

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.”**



**moonpig.com**

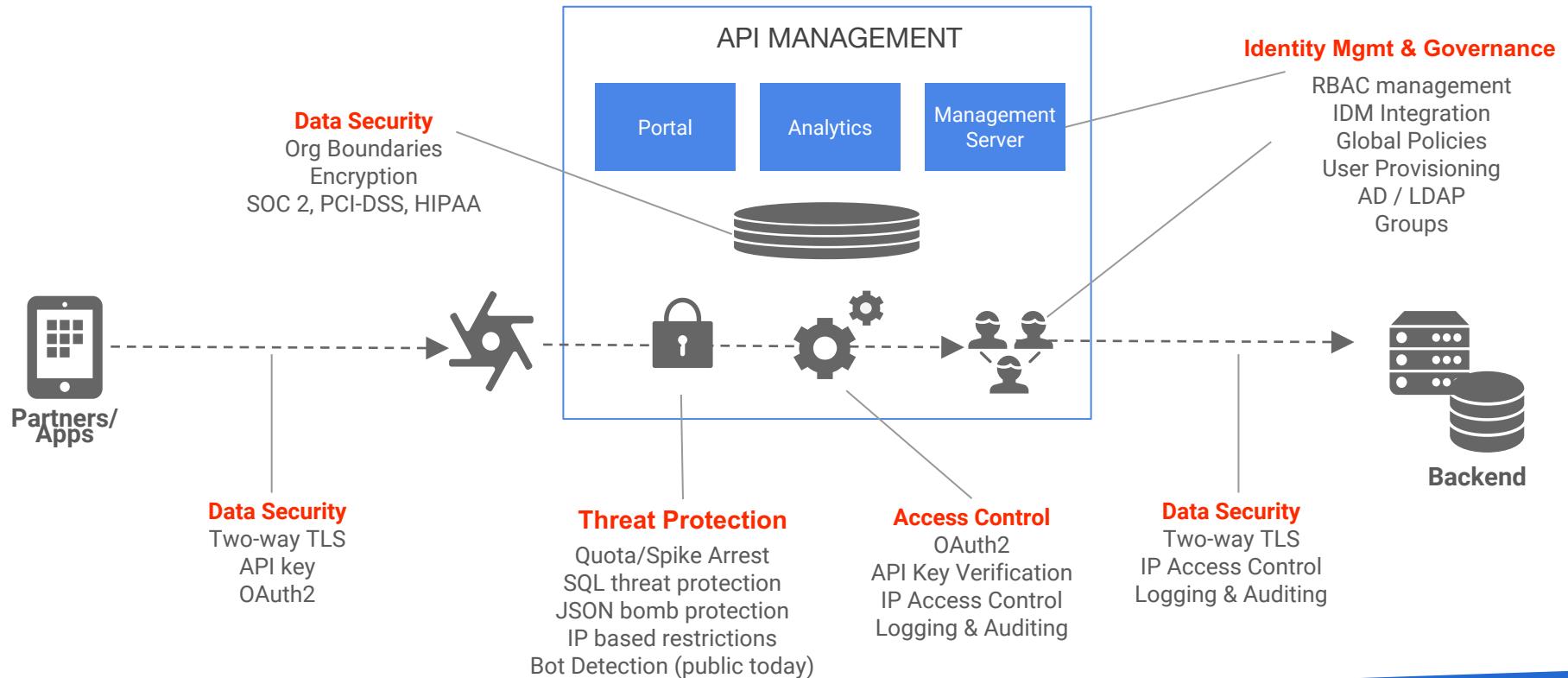


**“Nissan Leaf Hackable Through Insecure APIs.”**

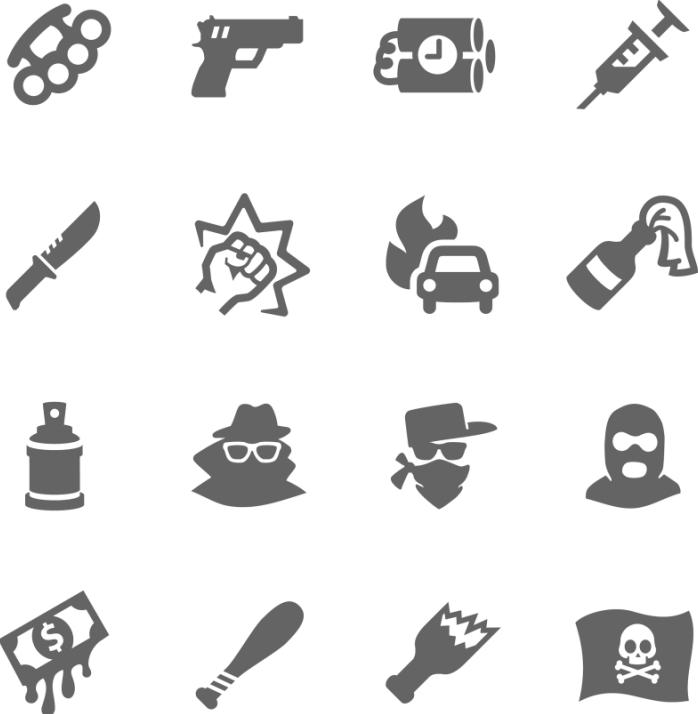


**“Thieves Stole Taxpayer Data from IRS ‘Get Transcript’ Service.”**

# Layered Security and Governance

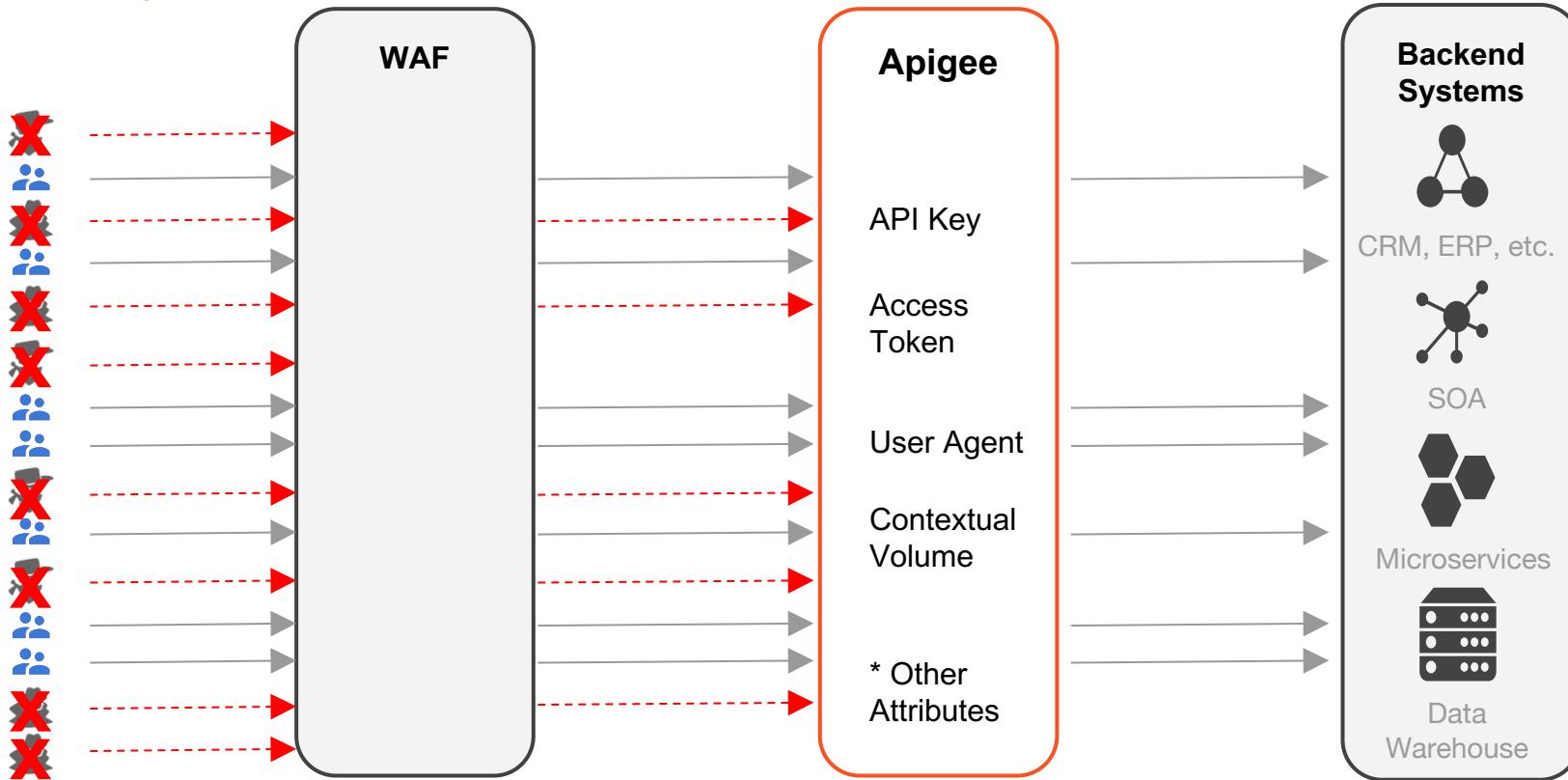


# Signs of Attack on APIs



- 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



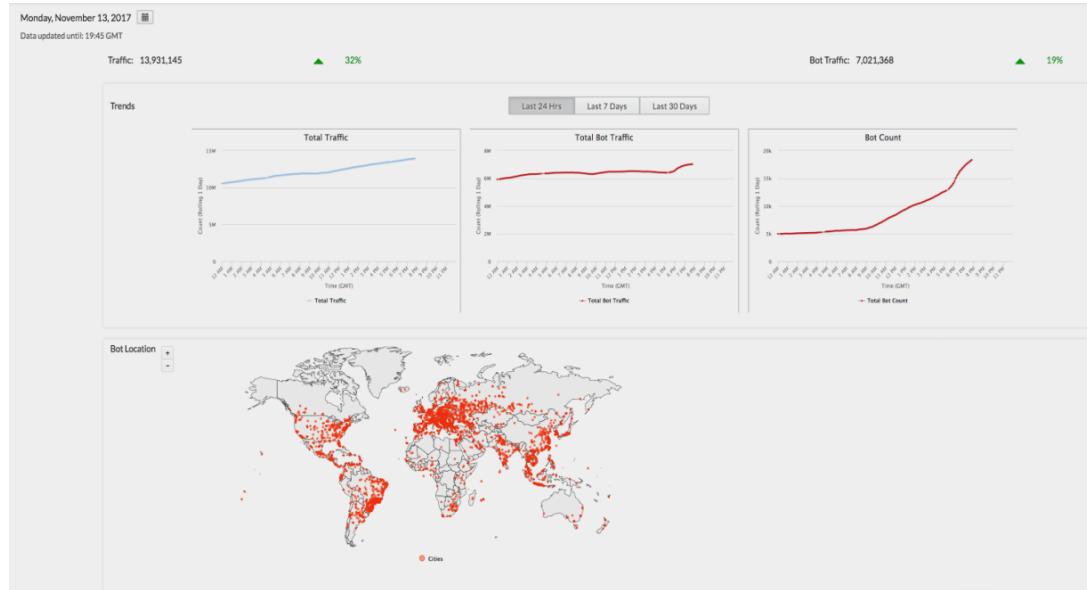
# Apigee Sense

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

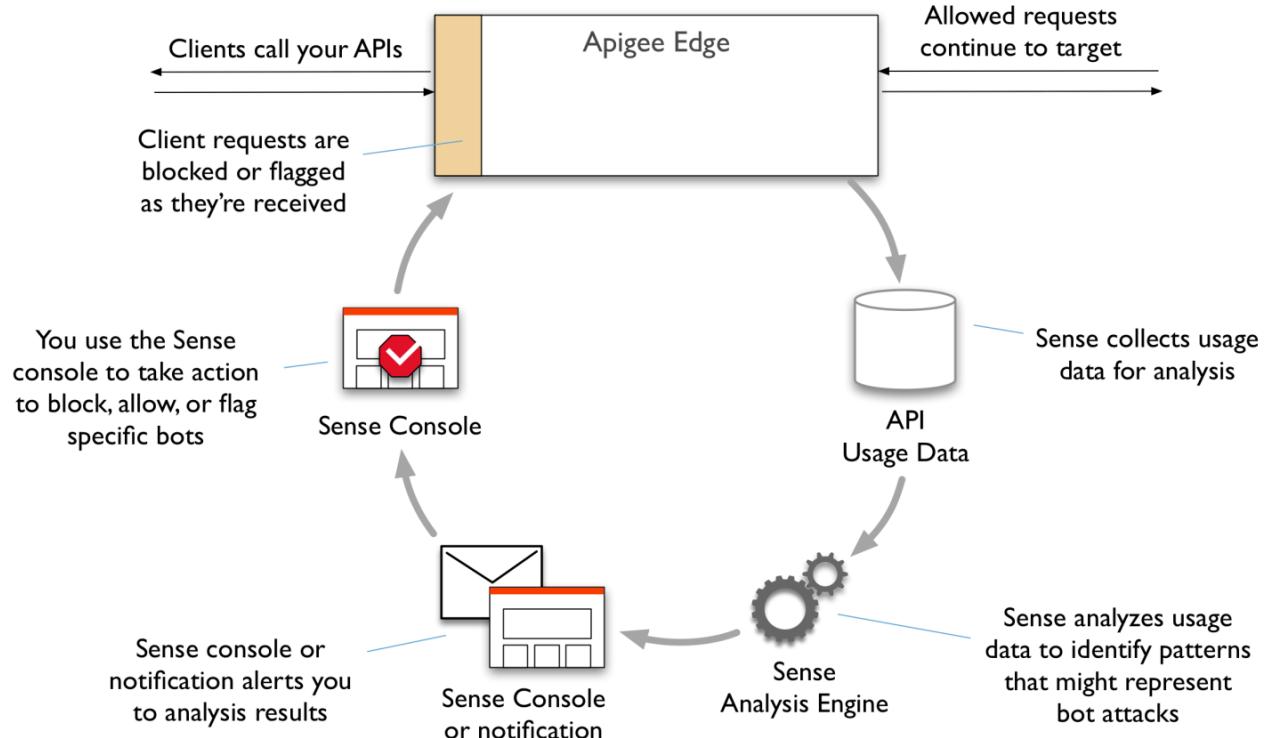
## Apigee Sense

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



# Closed Loop Protection:

## How Sense Works

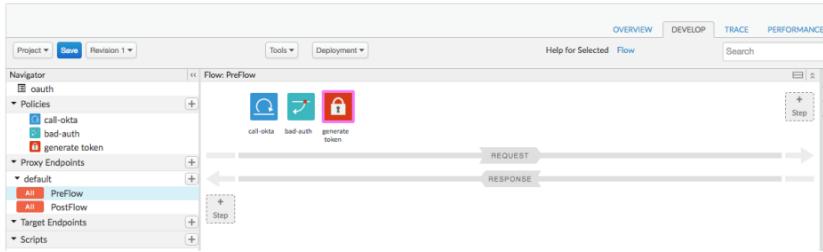


# Flexible Protection



Honeypot, Conditional Routing,  
Callouts, Logging

## Handle Flagged Requests via Configuration



01100  
10110  
11110



## Handle Flagged Requests via Code

```
Project Save Revision 1 Overview Develop Trace Performance Help for Selected Flow Search

Project Navigator Tools Deployment Help for Selected Project Save Revision 1 New New Policy Attach Policy Tools Deployment Node.js Logs Help for Selected Script

Navigator
  Policies
    - OAuth Validation
    - API Key Validation
    - CORS
    - CORSPreflight
    - DeveloperQuotas
    - XML2JSON
  Proxy Endpoints
    - default
      - All PreFlow
      - POST Create Offer
      - POST Add Product to Offer
      - GET Get Offer
      - GET Get Offer Details
  Scripts

Code: offerapi.js
<<
1 app.post('/', function(req,res){
2   var data = '';
3   req.on('data', function(chunk) {
4     data+=chunk;
5   });
6   req.on('end',function(){
7     var options = {'method':'POST','endpoint':'offers','body':data};
8     client.request(options,function(error,response){
9       if(error){
10         res.writeHead(200, {'Content-Type':'application/json'});
11         res.end(JSON.stringify(response));
12       }else{
13         res.writeHead(500,{'Content-Type':'application/json'});
14         res.end(JSON.stringify(options));
15       }
16     });
17   });
18 });
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
>>
```

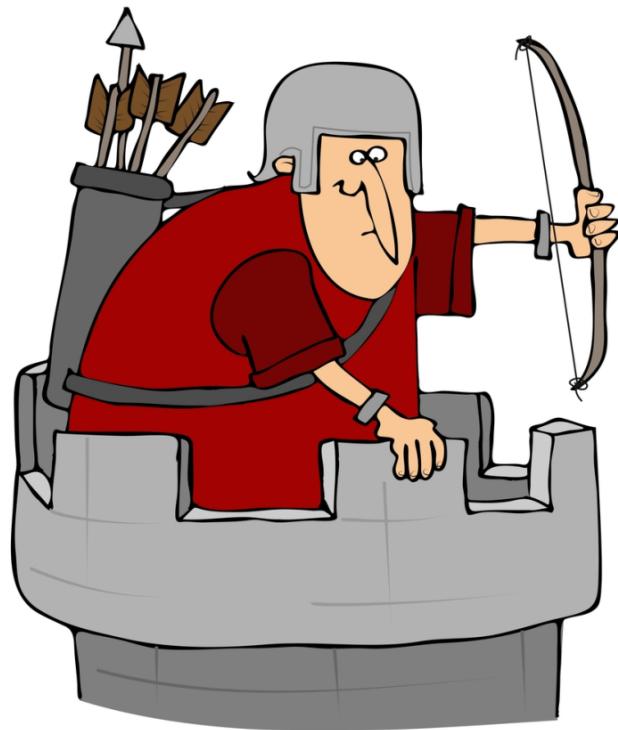
# A Secure Solution



# A Secure Solution... With Extreme Visibility



# The Best Defense Is A Good Offense



apigee

# Questions?