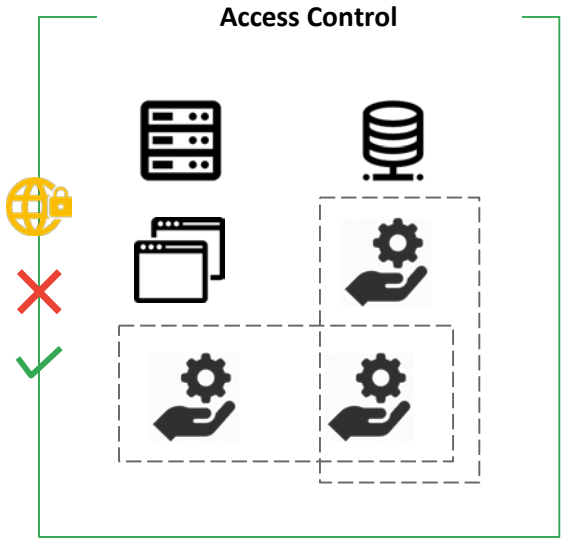
Cloud Identity Services
Provision & Authenticate
Users and Devices

How

Where

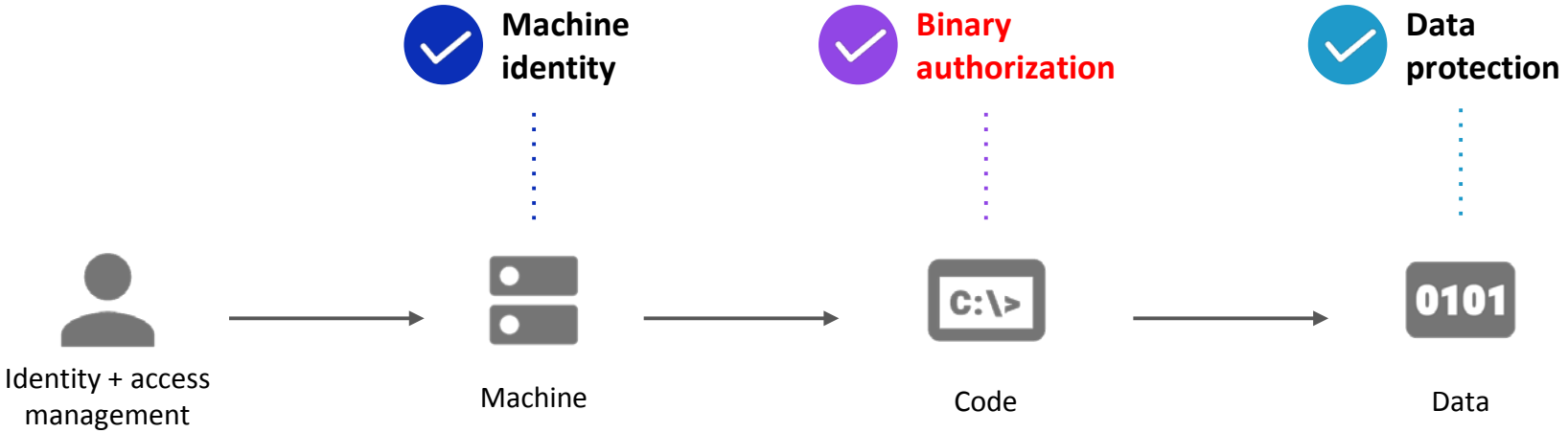
When

Smart Access Proxies
Context-aware policies



VPC Service Zones

Chain of Trust



Right code, running on the right machine, authorized by the right identity, accessing the right data at the right time

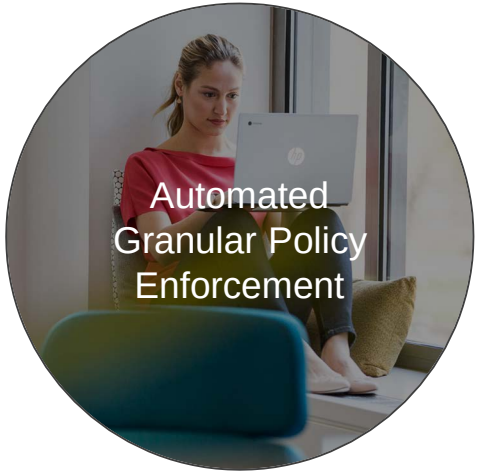
Trusted platform + granular policies

Services and Apps

User

Device

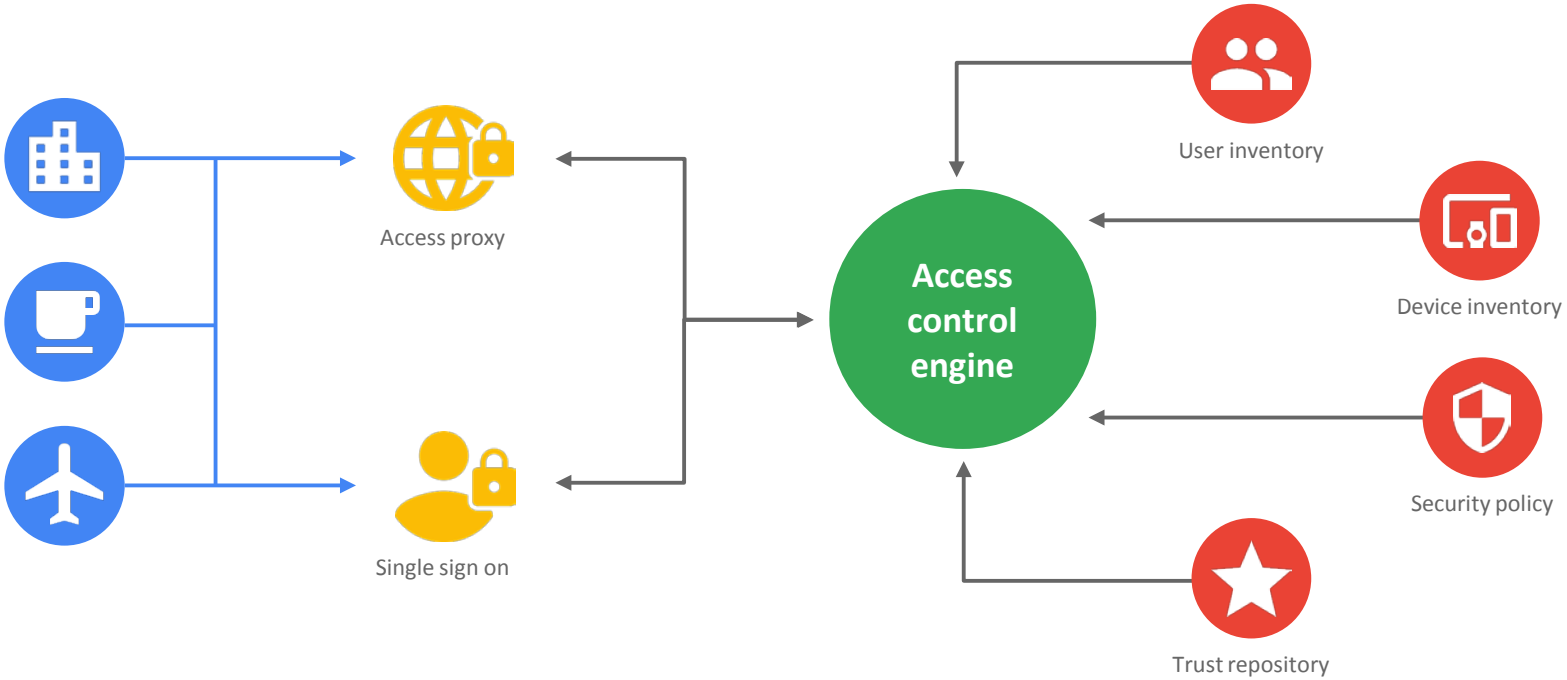
Platform with HW Root of Trust



Core principles of BeyondCorp

1. Access to services is granted based on what we know about you and your device
2. All access to services must be authenticated, authorized and encrypted
3. Enterprises define tiers to enforce access to applications

BeyondCorp software framework



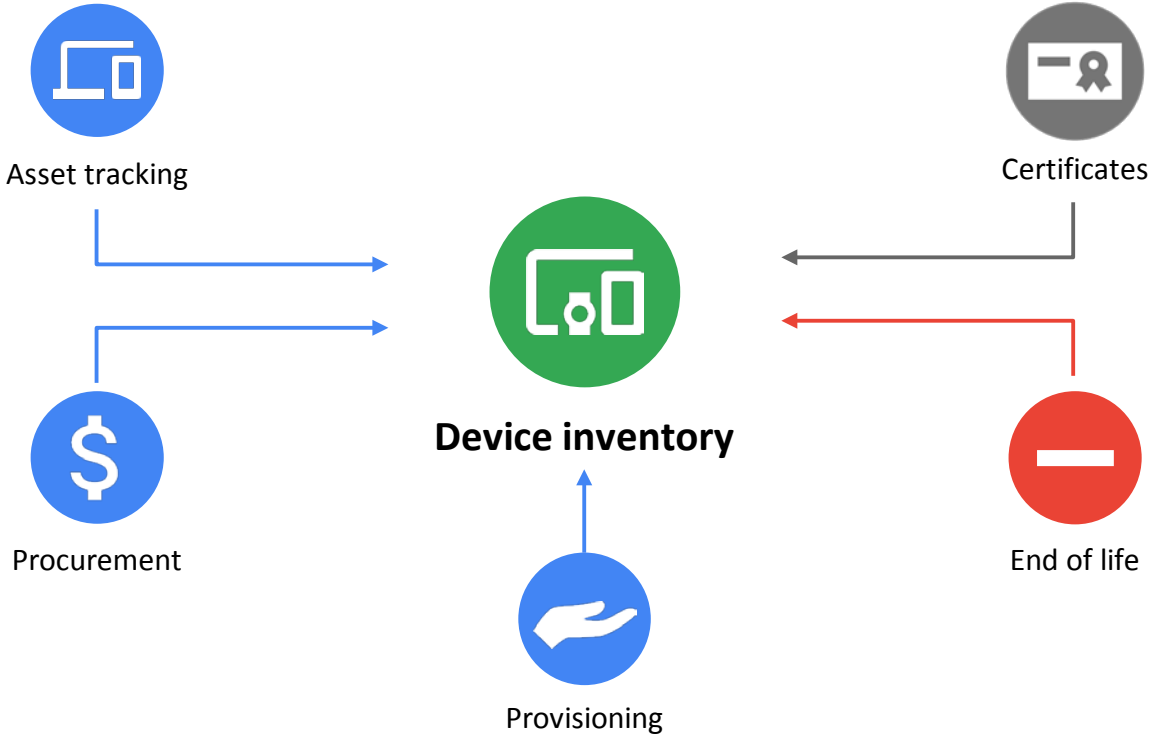
Securing the user: security keys

Second factor designed specifically to defeat phishing

Like smart card re-designed for web
- One key for multiple sites & accounts
- Simple UX: Insert & press button

Google login uses open FIDO standard
- Inter-domain privacy by design
- FIDO support in Chrome today,
  other browsers coming soon ...

Establishing device trust



Securing the device
Chrome & Android enterprise

android enterprise recommended

www.android.com/enterprise/recommended

chrome enterprise

Devices
Max protection and reduced risk with hardware security

Firmware
Verified Boot

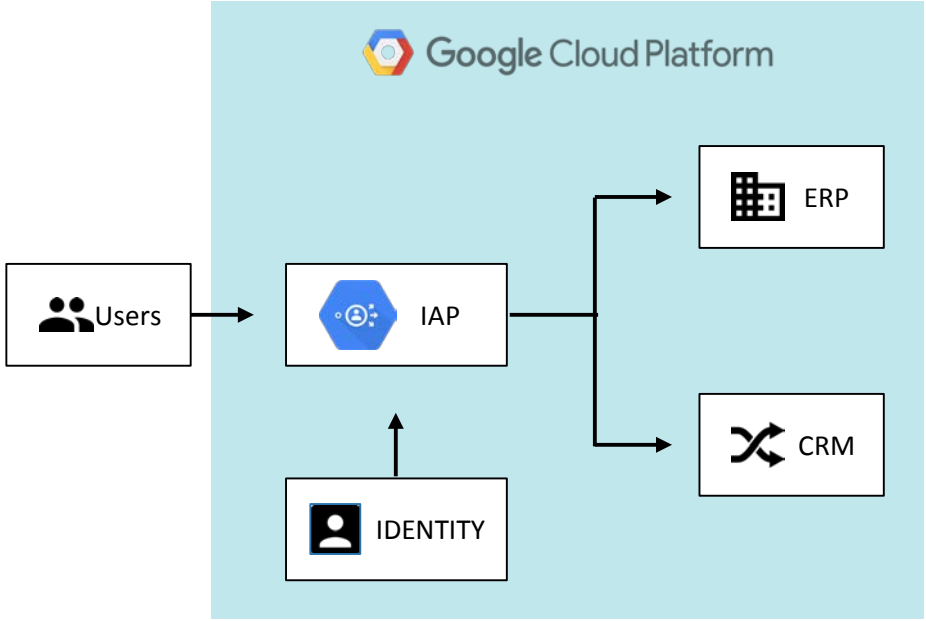
OS
Secure from boot up to shutdown with privilege separation, sandboxing, encryption and auto updates

Apps
Server-side malware detection

Browser
Safe browsing and Sandboxing tabs

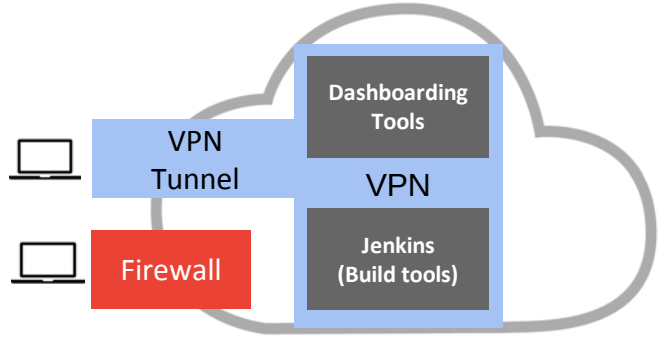
Productizing BeyondCorp
Identity-aware proxy on Google Cloud Platform

- Add access controls to those applications on GCP based on an end-user's identity.
- Shift access controls from the network perimeter to identities and attributes.
- Centralized, manageable layer where authorizations checks can be applied.

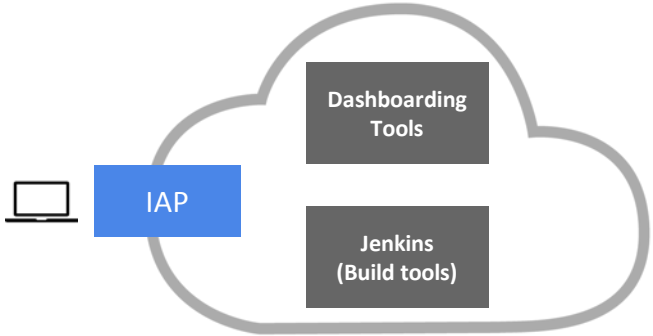


Whisper's BeyondCorp architecture

Before



After



- Applications run in containers (GKE)
- Used firewalls to protect access to internal employee applications
- VPNs were setup for end-user access
- Difficult to expose tools to the right employees

- Enabled IAP in front of applications in GKE
- Added user groups who can access the application

BeyondCorp papers

- An overview: *A New Approach to Enterprise Security*
- How Google did it: *Design to Deployment at Google*
- Google's front-end infrastructure: *The Access Proxy*
- Migrating to BeyondCorp: *Maintaining Productivity While Improving Security*
- The Human Element: *The User Experience*

https://cloud.google.com/beyondcorp/

Q&A

Thank you