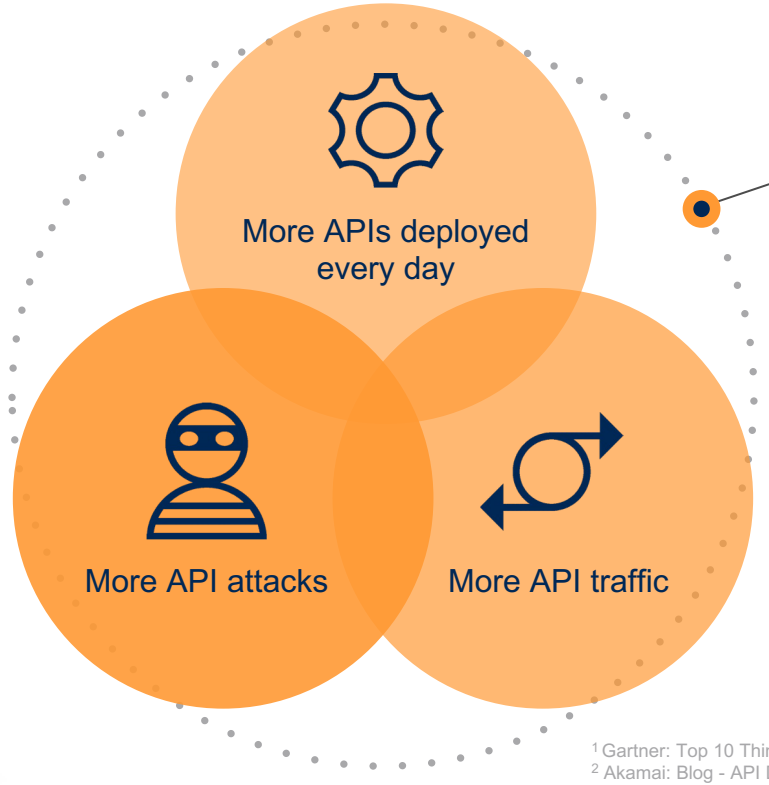

Akamai

API Threat Landscape: State of API Security

Garrett Weber
Field CTO

The API Security Environment



Existing application security solutions not built for APIs

By 2024, API abuses and related data breaches will nearly **double.**[1]

83%
of web traffic is APIs

[1] Gartner: Top 10 Things Software Engineering Leaders Need to Know About APIs
[2] Akamai: Blog - API Discovery and Profiling -- Visibility to Protection

API Risk Rapidly Expanding

4x

Increase in attacks targeting APIs over the last 6 months (Q1 2023)

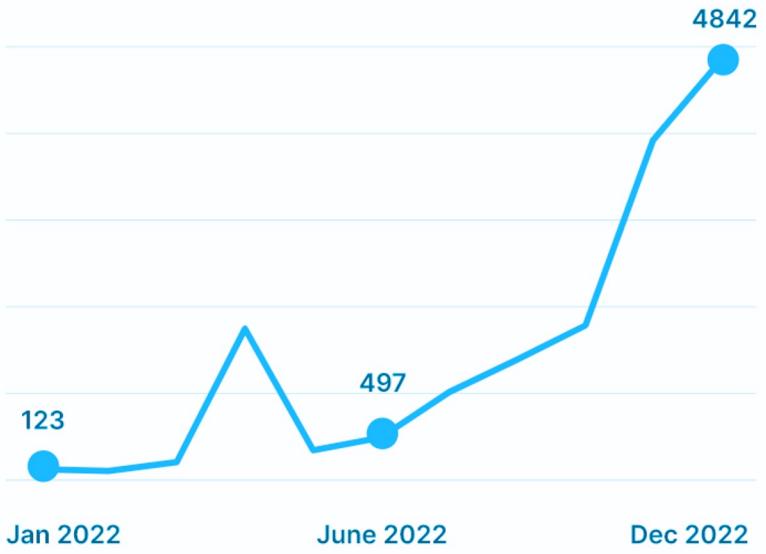
94%

Organizations experiencing security problems in production APIs (Q1 2023)

1/5

Organizations suffered a data breach as as result of security gaps in APIs (2022)

Unique Attackers Targeting Customer APIs[1]



Source: Salt Security (Customer Data Set)

Real World Attacks & Exposure Occurring Frequently

Large Service Provider

DATE: Disclosed in January ‘23 **(**occurred in November ‘22)

ATTACK: Undisclosed

OUTCOME: **37M customers** had personal and account information exposed, including names, account numbers, billing and email addresses, phone numbers, dates of birth, and information such as the number of lines on the account and plan features

Large Teleco

DATE: September ‘22

ATTACK: API Abuse | Unauthenticated API Server

OUTCOME: **10M customers** had records exposed, including driver's licenses, passports, Medicare ID numbers, in addition to names, phone numbers, and email addresses

Multiple Car Manufacturers

DATE: November ‘22 (research report published on vulnerabilities)

ATTACK: SSO misconfiguration, account takeover vulnerability

OUTCOME: **20 car manufacturers & 15M+ devices (mostly vehicles)** had API vulnerabilities that could have allowed hackers to perform malicious activity, ranging from unlocking, starting, and tracking cars to exposing customers' personal information

API Security Is a C-Suite Concern *Today*

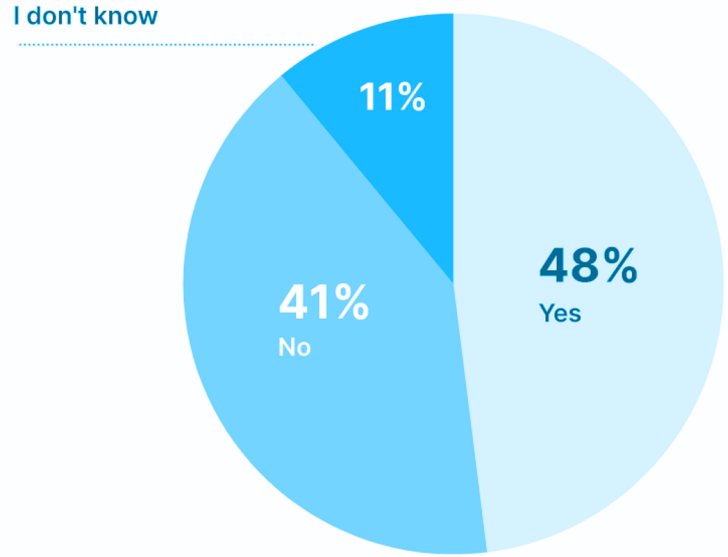
There is a **growing popularity of microservices** and the need for greater agility and flexibility in how applications are built and deployed

As more organizations move to microservices architecture, the **number of APIs they need to interact with is growing dramatically**

Most enterprises today do not even have visibility into their vast growing API estate, let alone the ability to detect vulnerabilities

Budget for API Security has already been established for many Global2000 enterprises

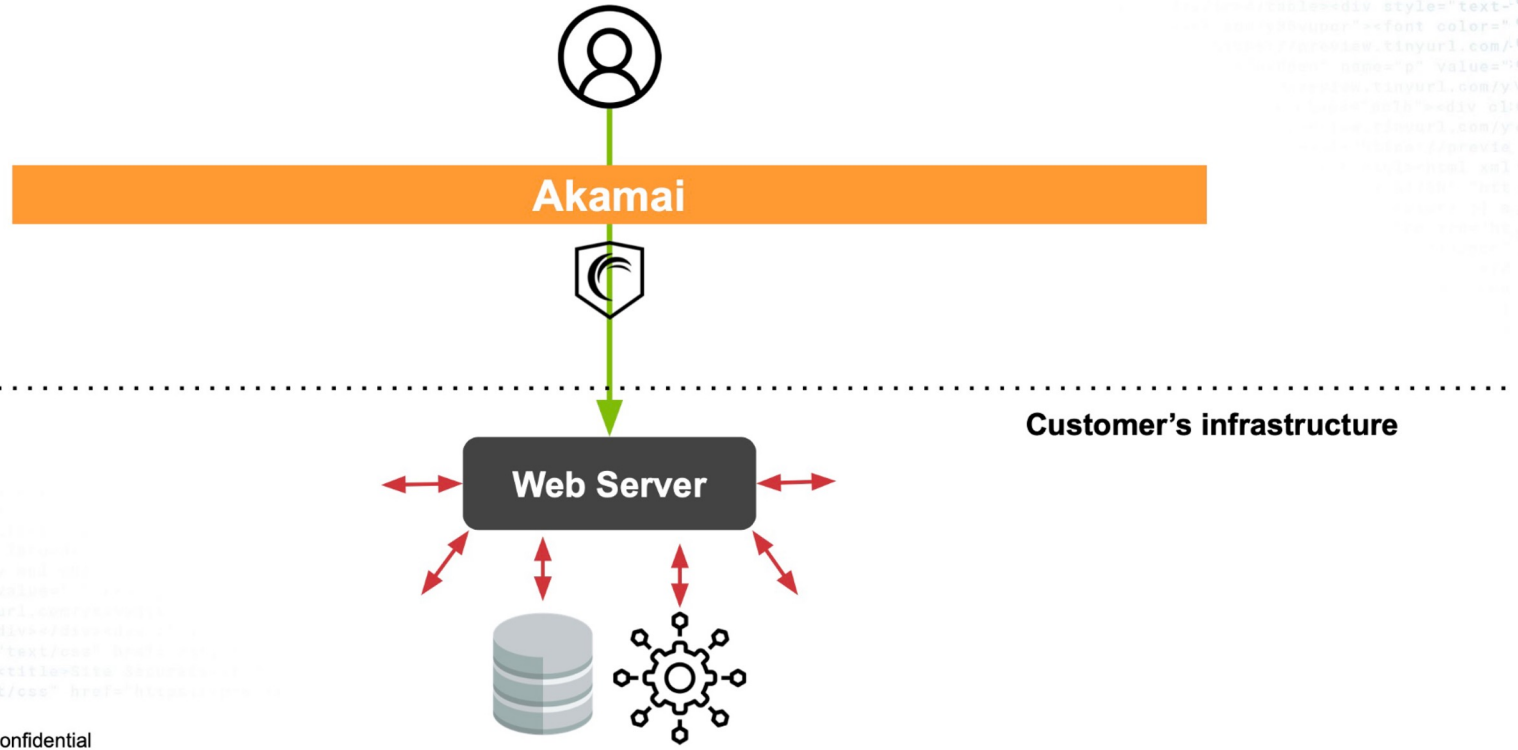
Is API Security a C-Level Discussion?



Source: Salt Security (Survey Respondents)

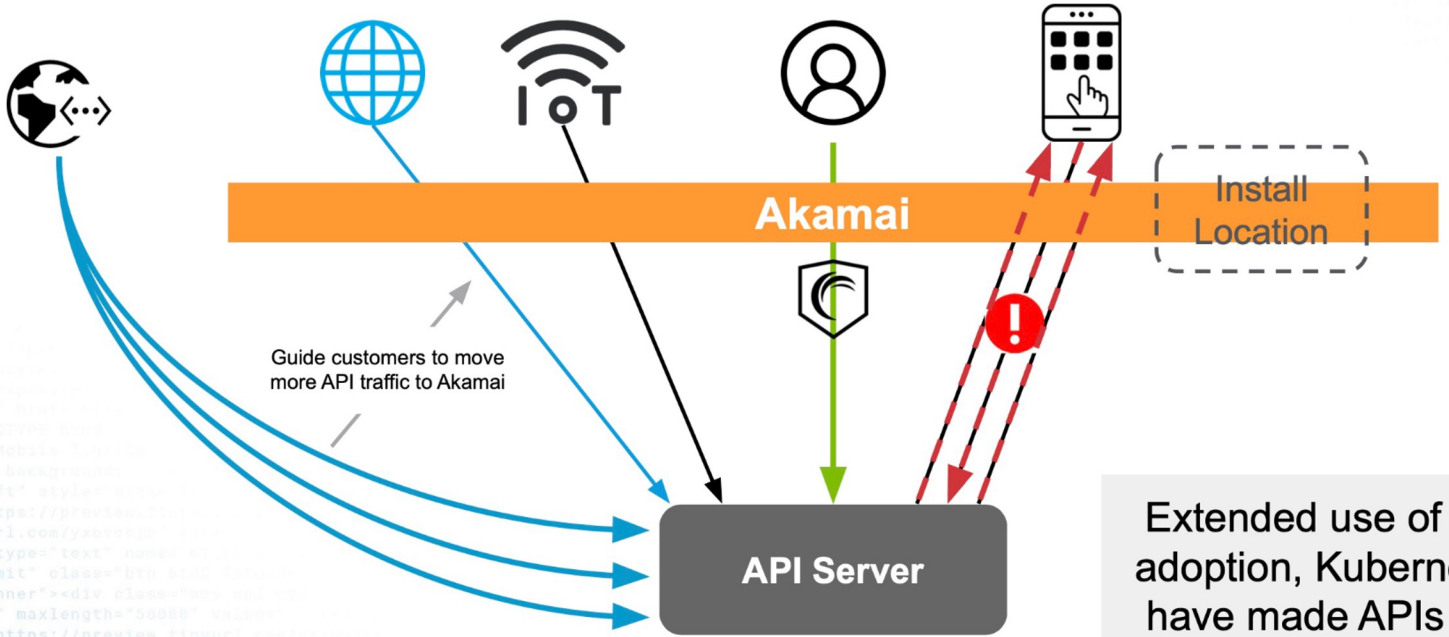
API Landscape - THEN

WAF was sufficient protection



API Landscape - NOW

The expanded attack surface requires broader protection

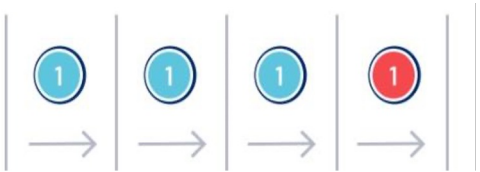


Extended use of Cloud native adoption, Kubernetes, IoT, etc. have made APIs so prevalent that's now how some people are writing web pages.

API attacks are evolving

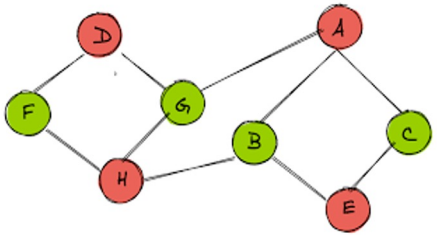
Past attacks

“One-and-Done”



Recent attacks

“Low-and-Slow”

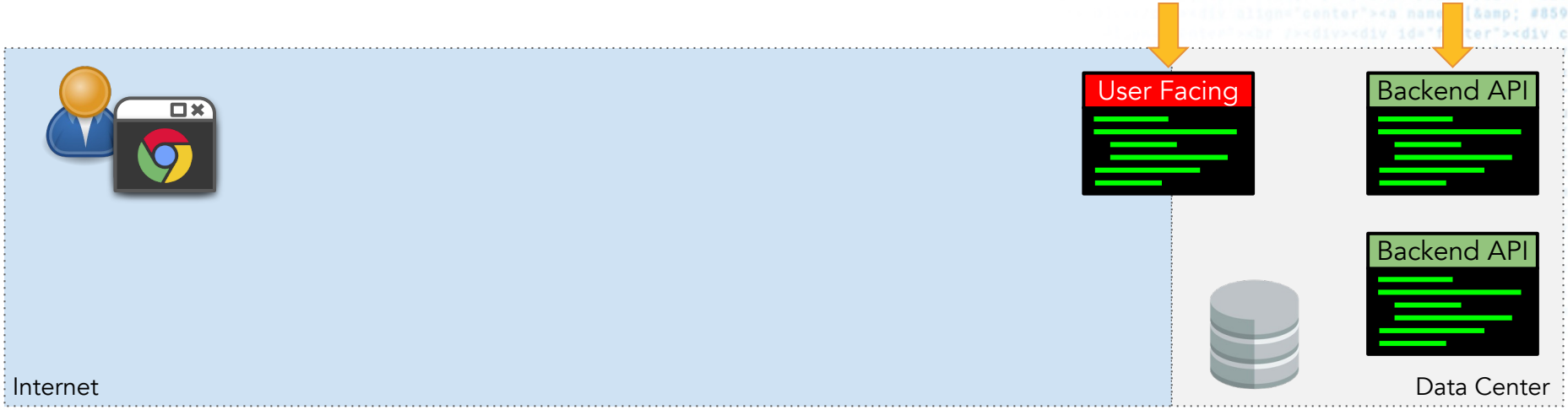


Current/future attacks

“Context-Based”

Akamai

Classic Web Architecture



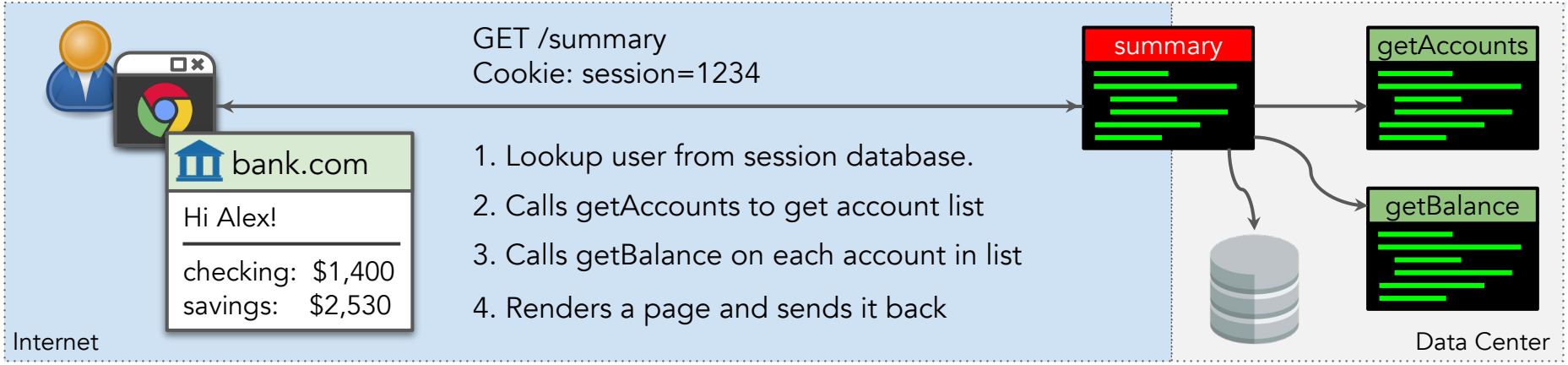
User Facing

- Takes a *single simple* request for a web page or resource and translates it into a *batch* of *highly complex* backend API calls in order to perform some business logic
- That business logic lives *within* the code located here
- Can be reached by malicious parties on the Internet

Backend API

- Performs some *piece* of *highly complex* business logic in concert with other *interdependent* Backend APIs on behalf of user facing code instructing it
- Cannot be accessed directly from the Internet
- Security comes from well-thought-out user facing code implemented by a capable developer

Classic Web Architecture - Example



User Facing

- Takes a *single simple* request for a web page or resource and translates it into a *batch* of *highly complex* backend API calls in order to perform some business logic
- That business logic lives *within* the code located here
- Can be reached by malicious parties on the Internet

Backend API

- Performs some *piece* of *highly complex* business logic in concert with other *interdependent* Backend APIs on behalf of user facing code instructing it
- Cannot be accessed directly from the Internet
- Security comes from well-thought-out user facing code implemented by a capable developer

Classic Web Architecture - Risk

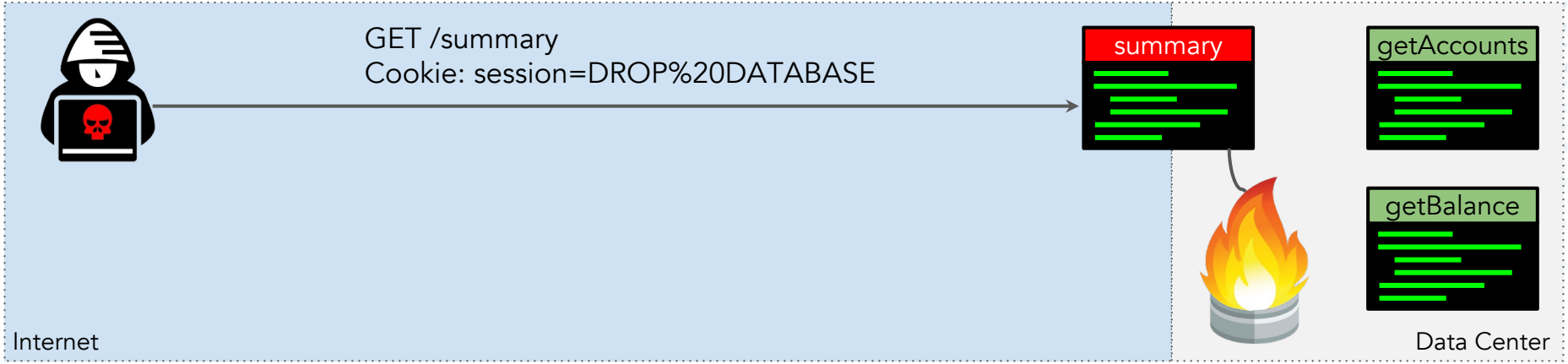
User Facing

- Takes a *single simple* request for a web page or resource and translates it into a *batch* of *highly complex* backend API calls in order to perform some business logic
- That business logic lives *within* the code located here
- Can be reached by malicious parties on the Internet

Backend API

- Performs some *piece* of *highly complex* business logic in concert with other *interdependent* Backend APIs on behalf of user facing code instructing it
- Cannot be accessed directly from the Internet
- Security comes from well-thought-out user facing code implemented by a capable developer

Classic Web Architecture - Risk



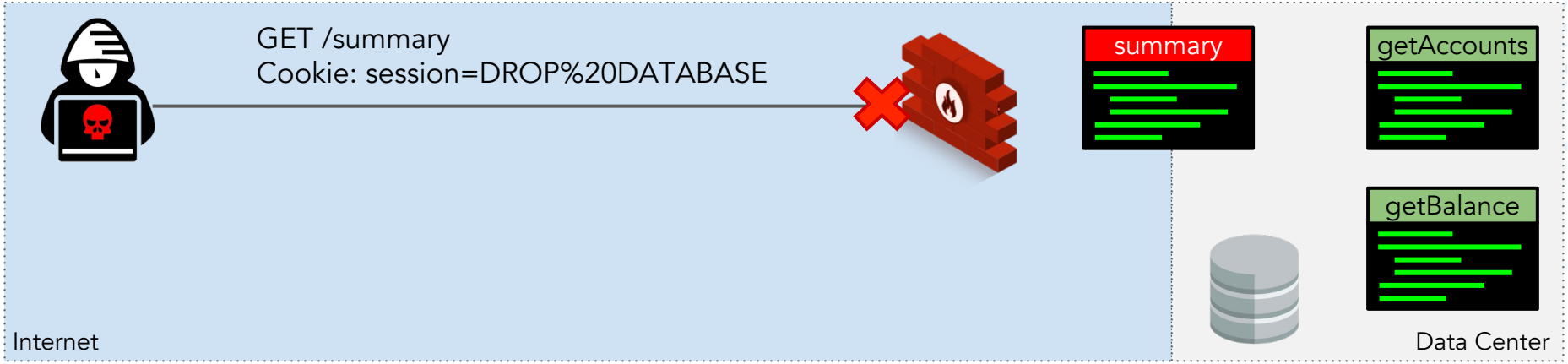
User Facing

- Takes a *single simple* request for a web page or resource and translates it into a *batch* of *highly complex* backend API calls in order to perform some business logic
- That business logic lives *within* the code located here
- Can be reached by malicious parties on the Internet

Backend API

- Performs some *piece* of *highly complex* business logic in concert with other *interdependent* Backend APIs on behalf of user facing code instructing it
- Cannot be accessed directly from the Internet
- Security comes from well-thought-out user facing code implemented by a capable developer

Classic Web Architecture - WAF Protection



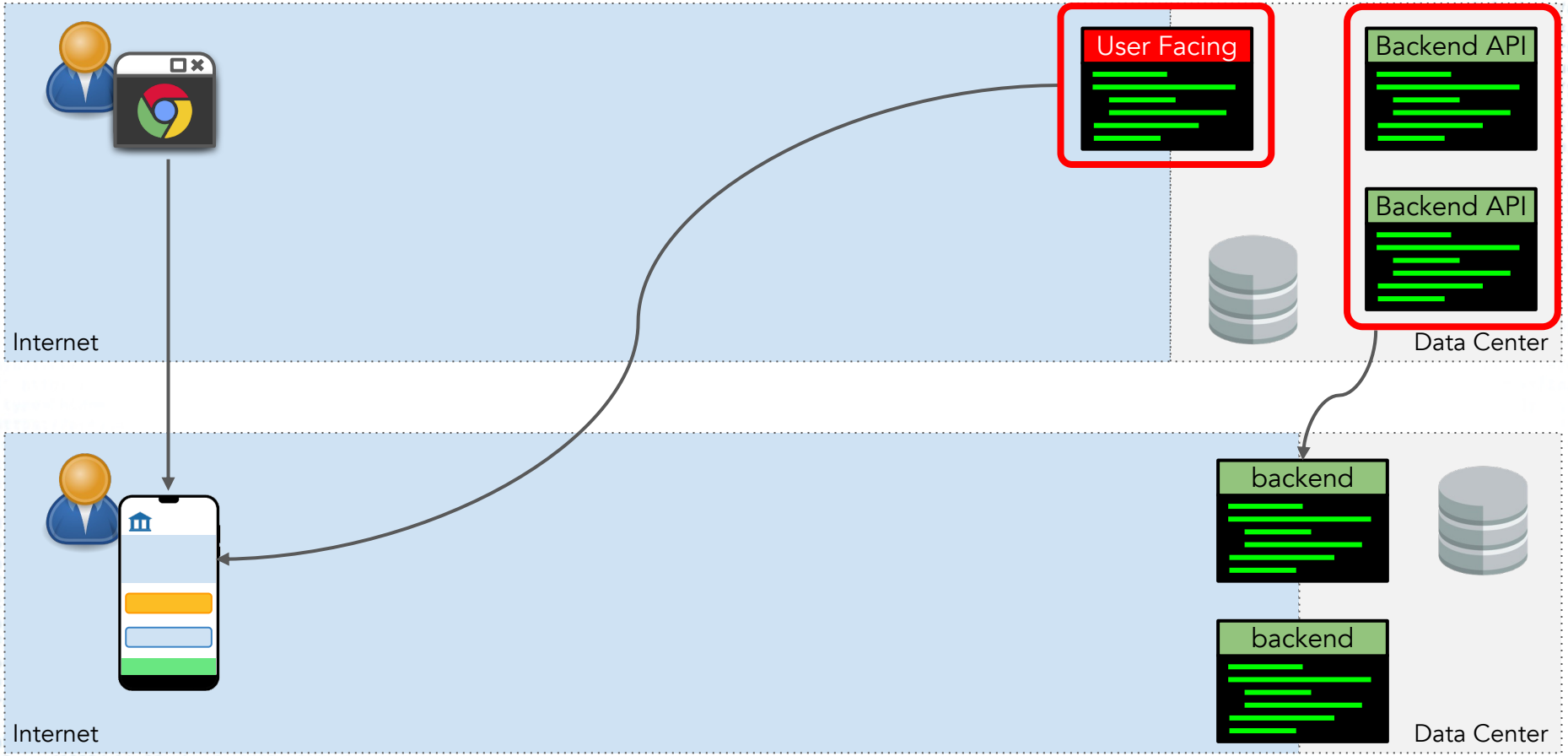
User Facing

- Takes a *single simple* request for a web page or resource and translates it into a *batch* of *highly complex* backend API calls in order to perform some business logic
- That business logic lives *within* the code located here
- Can be reached by malicious parties on the Internet

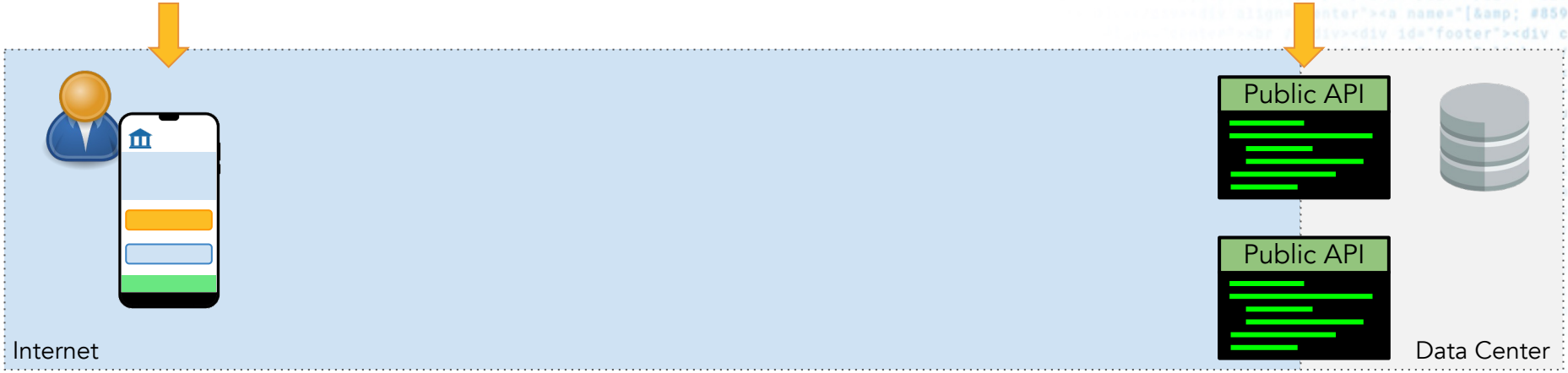
Backend API

- Performs some *piece* of *highly complex* business logic in concert with other *interdependent* Backend APIs on behalf of user facing code instructing it
- Cannot be accessed directly from the Internet
- Security comes from well-thought-out user facing code implemented by a capable developer

Modern API vs. Classic Web Architecture



Modern API Web Architecture



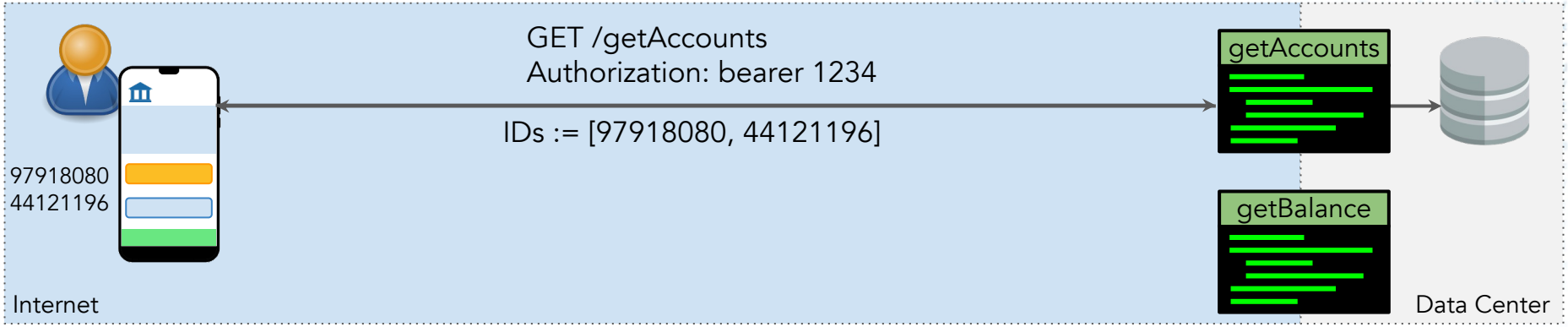
API Client

- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet - **DANGER!!!!**
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Modern API Web Architecture - Example



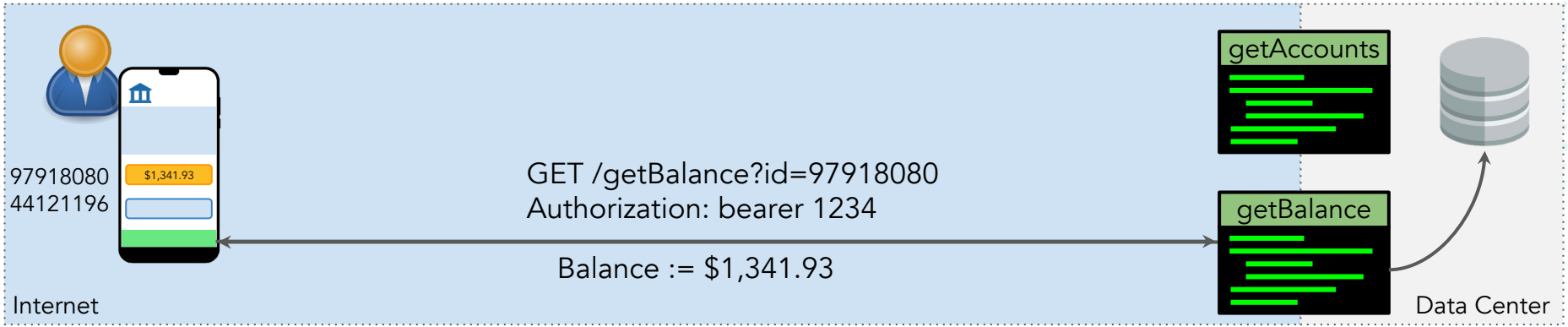
API Client

- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone - **DANGER!!!!**

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet - **DANGER!!!!**
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Modern API Web Architecture - Example



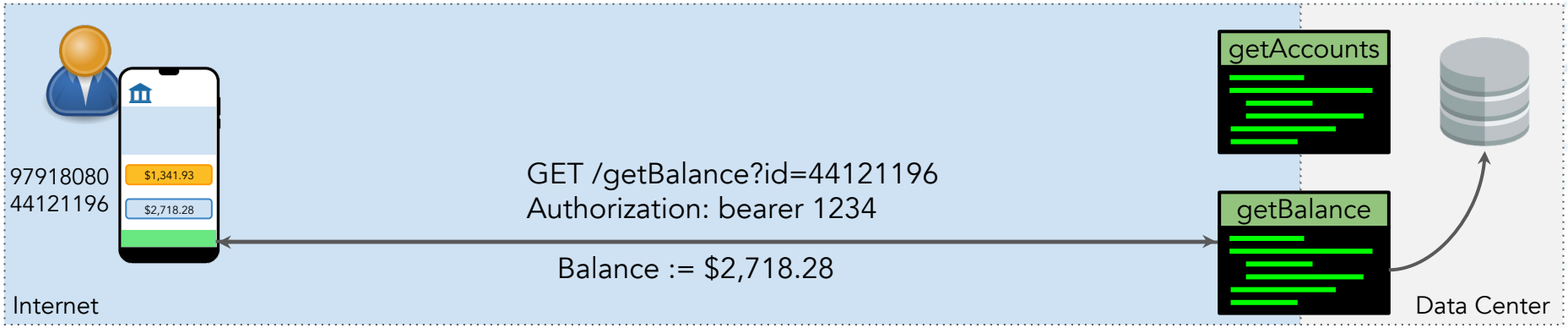
API Client

- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone - **DANGER!!!!**

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet - **DANGER!!!!**
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Modern API Web Architecture - Example



API Client

- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone - **DANGER!!!!**

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet - **DANGER!!!!**
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Modern API Web Architecture - Risk

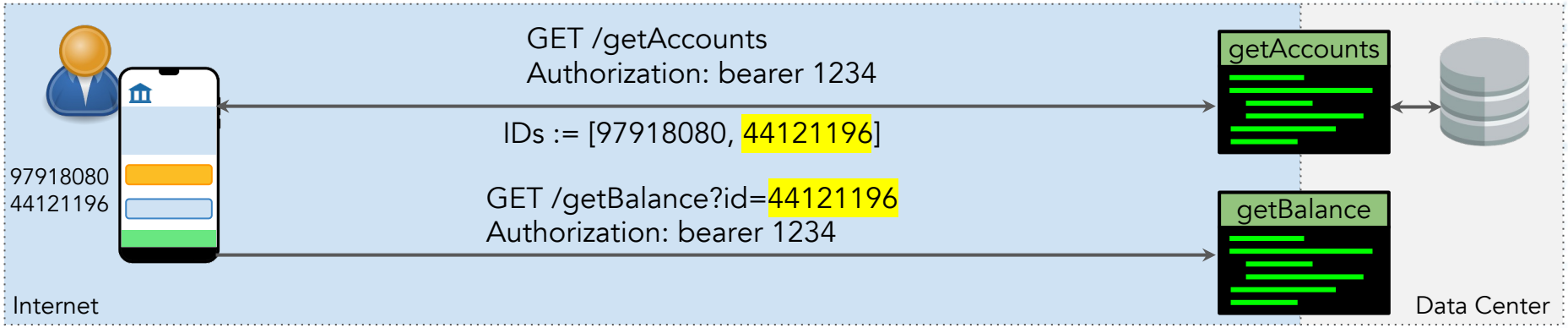
API Client

- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone - **DANGER!!!!**

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet - **DANGER!!!!**
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Modern API Web Architecture - Risk



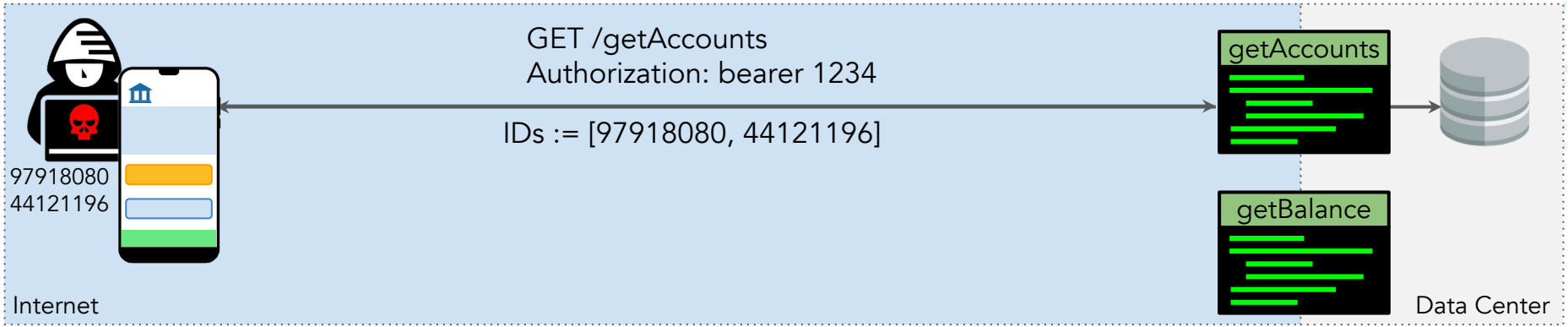
API Client

- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone - **DANGER!!!!**

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet - **DANGER!!!!**
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Modern API Web Architecture - Risk



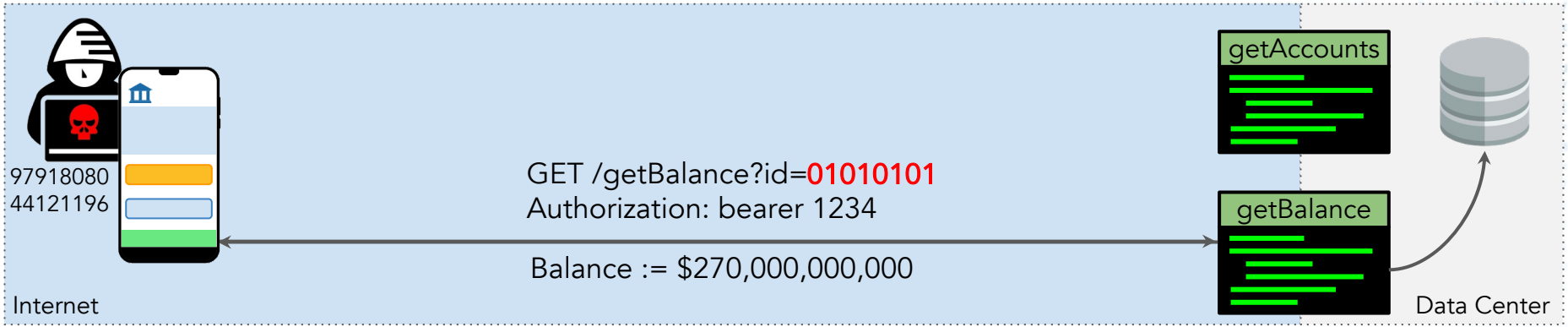
API Client

- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet - **DANGER!!!!**
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Modern API Web Architecture - Risk



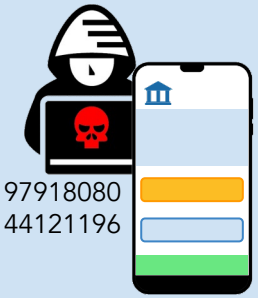
API Client

- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone - **DANGER!!!!**

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet - **DANGER!!!!**
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Modern API Web Architecture - Risk

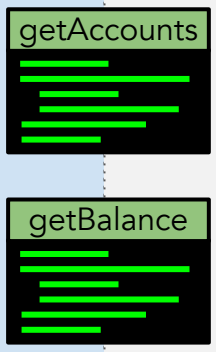


Internet

We were able to exfiltrate someone else's balance because the getBalance API didn't verify we owned the account we were querying!

This wasn't an issue in the classic web architecture. The developer wrote the user facing code so this couldn't happen and the API couldn't be accessed directly.

Now, with the API being publicly available, our malicious actor can do a lot more damage in more clever ways than ever before!



Data Center

API Client

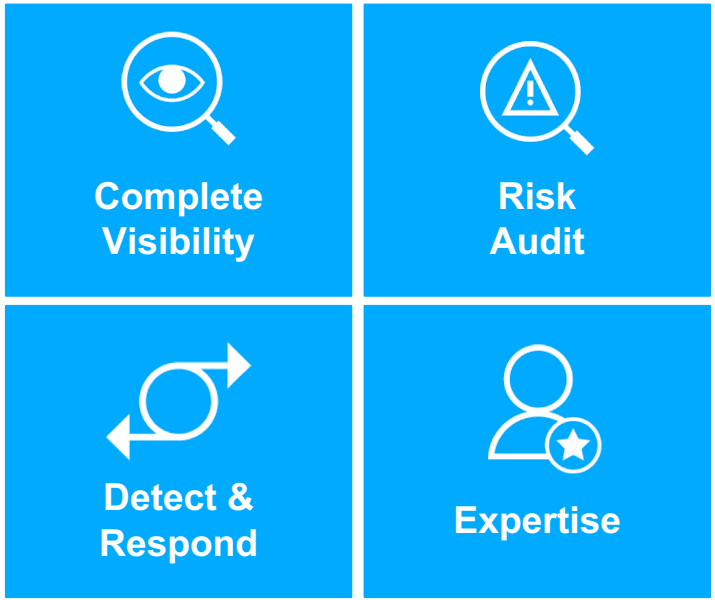
- The User Facing code moved here, out of the data center and onto other people's devices
- Can be a mobile app, partner app, devops tool, etc.
- Complex business logic lives here, but now is accessible and modifiable by anyone

Public APIs

- Exact same responsibilities as before, but now can be accessed directly from the Internet
- Security no longer comes from well-thought out business logic and code because both can now be manipulated!
- Complex interdependent relationships between API calls are now fully exposed!

Akamai Enhances API Security

Discover all APIs, assess their risk and respond to attacks



Combination makes it easy for customers to realize API security


Akamai