

# Protect Your APIs to Avoid Security Breaches

Dionisio Zumerle  
@ [LinkedIn](#)

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

**Gartner**®



**APIs are doorways into our organizations ...**

**... and of some them are wide open!**



# Key Issues

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



# Key Issues

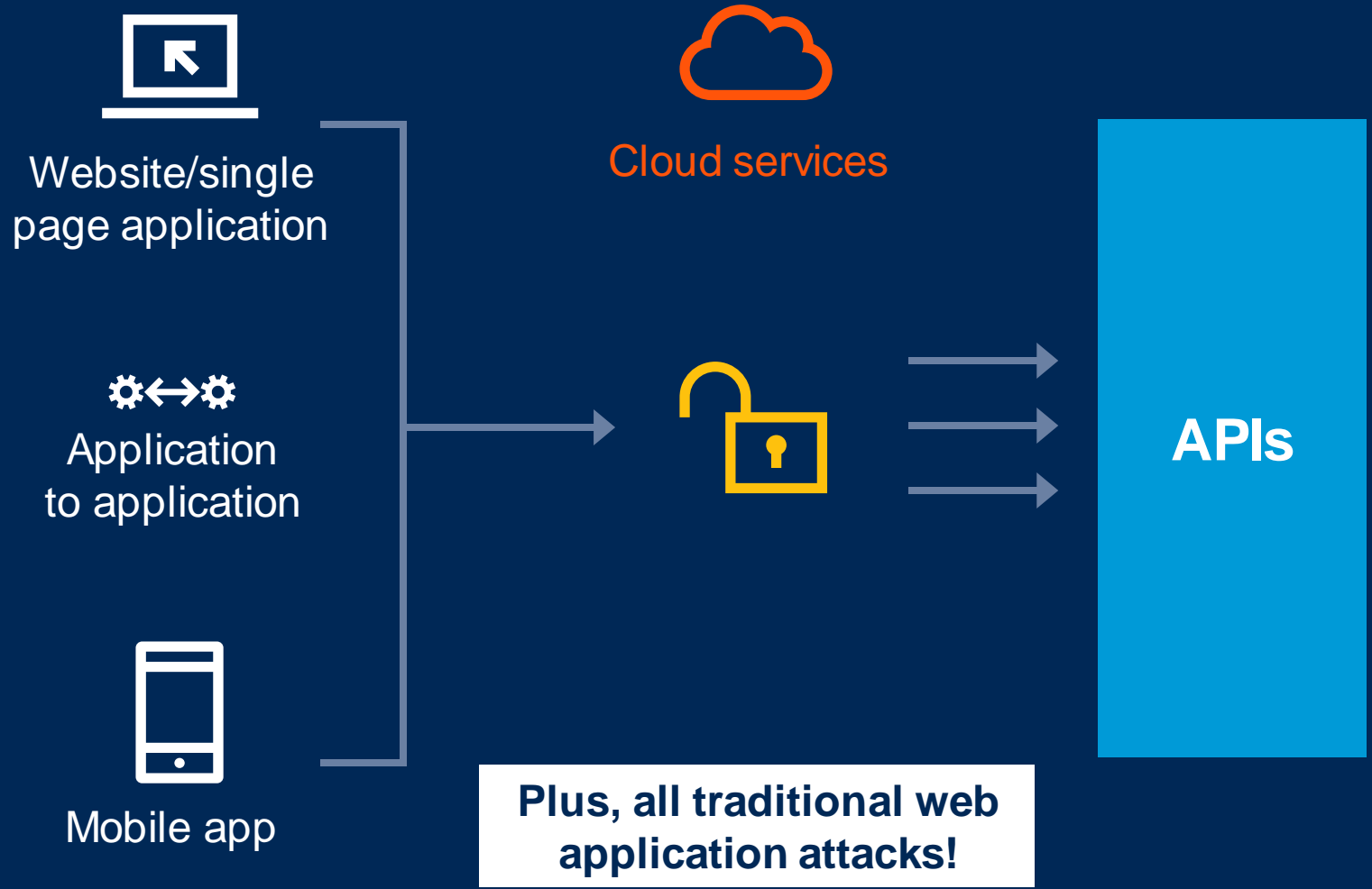


## 1. The API threat landscape

- 2. The elements of an API security strategy
- 3. API protection tools

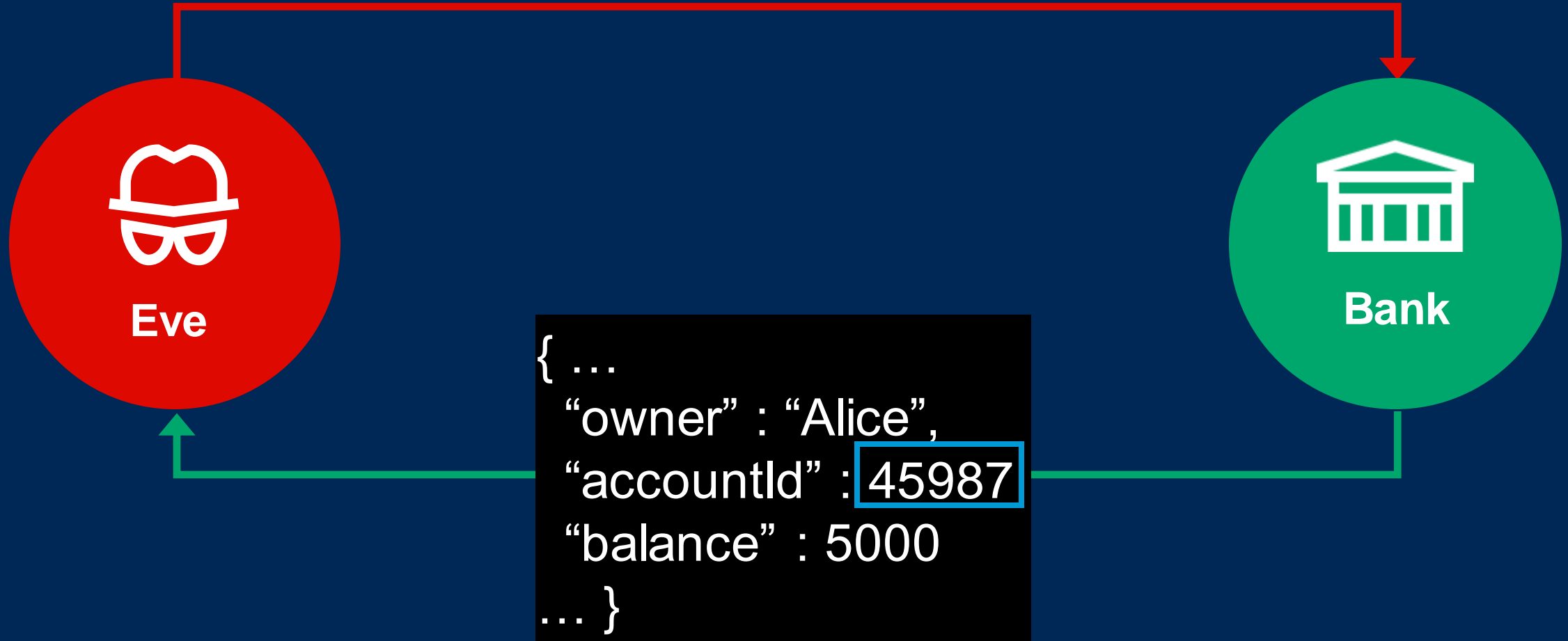
# How Are APIs Attacked?

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

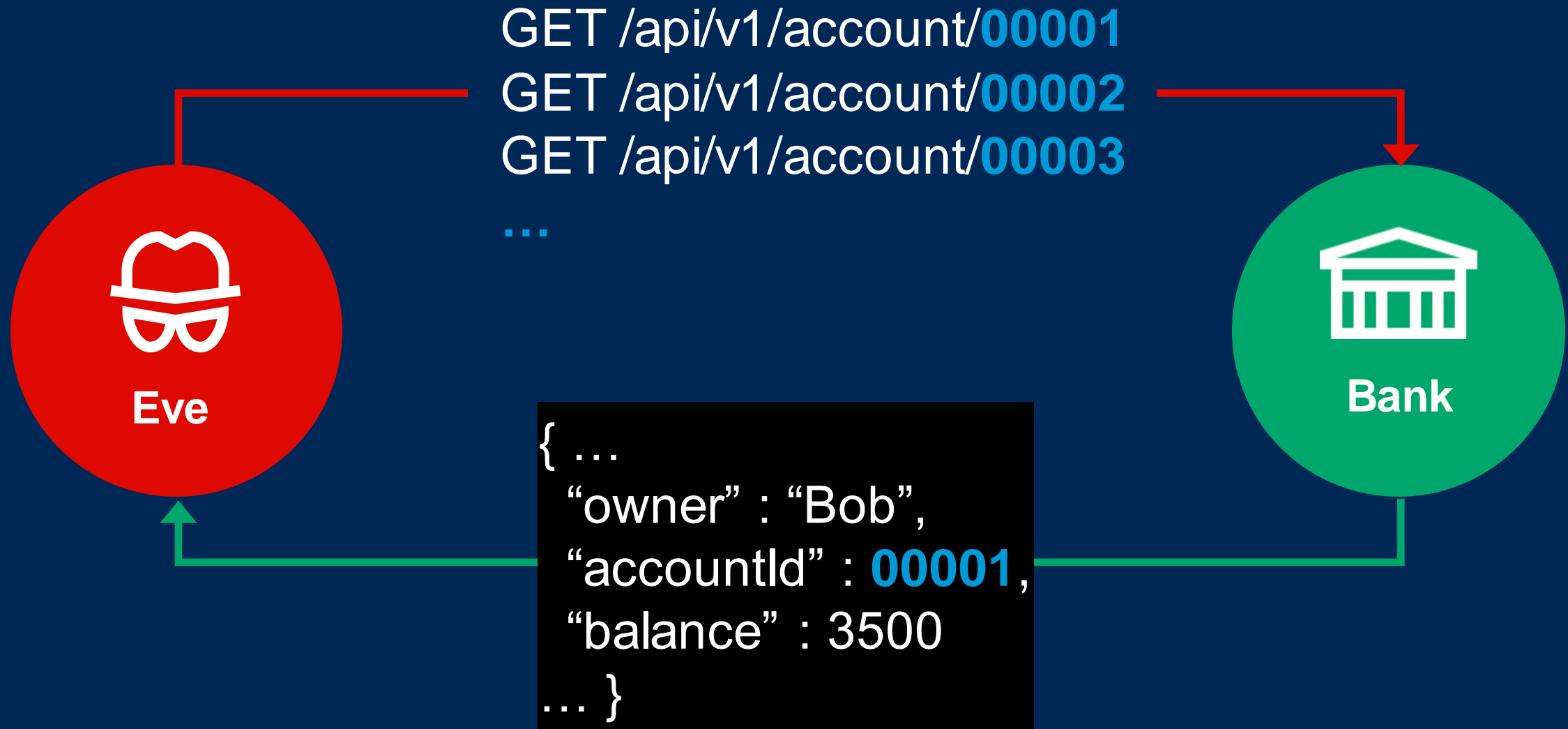


# API Attack Example

GET /api/v1/account/45987



# API Attack Example





# What Have API Attacks Taught Us So Far?

API security is a  
real problem

**1.45  
billion**

Records breached  
in API attacks

API blast radius  
is greater

At least  
**10x**  
greater  
damage

In terms of records  
breached compared to  
the average cyberattack\*

The security basics  
are still the basis

**1 out  
of 4**  
vulnerabilities  
is injection

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

Access control  
is “key”

**79%**  
of API issues  
are access  
control issues

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





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

# Key Issues

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



# 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)

# 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



# 3 Levels of API Credentials

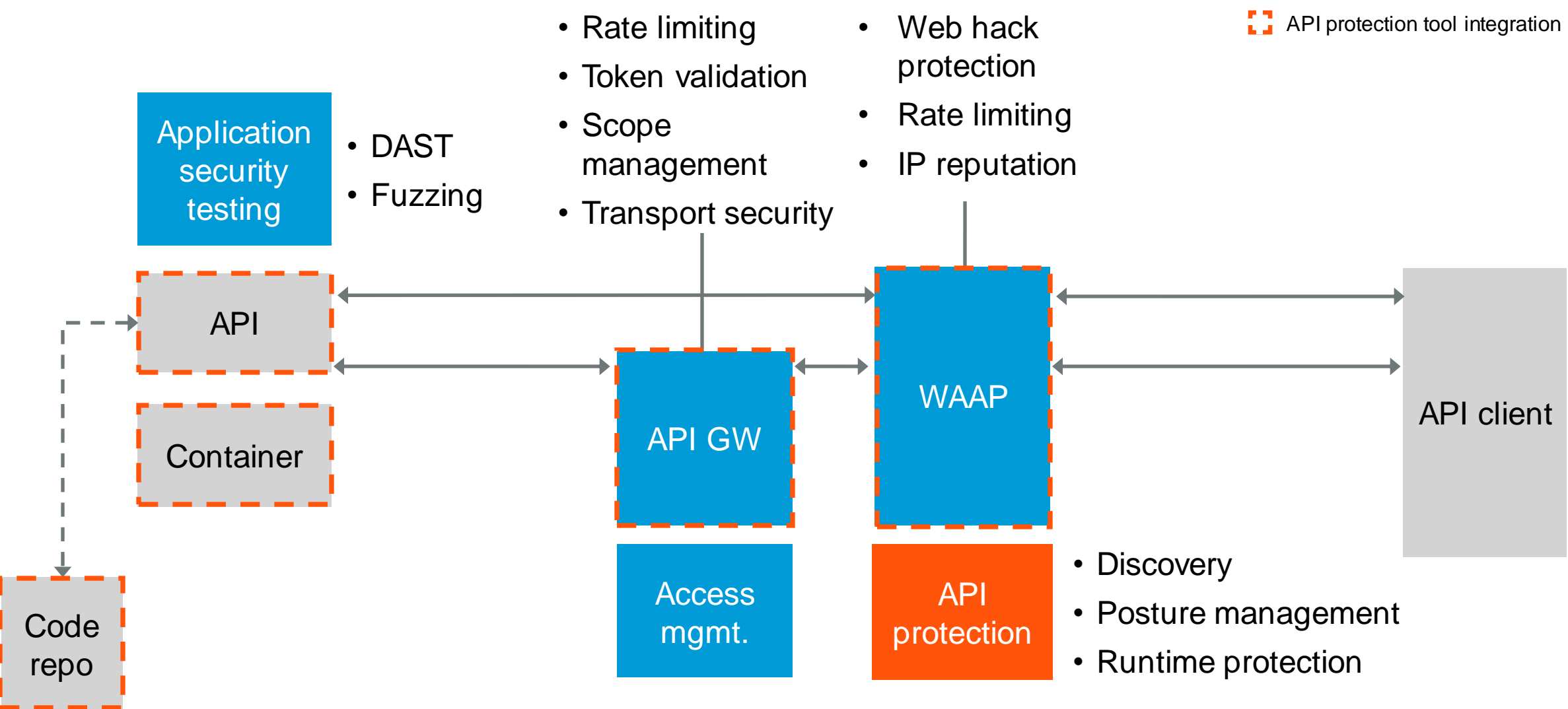


# Key Issues

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



# Delivering API Protection



# API Protection Tools



Sample vendors:





# 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](https://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