apigee

How Secure Are Your APIs?

Kevin Ford
Apigee | Google Cloud

Today’s Presenter

Kevin Ford

Google Cloud Platform Sales Engineer • kevinford

APIs Are Under Attack

- Standard Interface
- Consistent Resource model
- Easy Programmability
- Published Documentation
- Mobile App Proliferation

API Attacks That Made the News

“An Instagram Hack Hit Millions of Accounts, and Victims’ Phone Numbers are Now for Sale.”

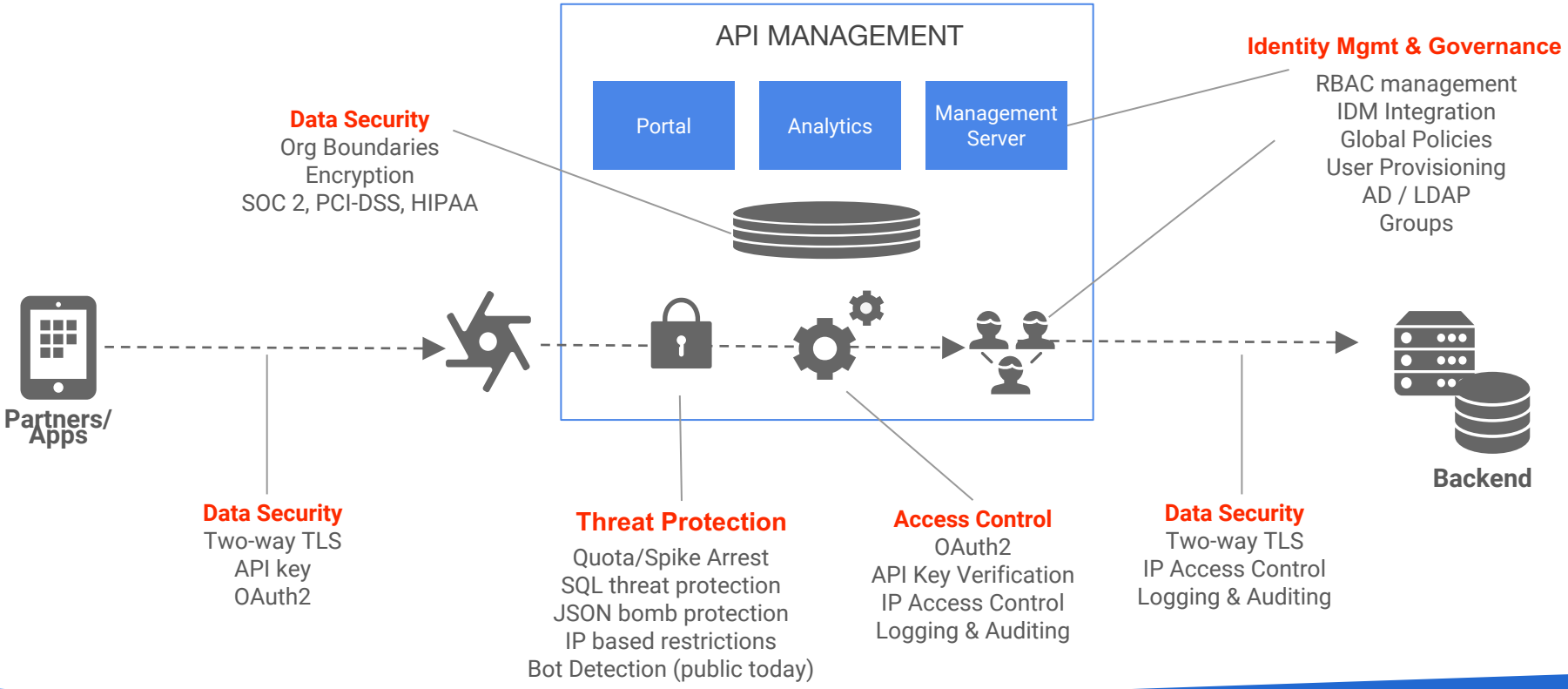
“No Butts About It, Some Pinterest Users Have Been Hacked.”

“Three Million Moonpig Accounts Exposed by Flaw.”

“Nissan Leaf Hackable Through Insecure APIs.”

“Thieves Stole Taxpayer Data from IRS ‘Get Transcript’ Service.”

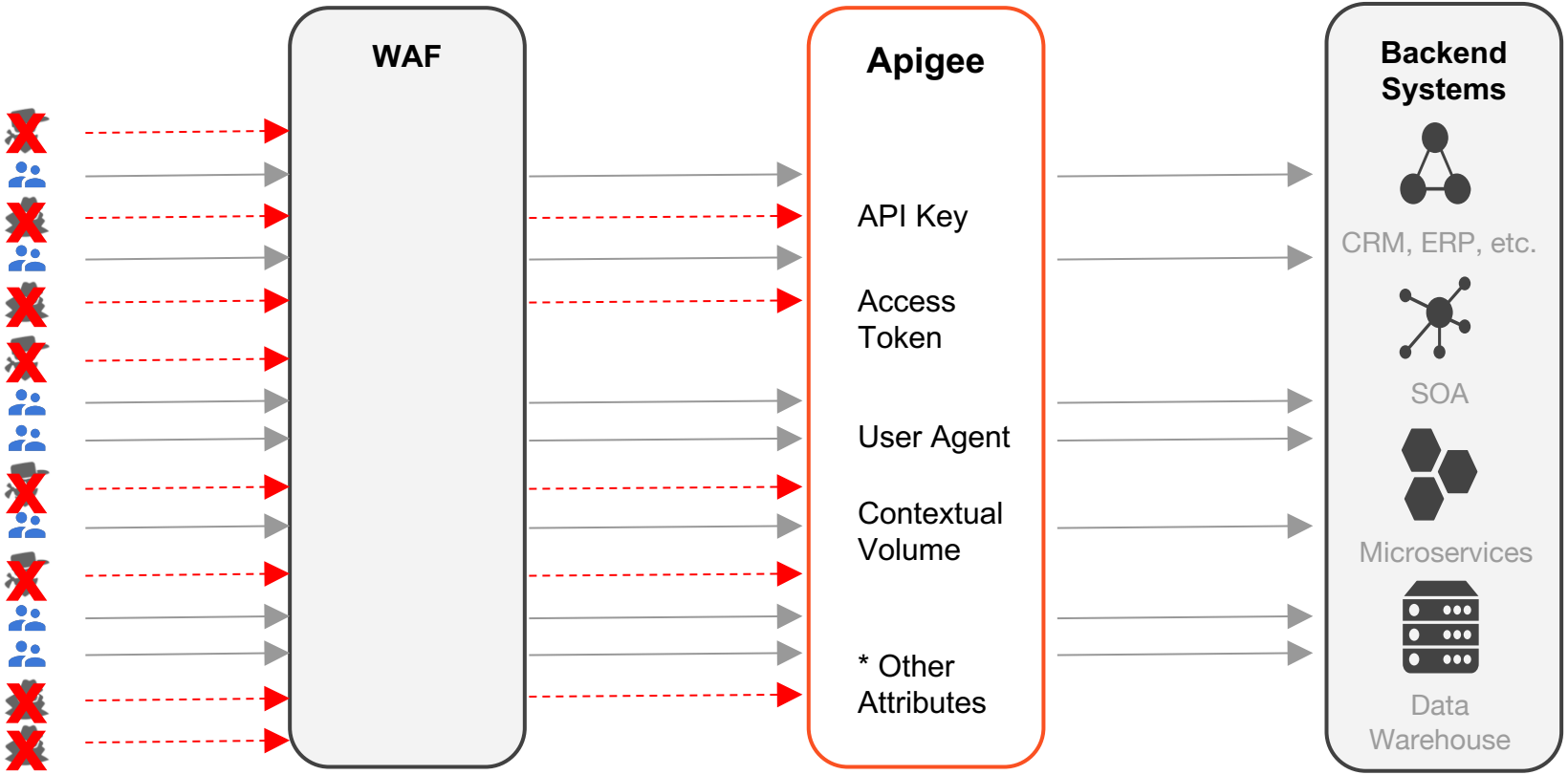
Layered Security and Governance



Signs of Attack on APIs

- Persistent attempts from same IP
- Unusual error rates
- Suspicious client requests
- Data crawling
- Key harvesting
- Activity bursts
- Geographical patterns
- Brute force attacks
- Bots probing for API security weakness
- Competitors scraping price data
- Credential stuffing
- Abuse of guest accounts
- Bot traffic skewing analytics and KPIs
- Using compromised API keys to access private APIs
- Dictionary-type attacks
- Man-in-the-Middle attacks

Why Traditional Approaches Fail



Solution: Dedicated API Security Infrastructure

APIs need a dedicated security infrastructure to protect against the increasing threat of malicious behavior.

Once is happenstance. Twice is coincidence. The third time it's enemy action.

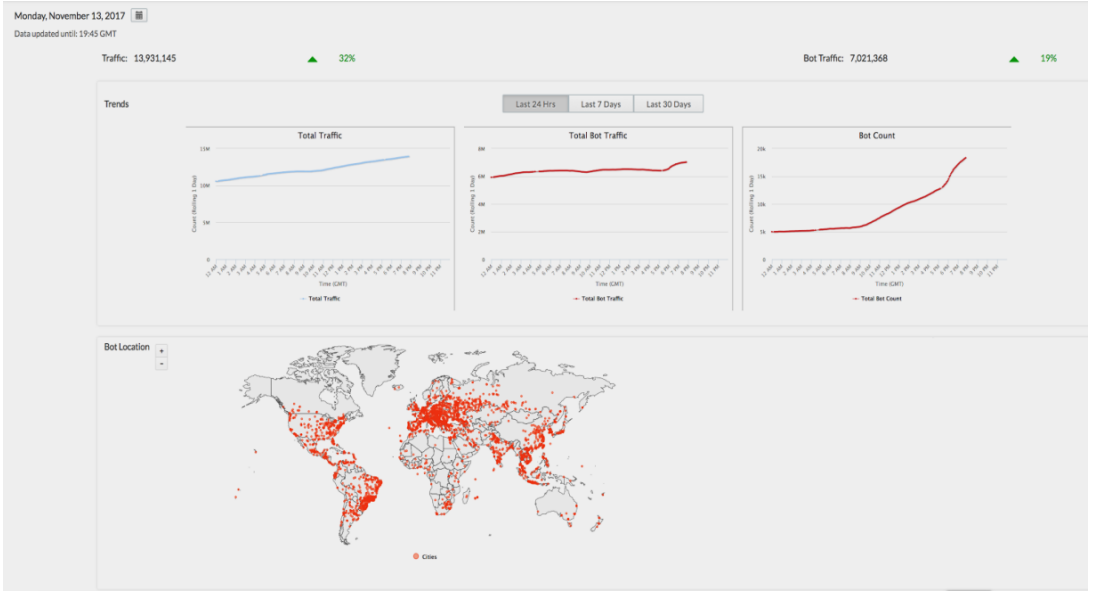
Ian Fleming

Apigee Sense

Intelligent behavior detection to protect APIs from attack.

How does Apigee Sense Protect your APIs?

- Purpose built for APIs
- Uses behavior-based rules and algorithms
- Detects anomalous behavior patterns at the API layer
- Complete closed-loop system Takes actions based on rules specified by administrators



Intelligent

Apigee Sense

- Studies call patterns from API metadata
- Algorithms detect anomalies
- Analyzes customer traffic over time

Behavior Detection

Apigee Sense

- Detects behavior
- Finds anomalies
- Proactively identifies threats
- Examines metadata
- Characterizes requests
- Flags suspicious requests
- Administrators apply desired action for a given behavior

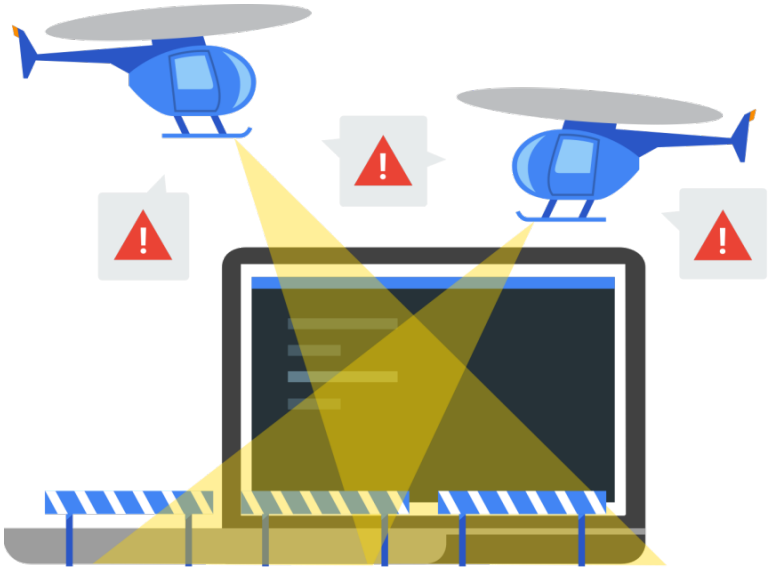
Brute Force Attacks

Hackers

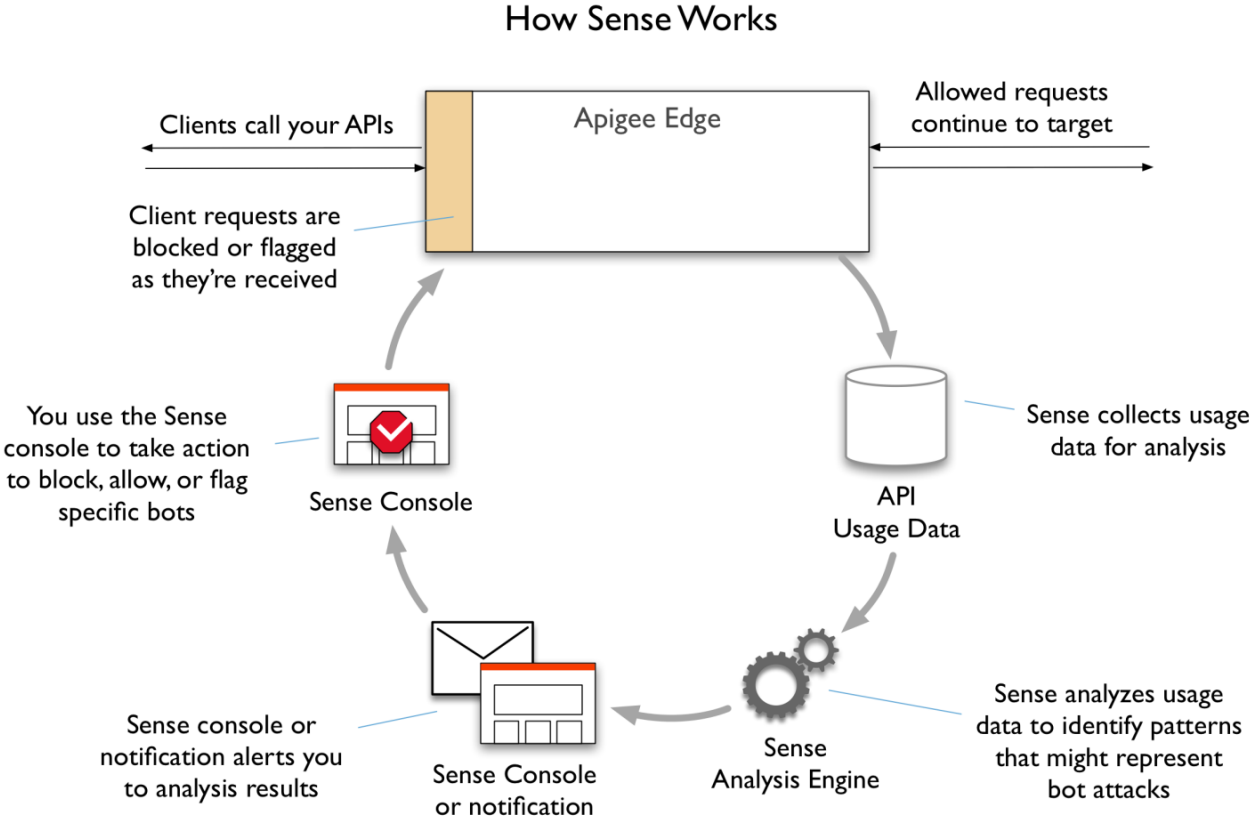
Protect APIs

Apigee Sense

- Alerts teams
- Tags or blocks
- Takes Action based on admin policies
- Closed-loop system



Closed Loop Protection:

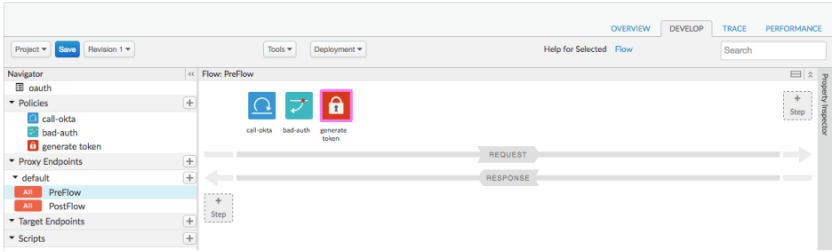


Flexible Protection

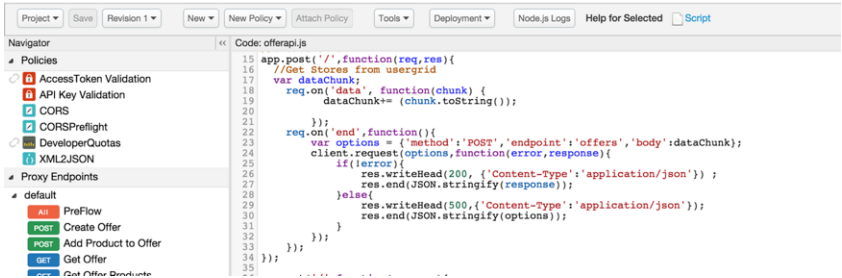
Honeypot, Conditional Routing,
Callouts, Logging

```
01100
10110
11110
```

Handle Flagged Requests via Configuration



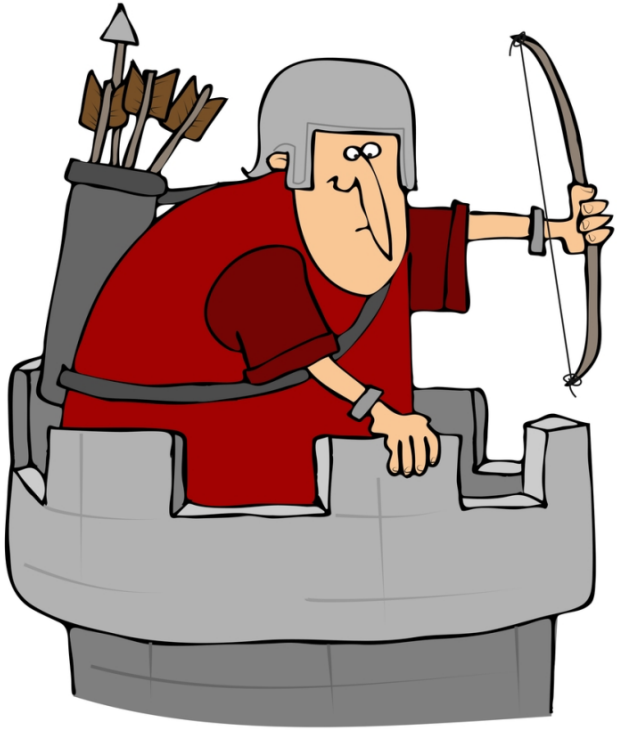
Handle Flagged Requests via Code



A Secure Solution

A Secure Solution… With Extreme Visibility

The Best Defense Is A Good Offense



apigee

Questions?