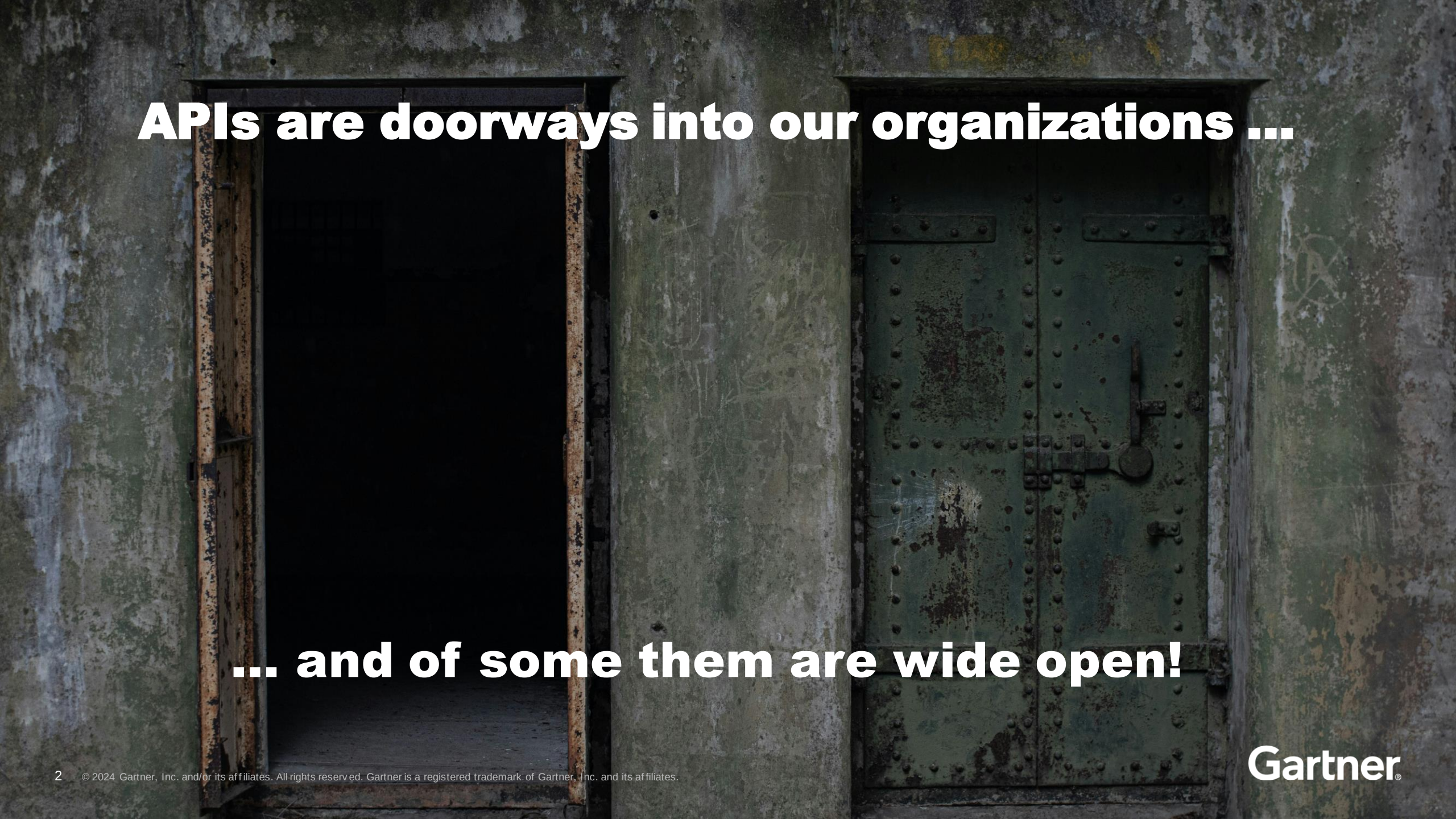
Protect Your APIs to Avoid Security Breaches

Dionisio Zumerle
@ LinkedIn

Gartner®



Gartner®

Key Issues

1. The API threat landscape
2. The elements of an API security strategy
3. API protection tools

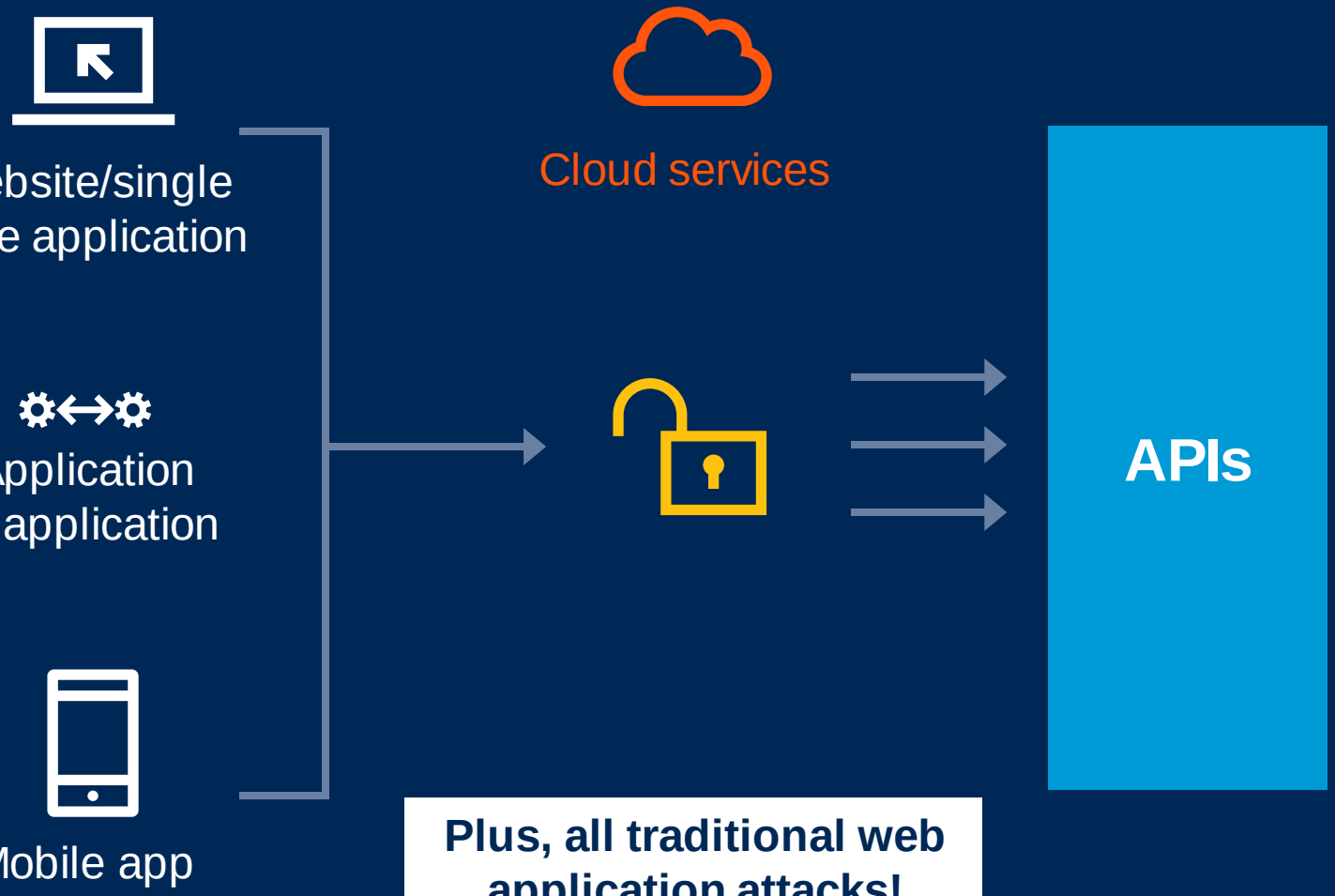
Gartner®

Key Issues

1. **The API threat landscape**
2. The elements of an API security strategy
3. API protection tools

How Are APIs Attacked?

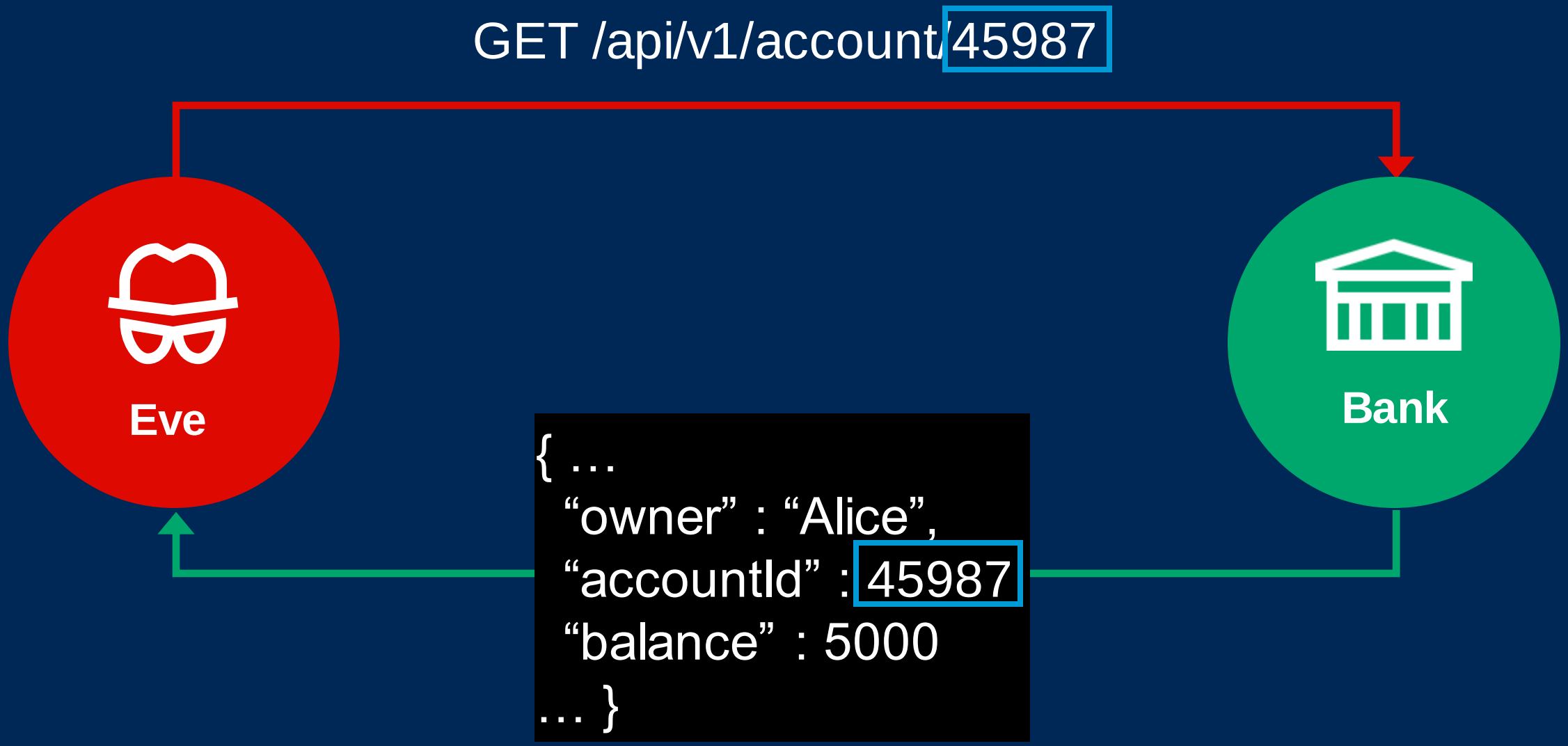
- Unsecured API credentials in repositories and storage
- Hard-coded API credentials in applications
- Unsecured API calls
- API logic flaws



Plus, all traditional web application attacks!

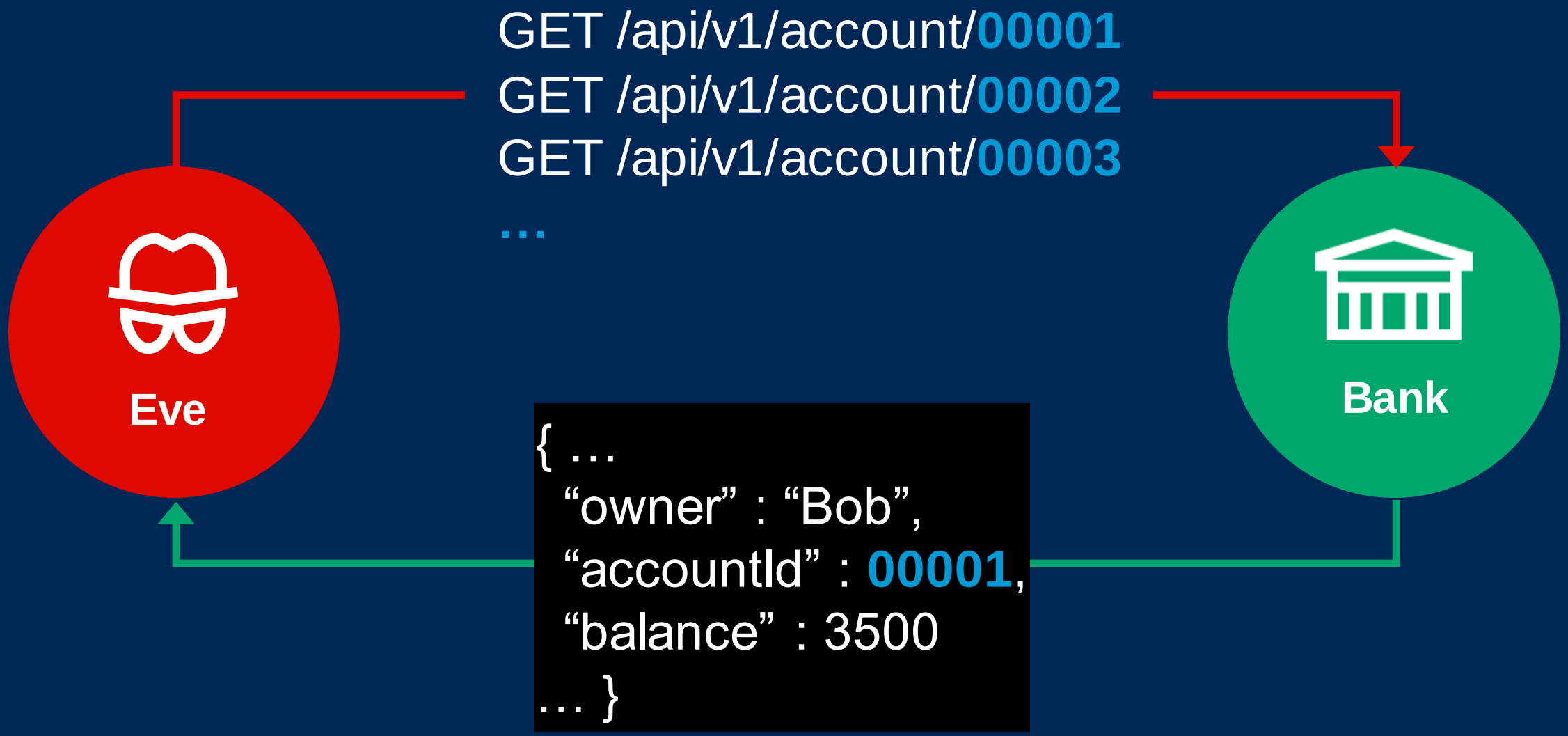
Gartner®

API Attack Example



Gartner®

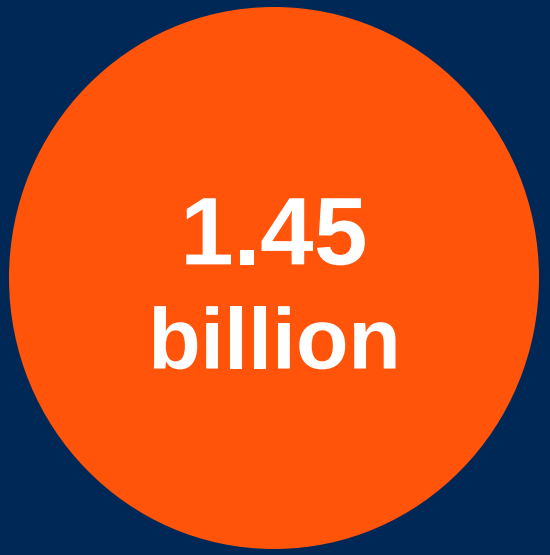
API Attack Example



Gartner®

What Have API Attacks Taught Us So Far?

API security is a real problem



Records breached in API attacks

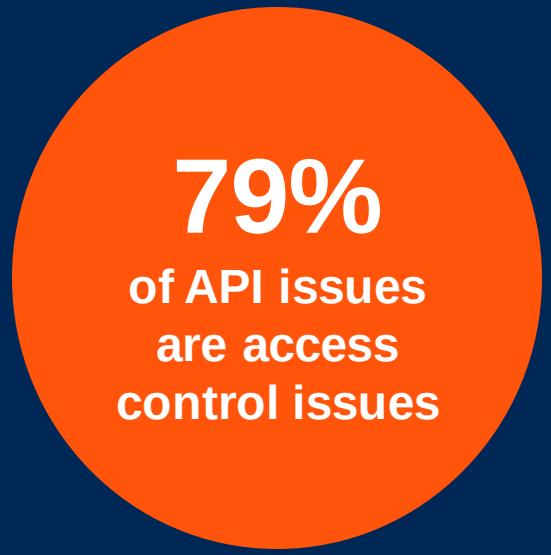
API blast radius is greater

In terms of records breached compared to the average cyberattack*

The security basics are still the basis

Injection vulnerabilities make up 25% of all API-related vulnerabilities

Access control is “key”



Authentication or authorization is the primary attack vector in 79% of API incidents**

Source: The State of API Security, FireTail (2023)
** Data does not yet include MoveIT wave of attacks based on injection

Gartner®

AI and APIs are symbiotic. Your API security impacts your AI security, and vice-versa.

Gartner®

Key Issues

1. The API threat landscape
2. **The elements of an API security strategy**
3. API protection tools

Gartner®

Your API Security Building Blocks

Authentication of the API client (e.g., mobile app)	JSON/XML element encryption	Quota management/ traffic throttling
Content inspection	Content validation (JSON schema, XML schema)	Tokenization of sensitive information (e.g., patient number)
Automated attack/bot detection	Usage plan management	Data transformation
Store audit logs	Digital signature	API key authentication
Fine-grained authorization	OAuth scope management	Transport security (TLS/SSL)
Integration with access management	XML/SOAP security (WS-security, etc.)	Alerting (including to SIEM)

Gartner®

How to Set Up an API Security Program?

Discovery

Inventory first- and third-party APIs in usage or in development

Posture management

Identify API misconfigurations or insecure implementations and suggest and prioritize remediations

Testing

Identify API vulnerabilities by using testing techniques such as DAST and fuzzing

Runtime protection

Identify known malicious or suspicious behavior in API traffic and events

Access control

Implement fine-grained API access control

Main stakeholders to engage with:
Enterprise architecture, infrastructure and operations, security operations, application development

Gartner®

3 Levels of API Credentials

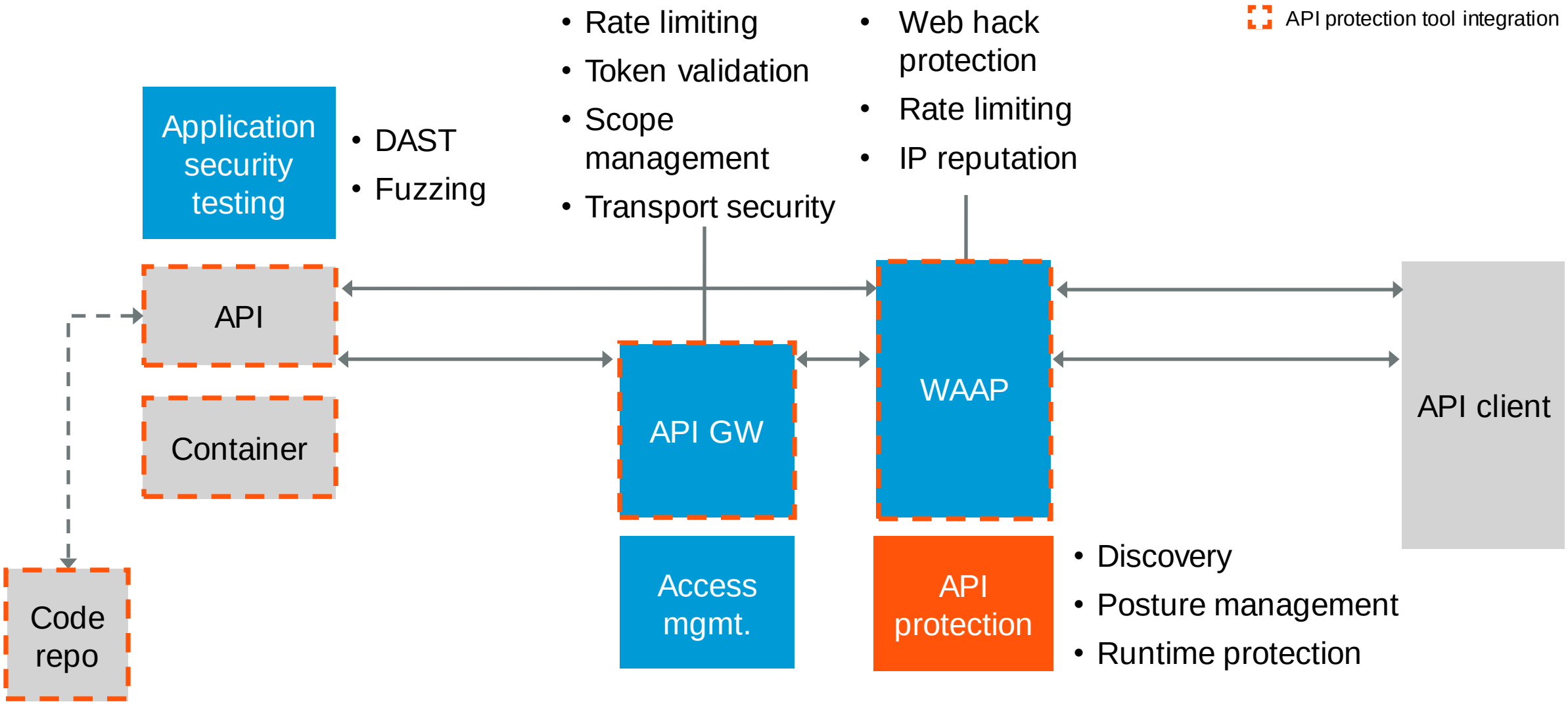
Gartner®

Key Issues

1. The API threat landscape
2. The elements of an API security strategy
3. **API protection tools**

Gartner®

Delivering API Protection



API Protection Tools

Sample vendors:

crunch
Akamai
APIsec
CEQUENCE SECURITY
CLOUDFLARE
datatheorem
f5
noname
SALT
TRACEABLE

Gartner

Recommendations

- Create and disseminate an API security policy to raise awareness and spread knowledge.
- Perform API discovery and posture management with a focus on access control issues.
- Start from your incumbent vendors and only then look at stand-alone products.
- Prepare for the additional workload that behavior-based API runtime protection will create.

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **Market Guide for API Protection**
  Dionisio Zumerle, Aaron Lord and Others
- **Research Index: Everything You Should Do to Address API Security**
  Dionisio Zumerle
- **API Security Maturity Model**
  William Dupre and Gary Olliffe
- **Reference Architecture Brief: API Access Control**
  Erik Wahlstrom

Access to Gartner research is subject to individual subscription type and product entitlements.